NE-ONE™

User and Administration Guide

Revision 8

Reproduction

Warranty

All information is believed to be true and correct at time of print. Information in this document is subject to change without notice and does not represent a commitment on the part of Calnex.

Calnex makes no warranties, expressed or implied of any kind with regards to this material or its products, including the implied warranties of merchantability and fitness for a particular purpose.

Calnex shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance or use of this material or supplied products.

Please note: there are no internal serviceable parts in any equipment supplied by Calnex. Opening the hardware voids all warranties.

Trademarks

Calnex NE-ONE is a registered trademark of Calnex. Other trademarks are the property of their respective owners.

Table of Contents

Chapter 4: Installation and Configuration

Chapter 5: Ports and Services Management

Chapter 6: User Administration

Chapter 7: System Maintenance

Chapter 8: General System Procedures

Chapter 9: Creating and Running Point-to-Point Networks

Chapter 10: Creating and Running Multi-Point Networks

Chapter 11: Creating and Running Scenarios

Chapter 12: Statistics, Graphing, Reporting and Packet Capturing

Chapter 16: The LCD Panel

Appendix 1: Specifying Expressions

Appendix 2: Available Functions

Appendix 3: Available Link Types and Link Sub-Types

CHAPTER 1 ABOUT THIS TECHNICAL PUBLICATION

1. INTRODUCTION

This User and Administration Guide describes how to administer and use the NE-ONE, and is intended for admin user and end users.

2. ASSOCIATED DOCUMENTS

This User and Administration Guide refers to the following documents:

- *NE-ONE AWS Installation Guide*
- *NE-ONE Azure Installation Guide*

3. DOCUMENTATION CONVENTIONS

The following conventions are used in the text of this document to distinguish particular types of information:

3-1. Special emphasis in text

The following table shows the types of emphasis used to distinguish particular elements in the text of this document:

Font Convention	Identifies
Bold	Graphical user interface (GUI) elements such as buttons, tiles, panels, menu items, fields, radio buttons, check boxes, etc. Command names, variable values, field values and executables.
Italic	Document names, external references to other documents, internal references and hyper links.
`Monospace`	File names, pathnames, variable names, File contents, program output, code examples, and command line interface (CLI) examples / syntax.
`Monospace bold`	Commands and text that users are instructed to enter at the keyboard.

3-2. User interface conventions

The following conventions are used:

- All button options are represented with the word on the button in bold font.

  For example, the Next button is represented as **Next**.

  All menu options are represented with the option name in bold. For example, the Connect option is represented as **Connect**.
- When an instruction to select a menu option is given, the path to the menu option is represented with the menu options in bold typeface and each level separated by a greater than symbol (>).

  For example, to select the Open command from the File menu you will be instructed to select the **File > Open** command.

3-3. Entering and typing

Depending on the situation, you may be instructed to type or enter a command or string of text. When you are required to press the return key after typing a command or string of text, the actual command or string of text is prefixed by enter or entering. For example, in a command line interface (CLI) you are instructed as follows:

Change to the `temp` directory by entering:

`cd temp`

In some cases you are not required to press the return key after typing a command or string of text, for example:

- field entries in a graphical user interface (GUI)
- typing a menu option in a CLI which does not require you to press the return key.

In these cases you are instructed to type the appropriate command or string of text. For example, to specify your name in a GUI field you are instructed as follows:

Type your first name in the **First Name** field.

3-4. Mouse Buttons

It is assumed that the left mouse button is the primary one.

3-5. Definition of Notices and Notes

! Notice:

Used for instructions to the user to prevent damage to property.

Note:

Used to draw attention to information that is important for the user to know.

4. CONTACT INFORMATION

If you need to contact Calnex regarding the installation or use of the NE-ONE, please do so using the following channels:

Postal Address	Calnex Solutions plc Oracle Campus Linlithgow West Lothian EH49 7LR United Kingdom
Telephone (Calnex EMEA and other regions)	+44 (0)1799 252 200
Telephone (Calnex Americas)	+1 888-448-4366
Global support email	support@ne-one.com
Website	http://www.ne-one.com

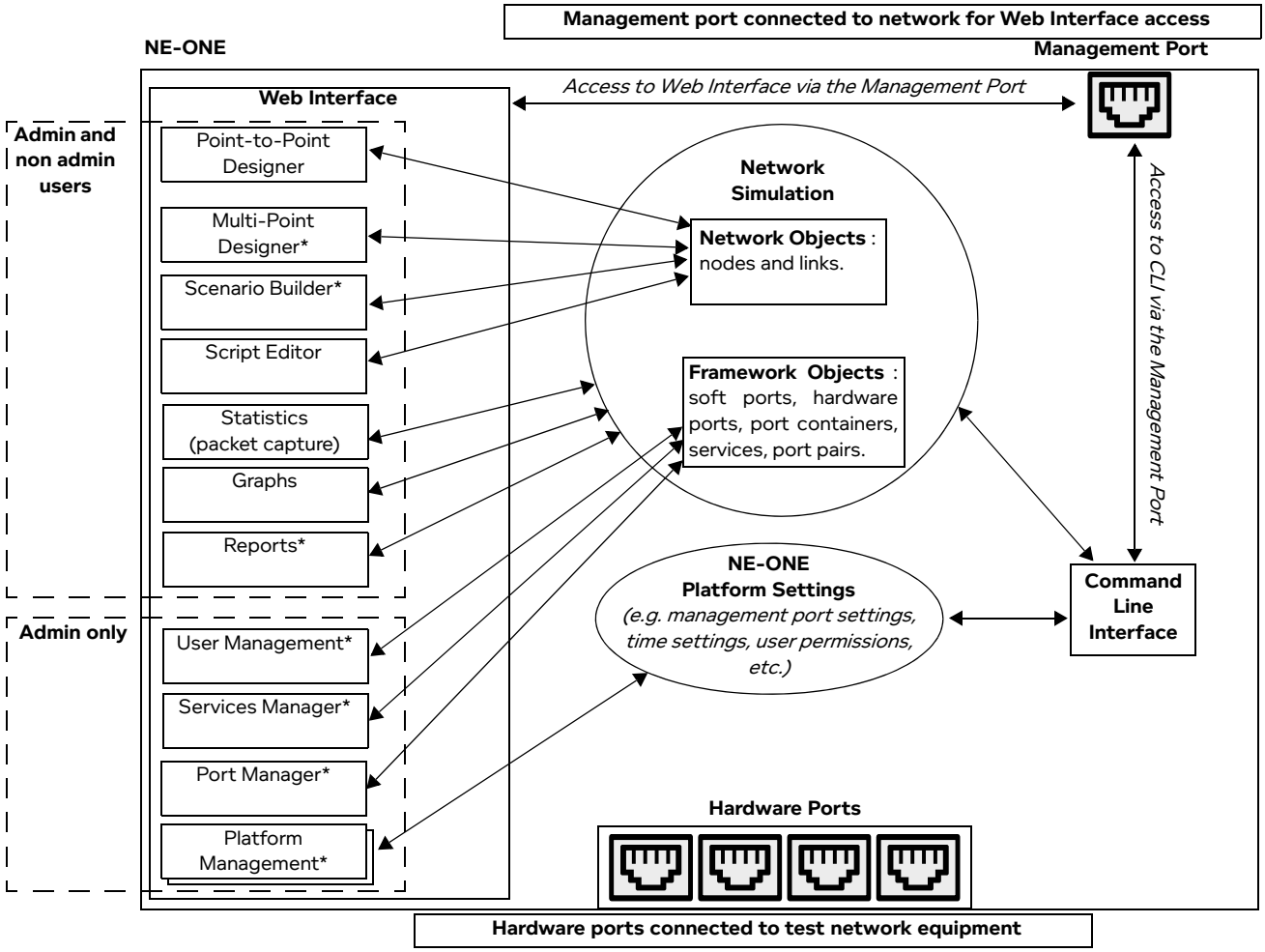
CHAPTER 2 NE-ONE OVERVIEW

1. INTRODUCTION

The NE-ONE is a flexible and easy to use network simulator letting you create Software Defined Test Networks (SDTNs) that simulate a wide range of network conditions, which can be used for testing real world applications. The NE-ONE lets you fully test your real world applications over the SDTN before deploying them in a real world network, ensuring that they are network ready for deployment into the real world. This is all done without investment in a huge array of network equipment. The NE-ONE lets you see how your applications perform both subjectively and objectively using the large number of provided graphing and reporting tools.

Illustration 1 shows a high-level functional overview of the NE-ONE. The NE-ONE has a powerful and intuitive Web Interface with different pages, allowing admin users to administer all aspects of the NE-ONE, and allowing non-admin users to create and run SDTNs for testing purposes. For more information on the user types and the roles they perform, see *User Types and Roles* on page 25.

ILLUSTRATION 1 - HIGH-LEVEL FUNCTIONAL OVERVIEW OF THE NE-ONE



Note:

Traffic cannot pass between the management port and hardware ports.

The asterisk (*) in *Illustration 1* indicates that some or all of the Web Interface is associated with a premium feature. For more information, see *Standard vs Premium Features* on page 18.

Note:

The NE-ONE also has a powerful and flexible command line interface (CLI), which can perform all the functional tasks (and more) than that of the Web Interface. This document describes only the use of the Web Interface. It is beyond the scope of this document to discuss the concepts and usage of the NE-ONE CLI.

The NE-ONE is an Appliance based solution that can be connected into an Ethernet network, supporting up to 10 Gbit/s.

The NE-ONE is supplied with two or more hardware ports and is delivered and rapidly deployed as one of the following:

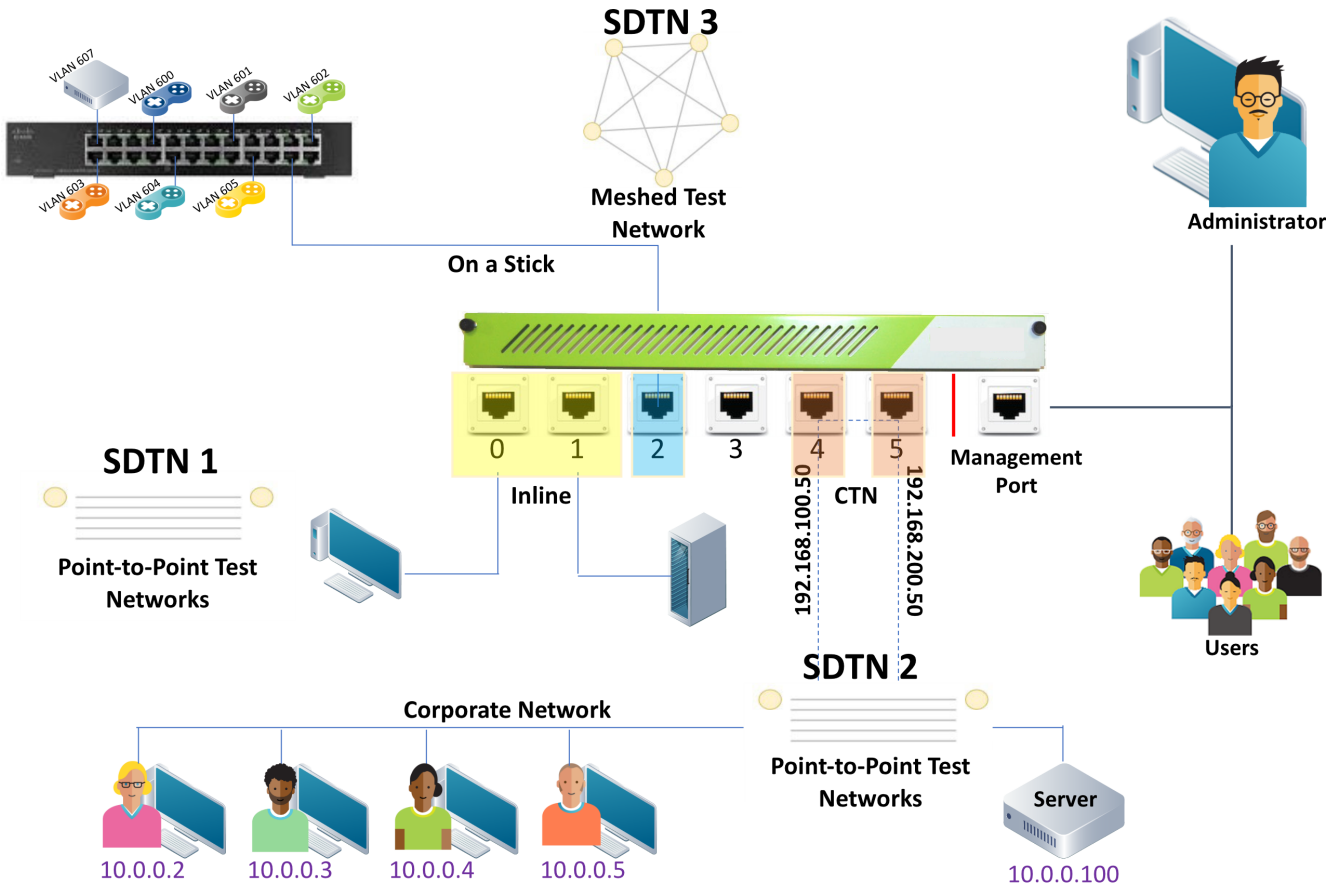
- Physical Desktop unit (which also includes an LCD panel (see *Chapter 16*, *The LCD Panel*) for quick access to certain configuration and network/scenario related operations)
- Physical a 1U rack mount system

Note:

Larger custom 2U or 5U rack mount systems (depending on exact options and ports) are available on special order. For more information, contact you Calnex sales representative.

- Virtual Appliance (supports VMWare and OpenStack).
- Cloud Appliance (supports Microsoft Azure and Amazon Web Services (AWS)).

ILLUSTRATION 2 - EXAMPLE OF RUNNING THREE SOFTWARE DESIGNED TEST NETWORKS



Some NE-ONE models support the ability for multiple users to simultaneously run independent SDTNs across different ports and port pairs, which is highly cost effective when compared to using separate dedicated appliances. *Illustration 2* shows an example of an NE-ONE with six hardware ports being used to simultaneously implement and run three different SDTNs. It is beyond the scope of this chapter to

describe this implementation in detail. More detailed information of this example implementation can be found in *Implementation of SDTNs with the NE-ONE* on page 53 in *Chapter 4*, *Installation and Configuration*.

Note:

SDTN3 in *Illustration 2* is a Fully Meshed network topology that is only available if the Multi-Point Designer premium feature activated. For more information on the different Premium features that are available, see *Standard vs Premium Features* on page 18.

Once connected, the user can easily configure a wide range of parameters, and can change these in real-time to mimic real network conditions. Timed scenarios of SDTN events can be recorded and re-run automatically. For example, timed scenarios could be created to simulate good, busy, and heavily congested network conditions so that applications can be benchmarked against each other.

Note:

Timed scenarios are only possible if the Automatic Scenario Builder premium feature activated. For more information on the different Premium features that are available, see *Standard vs Premium Features* on page 18.

1-1. Standard vs Premium Features

All entry level NE-ONEs have a standard feature set with basic user management and built-in authentication, letting you create simple Point-to-Point networks (using pre-defined port pairs), create manual scenarios, and generate standard reports.

The NE-ONE also has a payable premium feature set (summarized in *Table 1*) that can be customized according to your network simulation needs. The license on the NE-ONE determines which (if any) of the premium features are activated. For more information on the premium features and customizing your network simulation needs, contact your sales representative or Calnex sales.

TABLE 1 - NE-ONE PREMIUM FEATURES

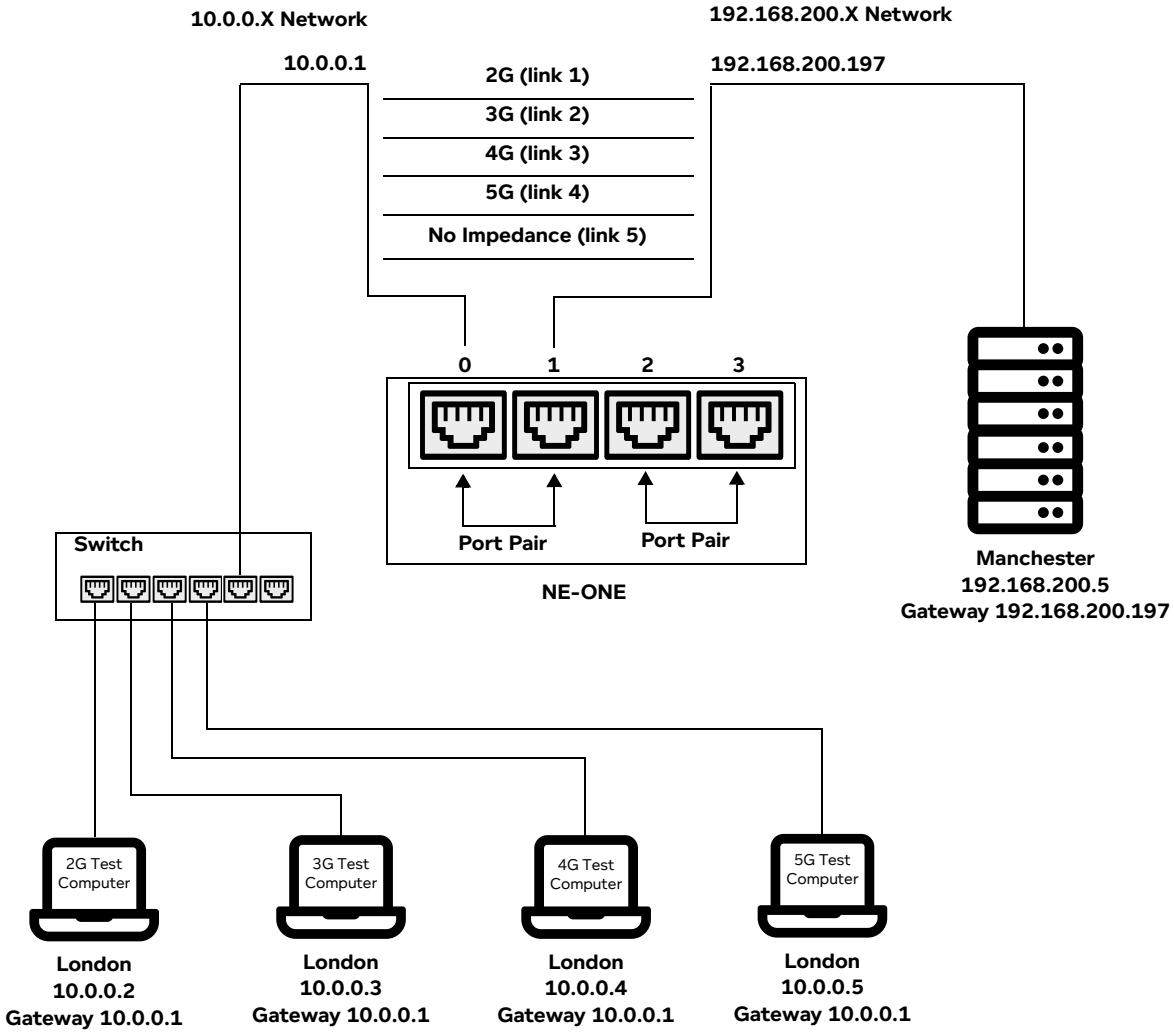
Premium Feature	Description
Automatic Scenario Builder	All NE-ONEs come with a simplistic Manual Scenario Builder (see *Illustration 7* on page 24) that lets you quickly create a simple network experience by graphically combining two or more networks together, that can then be manually selected and run. Compared to the more sophisticated Automatic Scenario Builder, the Manual Scenario Builder has a simpler interface with only a Workspace area (i.e. no Timeline area). The more sophisticated Automatic Scenario Builder feature (see *Illustration 8* on page 25) lets you to create a network experience over time by graphically combining two or more networks together, which can be automatically played on a Timeline. To provide a more realistic test scenario, the networks can be optionally joined together using one of three transitions.
Port Manager	An NE-ONE without the Port Manager feature comes with pre-defined port pairs allocated to the hardware ports, and the port pairs can be assigned to different users. An NE-ONE the Port Manager feature provides a diverse range of flexibility regarding the management of ports, letting you: • Create soft ports. Soft ports are very useful for port sharing in a multi user environment, and if you need a lot ports to plug test devices into, but your data rates are modest so that you can share a hardware port with a lot of test devices. For an example using soft ports in such an environment, see *Illustration 4* on page 21. • Create and manage pre-defined port pairs. • Assign not only port pairs, but also individual ports to different users.
Service Manager	All NE-ONEs come with some in-built services such as Port Addressing and Default Transmission for simple network testing environments. The Service Manager feature lets you to create and manage additional services for more complex network testing environments, such as: • using DHCP helper services • using background port to port transmission via either the Background service or Background Expression Routed service If the Service Management feature is activated on the NE-ONE, you can create and use these services to create more complex test networks with DHCP helpers and/or background port to port transmission (either with or without complex expression routing).

Premium Feature	Description
Advanced User Permissions	All NE-ONEs come with a ability to create and manage users, and determine whether the users are admin or non-admin users. The Advanced User Permissions feature additionally lets you, define the maximum number of networks and objects available for the user, and define whether or not a user can login to the Web Interface.
Advanced Functions	All NE-ONEs come with a standard library of realistic network impairment functions letting you easily mimic what happens in real-world networks, and test your applications. Each impairment function has multiple parameters letting you customize its behavior for your specific testing needs. The Advanced Functions feature provides you with larger list of network impairment functions compared to the standard library. **Note:** The latest library of functions can be found on the Calnex website at: https://ne-one.com/ne-one-family-impairments-sheet/
Advanced Authentication (*)	All NE-ONEs come with a built-in authentication, where the authentication of users is built-in and handled locally on the NE-ONE. The Advanced Authentication feature additionally lets you configure the NE-ONE to use either LDAP or RADUIS authentication methods so that the NE-ONE can be fully integrated into the enterprise's centralized authentication system.
Application Reporting	All NE-ONEs come with a standard reporting (i.e. a Configuration Report and a Test Report) which are useful for simple reporting needs. The Application Reporting feature provides two additional report types (i.e. a general Application Report and detailed Application Performance Report) to let you easily identify whether your applications are network ready for real world implementation, giving you accurate predictions on how an application will perform over a range of latencies and bandwidths.
Multi-Point Designer	All NE-ONEs come with a Point-to-Point Designer, which lets you create Point-to-Point network topologies. The Multi-Point Designer feature lets you create more sophisticated Multi-Point network topologies using either a free-form designer or fully meshed, hub and spoke, and cloud (star) topology templates.
Defense Pack	The Defense Pack feature provides an additional Defense node category (with defense related node icons) and a TDMA Mesh (Labs) function in the Multi-Point designer. These let you create and run networks using Time Division Multiple Access (TDMA).
* - If you have the Advanced Authentication feature and use RADIUS authentication, you must also have the Advanced User Permissions feature.	

1-2. Simple Test Networks Using the Standard Features

Illustration 3 shows an example of how the NE-ONE can used to simulate a simple Point-to-Point network using the standard (i.e. non-premium) features of the NE-ONE. This example is fully described in more detail in *Creating Point-to-Point Networks (Single)* on page 265 within *Chapter 9*, *Creating and Running Point-to-Point Networks*. In this case, the standard Point-to-Point Designer feature which is available on all NE-ONEs can be used to quickly create the Point-to-Point network.

ILLUSTRATION 3 - EXAMPLE POINT-TO-POINT NETWORK - 5 LINKS WITH PORT ADDRESSING



1-3. Sophisticated Test Networks Using the Port Manager and Multi-Point Designer Features

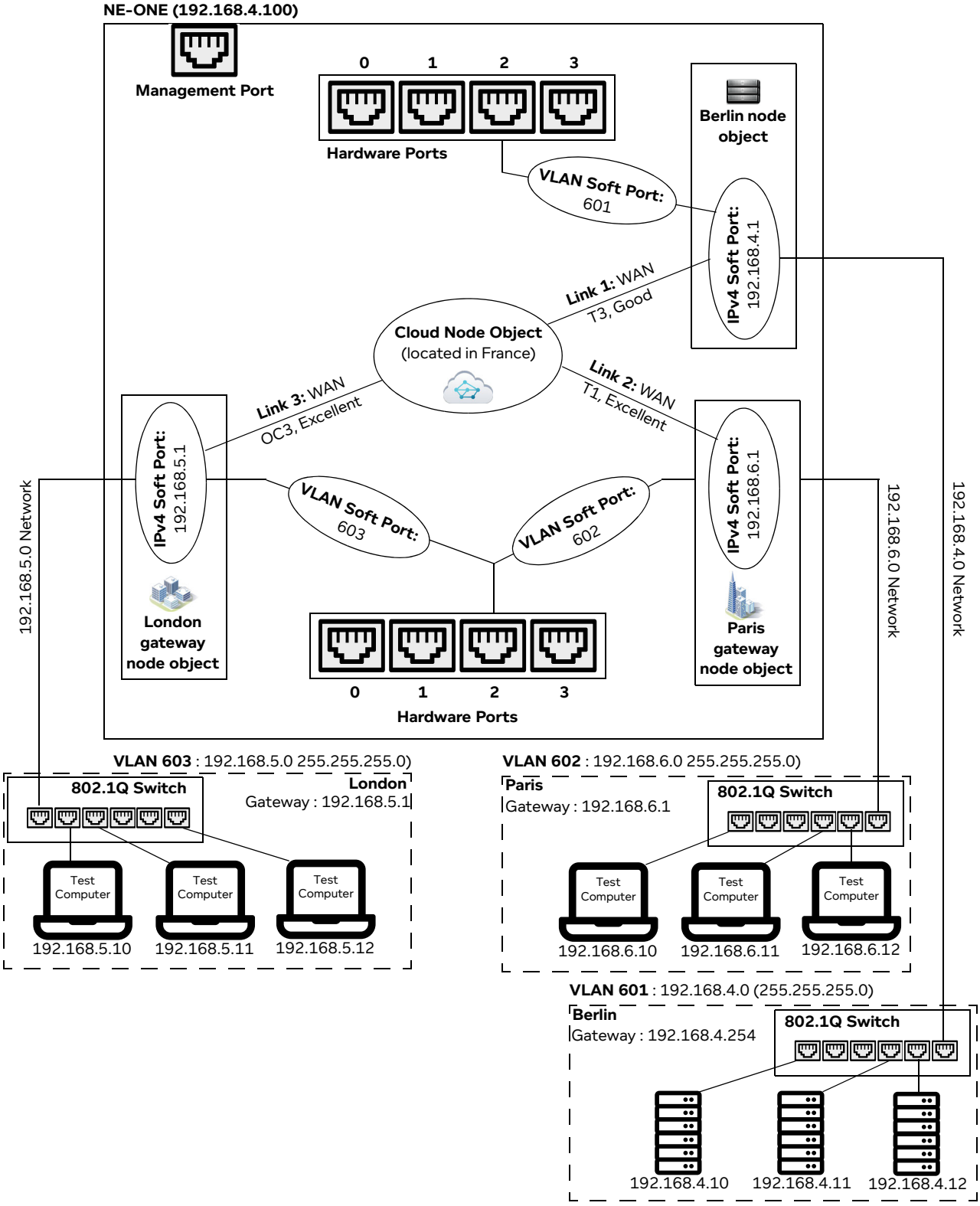
Illustration 4 shows an example of how the NE-ONE can used to simulate a cloud network for testing between different test networks with different VLANs on different networks.

It illustrates how simulations of sophisticated network environments can easily be created on the NE-ONE with the use of:

- soft ports that are only available with the Port Manager feature
- a cloud (star) topology that is only available with the Multi-Point Designer feature

This type of sophisticated network environment can only be created if the premium Port Manager and Multi-Point Designer features are activated on the NE-ONE.

ILLUSTRATION 4 - EXAMPLE OF A SIMULATED CLOUD NETWORK (WITH VLAN AND IPV4 SOFT PORTS)



In *Illustration 4*, we can see that with the use of VLAN and IPv4 soft ports, node routing functions, and cloud functions, that only one hardware port (in this case hardware port 2) is needed to connect to three test networks on three different VLANs via a simulated cloud network.

In reality, the three VLAN networks are connected to only one hardware port via a 802.1Q switch, and the simulated cloud network on the NE-ONE seamlessly filters and routes the traffic via the NE-ONE's VLAN and IPv4 soft ports, node route functions and cloud functions.

Thus, with the use of the NE-ONE's soft ports and node functions, you can easily and quickly simulate extremely large network testing environments.

2. NETWORK TYPES AND SCENARIOS

2-1. Point-to-Point vs Multi-Point Network Designers

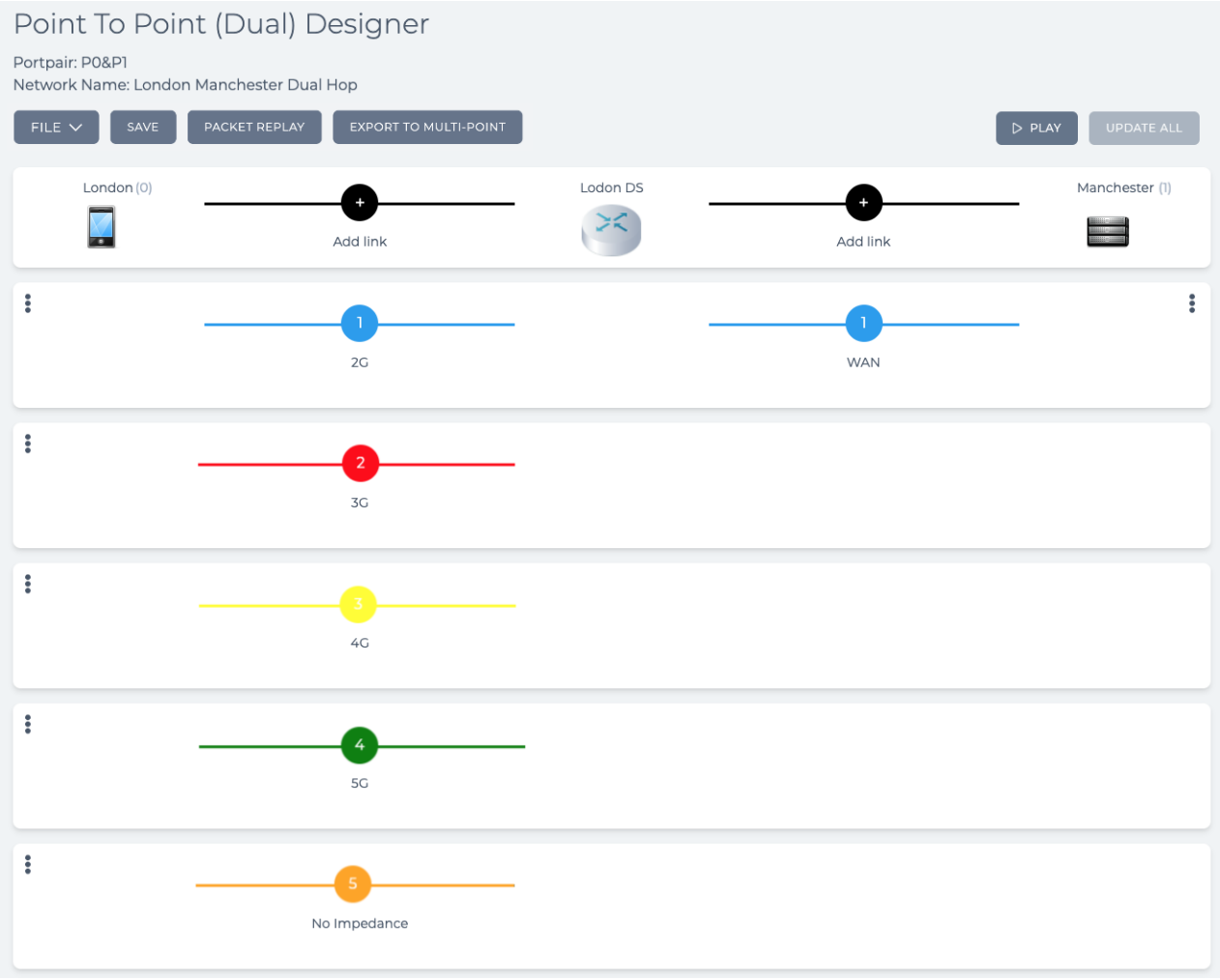
For ease of network creation, the NE-ONE distinguishes between two network topology types that can be categorized, as either Point-to-Point (including Point to Point (single) and Point to Point (dual hop)), and Multi-Point (including: Fully Meshed Hub and Spoke, Cloud (star), and Free Form).

Note:

The Multi-Point Designer and associated Multi-Point network topologies (i.e. Fully Meshed, Hub and Spoke, Cloud, and Free Form) are only available with the Multi-Point Designer feature. Depending on your license, the Multi-Point Designer and associated Multi-Point network topologies may be either activated or deactivated.

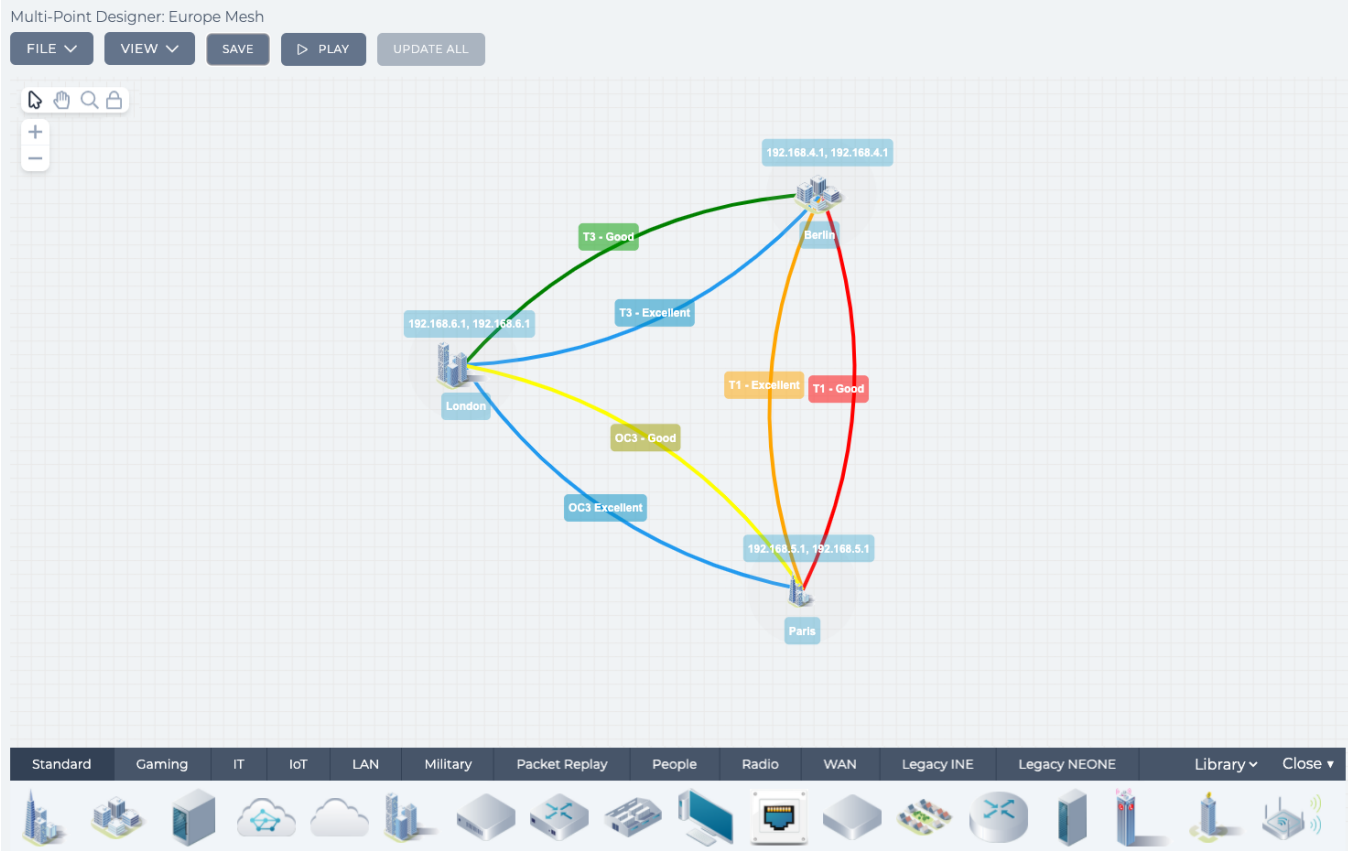
Point-to-Point networks can be rapidly created via the Point-to-Point Designer (*Illustration 5*), and assigned to port pairs, where the traffic routing is already implicitly applied to the nodes in the Point-to-Point network. All NE-ONE models support multiple links and dual hop/last mile capability.

ILLUSTRATION 5 - EXAMPLE POINT-TO-POINT DESIGNER WITH A IN A DUAL HOP NETWORK



For more complex network types, with more than two nodes, and more complex routing requirements, Multi-Point networks can be rapidly created via the Multi-Point Designer (*Illustration 6*), and complex routing can explicitly and quickly be defined. The Multi-Point Designer uses a leading edge, graphical Workspace, that lets you seamlessly create complex Multi-Point networks.

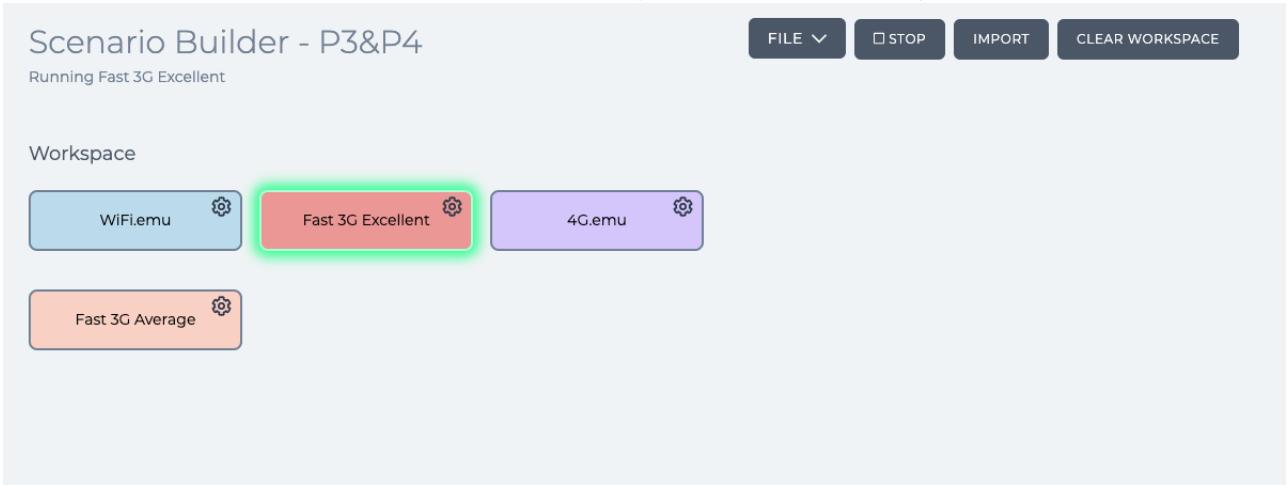
ILLUSTRATION 6 - EXAMPLE MULTI-POINT DESIGNER WITH A FULLY MESHED 3 NODE NETWORK



2-2. Manual Scenario Builder vs Automatic Scenario Builder

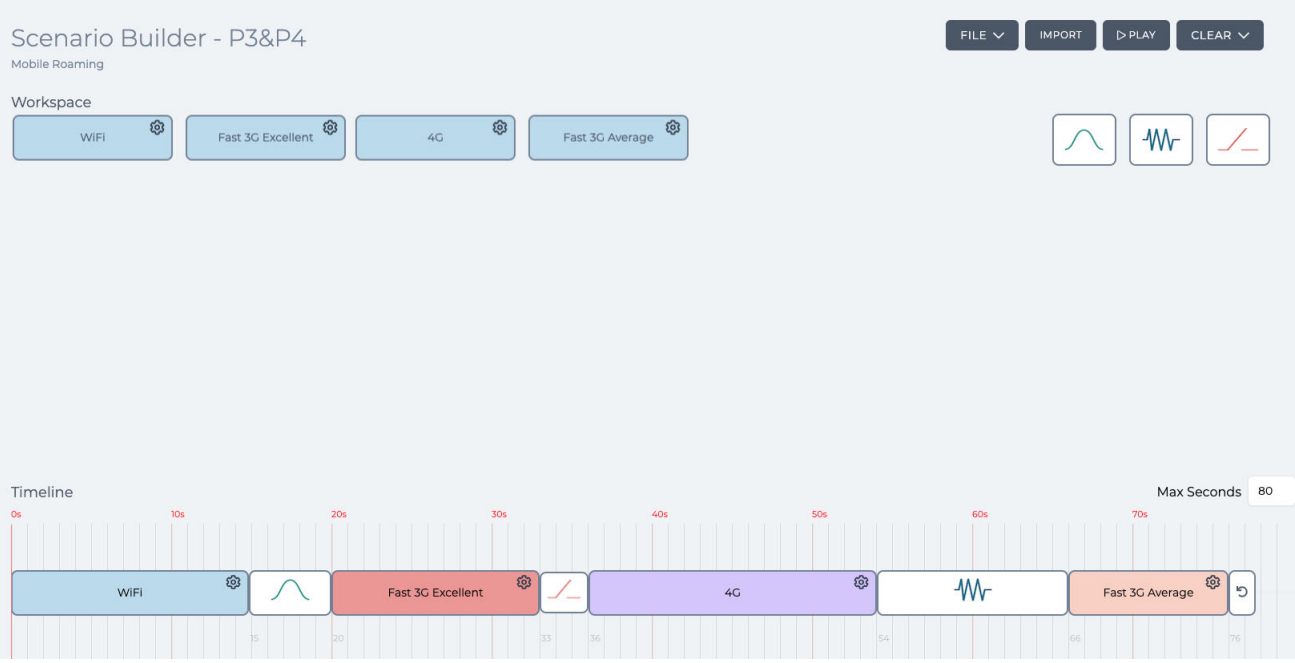
In addition to the Point-to-Point and Multi-Point network types, the NE-ONE's entry-level Manual Scenario Builder feature (*Illustration 7*) lets you create Point-to-Point and Multi-Point network types whose link characteristics change only with manual user intervention, and without different transition types between the change in link characteristics. These manually changing networks are know as Manual Scenarios.

ILLUSTRATION 7 - MANUAL SCENARIO BUILDER (STANDARD FEATURE)



In addition to the Point-to-Point and Multi-Point network types, the NE-ONE's Automatic Scenario Builder feature (*Illustration 8*) lets you create Point-to-Point and Multi-Point network types whose link characteristics dynamically change with time, and with different transition types between the change in link characteristics. These dynamically changing networks are know as Automatic Scenarios.

ILLUSTRATION 8 - AUTOMATIC SCENARIO BUILDER (PREMIUM FEATURE)



3. USER TYPES AND ROLES

The NE-ONE supports two type of user role:

- Admin user - with all rights, responsible for the following tasks:
  - Configuring and installing the NE-ONE in the company/corporate network (via the **Platform Management** pages).
  - Creating soft ports and port pairs (via the **Port Manager** pages) (if the Port Manager feature is activated).
  - Creating network services (via the **Service Manager** page) (if the Service Manager feature is activated). Thus allowing the NE-ONE to:
    - be integrated into an existing company/corporate network, and take on the routing functions if necessary,
    - act as a DHCP relay.
  - Creating users and assigning port pairs and individual ports to non-admin users (via the **User Management** pages).
  - Optionally creating and running Point-to-Point or Multi-Point networks (via the **Point-to-Point Designer** and **Multi-Point Designer** pages, respectively). Creation of Multi-Point networks is only possible if the Multi-Point Designer feature is activated.
  - Optionally creating and running scenarios (via the **Scenario Builder** page).
- Non-admin user - with limited rights (configured by an admin user), responsible for the following tasks:
  - Creating and running Point-to-Point or Multi-Point networks (via the **Point-to-Point Designer** and **Multi-Point Designer** pages, respectively). Creation of Multi-Point networks is only possible

if the Multi-Point Designer feature is activated.

- Optionally creating and running scenarios (via the **Scenario Builder** page).
- Creating reports (via the **Reports** page).
- Creating graphs (via the **Graphs** page).
- View statistics of Packet Processing Objects (PPOs) on running network simulations (via the **Statistics** pages).
- Creating packet capture files (`*.pcap`) for analysis in tools such as Wireshark.
- Monitoring live packet data for *in-situ* debug analysis of network applications in real-time.

CHAPTER 3 NE-ONE WEB INTERFACE OVERVIEW

1. ACCESSING THE WEB INTERFACE

The NE-ONE has an intuitive Web Interface, which is securely accessible using a web browser. *Table 2* summarizes the recommended web browsers that are compatible and available for use with the NE-ONE.

TABLE 2 - RECOMMENDED AND COMPATIBLE WEB BROWSERS

Web Browser**	Windows	MacOS
Safari ***	No*	Yes
Windows Edge	Yes	Not Applicable
Google Chrome	Yes	Yes
Mozilla Firefox	Yes	Yes

* - The last version (5.1.7) of Safari for Microsoft Windows is no longer maintained by Apple and is now obsolete.
** - In order for the Web Interface to function, JavaScript must be enabled on your web browser.
*** - Safari does not support named destination markers in PDF files. The context sensitive help of the Web Interface uses named destination markers within the embedded PDF file of this *User and Administration Guide*. If you want to benefit from the context sensitive help functionality, you must use either Google Chrome, Mozilla Firefox, or Windows Edge.

Your network administrator will have configured the NE-ONE so that its Web Interface is accessible on your network, and will provide you with the following access details:

- IP address and/or hostname
- Username
- Password

Note:
If your organization uses LDAP (Lightweight Directory Access Protocol) or RADIUS (Remote Dial-In User Service) authentication, the admin user will have configured the NE-ONE to use LDAP or RADIUS as its authentication method. If this is the case, simply use the same username and password that you use to login to your organization's network.

Note:
LDAP and RADIUS authentication methods are only available with the Advanced Authentication feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

Note:
Out of the box, the NE-ONE contains default factory settings that are not configured with users or your network. If you are the network/IT administrator (i.e. an admin user of the NE-ONE), the first time you use the NE-ONE you will need to know how to access the Web Interface. A leaflet is provided in the box describing how to access the NE-ONE for the first time so that it can be configured to be accessible on your network.

1-1. First time Web Interface access (accepting the default self-signed SSL certificate)

The NE-ONE's web server that hosts the Web Interface uses HTTPS (Secure Hypertext Transfer Protocol) and SSL (Secure Socket Layer) protocol.

When you try to access the NE-ONE's Web Interface over the SSL protocol, it has to identify itself with an SSL certificate to the web browser. In order for web browsers to trust the SSL certificate presented by the web server, the SSL certificate must be issued by a trusted Certificate Authority (CA). An SSL

certificate that is issued by a trusted CA is called a root SSL certificate, whereas an SSL certificate that is not issued by a trusted CA will be self-signed, and is called a self-signed SSL certificate.

The default SSL certificate supplied by Calnex on the NE-ONE's web server is a self-signed one, meaning that it has not been issued by a trusted CA. Instead, the NE-ONE has signed the SSL certificate as being valid. This works fine for encrypting data, but presents you with a "privacy" or "security risk" error/warning message in your web browser the first you try to access the secure content of the Web Interface.

Note:

The NE-ONE allows an admin user to install another SSL certificate to replace the default self-signed SSL certificate supplied by Calnex. If your organization uses a root SSL certificate issued by a trusted CA, the admin user will have configured the NE-ONE with that root SSL certificate (according to *Installing and Updating Root SSL Certificates* on page 81), and you will not need to configure your web browser to accept the default self-signed SSL certificate according to the steps below.

If the NE-ONE's web server is using the default Calnex self-signed SSL certificate then the first time you access the Web Interface, you will need to configure your web browser to trust that certificate. The way in which you configure your web browser to trust the default Calnex self-signed SSL certificate varies according to the web browser and operating system that you use.

Use the appropriate section below to configure your web browser to trust the default Calnex self-signed SSL certificate:

- *Section 1-1-1*, *Accepting the self-signed SSL certificate on MacOS with the Safari web browser* on page 28
- *Section 1-1-2*, *Accepting the self-signed SSL certificate on MacOS or Windows with the Google Chrome web browser* on page 30
- *Section 1-1-3*, *Accepting the self-signed SSL certificate on MacOS or Windows with the Mozilla Firefox web browser* on page 32
- *Section 1-1-4*, *Accepting the self-signed SSL certificate on Windows with the Microsoft Edge web browser* on page 33

1-1-1. Accepting the self-signed SSL certificate on MacOS with the Safari web browser

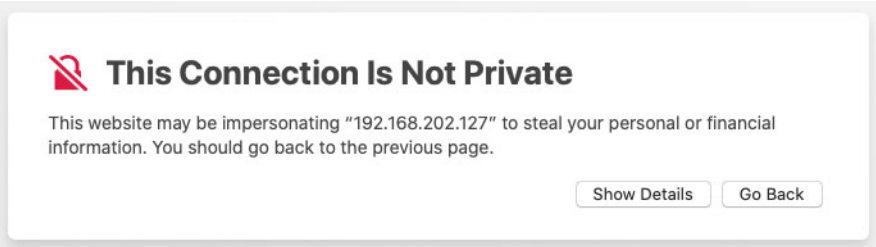
To access the Web Interface for the first time and configure the Safari web browser in MacOS to accept the self-signed SSL certificate, do the following:

1. Launch Safari, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

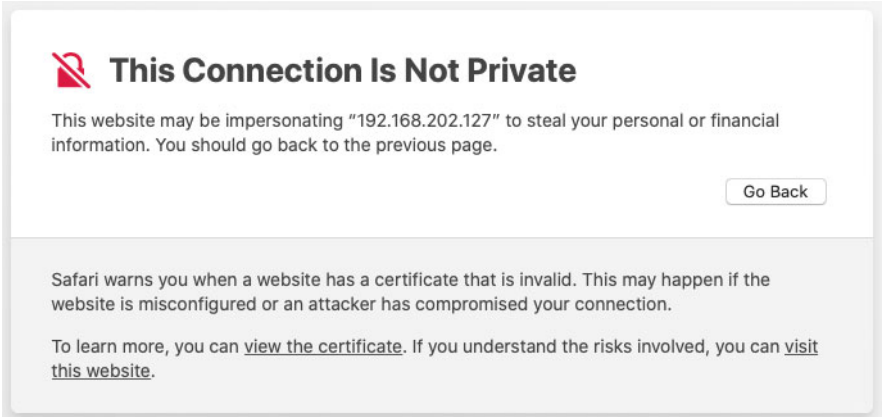
   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

   A **This Connection Is Not Private** dialog box appears.

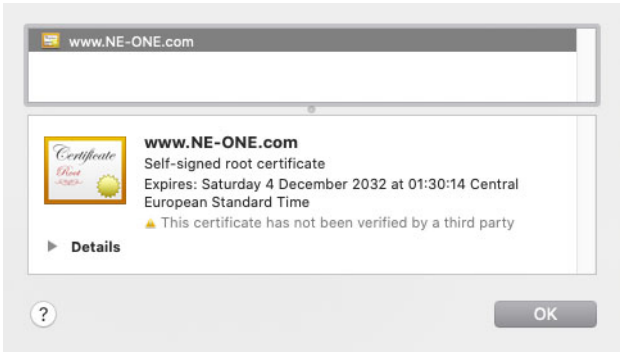
   

2. From the **This Connection Is Not Private** dialog box that appears, click **Show Details**.

The **This Connection Is Not Private** dialog box expands with more details.



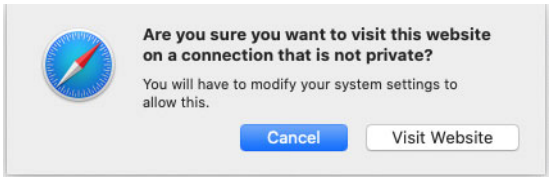
3. If you want to know when the self-signed SSL certificate expires, click the **view the certificate** link.
   A dialog box appears summarizing the details of the self-signed certificate.



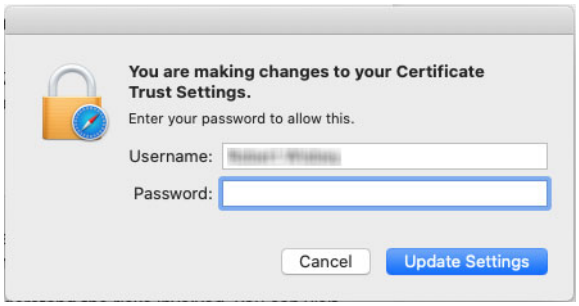
   Click **OK** to close the dialog box.

Note:
You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page* on page 40).

4. Click the **visit this website** link.
   A dialog box appears prompting you to confirm if you are sure you want to visit the website on a connection that is not private.



5. From the dialog box that appears, click **Visit Website**.
   A dialog box appears prompting you to specify your MacOS login credentials.



6. Type your MacOS username and password in the **Username** and **Password** fields, respectively. Then click **Update Settings**.

   The Web Interface login page appears. From now on (until it expires) you will no longer need to accept the self-signed SSL certificate for the NE-ONE.

Note:

You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page* on page 40).

7. From the **Login to your account** page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

1-1-2. Accepting the self-signed SSL certificate on MacOS or Windows with the Google Chrome web browser

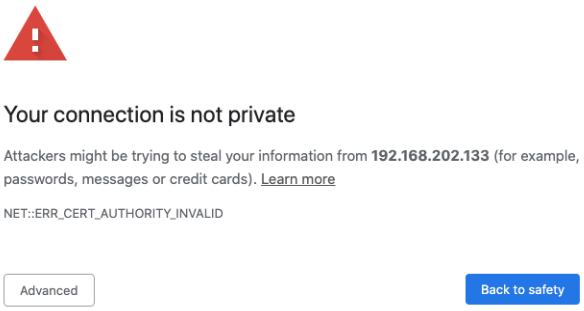
To access the Web Interface for the first time, and configure the Google Chrome web browser in MacOS or Windows to accept the self-signed SSL certificate, do the following:

1. Launch Google Chrome, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

   A **Your connection is not private** page appears.

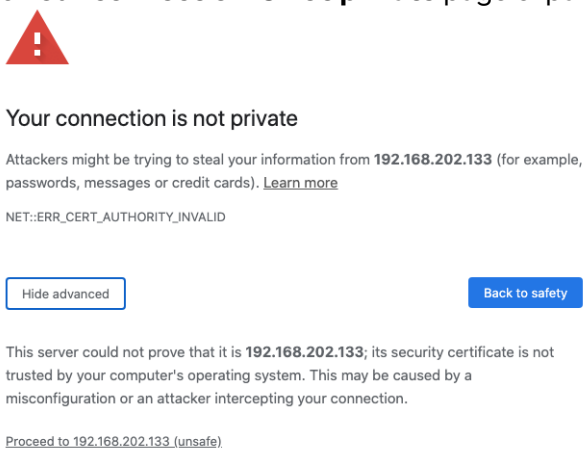


Note:

The Windows version of Google Chrome's **Your connection is not private** page contains an additional check box to help improve web security by sending URLs of some pages visited. This check box is irrelevant to this procedure.

2. From the **Your connection is not private** page that appears, click **Advanced**.

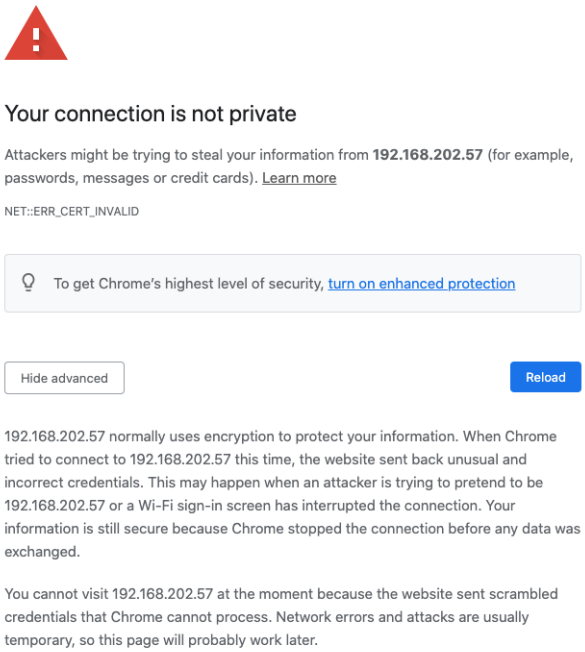
   The **Your connection is not private** page expands with more details.



3. Click the **Proceed to <IP address or hostname> (unsafe)** link.

Note:

Depending on your Chrome browser and computer's Operating System environment the **Proceed to <IP address or hostname> (unsafe)** link may not appear in the **Your connection is not private** page, and appears as follows. In this case, click within the Chrome browser on this page, and enter the following string: **`thisisunsafe`** (i.e this is unsafe, without the spaces).



The Web Interface login page appears. From now on (until it expires) you will no longer need to accept the self-signed SSL certificate for the NE-ONE.

Note:

You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page* on page 40).

4. From the **Login to your account** page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

1-1-3. Accepting the self-signed SSL certificate on MacOS or Windows with the Mozilla Firefox web browser

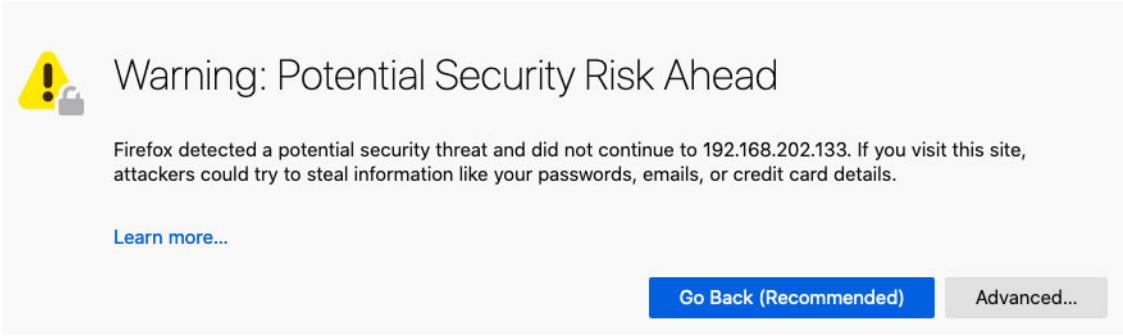
To access the Web Interface for the first time and configure the Mozilla Firefox web browser in MacOS or Windows to accept the self-signed SSL certificate, do the following:

1. Launch Mozilla Firefox, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

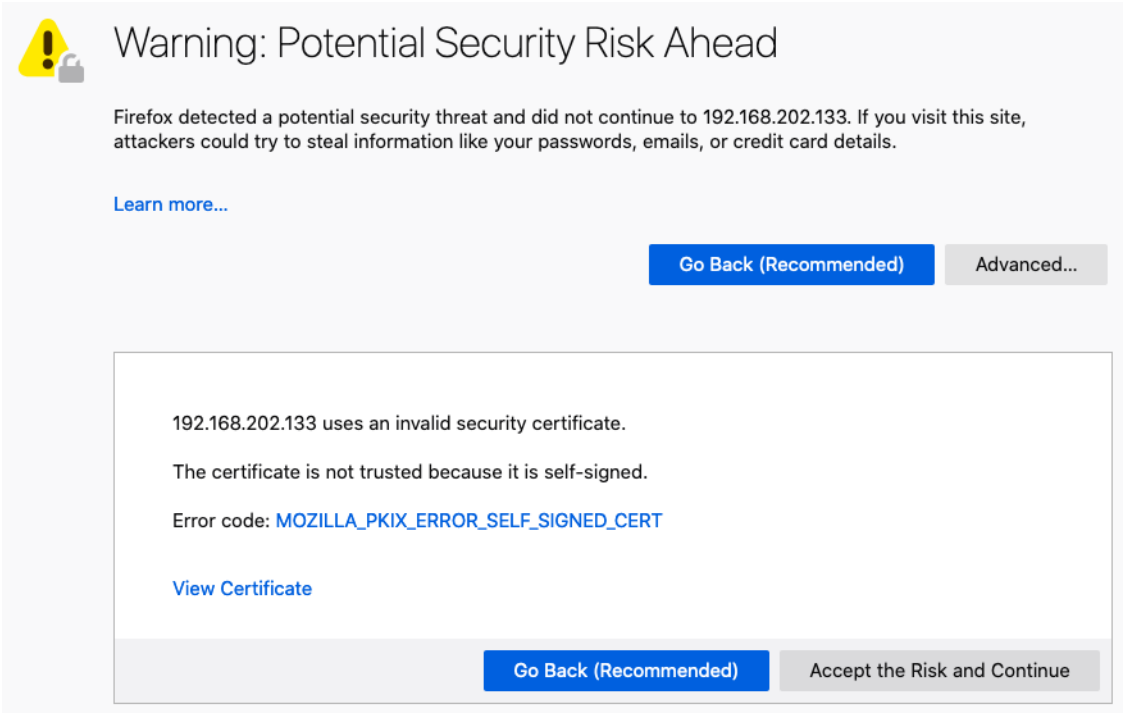
   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

   A **Warning: Potential Security Risk Ahead** page appears.



2. From the **Warning: Potential Security Risk Ahead** page that appears, click **Advanced...** .

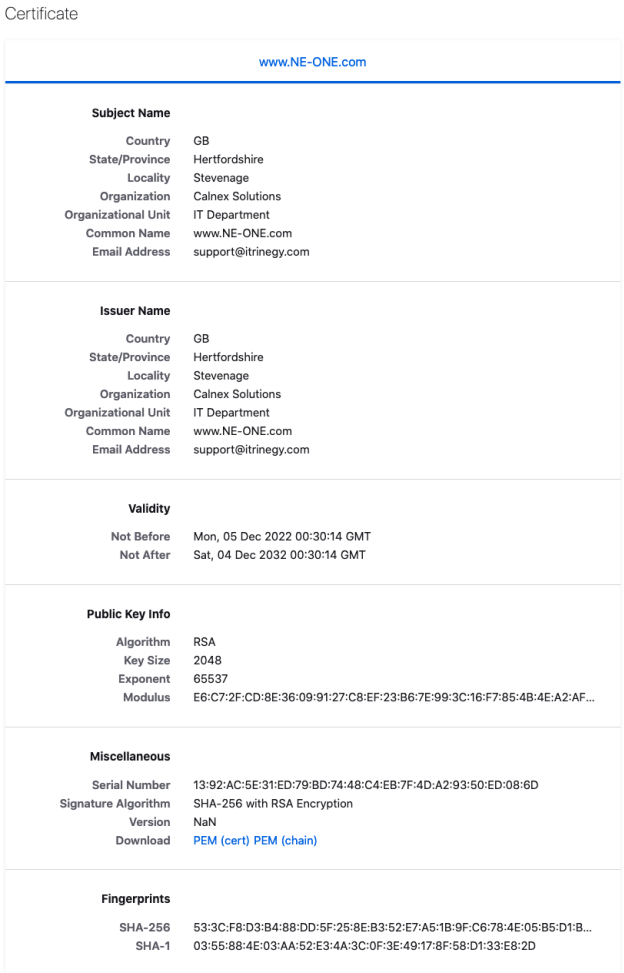
   The **Warning: Potential Security Risk Ahead** page expands with more details.



3. If you want to know when the self-signed SSL certificate expires, click the **View Certificate** link.

   A new **Certificate for www.NE-ONE.com** tab appears summarizing the details of the self-signed

certificate.



Click **X** to close the **Certificate for www.NE-ONE.com** tab.

Note:

You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page* on page 40).

4. Click **Accept the Risk and Continue**.

   The Web Interface login page appears. From now on (until it expires) you will no longer need to accept the self-signed SSL certificate for the NE-ONE.

5. From the **Login to your account** page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

1-1-4. Accepting the self-signed SSL certificate on Windows with the Microsoft Edge web browser

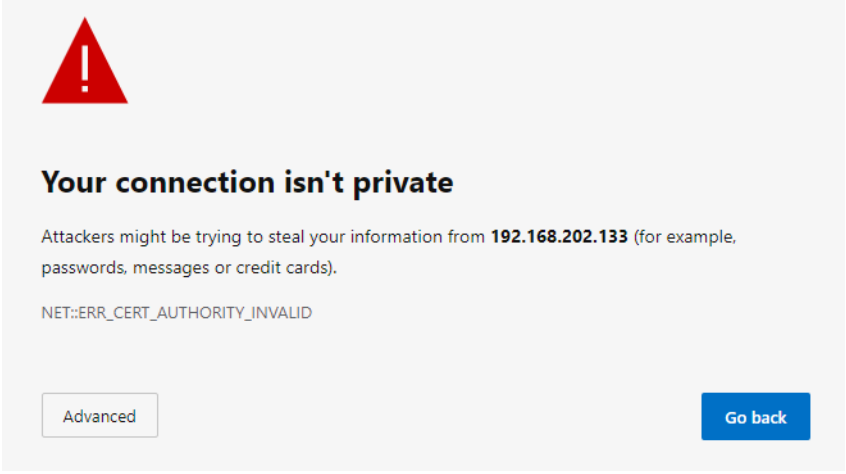
To access the Web Interface for the first time and configure the Microsoft Edge web browser in Windows to accept the self signed SSL certificate, do the following:

1. Launch Microsoft Edge, and specify the following URL in the address bar:

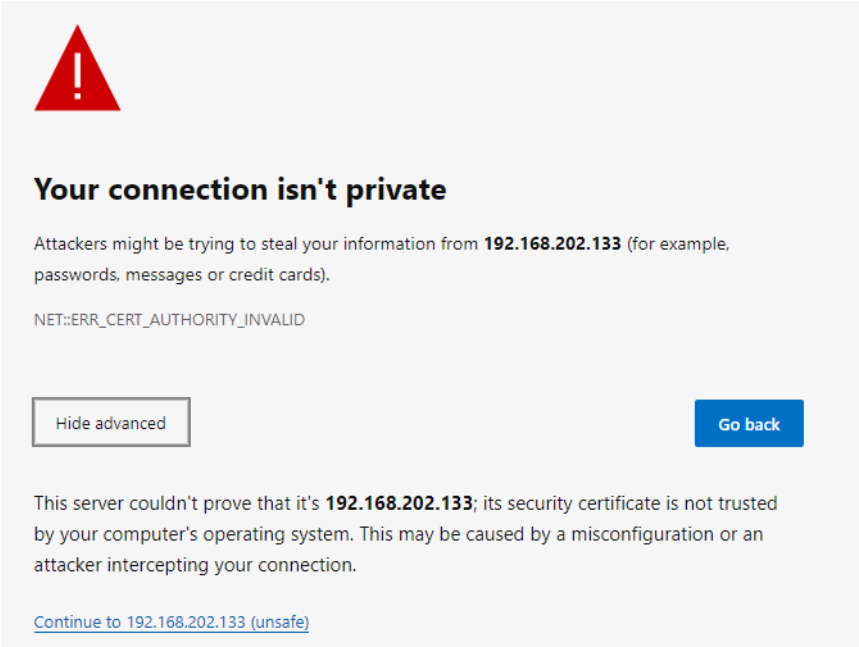
   `https://<IP address or hostname>`

   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

A **Your connection isn't private** page appears.



2. From the **Your connection isn't private** page that appears, click **Advanced**.
   The **Your connection isn't private** page expands with more details.



3. Click the **Continue to <IP address or hostname> (unsafe)** link.
   The Web Interface login page appears. From now on (until it expires) you will no longer need to accept the self-signed SSL certificate for the NE-ONE.

Note:
You can view the expiry date of the self-signed SSL certificate from the Web Interface Home page (see *Home Page* on page 40).

4. From the **Login to your account** page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

1-2. Accessing the Web Interface

Once you have configured your preferred web browser to accept the NE-ONE's self-signed SSL certificate (see *First time Web Interface access (accepting the default self-signed SSL certificate)* on page 27) or if the NE-ONE is configured with your organization's root SSL certificate, you can access the Web Interface directly, without needing to take additional configuration steps. Use the following steps to access and log in to the Web Interface:

1. Launch your preferred web browser, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

   where `<IP Address or hostame>` is the IP Address or hostname provided by your network administrator.

   A login page appears.

Note:
The login page above is the generic one supplied with the NE-ONE. The appearance of the login page may vary it if has been personalized by an admin user according to *Personalizing the Login Page* on page 71 in *Chapter 4*, *Installation and Configuration*.

2. From the login page that appears, specify your username and password in the **Username** and **Password** fields, respectively, then click **LOGIN**.

   Upon successfully logging in, you are presented with the Web Interface (see *Web Interface Layout* on page 36).

Note:
If you are logging in as the built-in local (built-in) admin user for the first time or after the admin user password has been reset, you will be promoted to change the default password before being presented with the Web Interface. For more information, see *Changing the Default Admin Password* on page 62 in *Chapter 4*, *Installation and Configuration*.

Note:
If you are logging in for the first time you must accept the Calnex terms and conditions before using the NE-ONE's Web Interface.

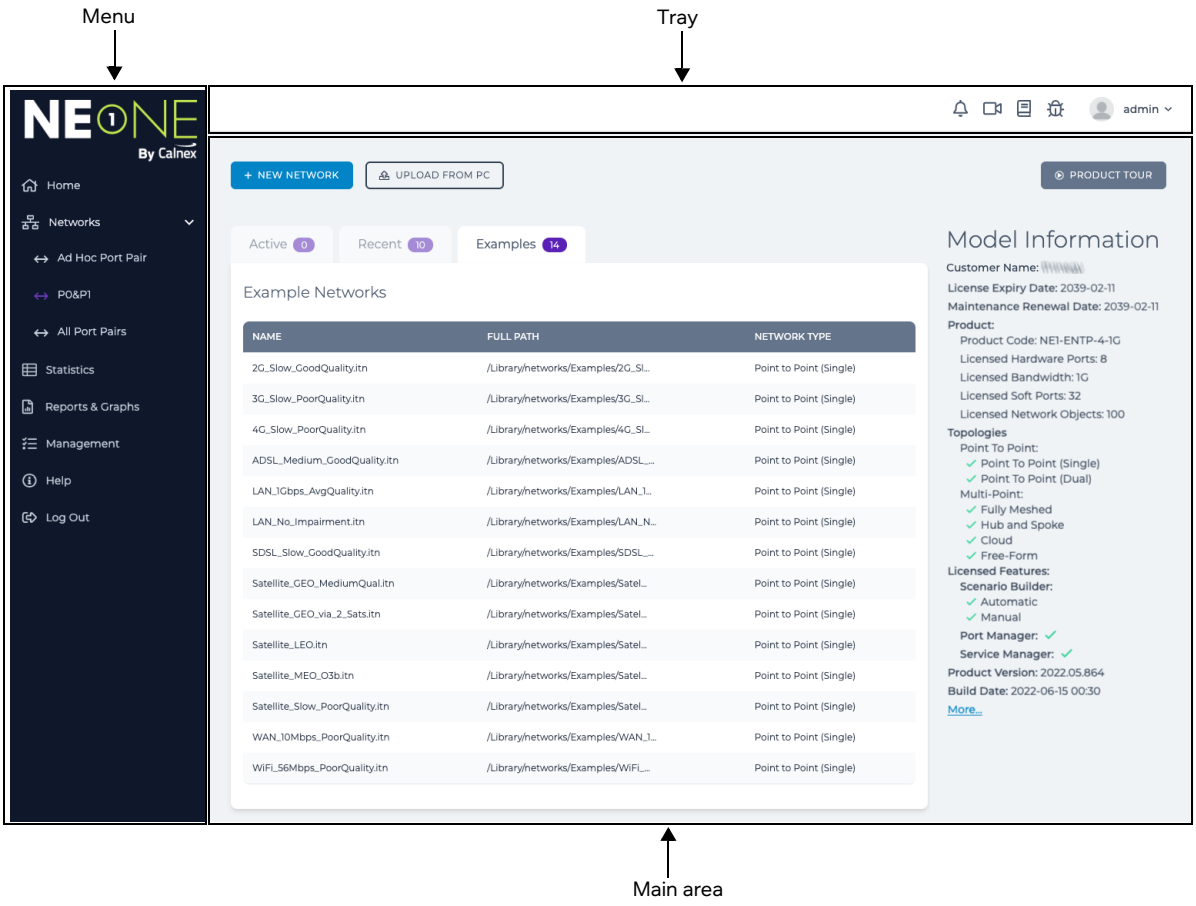
Note:
If your organization has an Audit and Compliance policy your admin user will have applied a customized User Acceptance Document according to *Applying a Compliance and Audit Acceptance Agreement* on page 73 in *Chapter 4*, *Installation and Configuration*. In this case, each time you login to the NE-ONE you must accept the terms and conditions of your organization's User Acceptance Document before using the NE-ONE's Web Interface.

2. WEB INTERFACE LAYOUT

Illustration 1 shows the layout of the Web Interface, which comprises the following three elements:

- Menu — contains different menu items that give you access to all functions to manage the NE-ONE. Clicking on a menu item updates the main area of the Web Interface with a corresponding page. For more information, see *The Web Interface Menu* on page 37.
- Tray — contains network/scenario status icons, notification icons, on-line help icons, and user drop-down menu. For more information, see *The Web Interface Tray* on page 38.
- Main area — updates with different pages according to the menu item you selected, or according to other actions you have taken within the different pages.

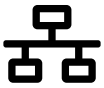
ILLUSTRATION 1 - NE-ONE WEB INTERFACE LAYOUT



2-1. The Web Interface Menu

The Menu provides a quick way to access all the functions on the NE-ONE. *Table 3* summarizes each of the Menu items.

TABLE 3 - MENU ITEMS

Menu Item	Menu Icon	Description
Home		Opens the **Home** page from where you can create new networks, edit existing networks and scenarios, and view your NE-ONE model information. For more information, see *Home Page* on page 40.
Networks		Opens the **Network** page, from where you can create, and edit (if they already exist) networks and scenarios. For more information, see *Networks Page* on page 42.
		If port pairs have been created by an administrator and assigned to another user (see *Creating Port Pairs* on page 158 and *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205), they are listed as sub-items underneath the **Networks** menu item if the user has starred (favorited) the port pair (see *Creating "Starred" Port Pair Favorites* on page 232). Clicking on a port pair opens the **Network Port Pair** page, from where you can do the following for the selected port pair: • create, and edit (if they already exist) networks and scenarios • edit the port settings (i.e. port addressing and default transmission) For more information, see *Network Port Pair Page* on page 43.
Statistics		Opens the **Statistics** page (see *Illustration 160* on page 527), which is the central location listing the statistics of the following objects from where you launch packet capture or data graphing for an object: • network objects (i.e. links and nodes) associated with any currently active (running) networks • framework objects (i.e. hardware port, soft port, port container, or service) For more information, see *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing* on page 525.
Reports & Graphs		Opens the **Reports And Graphs** page (see *Illustration 167* on page 555), from where you can do the following: • create graphs (see *The Graphs Page* on page 555) • generate reports (see *The Reporting Page* on page 568) • view historical statistics (see *The Historical Statistics Pages* on page 565) For more information, see *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing* on page 525.
Management		Opens the **Management** page, from where you can drill down further in order to manage all aspects of the NE-ONE. The management functions that are available vary according to your user profile type (admin or user). For more information, see *Management Page* on page 46.
Help		Opens the **Help** page, from where you view the embedded online documentation and videos, request support, and view the EULA agreement.
Log Out		Logs you out of the Web Interface and returns you to the **Login to your account** page.

2-2. The Web Interface Tray

The Web Interface Tray (see *Illustration 2* and *Table 4*) provides quick access to user centric functions, system notifications, context sensitive on-line help, and a quick access and status area for running and open (i.e. work-in-progress) networks/scenarios.

ILLUSTRATION 2 - THE WEB INTERFACE TRAY

TABLE 4 - WEB INTERFACE TRAY ICONS AND ELEMENTS

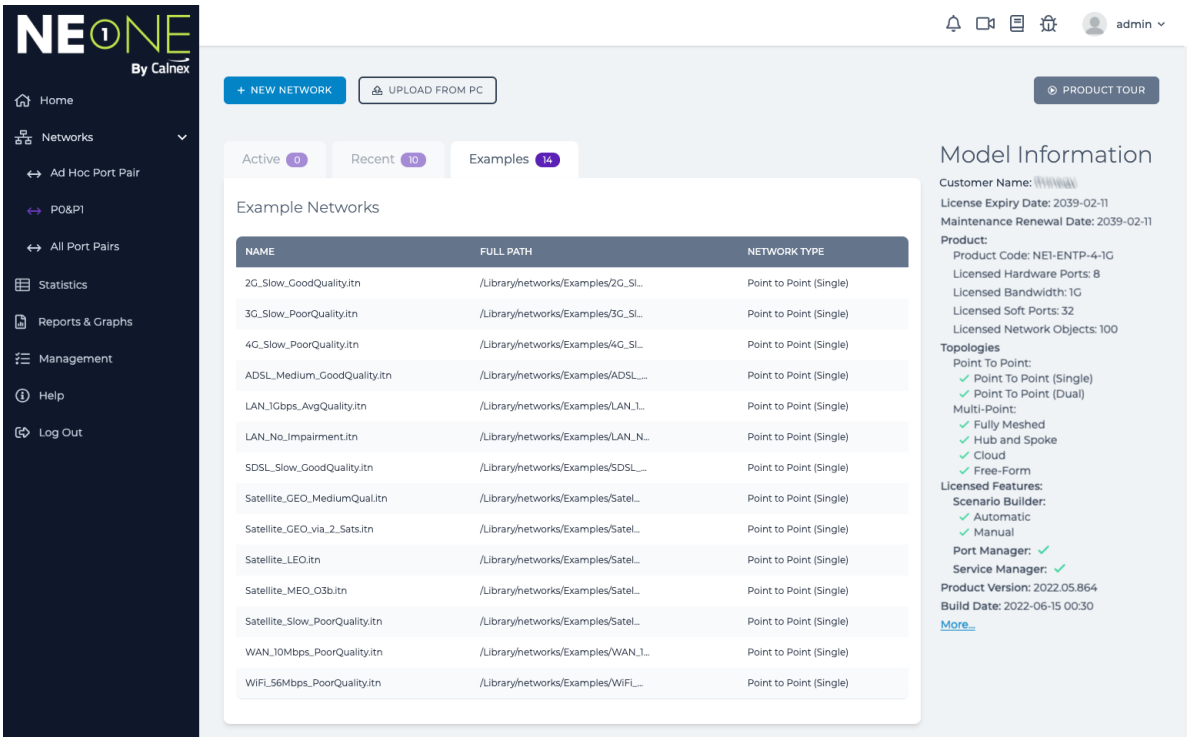
Tray icon or element	Description
	Only visible if a network or scenario is open, stopped and currently being created or edited. Clicking on this icon opens the currently work-in-progress network/scenario in the Main area, letting you continue to edit it and once finalized, run (play) it. Placing your mouse on this icon results in mouse over text appearing with the name of the network/scenario. Right mouse clicking on this icon reveals a **Close** pop-up menu, which upon selecting will close the network/scenario.
	Only visible if a network or scenario is currently running. Clicking on this icon opens the currently running network/scenario in the Main area, letting you stop running (playing) it for editing or launch graphs. Placing your mouse on this icon results in mouse over text appearing with the name of the network/scenario. Right mouse clicking on this icon reveals a **Close** pop-up menu, which upon selecting will close the network/scenario. The running network/scenario will continue running, and be listed in the **Active** tab of the **Home** page. **Note :** A running network or scenario is attached to the user who initially ran it. This icon only visible during the current login session for the user who run a network or scenario. This icon not visible if: • the user's Web Interface session closes and the same user logs back in • the same user logs out and logs back in to the Web Interface later on • if a different user logs in to the Web Interface
	The **View More** drop-down menu icon. Only visible if more than a total of six networks/scenarios are open, letting you select the additional (from the seventh onwards) open networks/scenarios.
	Displays the username of the currently logged in user. Contains the following menu items: • **Change Password** — opens a **User Profile** page allowing the logged in user to update their password. For more information, see *Changing Your User Password via the Tray User Menu* on page 230 in *Chapter 8*, *General System Procedures* **Note :** The **Change Password** menu item is only visible if the NE-ONE uses the built-in authentication method. If the NE-ONE is configured with LDAP or RADIUS authentication, the **Change Password** menu item will not be visible as the user passwords will be managed by the organization's Directory Access servers. • **Change Language** — opens a **Choose language** dialog box allowing the logged in user to set the language displayed in the Web Interface. For more information, see *Setting the Web Interface Language via the Tray User Menu* **on page 230** in *Chapter 8*, *General System Procedures*. • **Log Out** — allows the existing logged in user to log out of the Web Interface.

Tray icon or element	Description
	Opens a context sensitive help video (in a separate browser tab) that describes the use of the page that is currently open.
	Opens in a separate browser tab, context sensitive help documentation from the embedded PDF file of the *User and Administration Guide*, describing the use of the Web Interface page that is currently open. **Note :** Safari does not support named destination markers in PDF files. The context sensitive help of the Web Interface uses named destination markers within the embedded PDF file of this *User and Administration Guide*. If you want to benefit from the context sensitive help functionality, you must use either Google Chrome, Mozilla Firefox, or Windows Edge.
	Opens a **Report a Bug** page letting you submit a bug report to the technical support team at Calnex.
	Opens the **System Notifications** page, from where you can view a chronological list of system level events, categorized by event type. For more information, see *Viewing System Notifications* on page 233 in *Chapter 8*, *General System Procedures*. **Note :** The **System Notifications** page can also be opened via the **Management** page.
	Opens the **Live Packet Monitoring** page, from where you can monitor live packet data for any Packet Processing Objects (PPOs) that you have chosen to be added (pinned) to this page. For, more information, see *The Live Packets Dialog Box and the Live Packet Monitoring Page* on page 542 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*. **Note :** By default, initially no PPOs are being monitored, and this icon is not visible. Once one or more PPOs have been added (pinned) to the **Live Packet Monitoring** page, this icon becomes visible in the Tray.

3. HOME PAGE

The **Home** page (see *Illustration 3*) appears immediately after logging in to the Web Interface, or after clicking **Home** from the Menu.

ILLUSTRATION 3 - HOME PAGE



The **Home** page lets you quickly:

- create new networks based on existing network templates via the **Examples** tab
- view and if necessary edit recently created networks via the **Recent** tab
- view currently active networks via the **Active** tab.

Note:

Initially when the NE-ONE contains no user created networks, the **Recent** tab and **Active** tab are empty, and upon logging in, the **Home** page defaults to showing the **Examples** tab. This lets you quickly create new networks based on the network templates supplied with the NE-ONE.
As networks are open (i.e. created or edited) and run, they are listed in **Recent** tab and **Active** tab, respectively. Once a user created network exists on the NE-ONE, upon logging in the **Home** page defaults to showing the **Recent** tab.

Note:

Existing networks can also be opened, edited, and launched via the File Browser. For more information, see *Opening and Playing Networks and Scenarios via the File Browser* on page 589 in *Chapter 13*, *The File Browser*.

The **Home** page also lets you:

- launch the **Network** page by clicking on the **+ NEW NETWORK** button
- launch a useful product tour video by clicking on the **PRODUCT TOUR** button
- upload a network file or scenario file from your local PC to your `/Private/networks` directory by clicking on the **LOAD FROM PC** button

The **Model Information** section of the **Home** page also immediately provides you with the following

useful product licensing and system build information:

- NE-ONE product code, which has the following format:

  NE1-<Edition>-<Licensed Hardware Ports>-<Maximum Bandwidth>

  where:

  - <Edition> is the NE-ONE edition type (this will vary according to the feature set that was sold to you by your sales representative).
  - <Licensed Hardware Ports> is the number of licensed Hardware ports available for use.
  - <Maximum Bandwidth> is the maximum bandwidth permitted on the fastest port of the group of licensed Hardware ports. For example, if an NE-ONE has two 1 Gigabit/s Hardware ports and two 10 Gigabit/s Hardware ports, the maximum permitted bandwidth displayed is 10G.
- Maximum number of licensed Network Objects (i.e. packet processing objects).
- Maximum number of licensed links.

  Note:
  If your NE-ONE is licensed with an unlimited number of links, the line showing the number of licensed links is not present.
- Number of licensed Hardware ports.
- Number of licensed Soft ports.

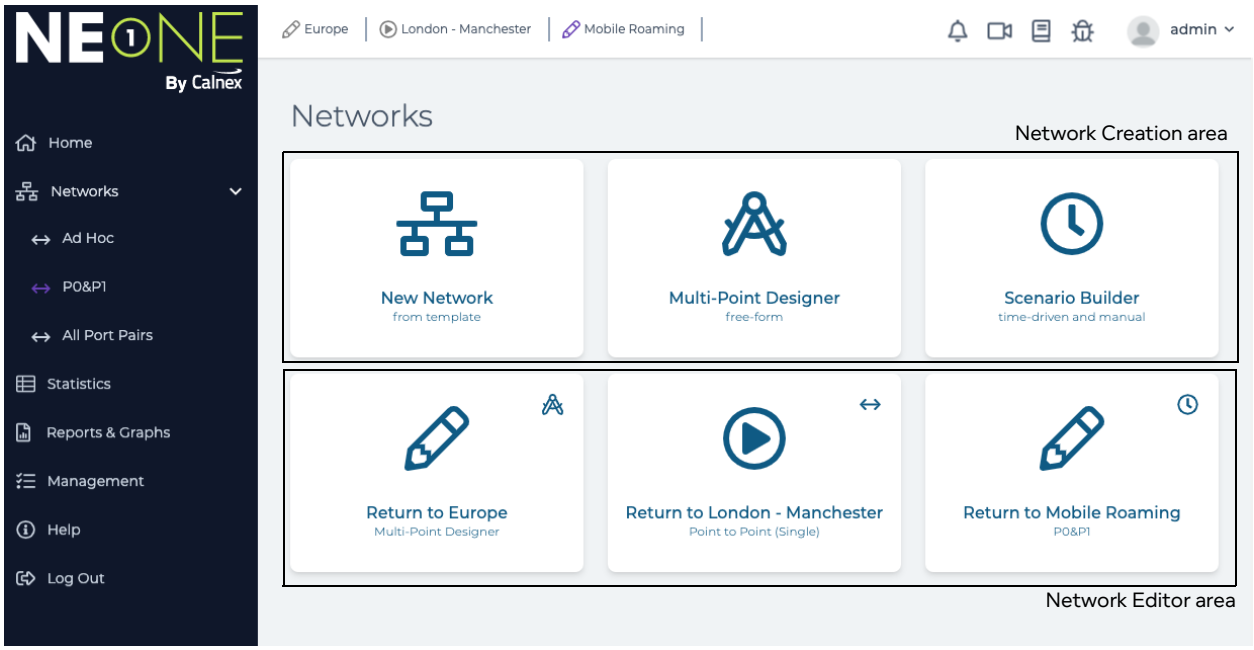
  Note:
  If your NE-ONE is not licensed to use the Port Manager feature, the line showing the number of licensed Soft ports is not present.
- License expiry date (once the license has expired, the Web Interface remains accessible).
- The maximum bandwidth permitted on the fastest port of the group of licensed Hardware ports. For example, if an NE-ONE has two 1 Gigabit/s Hardware ports and two 10 Gigabit/s Hardware ports, the maximum permitted bandwidth displayed is 10G.
- The product version, which has the following format: **<Year>.<Month>.<Incremental Build Number>**.
- Maintenance renewal date — once the maintenance renewal date has passed the NE-ONE remains fully functional. However, for unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date.
- The Scenario Builder feature licensing information, indicating whether or not the Manual and Automatic Scenario Builder features are licensed.
- The system build date of the following format: **<Year>:<Month>:<Day> <Hour>:<Minute>**.
- Port Manager licensing information, indicating whether or not the Port Manager feature is licensed.
- Service Manager licensing information, indicating whether or not the Service Manager feature is licensed.
- A **More...** link, which takes you to **License** page letting you manage the license on the NE-ONE. For more information, see *Viewing and Applying License Files* on page 83.

4. NETWORKS PAGE

The **Networks** page (see *Illustration 4*) appears after clicking **Networks** from the Menu, and contains the following two areas:

- Network Creation area
- Network Editor area

ILLUSTRATION 4 - NETWORKS PAGE



The network creation area of the **Networks** page lets you do one of the following:

- Launch the Network Wizard using predefined network topology templates.

  Clicking on the **New Network** tile opens the Network Wizard page which lets you create a network based on one of the different network topology templates.

  - For more information, see *The Network Wizard Page (From a Point-to-Point Perspective)* on page 240, in *Chapter 9*, *Creating and Running Point-to-Point Networks*.
  - For more information, see *The Network Wizard Page (from a Multi-Point Perspective)* on page 308, in *Chapter 10*, *Creating and Running Multi-Point Networks*.

  Note:

  The Multi-Point Designer and associated Multi-Point network topologies (i.e. Fully Meshed, Hub and Spoke, Cloud, and Free Form) are only available with the Multi-Point Designer feature. Depending on your license, the Multi-Point Designer and associated Multi-Point network topologies may be either activated or deactivated.

- Launch the Free Form **Multi-Point Designer** page.

  Clicking on the **Multi-Point Designer** tile opens a **Network Name** dialog box that prompts you to specify a new network name. Once you have specified and confirmed the new network name, the main area of the Web Interface updates with **Multi-Point Designer** page (in Free Form), from where you can create networks of any network topology.

- Launch the Scenario Builder.

  Clicking on the **Scenario Builder** tile opens the Scenario Builder page, which lets you either load, run, and stop an existing scenario, or create a new time based scenario (combination of networks with transitions).

The network editor area of the **Networks** page lists all the networks and scenarios that are open (i.e. either stopped for editing/creation ( )) or playing ( ). Each open network and scenario is represented by a tile, which has the following layout:

- the bottom of the tile displays the name of the network/scenario
- the middle of the tile displays a status icon for the open network/scenario, as follows:
  - represents stopped for editing/creation
  - represents currently playing
- the top right of the tile displays an icon representing the network or scenario type, as follows:
  - ↔ represents a Point-to-Point type network
  - represents a Multi-Point type network
  - represents a scenario

Note:

Initially when the NE-ONE has no open or playing networks or scenarios, the Network Editor area is empty. As networks or scenarios are opened (edited or being created) or running, they are listed in the Network Editor area of the Web Interface.

Clicking on the tile of an existing network or scenario within the Network Editor area opens it in the Main area of the Web Interface, letting you manage (i.e. edit, play, or stop) the selected network/scenario.

5. NETWORK PORT PAIR PAGE

The **Network Port Pair** page (see *Illustration 5*) appears after either:

- clicking a pre-defined port pair ( ) from within the expanded **Networks** item in the Menu, or
- selecting **Management > ↔ Port Pairs**, and clicking on a port pair tile in the **Port Pairs** page (*Illustration 38* on page 157) that appears.

Note:

Initially when the NE-ONE contains no pre-defined port pairs, the **Networks** item in the Menu contains no pre-defined port pairs, but only the **Ad Hoc** port pair item and **All Port Pairs** item. The **Ad Hoc** port pair item lets you create a temporary on-the-fly port pair for a networks. The **All Port Pairs** item opens the **Port Pairs** page where existing pre-defined port pairs can be managed.
Once an administrator has created, named, colored a port pair, and assigned the port pair to another user, that port pair will appear under the **Networks** item in the Menu if the user has starred (favorited) it.

5-1. Network Port Page Areas

The **Network Port Pair** page contains the following two areas:

- Port Pair Network Creation area
- Port Pair Network Editor area

The Port Pair Network Creation area of the **Network Port Pair** page lets you do one of the following for the selected port pair:

- Launch the Port Pair Network Wizard using one of the point to point templates.
  Clicking on the **New Network** tile opens the Port Pair Network Wizard page (see *The Port Pair Network Wizard Page* on page 242, in *Chapter 9*, *Creating and Running Point-to-Point Networks*), which lets you create either a Point to Point (Single) or Point to Point (Dual) network for the selected port pair.

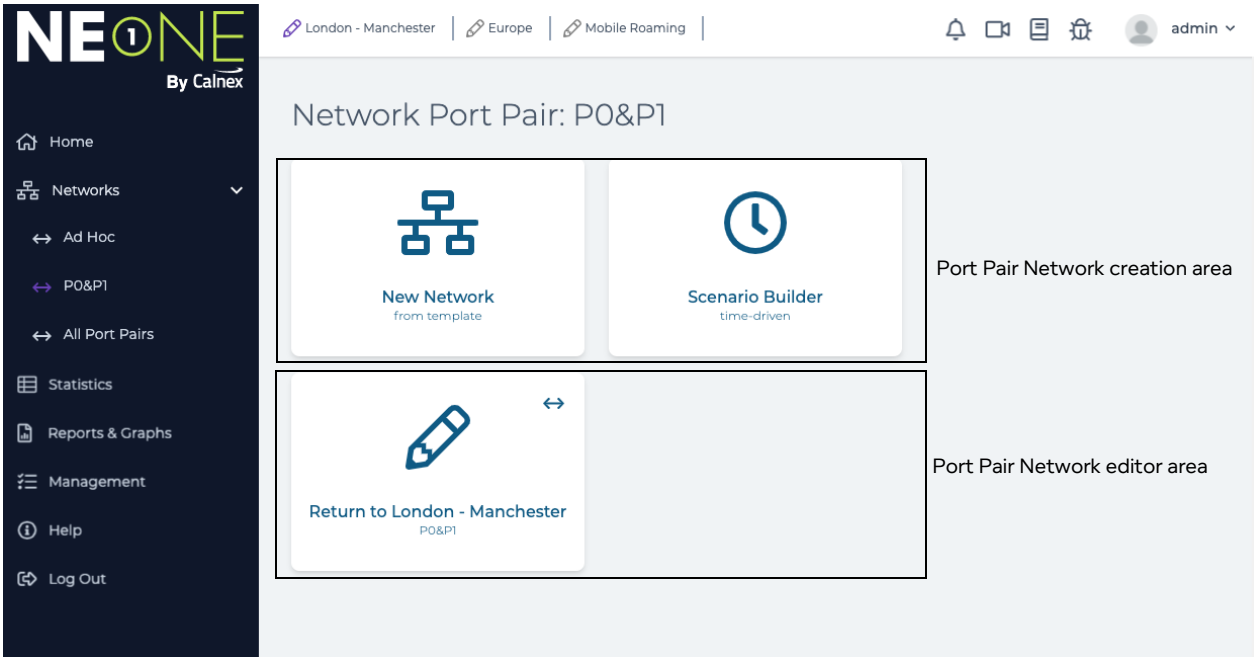
- Launch the Scenario Builder.

  Clicking on the **Scenario Builder** tile opens the **Scenario Builder** page, which lets you either load, run, and stop an existing scenario, or create a new time based scenario for the selected port pair.
- Configure the port addressing and default transmission settings.

  Clicking on the **Port Settings** tile opens the **Port Setting** page, which lets you configure the port addressing and default transmission settings for the selected port pair. For more information, see *Port Pair Settings* on page 162 in *Chapter 5*, *Ports and Services Management*.

  Note: Since an Ad Hoc port pair is a temporary 'on-the-fly' port pair for a network, port settings cannot be configured for an Ad Hoc port pair. Port settings can only be configured for pre-defined port pairs.

ILLUSTRATION 5 - NETWORK PORT PAIR PAGE



The Point Pair Network Editor area of the **Network Port Pair** page lists existing networks and scenarios for the selected port pair.

Note:

Initially when the NE-ONE contains no networks or scenarios associated with the selected port pair, the port pair network editor area is empty. As networks or scenarios are created for a selected port pair, they are listed in the Port Pair Network Editor area of the **Network Port Pair** page.

Clicking on an existing network or scenario within the Port Pair Network Editor area opens it in the main area of the Web Interface, letting you manage (i.e. edit, play, or stop) of the selected network/scenario for the selected port pair.

5-2. Networks Menu Port Pair Items

The **Networks** menu contains sub-menu items related to port pairs.

Depending on whether or not the Port Manager feature is activated on the NE-ONE, pre-defined port pairs will either already exist or not already exist, as follows:

- If the Port Manager feature is deactivated on the NE-ONE, then by default a set of pre-defined hardware port pairs will already be available and pre-configured, and will appear under the **Networks** item.
- If the Port Manager feature is activated on the NE-ONE, then by default, the NE-ONE is not configured with any point pairs. Port pairs can be created between the different port types using the Port Manager.

  In this case, initially when the NE-ONE (with Port Manager feature activated) contains no pre-defined port pairs, the **Networks** menu contains only the two following sub-menu items:

  - ↔ **Ad Hoc** port pair item. Clicking this launches a pair of **Choose Left Port** and **Choose Right Port** dialog boxes letting you select the left and right ports for creating a temporary on-the-fly port pair, which will be used for a new Point-to-Point type network. Once the temporary port pair is created, you are taken to the **Network Port Pair** page for that temporary port pair, from where you can create a new Point-to-Point network.
    Note: as long as you save them, any Point-to-Point type network created via a temporary port pair is not lost (i.e. they are not temporary like the port pair they were initially assigned to when you created the network). Saved Point-to-Point type networks can be launched later on either another temporary Ad Hoc port pair, or a pre-defined port pair.
  - ↔ **All Port Pairs** item opens the **Port Pairs** page where existing pre-defined port pairs can be managed. For more information on managing port pairs, see *Managing Port Pairs* on page 156 in *Chapter 5*, *Ports and Services Management*.

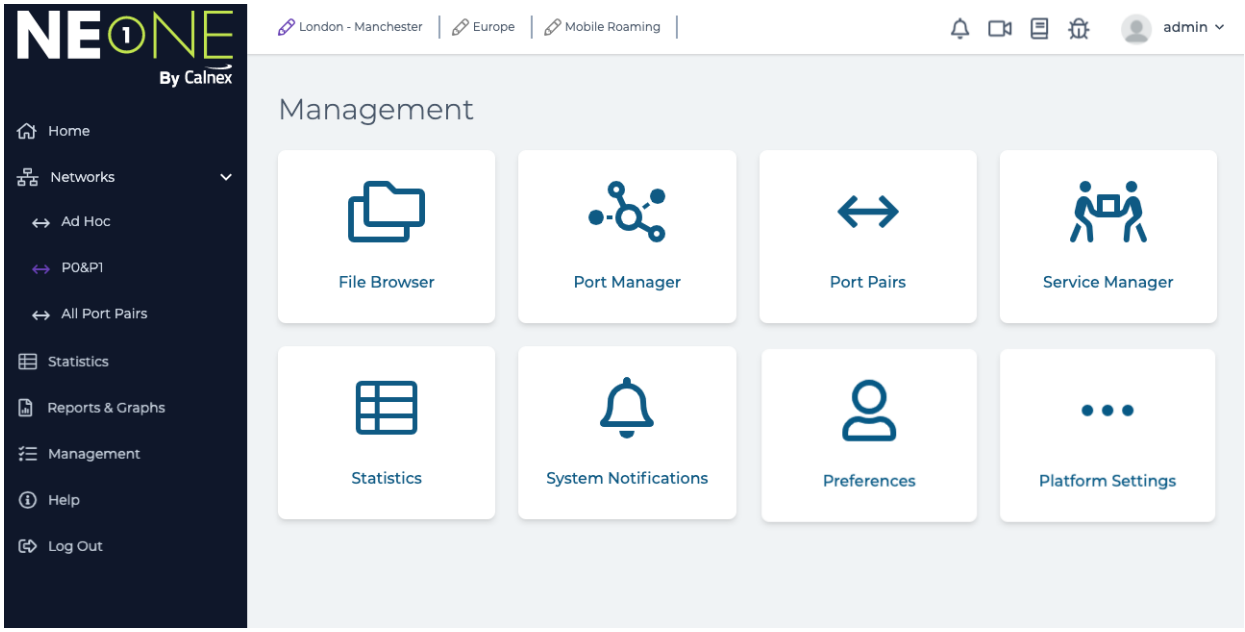
  Once an administrator has created, named, colored a port pair, and assigned the port pair to another user, that port pair will appear under the **Networks** item in the Menu if the user has starred (favorited) it.

6. MANAGEMENT PAGE

The **Management** page (see *Illustration 6*) appears after clicking **Management** from the Menu, and contains a set of management tiles that let you manage all aspects of the NE-ONE.

Note:
The management tiles that are visible vary according to the user type (i.e. admin or non-admin) logged in to the Web Interface.

ILLUSTRATION 6 - MANAGEMENT PAGE



Clicking on a management tile (see *Table 5*) opens an appropriate page in the Main area of the Web Interface.

TABLE 5 - MANAGEMENT TILES

Management Tile	Tile Icon	Description
File Browser		Opens the **File Browser** page (see *Illustration 185* on page 579) from where you can navigate the local filing system NE-ONE in order to perform various tasks such as: • opening a network or scenario file • opening a network or scenario file in script editor • share a network or scenario with another user A full description of the File Browser is beyond the scope of this chapter. For more information, see *Chapter 13*, *The File Browser* on page 579.
Port Manager*		Only available to admin type users. Opens a **Port Manager** page (see *Illustration 17* on page 103), allowing an admin user to create soft ports. For more information see, *Managing Ports* on page 103, in *Chapter 5*, *Ports and Services Management*.
Port Pairs		Only available to admin type users. Opens a **Port Pairs** page (see *Illustration 38* on page 157), allowing an admin user to create port pairs, modify existing port pairs and define whether a pre-defined port pair appears under the **Networks** item in the Menu. For more information see, *Managing Port Pairs* on page 156 in *Chapter 5*, *Ports and Services Management*.

Management Tile	Tile Icon	Description
Service Manager*		Only available to admin type users. Opens a **Services** page (*Illustration 49* on page 177), allowing an admin user to create and modify services which run background tasks (performing default transmission of data between ports or relaying of DHCP requests on a DHCP helper service). Once created and enabled, the service runs as a background task on the NE-ONE. For more information see, *Managing Services* on page 177 in *Chapter 5*, *Ports and Services Management*.
Statistics		Opens the **Statistics** page (see *Illustration 160* on page 527), which is the central location listing the statistics of the following objects from where you launch packet capture or data graphing for an object: • network objects (i.e. links and nodes) associated with any currently active (running) networks • framework objects (i.e. hardware port, soft port, port container, or service) For more information, see *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing* on page 525.
System Notifications		Opens the **System Notifications** page, from where you can view a chronological list of system level events, categorized by event type. For more information, see *Viewing System Notifications* on page 233 in *Chapter 8*, *General System Procedures*.
Preferences		Opens the **Preferences** page (see *Illustration 67* on page 235), from where you can access different user preferences. Allows the currently logged in user change their password, change the Web Interface language, and show/hide unlicensed features. For more information, see *User Related Preferences via the User Preferences Page* on page 235 in *Chapter 8*, *General System Procedures*.
Platform Settings		Only available to admin type users. Opens the **Platform Settings** page (see *Illustration 7*), which contains a set of platform settings tiles (see *Table 6*) that allow an admin user to manage platform specific aspects of the NE-ONE.
*- The Port Manager feature and Service Manager feature are premium features. Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated.		

7. PLATFORM SETTINGS PAGE

The **Platform Settings** page (see *Illustration 7*) appears after clicking **Management > ··· Platform Settings** from the Menu, and contains a set of tiles that let you manage all the platform specific aspects of the NE-ONE.

Note:

The **Platform Settings** page is only visible for admin type users logged in to the Web Interface.

ILLUSTRATION 7 - PLATFORM SETTINGS PAGE

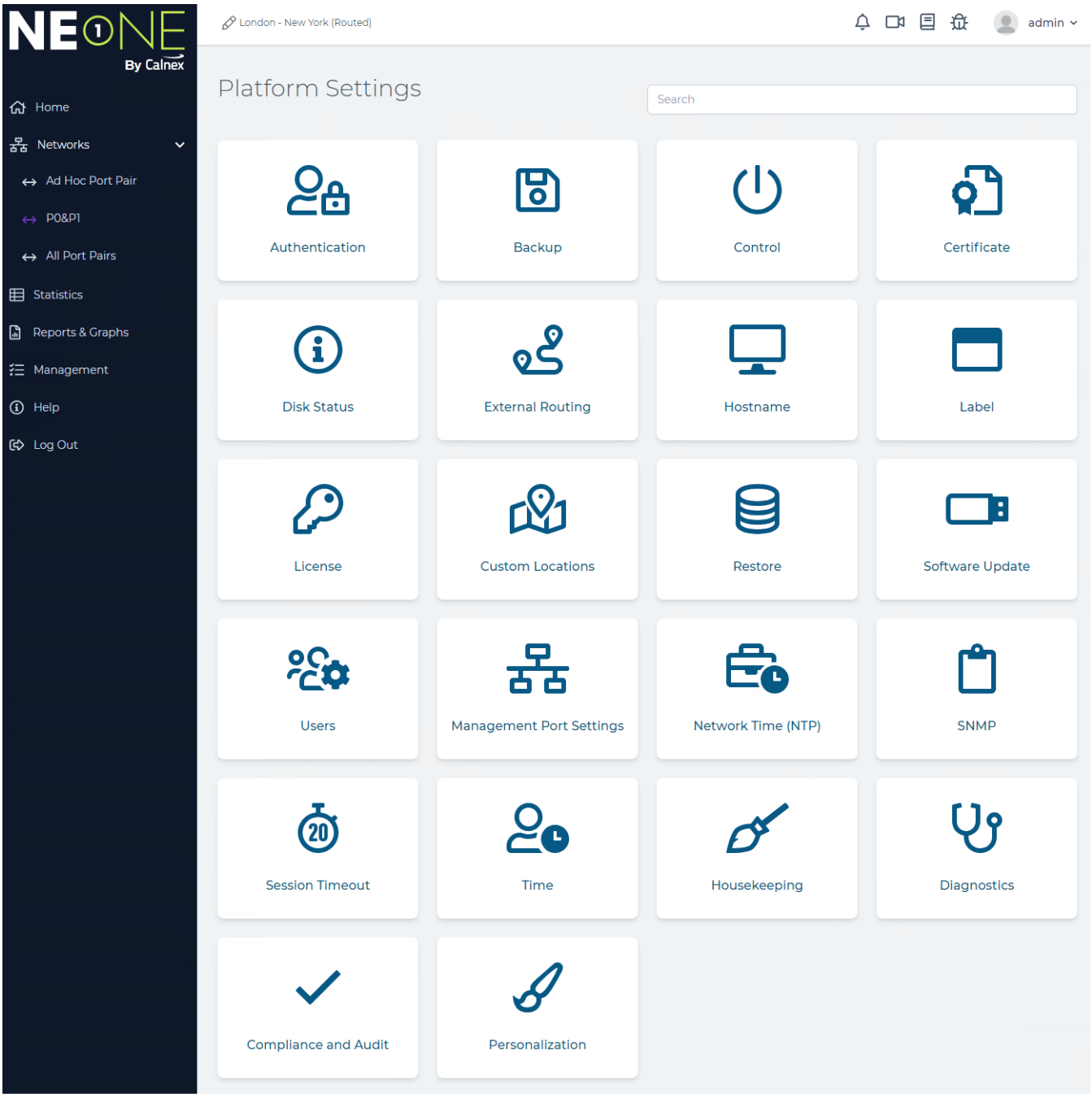
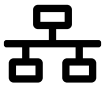


TABLE 6 - PLATFORM SETTINGS TILES

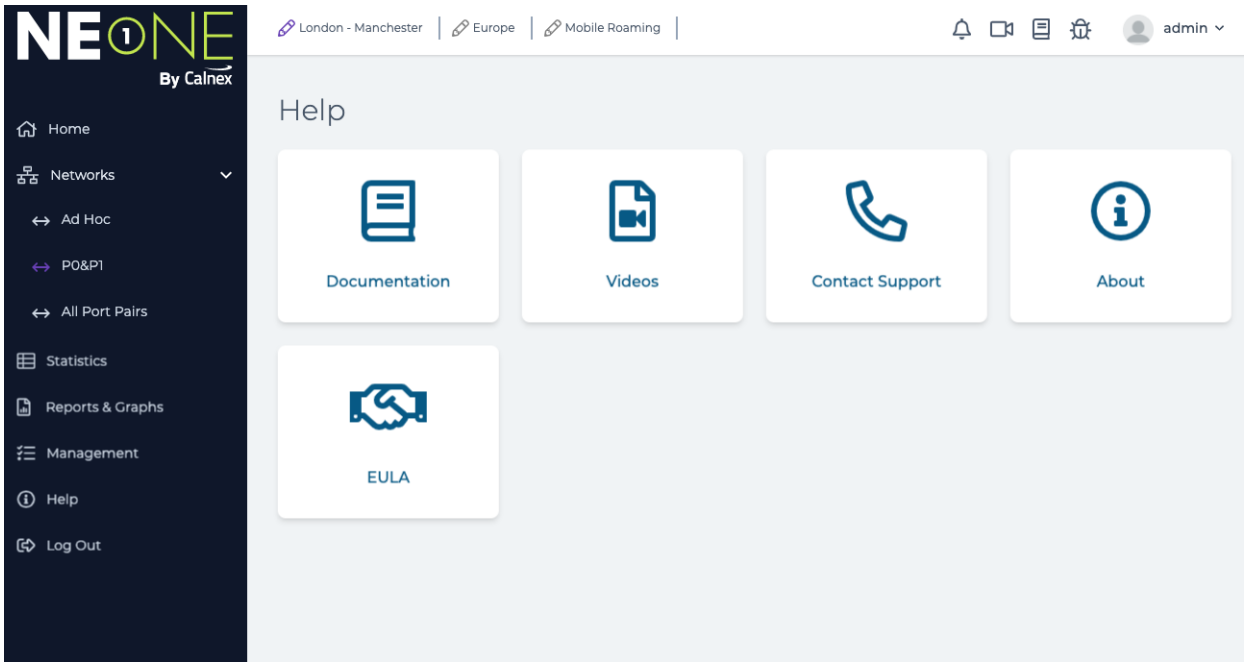
Platform Settings Tile	Tile Icon	Description
Authentication		Opens an **Authentication** page, allowing an admin user to optionally configure the NE-ONE to use either an LDAP or RADIUS server as its user authentication method if the Advanced Authentication feature is activated. For more information, see *Configuring the Authentication Method* on page 76 in *Chapter 4*, *Installation and Configuration*.
Backup		Opens a **Backup** page, allowing an admin user to view the existing backup history (if it exists), download the historical backup files (if they exist), and create/download a current backup of the NE-ONE user accounts, log files, and settings. For more information, see *Backing up the System* on page 220 *Chapter 7*, *System Maintenance*.
Control		Opens a **Control** page, allowing an admin user to shut down or reboot the NE-ONE. For more information, see *Controlling the System* on page 219 *Chapter 7*, *System Maintenance*.
Certificate		Opens a **Certificates** page, allowing an admin user to: • view the status of the SSL certificate currently installed on the NE-ONE • update the NE-ONE with a new SSL certificate and private key For more information, see *Installing and Updating Root SSL Certificates* on page 81 in *Chapter 4*, *Installation and Configuration*.
Disk Status		Opens a **Disk Status** page, allowing an admin user to view the disk status of NE-ONE. For more information, see *Monitoring System Disk Usage* on page 225 *Chapter 7*, *System Maintenance*.
External Routing		Opens an **External Routing** page, allowing an admin user to optionally configure external routing on the NE-ONE (if the NE-ONE is implemented within a network environment that uses dynamic routing). For more information, see *Configuring External Routing* on page 91 in *Chapter 4*, *Installation and Configuration*.
Hostname		Opens a **Hostname** page, allowing an admin user to set the hostname of the NE-ONE. For more information, see *Configuring the Hostname* on page 67 in *Chapter 4*, *Installation and Configuration*.
Label		Opens a **Label** page, allowing an admin user to optionally change the label (defined by the title tag) that appears in a web browser for the NE-ONE's Web Interface. For more information, see *Configuring the Web Interface Label* on page 68 in *Chapter 4*, *Installation and Configuration*.
License		Opens a **License** page, allowing an admin user to view the existing license information, and update the license on the NE-ONE. For more information, see *Viewing and Applying License Files* on page 83 in *Chapter 4*, *Installation and Configuration*.
Custom Locations		Allows an admin user to create a custom location with longitude and latitude coordinates. Once a custom location is created, it can be used for setting the location of a node within a network. For more information, see *Custom Locations* on page 84 in *Chapter 4*, *Installation and Configuration*.
Restore		Opens a **Restore** page, allowing an admin user to restore a backup from either an uploaded backup file, or restore a backup file from a list of backups that were previously created and/or uploaded locally on the NE-ONE. For more information, see *Restoring a System Backup* on page 223 *Chapter 7*, *System Maintenance*.

Platform Settings Tile	Tile Icon	Description
Software Update		Opens a **Software Update** page, allowing an admin user to view the existing software update history, and update the software on the NE-ONE. For more information, see *Viewing and Updating the System Software* on page 218 in *Chapter 7*, *System Maintenance*.
Users		Opens a **Users** page, allowing an admin user to manage the user accounts on the NE-ONE. For more information, see *Chapter 6*, *User Administration*.
Management Port Settings		Opens a **Management Port Settings** page, allowing an admin user to set the networking configuration (i.e. IP Address, Netmask, and Gateway) of the NE-ONE's management port. For more information, see *Configuring the Management Port Settings* on page 60 in *Chapter 4*, *Installation and Configuration*.
Network Time (NTP)		Opens a **Network Time** page, allowing an admin user to optionally configure the NE-ONE to use a network time protocol (NTP) servers for its time instead of a manually set time. For more information, see *Network Time Protocol (NTP) Configuration* on page 65 in *Chapter 4*, *Installation and Configuration*.
SNMP		Opens a **Network SNMP** page, allowing an admin user to optionally configure the NE-ONE to work with the Simple Network Management Protocol network management system. For more information, see *Configuring SNMP* on page 75 in *Chapter 4*, *Installation and Configuration*.
Session Timeout		Opens a **Session Timeout** page, allowing an admin user to define the NE-ONE's user session timeout value in seconds and configure whether user sessions can timeout when networks/scenarios are running. For more information, see *Session Timeout Configuration* on page 82 in *Chapter 4*, *Installation and Configuration*.
Time		Opens a **Time** page, allowing an admin user to define the NE-ONE's date, time and time zone. For more information, see *Time Configuration* on page 65 in *Chapter 4*, *Installation and Configuration*.
Housekeeping		Opens a **Housekeeping** page, allowing an admin user to configure the housekeeping properties of the NE-ONE. For more information, see *Configuring Housekeeping* on page 69 in *Chapter 4*, *Installation and Configuration*.
Diagnostics		Opens a **Diagnostics** page, allowing an admin user to run a system diagnostics that creates a binary diagnostics file, which can be sent to Calnex support or your support representative. For more information, see *Running Diagnostics* on page 226 in *Chapter 7*, *System Maintenance*.
Compliance and Audit		Opens a **Compliance and Audit** page, allowing an admin user to optionally apply a compliance and audit conditions that users will have to accept before using the NE-ONE. For more information, see *Applying a Compliance and Audit Acceptance Agreement* on page 73 in *Chapter 4*, *Installation and Configuration*.
Personalization		Opens a **Personalization** page, allowing an admin user to optionally personalize the appearance of the login page of the NE-ONE. For more information, see *Personalizing the Login Page* on page 71 in *Chapter 4*, *Installation and Configuration*.

8. HELP PAGE

The **Help** page (see *Illustration 8*) appears after clicking **Help** from the Menu, and contains a set of help tiles that let you view support related aspects of the NE-ONE.

ILLUSTRATION 8 - HELP PAGE



Clicking on a help tile (see *Table 7*) opens an appropriate page in the Main area of the Web Interface.

TABLE 7 - HELP TILES

Management Tile	Tile Icon	Description
Documentation		Opens the embedded user manual (in a separate browser tab), starting on the first page.
Videos		Opens the **Videos** page containing a list of all the help videos. Clicking on a video will open it in another web browser tab.
Contact Support		Opens a temporary dialogue box (that closes after several seconds) with the contact details of the Calnex support team.
About		Opens the **About** page, which provides the model information (same as that of the that displayed in the Home page), and general attributions information about the NE-ONE.
EULA		Opens the **EULA** page, which contains the end user license agreements associated with the NE-ONE.

This page is intentionally left blank.

CHAPTER 4 INSTALLATION AND CONFIGURATION

1. INTRODUCTION

This chapter is applicable to admin users, and describes the installation and configuration procedures that you use to initially install and configure the NE-ONE in your network.

1-1. Implementation of SDTNs with the NE-ONE

Before proceeding to the steps in the sub-sections below, it is useful to discuss some examples of the different ways in which the Software Defined Test Networks (SDTNs) on the NE-ONE can be implemented within a network.

ILLUSTRATION 9 - EXAMPLE OF THREE SOFTWARE DESIGNED TEST NETWORKS

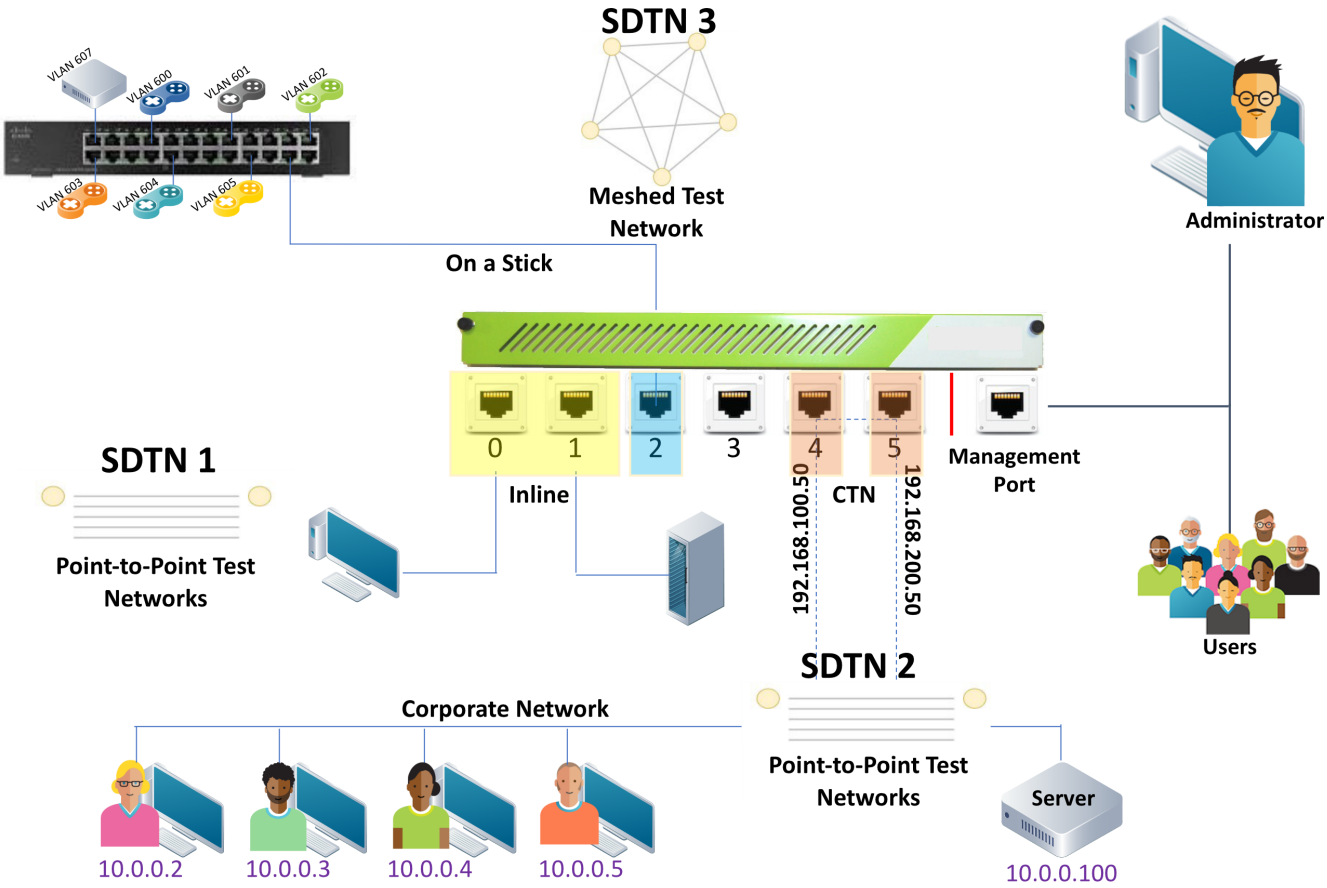


Illustration 9 shows an example of an NE-ONE being used to implement the following SDTNs:

- Inline (SDTN1)
  - Uses two out-of-band ports which can be bridge (Layer 2) or route (Layer 3).
  - Ethernet switches can be connected to the out-of-band ports so that multiple devices can use the Point-To-Point test network at the same time.
  - The Point-To-Point test network is setup with the appropriate impairments are created and configured using the Point-To-Point Designer. See *Creating Point-to-Point Networks (Single)* on page 265 in *Chapter 9*, *Creating and Running Point-to-Point Networks* as an example. In this example, port addressing is enabled on hardware ports 0 and 1 as the client test computers are on one network (i.e. 10.0.0.X) while the test server is on another network (e.g. 192.168.200.X).

  - There is no limit on the number of devices or users that can use the test network.
  - In this example, this configuration has no dynamic routing, and does not require external routes to be configured on the NE-ONE. However, if required, you can configure dynamic routing if needed, in which case external routing would need to be configured using the **External Routing** page (see *Configuring External Routing* on page 91).
- CTN - Continuous Test Network (SDTN2).

  The concept of the CTN is to let "client" users access the same server via either the production network (corporate network without any impairments) or the test network (via impairments that are defined in the NE-ONE).
  - Two out-of-band ports of the NE-ONE are attached to the corporate network.
  - The Network Administrator sets up two pools of IP addresses (typically, by using an alternate sub-net) for both the users and the server.

    One pool is assigned to the "production" environment (for DevOps use for example), where the packets are routed so they do not pass through the NE-ONE.

    The other pool is assigned to the "alternate" test network, where the packets are routed to pass through the NE-ONE instead.
  - The Network Administrator also sets up the core routers so that the "alternate" IP addresses are routed through the NE-ONE, while the "production" IP addresses are not routed through the NE-ONE.
  - The NE-ONE Administrator (normally a different person to the Network Administrator) configures client to server mappings on the NE-ONE by creating Static NAT soft ports. The Static NAT soft ports are configured to translate the "alternate" IP addresses to "production" IP addresses. For more information, see *Creating a Static NAT Soft Port* on page 138 in *Chapter 5*, *Ports and Services Management*.
  - When the user wants to access the server via the "alternate" test network, they specify the "alternate" NE-ONE IP Address instead of the normal "production" server IP address. In this case, the core routers redirect the users packets to the NE-ONE where impairments are introduced, and the Static NAT soft ports on the NE-ONE will translate the alternate address to production address, forwarding/receiving packets to/from the server.
  - When the user wants to access the server directly via the "production" network, they specify the normal "production" server IP address. In this case, the core routers will route the users packets to avoid passing through the NE-ONE and remain entirely within the corporate network without any impairments.
- On-a-stick (SDTN3)
  - Uses one out-of-band port for sending and receiving data between the NE-ONE and the VLAN switch.
  - The out-of-band port on the NE-ONE is connected to the trunk port on the VLAN switch, and each test device is on a separate VLAN connected to the VLAN switch.
  - The NE-ONE Administrator creates a VLAN soft ports for each VLAN so that each user has their own test network. For example, see *Creating a VLAN Soft Port* on page 107 in *Chapter 5*, *Ports and Services Management*.
  - The NE-ONE Administrator also creates a set of IPv4 soft ports under each VLAN soft port so that each user has their own test network, and can define their own SDTN. For example, see *Creating an IPv4 Soft Port* on page 114 in *Chapter 5*, *Ports and Services Management*. Each IPv4 soft port .
  - If necessary, routing can be setup between each VLAN so that devices/users can communicate

with each other.
If the routing between the VLAN and devices is configured to use static routing, external routes do not need to be configured on the NE-ONE.
If the routing between the VLAN and devices is configured to use dynamic routing, external routes need to be configured on the NE-ONE using the **External Routing** page (see *Configuring External Routing* on page 91).

- The test networks with the appropriate impairments can then be created and configured by the users via either the Point-to-Point Designer or Multi-Point Designer. The users will create their own SDTNs within each VLAN using the IPv4 soft ports that were assigned to them, and applying those IPv4 soft ports to each of the nodes in their SDTNs. In the example of *Illustration 9*, a Fully Meshed Multi-Point network is created by one user.

All three SDTNs can run at the same time with different test networks and different impairments.

Note:
The implementation of the Inline SDTN (SDTN1) is possible with all NE-ONEs. The implementation of the On-a-stick (SDTN3) and Continuous Test Network (SDTN2) SDTNs are only possible with NE-ONEs that have the Port Manager feature enabled, since in these examples soft ports are required.

2. PREREQUISITES

Before installing the NE-ONE in your network, do the following:

1. Obtain the appropriate license from Calnex (*https://itrinegysupport.force.com*).

   Note:
   If you do not initially have a license, the NE-ONE will operate with limited functionality so that it can be licensed.
2. Check with Calnex if there are software updates available for the NE-ONE.
3. Check with your network administrator if the NE-ONE can have a manually assigned static IP address, or whether it needs to dynamically obtain an IP address from your network's DHCP server. In the case the NE-ONE uses a static IP address, get the following network parameters from the network administrator:
   - IP Address
   - Network Mask
   - Default Gateway
   - Primary DNS Server
   - Secondary DNS Server

   Note:
   Ask the network administrator for the fully qualified domain name (FQDN) they will apply to the NE-ONE on the organization's domain name servers (DNS).
   If you choose to use a dynamic IP address, the IP address of the NE-ONE risks changing with time. In this case it is recommended that you communicate the FQDN of the NE-ONE to your users in order for them to access the Web Interface.
4. Check with your network administrator if the hostname to be used for the NE-ONE.

   Note:
   If you do not specify a hostname for the NE-ONE, it will use NE-ONE.

   Note:
   If the organization's network contains more than one NE-ONE, Calnex recommends that a unique hostname is defined on each of the NE-ONEs.

5. Check with your network administrator if the organization uses either the LDAP or RADIUS authentication method, and if it does, obtain the following:
   - Primary LDAP/RADIUS Server FQDN or IP address
   - Secondary Primary LDAP/RADIUS Server FQDN or IP address

   Note:
   LDAP and RADIUS authentication methods are only available with the Advanced Authentication feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.
6. Check with your network administrator if the organization uses Simple Network Management Protocol (SNMP) for its network management, and if does, obtain the community string, location, and contact.

   Note:
   At the current release, the NE-ONE does not support SNMP V3 username and password implementation.
7. Check with your network administrator if the organization uses a Root SSL Certificate (i.e. an SSL Certificate signed by a trusted Certificate Authority. If it does, obtain the Root SSL Certificate and Private Key from the organization's network administrator.

   Note:
   If the organization does not use a Root SSL Certificate, the NE-ONE will use the default supplied self-signed Calnex SSL Certificate. In this case, when users connect to the NE-ONE Web Interface for the first time, they will need to perform a few steps to accept the self-signed Calnex SSL Certificate. For more information, see *First time Web Interface access (accepting the default self-signed SSL certificate)* on page 27.
8. Check with your network administrator if the organization is using dynamic routing (adaptive routing) or static routing (non-adaptive routing). If the organization is using dynamic routing (adaptive routing), the network administrator will have chosen a routing protocol of preference (BGP, OSPF, OSPFv6, RIP, or RIPng) for the network. Ask the network administrator which routing protocol is implemented within the network, and the external routing tables that you need to define on the NE-ONE in order for the NE-ONE to inter-operate with the routing protocol that is implemented within the network.

   Note:
   At the time of publication, the NE-ONE currently supports BGP, OSPF, OSPFv6, RIP, and RIPng routing protocols. If your organization uses another routing protocol such as Interior Gateway Routing Protocol (IGRP) or Intermediate System to Intermediate System (IS-IS), contact your Calnex representative for more information on how and when those other routing protocols will be implemented on the NE-ONE.
9. If the NE-ONE is running on a virtual environment (i.e. VMWare or Openstack) or a cloud computing environment (i.e. Amazon Web Services (AWS) or Microsoft Azure), ensure that the environment has been set up for the NE-ONE.

   For more information on setting up the AWS cloud computing service to support the NE-ONE, refer to the *NE-ONE AWS Installation Guide*.

   For more information on setting up the Microsoft Azure cloud computing service to support the NE-ONE, refer to the *NE-ONE Azure Installation Guide*.

3. INSTALLATION WORK FLOW

When you install a new NE-ONE use the installation work flow summarized in *Illustration 10* and *Illustration 11*.

Note:

The sections referenced by the installation work flow are generically written as individual procedures, and describe the full set of steps to take to navigate within the Web Interface. However, when you are already within the **Management** pages and **Platform Settings** pages of the Web Interface, you can click on the **BACK** button to return up one level. For more information on general Web Interface navigation principles, refer to *Chapter 3, NE-ONE Web Interface Overview*.

Note:

Some parts of the installation work flow in *Illustration 10* and *Illustration 11* may not be applicable, and depend on the features that are licensed with your edition of NE-ONE.

LDAP and RADIUS authentication methods are only available with the Advanced Authentication feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

The Port Manager feature is a premium feature. Depending on your license, the Port Manager feature may be either activated or deactivated.

The Service Manager feature is a premium feature. Depending on your license, the Service Management feature may be either activated or deactivated.

In *Illustration 10* and *Illustration 11* below, these features are indicated by thicker, dashed rectangles.

ILLUSTRATION 10 - INSTALLATION AND CONFIGURATION WORK FLOW

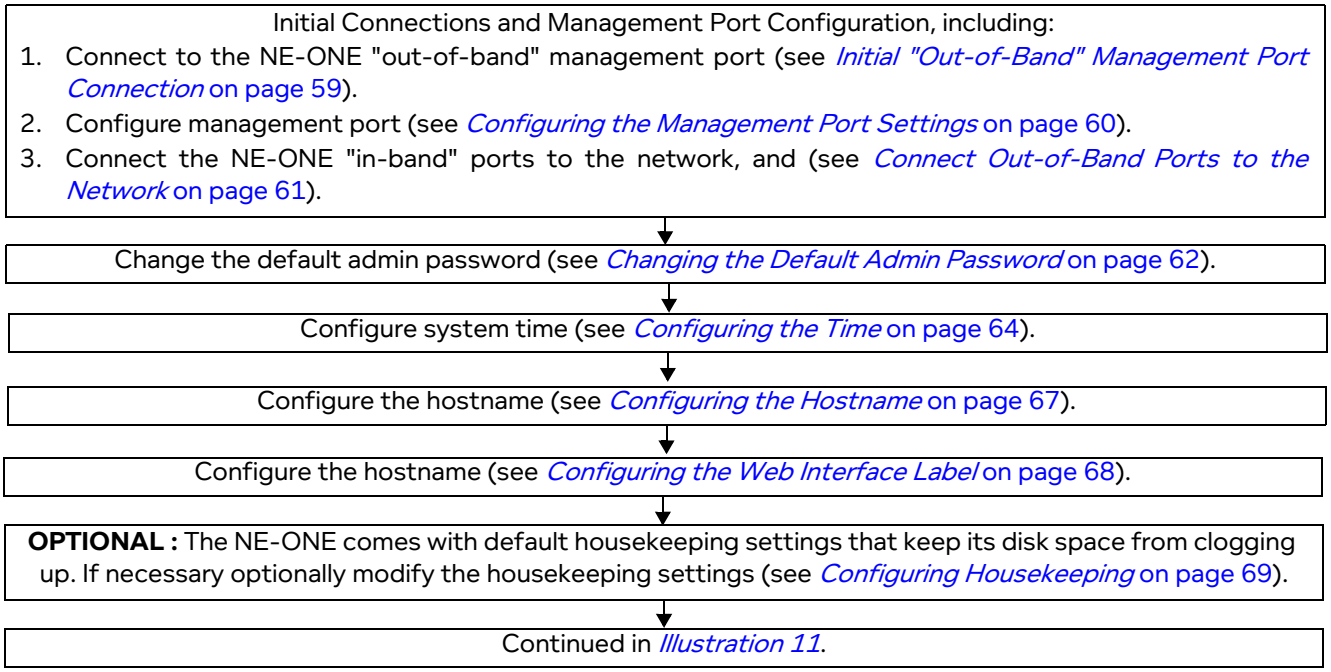
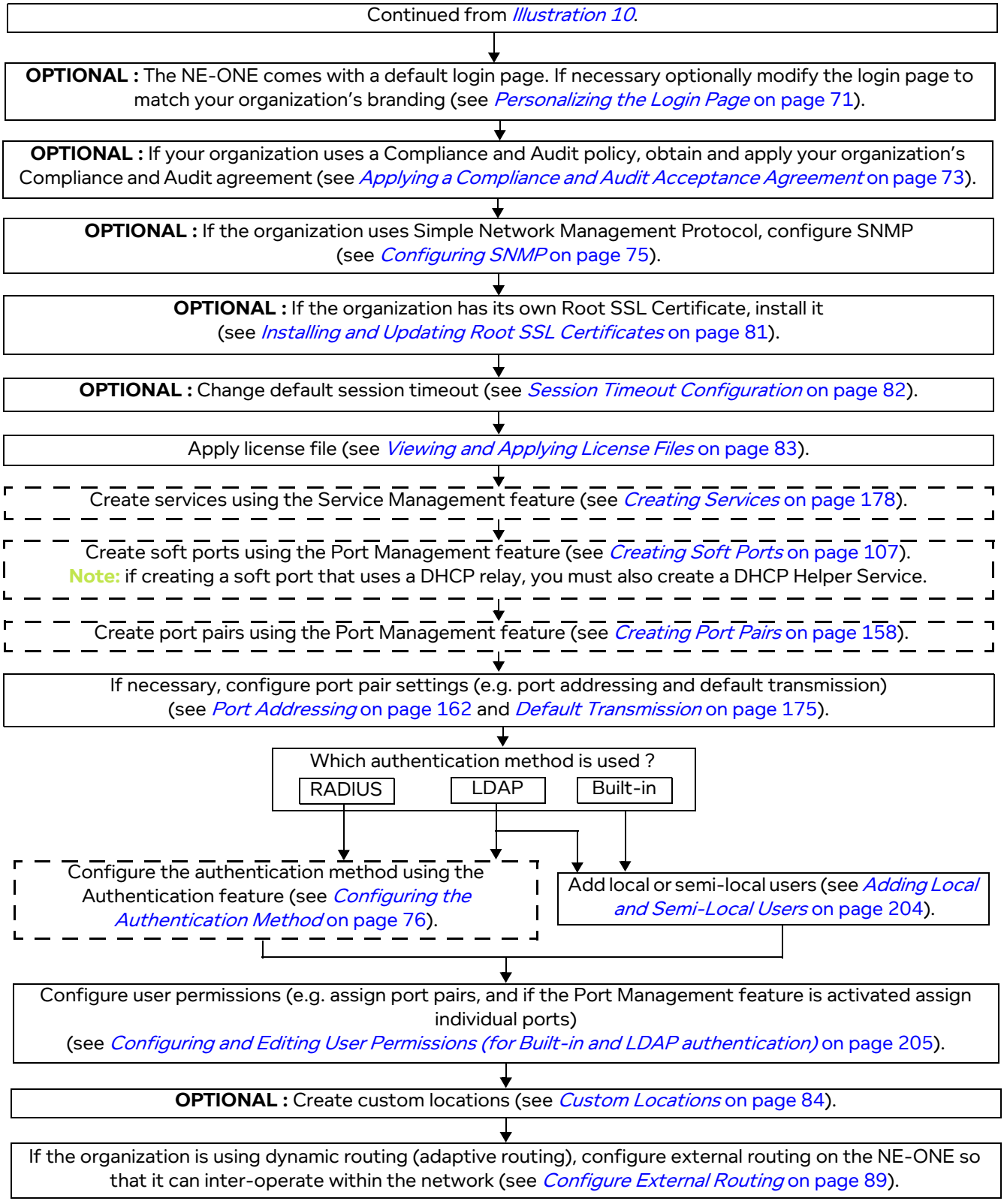


ILLUSTRATION 11 - INSTALLATION AND CONFIGURATION WORK FLOW (CONTINUED)



4. INITIAL CONNECTIONS AND MANAGEMENT PORT CONFIGURATION

Use this section when you install the NE-ONE for the first time within your network, or if you want to change how the NE-ONE is connected and configured within your network.

4-1. Initial "Out-of-Band" Management Port Connection

A *Setup Guide* is provided in the NE-ONE's packaging describing the initial steps you take to connect with the NE-ONE's "out-of-band" management port, and to access the Web Interface. Follow the steps described with the provided *Setup Guide*. The steps described with the provided *Setup Guide* vary according to the type of NE-ONE you have (see *Table 8*).

TABLE 8 - NE-ONE TYPE AND CORRESPONDING SETUP GUIDE INFORMATION

NE-ONE Type	Summary of type of information in provided Setup Guide
Physical : Desktop	• Because there is a visual method to view a dynamically assigned IP address on the NE-ONE via an LCD panel, the management port IP address obtained automatically via DHCP (if DHCP server exists and reachable in the network). • Connect NE-ONE's management port located on the rear panel to the network. • Use the NE-ONE's LCD panel to view and determine the dynamically assigned IP address of the management port. For more information, see *Show IP Address* on page 704 in the *Network Settings* section of *Chapter 16*, *The LCD Panel*. • If no IP address is dynamically assigned (because the network's DHCP server was not reachable) or you want to manually change the dynamically assigned IP address, use the front panel buttons to manually configure a static IP address for the management port. For more information, see *DHCP* on page 705 and *Static IP Address* on page 705 in the *Network Settings* section of *Chapter 16*, *The LCD Panel*. • Connect to the Web Interface via **https://<Management Port IP address>**
Physical : Rack mount (half rack or 1U)	• Because there's no visual method to view a dynamically assigned IP address, the default management port IP address configured on the NE-ONE is 192.168.0.10 (netmask 255.255.255.0). • Connect NE-ONE's management port located on the rear panel to the a laptop PC who's NIC is configured within the 192.168.0.0 network with netmask 255.255.255.255. • Connect to the Web Interface via **https://192.168.0.10**
Virtual Appliance (VMWare or OpenStack) Cloud Appliance (AWS or Microsoft Azure)	• The network interfaces of the NE-ONE will have been defined within the cloud computing environment. • The management port IP address is created and defined by the cloud computing environment. • Use cloud computing environment's interface to view and determine the IP address of the NE-ONE's management port. For more information on determining the IP address of the NE-ONE's management port within the AWS cloud computing service, refer to the *NE-ONE AWS Installation Guide*. For more information on determining the IP address of the NE-ONE's management port within the Microsoft Azure cloud computing service, refer to the *NE-ONE Azure Installation Guide*. • Connect to the Web Interface via **https://<Management Port IP address>**

Note:

Initially the NE-ONE contains a self-signed Calnex SSL Certificate. When connecting to the Web Interface for the first time, you need to accept the self-signed Calnex SSL Certificate according to *First time Web Interface access (accepting the default self-signed SSL certificate)* on page 27.

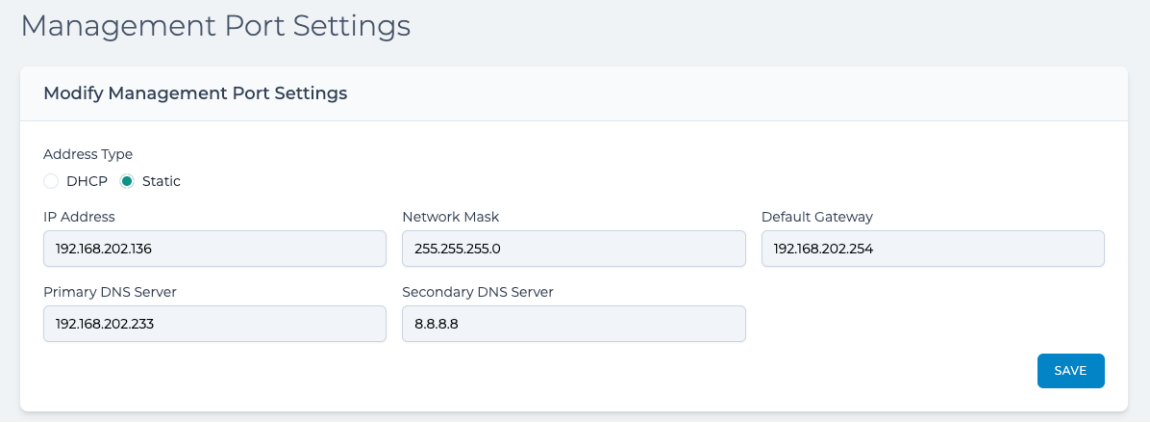
4-2. Configuring the Management Port Settings

Use this section when you install the NE-ONE for the first time, or if you want to change the existing network settings of the NE-ONE's management port.

As summarized in *Table 8* on page 59, depending on the type of NE-ONE you have, the NE-ONE is delivered with its management port to either obtain its network configuration automatically via a DHCP server (for Physical Desktop and Virtual Appliance NE-ONEs) or have a static network configuration (for the Physical Rack mount NE-ONEs).

Use the following steps to configure the network configuration of the NE-ONE's management port:

1. From the Web Interface, click **Management > Platform Settings > Management Port Settings**.



2. From the **Management Port Settings** page that appears, do the following:
   a. Enable the appropriate **Address Type** radio button:
      Enable the **DHCP** radio button if the NE-ONE is to get its network configuration from a DHCP server on the organization's network.
      Enable the **Static** radio button if the NE-ONE is to have a manually configured static IP address, network mask, default gateway, and DNS servers.
   b. If you enabled the **Static** radio button, additionally do the following:
      In the **IP Address** field, type the IP address for the NE-ONE (given to you by the network administrator).
      In the **Netmask** field, type the netmask used by the NE-ONE (given to you by the network administrator).
      In the **Default Gateway** field, type the IP address of the Default Gateway used by the NE-ONE (given to you by the network administrator).
      In the **DNS Server 1** field, type the IP address of the primary DNS server used by the NE-ONE (given to you by the network administrator).
      In the **DNS Server 2** field, type the IP address of the primary DNS server used by the NE-ONE (given to you by the network administrator).
   c. Click **SAVE**.
3. From the confirmation dialog that appears, click **OK**.

4-3. Connect Out-of-Band Ports to the Network

The NE-ONE needs to be connected "between" your user(s) and server(s) systems (or indeed any systems which you want to test in "impaired" networks) either directly or via switches and routers.

The simplest configuration of all is to connect the test user (client) to the NE-ONE and the NE-ONE to the server. This is often possible in a "lab" type environment (but rarely in a corporate network). With this configuration, there is no risk of other network activities impacting on the data flow. Such a configuration is shown by SDTN1 in *Illustration 9* on page 53, where the NE-ONE is directly connected in-line between the test user's client PC on hardware port 0 and the server on hardware port 1.

However, if your test users (clients) and server(s) are connected via switches, hubs and (possibly) routers (as is most usual), and cannot be connected directly, you can connect the NE-ONE at some other suitable point between the test users (clients) and the servers. One possible such configuration is shown by SDTN2 in *Illustration 9* on page 53, where the NE-ONE is indirectly connected in-line between multiple test user client PCs via a hub/switch/router on hardware port 3 and the server via a hub/switch/router on hardware port 4. In this configuration, if dynamic routing is being used by the routers, you must also configure external routing on the NE-ONE according to *Configure External Routing* on page 89.

A third possibility is that the NE-ONE is not physically connected between the client and server (or other devices) in the test, but rather network routing is set up to direct traffic from systems or networks under test to the NE-ONE, which can then be itself configured to route traffic to the target networks (having first "impaired" or "restricted" the traffic as required). Using this principle, the NE-ONE can be inserted into any desired configuration. The example configurations of SDTN1 and SDTN2 in *Illustration 9* on page 53 show just two possibilities. There are of course many other configuration possibilities such as inserting the NE-ONE in the uplink/downlink between two switches, placing it in a VLAN trunk and even using it as an "SDTN on a stick" as shown by the SDTN3 configuration *Illustration 9* on page 53. The advantage of this type of configuration is that you only use up one hardware port of the NE-ONE. In this configuration, if dynamic routing is being used by the routers, you must also configure external routing on the NE-ONE according to *Configure External Routing* on page 89.

If you are using a physical (desktop or rack mount) NE-ONE, connect the out-of-band ports of the NE-ONE to your network as required using an Ethernet cable. In the example of *Illustration 9* on page 53, the NE-ONE ports are connected as follows:

- Hardware port 0 is connected to a test user's client PC
- Hardware port 1 is connected to a server
- Hardware port 2 is connected to a port on a Cisco switch which is configured with different VLANs.
- Hardware port 3 is connected within the corporate network
- Hardware port 4 is connected within the corporate network

Note:

At this stage the NE-ONE's in-band ports do not need to be connected to your network. You can connect them later on at any point during the configuration work flow summarized in *Illustration 11* on page 58.

If you are using an NE-ONE Virtual Appliance, use the virtual appliance management tools to configure (map) the out-of-band ports of the NE-ONE Virtual Appliance to virtual hardware ports in your virtual environment, then connect the physical NIC of the server hosting the NE-ONE Virtual Appliance to the network.

Note:

It is beyond the scope of this *User and Administration Guide* to describe how the NE-ONE Virtual Appliance's out-of-band ports are configured (mapped). The *Setup Guide* and other instructions

provided in the NE-ONE Virtual Appliance's packaging describe how to configure the NE-ONE Virtual Appliance's out-of-band ports.

Note:
If you are using an NE-ONE Virtual Appliance, the physical NIC of the server hosting the NE-ONE Virtual Appliance will probably already be connected to the network.

Note:
By convention, the example test networks described in this *User and Administration Guide* it's assumed that for two-port in-line configurations that test users (clients) are connected to the NE-ONE's hardware port 0 and the servers to the NE-ONE's hardware port 1, but this is not mandatory. Additionally, if you have the Port Manager feature activated on the NE-ONE, which lets you configure port pairs for your test users, you could for example leave hardware port 0 assigned to an "SDTN on a stick" configuration, and create a port pair on hardware ports 1 and 2 for a two-port in-line configurations. The Port Manager feature gives you the flexibility in letting you define how you want to allocate single ports and port pairs.

5. CHANGING THE DEFAULT ADMIN PASSWORD

The default password for the local (built-in) admin user on the NE-ONE is admin. Upon connecting to the Web Interface for the first time, you will be prompted to change the password for the admin user to another password other than admin. Once you have changed the default admin password you will be able to access the Web Interface pages.

Use the steps below to change the default admin user password.

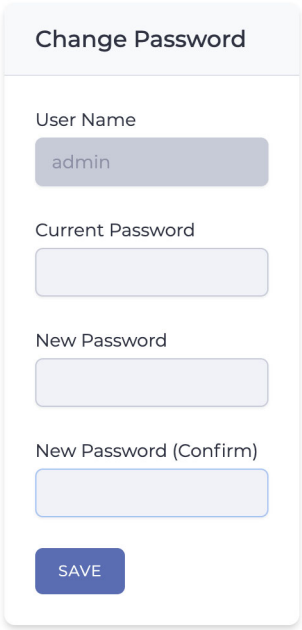
1. Launch your preferred web browser, and specify the following URL in the address bar:

   `https://<IP address or hostname>`

   where `<IP Address or hostame>` is the IP Address or hostname of the NE-ONE Management Port.

   A login page appears.

2. From the login page that appears, type **`admin`** in the **Username** field and type **`admin`** in the **Password** field, then click **LOGIN**.
   Upon successfully logging in, the following dialog box appears, prompting you to change the admin password.



3. In the **Current Password** field, type **`admin`**.
4. In the **New Password** and **New Password (Confirm)** fields, type the new password for the admin user.
5. Click **SAVE**.
   A **Changed!** dialog box appears confirming that the admin password has been successfully changed.
6. From the **Changed!** dialog box that appears, click **OK**.
   You are automatically logged out of the Web Interface, and are returned to the **Login to your account** page.
7. From the login page that appears, type **`admin`** in the **Username** field and type the new password that you had created in the **Password** field, then click **LOGIN**.
   Upon successfully logging in, you are presented with the Web Interface (see *Web Interface Layout* on page 36).

6. CONFIGURING THE TIME

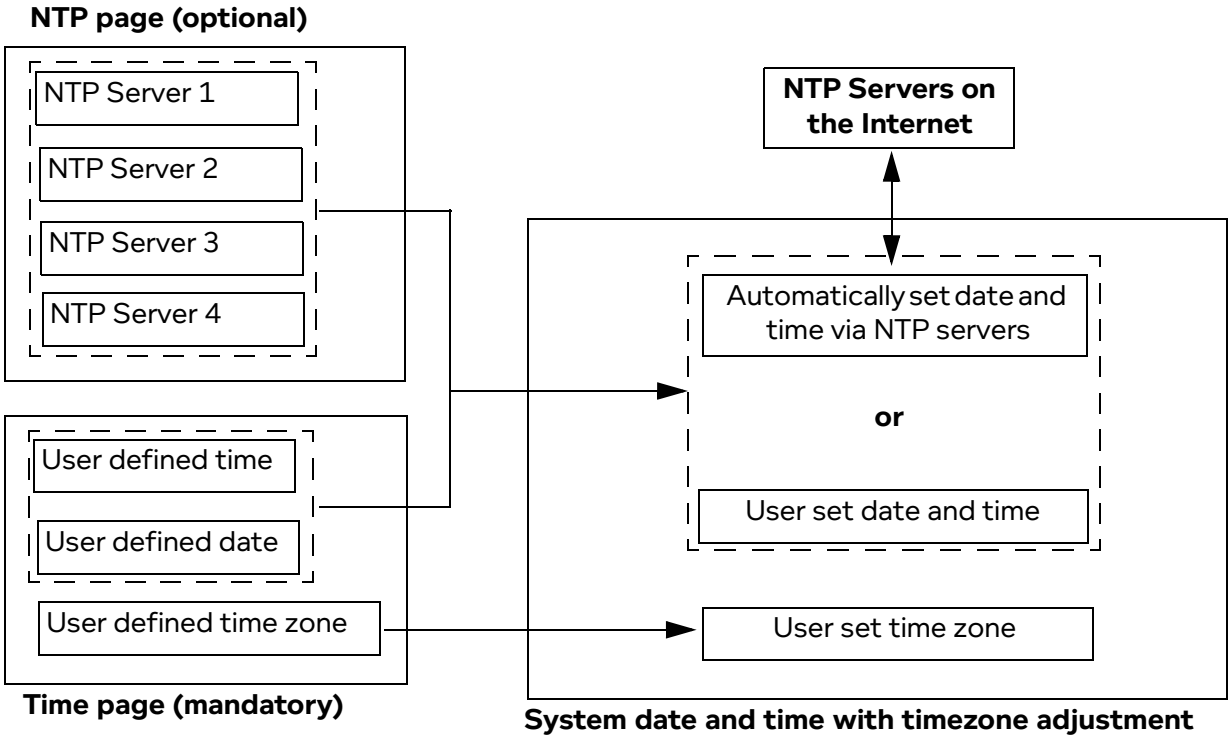
Use this section when you install the NE-ONE for the first time, or if you want to change the existing time settings of the NE-ONE.

The time configuration is separated into two separate areas on the Web Interface, as follows:

- a mandatory **Time** page where you must select the time zone, and manually specify a time and date (see *Time Configuration* on page 65)
- an optional **Network Time Protocol (NTP)** page, where you can optionally define NTP servers that can be used to override the manual date and time setting (see *Network Time Protocol (NTP) Configuration* on page 65)

Illustration 12 illustrates the way in which the time configuration is implemented on the NE-ONE.

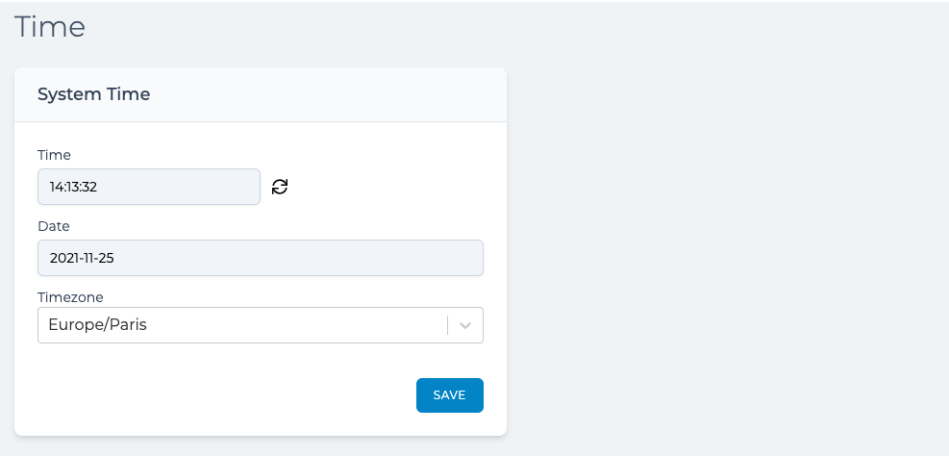
ILLUSTRATION 12 - TIME CONFIGURATION



6-1. Time Configuration

Use the following steps to set the time zone, and manually specify a time and date:

1. From the Web Interface, click **Management > ··· Platform Settings > Time**.



2. From the **Time** page that appears, do the following:
   a. Select the appropriate timezone from the **Timezone** drop-down field.
   b. In the **Time** field, type the current time.
      The time must be in 24 hour format, as follows : `HH:MM:SS`.
   c. In the **Date** field, type the current date.
      The date format must use the following international format : `YYYY-MM-DD`.

   Note:
   A refresh time icon exists next to the **Time** field. Clicking on the refresh time icon updates the **Time** field with the current time and **Date** field with the current date based on the local system time and date, and is not linked to the time and date optionally obtained via NTP servers (if configured).

   d. Click **SAVE**.
3. From the confirmation dialog that appears, click **OK**.

6-2. Network Time Protocol (NTP) Configuration

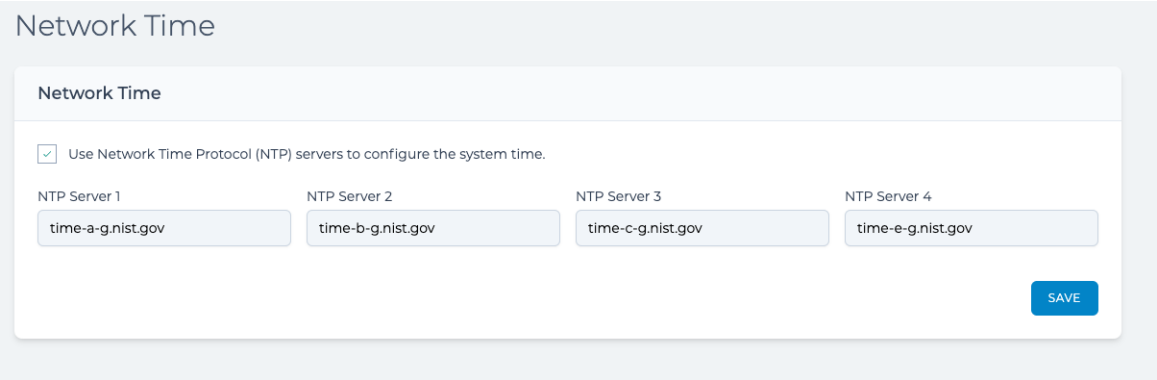
The NE-ONE lets you use the network time protocol (NTP) to set the time instead of manually configuring the time and date. For redundancy purposes, you can specify up to four different NTP servers.

Note:
If you enable NTP, the manual date and time settings defined in the **Time** page (see *Time Configuration* on page 65) are overridden, but you must still configure the timezone.

Note:
For redundancy purposes, Calnex recommends that you specify four NTP servers.

Use the following steps if you want to use NTP for setting the NE-ONE's date and time:

1. From the Web Interface, click **Management > Platform Settings > Network Time (NTP)**.



2. From the **Network Time** page that appears, do the following:
   a. Enable the **Use Network Time Protocol (NTP) servers to configure system time** check box.
      The **Time Server 1**, **Time Server 2**, **Time Server 3**, and **Time Server 4** fields are no longer grayed out.
   b. In the **Time Server 1** field, type the address of the primary NTP server.
   c. In the **Time Server 2** field, type the address of a second backup NTP server.
   d. In the **Time Server 3** field, type the address of a third backup NTP server.
   e. In the **Time Server 4** field, type the address of a fourth backup NTP server.
   f. Click **SAVE**.
3. From the confirmation dialog that appears, click **OK**.

7. CONFIGURING THE HOSTNAME

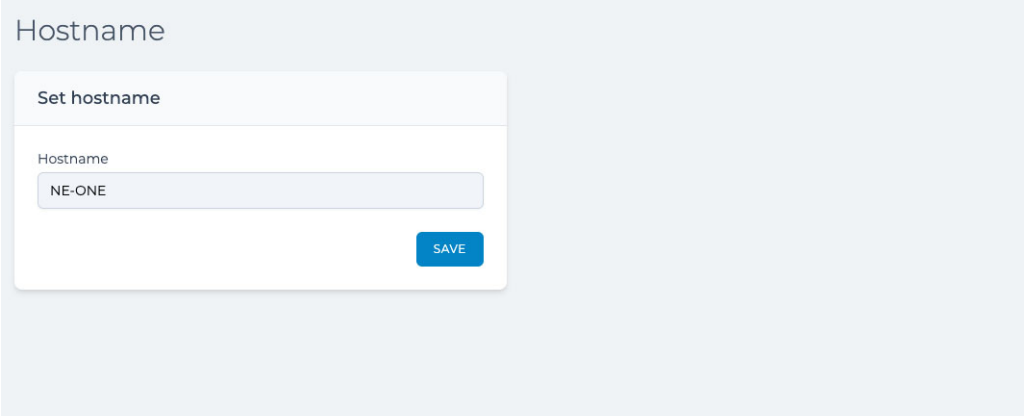
Use this section when you install the NE-ONE for the first time, or if you want to change the existing hostname of the NE-ONE. By default, the hostname assigned to the NE-ONE is NE-ONE.

Note:

If the organization's network contains more than one NE-ONE, Calnex recommends that a unique hostname is defined on each of the NE-ONEs.

Use the following steps to change the hostname of the NE-ONE:

1. From the Web Interface, click **Management > ••• Platform Settings > Hostname**.



2. From the **Hostname** page that appears, do the following:
   a. In the **Hostname** field, type the hostname that you want to assign to the NE-ONE.
   b. Click **SAVE**.
3. From the **Success** confirmation dialog that appears, click **OK**.

8. CONFIGURING THE WEB INTERFACE LABEL

Use this section when you install the NE-ONE for the first time, or if you want to change the existing label assigned to the NE-ONE's Web Interface.

The NE-ONE's Web Interface has a label (defined by the title tag) that appears in a web browser (see *Illustration 13*).

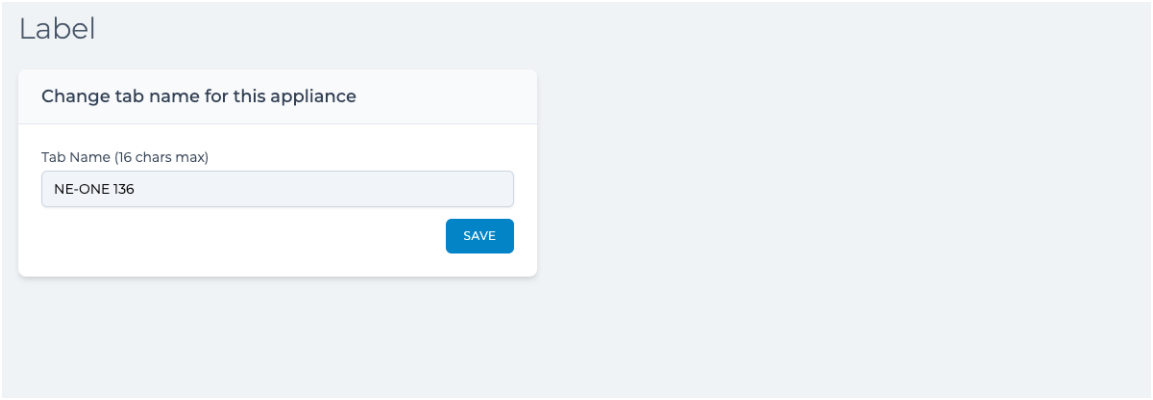
ILLUSTRATION 13 - MULTIPLE WEB INTERFACES OPEN IN A WEB BROWSER

The label is useful for situations where users have multiple NE-ONE Web Interfaces open in a web browser, and they want to quickly identify and switch between them via the web browser tabs. The label parameter lets you define a unique label for each NE-ONE so that a user can easily identify between them if they have more than one Web Interface open in their web browser.

By default, the label assigned to the NE-ONE's Web Interface is NE-ONE.

Use the following steps to change the label assigned to the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Label**.



2. From the **Label** page that appears, do the following:
   a. In the **Tab Name** field, type the label that you want to assign to the NE-ONE. The label can contain up to 16 alphanumeric characters.
   b. Click **SAVE**.
3. From the **Success** confirmation dialog that appears, click **OK**.

9. CONFIGURING HOUSEKEEPING

By default the NE-ONE is delivered with a housekeeping agent active so that it does not run out of disk space.

The housekeeping agent is initially configured as follows:

- housekeeping starts deleting files when the used storage reaches the high watermark level of 30%
- housekeeping stops deleting files when the used storage reaches the low watermark level of 20%
- the files older than 20 days are deleted in the following order (from top to bottom) until the low watermark level is reached:
  - Upgrade kits
  - System statistics
  - Network statistics
  - Operating system logs
  - User logs
  - Debug files

For example, if the used storage reaches 30% (i.e. high watermark level) and deleting some upgrade kits results in the used storage reaching 20% (i.e. the low watermark level), the housekeeping agent stops deleting files (i.e. System statistics, network statistics, etc. are not deleted).

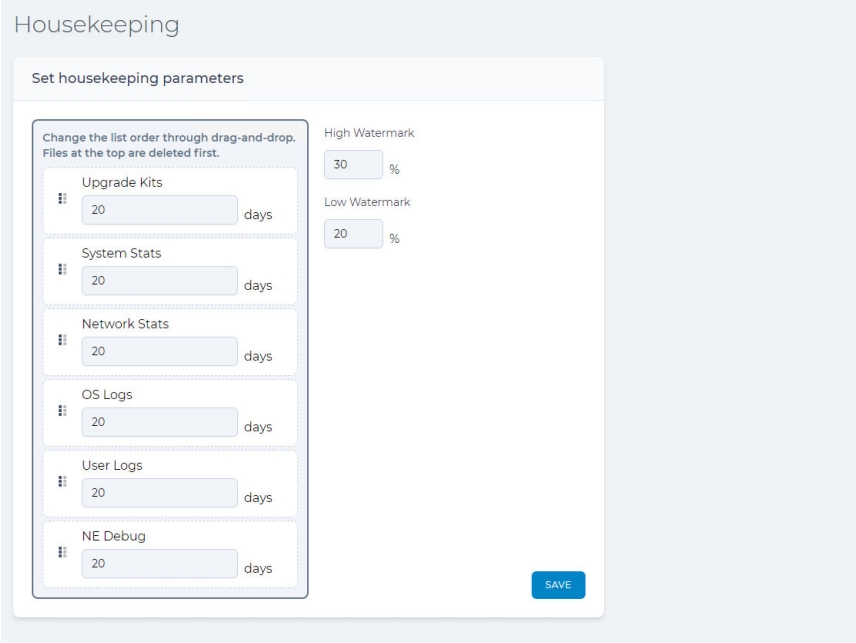
If desired, you can modify the housekeeping agent's high watermark level, low watermark level, the order in which the files are deleted, and the ages of the files that are deleted.

Note:

Setting the days value to -1 for a file type prevents that file type from being deleted. Therefore, if you set the days value to -1 for all file types, the housekeeping agent is effectively disabled.

If you want to modify the default housekeeping configuration, do the following:

1. From the Web Interface, click **Management > Platform Settings > Housekeeping**.
   A **Housekeeping** page appears.



2. From the **Housekeeping** page that appears, do the following:

a. Optionally change the **High Watermark %** value (i.e. the percentage of the used storage at which the system will start deleting files). The default value is 30%.
b. Optionally change the **Low Watermark %** value (i.e. the percentage of the used storage at which the system will stop deleting files). The default value is 20%.
c. In the days field for each of the file types, optionally modify the age at which the housekeeping agent will start deleting those file types. The default age threshold deletion date for each file type is 20 days.
d. Optionally re-order the order in which the file types are deleted. To do this, do the following:
   - Place the mouse over the icon on the left hand side of the file type. The mouse icon changes to a cross.
   - Click the mouse button to grab and select the file type.
   - Drag the file type above or below another file type to the required position.
   - Un-click the mouse button let go of the selected file type.
   - Repeat these sub-steps above until the desired file type deletion order is achieved.
e. Click **SAVE**.

3. From the **Success** confirmation dialog that appears, click **OK**.

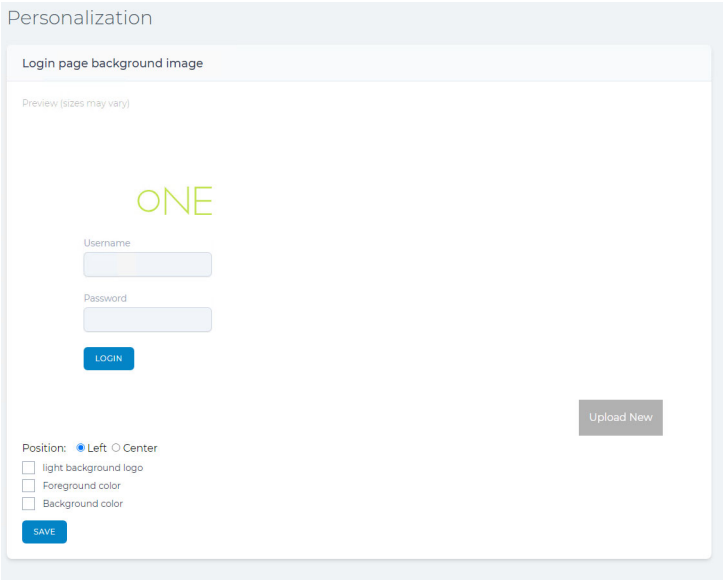
10. PERSONALIZING THE LOGIN PAGE

The NE-ONE login page can be personalized so that it matches your organizations branding. The personalization page lets you choose:

- the position of the login fields (left or center)
- whether the NE-ONE logo is dark (white NE and green ONE) or light (green NE and black ONE)
- the foreground color (i.e. the color of the login area)
  - if the login position is set to left, the chosen foreground color appears as a strip on the left hand side of the login page
  - if the login position is set to center, the chosen foreground color appears as a rectangle around the login fields
  - if no foreground color is chosen (i.e. transparent), the defined background color (bottom layer) or background image (middle layer) will be visible
- the background color (i.e. the color of the background (middle layer))
  - if no background color is chosen (i.e. transparent), the defined background image (middle layer) will be visible
  - if no background color is chosen and a background image is chosen, defined background image (middle layer) will be visible because it is above the background (bottom layer)
- an image
  - if the login position is set to left, the chosen image appears and is scaled within the area to the right hand side of the left hand side strip
  - if the login position is set to center, the chosen background appears and is scaled across the entire login page
  - if a background image is chosen, it replaces the chosen background color (i.e. the background image is the middle layer above the background layer, and below the layer of the foreground layer)

To personalize the login page, do the following:

1. From the Web Interface, click **Management > ··· Platform Settings > Personalization**.
   A **Personalization** page appears.



2. Select the **Position** radio button (i.e. **Left** or **Center**) to set the position of the login fields. By default, **Left** is selected.

3. If required, ticked the light background check box.
   - If ticked, the NE-ONE logo is light (green NE and black ONE).
   - If ticked, the NE-ONE logo is dark (white NE and green ONE).
4. Optionally change foreground color (i.e. the color of the login area). To do this, tick the **Foreground color** and from the color palette that appears, select the desired color.
5. Optionally change background color. To do this, tick the **Background color** and from the color palette that appears, select the desired color.
6. Optionally upload a custom image. To do this, do the following:
   a. Click the **Upload New** button, and from the **Open** dialog box that appears navigate to and select an appropriate image, then click **Open**.

      The selected image gets uploaded to the NE-ONE and appears in the image gallery area of the **Personalization** page. It can now be chosen from the gallery by clicking on it.

      If necessary, repeat this step to upload additional images to add them to the image gallery area.

   b. Click on the uploaded image within the image gallery area to select the image. The selected image is indicated by a tick and appears in the preview area on the **Personalization** page.

      The example below shows an uploaded image selected with a gray foreground and a left login position.

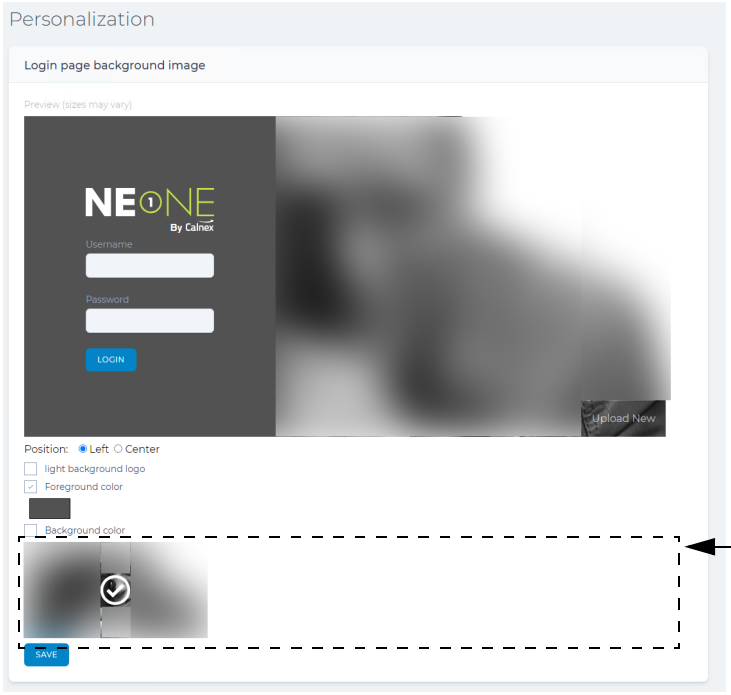


Image Gallery Area
Uploaded images can be selected by clicking on them in the image gallery area.

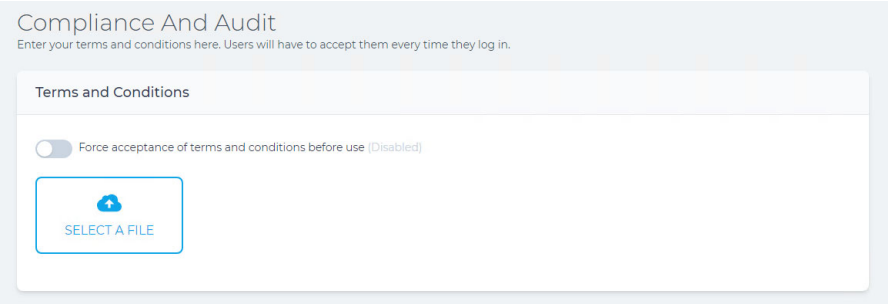
7. Click **SAVE**.
8. From the **Successfully updated login** page dialog, click **OK**.

11. APPLYING A COMPLIANCE AND AUDIT ACCEPTANCE AGREEMENT

If your organization has a compliance and audit policy, you can upload a User Acceptance Document (in PDF format) to the NE-ONE and configure the NE-ONE so that it forces all users to agree to that policy each time they log in. To do this, use the following steps:

1. Obtain the User Acceptance Document (in PDF format) from the appropriate department in your organization. Copy it to an appropriate location on your PC (in our example, the Downloads folder).
2. From the Web Interface, click **Management > Platform Settings > Compliance and Audit**.

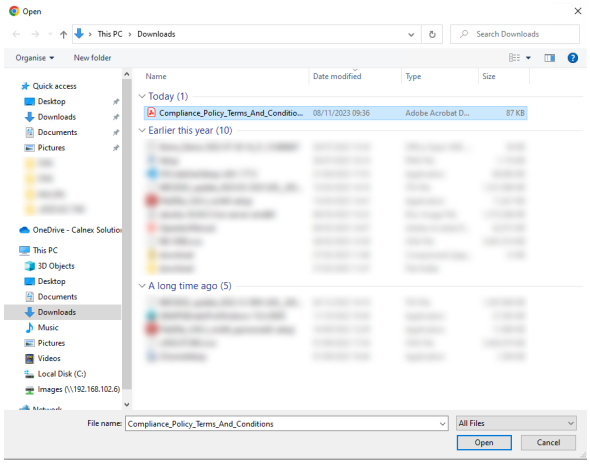
   A **Compliance And Audit** page appears.



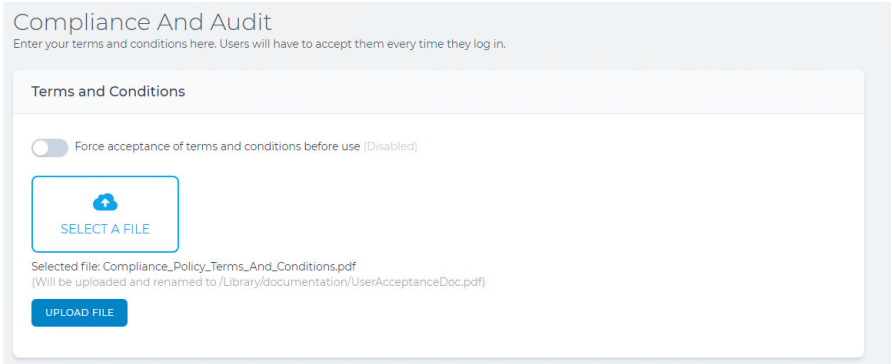
Note:

If a User Acceptance Document has previously been uploaded, an additional **DOWNLOAD CURRENT** button exists.

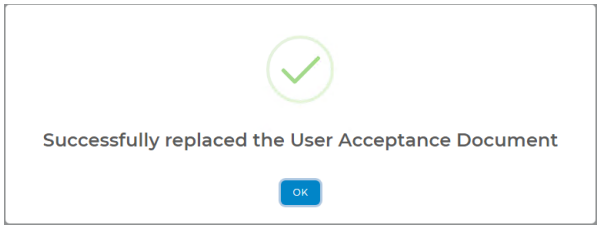
3. Click the **Select a File** button. From the **Open** dialog box that appears navigate to and select the User Acceptance Document PDF file that you copied to your PC and click **Open**.



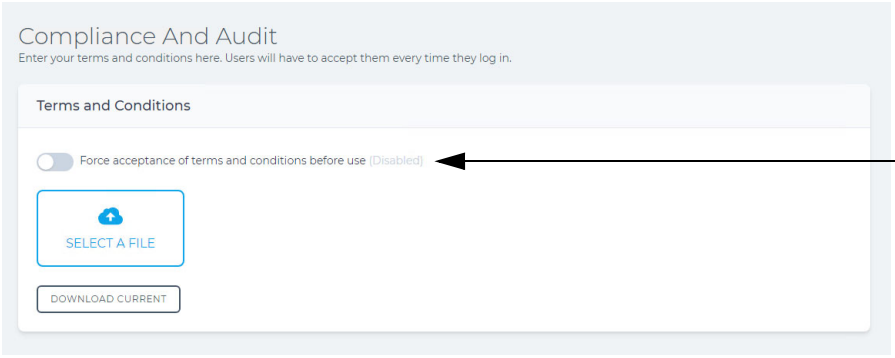
The **Compliance And Audit** page updates with the selected file.



4. Click the **UPLOAD FILE** button.
   A **Successfully replaced the User Acceptance Document** dialog box appears.

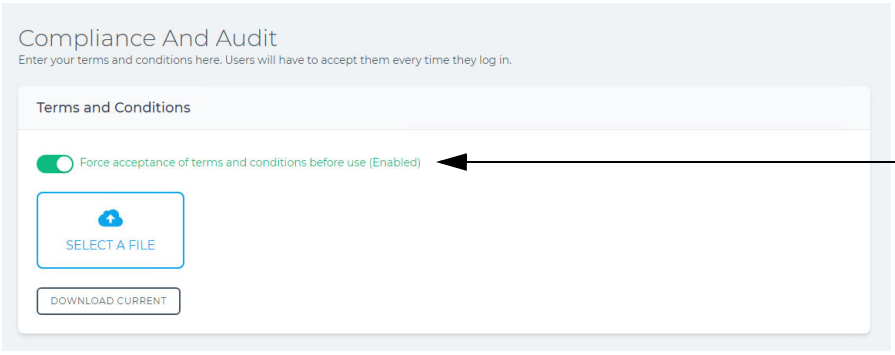


5. From the **Successfully replaced the User Acceptance Document** dialog box that appears, click **OK**.
   The **Compliance And Audit** page updates containing a **DOWNLOAD CURRENT** button, indicating that a User Acceptance Document exists on the NE-ONE.



With the toggle button disabled, the users are not prompted to agree with the terms and conditions of the uploaded User Acceptance Document each time they log in.

6. Enable the **Force acceptance of terms and conditions** toggle button.



With the toggle button enabled, the users are prompted to agree with the terms and conditions of the uploaded User Acceptance Document each time they log in.

Note:

Clicking the **DOWNLOAD CURRENT** button lets you download the currently uploaded User Acceptance Document.

12. CONFIGURING SNMP

If the organization uses Simple Network Management Protocol (SNMP) as a method of network management, then use this section when you install the NE-ONE for the first time, or at a later date if the organization's SNMP configuration changes.

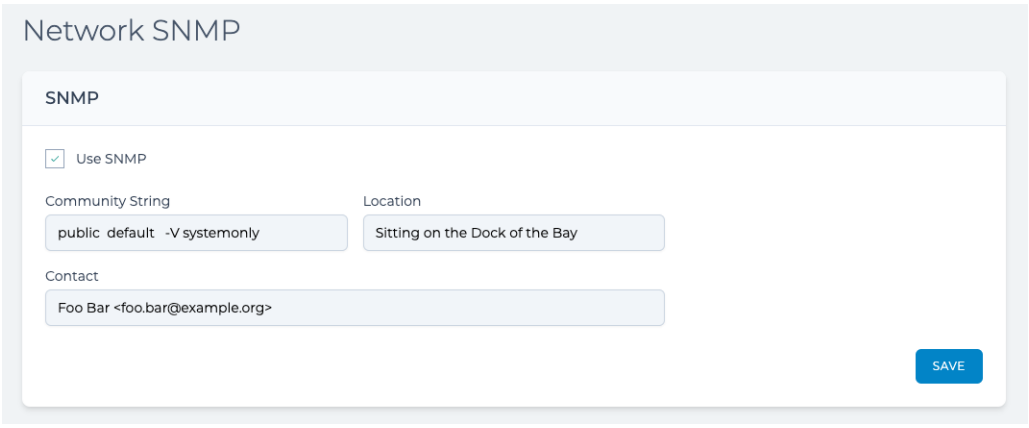
By default, the NE-ONE is not configured to use SNMP (i.e. the SNMP service is not enabled and not configured). If the organization uses SNMP, their network administrator will provide you with the following the Community String, location and contact.

Note:

At the current release, the NE-ONE does not support SNMP V3 username and password implementation.

Use the following steps to change the SNMP configuration of the NE-ONE:

1. From the Web Interface, click **Management > ••• Platform Settings > SNMP**.



2. From the **Network SNMP** page that appears, do the following:
   a. If you want the SNMP service to be active, check the **Use SNMP** check box. If you do not want the SNMP service to be active, uncheck the **Use SNMP** check box.
   b. If the SNMP service is enabled, define the following values:

      In the **Device Location** field, type an appropriate location corresponding to where the NE-ONE is located in the organization. The **Device Location** field accepts alphanumeric characters and spaces.

      In the **Community String** field, type an appropriate community string (e.g. `public default -V systemonly`). The **Device Location** field accepts alphanumeric characters and spaces.

      In the **Contact** field type the name and email address of the contact person responsible for managing the NE-ONE. The email address must be surrounded by angled brackets. For example, it the contact person is called Foo Bar with the e-mail address foo.bar@example.org, you would type `Foo Bar <foo.bar@example.org>`.
   c. Click **SAVE**.
3. From the **Success** confirmation dialog that appears, click **OK**.

13. CONFIGURING THE AUTHENTICATION METHOD

Use this section when you install the NE-ONE for the first time, or at a later date if the organization's authentication method has changed and you need to change the existing authentication method used by the NE-ONE.

By default, the NE-ONE is configured to use built-in authentication, with locally (built-in) defined users. In this case, the authentication and users are managed locally on the NE-ONE.

In addition to local (built-in) authentication, the NE-ONE also supports LDAP and RADIUS authentication methods.

Note:

LDAP and RADIUS authentication methods are only available with the Advanced Authentication feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

If the NE-ONE uses local (built-in) authentication or LDAP authentication, you must also add local users (see *Adding Local and Semi-Local Users* on page 204).

Table 9 summarizes the differences between how the Built-in, LDAP and RADIUS authentication methods are implemented on the NE-ONE.

Note:

In order to access the NE-ONE for the first time, a built-in admin user exists, which cannot be removed even if LDAP or RADIUS authentication is configured. This is normal so that the built-in admin user can be used for initial access, and if necessary future access in cases where the organization's LDAP or RADIUS server may be down.

TABLE 9 - DIFFERENCES BETWEEN BUILT-IN, LDAP, AND AUTHENTICATION METHODS

	Built-in	LDAP	RADIUS
User type	Local	Semi-local	Non-local
Creation of users	On the NE-ONE's **Users** Web Interface page.	Users (usernames and passwords) exist on the LDAP server. These users must also be created on the NE-ONE's **Users** Web Interface page, but no password is specified as it is managed by the LDAP server.	Users (usernames and passwords) exist on the RADIUS server.
Configuration of user permissions (i.e. assigned ports, number of networks, number of objects, number of links)	On the NE-ONE's **Edit User Details** Web Interface page.		On the RADIUS server: • by importing the `dictionary.itrinegy` file into the RADIUS sever • by adding appropriate `iTrinegy-NEONE` attributes to the user
Web Interface user authentication method	Locally on the NE-ONE, via the local database.	Remotely on the LDAP server: • login request from NE-ONE sent to LDAP server • if username does not exist on LDAP server the login request is rejected • if username exists on LDAP server, but the specified password is wrong the login request is rejected • if username exists on LDAP server, and the specified password is correct the login request is accepted	Remotely on the RADIUS server: • login request from NE-ONE sent to RADIUS server • if username does not exist on RADIUS server the login request is rejected • if username exists on RADIUS server, but the specified password is wrong the login request is rejected • if username exists on RADIUS server, and the specified password is correct the login request is accepted • if the successfully logged in user has connected to the NE-ONE for the first time, a `/Private` directory is created for that user
Presentation of the user permissions to the logged in user on the Web Interface	Determined locally on the NE-ONE, via the local database, and what an admin type user had configured for the user within the **Edit User Details** Web Interface page.		Determined remotely on the RADIUS server according to the different `iTrinegy-NEONE` attributes that were assigned to the user.

13-1. Configuring Built-in Authentication

By default, the NE-ONE is configured to use built-in authentication, with locally (built-in) defined users. You would only use the steps below in the rare situation where you had previously configured LDAP or RAIDUS authentication, but want to revert back to using built-in authentication.

1. From the Web Interface, click **Management > Platform Settings > Authentication**.
2. From the **Authentication** page that appears, select **Built-in** in the **Authentication Method** drop-down field.
3. Click **SAVE**.
4. From the **Success** confirmation dialog that appears, click **OK**.

Note:
If you were previously using the LDAP authentication method, you will need to edit each of the existing users on the NE-ONE to configure their passwords as previously the NE-ONE was getting their passwords from the LDAP server. For more information, see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205.

Note:
If you were previously using the RADIUS authentication method, the `/Private` directories for each of those users will already exist on the NE-ONE. You will need to create the users (according to *Adding Local and Semi-Local Users* on page 204) and define permissions (according to *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205). In this rare case, if you require additional help to know how to find the usernames that have been created on the NE-ONE, contact your Calnex support representative, or Calnex support.

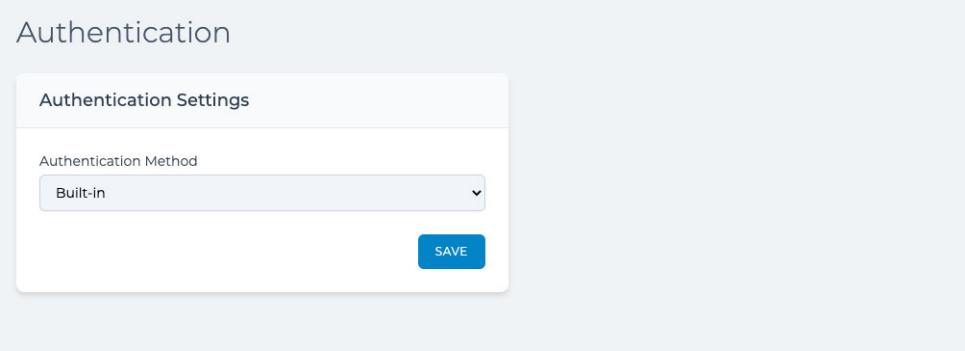
13-2. Configuring LDAP Authentication

If the organization uses either the LDAP authentication method, their network administrator will provide you with the following:

- Primary LDAP Server FQDN or IP address
- Secondary Primary LDAP Server FQDN or IP address

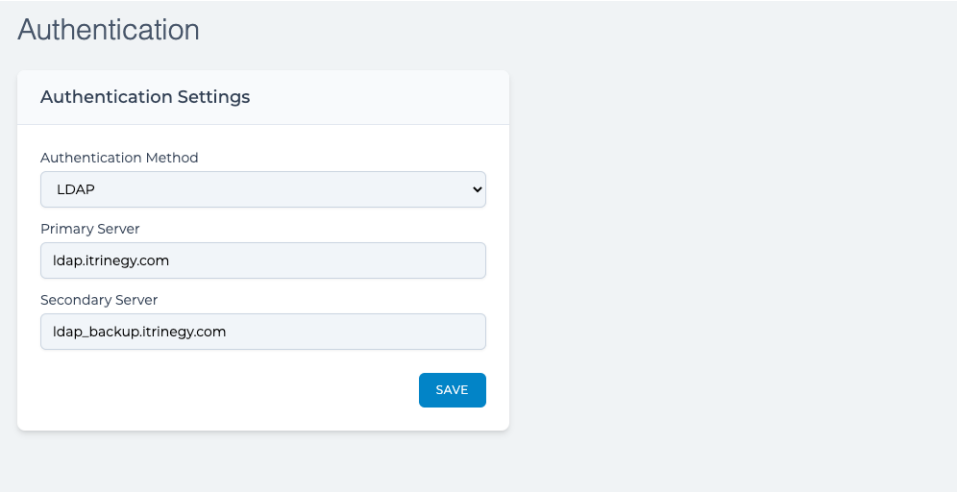
Use the following steps to configure the NE-ONE to use the LDAP authentication method:

1. From the Web Interface, click **Management > Platform Settings > Authentication**.



2. From the **Authentication** page that appears, select **LDAP** in the **Authentication Method** drop-down field.
   The **Authentication Settings** tile of the **Authentication** page updates with fields corresponding to

configuring the LDAP servers.



3. In the **Primary Server** field, type the FQDN or IP address of the organization's Primary LDAP Server.
4. In the **Secondary Server** field, type the FQDN or IP address of the organization's Secondary LDAP Server.
5. Click **SAVE**.
6. From the **Success** confirmation dialog that appears, click **OK**.

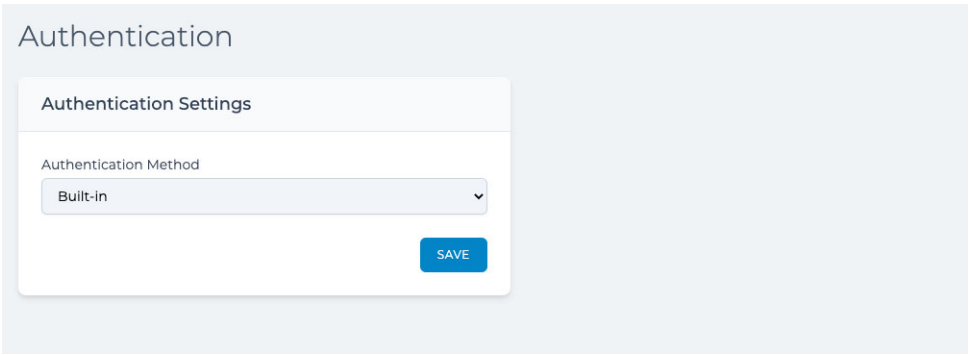
13-3. Configuring RADIUS Authentication

If the organization uses the RADIUS authentication method, obtain the following information from the network administrator:

- Primary RADIUS server FQDN or IP address.
- Primary RADIUS server pre-shared key (PSK).
- Backup RADIUS server FQDN or IP address.
- Backup RADIUS server PSK.
- The shared secret used by the Primary and Backup RADIUS servers.
- Determine whether or not the RADIUS servers are using RADIUS over TLS with the PSKs (i.e. the RADIUS servers are using secure communication via the Transport Layer Security (TLS) protocol with the PSKs).

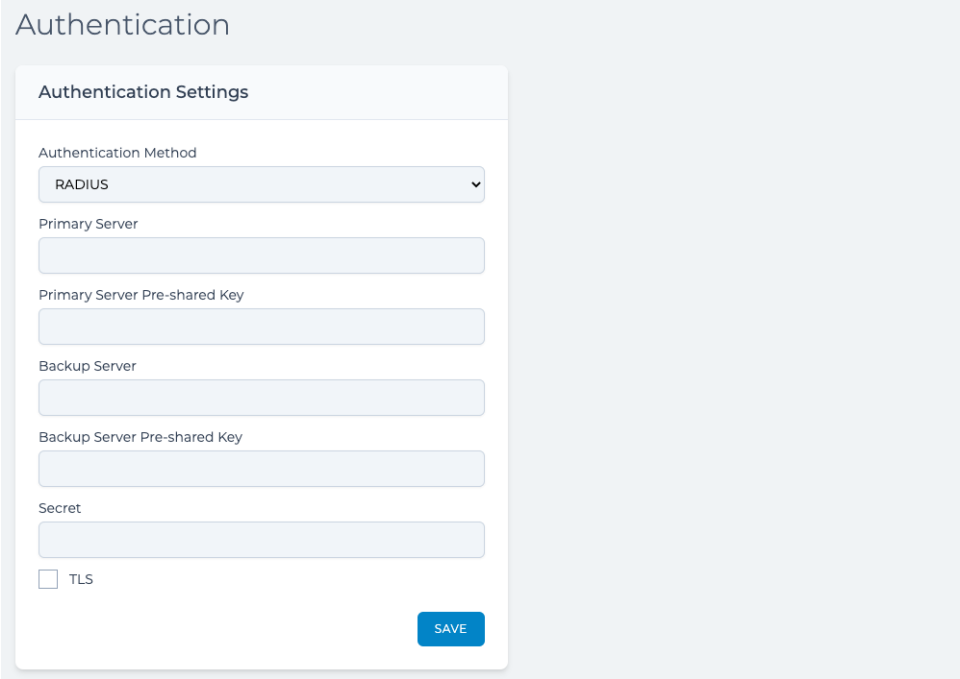
Use the following steps to configure the NE-ONE to use the LDAP authentication method:

1. From the Web Interface, click **Management > Platform Settings > Authentication**.



2. From the **Authentication** page that appears, select **RADIUS** in the **Authentication Method** drop-down field.

The **Authentication Settings** tile of the **Authentication** page updates with fields corresponding to configuring the RADIUS servers.



3. In the **Primary Server** field, type the FQDN or IP address of the organization's Primary Radius Server.
4. In the **Primary Server Pre-shared Key** field, type the PSK of the organization's Primary Server.
5. In the **Backup Server** field, type the FQDN or IP address of the organization's Backup Radius Server.
6. In the **Backup Server Pre-shared Key** field, type the PSK of the organization's Backup Server.
7. In the **Secret** field, type the shared secret that is used to send its encrypted access-request to the RADIUS servers.
8. If the RADIUS servers are using secure communication via the TLS protocol (using the PSK), check the **TLS** check box. If the RADIUS servers are not using secure communication via the TLS protocol (using PSK), un-check the **TLS** check box.
9. Click **SAVE**.
10. From the **Success** confirmation dialog that appears, click **OK**.

14. INSTALLING AND UPDATING ROOT SSL CERTIFICATES

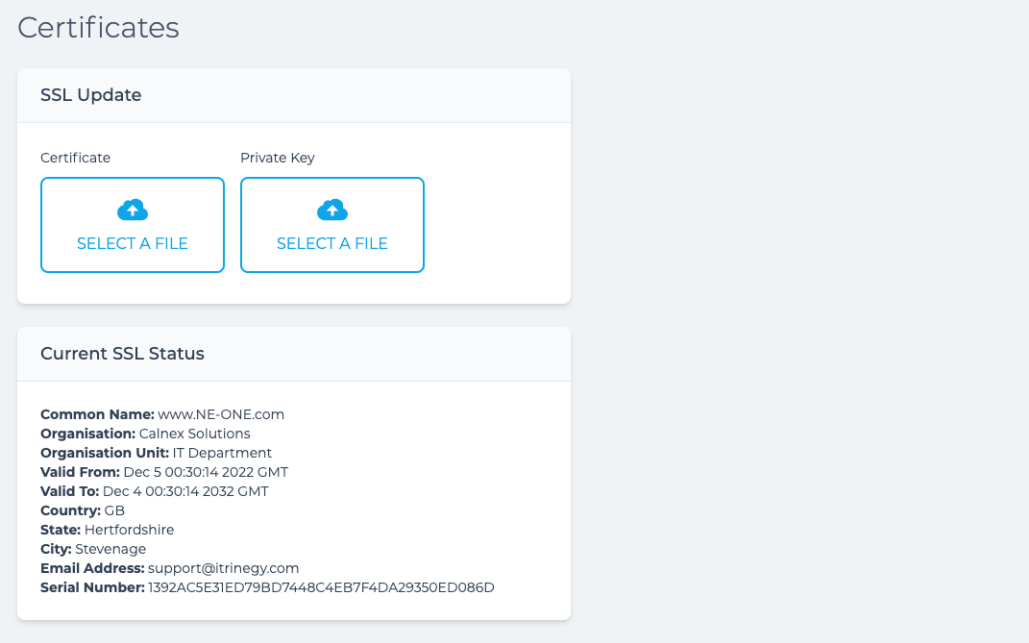
If the organization uses a Root SSL Certificate, then use this section when you install the NE-ONE for the first time, or at a later date when the organization's current Root SSL Certificate is due to expire.

Note:

If the organization does not use a Root SSL Certificate, the NE-ONE will use the default supplied self-signed Calnex SSL Certificate. In this case, when users connect to the NE-ONE Web Interface for the first time, they will need to perform a few steps to accept the self-signed Calnex SSL Certificate. For more information, see *First time Web Interface access (accepting the default self-signed SSL certificate)* on page 27.

Use the following steps to install a Root SSL Certificate and Private Key on the NE-ONE:

1. Obtain the latest Root SSL Certificate and Private Key from the organization's network administrator, and copy them to your preferred location on your computer's filing system.
2. From the Web Interface, click **Management > ··· Platform Settings > Certificate**.



Note:

The **Current SSL Status** section of the **Certificates** page contains the SSL certificate expiry date (indicated by **Valid To:**). This information is useful to ensure that you have the time to plan and acquire a new Root SSL certificate from a trusted CA before the current Root SSL certificate runs out.

3. From the **Certificates** page that appears, do the following:
   a. Click the **Certificate SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the SSL Root Certificate to upload.
   b. Click the **Private Key SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the Private Key to upload.
4. From the **Success** confirmation dialog that appears, click **OK**.

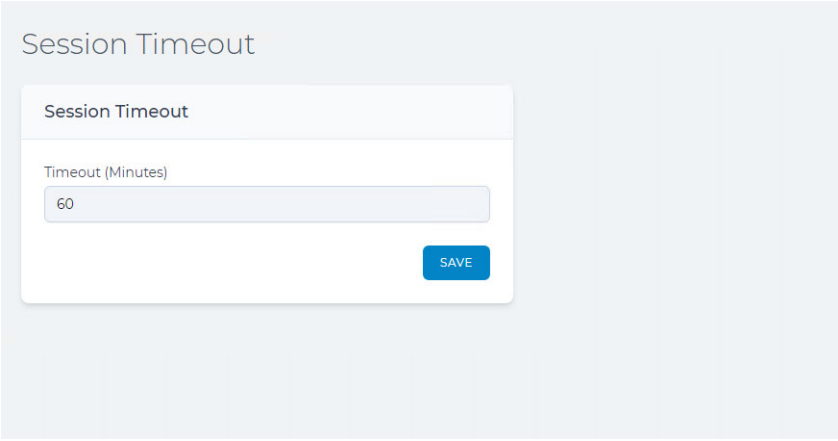
15. SESSION TIMEOUT CONFIGURATION

Use this section when you install the NE-ONE for the first time, or if you want to change the existing session timeout configuration of the NE-ONE.

The session timeout configuration defines how long an inactive Web Interface session remains open before automatically logging out. By default the session timeout configuration is set to 60 minutes.

Use the following steps if you want to change the existing session timeout configuration of the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Session Timeout**.



2. From the **Session Timeout** page that appears, do the following:
   a. In the **Timeout (Minutes)** field, type the value in minutes (or use the up/down arrows) to define the session timeout.
   b. Click **SAVE**.
3. From the **Success** confirmation dialog that appears, click **OK**.

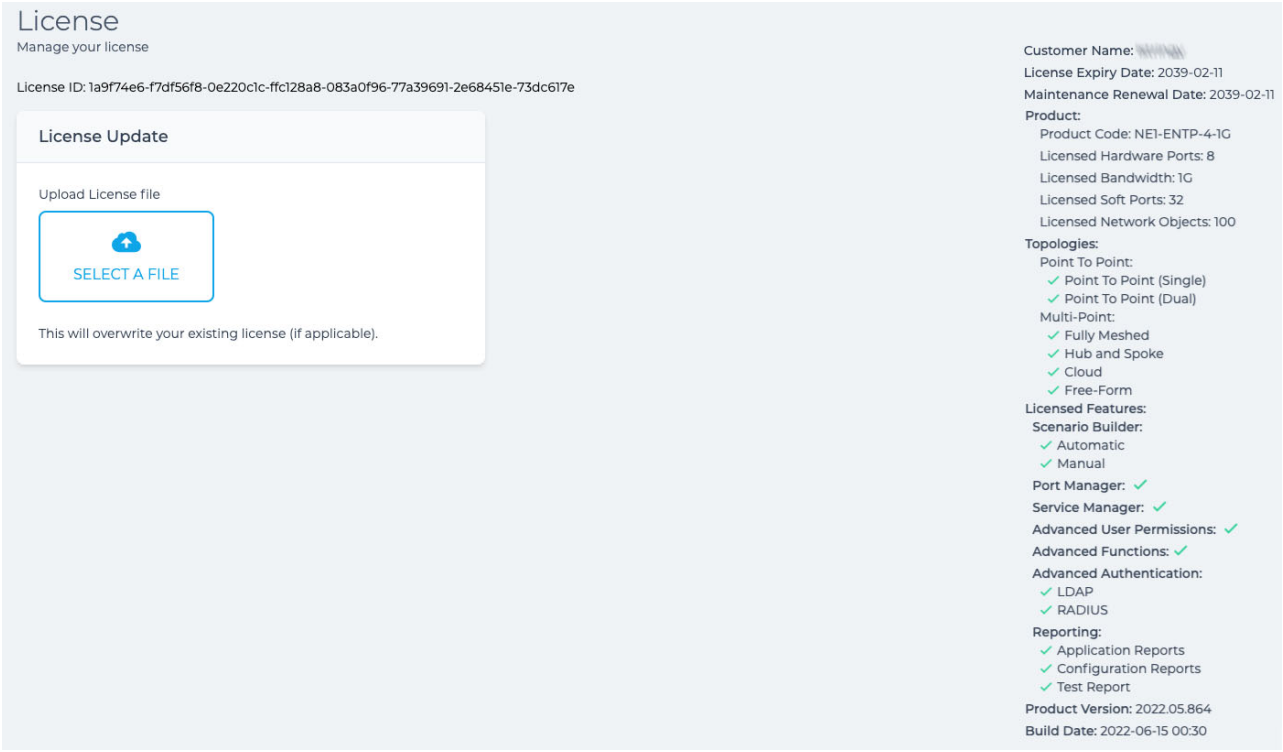
16. VIEWING AND APPLYING LICENSE FILES

Use this section when you install the NE-ONE for the first time, or if you want to view and/or update the existing license file that is installed on the NE-ONE.

By default, the NE-ONE is supplied with a temporary license file with limited functionality. In order to make the NE-ONE fully functional, you must obtain a license file from Calnex and apply it on the NE-ONE.

Use the following steps to view and install a license file on the NE-ONE:

1. Obtain the license file from the Calnex customer support site:
   a. Go to *https://itrinegysupport.force.com*, and login with your Calnex provided customer username and password.
   b. In the Calnex customer support site, navigate to the licenses area, and download the license associated with your NE-ONE to your computer's local filing system.
2. From the Web Interface, click **Management > ••• Platform Settings > License**.



3. From the **License** page that appears, do the following:
   a. Click the **SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the license to upload.
4. From the **Success** confirmation dialog that appears, click **OK**.

17. CUSTOM LOCATIONS

By default, the NE-ONE is delivered with the majority of locations within the world. The locations are used when configuring a node's location from within the **Edit node** panel of either the Point-to-Point Designer (see *Illustration 74* on page 249) or Mutli-Point Designer (see *Illustration 88* on page 319).

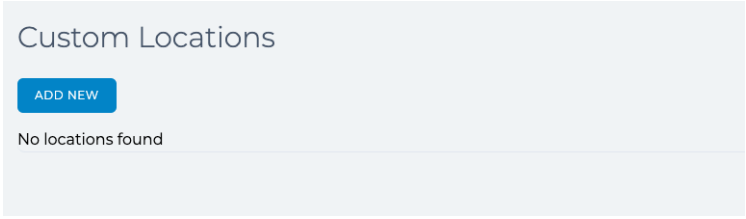
If compared to those included with the NE-ONE, your non-admin users require additional locations for the nodes that they create within their networks, follow the steps described in *section 17-1*, *Creating Custom Locations*.

17-1. Creating Custom Locations

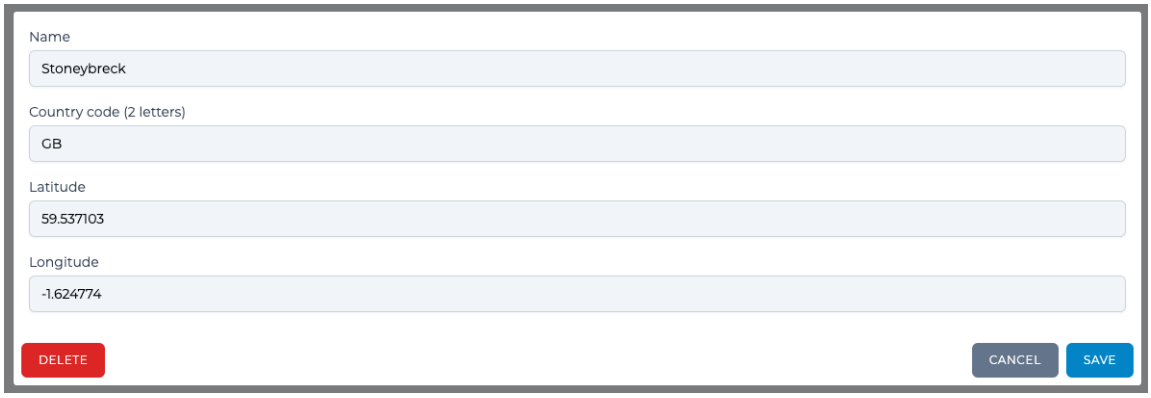
Use the steps below to create a custom location.

Note:
The example below shows adding the small island of Stonybreck in the sea, just north of Scotland.

1. From the Web Interface, click **Management > ••• Platform Settings > Custom Locations**.
   A **Custom Locations** page appears with a list of custom locations that already exist (if any) on the NE-ONE.

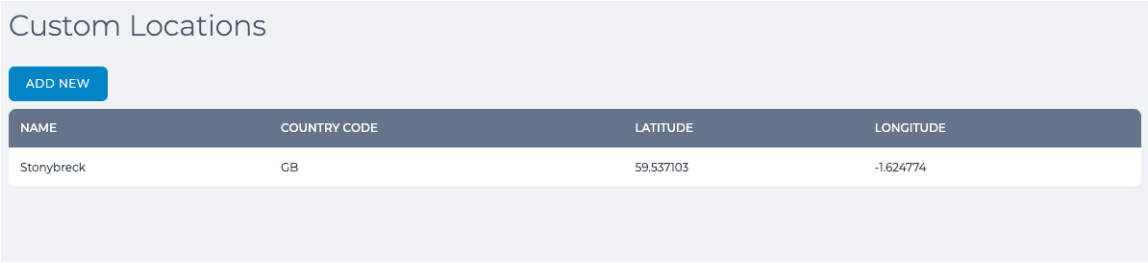


2. From the **Custom Locations** page that appears, click the **ADD NEW** button.
   A dialog box appears letting you define the parameters of the custom location.



3. From the dialog box that appears, do the following:
   a. In the **Name** field, type the name of the location.
   b. In the **Country code (2 letters)** field, type the two letter ISO3166-1 alpha-2 Country Code corresponding to the country in which the location exists.
   c. In the **Latitude** field, type the latitude coordinate of the location. The latitude coordinate must be of the format used by the geographic coordinate system.
   d. In the **Longitude** field, type the longitude coordinate of the location. The latitude coordinate must be of the format used by the geographic coordinate system.
   e. Click **SAVE**.
4. From the **Successfully added location** confirmation dialog that appears, click **OK**.
   The **Successfully added location** confirmation dialog box closes, and the **Custom Locations** page

updates with the newly added custom location.



Once a custom location has been created, if necessary, it can be edited or deleted. For more on editing and deleting a custom location, see *section 17-2*, *Editing Custom Locations* and *section 17-3*, *Deleting Custom Locations*, respectively.

Notice:

Once you have created all of your custom locations, instead of having to re-create them all again on a different NE-ONE, they can be quickly imported to a different NE-ONE. For more information, see *section 17-4*, *Importing Already Created Custom Locations to Other NE-ONEs*.

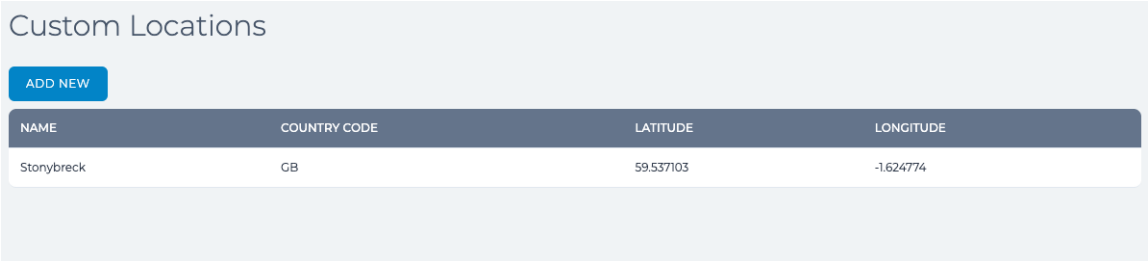
17-2. Editing Custom Locations

Once one or more custom locations have been created, they are listed in the **Custom Locations** page, from where their parameters (i.e. country code and latitude/longitude coordinates) can be edited if necessary. If you want to edit an existing custom location, use the steps below.

Note:

You cannot edit the name of an existing custom location. If you created a location with the wrong name, delete it according to *section 17-3*, *Deleting Custom Locations*, then re-create it with the correct name according to *section 17-1*, *Creating Custom Locations*.

1. From the Web Interface, click **Management > Platform Settings > Custom Locations**.
   A **Custom Locations** page appears with a list of custom locations that already exist on the NE-ONE.



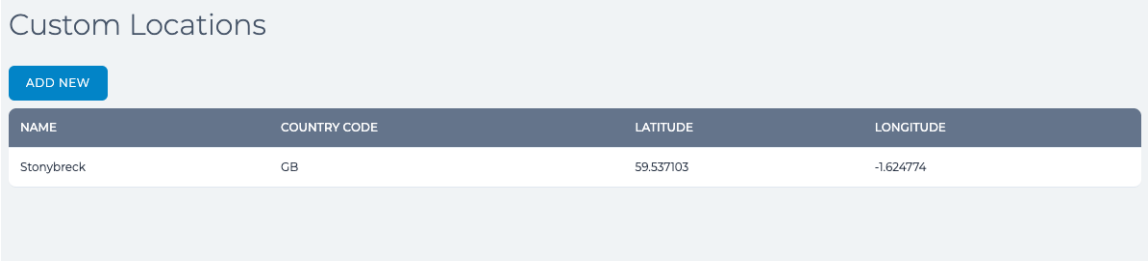
2. From the **Custom Locations** page that appears, click the custom location that you want to edit.
   A dialog box appears letting you edit the existing parameters of the custom location.

3. From the dialog box that appears, do the following:
   a. If necessary, in the **Country code (2 letters)** field, modify the two letter ISO3166-1 alpha-2 Country Code corresponding to the country in which the location exists.
   b. If necessary, in the **Latitude** field, modify the latitude coordinate of the location. The latitude coordinate must be of the format used by the geographic coordinate system.
   c. If necessary, in the **Longitude** field, modify the longitude coordinate of the location. The latitude coordinate must be of the format used by the geographic coordinate system.
   d. Click **SAVE**.
4. From the **Successfully edited location** confirmation dialog that appears, click **OK**.
   The **Successfully added location** confirmation dialog box closes, and you are returned to the **Custom Locations** page.

17-3. Deleting Custom Locations

Once one or more custom locations have been created, they are listed in the **Custom Locations** page, from where they can be edited if necessary. Typically, you would not want to delete a custom location, unless you had incorrectly named it during its initial creation. If you want to delete an existing custom location, use the steps below.

1. From the Web Interface, click **Management > Platform Settings > Custom Locations**.
   A **Custom Locations** page appears with a list of custom locations that already exist on the NE-ONE.



2. From the **Custom Locations** page that appears, click the custom location that you want to delete.
   A dialog box appears letting you delete the custom location.

3. From the dialog box that appears, click **DELETE**.
   The custom location is immediately deleted, and **Deleted location successfully** confirmation dialog appears.
4. From the **Deleted location successfully** confirmation dialog that appears, click **OK**.
   The **Deleted location successfully** confirmation dialog box closes, and you are returned to the **Custom Locations** page.

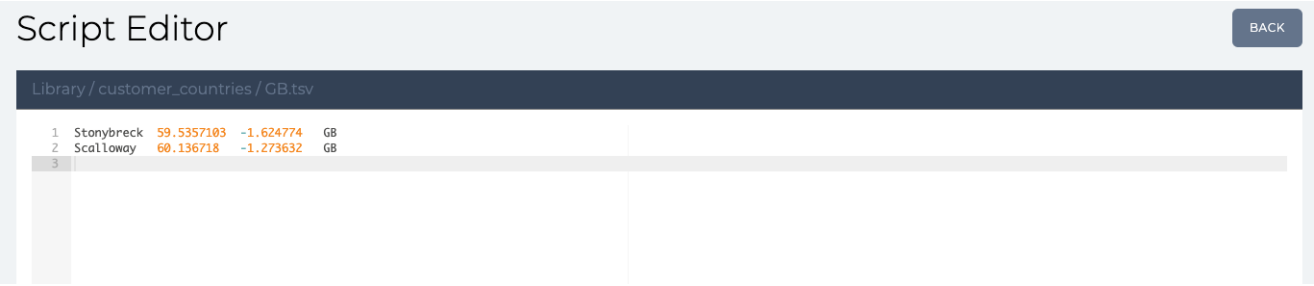
17-4. Importing Already Created Custom Locations to Other NE-ONEs

When you create a custom location, a `<country code>.tsv` file gets created in the `/Library/customer_countries` directory, where `<country code>` is the two letter ISO3166-1 alpha-2 Country Code. Each time you add a custom location belonging to the same `<country code>`, its parameters get appended to the `<country code>.tsv` file on a new line. Each custom location in the `<country code>.tsv` file is a separate line, in tab delimited form of the following format:

`<location name> <latitude> <longitude> <country code>`

Illustration 14 shows an example of two custom locations called Stonybreck and Scalloway belonging to the same GB country code that get created in a `GB.tsv` file. In this example, when you create the first custom location (e.g. Stonybrock) belonging to the GB country code, a `GB.tsv` file gets created within the directory `/Library/customer_countries`. If you add additional custom locations within the same GB country code (e.g. Scalloway), they get appended to the `GB.tsv` file.

ILLUSTRATION 14 - EXAMPLE TSV FILE FOR TWO CUSTOM LOCATIONS WITHIN COUNTRY CODE GB



Note:

You can view *.tsv files in the script editor for viewing, but the possibility to modify the file and save it is intentionally dis-activated.

Illustration 15 shows how the same two locations (e.g. Stonybreck and Scalloway) belonging to the same GB country code are represented in the **Custom Locations** page.

ILLUSTRATION 15 - EXAMPLE CUSTOM LOCATIONS PAGE FOR TWO CUSTOM LOCATIONS WITHIN COUNTRY CODE GB

If you have created many custom locations belonging to different country codes and have multiple NE-ONEs in your environment, rather than taking time re-create them on the other NE-ONEs you can download each of the finalized `<country code>.tsv` files from the "master" NE-ONE where you created them, and upload them to the "other" NE-ONEs in your environment. To do this, use the following steps below:

1. Login to the "master" NE-ONE as an admin user, and create all of your custom locations for each county code according to *section 17-1, Creating Custom Locations*.
2. Once you are happy with the finalized set of locations for each country code on the "master" NE-ONE, do the following:

a. From the Web Interface, click **Management > ••• Platform Settings > File Browser**.
   The **File Browser** page opens with the path of your `/Private` directory.
b. Navigate to the `/Library/customer_countries` directory.
c. For each of the `<country code>.tsv` files that exist, right mouse click on them, and select **Download selected File**.
   Each of the `<country code>.tsv` files are downloaded to your computer's local filing system, and are now ready for uploading to all the "other" NE-ONEs in your environment.

3. For each of the "other" NE-ONEs in your environment that you want to import the `<country code>.tsv` files, do the following:
   a. Login as an admin user on the "other" NE-ONE.
   b. From the Web Interface, click **Management > ••• Platform Settings > File Browser**.
      The **File Browser** page opens with the path of your `/Private` directory.
   c. Navigate to the `/Library/customer_countries` directory.
   d. Right mouse click and select **Upload new File**.
      A dialog box appears prompting you to select a file to upload.
   e. Click the **SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the appropriate `<country code>.tsv` file to upload. Then click **OK**.
   f. Repeat sub-steps d to e until all the `<country code>.tsv` files are uploaded to the "other" NE-ONE.

   The custom locations from the "master" NE-ONE are now available on the "other" NE-ONE.

18. CONFIGURE EXTERNAL ROUTING

Use this section when you install the NE-ONE for the first time within your network if it uses dynamic routing (adaptive routing), or at a later time if the network has changed to use dynamic routing (adaptive routing).

Note:

At the time of publication, the NE-ONE currently supports BGP, OSPF, OSPFv6, RIP, and RIPng routing protocols. If your organization uses another routing protocol such as Interior Gateway Routing Protocol (IGRP) or Intermediate System to Intermediate System (IS-IS), contact your Calnex representative for more information on how and when those other routing protocols will be implemented on the NE-ONE.

In order for the NE-ONE to inter-operate with networks using dynamic routing (adaptive routing), external routing must be configured on NE-ONE for the routing protocols used within the network.

External routing on the NE-ONE is configured for example in production or DevOps environments, when connecting to the edge of the corporate network. External routing on the NE-ONE would not be configured in a pure test environment.

Table 10 provides a high level comparison between the different routing protocols supported by the NE-ONE, and when they are typically used. If you require assistance defining your external routing requirements, contact your Calnex support representative for further support.

TABLE 10 - HIGH LEVEL COMPARISON BETWEEN ROUTING PROTOCOLS SUPPORTED ON THE NE-ONE

Comparison Criteria		RIP RIPng	BGP	OSPF OSPFv6
Algorithm used		Bellman Ford	Best Path Selection	Dijkstra algorithm
Routing Protocol Method		Distance Vector Routing (DVR) protocol that uses the distance or hops count to determine the transmission path.	Path Vector Routing (PVR) protocol that provides routing information for autonomous systems on the Internet via its AS-Path	Link State Routing (LSR) protocol and it analyzes different sources like the speed, cost and path congestion while identifying the shortest path.
Organization size used within		Small	Large (exterior gateway protocol, typically only at edge locations)	Large (interior gateway protocol)
Typical use within the large organization (between BGP and OSPF)	Internet redundancy	Not applicable for comparison	Most often used	Never or rarely used
	LAN environments		Never or rarely used	Most often used
	WAN environments		Most often used	Occasionally used
	Data center		Never or rarely used	Most often used
	IaaS environments		Most often used	Occasionally used
Maximum hops allowed	Maximum hops allowed	15	255	No restriction on the hop count.

Comparison Criteria		RIP RIPng	BGP	OSPF OSPFv6
Networks classified as	Networks classified as	Areas and tables.	Peers.	Areas, sub areas, autonomous systems and backbone areas.
Default administrative distance	Default administrative distance	120	20	110
Protocol (port) used	Protocol used	UDP (520)	TCP (179)	IP (89)
By default, for path selection calculates the metric in terms of	By default, for path selection calculates the metric in terms of	Hop Count (only next hop in calculation)	Hop Count (determines best path as calculation, includes the 'path' of ASes that are used to reach the destination)	Bandwidth

18-1. External Routing Prerequisites

Check with your network administrator if the organization is using dynamic routing (adaptive routing) or static routing (non-adaptive routing).

- If the organization is static routing (non-adaptive routing), no further action is required (i.e. external routing on the NE-ONE does not need to be configured).
- If the organization is using dynamic routing (adaptive routing), the network administrator will have chosen a routing protocol of preference (BGP, OSPF, OSPFv6, RIP, or RIPng) for the network and will have defined routing tables on the routers within the network. In this case external routing on the NE-ONE needs to be configured.
  - Ask the network administrator which routing protocol is implemented within the network, and the external routing tables that you need to define on the NE-ONE in order for the NE-ONE to inter-operate with the routing protocol that is implemented within the network.

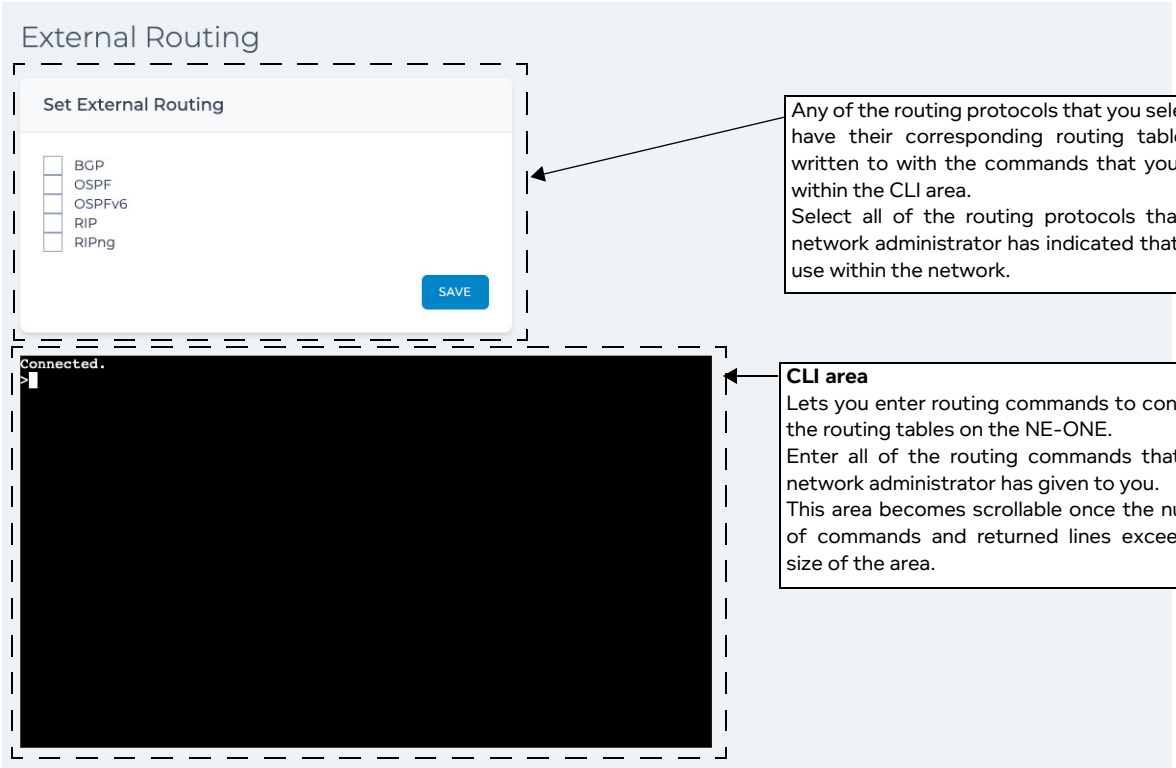
    The network administrator will indicate which routing protocol is implemented within the network and the routing commands that you need to specify in order to build the routing tables on the NE-ONE. Once you have this information from the network administrator, proceed to *Configuring External Routing* on page 91.

18-2. Configuring External Routing

If the NE-ONE is implemented in a network where dynamic routing (adaptive routing) is used then the NE-ONE must be configured to use external routing based upon the routing information that you obtained from your network administrator.

The **External Routing** page (see *Illustration 16*) lets you set up external routing on the NE-ONE so that it can inter-operate within networks that use dynamic routing (adaptive routing).

ILLUSTRATION 16 - THE EXTERNAL ROUTING PAGE



The **External Routing** page contains the following:

- A **Set External Routing** tile with check boxes allowing to select one or more of the following routing protocols:
  - **BGP** - Border Gateway Protocol
  - **OSPF** - Open Shortest Path First
  - **OSPFv6** - Open Shortest Path First for IPv6 (used only for Cisco devices to define the configuration done with the `ipv6 router ospf` command).
  - **RIP** - Routing Information Protocol
  - **RIPng** - Routing Information Protocol (next generation for IPv6)
- A command line interface (CLI) area lets you enter routing commands letting you set up your routing table and routing rules according to your routing requirements. Any of the routing commands that you enter in the CLI area will get written to the routing table file(s) of the selected routing protocol(s).

  The command line interface (CLI) area initially appears with the top-level command prompt, >.

  To enter a particular routing mode's command line in the command line window, the appropriate check box in the **Set External Routing** tile must be checked, and you must enter the appropriate command of the format **`ip-routing <routing protocol>`**, where **`<routing protocol>`** is

either **bgp**, **ospf**, **ospfv6**, **rip**, or **ripng**. For example:

- To enter the BGP routing mode, enter **ip-routing bgp**

  A bgp# prompt will appear. Any commands you enter from the bgp# prompt will be applied to the BGP routing table.
- To enter the OSPF routing mode, enter **ip-routing ospf**

  An opsf# prompt will appear. Any commands you enter from the ospf# prompt will be applied to the OSPF routing table.
- To enter the OSPFv6 routing mode, enter **ip-routing ospfv6**

  An opsfv6# prompt will appear. Any commands you enter from the ospfv6# prompt will be applied to the OSPFv6 routing table.
- To enter the RIP routing mode, enter **ip-routing rip**

  A rip# prompt will appear. Any commands you enter from the rip# prompt will be applied to the RIP routing table.
- To enter the RIPng routing mode, enter **ip-routing ripng**

  A ripv6# prompt will appear. Any commands you enter from the ripng# prompt will be applied to the RIPv6 routing table.

To exit a particular routing mode, enter **exit**. The command prompt returns to the top level command prompt, >.

Entering **?** at any time returns the help pages associated to where you are within the command line hierarchy.

Entering **ippe-interfaces** at the top-level command prompt results in returning the list of configurable interfaces on the NE-ONE.

Pressing the **Tab** key at any time auto-completes and proposes any applicable commands that correspond to where you are within the command line hierarchy.

Continuously pressing the **Up Arrow** cursor key any time cycles through the previously entered commands.

Use the following steps to configure the external routing tables on the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > External Routing**.
2. From the **External Routing** page (see *Illustration 16*) that appears, do the following:
   a. In the **Set External Routing** tile, tick the appropriate check boxes corresponding to the routing protocols that you want the NE-ONE to use.

      During the *External Routing Prerequisites* on page 90, your network administrator will have communicated to you which routing protocols are implemented in the network, and which routing protocols that they want you to implement on the NE-ONE.
   b. Click **SAVE**.

      The NE-ONE will write the commands entered into the routing files of routing protocols that you selected in the **Set External Routing** tile.
3. In the CLI area, do the following for each of the routing protocols that you want to configure.
   a. Enter an appropriate routing mode, by entering the appropriate command of the format:

      ip-routing <routing protocol>

      where **<routing protocol>** is either **bgp**, **ospf**, **ospfv6**, **rip**, or **ripng**.

      The command line prompt changes according to the routing mode that you entered. For example, if you had entered **ip-routing ospf**, an ospf# prompt appears.
   b. Enter all the appropriate routing commands to set up your routing tables as required.

During the *External Routing Prerequisites* on page 90, your network administrator will have communicated to you which routing commands to specify in order to build the routing tables on the NE-ONE.

c. Once you have finished setting up the appropriate routing, enter **`wr f`** to in order write all of the routing commands that you had entered into the routing table file for the current routing protocol.

d. Exit the routing mode, by entering:

`exit`

The command prompt returns to the top level command prompt, >.

e. Repeat the sub-steps a to d for each of the routing protocols that you want to configure.

18-3. OSPF Routing Example

It is beyond the scope of this *User and Administration Guide* to go into detail about all routing examples. Your Network Administrator will provide you with the actual routing commands to enter. However, the example below shows the steps you take to illustrate the general usage of the **External Routing** page command line area.

In the example below, of the two interfaces (ippe1 and ippe2) that exist on the NE-ONE, the interface **ippe1** is configured using the OSPF routing protocol, and has a not-so-stubby (NSSA) type area with a decimal ID of 1 (i.e. **area 1**) assigned to it with the class 2 **10.0.0.0/24** network.

1. From the Web Interface, click **Management > ··· Platform Settings > External Routing**.
2. From the **External Routing** page (see *Illustration 16*) that appears, do the following:
   a. In the **Set External Routing** tile, tick the **OSPF** check box.
   b. Click **SAVE**.
   The NE-ONE will write the commands you enter into the OSPF daemon file `ippe/config/external_routing/ospdf.conf`.
3. Query the available interfaces on the NE-ONE, by entering:
   `ippe-interfaces`
   The command line returns the available interfaces. For our example above, the following available interfaces are returned.
   ```
   ippe1    1
   ippe2    2
   ```
   Make a mental note of the interface that you want to configure. In our example, we will configure the interface called **ippe1** later on.
4. Go into the OSPF routing mode, by entering:
   `ip-routing ospf`
   The command line prompt changes to `ospf#`, indicating that you are currently in the OSPF routing mode.
5. Go into configure terminal mode, by entering:
   `conf t`

   Note:
   You can also use **`configure terminal`**, however, the shorthand command **`conf t`** is quicker to type.

   The command line prompt changes to `ospf(config)#`, indicating that you are currently in the OSPF configure terminal mode.
6. Go into configure router mode, by entering:

`router ospf`

The command line prompt changes to `ospf(config-router)#`, indicating that you are currently in the OSPF router configuration mode.

7. Create an OSPF area with decimal value 1 to be a not-so-stubby (NSSA) type area, by entering:

   `area 1 nssa`

8. Assign the class 2 network of 10.0.0.0/24 to the **area 1** that you just created, by entering:

   `network 10.0.0.0/24 area 1`

   The OSPF area 1 has now been configured, and is ready to be assigned to interface ippe1.

9. Exit the OSPF router configuration mode, and return up one level in the command line, by entering:

   `exit`

   The command line prompt changes to `ospf(config)#`, indicating that you are back in the OSPF configure terminal mode.

10. Select the interface called **ippe1** to be configured, by entering:

    `interface ippe1`

    The command line prompt changes to `ospf(config-if)#`, indicating that you are currently in the OSPF interface configuration mode.

11. Assign the OSPF router **area 1** to the interface ippe1, by entering:

    `ip ospf area 1`

    The interface ippe1 is now configured to use the OSPF area 1 that you had created in steps 7 to 8 above.

    At this stage the OSPF routing commands that you entered have not yet been saved (i.e. written) to file on the NE-ONE.

12. Write the OSPF routing configuration that you had made to file by entering:

    `wr f`

    Note:

    You can also use **`write file`**, however, the shorthand command **`wr f`** is quicker to type.

    Note:

    You can use **`write file`** or **`wr f`** at any time (i.e. any position within the command line hierarchy). Any of the routing commands that you have entered will be saved to file. If you have a large number of routing commands to enter, it is useful to progressively write them to file by using the **`write file`** or **`wr f`** command.

    The routing commands you had entered are now written into the OSPF daemon file `ippe/config/external_routing/ospfd.conf`. The changes take effect immediately (i.e. the NE-ONE does not need to be rebooted).

13. Exit the OSPF interface configuration mode, and return up one level in the command line, by entering:

    `exit`

    The command line prompt changes to `ospf(config)#`, indicating that you are back in the OSPF configure terminal mode.

14. Exit terminal mode, by entering:

    `exit`

    The command line prompt changes to `ospf#`, indicating that you are back in the OSPF routing mode.

15. Exit OSPF routing mode, by entering:

    `exit`

    The command line prompt changes to >, indicating that you are back to the top level of the command line.

CHAPTER 5 PORTS AND SERVICES MANAGEMENT

1. INTRODUCTION

This chapter is applicable to admin users, and describes managing ports and services on the NE-ONE.

Typically an admin user uses the procedures in this chapter at installation time and/or at a later date in order to set up soft ports, port pairs, and services on the NE-ONE, and to configure port addressing of port pairs.

Note:

If the NE-ONE is to be used in a network implementation where dynamic routing is required between soft ports used within the user's SDTNs and the test network environment, the admin user must also configure external routing (see *Configure External Routing* on page 89) according to their routing needs **after** the creation of the required soft ports that is undertaken within this chapter.

Once set up, soft ports, and port pairs are available to users for use within the Web Interface when they create Point-to-Point or Multi-Point networks.

! Notice:

Before creating users, Calnex recommends that you create and configure all the soft ports and port pairs that will be needed on the NE-ONE. This is because the **Edit User Details** page (see *Illustration 58* on page 202) which is used when creating a user includes a dynamic list of soft ports and port pairs, which can change as more soft ports are added or deleted. If you create additional soft ports or port pairs after creating a user, those new soft ports/port pairs are not enabled by default for those users, and you would have to reconfigure the user's permissions in order to add the new soft ports/port pairs.

Note:

Not all, but the majority of the information in this chapter is related to use with the Port Manager feature and Service Manager feature (see *Table 12*). Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated.

TABLE 11 - SUMMARY OF FEATURE SPECIFIC INFORMATION

Section within chapter	Specific to the Port Manager feature ?	Specific to the Service Manager feature ?
Section 1-1, *Ports Management*	YES	N/A
Section 1-2, *Port Pairs*	NO	N/A
Section 1-3, *Available Port Management Capabilities*	NO	N/A
Section 1-4, *Service Management*	N/A	YES
Section 2, *Managing Ports*	YES	N/A
Section 3, *Managing Port Pairs*, containing: *Section 3-1*, *Creating Port Pairs* *Section 3-2*, *Editing Port Pairs* *Section 3-3*, *Deleting Port Pairs* *Section 3-4*, *Port Pair Settings*	 YES YES YES NO	 N/A N/A N/A N/A
Section 4, *Managing Services*	N/A	YES

Table 12 summarizes the tasks an admin user can undertake within this chapter.

TABLE 12 - HIGH LEVEL STEERING GUIDE

Step	Task	Specific to the Port Manager feature ?	Specific to the Service Manager feature ?
1	Configure all the necessary soft ports and port pairs, according to *Managing Ports* on page 103 and *Managing Port Pairs* on page 156, respectively.	YES	N/A
2	If necessary, configure Port Addressing according to *Configuring Port Addressing* on page 167 in *Chapter 5*, *Ports and Services Management*	NO	N/A
3	If necessary, configure services according to *Managing Services* on page 177 within *Chapter 5*, *Ports and Services Management*	N/A	YES
4	If necessary, configure a DHCP relay according to *DHCP Server / DHCP Relay* on page 172 in *Chapter 5*, *Ports and Services Management*	N/A	YES

1-1. Ports Management

1-1-1. Soft Ports

The NE-ONE has a minimum of two hardware ports. Depending on your NE-ONE model, you can have up to eight hardware ports, numbered 0 to 7.

In addition to the hardware ports, if the Port Manager feature is activated, the NE-ONE additionally lets you create soft ports.

Soft ports are very useful for:

- port sharing in a multi user environment,
  or
- if you need a lot ports to plug test devices into, but your data rates are modest so that you can share a hardware port with a lot of test devices.

If you have many users, you can create many soft ports, and assign certain soft ports to certain users according to their testing needs. For more information on assigning soft ports to users, see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205 in *Chapter 6*, *User Administration*.

Soft ports are also very useful for generating traffic, creating ping targets, and for dumping packets.

Different types of soft ports are created via soft port functions. Each of the soft port functions, and their typical use cases are described in *Available Soft Port Functions* on page 96.

1-1-1-1. Available Soft Port Functions

Table 13 lists the types of soft port functions available to the NE-ONE.

Note:

For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date. As new soft port functions get developed, having an active maintenance contract lets you add those new soft port functions via software updates.

TABLE 13 - AVAILABLE SOFT PORT TYPES

Soft Port Function	Description
Soft Port : VLAN (for more information, see *Creating a VLAN Soft Port* on page 107).	This function lets you select traffic from the parent port by VLAN Id. Unlike the more generic *Soft Port : Filter* described below this port is also intelligent with the ability to detag and retag (i.e. change the tag) VLAN Ids in packets on output. Thus the port you define has just some of the data that came into the parent port. This function uses hashing to provide extremely fast mapping of the 802.1q VLAN tags to the relevant soft port. This is especially useful in cases where parent ports (typically hardware ports) are divided into larger numbers (i.e. >10) of VLAN child ports. Multiple VLAN Ports can be defined for a parent port letting you carve up a VLAN Trunk – effectively "pretending" that the traffic originated at its own port. This feature is very useful for port sharing in a multi user or multi port environment.
Soft Port : IPv4 (for more information, see *Creating an IPv4 Soft Port* on page 114).	This function lets you create a child port of a parent port that has an IPv4 address (as well as a Netmask, Gateway, DHCP Relay and Multicast – or not – capability), and supports Dynamic NAT. Unlike the more generic *Soft Port : Filter* port described below, this port is also intelligent with the ability to Respond to ARP requests, Make ARP requests and Respond to Pings (ICMP Echo) both externally and internally. Thus the port you define has just some of the data that came into the parent port. Multiple IPv4 soft ports can be defined for a parent port allowing the parent to appear to have many IPv4 addresses on the same hardware port for routing. This feature is very useful for port sharing in a multi user or multi port environment and also for having the NE-ONE route either between ports or on a "stick" (out of the same port). **Note:** DHCP Relay is performed together with the DHCP Relay Service (see *Managing Services* on page 177). Using the DHCP Relay service, up to 10 DHCP servers are supported.
Soft Port : IP (for more information, see *Creating an IP Soft Port* on page 122).	This function lets you create a child port of a parent port that has both an IPv4 address and an IPv6 address (as well as a Netmask, Gateway, DHCP Relay and number of significant bits of the network portion for IPv6 addresses). Unlike the more generic *Soft Port : Filter* soft port function described above this port is also intelligent with the ability to Respond to ARP requests, Make ARP requests, Make Neighborhood solicitations and respond to Neighborhood solicitations and Respond to Pings (ICMP Echo – IPv4 and IPv6) both externally and internally. You can also define the MAC address or the port or let one be constructed for you. Thus the port you define has just some of the data that came into the parent port. Multiple IP Ports can be defined for a parent port allowing the parent to appear to have many IPv4 and IPv6 addresses on the same hardware port for routing. This feature is very useful for port sharing in a multi user or multi port environment and also for having the NE-ONE route either between ports or on a "stick" (out of the same port). **Note:** DHCP Relay is performed together with the DHCP Relay Service (see *Managing Services* on page 177). Using the DHCP Relay service, up to 10 DHCP servers are supported.

Soft Port Function	Description
Soft Port : Filter (for more information, see *Creating a Filter Soft Port* on page 124).	This function lets you select traffic from the parent port by source and/or destination IP address and/or TCP/UDP port and/or VLAN Id. Thus the port you define has just some of the data that came into the parent port. Multiple filter ports can be defined for a parent port letting you carve up its traffic – effectively "pretending" that the traffic originated at its own port. This feature is very useful for port sharing in a multi user environment. For example, you may want to filter by an end user's IP address in a large multi-user environment. In this case, you could create a VLAN parent soft port, which accommodates an IPv4 child soft port which acts as a network gateway for a set of end users. Then within the IPv4 child soft port you could create hardware filter soft ports filtering on each end user's source IP address.
Soft Port : Expression Filter (for more information, see *Creating an Expression Filter Soft Port* on page 132).	This function lets you select traffic from the parent port by using the "Wireshark like" expression syntax. This allows many more possibilities than the *Soft Port : Filter* soft port function on which it is based - other than this its function is similar. Thus the port you define has just some of the data that came into the parent port. Multiple Expression Filter Ports can be defined for a parent port letting you carve up its traffic – effectively "pretending" that the traffic originated at its own port. This feature is very useful for port sharing in a multi user environment.
Soft Port : Static NAT (for more information, see *Creating a Static NAT Soft Port* on page 138).	This soft port function is Network Address Translation (NAT) function designed to perform static NATing and de-NATing of source and destination IPv4 addresses. This function has the following parameters: • Source IP Address - as a packet enters the soft port from the outside, if it matches this source address its source IPv4 address will changed to Inside Source IP Address (see below) • Dest IP Address - as a packet enters the soft port from the outside, if it matches this destination address its destination IPv4 address will changed to Inside DestIP Address (see below) • Inside Source IP Address - as a packet leaves the soft port from the inside, if it matches this source address its source IPv4 address will changed to Source IPAddress (see above) • Inside Dest IP Address - as a packet leaves the soft port from the inside, if it matches this destination address its destination IPv4 address will changed to Dest IP Address (see above) The idea behind this soft port is to allow, for example, a server with a real destination address of 10.10.10.10 (say) to be accessed by client 192.168.10.10 (say) as address 10.10.11.10 (say). The server would believe that the client had address 192.168.11.10 (say). This would mean that the server would remain accessible by its normal address 10.10.10.10 but if a user specified 10.10.11.10 then the core routers would direct that traffic to the NE-ONE which would NAT the destination addresses to be the real server and the source address to be a spoofed client. On the way back the NAT would be reversed to allow the server to respond indirectly to the real client.

Soft Port Function	Description
Generate : Hardware Traffic Generation (for more information, see *Creating a Hardware Traffic Generation Soft Port* on page 145).	This function creates a multi stream traffic generation port. In general (in order to not waste the use of a top level hardware port) because it is a traffic generating object it will not be set up as a child port. Instead it will be a top level port. Streams consist of: • VLAN Id (optional) – 0 = No VLAN Tag • Stream Type – TCP or UDP Ethernet Source Address Ethernet Destination Address Source TCP/UDP Port Destination TCP/UDP Port TTL • IP (V4 or V6) Source Address • IP (V4 or V6) Destination Address • Packet Data – partial contents Packet Size (without CRC) Packets per second (rate) • Bits per second (rate) • Stream enabled i.e. is generating One of Packets per second or Bits per second must be non zero. Multiple Generating Ports can be defined. This feature is very useful for: • Loading links with traffic which may compete with real traffic and create bottlenecks for testing. • Generate external traffic. **Note:** For simplicity, consolidation, and ease of use within the Web Interface, the Generate : Hardware Traffic Generation function is grouped with the other soft port functions. However, in terms of networking, the Generate : Hardware Traffic Generation function does not create a parent port that accepts traffic from other ports - it is simply a traffic generation object.

1-1-1-2. Soft Port Rules

Soft ports adhere to the following rules:

- You can define more than one soft port child for a parent port.
- You can also define multiple levels of soft ports, such that you can define more than one child soft port within a parent soft port.

  The normal use of this is to create parent VLAN soft ports and child IPv4 / IP soft ports of these parent VLAN soft ports. Furthermore, if necessary you can create child Filter soft ports within the IPv4 / IP soft ports for further filtering in an extremely large multi-user environment.
  VLAN soft ports are discussed in *Creating a VLAN Soft Port* on page 107. IPv4 soft ports and IP soft ports are discussed in *Creating an IPv4 Soft Port* on page 114, and *Creating an IP Soft Port* on page 122, respectively. Filter soft ports are discussed in *Creating a Filter Soft Port* on page 124.
- Once you have created a soft port (child) of a parent port, the original parent port is no longer available for a network, only the child soft ports are available.
- Soft ports are semi-permanent (i.e. they will be recreated on a reboot) and exist outside any particular network. A soft port that you define may be used by other users (provided their security permits it) on the NE-ONE, but a soft (or hardware port) may only be used in one running network at a time.
- You cannot create a soft port on a port that is already part of a port pair.
- You can create top level soft ports at the same level as hardware ports. Typically you create top level soft ports when not needing (or not wanting to waste using a top level hardware port) in situations such as
  - generating traffic (with the use of the *Generate : Hardware Traffic Generation* function)
  - creating ping targets (with the use of either the *Soft Port : IPv4* or *Soft Port : IP* function)

  - creating a port for packet dumping (with the use of the *Soft Port : VLAN* function)
- Child soft ports of parent hardware ports are always subject to the fact that their parent port can only handle a certain total I/O – 1 Gbps for Gigabit Ports, and 10 Gbps for 10 Gigabit ports.

1-2. Port Pairs

Port pairs are extremely useful as they allow NE-ONE users to rapidly create Point-to-Point type network based on pre-defined port pairs. Port pairs, thus avoid the need for the user to additionally select the ports during the Point-to-Point network creation process.

Depending on whether or not the Port Manager feature is activated on the NE-ONE, pre-defined port pairs will either already exist or not already exist, as follows:

- If the Port Manager feature is deactivated on the NE-ONE, then by default a set of pre-defined hardware port pairs will already be available and pre-configured.
- If the Port Manager feature is activated on the NE-ONE, then by default, the NE-ONE is not configured with any point pairs. Port pairs can be created between the different port types using the Port Manager, as follows:
  - between two hardware ports
  - between two soft ports
  - between a hardware port and a soft port

Note:

The NE-ONE is flexible in its use letting you create port pairs between a hardware port and a soft port. However, even if this is possible, it usually makes no networking sense to create a port pair between a hardware port and a soft port.

Additionally, port pairs also allow Point-to-Point networks to be created to run over port pairs configured with specific port addressing criteria (e.g. to operate like a network router or to bridge two sub-networks). For more information on configuring a specific port addressing criteria for a port pair, see *Port Addressing* on page 162.

1-3. Available Port Management Capabilities

Table 14 below summarizes the different port management capabilities that are available on the NE-ONE according to weather or not the Port Management feature is activated.

TABLE 14 - PORT MANAGEMENT CAPABILITIES

Port Management Capabilities	Port Manager Feature Activated	Port Manager Feature Deactivated	For more information, see
See and use the Port Manager	Yes	No	*The Port Manager Page* on page 103
Create soft ports	Yes	No	*Creating Soft Ports* on page 107
Edit soft ports	Yes	No	*Editing Soft Ports* on page 151
Delete soft ports	Yes	No	*Deleting Soft Ports* on page 151
Create port pairs	Yes	No	*Creating Port Pairs* on page 158
Edit port pair	Yes	No	*Editing Port Pairs* on page 160
Delete port pair	Yes	No	*Deleting Port Pairs* on page 161
Configure specific port addressing	Yes	Yes	*Port Addressing* on page 162
Configure default transmission	Yes	Yes	*Default Transmission* on page 175

1-4. Service Management

An NE-ONE without the Service Manager feature already comes with some in-built services such as Port Addressing (see *Port Addressing* on page 162) and Default Transmission (see *Default Transmission* on page 175) for simple network testing environments.

The Service Manager feature of the NE-ONE lets you create and manage additional services for more complex network testing environments, such as:

- using DHCP helper services
- using background port to port transmission via either the Background service or Background Expression Routed service

If the Service Management feature is activated on the NE-ONE, you can create and use these services to create more complex test networks with DHCP helpers and/or background port to port transmission (either with or without complex expression routing).

Services are an additional capability that in many ways function like soft ports (see *Available Soft Port Functions* on page 96), in that they are independent of running networks. Unlike soft ports they are not directly associated with any particular hardware.

1-4-1. Available Services Functions

The NE-ONE currently has the following service functions available that you can use to create and assign to ports:

- DHCP Helper
- Background Expression Routed
- Background

Note:

For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date. As new service functions get developed, having an active maintenance contract lets you add those new service functions via software updates.

Table 15 describes the differences between the service functions available to the NE-ONE, and indicate what service function/type you would use according to your networking needs.

TABLE 15 - HIGH LEVEL COMPARISON BETWEEN SERVICES

Service Function	Service Type	Services to be run	Ports (Hardware /Soft)	Implementation Remarks
Service:DHCP_Helper	Helper (see *section 1-4-1-1*)	Multiple	IPv4 and IP soft ports	For use with one or multiple DHCP servers (up to 10) in the network
Service:Background_Expression_Routed	Background (see *section 1-4-1-2*)	Single	Hardware or soft ports	Best for port pairs
Service:Background		Single		Best for meshes between three or more ports

1-4-1-1. The DHCP Helper Service

The DHCP Helper service lets you create and run up to 10 DHCP Helper services. This service is intrinsically linked with the DHCP Relay function of IP and IPv4 soft ports, and so is described there in *Creating an IPv4 Soft Port* on page 114 and *Creating an IP Soft Port* on page 122. When creating an IP soft port or IPv4 soft port you can specify which of the 10 DHCP Helper services you want to use.

1-4-1-2. The Background Services

Background services allow port to port transmission when no network is running. The difference between the two Background services is that Background is the best to use for connecting ports in pairs and Background Expression Routed is the one to use for creating meshes between three or more ports.

The services Service:Background Expression Routed and Service:Background allow the creation of background services that connect ports together, and passes packets between those ports when no network is running on those ports.

When a network requests some of the ports managed (controlled) by these background services they are released for use by the network. The background service continues to run managing any other ports that are not in use in any running network.

When a network stops running, the background service is notified and resumes management of the ports. It is possible to have many background services, if required.

The ports used in the background can be either hardware ports or soft ports (or both). There are many possible configurations of background service, which are discussed in the examples within *Section 4-2*, *Creating Services* on page 178.

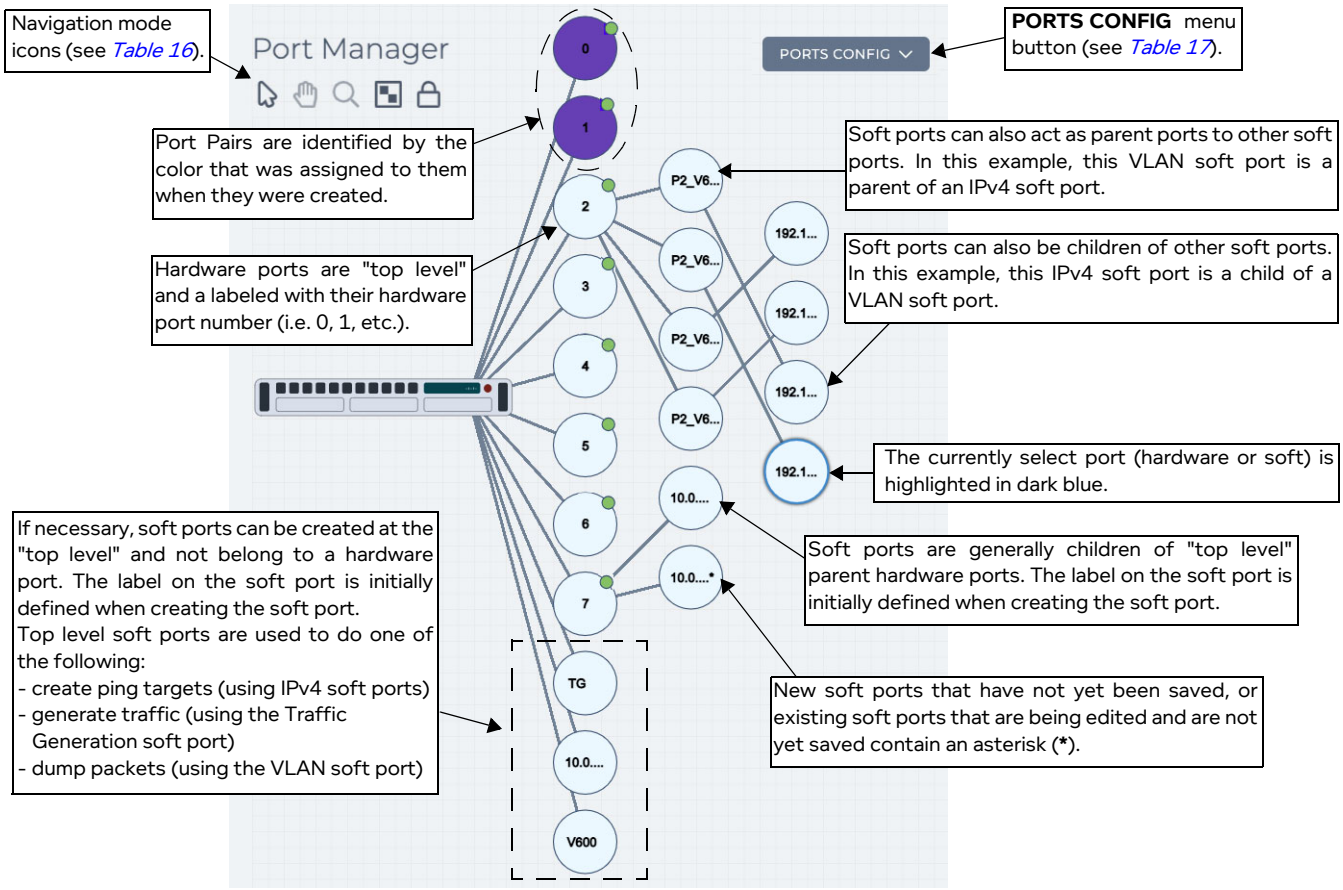
2. MANAGING PORTS

This section is only applicable to the NE-ONE with the Port Manager feature activated. Depending on your license, the Port Manager feature may be activated or deactivated.

2-1. The Port Manager Page

To launch the **Port Manager** page (see *Illustration 17*) select **Management > Port Manager**.

ILLUSTRATION 17 - PORT MANAGER PAGE (WITH EDIT PORT PANEL HIDDEN)



The **Port Manager** page (see *Illustration 17*) provides a visual editor letting you manage all soft port related functions on the NE-ONE, such as:

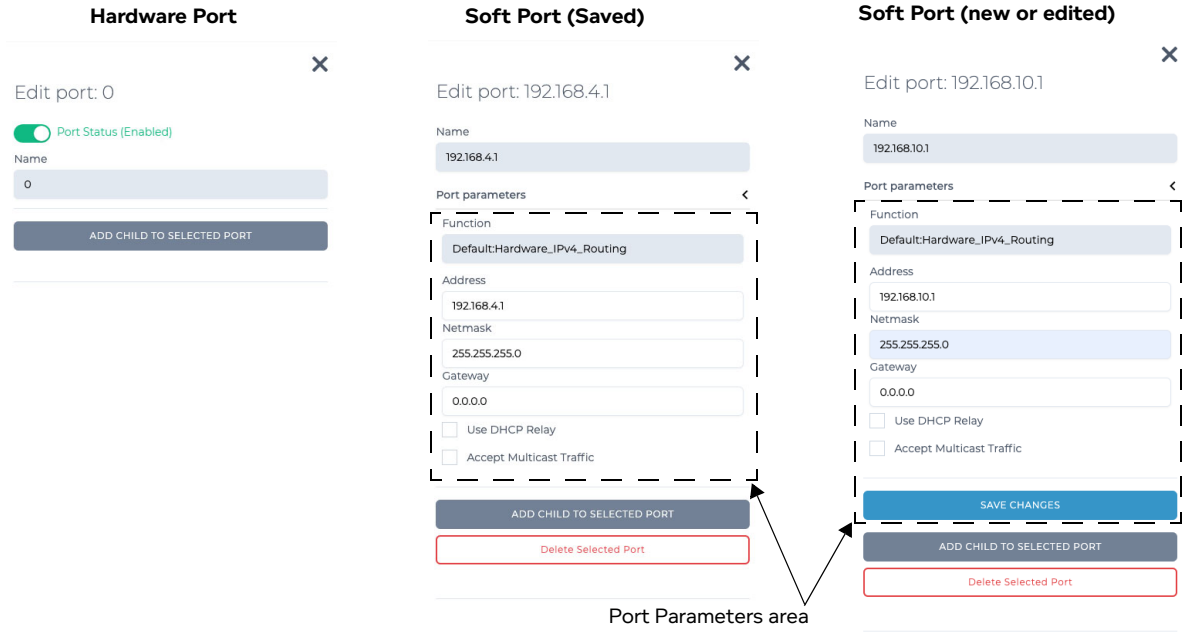
- creating soft ports (i.e. adding a child soft port to an existing parent (hardware or soft) port)
- editing soft ports (i.e. editing the parameters of an existing soft port's function)
- deleting soft ports (i.e. deleting an existing soft port from its parent port)

Note:

The **Port Manager** page shows any pre-defined port pairs that exist. Creation and management of port pairs are done from within the **Port Pairs** page. For more information, see *Managing Port Pairs* on page 156.

Ports (hardware or soft) are represented by circles in the **Port Manager** page. Clicking on a port (hardware or soft) reveals an **Edit Port** side panel (see *Illustration 18*) on the right hand side of the **Port Manager** page. The circles representing a port may have a lock icon attached to them, representing that a network is currently running on that port. If a circle representing a port has a lock icon attached to it, the port cannot be edited until the currently running network is stopped.

ILLUSTRATION 18 - COMPARISON OF EDIT PORT SIDE PANEL - HARDWARE VS SOFT PORT



The elements (i.e. buttons, fields, and check boxes) available on the **Edit Port** side panel depend on the type of port selected. Hardware ports cannot be deleted, whereas soft ports can be deleted (if they are not parents to other lower level children soft ports).

- If a hardware port is selected, the **Edit Port** side panel provides an **ADD CHILD TO SELECTED PORT** button and a **Port Status (Enabled)** toggle button.
  - Clicking on the **ADD CHILD TO SELECTED PORT** button invokes the Soft Port Creation Wizard, from where you can create a new soft port (i.e. choose the soft port function, and define all the parameters of that soft port function). The created soft port will be a child of the parent port from where it was created.

    For more information about the available soft port functions, see *Available Soft Port Functions* on page 96. For more information on the Soft Port Creation Wizard and creating soft ports, see *Creating Soft Ports* on page 107.
  - Clicking on the **Port Status (Enabled)** button toggles between enabling and disabling the hardware port. By default all hardware ports are enabled. An enabled hardware port contains a small green circle, while a disabled hardware port contains a small red circle. In the example **Port Manager** page in *Illustration 17* all hardware ports 0 - 7 are enabled.
- If a soft port is selected, the **Edit Port** side panel provides:
  - An expandable/collapsible **Port Parameters** area. The **Port Parameters** area is visible (i.e. expanded) by default.

    Clicking on the **<** icon hides (i.e. collapses) the **Port Parameters** area. Clicking on the ⌄ icon shows (i.e. expands) the **Port Parameters** area.

    The **Port Parameters** area shows the soft port function that was selected when the soft port was created, and elements (i.e. fields and check boxes) associated to defining the parameters of the soft port function.
  - An **ADD CHILD TO SELECTED PORT** button. Clicking on the **ADD CHILD TO SELECTED PORT** button invokes the Soft Port Creation Wizard, from where you can create a new soft port (i.e. choose the soft port function, and define all the parameters of that soft port function). The created soft port will be a child of the parent port from where it was created.

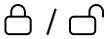
For more information about the available soft port functions, see *Available Soft Port Functions* on page 96. For more information on the Soft Port Creation Wizard and creating soft ports, see *Creating Soft Ports* on page 107.

- A **Delete Selected Port** button. Clicking on the **Delete Selected Port** button invokes a **Delete port** confirmation dialog box, from where you confirm whether the soft port is removed. For more information, see *Deleting Soft Ports* on page 151.
- A **SAVE CHANGES** button (if the soft port is new or being edited). Clicking the **SAVE CHANGES** button commits the parameters of the soft port function to the NE-ONE.

Note:
If a "parent" soft port containing other "child" soft ports is selected, the **Edit Port** side panel will not contain the **Delete Selected Port** button. This is normal because you cannot delete a "parent" soft port if it contains "child" soft ports.

The **Port Manager** page (see *Illustration 17*) also contains the navigation mode icons summarized in *Table 16*.

TABLE 16 - PORT MANAGER NAVIGATION MODE ICONS

Port Manager Navigation Icon	Description
	When you arrive in the **Port Manager** page, this icon (object select mode) is selected by default. Clicking on this icon selects and enables object select mode. When object select mode is enabled you can click on ports and the NE-ONE within the **Port Manager** page in order to select them for editing or adding additional soft ports.
	Clicking on this icon selects and enables canvas pan mode. When canvas pan mode is enabled, you can move the canvas (which contains the image of the NE-ONE and is associated ports) in the appropriate direction when the left mouse button is clicked.
	Clicking on this icon selects and enables canvas zoom mode. When canvas zoom mode is enabled, you can zoom in and out, as follows: • Zoom in on the canvas by clicking the left mouse button and moving the mouse to the right. • Zoom out on the canvas right by clicking the left mouse button and moving the mouse to the left.
	Clicking on this icon at any time results in auto-arranging the ports back into the columns associated to their hierarchy.
	The padlock open ( ) and padlock closed ( ) icons determine whether you can move or not move the position of the soft ports within the **Port Manager** page, respectively. When you arrive in the **Port Manager** page, the padlock closed icon ( ) is active by default. Clicking on the padlock icons toggles between their open and closed states. • When the padlock closed icon ( ) is active, the soft port positions are locked, and cannot be moved. • When the padlock open icon ( ) is active, the soft port positions are unlocked, and can be moved. To move a soft port, do the following: 1. While left mouse clicking on the soft port drag the mouse to the desired location. 2. Once the soft port is at the desired position let go of the left mouse button.

The **Port Manager** page (see *Illustration 17*) also contains the **PORTS CONFIG** menu button, with menu items summarized in *Table 17*.

TABLE 17 - PORTS CONFIG MENU ITEMS

Ports Config Menu Item	Description
Save As	The **Save As** menu item lets you save the current ports configuration to a filename. The ports configuration file is written to the `/Private/ports_config` directory. Selecting the **Save As** menu item invokes a dialog box letting you specify a filename to save the current ports configuration. For more information, see *Saving a Ports Configuration* on page 152.
Clear	The **Clear** menu item lets you remove the current soft port configuration and revert the NE-ONE back to its initial hardware port configuration. Selecting the **Clear** menu item invokes a dialog box letting you confirm the removal of all the soft ports and revert the NE-ONE back to its initial hardware port configuration. For more information, see *Deleting (Clearing) All Soft Ports* on page 152.
Load	The **Load** menu item lets you load a previously saved ports configuration on to the NE-ONE. Selecting the **Load** menu item invokes a dialog box letting you select and load the filename of a previously saved soft ports configuration (located in the are located the `/Private/ports_config` directory) on to the NE-ONE. For more information, see *Loading a Ports Configuration* on page 153.

2-2. Creating Soft Ports

Use one of the following sections, according to the type of soft port function that you want to create:

- *Section 2-2-1*, *Creating a VLAN Soft Port* on page 107
- *Section 2-2-2*, *Creating an IPv4 Soft Port* on page 114
- *Section 2-2-3*, *Creating an IP Soft Port* on page 122
- *Section 2-2-4*, *Creating a Filter Soft Port* on page 124
- *Section 2-2-5*, *Creating an Expression Filter Soft Port* on page 132
- *Section 2-2-6*, *Creating a Static NAT Soft Port* on page 138
- *Section 2-2-7*, *Creating a Hardware Traffic Generation Soft Port* on page 145

For more high level information on soft port functions, see *Available Soft Port Functions* on page 96.

Note:

The sections below provide example networks. Adapt the examples to your actual networking needs.

! Notice:

When using the NE-ONE with RADIUS authentication, you cannot define spaces in of the port names when adding the `iTrinegy-NEONE-Ports` attribute to users. For more information, see *Add iTrinegy-NEONE Attributes to New or Existing RADIUS Users* on page 211 in *Chapter 6*, *User Administration*. Therefore, if you use the NE-ONE with RADIUS authentication, you must not use spaces in any of the names of the soft ports that you create. Calnex recommend that you the underscore (_) symbol if required. Additionally, even if the NE-ONE is currently implemented without using RADIUS authentication, in order to future proof the naming of soft ports, never use spaces within the soft port names.

! Notice:

Since the NE-ONE uses the comma (,) symbol as a delimiter within its source code, do not use commas within soft port names.

2-2-1. Creating a VLAN Soft Port

VLAN soft ports let you connect an 802.1Q VLAN trunk from a switch or similar and divide it up, as far as the NE-ONE is concerned, into separate soft ports each selecting one VLAN from the trunk. This allows the NE-ONE to be “fronted” by an 802.1Q capable switch and appear to have many more ports than the NE-ONE physically has built in.

Even very inexpensive switches like the Netgear GS108T can be used. In the example below in *Illustration 19*, the switch’s individual ports are set for separate VLANs as follows:

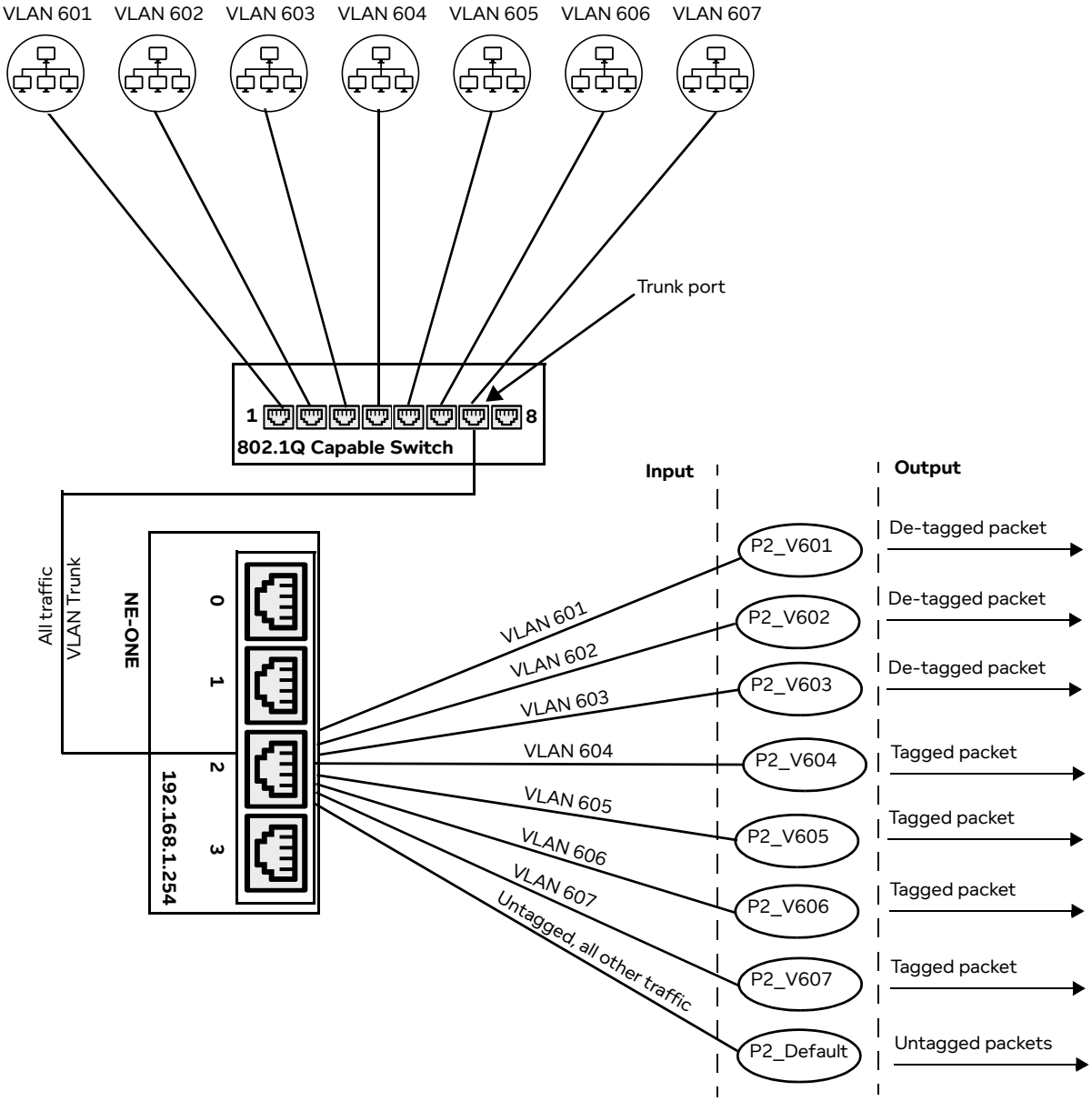
- Switch Port 1 – VLAN 601
- Switch Port 2 – VLAN 602
- Switch Port 3 – VLAN 603
- Switch Port 4 – VLAN 604
- Switch Port 5 – VLAN 605
- Switch Port 6 – VLAN 606
- Switch Port 7, say, Trunk with 802.1Q VLAN tagging on. This Trunk port is now connected to a hardware port 2 on the NE-ONE.

! Notice:

At the time of writing, the cloud computing environments such as AWS and Microsoft Azure do not allow users to create VLANs within their cloud computing environment. Therefore, the use of

VLAN soft ports on the NE-ONE is currently not possible within the AWS and Microsoft Azure cloud computing environments.

ILLUSTRATION 19 - USE OF THE VLAN SOFT PORT FUNCTION TO DIVIDE UP TRAFFIC



Behavior of VLAN soft ports on input:

- A VLAN soft port only receives packets which are tagged (in the 802.1Q sense) with its VLAN Id
- The first VLAN port with **Use as Default Interface** checked (ticked) receives tagged or untagged packets for all VLANs not specifically defined for the port
- The P2_Default soft port is defined with a VLAN Id that does not exist on the 802.1Q switch (e.g VLAN Id of 650). The NE-ONE treats VLAN Id of 650 as meaning untagged packets (on input).

Behavior of VLAN soft ports on output:

- A packet sent out of a tagged VLAN soft port is
  - Re-tagged to the ports VLAN Id if it had a different VLAN tag
  - Tagged to the ports VLAN Id if it had no tag

- De-tagged if the **Detag Packets on Output** flag is set

In the example above in *Illustration 19* the input/output behavior of the VLAN soft ports is as follows:

- P2_V601 receives packets from VLAN Id 601, and removes the VLAN tags on the packets on output.
- P2_V602 receives packets from VLAN Id 602, and removes the VLAN tags on the packets on output.
- P2_V603 receives packets from VLAN Id 603, and removes the VLAN tags on the packets on output.
- P2_V604 receives packets from VLAN Id 604, and keeps the VLAN tags on the packets on output.
- P2_V605 receives packets from VLAN Id 605, and keeps the VLAN tags on the packets on output.
- P2_V606 receives packets from VLAN Id 606, and keeps the VLAN tags on the packets on output.
- P2_V607 receives packets from VLAN Id 607, and keeps the VLAN tags on the packets on output.
- P2_Default receives all untagged packets, and removes the VLAN tags on the packets on output.

Note:

These VLAN soft ports may be given child IPv4 soft ports if you wish, thus creating an IP gateway address in each VLAN. Soft ports are hierarchical. For example, if you were to create the SDTN 3 shown in *Illustration 9* on page 53, where you are sharing ports for each user (each test device) "on a stick", each VLAN soft port that you create would then be given a set of IPv4 child soft ports (see *Creating an IPv4 Soft Port* on page 114). Each test user on each VLAN would then be able to create their own Meshed Network (using the Multi-Point Designer) with the IPv4 soft ports that were created within their VLAN and that was assigned to them by the admin user.

Use the following steps to create a soft port with the Soft Port : VLAN function. The steps below use the VLAN IDs, de-tagging configuration, and default interface (for all other untagged traffic) according to the example above in *Illustration 19*. Adjust the steps below according to your VLAN requirements.

1. From the Web Interface, click **Management > Port Manager**.
   A **Port Manager** page appears (see *Illustration 17*) displaying the hardware ports and soft ports (if any exist).
2. Click on the intended parent port (either hardware or soft port) which will accommodate the new soft port you are about to create. In our example (*Illustration 19*), hardware port 2.
   The right hand side of the **Port Manager** page updates with an **Edit Port:** panel, and the selected parent port becomes highlighted.
3. In the **Edit Port:** panel that appears, click the **Add Child To Selected Port** button.
   A **Port Name** dialog box appears.
4. In the **Port Name** dialog box that appears, type the name for the VLAN soft port you are creating, and click **OK**. The name can contain alphanumeric characters and spaces. Choose a name that signifies the type of VLAN soft port you are creating.
   For the example in *Illustration 19*, you would do the following:
   - For the first VLAN soft port, type **`P2_V601`** for the port name.
   - For the second VLAN soft port, type **`P2_V602`** for the port name.
   - For the third VLAN soft port, type **`P2_V603`** for the port name.
   - For the fourth VLAN soft port, type **`P2_V604`** for the port name.
   - For the fifth VLAN soft port, type **`P2_V605`** for the port name.
   - For the sixth VLAN soft port, type **`P2_V606`** for the port name.
   - For the seventh VLAN soft port, type **`P2_V607`** for the port name.
   - For the eighth VLAN soft port, type **`P2_Default`** for the port name.

Note:
You can use any port name you want, but here we use very careful naming of the VLAN soft port so we can see which hardware port it is on (e.g. **P2**) and which VLAN (e.g. **V601**) – this approach is recommended, particularly when the same VLANs are being used on more that one physical port.

Note:
Once created, the port name for a soft port is not editable. Therefore, ensure that you choose a soft port name that is meaningful for you or your end users to identify later on.

! Notice:
When using the NE-ONE with RADIUS authentication, you cannot not use spaces in any of the names of the soft ports that you create. Calnex recommend that you the underscore (_) symbol if required.

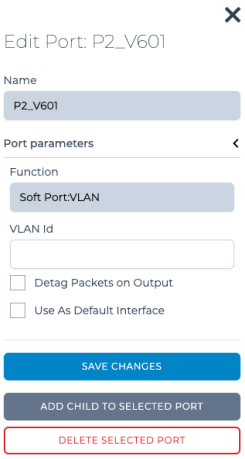
! Notice:
Since the NE-ONE uses the comma (,) symbol as a delimiter within its source code, do not use commas within soft port names.

Note:
The **Port Manager** page represents soft ports by small circles. The port name that you define appears within the small circles that represent the soft ports in the **Port Manager** page. Although the **Port Name** dialog box accepts a long string of alphanumeric characters with spaces, Calnex recommends that you keep the port name to no more than five characters long.

5. In the **Port Type** dialog box that appears, select **Soft port:vlan**, and click **OK**.

Note:
The **Port Type** dialog box only appears once when the first child soft port is being created within the parent port. Once the first child soft port is created within the parent port, all further created child soft ports inherit the port type used by the first child port, and thus you are immediately taken to the **Edit Port:** panel with the **Port Parameters** area.

The **Port Manager** page updates with and automatically selects the newly created VLAN soft port. The **Edit Port:** panel updates with information associated with the newly created VLAN soft port.



6. In the **VLAN Id** field, type an appropriate VLAN Id. This is the 802.1Q VLAN id (or tag) – a number between 1 and 4095.

   For the example in *Illustration 19*, you would do the following:

   - For the first VLAN soft port, type **601** for the VLAN Id.
   - For the second VLAN soft port, type **602** for the VLAN Id.

- For the third VLAN soft port, type **603** for the VLAN Id.
- For the fourth VLAN soft port, type **604** for the VLAN Id.
- For the fifth VLAN soft port, type **605** for the VLAN Id.
- For the sixth VLAN soft port, type **606** for the VLAN Id.
- For the seventh VLAN soft port, type **607** for the VLAN Id.
- For the eighth VLAN soft port, type **650** for the VLAN Id.

  Note: The eighth VLAN soft port has VLAN Id 650, which although it is a valid VLAN Id according to the 802.1Q standard, the packets will never be received with that tag because the VLAN Id of 650 is not configured on the 802.1Q switch. This is useful for creating a default port for all other (unspecified VLANs).

7. Define whether or not the VLAN soft port will remove the VLAN tag from the packets on output.
   - If you want this soft port to remove the VLAN tag from the packets on output, tick the **Detag Packets On Output** check box.
   - If you want this soft port to not remove the VLAN tag from the packets on output, untick the **Detag Packets On Output** check box.

   For the example in *Illustration 19*, you would do the following:
   - For the first VLAN soft port (i.e. P2_V601), tick the **Detag Packets On Output** check box.
   - For the second VLAN soft port (i.e. P2_V602), tick the **Detag Packets On Output** check box.
   - For the third VLAN soft port (i.e. P2_V603), tick the **Detag Packets On Output** check box.
   - For the fourth VLAN soft port (i.e. P2_V604), untick the **Detag Packets On Output** check box.
   - For the fifth VLAN soft port (i.e. P2_V605), untick the **Detag Packets On Output** check box.
   - For the sixth VLAN soft port (i.e. P2_V606), untick the **Detag Packets On Output** check box.
   - For the seventh soft VLAN port (i.e. P2_V607), untick the **Detag Packets On Output** check box.
   - For the eighth VLAN soft port (i.e. P2_Default), tick the **Detag Packets On Output** check box.
8. Define whether or not the VLAN soft port will act as a default interface (i.e. handle all traffic for undefined VLANs including untagged packets):
   - If you want this soft port to handle all traffic for undefined VLANs including untagged packets which arrive at the parent port of this port, tick the **Use As Default Interface** check box.
   - If you do not want this soft port to handle all traffic for undefined VLANs including untagged packets which arrive at the parent port of this port, untick the **Use As Default Interface** check box.

   For the example in *Illustration 19*, you would do the following:
   - For the first VLAN soft port (i.e. P2_V601), untick the **Use As Default Interface** check box.
   - For the second VLAN soft port (i.e. P2_V602), untick the **Use As Default Interface** check box.
   - For the third VLAN soft port (i.e. P2_V603), untick the **Use As Default Interface** check box.
   - For the fourth VLAN soft port (i.e. P2_V604), untick the **Use As Default Interface** check box.
   - For the fifth VLAN soft port (i.e. P2_V605), untick the **Use As Default Interface** check box.
   - For the sixth VLAN soft port (i.e. P2_V606), untick the **Use As Default Interface** check box.
   - For the seventh VLAN soft port (i.e. P2_V607), untick the **Use As Default Interface** check box.
   - For the eighth VLAN soft port (i.e. P2_Default), tick the **Use As Default Interface** check box.

     Note: The eighth VLAN soft port has VLAN Id 650, which although it is a valid VLAN Id according to the 802.1Q standard, the packets will never be received with that tag because the VLAN Id of 650 is not configured on the 802.1Q switch. This is useful for creating a default port for all other (unspecified VLANs) which is why we tick the **Use as Default Interface**.

9. Click **SAVE CHANGES** to save the soft port that you have just finished creating/editing.
10. Click ✕ to close the **Edit Port:** panel for the VLAN soft port that you have just finished creating/editing.

    You are returned to the **Port Manager** page from where you can add/edit additional soft ports.

    The created VLAN soft port will appear in the **Statistics** page (see *Illustration 160* on page 527), with the following three associated object types (see *Illustration 20*):

    Object Type : Port Container, with:
    - Name : <Parent Port name> <--> Soft_Port:VLAN.
    - Object type : Port Container.
    - Description : Sub Port Container for <Parent Port name>.

    Object Type : Link, with:
    - Name : [<Parent Port name> <--> Soft_Port:VLAN] -> [<Parent Port name>].
    - Object type : Link.
    - Description : blank (this is normal)

    Object Type : Soft Port, with:
    - Name : the name you gave to the VLAN soft port (e.g. P2_V601).
    - Object type : Soft Port.
    - Description : the name of the parent port the child VLAN soft port belongs to (e.g. 2 for hardware port 2, Top Level if the VLAN soft port was created at the top level with no parent).

    Note:

    The Port Container and Link object types related the VLAN soft port only get created once (i.e. when the first VLAN soft port is created in the parent port). When additional VLAN soft ports get created within the same parent port, only additional Soft Port object types get created. This is normal behavior, as a parent port only requires one Port Container object and one Link object in order to support multiple VLAN soft ports.

    Illustration 20 shows an example of the eight VLAN soft ports that were created for the example in *Illustration 19* on page 108. For any parent port, the child VLAN soft ports are listed in the order that they were created (i.e. not listed in alpha-numeric order). Therefore, if you want an alpha-numeric ordering of VLAN soft ports within the **Statistics** page, ensure that you create the VLAN soft ports in a chronological order that is the same as the alpha-numeric ordering that you desire.
11. Repeat steps 2 to 10 for each of the VLAN soft ports you want to add using the Soft Port : VLAN function.

    Illustration 21 shows how the Port Manager page appears once all of the VLAN soft ports have been created on hardware port 2 following the example shown in *Illustration 19*.

ILLUSTRATION 20 - EXAMPLE RESULT OF ADDING EIGHT VLAN SOFT PORTS TO HARDWARE PORT 2

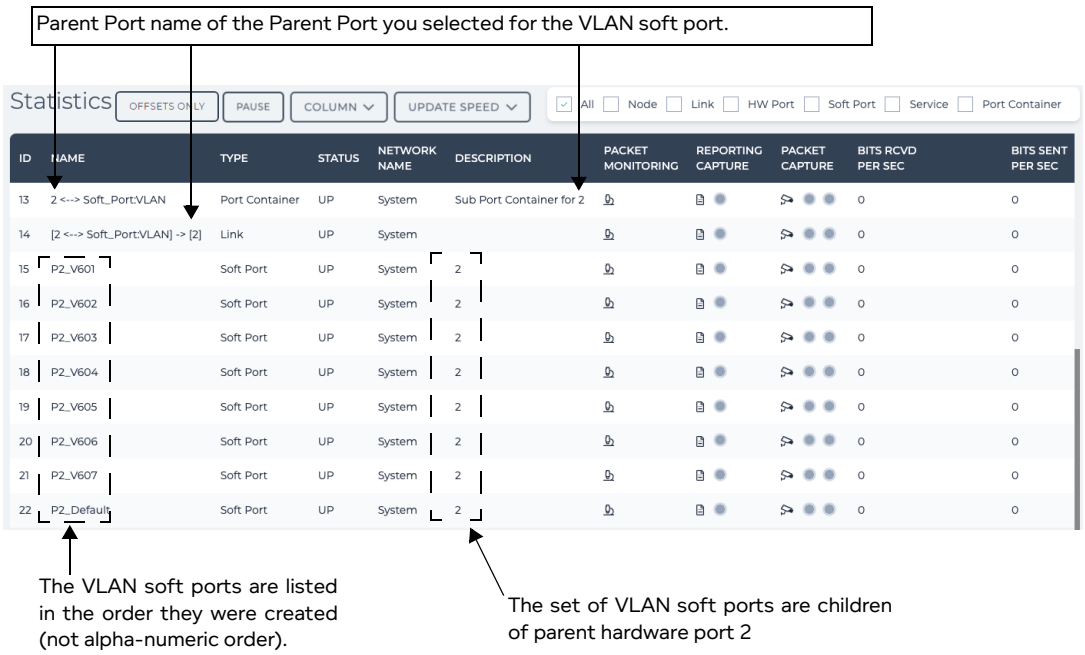
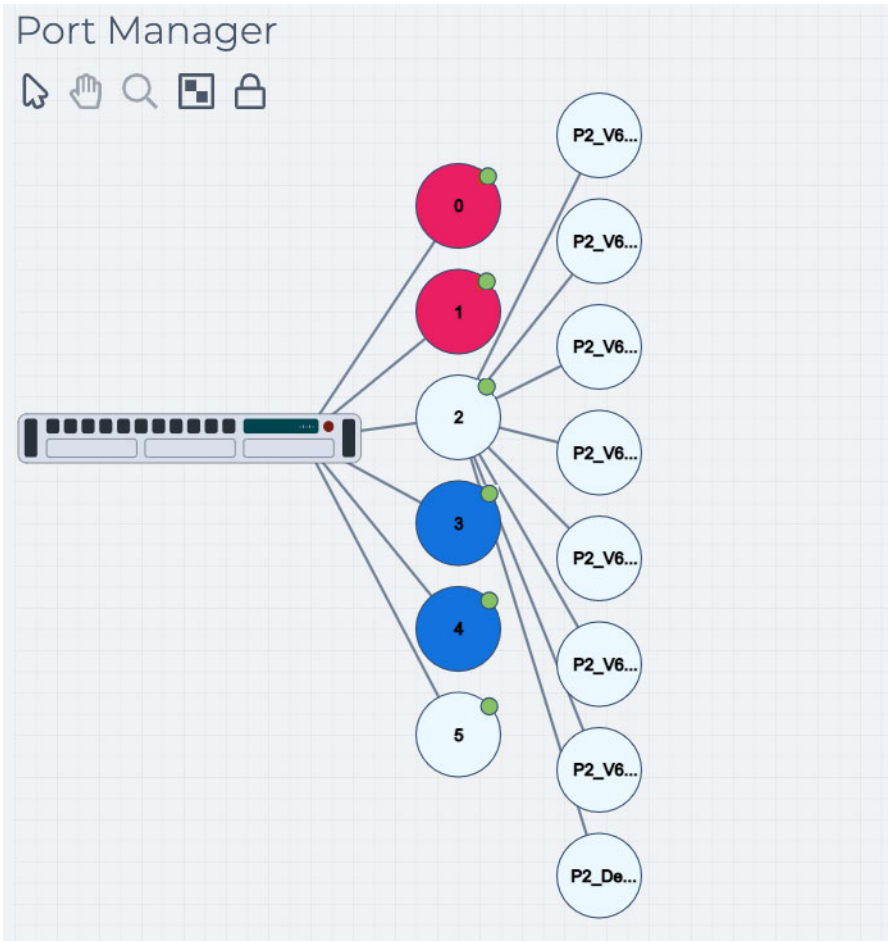


ILLUSTRATION 21 - EXAMPLE PORT MANAGER PAGE WITH VLAN SOFT PORTS ON HARDWARE PORT 2



2-2-2. Creating an IPv4 Soft Port

To set up an IP address on a hardware port or soft port, you use *Soft Port : IPv4* function. Multiple IPv4 soft ports can be defined for a parent port, allowing the parent to appear to have many IPv4 addresses on the same hardware port for routing. This feature is very useful for port sharing in a multi user or multi port environment, and also for having the NE-ONE route either between ports or on a “stick” (out of the same port).

- In some cases you might want to create an IPv4 soft port belonging to a parent VLAN soft port.

  For example, to create a gateway for a VLAN where all the VLAN traffic arrives (see *Illustration 29* with the example used for creating an Expression Filter soft port).

  For example, if you were to create the SDTN 3 shown in *Illustration 9* on page 53, where you are sharing ports for each user (each test device) "on a stick", each VLAN soft port that you created would then be given a set of IPv4 child soft ports. Each test user on each VLAN would then be able to create their own Meshed Network (using the Multi-Point Designer) with the IPv4 soft ports that were created within their VLAN and that was assigned to them by the admin user.
- In other cases you might want to set up an IPv4 soft port on a parent hardware port.
- In cases where you want to create a ping target, you would create an IPv4 soft port at the top level (i.e. no parent port).

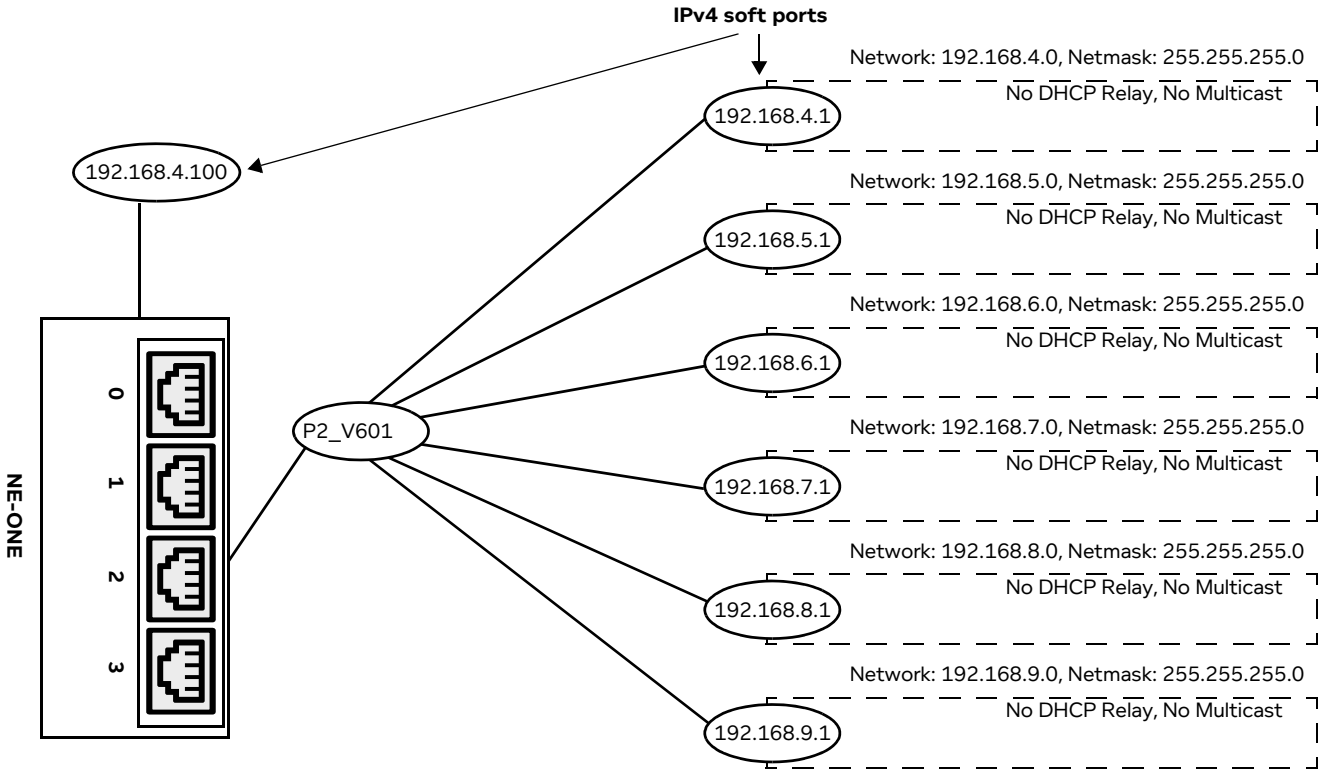
Note:

If you want to create a port with an IPv6 IP address, use the *Soft Port : IP* function instead. For more information, see *Creating an IP Soft Port* on page 122.

The example in *Illustration 22* shows the following:

- Six IPv4 soft ports set up on the parent VLAN soft port that was set up on hardware port 2.
- One IPv4 soft port set up at the top level as a ping target.

ILLUSTRATION 22 - USE OF THE IPV4 FUNCTION TO HAVE MULTIPLE IP ADDRESSES ON THE SAME VLAN SOFT PORT AND A PING TARGET



Once a set of IPv4 soft ports have been set-up on a parent port, if necessary they can be bound together in a fully meshed background service (where any IPv4 soft port can transmit and receive from any other IPv4 soft port), so that packets can pass between them when no Point-to Point or Multi-Point network is running on those IPv4 soft ports. If you want to bind a set of IPv4 soft ports together, you add them and configure them in one of the two following services:

- For a set of two soft ports (used in Point-to-Point networks), use the Service:Background service. For more information, see *Creating a Background Service* on page 190.
- For a set of three or more soft ports (used in Multi-Point networks), use the Service:Background Expression Routed service. For more information, see *Creating a Background Expression Routed service* on page 178.

Use the following steps to create a soft port with the Soft Port : IPv4 function. The steps below use the IP addresses and network configuration according to the example above in *Illustration 22*. Adjust the steps below according to your IPv4 soft port and networking requirements.

Note:

When creating IPv4 soft ports, consider your user's SDTN requirements. For example, in the SDTN 3 shown in *Illustration 9* on page 53, there is a meshed network with five nodes. In this case, creating six IPv4 soft ports and assigning them to a user will be sufficient for that user if they want to create a multi-point network of up to six nodes. Ensure that you set up enough IPv4 soft ports to support each of your users.

1. From the Web Interface, click **Management > Port Manager**.
   A **Port Manager** page appears (see *Illustration 17*) displaying the hardware ports and soft ports (if any exist).
2. Click on the intended parent port (either hardware or soft port) which will accommodate the new IPv4 soft port you are about to create. In our example (*Illustration 22*), hardware port 0.
   The right hand side of the **Port Manager** page updates with an **Edit Port:** panel, and the selected parent port becomes highlighted.
3. In the **Edit Port:** panel that appears, click the **Add Child To Selected Port** button.
   A **Port Name** dialog box that appears.
4. In the **Port Name** dialog box that appears, type the name for the soft port you are creating, and click **OK**. The name can contain alphanumeric characters and spaces. Choose a name that signifies the type of soft port you are creating. It can be anything, though for convenience and easy recognition, many users use the IP address or a variant of the IP address. For example, you could use the IP Address of the IPv4 soft port you are creating (e.g. 192.168.4.1) or the IP address of the IPv4 soft port you are creating, prefixed by the hardware port it belongs to (e.g. P2_192.168.4.1).

Note:

Once created, the port name for a IPv4 soft port is not editable. Therefore, ensure that you choose a IPv4 soft port name that is meaningful for you or your end users to identify later on (e.g. 192.168.4.1 or P2_192.168.4.1).

! Notice:

When using the NE-ONE with RADIUS authentication, you cannot not use spaces in any of the names of the soft ports that you create. Calnex recommend that you the underscore (_) symbol if required.

! Notice:

Since the NE-ONE uses the comma (,) symbol as a delimiter within its source code, do not use commas within soft port names.

For the example in *Illustration 22*, you would do the following:

- For the first IPv4 soft port, type **`192.168.4.1`** for the port name.
- For the second IPv4 soft port, type **`192.168.5.1`** for the port name.
- For the third IPv4 soft port, type **`192.168.6.1`** for the port name.
- For the fourth IPv4 soft port, type **`192.168.7.1`** for the port name.
- For the fifth IPv4 soft port, type **`192.168.8.1`** for the port name.
- For the sixth IPv4 soft port, type **`192.168.9.1`** for the port name.
- For the seventh IPv4 soft port which will be the ping target at the top level, type **`192.168.4.100`** for the port name.

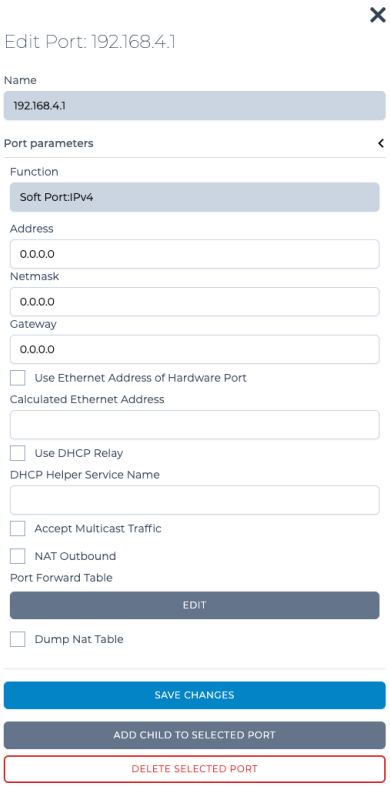
5. In the **Port Type** dialog box that appears, select **Soft port:ipv4**, and click **OK**.

   The **Port Manager** page updates with and automatically selects the newly created IPv4 soft port.

Note:

The **Port Type** dialog box only appears once when the first child soft port is being created within the parent port. Once the first child soft port is created within the parent port, all further created child soft ports inherit the port type used by the first child port, and thus you are immediately taken to the **Edit Port:** panel with the **Port Parameters** area.

The **Edit Port:** panel updates with information associated with the newly created IPv4 soft port.



6. Complete the fields and check boxes as summarized in *Table 18*.

TABLE 18 - IPV4 INTERFACE PARAMETERS FOR THE SOFT PORT : IPV4 FUNCTION

Field / Checkbox	Description
Address	The IP address that you want this soft port to have, in the usual dotted notation e.g. 192.168.4.1. This address can act as the gateway or routing port for other systems using the NE-ONE as their router.

Field / Checkbox	Description
Netmask	This is the IP Network Mask in the usual dotted format e.g. 255.255.255.0 for a class C type address. As usual the (bitwise ANDed) combination of Address and Netmask define the Network e.g. 192.168.4.0 in our example.
Gateway	This is the IP address of the device you will use as your gateway for this traffic (i.e. a router). If the IPv4 soft port you are creating is itself acting as a gateway, set this to 0.0.0.0.
Use Ethernet Address of Hardware Port	This check box determines whether or not the IPv4 soft port will use the MAC address of the parent hardware IPv4 port it belongs to. • If you want the IPv4 soft port to use the MAC address of the parent hardware port it belongs to tick this check box. • If you want the IPv4 soft port to not use the MAC address of the parent hardware port it belongs to untick this check box. • If the IPv4 soft port does not belong to a parent hardware port, but belongs to a parent soft port untick this check box (as it cannot inherit a MAC address from a parent hardware port). • If the IPv4 soft port has been created as a ping target as a top level port, and is not a child belonging to a parent port untick this check box (as it cannot inherit a MAC address from a parent hardware port). If this is unticked, the IPv4 soft port will use 00:11:<IP address in HEX format> for the MAC address. For example, if you specified 192.168.4.1 in the **IP Address** field, the Iv4 soft port would have an auto-generated MAC address of 00:11:C0:A8:04:01. **Note:** Do not tick this if you have two IPv4 soft ports in the same HW port or VLAN soft port. Doing so would result in cloned MAC address issues.
Calculated Ethernet Address	If the IPv4 soft port does not inherit the MAC address of the hardware port (i.e. the **Use Ethernet Address of Hardware Port is** unticked), you must specify a MAC address that you want the IPv4 soft port to have. ICalnex recommends that you use the prefix provided (00:10), and define the MAC address as 00:10:w:x:y:z where w, x, y and z are the hexadecimal representations of the four portions of the IPv4 address. For example, where the IPv4 address is 192.168.10.1 the MAC address would be: 00:01:C0:A8:0A:01 (C0 hex = 192 decimal, A8 hex = 168 decimal etc.).
Use DHCP Relay	Enabling this check box allows DHCP request and response packets to be sent from one IPv4 soft port in the NE-ONE to another IPv4 soft port, even with no network running. In order to do this you must have at least two IPv4 soft ports defined with DHCP relay enabled, and you must also define the DHCP Relay Service according to *Creating Multiple DHCP Helper Services* on page 188.
DHCP Helper Service Name	If you enabled the **Use DHCP Relay** check box, you must specify the name of the DHCP Helper Service that you will have either already created or will create according to *Creating Multiple DHCP Helper Services* on page 188. **Note:** For each IPv4 soft port that you create, you can only specify one DHCP Helper Service.
Accept Multicast Traffic	Enabling this check box will allow multicast traffic to be passed (i.e. sent and received) through this IPv4 soft port.
NAT Outbound	Enabling this check box results in NATing all outbound traffic to the IPv4 soft port's IP Address, and inbound traffic will also be de-NATed.

Field / Checkbox	Description
Port Forward Table EDIT	Clicking this button opens a dialog box, allowing you create port forwarding table. Within this dialog box you can click **ADD** to open an additional dialog box which then lets you specify a new row in the port forwarding table, with the following values: External Port Internal IP Address Internal Port If you need to define a port forwarding table, click **ADD**, and define the External Port, Internal IP Address, and Internal Port for all the port forwarding rows that you require.
Dump NAT Table	Enabling this dumps the NAT table data in the `ippe.log` file. This is a test feature, which only works in Port Update mode (i.e. when editing an IPv4 soft port, not adding an IPv4 soft port). **Note:** enabling this can result in having the NAT table reach over 60,000 entries.

For the example in *Illustration 22*, you define each of the IPv4 parameters on each of the sevent IPv4 soft ports, as summarized in *Table 19*.

TABLE 19 - IPV4 INTERFACE PARAMETERS FOR THE EXAMPLE IN ILLUSTRATION 22

Field / Checkbox	Setting for example in **Illustration 22**
Address	First IPv4 soft port : type **`192.168.4.1`** Second IPv4 soft port : type **`192.168.5.1`** Third IPv4 soft port : type **`192.168.6.1`** Fourth IPv4 soft port : type **`192.168.7.1`** Fifth IPv4 soft port : type **`192.168.8.1`** Sixth IPv4 soft port : type **`192.168.9.1`** Seventh IPv4 soft port : type **`192.168.4.100`**
Netmask	First IPv4 soft port : type **`255.255.255.0`** (e.g. 192.168.4.0 network) Second IPv4 soft port : type **`255.255.255.0`** (e.g. 192.168.5.0 network) Third IPv4 soft port : type **`255.255.255.0`** (e.g. 192.168.6.0 network) Fourth IPv4 soft port : type **`255.255.255.0`** (e.g. 192.168.7.0 network) Fifth IPv4 soft port : type **`255.255.255.0`** (e.g. 192.168.8.0 network) Sixth IPv4 soft port : type **`255.255.255.0`** (e.g. 192.168.9.0 network) Seventh IPv4 soft port : type **`255.255.255.0`** (e.g. 192.168.4.0 network)
Gateway	First IPv4 soft port : type **`0.0.0.0`** (as it is itself acting as a gateway) Second IPv4 soft port : type **`0.0.0.0`** (as it is itself acting as a gateway) Third IPv4 soft port : type **`0.0.0.0`** (as it is itself acting as a gateway) Fourth IPv4 soft port : type **`0.0.0.0`** (as it is itself acting as a gateway) Fifth IPv4 soft port : type **`0.0.0.0`** (as it is itself acting as a gateway) Sixth IPv4 soft port : type **`0.0.0.0`** (as it is itself acting as a gateway) Seventh IPv4 soft port : type **`0.0.0.0`** (as it is itself acting as a gateway)
Use Ethernet Address of Hardware Port	For all the IPv4 soft ports in our example, leave this check box unchecked (as we do not want MAC address cloning issues). • The first IPv4 soft port is auto-assigned MAC address of 00:11:C0:A8:04:01. • The second IPv4 soft port is auto-assigned MAC address of 00:11:C0:A8:05:01. • The third IPv4 soft port is auto-assigned MAC address of 00:11:C0:A8:06:01. • The fourth IPv4 soft port is auto-assigned MAC address of 00:11:C0:A8:07:01. • The fifth IPv4 soft port is auto-assigned MAC address of 00:11:C0:A8:08:01. • The sixth IPv4 soft port is auto-assigned MAC address of 00:11:C0:A8:09:01. • The seventh IPv4 soft port is auto-assigned MAC address of 00:11:C0:A8:10:01.
Use DHCP Relay	For all the IPv4 soft ports in our example, leave this check box unchecked (as no DHCP relay service used).

Field / Checkbox	Setting for example in **Illustration 22**
Accept Multicast Traffic	For all the IPv4 soft ports in our example, leave this check box unchecked (no multicast traffic passed through the soft port).
NAT Outbound	For all the IPv4 soft ports in our example, leave this check box unchecked (no NATing is required).
Port Forward Table EDIT	For all the IPv4 soft ports in our example, do not create a port forward table (no port forwarding is required).
Dump NAT Table	For all the IPv4 soft ports in our example, leave this check box unchecked (no dumping of the NAT table is required).

7. Click **SAVE CHANGES** to save the IPv4 soft port that you have just finished creating/editing.
8. Click ✕ to close the **Edit Port:** panel for the IPv4 soft port that you have just finished creating/editing.

   You are returned to the **Port Manager** page from where you can add/edit additional soft ports.

   The IPv4 soft port is now ping-able (from systems on its subnet, or reachable via the gateway you defined when defining the IPv4 soft port). The IPv4 soft port is also ping-able on systems connected to other ports in the NE-ONE if a Point-to-Point or Multi-Point network has been started, and there is a path defined through to the IPv4 soft port.

   The IPv4 soft port will respond to ARP requests even if a network is not running. It also maintains an ARP cache for addresses that it sends packets to. The cache persists until the NE-ONE is rebooted or the IPv4 soft port is deleted.

   The created IPv4 soft port will appear in the **Statistics** page (see *Illustration 160* on page 527), with the following three associated object types (see *Illustration 23*):

   Object Type : Port Container, with:
   - Name : <Parent Port name> <--> Soft_Port:IPv4.
   - Object type : Port Container.
   - Description : Sub Port Container for <Parent Port name>.

   Object Type : Link, with:
   - Name : [<Parent Port name> <--> Soft_Port:IPv4] -> [<Parent Port name>].
   - Object type : Link.
   - Description : blank (this is normal)

   Object Type : Soft Port, with:
   - Name : the name you gave to the IPv4 soft port (e.g. 192.168.4.1).
   - Object type : Soft Port.
   - Description : the name of the parent port the child IPv4 soft port belongs to (e.g. 0 for hardware port 0, Top Level if the IPv4 soft port was created at the top level with no parent, or P2_V601 if the IPv4 soft port was created within a VLAN soft port called P2_V601).

   Note:

   The Port Container and Link object types related the IPv4 soft port only get created once (i.e. when the first IPv4 soft port is created in the parent port). When additional IPv4 soft ports get created within the same parent port, only additional Soft Port object types get created. This is normal behavior, as a parent port only requires one Port Container object and one Link object in order to support multiple IPv4 soft ports.

   Illustration 23 shows an example of the seven IPv4 soft ports that were created for the example in *Illustration 22* on page 114. Notice how the IPv4 soft port called 192.168.9.1 does not appear at the

bottom of the set of six IPv4 soft ports located within the P2_V601 soft port. This is because for any parent port, the child IPv4 soft ports are listed in the order that they were created (i.e. not listed in alpha-numeric order). Therefore, if you want an alpha-numeric ordering of IPv4 soft ports within the **Statistics** page, ensure that you create the IPv4 soft ports in a chronological order that is the same as the alpha-numeric ordering that you desire.

9. Repeat steps 2 to 8 for each of the IPv4 soft ports you want to add using the Soft Port : IPv4 function.

   Illustration 24 shows how the **Port Manager** page appears once all of the six IPv4 soft ports have been created on the VLAN soft port P2_V601, and the seventh IPv4 soft ports has been created at the top level as a ping target, by following the example shown in *Illustration 23*.

ILLUSTRATION 23 - EXAMPLE RESULT OF ADDING SIX IPV4 SOFT PORTS TO A VLAN SOFT PORT ON HARDWARE PORT 2 AND ONE IPV4 SOFT PORT AS A PING TARGET AT THE TOP LEVEL

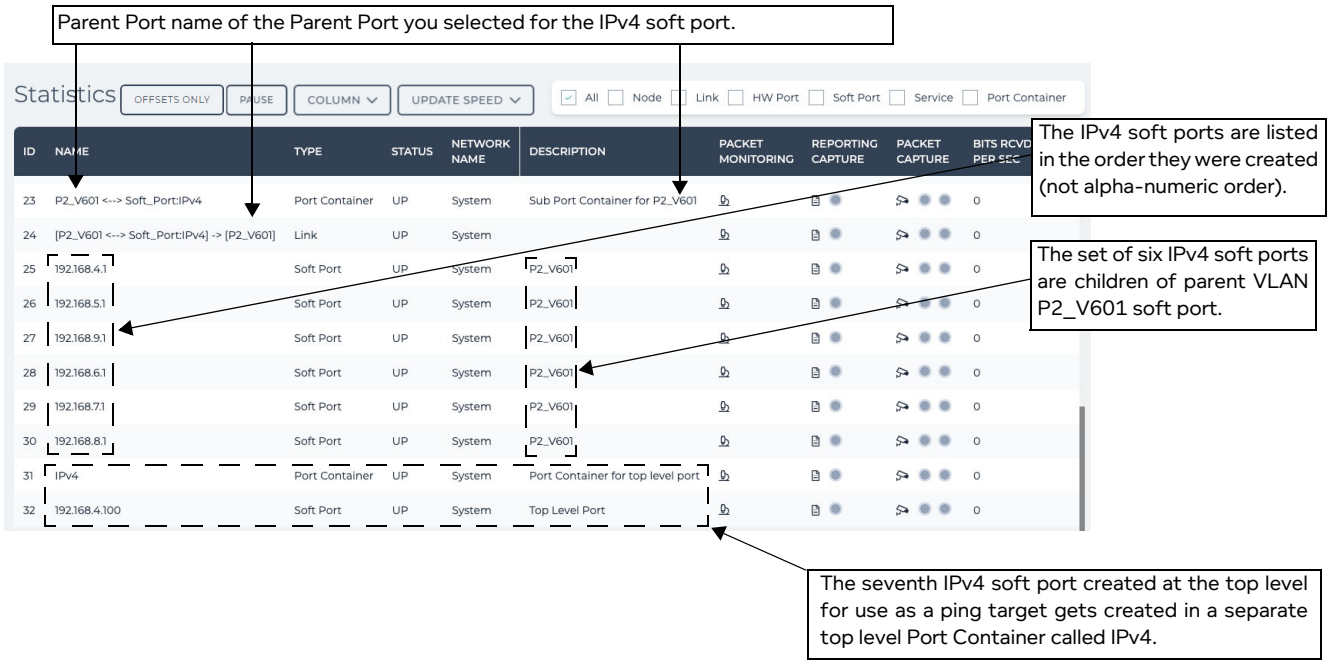
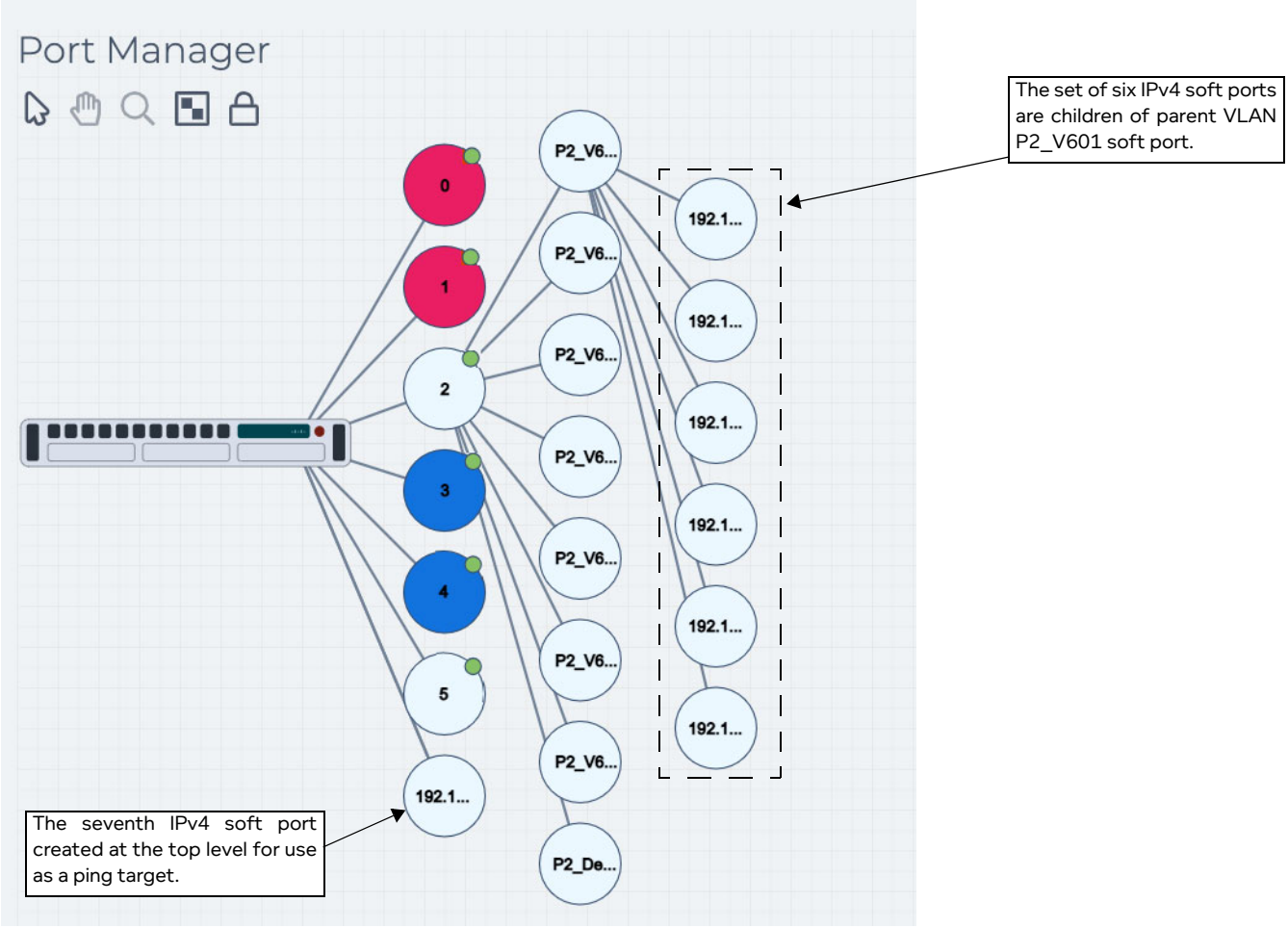


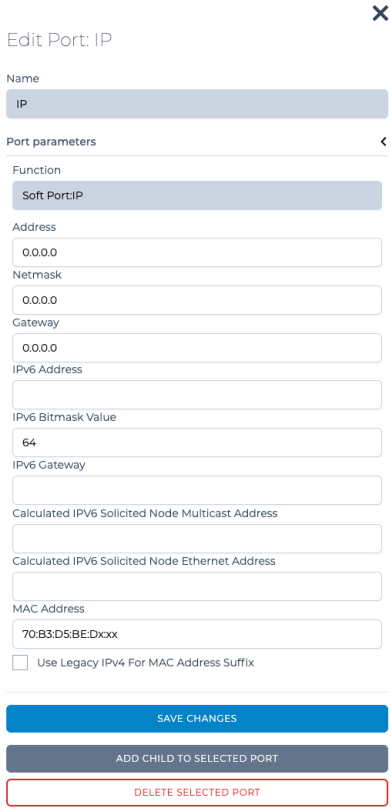
ILLUSTRATION 24 - EXAMPLE PORT MANAGER PAGE WITH SEVEN IPV4 SOFT PORTS



2-2-3. Creating an IP Soft Port

The purpose of the IP soft port is to allow a port to have both an IPv4 and IPv6 address, as well as providing more control over the MAC address. The principles are the same as creating an IPv4 soft port. So for brevity, and an example procedure is not given. *Illustration 25* and *Table 20* describes the parameters that appear in the **Edit Port:** panel when creating/editing an IP soft port.

ILLUSTRATION 25 - EDIT PORT PANEL FOR THE IP SOFT PORT FUNCTION



Note:

The port name define for an IP soft port can be anything, though for convenience and easy recognition, many users use the IP address or a variant of the IP address.

! Notice:

When using the NE-ONE with RADIUS authentication, you cannot not use spaces in any of the names of the soft ports that you create. Calnex recommend that you the underscore (_) symbol if required.

! Notice:

Since the NE-ONE uses the comma (,) symbol as a delimiter within its source code, do not use commas within soft port names.

TABLE 20 - PARAMETERS FOR THE IP SOFT PORT FUNCTION

Field / Checkbox	Description
Address	The IPv4 address that you want this IP soft port to have, in the usual dotted notation e.g. 192.168.10.1. This address can act as the gateway or routing port for other systems using the NE-ONE as their router.

Field / Checkbox	Description
Netmask	This is the IPv4 Network Mask in the usual dotted format e.g. 255.255.255.0 for a class C type address. As usual the (bitwise ANDed) combination of Address and Netmask define the Network e.g. 192.168.10.0.
Gateway	The IPv4 address of a router in that network which will act as a gateway between this port and other networks. Do not confuse this with the Address of the soft port itself.
IPv6 Address	This is the IPv6 address of this IP soft port in the usual IPv6 notation (e.g. 4037::01:800:200E:8C6C, FE80::4A5D:60FF:FEE8:658F, etc.).
IPv6 Bitmask Value	This is the number of bits in the IPv6 address that represent the network – the default value is 64.
IPv6 Gateway	The IPv6 address of a router in that network which will act as a gateway between this port and other networks. Do not confuse this with the Address of the soft port itself.
Calculated IPv6 Solicited Node Multicast Address	This is the calculated solicited node multicast address based on the IPv6 Address that you specified in the IPv6 Address field above. The solicited node multicast address is computed as a function of a node's unicast and anycast addresses. A solicited node multicast address is formed by taking the low-order 24 bits of an address (unicast or anycast) and appending those bits to the prefix FF02:0:0:0:0:1:FF00::/104 resulting in a multicast address in the range FF02:0:0:0:0:1:FF00:0000 to FF02:0:0:0:0:1:FFFF:FFFF For example, the solicited node multicast address corresponding to the IPv6 address 4037::01:800:200E:8C6C is FF02::1:FF0E:8C6C.
Calculated IPv6 Solicited Node Ethernet Address	This is the calculated solicited node Ethernet address based on the IPv6 Address that you specified in the **IPv6 Address** field above. Ethernet has "multicast" MAC addresses. Any MAC address with the "group" bit set is technically a multicast address; IPv6 uses the prefix 33:33:*, while IPv4 uses 01:00:5E:*. For IPv6 multicast addresses, the last 32 bits of the IPv6 address are ORed with 33:33:00:00:00:00. For example: The "all nodes" address FF02::1 is converted to 33:33:00:00:00:01. Neighbor solicitations for an example IPv6 address FE80::4A5D:60FF:FEE8:658F are sent to the corresponding Solicited-Node multicast address FF02::1:FFE8:658F, which is converted to Ethernet address 33:33:FF:E8:65:8F.
MAC Address	This is the MAC address you want the soft port to have. Calnex recommends that you use the prefix provided, as this is registered: 70:B3:D5:BE:Dx:xx – replacing the x:xx values with your choice.
Use Legacy IPv4 For MAC Address Suffix	If this is check box is checked (ticked) then the pseudo MAC address is implicitly defined as 00:10:w:x:y:z where w, x, y and z are the hexadecimal representations of the four portions of the IPv4 address. For example, where the IPv4 address is 192.168.10.1 the MAC address would be: 00:01:C0:A8:0A:01 (C0 hex = 192 decimal, A8 hex = 168 decimal etc.). This ability to easily see MAC addresses is very useful in tracking packets in utilities like tcpdump and Wireshark. If this is check box is unchecked (unticked) then the value specified in the MAC address field (described above) is used.

2-2-4. Creating a Filter Soft Port

The Soft Port : Filter function lets you create soft ports to select traffic from the parent port by:

- Source IP Address and/or Destination IP Address
- Source Port and/or Destination Port (you cannot distinguish between UDP and TCP - if you want explicit filtering on UDP and TCP ports, use the Expression Filter Port instead (see *Creating an Expression Filter Soft Port* on page 132))
- VLAN Id

Thus the port you define has just some of the data that came into the parent port.

Multiple such Filter Ports can be defined for a parent port letting you carve up its traffic – effectively "pretending" that the traffic originated at its own port. This feature is very useful for port sharing in a multi user environment.

Note:
The Soft Port Filter function is useful for setting up arrays of filters (i.e. multiple filter ranges) within one soft port.

Note:
The Soft Port Filter function does not let you filter using complex expressions. If you require filtering using complex expressions, use the more advanced Expression Filter Soft Port (see *Creating an Expression Filter Soft Port* on page 132).

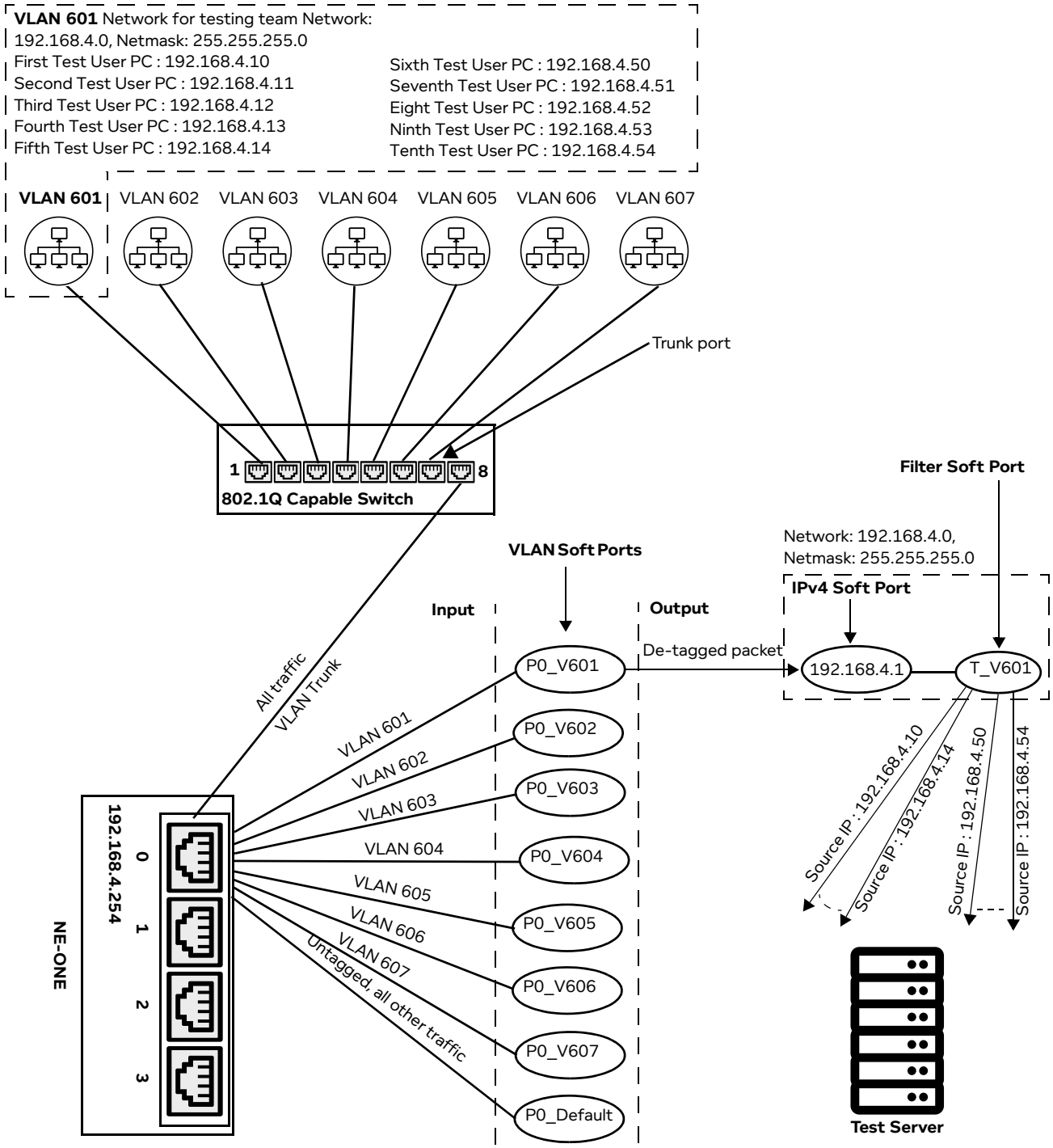
This section describes an example of using the Soft Port : Filter function to create a soft port on a parent port to carve up the parents port's traffic based on the Source IP address.

In the example below in *Illustration 26*, the a Filter soft port is set up on a parent IPv4 soft port (192.168.4.1), which is a child of a VLAN soft port (VLAN_601), which is a child belonging to hardware port 0.

In this example, the Filter is used to filter on IP address ranges from different testing team users from within VLAN 601, with the naming convention T_V<VLAN ID> (where T represents Test user). Within the Filter, you can create an array of filter ranges, an in our example, the following two rows are set up for the Source IP address filter array:

- IP address range 192.168.4.10 to 192.168.4.14 will filter for all traffic coming from testers whose client PCs have source IP address 192.168.4.10, 192.168.4.11, 192.168.4.12, 192.168.4.13, 192.168.4.14 from VLAN 601.
- IP address range 192.168.4.50 to 192.168.4.54 will filter for all traffic coming from testers whose client PCs have source IP address 192.168.4.50, 192.168.4.51, 192.168.4.52, 192.168.4.53, 192.168.4.54 from VLAN 601.

ILLUSTRATION 26 - USE OF THE FILTER SOFT PORT FUNCTION TO SELECT TRAFFIC FOR DIFFERENT TESTERS BASED ON THEIR SOURCE IP ADDRESS WITHIN A VLAN



Use the following steps to create a soft port with the Soft Port : Filter function. The steps below use the VLAN ID, IP addresses and network configuration according to the example above in *Illustration 26*. Adjust the steps below according to your networking and traffic filtering requirements.

1. From the Web Interface, click **Management > Port Manager**.

   A **Port Manager** page appears (see *Illustration 17*) displaying the hardware ports and soft ports (if any exist).

2. Click on the intended parent port (either hardware or soft port) which will accommodate the new soft port you are about to create. In our example (*Illustration 26*), hardware port 0.

   In our example, you would select the IPv4 soft port **192.168.4.1** that is a child of VLAN soft port **P_V601**. Both the IPv4 soft port and VLAN soft port would have already been created according to *Creating a VLAN Soft Port* on page 107 and *Creating an IPv4 Soft Port* on page 114, respectively.

   The right hand side of the **Port Manager** page updates with an **Edit Port:** panel, and the selected parent port becomes highlighted.
3. In the **Edit Port:** panel that appears, click the **Add Child To Selected Port** button.

   A **Port Name** dialog box appears.
4. In the **Port Name** dialog box that appears, type the name for the soft port you are creating, and click **OK**. The name can contain alphanumeric characters and spaces. Choose a name that signifies the type of soft port you are creating.

   For the example in *Illustration 26*, you would type **`T_V601`** for the port name.

Note:

Once created, the port name for a soft port is not editable. Therefore, ensure that you choose a soft port name that is meaningful for you or your end users to identify later on.

! Notice:

When using the NE-ONE with RADIUS authentication, you cannot not use spaces in any of the names of the soft ports that you create. Calnex recommend that you the underscore (_) symbol if required.

! Notice:

Since the NE-ONE uses the comma (,) symbol as a delimiter within its source code, do not use commas within soft port names.

Note:

The **Port Manager** page represents soft ports by small circles. The port name that you define appears within the small circles that represent the soft ports in the **Port Manager** page. Although the **Port Name** dialog box accepts a long string of alphanumeric characters with spaces, Calnex recommends that you keep the port name to no more than five characters long.

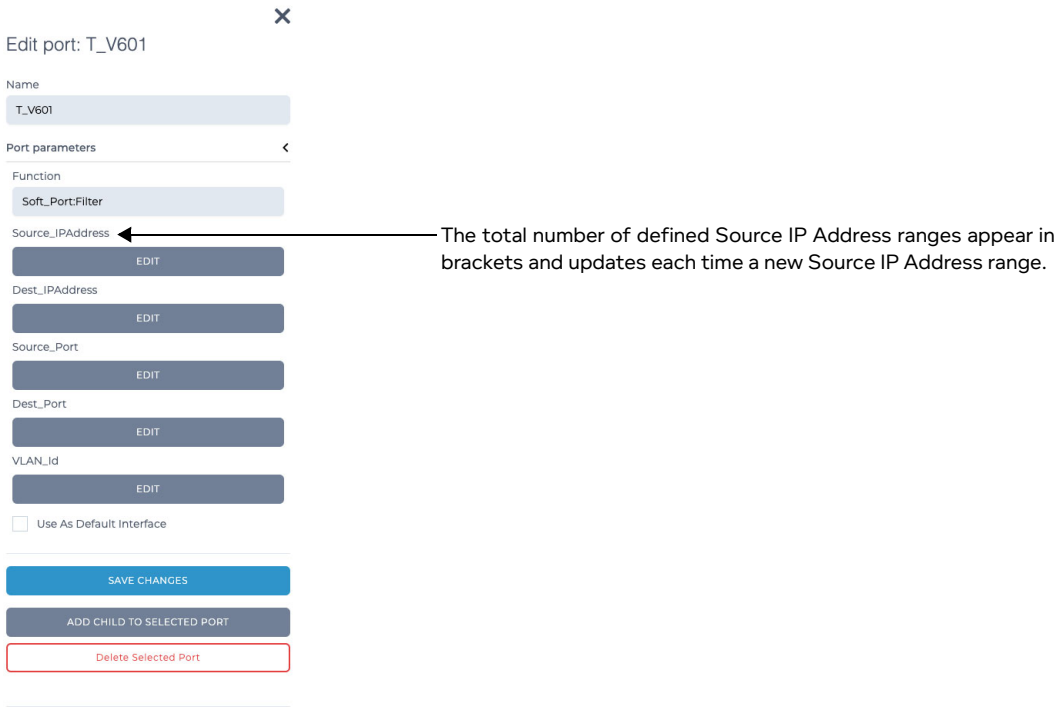
5. In the **Port Type** dialog box that appears, select **Soft port:filter**, and click **OK**.

Note:

The **Port Type** dialog box only appears once when the first child soft port is being created within the parent port. Once the first child soft port is created within the parent port, all further created child soft ports inherit the port type used by the first child port, and thus you are immediately taken to the **Edit Port:** panel with the **Port Parameters** area.

The **Port Manager** page updates with and automatically selects the newly created soft port. The

Edit Port: panel updates with information associated with the newly created soft port.



6. Click the **EDIT** button associated with the type of filter you are creating (i.e. Source IP address, Destination IP address, Source Port, Destination Port, or VLAN ID).

   In our example, we are setting up filters on a range of Source IP addresses, so click the **Source_IPAddress EDIT** button.

   An empty **Source IPAddress** dialog box appears, letting you define the range of Source IP addresses.

7. From the **Source IPAddress** dialog box that appears, do the following:
   a. Click **ADD ROW**.

      A new **Source_IPAddress (0)** row appears in the **Source IPAddress** dialog box with **Minimum** and **Maximum** fields.

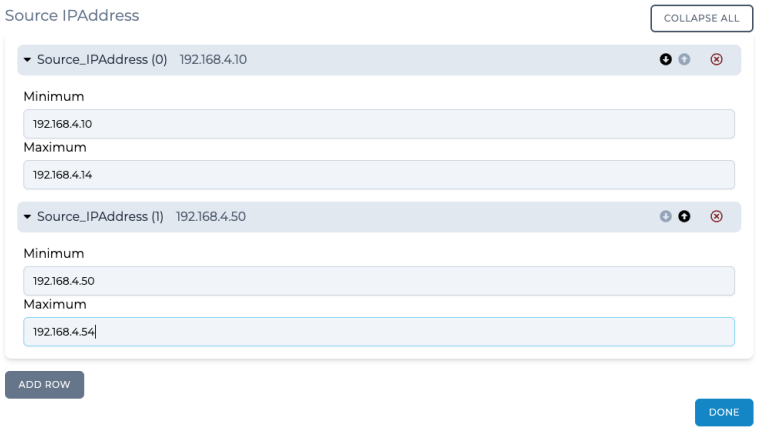
   b. In the new **Source_IPAddress (0)** row that appears, type **`192.168.4.10`** from the **Minimum**

field and type **`192.168.4.14`** from the **Maximum** field.

c. Click **ADD ROW**.

A new **Source_IPAddress (1)** row appears in the **Source IPAddress** dialog box with **Minimum** and **Maximum** fields.

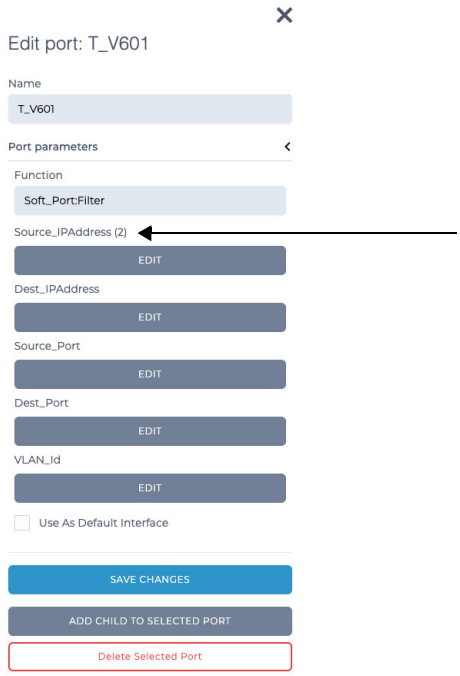
d. In the new **Source_IPAddress (1)** row that appears, type **`192.168.4.50`** from the **Minimum** field and type **`192.168.4.54`** from the **Maximum** field.



At this stage, all the both Source IP ranges (192.168.4.10 to 192.168.4.14 and 192.168.4.50 to 192.168.4.54) have been added to the Soft Port : Filter function.

e. Click **DONE** to return to **Edit Port:** panel.

The **Edit Port:** panel appears, and now contains the two Source IP Address ranges that you added.



The total number of defined Source IP Address ranges appear in brackets and updates each time a new Source IP Address range. The value two appears, summarizing the two Source IP Address ranges you added.

8. Define whether or not the Filter soft port will act as a default interface (i.e. handle all traffic for undefined packets):
   - If you want this Filter soft port to handle all traffic for undefined packets which arrive at the parent port of this port, tick the **Use As Default Interface** check box.
   - If you do not want this Filter soft port to handle all traffic for undefined packets which arrive at the parent port of this port, untick the **Use As Default Interface** check box.

   For the example in *Illustration 26*, you would untick the **Use As Default Interface** check box.
9. Click **SAVE CHANGES** to save the Filter soft port that you have just finished creating/editing.
10. Click ✕ to close the **Edit Port:** panel for the Filter soft port that you have just finished creating/editing.

    You are returned to the **Port Manager** page from where you can add/edit additional Filter soft ports.

    The Filter soft port will now perform filtering according to the criteria that you defined.

    The created Filter soft port will appear in the **Statistics** page (see *Illustration 160* on page 527), with the following three associated object types (see *Illustration 27*):

    Object Type : Port Container, with:
    - Name : Filter.
    - Object type : Port Container.
    - Description : Sub Port Container for <Parent Port name>.

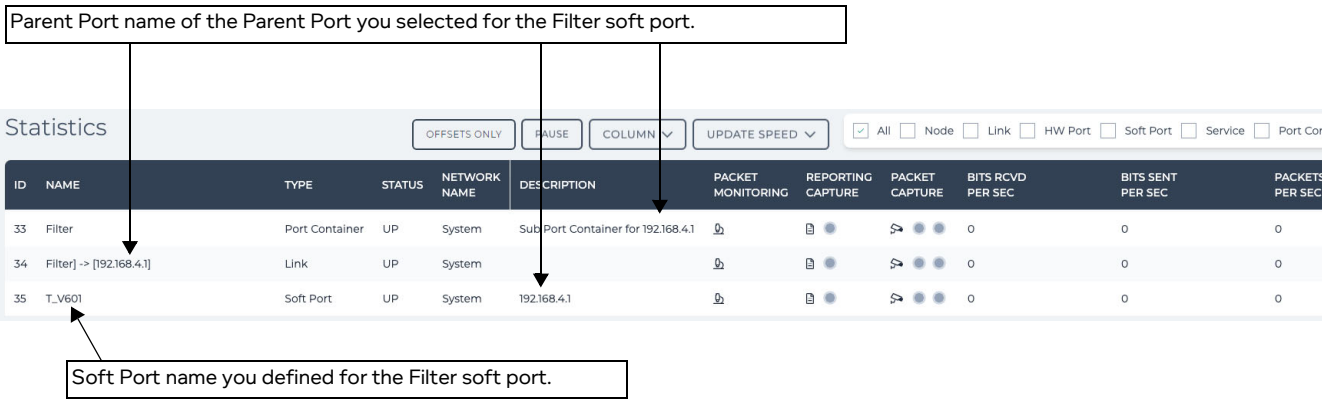
    Object Type : Link, with:
    - Name : [Filter] -> [<Parent Port name>].
    - Object type : Link.
    - Description : blank (this is normal)

    Object Type : Soft Port, with:
    - Name : the name you gave to the Filter soft port (e.g. T_V601).
    - Object type : Soft Port.

- Description : the name of the parent port the child Filter soft port belongs to (e.g. 0 for hardware port 0).

Illustration 27 shows an example of the three associated Filter soft port objects that are created when creating one Filter soft port for the example in *Illustration 26* on page 125.

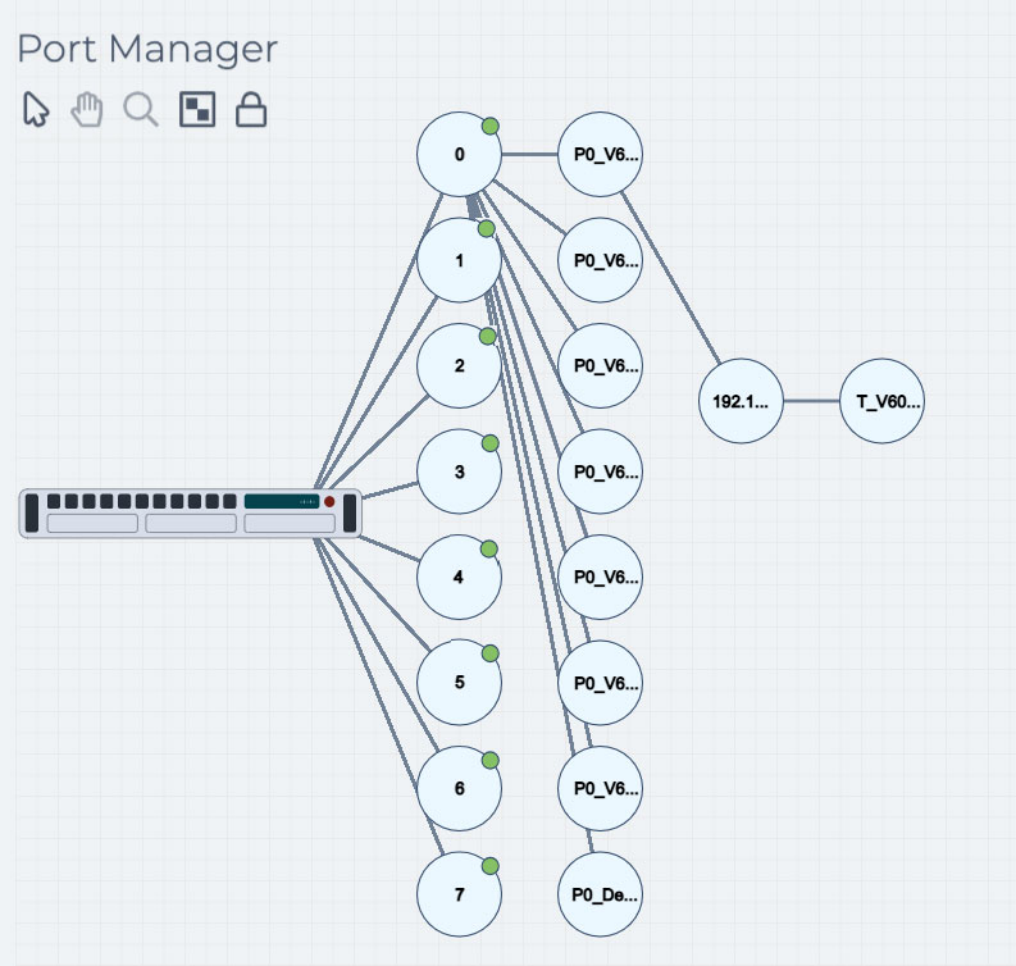
ILLUSTRATION 27 - EXAMPLE RESULT OF ADDING A FILTER SOFT PORT TO AN IPV4 SOFT PORT CALLED 192.168.4.1



11. Repeat steps 2 to 8 for each of the Filter soft ports you want to add using the Soft Port : Filter function.

Illustration 28 shows how the **Port Manager** page appears once the Filter soft port has been created following the example shown in *Illustration 26*.

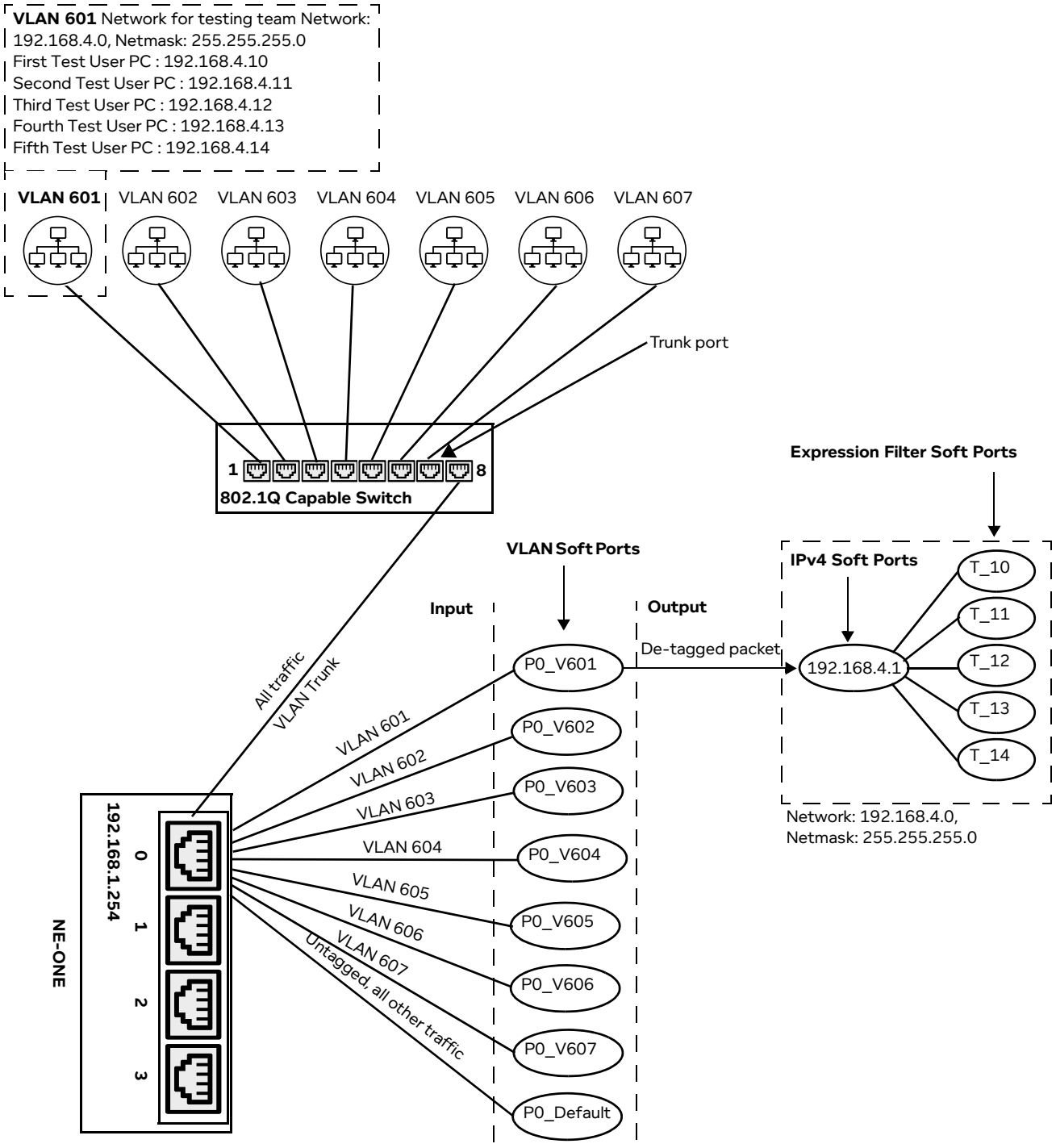
ILLUSTRATION 28 - EXAMPLE PORT MANAGER PAGE WITH A FILTER SOFT PORT



2-2-5. Creating an Expression Filter Soft Port

This function lets you select traffic from the parent port by using the "Wireshark like" expression syntax. This allows many more possibilities than the *Soft Port : Filter* soft port function on which it is based - other than this its function is similar. Multiple Expression Filter Ports can be defined for a parent port letting you carve up its traffic – effectively "pretending" that the traffic originated at its own port. This feature is very useful for port sharing in a multi user environment.

ILLUSTRATION 29 - USE OF THE EXPRESSION FILTER SOFT PORT FUNCTION TO SELECT TRAFFIC FOR DIFFERENT TESTERS BASED ON THEIR IP ADDRESS WITHIN A VLAN



In the example above in *Illustration 29*, the following five Expression Filter soft ports are set up on a parent IPv4 soft port (192.168.4.1), which is a child of a VLAN soft port (VLAN_601), which is a child belonging to hardware port 0. In this example, the Expression Filters are used to filter on IP addresses from different testing team users from within VLAN 601, with the naming convention T_<last decimal digit of the IP address of the Test user's PC> (where T represents Test user):

- T_10 will filter for all traffic coming from a tester whose client PC has source IP address 192.168.4.10 from VLAN 601
- T_11 will filter for all traffic coming from a tester whose client PC has source IP address 192.168.4.11 from VLAN 601
- T_11 will filter for all traffic coming from a tester whose client PC has source IP address 192.168.4.12 from VLAN 601
- T_11 will filter for all traffic coming from a tester whose client PC has source IP address 192.168.4.13 from VLAN 601
- T_11 will filter for all traffic coming from a tester whose client PC has source IP address 192.168.4.14 from VLAN 601
- T_11 will filter for all traffic coming from a tester whose client PC has source IP address 192.168.4.15 from VLAN 601

Use the following steps to create a soft port with the Soft Port : Expression Filter function. The steps below use the VLAN ID, IP addresses and network configuration according to the example above in *Illustration 29*. Adjust the steps below according to your networking and traffic filtering requirements.

1. From the Web Interface, click **Management > Port Manager**.

   A **Port Manager** page appears (see *Illustration 17*) displaying the hardware ports and soft ports (if any exist).
2. Click on the intended parent port (either hardware or soft port) which will accommodate the new soft port you are about to create.

   In our example, you would select the IPv4 soft port **192.168.4.1** that is a child of VLAN soft port **P_V601**. Both the IPv4 soft port and VLAN soft port would have already been created according to *Creating a VLAN Soft Port* on page 107 and *Creating an IPv4 Soft Port* on page 114, respectively.

   The right hand side of the **Port Manager** page updates with an **Edit Port:** panel, and the selected parent port becomes highlighted.
3. In the **Edit Port:** panel that appears, click the **Add Child To Selected Port** button.

   A **Port Name** dialog box appears.
4. In the **Port Name** dialog box that appears, type the name for the soft port you are creating, and click **OK**. The name can contain alphanumeric characters and spaces. Choose a name that signifies the type of soft port you are creating.

   For the example in *Illustration 29*, you would do the following:
   - For the first Expression Filter port, you would type **T_10** for the port name.
   - For the second Expression Filter port, you would type **T_11** for the port name.
   - For the third Expression Filter port, you would type **T_12** for the port name.
   - For the fourth Expression Filter port, you would type **T_13** for the port name.
   - For the fifth Expression Filter port, you would type **T_14** for the port name.

Note:

Once created, the port name for a soft port is not editable. Therefore, ensure that you choose a soft port name that is meaningful for you or your end users to identify later on.

Notice:

When using the NE-ONE with RADIUS authentication, you cannot not use spaces in any of the names of the soft ports that you create. Calnex recommend that you the underscore (_) symbol if required.

Notice:

Since the NE-ONE uses the comma (,) symbol as a delimiter within its source code, do not use commas within soft port names.

Note:

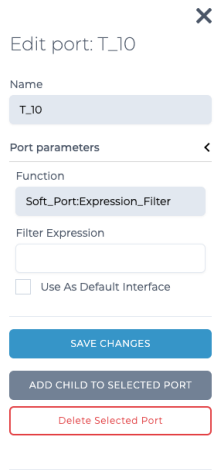
The **Port Manager** page represents soft ports by small circles. The port name that you define appears within the small circles that represent the soft ports in the **Port Manager** page. Although the **Port Name** dialog box accepts a long string of alphanumeric characters with spaces, Calnex recommends that you keep the port name to no more than five characters long.

5. In the **Port Type** dialog box that appears, select **Soft port:expression filter**, and click **OK**.

Note:

The **Port Type** dialog box only appears once when the first child soft port is being created within the parent port. Once the first child soft port is created within the parent port, all further created child soft ports inherit the port type used by the first child port, and thus you are immediately taken to the **Edit Port:** panel with the **Port Parameters** area.

The **Port Manager** page updates with and automatically selects the newly created soft port. The **Edit Port:** panel updates with information associated with the newly created soft port.



6. In the **Filter Expression** field, type an appropriate filter expression (in Wireshark syntax). For more information on filter expressions, see *Appendix 1*, *Specifying Expressions* on page 731.

   For the example in *Illustration 29*, you would do the following:

   - For the first Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.10, you would type **`ipv4.src = 192.168.4.10`** for the filter expression.
   - For the second Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.11, you would type **`ipv4.src = 192.168.4.11`** for the filter expression.
   - For the third Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.12, you would type **`ipv4.src = 192.168.4.12`** for the filter expression.
   - For the fourth Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.13, you would type **`ipv4.src = 192.168.4.13`** for the filter expression.
   - For the fifth Expression Filter port, which is for all traffic coming from a Tester's PC with source IP

address 192.168.4.14, you would type **`ipv4.src = 192.168.4.14`** for the filter expression.

7. Define whether or not the Expression Filter soft port will act as a default interface (i.e. handle all traffic for undefined packets):
   - If you want this Expression Filter soft port to handle all traffic for undefined packets which arrive at the parent port of this port, tick the **Use As Default Interface** check box.
   - If you do not want this Expression Filter soft port to handle all traffic for undefined packets which arrive at the parent port of this port, untick the **Use As Default Interface** check box.

   For the example in *Illustration 29*, you would do the following:
   - For the first Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.10, you would untick the **Use As Default Interface** check box.
   - For the second Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.11, you would untick the **Use As Default Interface** check box.
   - For the third Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.12, you would untick the **Use As Default Interface** check box.
   - For the fourth Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.13, you would untick the **Use As Default Interface** check box.
   - For the fifth Expression Filter port, which is for all traffic coming from a Tester's PC with source IP address 192.168.4.14, you would untick the **Use As Default Interface** check box.
8. Click **SAVE CHANGES** to save the Expression Filter soft port that you have just finished creating/editing.
9. Click ✕ to close the **Edit Port:** panel for the Expression Filter soft port that you have just finished creating/editing.

   You are returned to the **Port Manager** page from where you can add/edit additional Expression Filter soft ports.

   The created Expression Filter soft port will appear in the **Statistics** page (see *Illustration 160* on page 527), with the following three associated object types (see *Illustration 23*):

   Object Type : Port Container, with:
   - Name : Expression_Filter.
   - Object type : Port Container.
   - Description : Sub Port Container for <Parent Port name>.

   Object Type : Link, with:
   - Name : [Expression_Filter] -> [<Parent Port name>].
   - Object type : Link.
   - Description : blank (this is normal)

   Object Type : Soft Port, with:
   - Name : the name you gave to the Filter Expression soft port (e.g. T_10).
   - Object type : Soft Port.
   - Description : the name of the parent port the child Filter Expression soft port belongs to (e.g. 0 for hardware port 0, Top Level if the IPv4 soft port was created at the top level with no parent).

Note:

The Port Container and Link object types related the Filter Expression soft port only get created once (i.e. when the first Filter Expression soft port is created in the parent port). When additional Filter Expression soft ports get created within the same parent port, only additional Soft Port

object types get created. This is normal behavior, as a parent port only requires one Port Container object and one Link object in order to support multiple Filter Expression soft ports.

Illustration 30 shows an example of the five Filter Expression soft ports that were created for the example in *Illustration 29* on page 132. For any parent port, the child Filter Expression soft ports are listed in the order that they were created (i.e. not listed in alpha-numeric order). Therefore, if you want an alpha-numeric ordering of Filter Expression soft ports within the **Statistics** page, ensure that you create the Filter Expression soft ports in a chronological order that is the same as the alpha-numeric ordering that you desire.

10. Repeat steps 2 to 9 for each of the Expression Filter soft ports you want to add using the Soft Port : Expression Filter function.

    Illustration 29 shows how the **Port Manager** page appears once the Expression Filter soft port has been created following the example shown in *Illustration 31*.

ILLUSTRATION 30 - EXAMPLE RESULT OF ADDING FIVE EXPRESSION FILTER SOFT PORTS TO IPV4 SOFT PORT 192.168.4.1

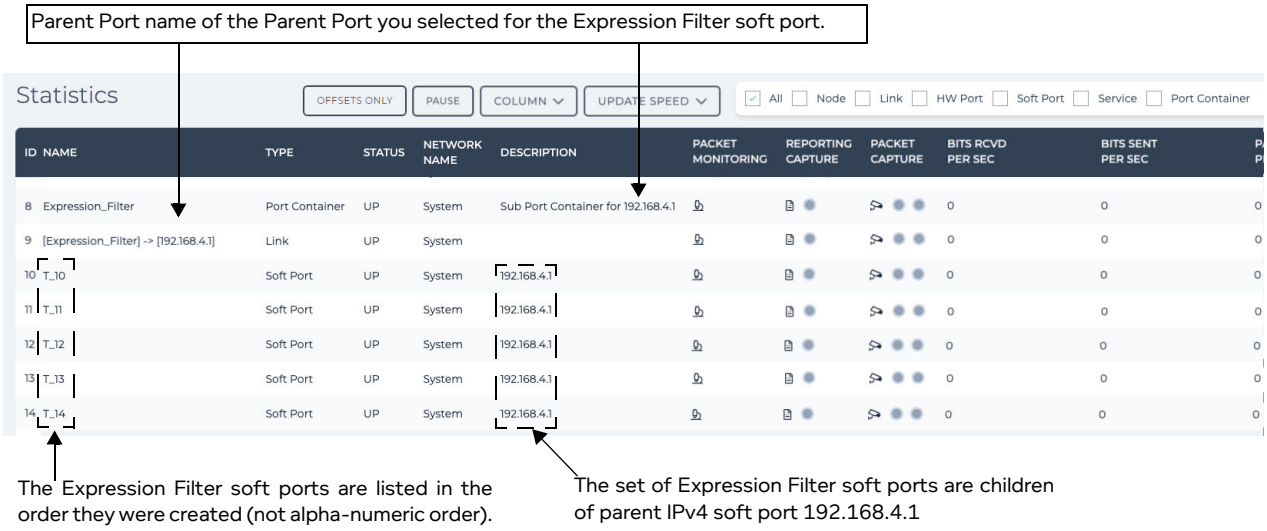
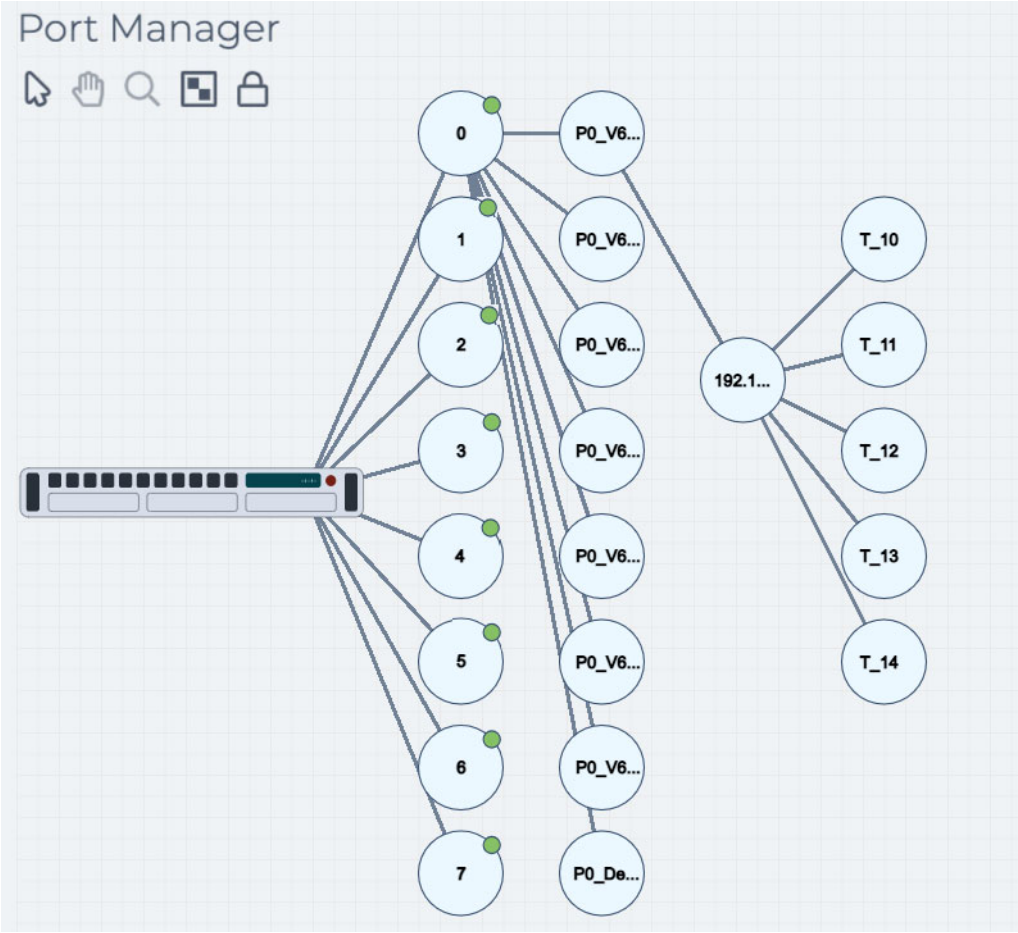


ILLUSTRATION 31 - EXAMPLE PORT MANAGER PAGE WITH AN EXPRESSION FILTER SOFT PORT



2-2-6. Creating a Static NAT Soft Port

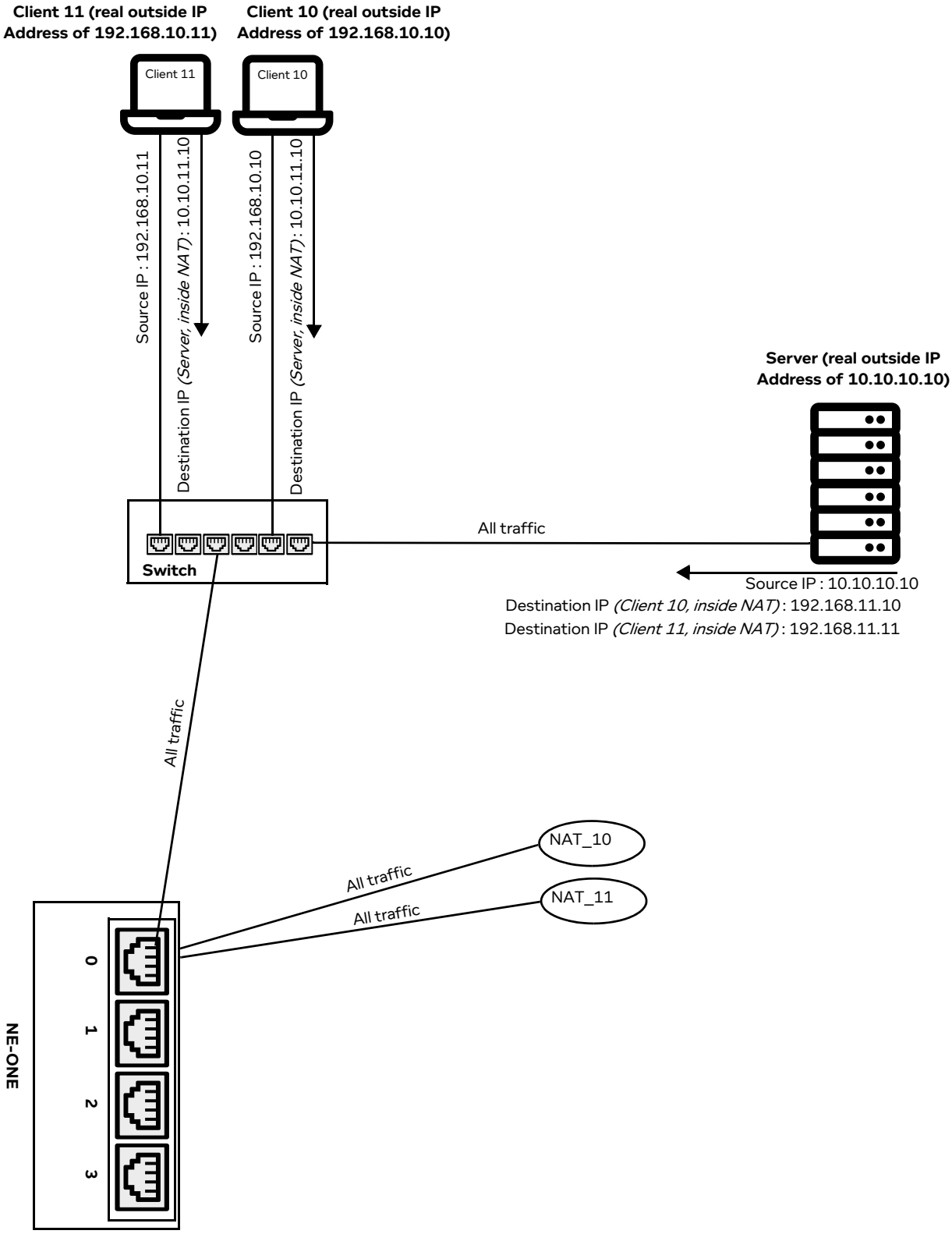
The Static NAT soft port function lets you create Network Address Translation (NAT) operations between static IP addresses of a source (client) hosts and destination (server) hosts. The Static NAT soft port function uses the following parameters:

- **Source IP Address** - as a packet enters the Static NAT soft port from the outside, if it matches this Source IP address its source IPv4 address will changed to Inside Source IP Address (see below).
- **Destination IP Address** - as a packet enters the Static NAT soft port from the outside, if it matches this Destination IP address its destination IPv4 address will changed to Inside Destination IP Address (see below).
- **Inside Source IP Address** - as a packet leaves the Static NAT soft port from the inside, if it matches this Inside Source IP address its source IPv4 address will changed to Source IP Address (see above).
- **Inside Destination IP Address** - as a packet leaves the Static NAT soft port from the inside, if it matches this Inside Destination address its destination IPv4 address will changed to Destination IP Address (see above).

The idea behind the Static NAT soft port function is to allow, for example a server with a real destination address of 10.10.10.10 (say) to be accessed by client 192.168.10.10 (say) as address 10.10.11.10 (say). The server would believe that the client had address 192.168.11.10 (say). This would mean that the server would remain accessible by its normal address 10.10.10.10 but if a user specified 10.10.11.10 then the core routers would direct that traffic to the NE-ONE which would NAT the destination addresses to be the real server and the source address to be a spoofed client. On the way back the NAT would be reversed to allow the server to respond indirectly to the real client.

Extending this example to two clients with (real, "outside") IP addresses 192.168.10.10 and 192.168.10.11 (see *Illustration 32*), you would create two Static NAT soft ports (i.e. a Static NAT soft port for each client source IP address and server destination IP address that needs NATing/De-NATing.

ILLUSTRATION 32 - NETWORK ADDRESS TRANSLATION EXAMPLE USING THE STATIC NAT SOFT PORT



Use the following steps to create a soft port with the Soft Port : Static NAT function. The steps below use the IP addresses of two clients and a server with a NAT configuration according to the example

above in *Illustration 32*. Adjust the steps below according to the clients and servers in your network and your NAT requirements.

1. From the Web Interface, click **Management > Port Manager**.
   A **Port Manager** page appears (see *Illustration 17*) displaying the hardware ports and soft ports (if any exist).
2. Click on the intended parent port (either hardware or soft port) which will accommodate the new Static NAT soft port you are about to create.
   In our example, the Static NAT soft port is added to hardware port 1.
   The right hand side of the **Port Manager** page updates with an **Edit Port:** panel, and the selected parent port becomes highlighted.
3. In the **Edit Port:** panel that appears, click the **Add Child To Selected Port** button.
   A **Port Name** dialog box that appears.
4. In the **Port Name** dialog box that appears, type the name for the Static NAT soft port you are creating, and click **OK**. The name can contain alphanumeric characters and spaces. Choose a name that signifies the type of Static NAT soft port you are creating. It can be anything, though for convenience and easy recognition, you could use a combination of the acronym Network Address Translation (NAT) and the last digital digit of the client's IP Addresses you are NATing/De-NATing (e.g. 10 from 192.168.10.10).

Note:
Once created, the port name for a Static NAT soft port is not editable. Therefore, ensure that you choose a Static NAT soft port name that is meaningful for you or your end users to identify later on (e.g. NAT_10).

! Notice:
When using the NE-ONE with RADIUS authentication, you cannot not use spaces in any of the names of the soft ports that you create. Calnex recommend that you the underscore (_) symbol if required.

! Notice:
Since the NE-ONE uses the comma (,) symbol as a delimiter within its source code, do not use commas within soft port names.

For the example in *Illustration 32*, you would do the following:

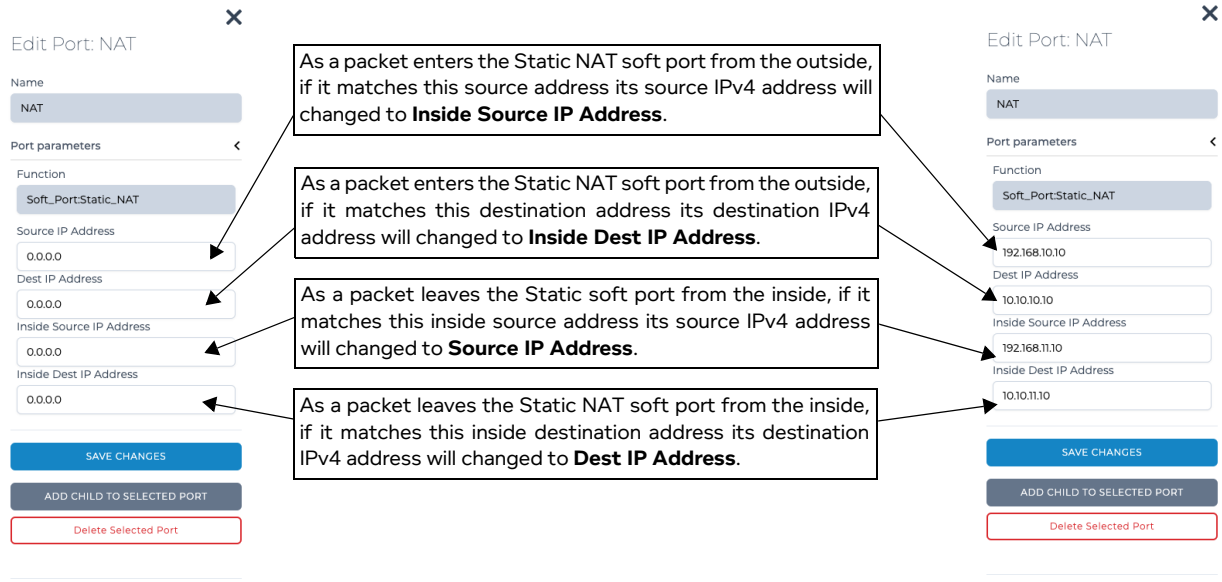
- For the first Static NAT soft port (for client 10), you would type **`NAT_10`** for the port name.
- For the second Static NAT soft port (for client 11), you would type **`NAT_11`** for the port name.

5. In the **Port Type** dialog box that appears, select **Soft port:static nat**, and click **OK**.
   The **Port Manager** page updates with and automatically selects the newly created Static NAT soft port.

Note:
The **Port Type** dialog box only appears once when the first child soft port is being created within the parent port. Once the first child soft port is created within the parent port, all further created child soft ports inherit the port type used by the first child port, and thus you are immediately taken to the **Edit Port:** panel with the **Port Parameters** area.

The **Edit Port:** panel updates with information associated with the newly created Static NAT soft

port.



Initial **Edit Port:** panel for Static NAT soft port function.

Example **Edit Port:** panel for Static NAT soft port function for Client 10 in our example in *Illustration 32*.

6. Complete the fields as summarized in *Table 21*.

TABLE 21 - PARAMETERS FOR THE SOFT PORT : STATIC FUNCTION

Field	Description
Source IP Address	This defines the Source IP Address that you want to change to the Inside Source IP Address using the Static NAT soft port function. As a packet enters the Static NAT soft port from the outside, if it matches this source address its source IPv4 address will changed to Inside Source IP Address you define in the **Inside Source IP Address** field.
Dest IP Address	This defines the Destination IP Address that you want to change to the Inside Destination IP Address using the Static NAT soft port function. As a packet enters the Static NAT soft port from the outside, if it matches this destination address its destination IPv4 address will changed to the Inside Destination IP Address that you define in the Inside Dest IP Address field.
Inside Source IP Address	This defines the Inside Source IP Address used by the Static NAT soft port function. As a packet leaves the Static NAT soft port from the inside, if it matches this Inside Source IP Address its source IPv4 address will changed to the Source IP Address that you defined in the **Source IP Address** field.
Inside Dest IP Address	This defines the Inside Destination IP Address used by the Static NAT soft port function. As a packet leaves the Static NAT soft port from the inside, if it matches this Inside Destination IP Address its destination IPv4 address will changed to that you defined in the **Dest IP Address** field.

For the example in *Illustration 32*, you define each of the Static NAT parameters on the single Static NAT soft port, as summarized in *Table 22*.

TABLE 22 - IPV4 INTERFACE PARAMETERS FOR THE EXAMPLE IN ILLUSTRATION 32

Field	Setting for example in Illustration 32
Source IP Address	First Static NAT soft port for client 10, type **192.168.10.10** Second Static NAT soft port for client 11, type **192.168.10.11**
Dest IP Address	First Static NAT soft port for client 10, type **10.10.10.10** Second Static NAT soft port for client 11, type **10.10.10.10** **Note:** it is normal that the value (i.e. **10.10.10.10**) is the same for both clients 10 and 11, as we are defining the destination IP address of the Server that they are connecting to via the Static NAT soft port function.
Inside Source IP Address	First Static NAT soft port for client 10, type **192.168.11.10** Second Static NAT soft port for client 11, type **192.168.11.11**
Inside Dest IP Address	First Static NAT soft port for client 10, type **10.10.11.10** Second Static NAT soft port for client 11, type **10.10.11.10** **Note:** it is normal that the value (i.e. **10.10.11.10**) is the same for both clients 10 and 11, as we are defining the inside destination IP address of the Server that they are connecting to via the Static NAT soft port function.

7. Click **SAVE CHANGES** to save the Static NAT soft port that you have just finished creating/editing.
8. Click ✕ to close the **Edit Port:** panel for the Static NAT soft port that you have just finished creating/editing.

   You are returned to the **Port Manager** page from where you can add/edit additional soft ports.

   The Static NAT soft port will now perform NATing according to the criteria that you defined.

   The created Static NAT soft port will appear in the **Statistics** page (see *Illustration 160* on page 527), with the following three associated object types (see *Illustration 33*):

   Object Type : Port Container, with:
   - Name : <Parent Port name> <--> Soft_Port:Static_NAT.
   - Object type : Port Container.
   - Description : Sub Port Container for <Parent Port name>.

   Object Type : Link, with:
   - Name : [<Parent Port name> <--> Soft_Port:Static_NAT] -> [<Parent Port name>].
   - Object type : Link.
   - Description : blank (this is normal)

   Object Type : Soft Port, with:
   - Name : the name you gave to the Static NAT soft port (e.g. NAT_10).
   - Object type : Soft Port.
   - Description : the name of the parent port the child Static NAT soft port belongs to (e.g. 1 for hardware port 1).

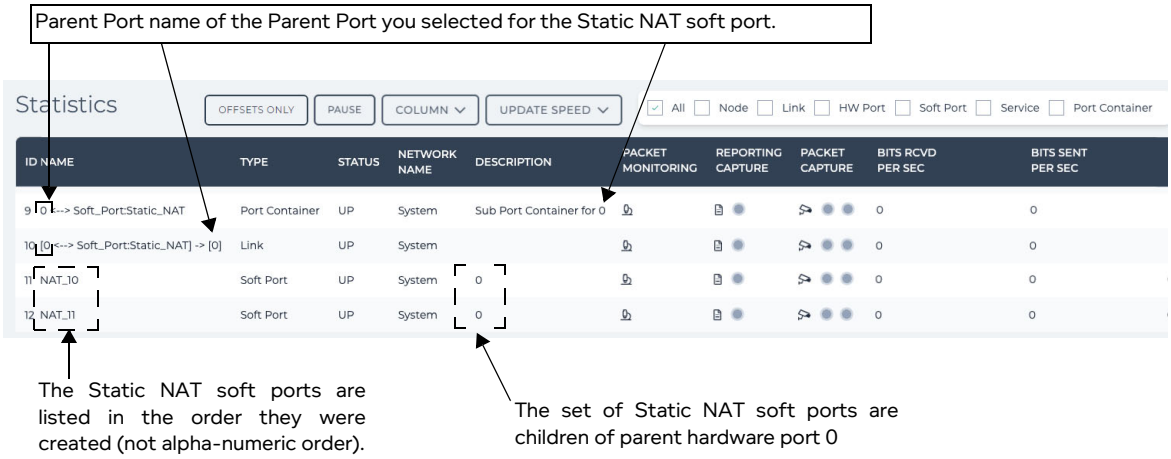
Note:

The Port Container and Link object types related the Static NAT soft port only get created once (i.e. when the first Static NAT soft port is created in the parent port). When additional Static NAT soft ports get created within the same parent port, only additional Soft Port object types get

created. This is normal behavior, as a parent port only requires one Port Container object and one Link object in order to support multiple Static NAT soft ports.

Illustration 33 shows an example of the three associated Static NAT soft port objects that are created when creating two Static NAT soft ports for the example in *Illustration 32* on page 139. For any parent port, the child Static NAT soft ports are listed in the order that they were created (i.e. not listed in alpha-numeric order). Therefore, if you want an alpha-numeric ordering of Static NAT soft ports within the **Statistics** page, ensure that you create the Static NAT soft ports in a chronological order that is the same as the alpha-numeric ordering that you desire.

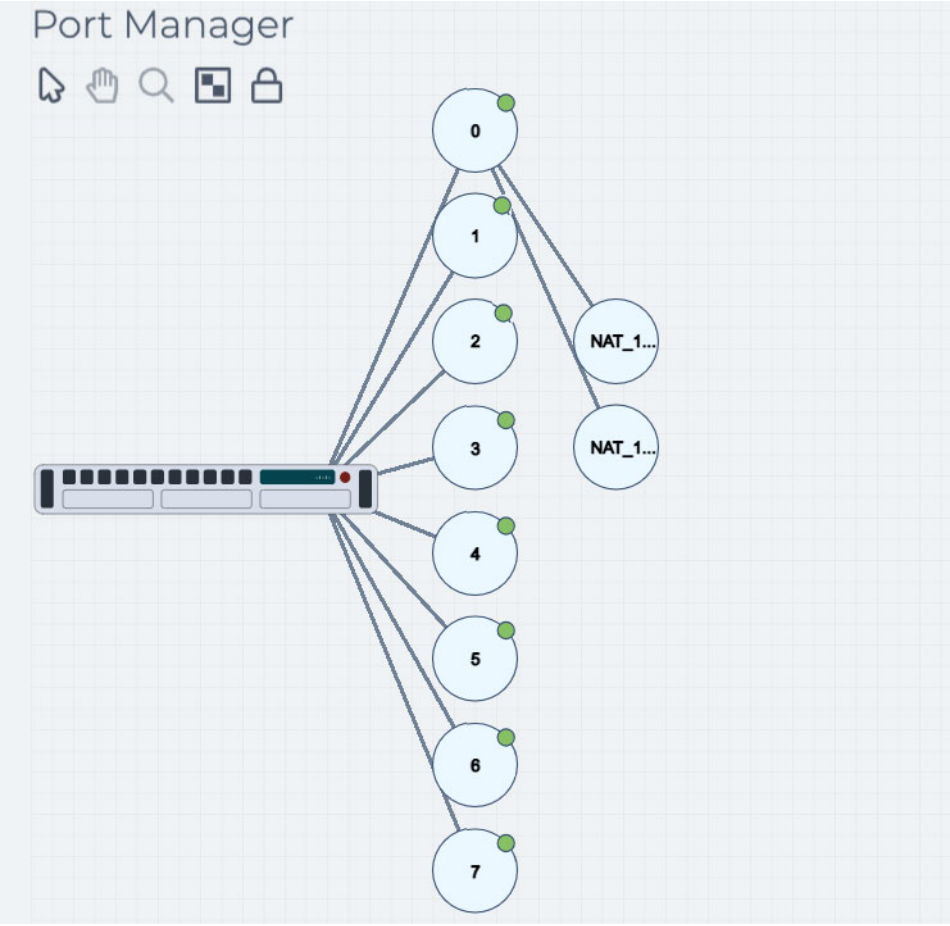
ILLUSTRATION 33 - EXAMPLE RESULT OF ADDING A STATIC NAT SOFT PORT TO HARDWARE PORT 0



9. Repeat steps 2 to 8 for each of the Static NAT soft ports you want to add using the Soft Port : Static NAT function.

   Illustration 34 shows how the **Port Manager** page appears once all of the Static NAT soft ports have been created on hardware port 0 following the example shown in *Illustration 32*.

ILLUSTRATION 34 - EXAMPLE PORT MANAGER PAGE WITH A STATIC NAT SOFT PORT



2-2-7. Creating a Hardware Traffic Generation Soft Port

You can use the soft ports feature to create special traffic generation soft ports, each soft port having one or more attached streams. Each stream, when enabled will generate packets of data according to the stream specifications you have defined. Typically (in order to not waste the use of one top level hardware ports), you create a traffic generation soft port at the top level on the NE-ONE.

Note:

For simplicity, consolidation, and ease of use within the Web Interface, the Generate : Hardware Traffic Generation function is grouped with the other soft port functions. However, in terms of networking, the Generate : Hardware Traffic Generation function does not create a parent port that accepts traffic from other ports - it is simply a traffic generation object.

Use the following steps to create a soft port with the Generate : Hardware Traffic Generation function:

1. From the Web Interface, click **Management > Port Manager**.

   A **Port Manager** page appears (see *Illustration 17*) displaying the hardware ports and soft ports (if any exist).
2. Click on the image of the NE-ONE to create a top level soft port.

   The right hand side of the **Port Manager** page updates with a **Top Level Ports** panel containing a **CREATE A TOP LEVEL PORT** button.
3. In the **Top Level Port**s panel that appears, click the **CREATE A TOP LEVEL PORT** button.

   A **Port Name** dialog box appears.
4. In the **Port Name** dialog box that appears, type the name for the Traffic Generation soft port you are creating, and click **OK**. The name can contain alphanumeric characters and spaces. Choose a name that signifies the type of Traffic Generation soft port you are creating (e.g. TG, TG1, TG_1, or TG 1).

Note:

Once created, the port name for a soft port is not editable. Therefore, ensure that you choose a soft port name that is meaningful for you or your end users to identify later on (e.g. TG1, TG_1, or TG 1).

! Notice:

When using the NE-ONE with RADIUS authentication, you cannot not use spaces in any of the names of the soft ports that you create. Calnex recommend that you the underscore (_) symbol if required.

! Notice:

Since the NE-ONE uses the comma (,) symbol as a delimiter within its source code, do not use commas within soft port names.

Note:

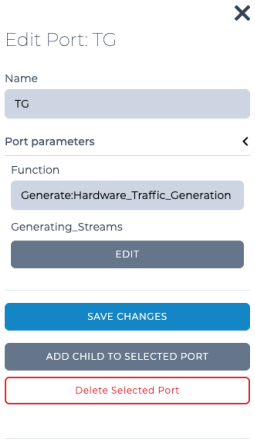
The **Port Manager** page represents soft ports by small circles. The port name that you define appears within the small circles that represent the soft ports in the **Port Manager** page. Although the **Port Name** dialog box accepts a long string of alphanumeric characters with spaces, Calnex recommends that you keep the port name to no more than five characters long.

5. In the **Port Type** dialog box that appears, select **Generate:hardware traffic generation**, and click **OK**.

Note:

The **Port Type** dialog box only appears once when the first child soft port is being created within the parent port. Once the first child soft port is created within the parent port, all further created child soft ports inherit the port type used by the first child port, and thus you are immediately taken to the **Edit Top Level Soft Port:** panel with the **Port Parameters** area.

The **Port Manager** page updates with and automatically selects the newly created Traffic Generation soft port. An **Edit Port:** panel appears on the right with information associated with the newly created Traffic Generation soft port.



6. In the **Edit Port:** panel for the newly created Traffic Generation soft port, click the **EDIT** button.

   A **Generating Streams** dialog box appears listing the defined traffic streams for the Traffic Generation soft port.

   Note: The **Generating Streams** dialog box is empty for new a soft port, and will only be populated if you are editing an already created soft port, or currently creating a soft port and have added at least one port.

   A **Generating Streams** dialog box lets you:

   - add multiple traffic streams (via the **ADD ROW** button) (i.e. create an array of traffic streams, where each row in the array represents a traffic stream)
   - edit existing traffic streams in the traffic stream array
   - delete an existing traffic stream from the traffic stream array
   - change the order of traffic streams in the traffic stream array

7. The Generate : Hardware Traffic Generation function lets you create multiple streams for the soft port. Use the following sub-steps for each stream that you want to create:

   a. From the **Generating Streams** dialog box, click the **ADD ROW** button.

      A new **Generating_Streams (0)** row appears in the **Generating Streams** dialog box with the fields and check boxes as summarized in *Table 23*.

   b. In the new **Generating_Streams (0)** row appears, complete the fields and check boxes as summarized in *Table 23*.

TABLE 23 - STREAM PARAMETERS FOR THE TRAFFIC GENERATION FUNCTION

Field / Checkbox	Description
VLAN Id	If this field is blank or set to zero and **Stream Type** is set to TCP a non-VLAN stream will be generated. If this field is specified you must set the **Stream Type** to TCP to generate a VLAN tagged TCP stream, otherwise this field is ignored and a UDP stream will be generated.
Stream Type	Defines the stream type; either UDP or TCP.
Ethernet Source Address	Defines the MAC address of where the packet is deemed to be from.

Field / Checkbox	Description
Ethernet Destination Address	Defines the MAC address of where the packet is deemed to be going.
Source Port	Defines the port where the packet is deemed to be coming from.
Destination Port	Defines the port where the packet is deemed to be going to.
TTL	Defines the time to live value the packet is deemed to be set to.
IP Source Address	Defines the IP address the packet is deemed to be coming from. This can be either an IPv4 or an IPv6 specified address.
IP Destination Address	Defines the IP address the packet is deemed to be going to. This can be either an IPv4 or an IPv6 specified address.
Packet Data	This is a free text field, and can be anything you want. The length of the packet headers plus the length of the packet data must not be greater than the packet size specified in the **Packet Size** field. **Note:** It is recommended to put something meaningful, linking the stream's packet data to the name of the soft port you are creating so that it is easily identifiable in the reports, packet capture and Statistics. For example, if you have created a soft port with name TG1 then you could specify `TG1_STREAM1` for the first stream, `TG1_STREAM2` for the second stream, etc.. Alternatively, if you have created a soft port with name TG_1 then you could specify `TG_1_STREAM_1` for the first stream, `TG_1_STREAM_2` for the second stream, etc.
Packet Size	Defines the size of the packet including headers and data but no the checksum added at the end before transmission.
Packets Per Second	Defines the rate at which the traffic generation function should send packets for this stream. If this value is zero then the Bits Per Second field must be non-zero.
Bits Per Second	Defines the rate at which the traffic generation function should send packets for this stream based on the number of bits per second to be streamed.
Enabled	Flag (`1` or `0`) to indicate whether stream is active and generating packets or disabled and non-active. To enable the stream, type **1**. To disable the stream, type **0**.

ILLUSTRATION 35 - GENERATING STREAMS DIALOG BOX

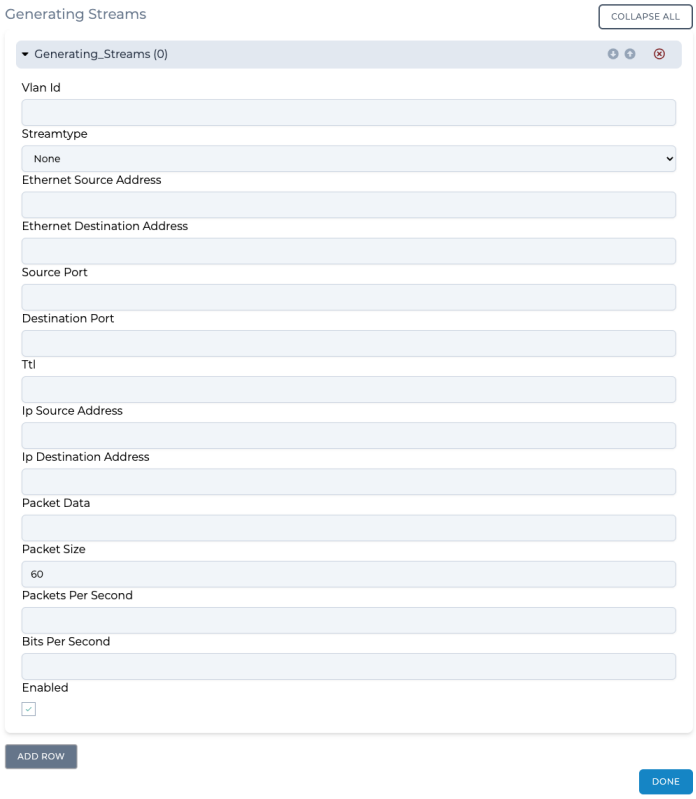


TABLE 24 - EXAMPLE STREAM PARAMETERS FOR THE TWO STREAMS IN A TRAFFIC GENERATION FUNCTION

Field / Checkbox	Traffic Stream 1 (row 0)	Traffic Stream 2 (row 1)
VLAN Id	0	0
Stream Type	TCP	TCP
Ethernet Source Address	00:4f:2c:9a:92:38	00:4f:2c:9a:92:39
Ethernet Destination Address	00:44:65:20:34:d3	00:44:65:20:34:d4
Source Port	0	0
Destination Port	0	0
TTL	0	0
IP Source Address	192.168.5.100	192.168.5.100
IP Destination Address	192.168.6.100	192.168.6.100
Packet Data	TG_STREAM_1	TG_STREAM_1
Packet Size	60	60
Packets Per Second	2	2
Bits Per Second	10000000	10000000
Enabled	Ticked (i.e. enabled)	Ticked (i.e. enabled)

c. Determine your next step:

To create another stream, click **ADD ROW**, and repeat sub-steps a and b above.

To edit an existing stream, click on ▸ to expand the desired **Generating_Streams (N)** and update the fields and check boxes (summarized in *Table 23*) according to your new stream requirements.

To delete an existing stream, click the ⊗ icon of the desired **Generating_Streams (N)** row corresponding to the traffic stream that you want to delete.

To move a traffic stream down within the traffic stream array, click the ⬇ icon of the desired **Generating_Streams (N)** row corresponding to the traffic stream that you want to move down.

To move a traffic stream up within the traffic stream array, click the ⬆ icon of the desired **Generating_Streams (N)** row corresponding to the traffic stream that you want to move up.

To apply the existing list of streams of the Traffic Generation soft port, click **DONE**. Upon clicking **DONE**, you are returned to the **Port Manager** page, and the **Edit Top Level Soft Port:** panel remains open.

8. Click **SAVE CHANGES**.
9. Click ✕ to close the **Edit Port:** panel for the Traffic Generation soft port that you have just finished creating/editing.

The Traffic Generation soft port will now create one or more traffic streams according to the criteria that you defined.

The created Traffic Generation soft port will appear in the **Statistics** page (see *Illustration 160* on page 527), with the following four associated objects (see *Illustration 36*):

Port Container, with:

- Name : Generate:Hardware_Traffic_Generation.
- Type : Port Container.
- Description : Port Container.

Soft Port, with:

- Name : the name you gave to the Traffic Generation soft port (e.g. TG).
- Type : Soft Port.
- Description : Top Level Port.

Illustration 36 shows an example of the four associated Traffic Generation soft port objects that are created when creating one Traffic Generation soft port for the example in *Table 24* on page 148.

ILLUSTRATION 36 - EXAMPLE OF ADDING A TRAFFIC GENERATION SOFT PORT TO THE TOP LEVEL

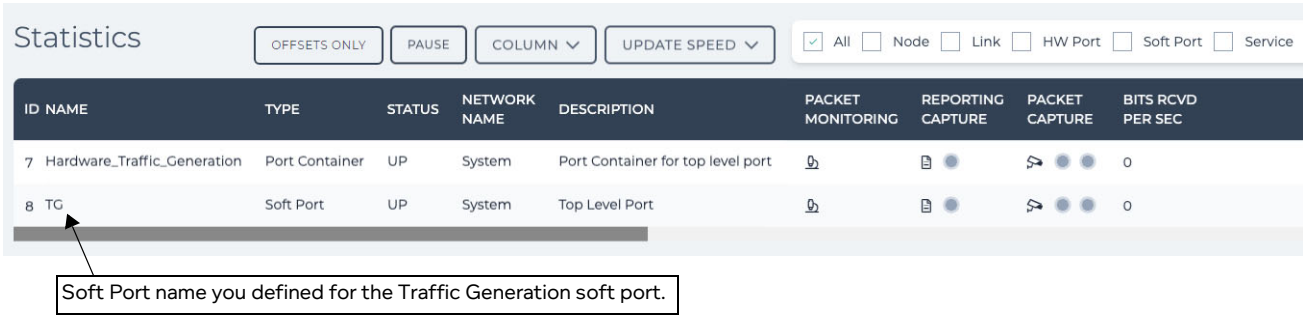
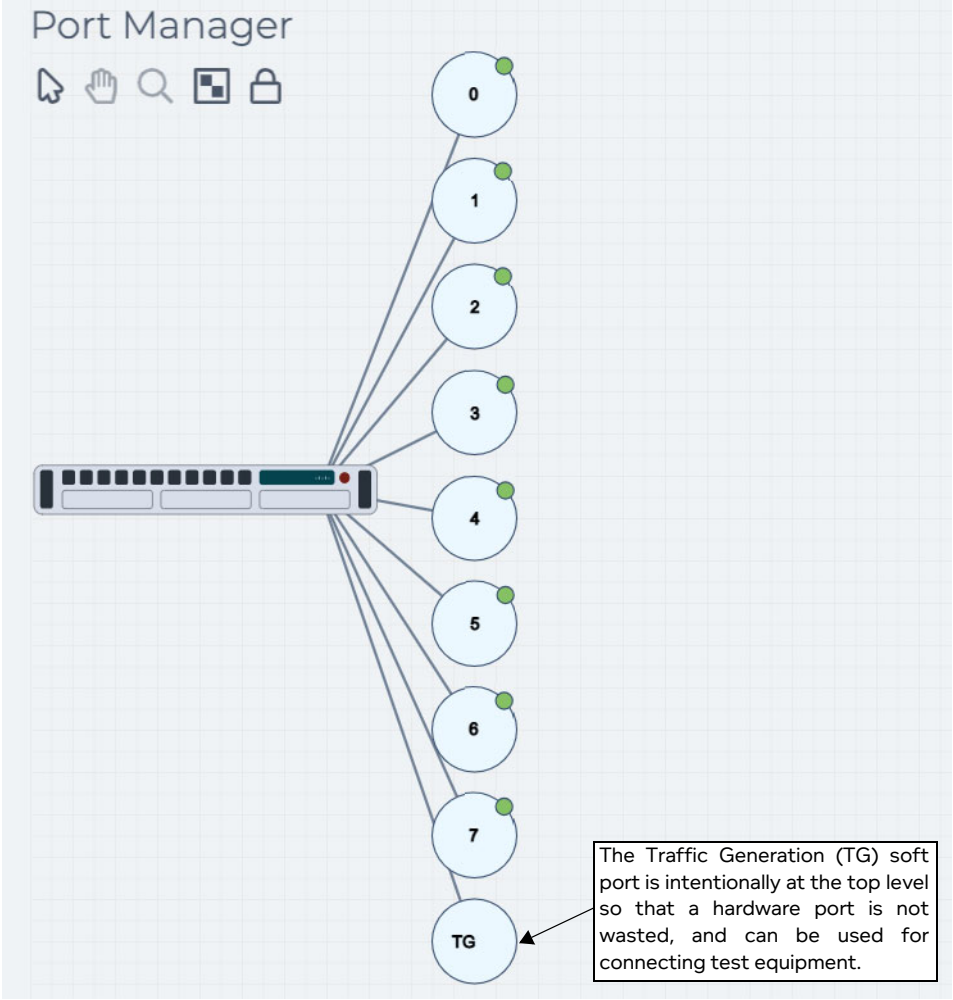


Illustration 37 shows how the **Port Manager** page appears once that the Traffic Generation soft port has been created at the top level (i.e. no parent port).

ILLUSTRATION 37 - EXAMPLE PORT MANAGER PAGE WITH A TRAFFIC GENERATION SOFT PORT



2-3. Editing Soft Ports

Once a soft port has been created, if needed it can be edited at a later date. If you edit an existing soft port, ensure that you communicate to the NE-ONE users the changes you made so they are aware the soft port is now functioning differently to before.

Use the following steps to edit an existing soft port:

1. From the Web Interface, click **Management > Port Manager**.
   A **Port Manager** page (*Illustration 17* on page 103) appears displaying the hardware ports and soft ports (if any exist).
2. Click on the soft port that you intend to edit.
   The right hand side of the **Port Manager** page updates with an **Edit Port:** panel, and the selected port becomes highlighted.
3. In the **Edit Port:** panel that appears, click on **<** to the right of **Port Parameters** to expand the **Port Parameters** area and click the **EDIT** button.
4. The steps to edit the soft port depend on the soft port function you are editing, and those steps are the same as when creating the soft port. Use the one of the appropriate sections below to edit the soft port according to your new requirements:
   - *Creating a Filter Soft Port* on page 124
   - *Creating a VLAN Soft Port* on page 107
   - *Creating an IPv4 Soft Port* on page 114
   - *Creating an Expression Filter Soft Port* on page 132
   - *Creating an IP Soft Port* on page 122
   - *Creating a Static NAT Soft Port* on page 138
   - *Creating a Hardware Traffic Generation Soft Port* on page 145

2-4. Deleting Soft Ports

! Notice:

You cannot delete a soft port if it is being used by a running network or running scenario. If a soft port is currently being used by a running network or running scenario it has a lock icon attached to it.

You can, however, delete a soft port that is used by a network or scenario if the network or scenario is not currently running. Ensure that you really want to delete the soft port because any networks/scenarios that use that soft port will be impacted, and require new soft ports assigned to their nodes. Be careful to communicate with the non-admin users (who make networks and scenarios) so they are aware that they may need to re-assign a new soft port to their existing network/scenario.

You can only delete soft ports that do not contain any "child" soft ports. Use the following steps to delete an unneeded soft port:

1. Check with all the NE-ONE users that they are no longer using the soft port you intend to delete with their networks/scenarios.
2. From the Web Interface, click **Management > Port Manager**.
   A **Port Manager** page (*Illustration 17* on page 103) appears displaying the hardware ports and soft ports (if any exist).
3. Click on the soft port that you intend to delete.
   The right hand side of the **Port Manager** page updates with an **Edit Port:** panel, and the selected

port becomes highlighted.

4. In the **Edit Port:** panel that appears, click **Remove Selected Port**.
5. In the **Delete port** dialog box that appears, click **OK**.

   The **Delete port** dialog box closes and the deleted soft port no longer exists in the **Port Manager** page. The deleted soft port is no longer available to users when they create networks/scenarios.

2-5. Deleting (Clearing) All Soft Ports

Notice:

You cannot delete (clear) all soft ports if any of them being used by a running network or running scenario. If a soft port is currently being used by a running network or running scenario it has a lock icon attached to it.

You can, however, delete (clear) all soft ports that are used by a network or scenario if the network or scenario is not currently running. Ensure that you really want to delete (clear) all soft ports because any networks/scenarios that use that soft port will be impacted, and require new soft ports assigned to their nodes. Be careful to communicate with the non-admin users (who make networks and scenarios) so they are aware that they may need to re-assign a new soft port to their existing network/scenario.

Notice:

Deleting (clearing) all soft ports results in removing the current soft port configuration and reverting the NE-ONE back to its initial hardware port configuration. Before clearing all soft ports, Calnex recommend that you backup your current ports configuration according to *Saving a Ports Configuration* on page 152, so that if required it can be restored according to *Loading a Ports Configuration* on page 153.

Use the following steps to remove the current soft port configuration and revert the NE-ONE back to its initial hardware port configuration:

1. Check with all the NE-ONE users that they are no longer using any of the soft ports that exist on the NE-ONE with their networks/scenarios.
2. From the Web Interface, click **Management > Port Manager**.

   A **Port Manager** page (*Illustration 17* on page 103) appears displaying the hardware ports and soft ports (if any exist).
3. From the **Port Manager** page, click on the **PORTS CONFIG** button, and select **Clear**.
4. In the confirmation dialog box that appears, click **OK**.

   The confirmation dialog box closes and the all the soft ports are deleted and no longer exists in the **Port Manager** page. The soft ports are no longer available to users when they create networks/scenarios. Until new soft ports are created or a previously saved ports configuration is loaded, only the hardware ports are available to users when they create networks/scenarios.

2-6. Saving a Ports Configuration

Calnex recommend that you save your ports configuration regularly for backup purposes. You can also save the ports configuration so that it can be copied to another NE-ONE (if is has the same number of hardware ports). You can also save the ports configuration incrementally at different stages of your soft ports creation process. When you save a ports configuration, an associated ports configuration file gets created in the `/Private/port_configs` directory. The ports configuration file will contain the following:

- all port pair definitions
- all port pair favorite definitions

- all soft port configurations
- all port hierarchy

Use the following steps to save the NE-ONE's current ports configuration:

1. From the Web Interface, click **Management > Port Manager**.
   A **Port Manager** page (*Illustration 17* on page 103) appears displaying the hardware ports and soft ports (if any exist).
2. From the **Port Manager** page, click on the **PORTS CONFIG** button, and select **Save As**.
3. In the confirmation dialog box that appears type the filename for the ports configuration, then click **OK**.
   A ports configuration file with the filename you specified gets created in the `/Private/port_configs` directory.

2-7. Loading a Ports Configuration

Any previously saved ports configurations or manually copied ports configurations from another NE-ONE are located in the `/Private/port_configs` directory.

Notice:

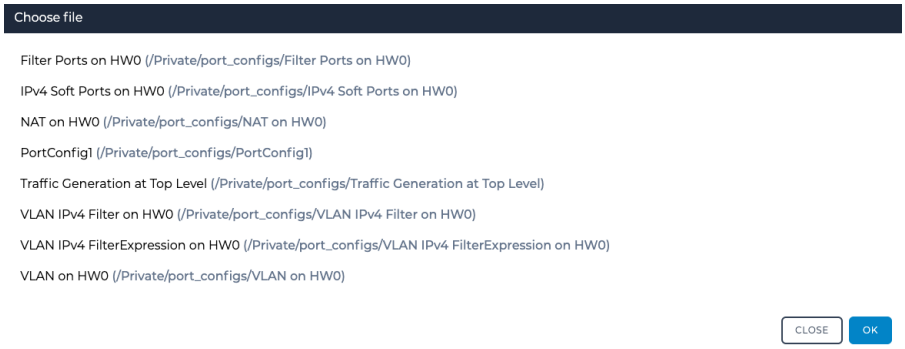
Loading a ports configuration on the NE-ONE replaces the existing ports configuration, which can impact your existing users networks/scenarios. Loading a ports configuration may result in deleting one or more soft ports, and thus require that impacted users re-assign other soft ports to their nodes. Be careful to communicate with the non-admin users (who make networks and scenarios) so they are aware that they may need to re-assign a new soft port to their existing network/scenario.

Notice:

Before loading a ports configuration, Calnex recommend that you backup your current ports configuration according to *Saving a Ports Configuration* on page 152, so that if required it can be re-loaded (using the same generic steps below).

Use the following steps to load a ports configuration on the NE-ONE:

1. From the Web Interface, click **Management > Port Manager**.
   A **Port Manager** page (*Illustration 17* on page 103) appears displaying the hardware ports and soft ports (if any exist).
2. From the **Port Manager** page, click on the **PORTS CONFIG** button, and select **Load**.
   A **Choose file** dialog box appears listing the existing ports configuration files (if any) that are located in the `/Private/port_configs` directory.



Note:
The `/Private/port_configs` directory is specific to the currently logged in admin user. If there are currently no ports configuration files, the currently logged in admin user has not yet saved any ports configurations on the NE-ONE. In this case, you can ask another admin user who has already saved ports configurations to share their ports configuration files with you, and then use the File Browser to manually upload them into your `/Private/port_configs` directory.

3. In the **Choose file** dialog box that appears select the filename corresponding to the ports configuration that you want to load, then click **OK**.

   A **Previewing** dialog box appears with a preview of the ports configuration that you are about to load on the NE-ONE.

4. In the **Previewing** dialog box that appears review the proposed ports configuration to ensure that you are happy, then do the following:
   - If you want to load the previewed ports configuration on the NE-ONE and replace the existing ports configuration, click **LOAD**.
   - If you do not want to load the previewed ports configuration on the NE-ONE and keep the existing ports configuration, click **CANCEL**.

2-8. Copying Ports Configurations Between Different NE-ONEs

If you have created many soft ports and port pairs (i.e. ports configuration) on an NE-ONE, and have multiple NE-ONEs in your environment, rather than taking time to re-create the ports configuration on the other NE-ONEs, you can download the finalized ports configuration file from the "master" NE-ONE, and apply them to the "other" NE-ONEs in your environment. To do this, use the following steps below:

Note:
The steps below only work if the "other" NE-ONE has the same number of hardware ports as the "master" NE-ONE.

1. Login to the "master" NE-ONE as an admin user, and create all of the definitive set of soft ports and port pairs according to your users envisaged network simulation needs.
2. Once you are happy with the definitive set of soft ports and port pairs, save the ports configuration according to *Saving a Ports Configuration* on page 152. For the ports configuration filename using something meaningful (e.g. `DefinitivePortsConfig_2021_12_14`).
3. set of locations for each country code on the "master" NE-ONE, do the following:
   a. From the Web Interface, click **Management > Platform Settings > File Browser**.
      The **File Browser** page opens with the path of your `/Private` directory.
   b. Navigate to the `/Private/port_configs` directory.
   c. For each of the ports configuration files that exist, right mouse click on them, and select **Download selected File**.
      Each of the ports configuration files are downloaded to your computer's local filing system, and are now ready for uploading to all the "other" NE-ONEs in your environment.
4. For each of the "other" NE-ONEs in your environment that you want to import the ports configuration files, do the following:
   a. Login as an admin user on the "other" NE-ONE.
   b. From the Web Interface, click **Management > Platform Settings > File Browser**.
      The **File Browser** page opens with the path of your `/Private` directory.
   c. Navigate to the `/Private/port_configs` directory.
   d. Right mouse click and select **Upload new File**.

A dialog box appears prompting you to select a file to upload.

e. Click the **SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the appropriate ports configuration file to upload. Then click **OK**.

f. If necessary, repeat sub-steps d to e until all the ports configuration files are uploaded to the "other" NE-ONE.

The ports configuration file(s) from the "master" NE-ONE are now available on the "other" NE-ONE within the `/Private/port_configs` directory, but not yet loaded on the "other" NE-ONE.

5. Use the steps in *Loading a Ports Configuration* on page 153 to load the ports configuration file corresponding to the definitive set of soft ports and port pairs.

3. MANAGING PORT PAIRS

Port pairs are extremely useful as they allow NE-ONE users to rapidly create Point-to-Point networks based on pre-defined port pairs. Port pairs, thus avoid the need for the user to additionally select the port pairs during the Point-to-Point network creation process.

Additionally, port pairs also allow Point-to-Point networks to be created to run over port pairs configured with specific port addressing criteria (e.g. to operate like a network router or to bridge two sub-networks). For more information on configuring a specific port addressing criteria for a port pair, see *Port Pair Settings* on page 162.

Note:

When a user does not use a port pair for creating a Point-to-Point network, they select which ports to use for the port pair. This is referred to as an Ad Hoc port pair. Because Ad Hoc port pairs are created on the fly by a user, they do not have capability of having a specific port addressing criteria defined for them by the admin user. Therefore, Point-to-Point networks running on Ad Hoc port pairs can only run as follows:
- with the hardware port pairs in the same sub-network (i.e operating as a switch),
- with the soft port pairs (running IPv4 routing or IP routing) in the same sub-network.

Depending on whether or not the Port Manager feature is activated on the NE-ONE, pre-defined port pairs will either already exist or not already exist, as follows:

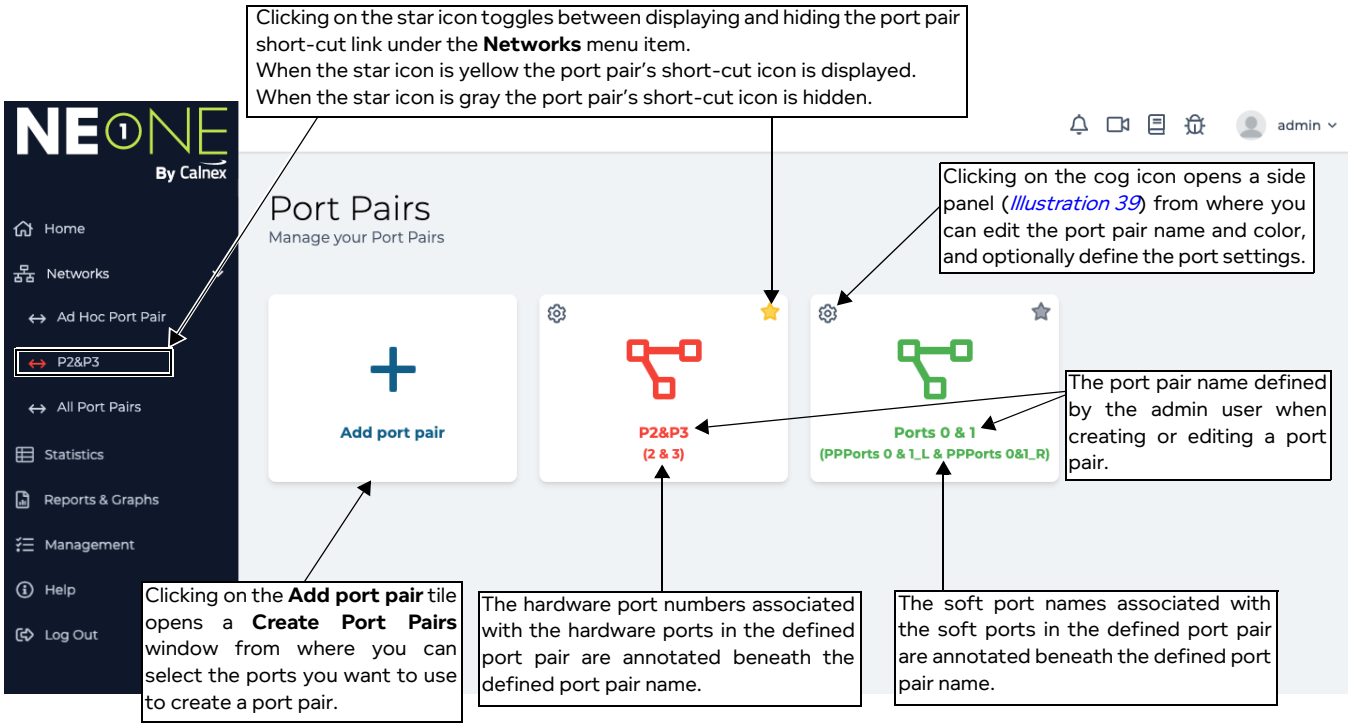
- If the Port Manager feature is deactivated on the NE-ONE, then by default a set of pre-defined hardware port pairs will already be available and pre-configured.
- If the Port Manager feature is activated on the NE-ONE, then by default, the NE-ONE is not configured with any point pairs. Port pairs can be created between the different port types using the Port Manager, as follows:
  - between two hardware ports
  - between two soft ports
  - between a hardware port and a soft port

Note:

The NE-ONE is flexible in its use letting you create port pairs between a hardware port and a soft port. However, even if this is possible, it usually makes no networking sense to create a port pair between a hardware port and a soft port.

All aspects of port pairs are managed from the **Port Pairs** page (*Illustration 38*).

ILLUSTRATION 38 - EXAMPLE PORT PAIRS PAGE



To launch the **Port Pairs** page, from the Web Interface, click **Management > Port Pairs**.

The **Port Pairs** page contains the following:

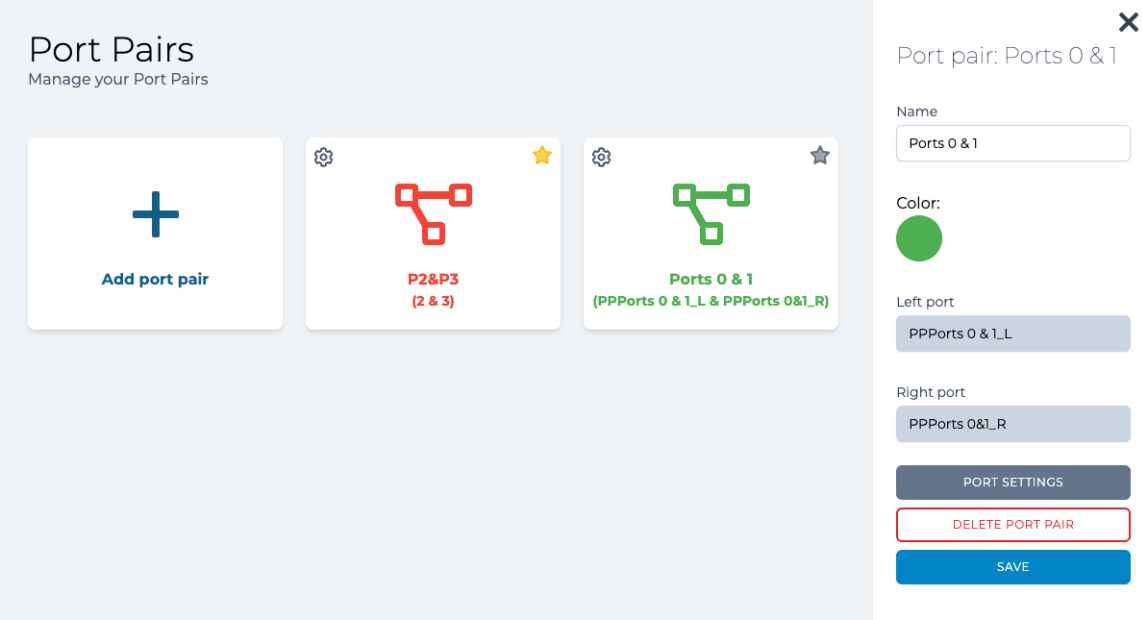
- An **Add port pair** tile. Clicking this tile opens a **Create Port Pairs** dialog box from where you can select the ports you want to use to create a port pair. For more information on creating port pairs, see *Creating Port Pairs* on page 158.
- Tiles for any port pairs that have been created (if they exist). Port pair tiles contain the following icons:
  - Star icon (★). Clicking on the star (★) icon toggles between displaying and hiding the port pair short-cut link under the **Networks** menu item. When the star (★) icon is yellow the port pair's shot-cut icon is displayed. When the star (★) icon is gray the port pair's shot-cut icon is hidden.

    Note: The star (favorite) function is specific to the currently logged in user. For example, if an admin user is logged in, and stars (favorites) a port pair, the starred (favorited) port pair only appears as short-cut link under the **Networks** menu item for the admin user's login session. Similarly, if an admin user has assigned a port pair to another user (see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205), and then the other user stars (favorites) the port pair, the starred (favorited) port pair only appears as short-cut link under the **Networks** menu item for the other user's login session).

    For more information, see *Creating "Starred" Port Pair Favorites* on page 232 in *Chapter 8, General System Procedures*.
  - Cog icon (⚙). Clicking on the cog icon opens a side **Port Pair** panel (*Illustration 39*) from where you can edit the port pair name and color, delete the port pair, and optionally define the port settings. For more information, see *Editing Soft Ports* on page 151, *Deleting Soft Ports* on page 151, and *Port Pair Settings* on page 162.

  Clicking on a port pair tile opens the **Network Port Pair** page (see *Illustration 5* on page 44) for that port pair from where you can create a Point-to-Point network or scenario on that port pair.

ILLUSTRATION 39 - EXAMPLE PORT PAIRS PAGE WITH PORT PAIR SETTINGS SIDE PANEL VISIBLE



3-1. Creating Port Pairs

Note:

Creating port pairs is only possible if the Port Manager feature is activated. Depending on your license, the Port Manager feature may either be activated (i.e. you are able to create port pairs) or deactivated (i.e. you are unable to create port pairs).

Note:

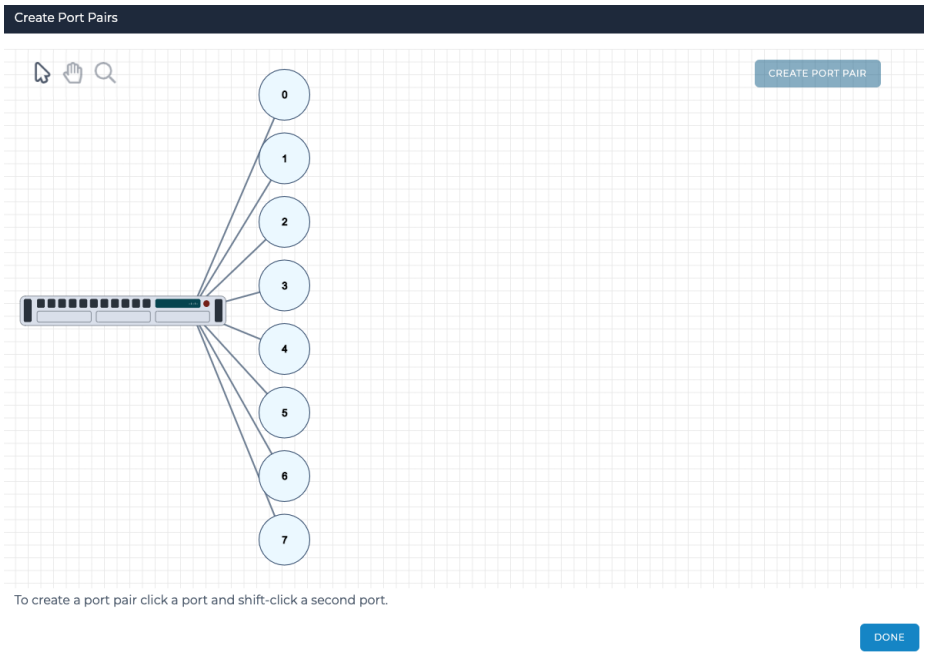
Selecting two ports (i.e. clicking on the first port, and with the **Shift** key pressed clicking on a second port) results in additionally displaying a **Create Port Pair** tile. Clicking on the **Create Port Pair** tile invokes the Port Pair Creation Wizard, from where you can create a new port pair. For more information, see *Creating Port Pairs* on page 158.

Port pairs can be comprised of neighboring ports (e.g. 0 and 1) or non neighboring ports (e.g. 1 and 5).

Use the following steps to create a port pair (the following steps show an example of creating port pairs for the hardware ports 0 and 1):

1. From the Web Interface, click **Management** > **Port Pairs**.
   A **Port Pairs** page (*Illustration 38* on page 157) appears.
2. Click the **Add port pair** tile.

A **Create Port Pairs** window appears.



The **Create Port Pairs** window contains the navigation mode icons summarized in *Table 25*.

TABLE 25 - PORT PAIRS NAVIGATION MODE ICONS

Port Manager Navigation Icon	Description
	When you arrive in the **Create Port Pairs** window, this icon (object select mode) is selected by default. Clicking on this icon selects and enables object select mode. When object select mode is enabled you can click on ports within the **Create Port Pairs** window in order to select them for creating a port pair.
	Clicking on this icon selects and enables canvas pan mode. When canvas pan mode is enabled, you can move the canvas (which contains the image of the NE-ONE and is associated ports) in the appropriate direction when the left mouse button is clicked.
	Clicking on this icon selects and enables canvas zoom mode. When canvas zoom mode is enabled, you can zoom in and out, as follows: • Zoom in on the canvas by clicking the left mouse button and moving the mouse to the right. • Zoom out on the canvas right by clicking the left mouse button and moving the mouse to the left.

3. Click on the first port to select it (in this example, port 0 is selected).
   The first selected port gets highlighted blue.
4. While holding down the **Shift** key, click on the second port to select it (in this example, port 1 is selected).
   The second selected port becomes highlighted green.
5. Click the **CREATE PORT PAIR** button.
   A dialog box appears letting you specify the parameters (i.e. name, color, and left/right port

assignments).

6. In the dialog box that appears, do the following:
   a. In the **Name** field, type an appropriate name to represent the port pair you are creating. The name can contain up to alpha-numeric characters, special characters, and spaces.

Note:
Because other users can favorite this port pair after it is assigned to them (see *Creating "Starred" Port Pair Favorites* on page 232), keep the length of the name reasonable so that it does not appear truncated in the Menu area of the Web Interface.

Note:
If creating a port pair on an NE-ONE Desktop which has an LCD panel, consider the fact that it has two lines of 20 characters. If a port pair name exceeds 20 characters, it will appear truncated in the LCD panel.

   b. Select an appropriate color to represent the port pair.
   c. In the **Left Port** drop-down field, select the port that you want to assign to the left port (by default, the first port you selected is initially chosen).
   d. In the **Right Port** drop-down field, select the port that you want to assign to the left port (by default, the second port you selected is initially chosen).
   e. Click **OK** to confirm the port pair configuration.

The **Port Pairs** page updates with the port pair you created, and the created port pair is committed to the NE-ONE.

7. Click **DONE** to return to the **Port Pairs** page.
   If required the port pair can be further edited (see *Editing Port Pairs* on page 160).

3-2. Editing Port Pairs

Note:
Editing port pairs is only possible if the Port Manager feature is activated. Depending on your license, the Port Manager feature may either be activated (i.e. you are able to edit port pairs) or deactivated (i.e. you are unable to edit port pairs).

Once a port pair has been created, you may want to change the name and/or color that you originally assigned to the port pair at a later date. To change the name and/or color of an existing port pair, you edit the port pair. You can edit a port pair via the **Port Pairs** page (*Illustration 38* on page 157).

Note:
The left and right port assignments of an existing port pair cannot be changed. This is design intent as it assumes that users making Point-to-Point networks based on an existing port pair will have in mind to use the same left and right port assignments. If you want to change the left and right port assignments for an existing port pair, you can delete the existing port pair (see *Creating Port Pairs* on page 158) and re-create a new port pair (see *Deleting Port Pairs* on page 161) with reversed left and right port assignments.

Use the following steps to edit an existing port pair:

1. From the Web Interface, click **Management > ↔ Port Pairs**.
   A **Port Pairs** page (*Illustration 38* on page 157) appears, containing a tile for each port pair.
   Each port pair tile contains a cog icon (⚙) letting you edit it, and a star icon (★) letting you favorite it.
2. Click on the cog (⚙) corresponding to the port pair you want to edit.
   The right hand side of the **Port Pairs** page updates with a **Port Pair** panel (*Illustration 39* on page 158).
3. If you want to change the port pair name, type a new name for the port pair in the **Name** field of the **Port Pair** panel.The port pair name can contain up to alpha-numeric characters, special characters, and spaces.

   Note:
   Because other users can favorite this port pair after it is assigned to them (see *Creating "Starred" Port Pair Favorites* on page 232), keep the length of the name reasonable so that it does not appear truncated in the Menu area of the Web Interface.
4. If you want to change the color of the port pair, click on the existing color under **Color:**, and select a new color from the list of colors that appear.
   The changes you make are immediate reflected in the **Port Pairs** page, but are not yet fully committed.
5. Click the **SAVE** button to commit the changes to the port pair name.
6. In the **Changes saved successfully** dialog box that appears, click **OK**.
   You are returned to the **Port Pairs** page.

3-3. Deleting Port Pairs

Note:
Deleting port pairs is only possible if the Port Manager feature is activated. Depending on your license, the Port Manager feature may either be activated (i.e. you are able to delete port pairs) or deactivated (i.e. you are unable to delete port pairs).

In some cases you may want to delete an existing port pair.

Use the following steps to delete an existing port pair:

1. From the Web Interface, click **Management > ↔ Port Pairs**.
   A **Port Pairs** page (*Illustration 38* on page 157) appears, containing a tile for each port pair.
   Each port pair tile contains a cog icon (⚙) letting you edit it, and a star icon (★) letting you favorite it.
2. Click on the cog (⚙) corresponding to the port pair you want to delete.
   The right hand side of the **Port Pairs** page updates with a **Port Pair** panel (*Illustration 39* on page 158).

3. Click on the **DELETE PORT PAIR** button.
4. From the **Confirm delete** confirmation dialog box that appears, click **OK**.
   The port pair is deleted, you are returned to **Port Pairs** page.

3-4. Port Pair Settings

Note:

Port pair settings (i.e. port addressing and default transmission) are available on all versions of the NE-ONE, and are not part of the Port Manager feature. Even if the Port Manager feature is not activated, you can configure port addressing and default transmission on a port pair, if required.

For each pre-defined port pair it is possible to configure Port Addressing for those ports, and/or enable a Default Transmission background service.

- Enabling and configuring Port Addressing allows the NE-ONE to bridge two sub-networks on the pre-defined port pair. For more information, see *Port Addressing* on page 162.
- Enabling the Default Transmission service, means that when no Point-to-Point network is running on that port pair, packet traffic can still pass through that port pair via a pre-configured background service.

3-4-1. Port Addressing

Not all types of port pairs can support port addressing. *Table 26* summarizes the port pair types that support and do not support port addressing.

TABLE 26 - PORT ADDRESSING SUPPORT PER PORT PAIR TYPE

Port Pair Type	Soft Port Type	Support Port Addressing
Hardware Ports (0, 1, 2, etc.)	Not Applicable	Yes
Soft Ports*	Soft Port : Filter	Yes
	Soft Port : VLAN	Yes
	Soft Port : IPv4	Yes
	Soft Port : Expression Filter	Yes
	Soft Port : IP	Yes
	Soft Port : Static NAT	Yes
	Generate:Hardware Traffic Generation	Yes
Hardware Port and Soft Port*	Possible, but not recommended	No
* - Soft ports can only be created and managed if the Port Manager feature is activated.		

The **PORT ADDRESSING** tab of the **Port Settings** page (*Illustration 40*) contains the elements summarized in *Table 27*.

ILLUSTRATION 40 - PORT SETTINGS PAGE - PORT ADDRESSING TAB

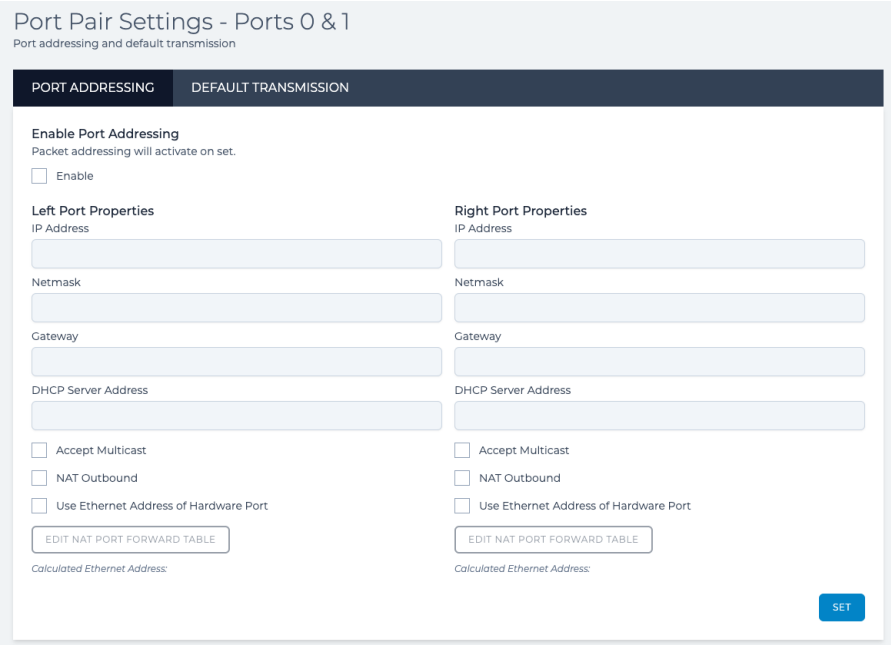


TABLE 27 - PORT SETTINGS PORT ADDRESSING ELEMENTS

Port Settings - Port Addressing Element	Description
Enable check box	This check box determines whether or not port addressing is active (enabled) on the port pair. • If ticked, port addressing is active for the port pair, and you must define the network settings (IP Address and Netmask are mandatory) for the left and right ports. • If unticked, port addressing is inactive for the port pair.
SET button	Clicking this button will immediately set and override the existing port Port Addressing setting for the port pair.
Left Port Properties	
IP Address field	This is a mandatory field, and defines the IP address of the left port, in the usual dotted notation (e.g. 10.0.0.1, or 192.168.2.254). This address can act as the gateway or routing port for other systems using the NE-ONE as their router.
Netmask field	This is a mandatory field, and defines the IP Network Mask in the usual dotted format e.g. 255.255.255.0 for a class C type address. As usual the (bitwise ANDed) combination of Address and Netmask define the Network (e.g. 10.0.0.0 or 192.168.2.0).

Port Settings - Port Addressing Element	Description
Gateway field	This is the IP address of the device (i.e. a router) you will use as your gateway for clients connected to the left port. This optional field lets you specify the IP address of another (i.e. not the NE-ONE) router in that network in the event that the network is more complex and requires further routing. For example, if a DHCP server is not within the network where the left port is connected then a Gateway would be required in order to route DHCP requests to it. • If you want the left port to act as a gateway itself, you can leave this field blank or specify 0.0.0.0. • If you want another device (i.e. a router) in your network to act as the gateway, specify the IP Address of that device.
DHCP Server field	This optional field is provided so that devices/clients connected to the left port requiring an IP address to be assigned by DHCP can have their "DHCP requests" relayed across the NE-ONE to the specified DHCP Server, even when no Point-to-Point network is running. This is explained in more detail in *Section 3-4-1-2, DHCP Server / DHCP Relay* on page 172. **Note:** You are not allowed to configure DHCP servers on both Ports in a Port Pair. Relaying DHCP requests goes in one direction – from either the Left Port to the Right Port to the DHCP server, or from the Right Port to the Left Port to the DHCP server. If you specify the IP address of a DHCP server in this field, the DHCP Server field for the Right Port becomes grayed out.
Accept Multicast check box	This check box optionally lets you decide whether multicast traffic is allowed through the left port. • If this check box is ticked, multicast traffic is allowed through the left port. • If this check box is not ticked, multicast traffic is not allowed through the left port.
NAT Outbound check box	This check box optionally lets you decide whether Network Address Translation (NAT) is applied to outbound traffic from clients connected to the left port. • If this check box is ticked, outbound client traffic through the left port is NATed. The NAT configuration is defined via clicking on the **EDIT NAT PORT FORWARD TABLE** button. • If this check box is unticked, outbound client traffic through the left port is not NATed.
Use Ethernet Address of Hardware Port check box	This check box optionally lets you decide whether the left port will inherit the MAC address of its parent hardware port. This is only required if the left port in the port pair is a soft port (since a hardware port will already have its own MAC address) • If this check box is ticked, the left port will inherit its MAC address from its parent hardware port. • If this check box is unticked, the left port will not inherit its MAC address from its parent hardware port.
EDIT NAT PORT FORWARD TABLE button	When clicked, a **NAT Port Forwarding** page opens, letting you define port forwarding on the left port.
Right Port Properties	
IP Address field	This is a mandatory field, and defines the IP address of the right port, in the usual dotted notation (e.g. 192.168.2.197 or 192.168.1.254). This address can act as the gateway or routing port for other systems using the NE-ONE as their router.

Port Settings - Port Addressing Element	Description
Netmask field	This is a mandatory field, and defines the IP Network Mask in the usual dotted format e.g. 255.255.255.0 for a class C type address. As usual the (bitwise ANDed) combination of Address and Netmask define the Network (e.g. 192.168.2.0 or 192.168.1.0).
Gateway field	This is the IP address of the device (i.e. a router) you will use as your gateway for clients connected to the right port. This optional field lets you specify the IP address of another (i.e. not the NE-ONE) router in that network in the event that the network is more complex and requires further routing. For example, if a DHCP server is not within the network where the right port is connected then a Gateway would be required in order to route DHCP requests to it. • If you want the left port to act as a gateway itself, you can leave this field blank or specify 0.0.0.0. • If you want another device (i.e. a router) in your network to act as the gateway, specify the IP Address of that device.
DHCP Server field	This optional field is provided so that devices/clients connected to the right port requiring an IP address to be assigned by DHCP can have their "DHCP requests" relayed across the NE-ONE to the specified DHCP Server, even when no Point-to-Point network is running. This is explained in more detail in *Section 3-4-1-2, DHCP Server / DHCP Relay* on page 172. **Note:** You are not allowed to configure DHCP servers on both Ports in a Port Pair. Relaying DHCP requests goes in one direction – from either the Left Port to the Right Port to the DHCP server, or from the Right Port to the Left Port to the DHCP server. If you specify the IP address of a DHCP server in this field, the DHCP Server field for the Right Port becomes grayed out.
Accept Multicast check box	This check box optionally lets you decide whether multicast traffic is allowed through the right port. • If this check box is ticked, multicast traffic is allowed through the right port. • If this check box is not ticked, multicast traffic is not allowed through right left port.
NAT Outbound check box	This check box optionally lets you decide whether Network Address Translation (NAT) is applied to outbound traffic from clients connected to the right port. • If this check box is ticked, outbound client traffic through the right port is NATed. The NAT configuration is defined via clicking on the **EDIT NAT PORT FORWARD TABLE** button. • If this check box is unticked, outbound client traffic through the right port is not NATed.
Use Ethernet Address of Hardware Port check box	This check box optionally lets you decide whether the right port will inherit the MAC address of its parent hardware port. This is only required if the right port in the port pair is a soft port (since a hardware port will already have its own MAC address) • If this check box is ticked, the right port will inherit its MAC address from its parent hardware port. • If this check box is unticked, the right port will not inherit its MAC address from its parent hardware port.
EDIT NAT PORT FORWARD TABLE button	When clicked, a **NAT Port Forwarding** page opens, letting you define port forwarding on the right port.

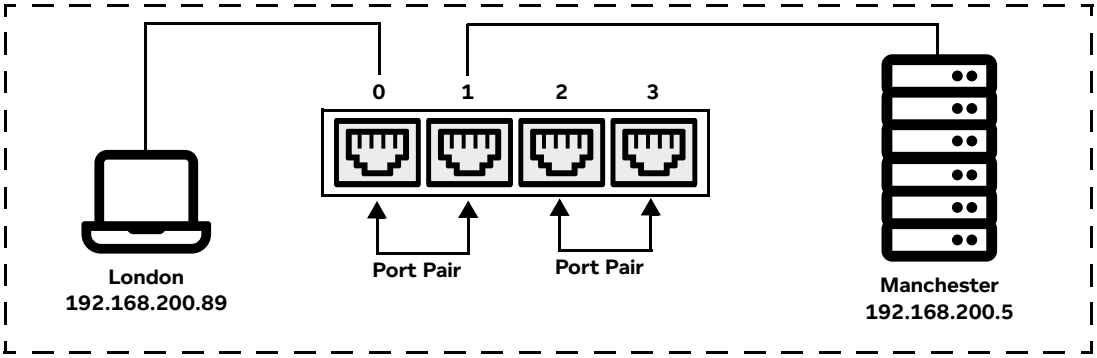
Notice:

If you make changes, then click **SET**, and the Port Addressing settings are immediately applied to the port pair. They will then be stored and return if the NE-ONE is rebooted.

If you make changes to an existing port pair's Port Addressing settings, be sure to communicate those changes to the users who use that port pair for their Point-to-Point networks. This is extremely important so that the users can create and edit their Point-to-Point networks corresponding with the Port Addressing settings of the port pair. For example, if a user had created a Point-to-Point networks with four computers with static IP addresses, with Link Qualifications defined for each of the four static IP addresses (see the example in *Creating Point-to-Point Networks (Single)* on page 265), you would not want to unknowing make that Point-to-Point network unusable for the user because you had changed the IP addresses of Port 0 and Port 1. In the case you changed the IP addresses of Port 0 and Port 1, the user of the Point-to-Point networks would have to update each computer's network settings to use a new static IP address and gateway, and also update their Link Qualification settings on each of the links to match the new static IP addresses of each computer.

By default, Port Addressing is disabled for a port pair, which means that the NE-ONE's hardware ports operate like a network switch (or bridge). Therefore, a device connected to Port 0 can be configured on the same subnet as Port 1 as shown in *Illustration 41*.

ILLUSTRATION 41 - EXAMPLE OF DEFAULT NETWORK SWITCH/BRIDGE PORT PAIR OPERATION

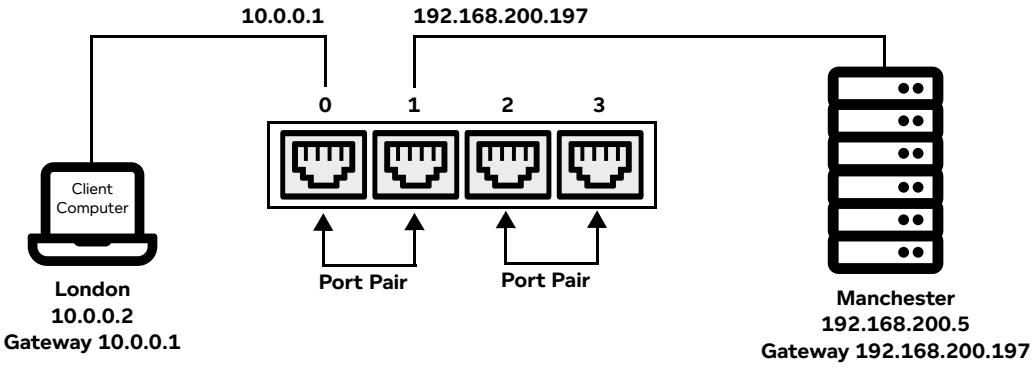


Same 192.168.200.x network. Therefore, no routing required (Port Pair 0 and 1 work in switch/bridge mode).

The port pair can also be configured to operate like a network router with each hardware port having its own IP Address. In the example shown in *Illustration 42* the client computer is now on a different subnet of 10.0.0.x with 10.0.0.1 configured on Port 0. The client computer must set its default gateway to 10.0.0.1 so that packets intended for other networks can be forwarded via Port 0. Conversely, the server must be configured to use 192.168.200.197 as its gateway so that it can send a response to the client.

ILLUSTRATION 42 - EXAMPLE OF PORT PAIR OPERATION WITH BASIC ROUTING

Different 10.0.0.x and 192.168.2.x networks. Therefore, routing required for Port Pair 0 and 1, configured by Port Addressing.



3-4-1-1. Configuring Port Addressing

Note:

The following procedure uses the network example of *Illustration 42*. Adapt the procedure to your actual networking needs.

Use the following steps to enable and configure Port Addressing on a pre-defined port pair:

1. From the Web Interface, access the **Port Settings** page via one of the following methods:

   Method 1 (quickest method):

   a. Under **Networks** in the menu, click on the appropriate port pair ↔.
   b. From the Network Port Pair page that appears, click **Port Settings**.

   Method 2 (only possible when the Port Manager feature is present):

   a. Click **Management > ↔ Port Pairs**.

      A **Port Pairs** page (*Illustration 38* on page 157) appears, containing a tile for each port pair.

      Each port pair tile contains a cog icon (⚙) letting you edit it, and a star icon (★) letting you favorite it.

   b. Click on the cog (⚙) corresponding to the port pair on which you want to configure port addressing.

      The right hand side of the **Port Pairs** page updates with a **Port Pair** panel (*Illustration 39* on page 158).

   c. Click on the **PORT SETTINGS** button.

   A **Port Settings** page appears with the **PORT ADDRESSING** tab active (*Illustration 41*).

2. Tick the **Enable** check box.
3. In the **Left Port Properties** area, do the following:
   a. In the **IP Address** field type the IP Address for the left port (in the example from *Illustration 42*, you would type **`10.0.0.1`**).
   b. In the **Netmask** field type the netmask of the network for the left port (in the example from *Illustration 42*, you would type **`255.255.255.0`**).
   c. In the **Gateway** field type the gateway of the network for the left port (in the example from *Illustration 42*, you would leave this blank or type **`0.0.0.0`**).
   d. In the **Relayed DHCP Server** field, optionally specify the IP address of the relayed DHCP Server

(in the example from *Illustration 42*, this would be blank).

e. If you want to allow multicast traffic through the right port, tick the **Accept Multicast** check box (in the example from *Illustration 42*, you would leave this unticked).

f. If you want the left port to automatically perform Network Address Translation (NAT) for the (outbound traffic of) clients connected on the left port, enable the **NAT Outbound** check box (in the example from *Illustration 42*, you would leave this unticked).

g. If you want the left port to inherit the MAC address of its parent hardware port, enable the **Use Ethernet Address of Hardware Port** check box (in the example from *Illustration 42*, you would leave this unticked).

4. In the **Right Port Properties** area, do the following:

a. In the **IP Address** field type the IP Address for the right port (in the example from *Illustration 42*, you would type **`192.168.200.197`**).

b. In the **Netmask** field type the netmask of the network for the right port (in the example from *Illustration 42*, you would type **`255.255.255.0`**).

c. In the **Gateway** field type the gateway of the network for the right port (in the example from *Illustration 42*, you would leave this blank or type **`0.0.0.0`**).

d. In the **Relayed DHCP Server** field, optionally specify the IP address of the relayed DHCP Server (in the example from *Illustration 42*, this would be blank).

e. If you want to allow multicast traffic through the right port, tick the **Accept Multicast** check box (in the example from *Illustration 42*, you would leave this unticked).

f. If you want the right port to automatically perform Network Address Translation (NAT) for the (outbound traffic of) clients connected on the left port, enable the **NAT Outbound** check box (in the example from *Illustration 42*, you would leave this unticked).

g. If you want the right port to inherit the MAC address of its parent hardware port, enable the **Use Ethernet Address of Hardware Port** check box (in the example from *Illustration 42*, you would leave this unticked).

5. Click **SET**.

   The Port Addressing settings are immediately applied and the ports will now respond to a ping request. The Port Addressing settings are persistent and will return after the NE-ONE is rebooted.

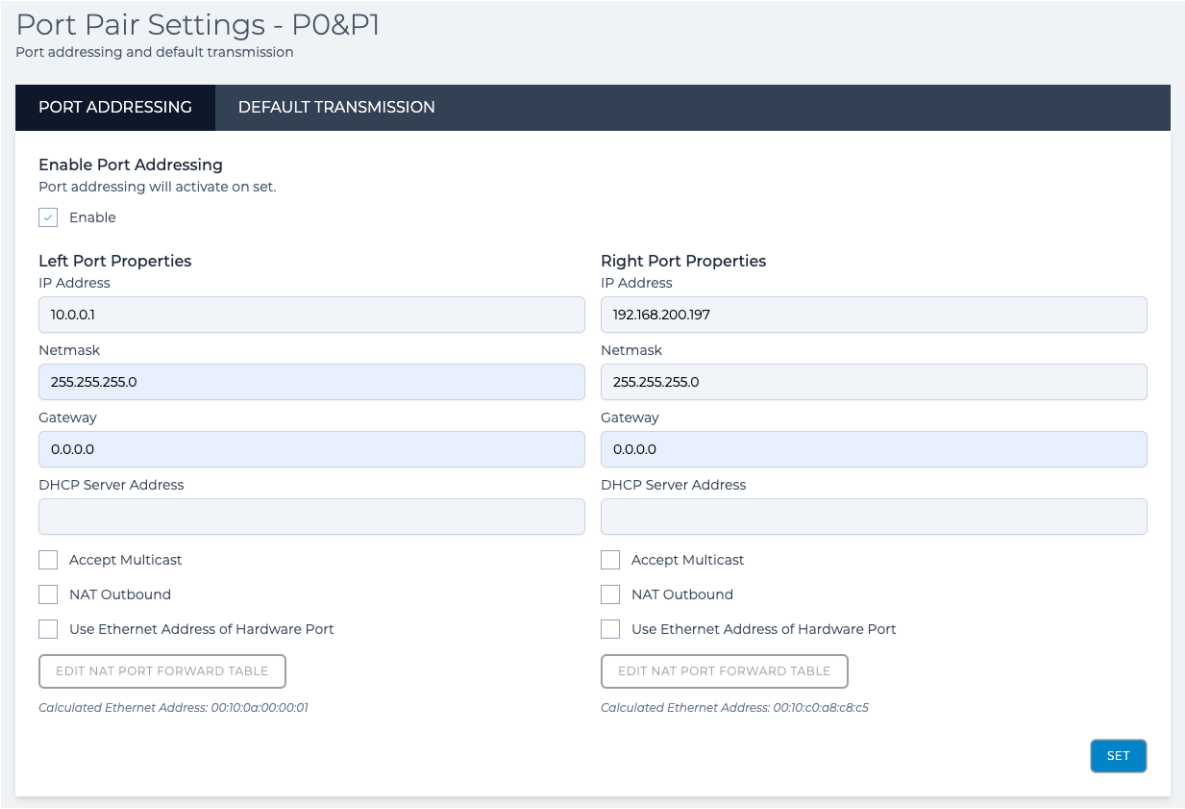
It is interesting to understand the effects of enabling and configuring Port Addressing on a port pair. Using the example from the steps above on a port pair called P0&P1 on hardware ports 0 (left) and 1 (right), and configuring Port Addressing will result with the **PORT ADDRESSING** tab will looking like that in *Illustration 43*, and the NE-ONE automatically creating the additional six System PPOs summarized in *Table 28*. These six additional System PPOs are visible in the **Statistics** page (*Illustration 45*).

TABLE 28 - ADDITIONAL PPOS AUTOMATICALLY CREATED WHEN ENABLING PORT ADDRESSING

PPO Type	PPO Name Format	PPO Name in our example	Description/relevance in our example
Soft Port	PP<Port Pair Name>_L	PPP0&P1_L	For the automatically created IPv4 soft port on the left port
Link	[<Parent Port> <--> Soft Port:IPv4] -> <Parent Port>	[0 <--> Soft Port:IPv4] -> 0	The associated link PPO that is also automatically created for the IPv4 soft port on the left port
Port Container	<Parent Port> <--> Soft Port:IPv4	0 <--> Soft Port:IPv4	The associated port container PPO that is also automatically created for the IPv4 soft port on the left port

PPO Type	PPO Name Format	PPO Name in our example	Description/relevance in our example
Soft Port	PP<Port Pair Name>_R	PPP0&P1_R	For the automatically created IPv4 soft port on the right port
Link	[<Parent Port> <--> Soft Port:IPv4] -> <Parent Port>	[1 <--> Soft Port:IPv4] -> 1	The associated link PPO that is also automatically created for the IPv4 soft port on the right port
Port Container	<Parent Port> <--> Soft Port:IPv4	1 <--> Soft Port:IPv4	The associated port container PPO that is also automatically created for the IPv4 soft port on the right port

ILLUSTRATION 43 - PORT ADDRESSING EXAMPLE ON A PORT PAIR



Enabling and configuring Port Addressing results in the NE-ONE automatically doing the following:

- Creating a child IPv4 soft port whose name is of the format **PP<Port Pair Name>_L** on the left port. In our example, the child IPv4 soft port that is automatically created is called **PPP0&P1_L**.

  The automatically created child IPv4 soft port **PP<Port Pair Name>_L** will appear in the **Port Manager** page (*Illustration 44*), and inherit the **Left Port Properties** (IP Address, Netmask, etc.) that were defined in the **PORT ADDRESSING** tab of the **Port Pair Settings** page (*Illustration 43*).

  The automatically created child IPv4 soft port **PP<Port Pair Name>_L** will also appear in the **Statistics** page (*Illustration 45*).

  The automatically created child IPv4 soft port **PP<Port Pair Name>_L** also has an automatically created link PPO of the format **[<Parent Port> <--> Soft Port:IPv4] -> <Parent Port>** that also appears in the **Statistics** page (*Illustration 45*). In our example, it is called **[0 <--> Soft Port:IPv4] -> 0** since it is on hardware port 0.

  The automatically created child IPv4 soft port **PP<Port Pair Name>_L** also has an automatically

created port container PPO of the format **<Parent Port> <--> Soft Port:IPv4]** that also appears in the **Statistics** page (*Illustration 45*). In our example, it is called **0 <--> Soft Port:IPv4** since it is on hardware port 0.

- Creating a child IPv4 soft port whose name is of the format **PP<Port Pair Name>_R** on the right port. In our example, the child IPv4 soft port that is automatically created is called **PPP0&P1_R**.

  The automatically created child IPv4 soft port **PP<Port Pair Name>_R** will appear in the **Port Manager** page (*Illustration 44*), and inherit the **Right Port Properties** (IP Address, Netmask, etc.) that were defined in the **PORT ADDRESSING** tab of the **Port Pair Settings** page (*Illustration 43*).

  The automatically created child IPv4 soft port **PP<Port Pair Name>_R** will also appear in the **Statistics** page (*Illustration 45*).

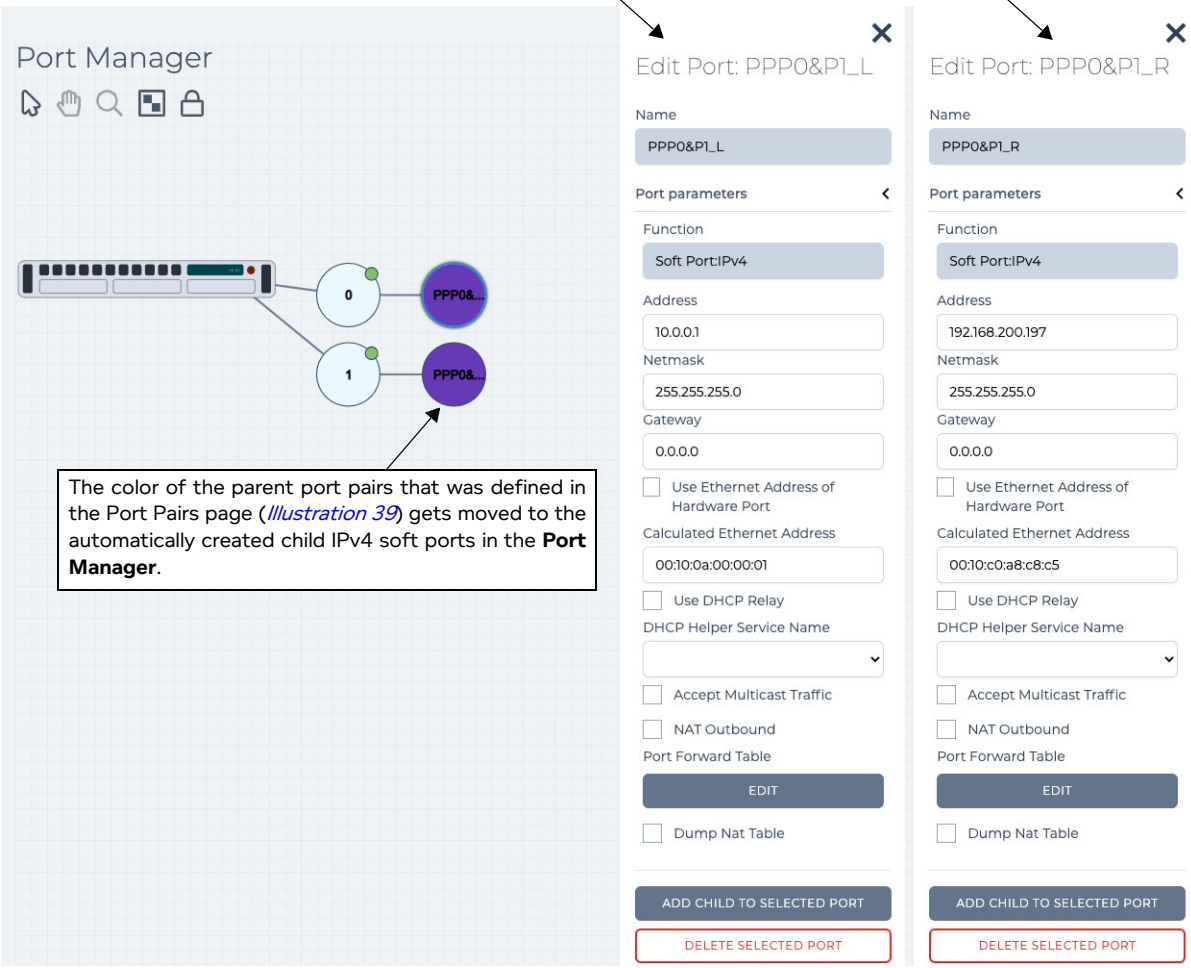
  The automatically created child IPv4 soft port **PP<Port Pair Name>_R** also has an automatically created link PPO of the format **[<Parent Port> <--> Soft Port:IPv4] -> <Parent Port>** that also appears in the **Statistics** page (*Illustration 45*). In our example, it is called **[1 <--> Soft Port:IPv4] -> 1** since it is on hardware port 1.

  The automatically created child IPv4 soft port **PP<Port Pair Name>_R** also has an automatically created port container PPO of the format **<Parent Port> <--> Soft Port:IPv4]** that also appears in the **Statistics** page (*Illustration 45*). In our example, it is called **1 <--> Soft Port:IPv4** since it is on hardware port 1.
- Within the **Port Manager** page (*Illustration 44*), the color that was originally assigned to the parent port pair gets moved to the automatically created child IPv4 soft ports **PP<Port Pair Name>_L** and **PP<Port Pair Name>_R**.

ILLUSTRATION 44 - PORT ADDRESSING IMPACT ON THE PORT MANAGER PAGE

The properties of the automatically created child IPv4 soft port of the parent left port in the **Port Manager** page are inherited from the **Left Port Properties** that were defined in the **PORT ADDRESSING** tab of the **Port Pair Settings** page (*Illustration 43*).

The properties of the automatically created child IPv4 soft port of the parent right port in the **Port Manager** page are inherited from the **Right Port Properties** that were defined in the **PORT ADDRESSING** tab of the **Port Pair Settings** page (*Illustration 43*).



The color of the parent port pairs that was defined in the Port Pairs page (*Illustration 39*) gets moved to the automatically created child IPv4 soft ports in the **Port Manager**.

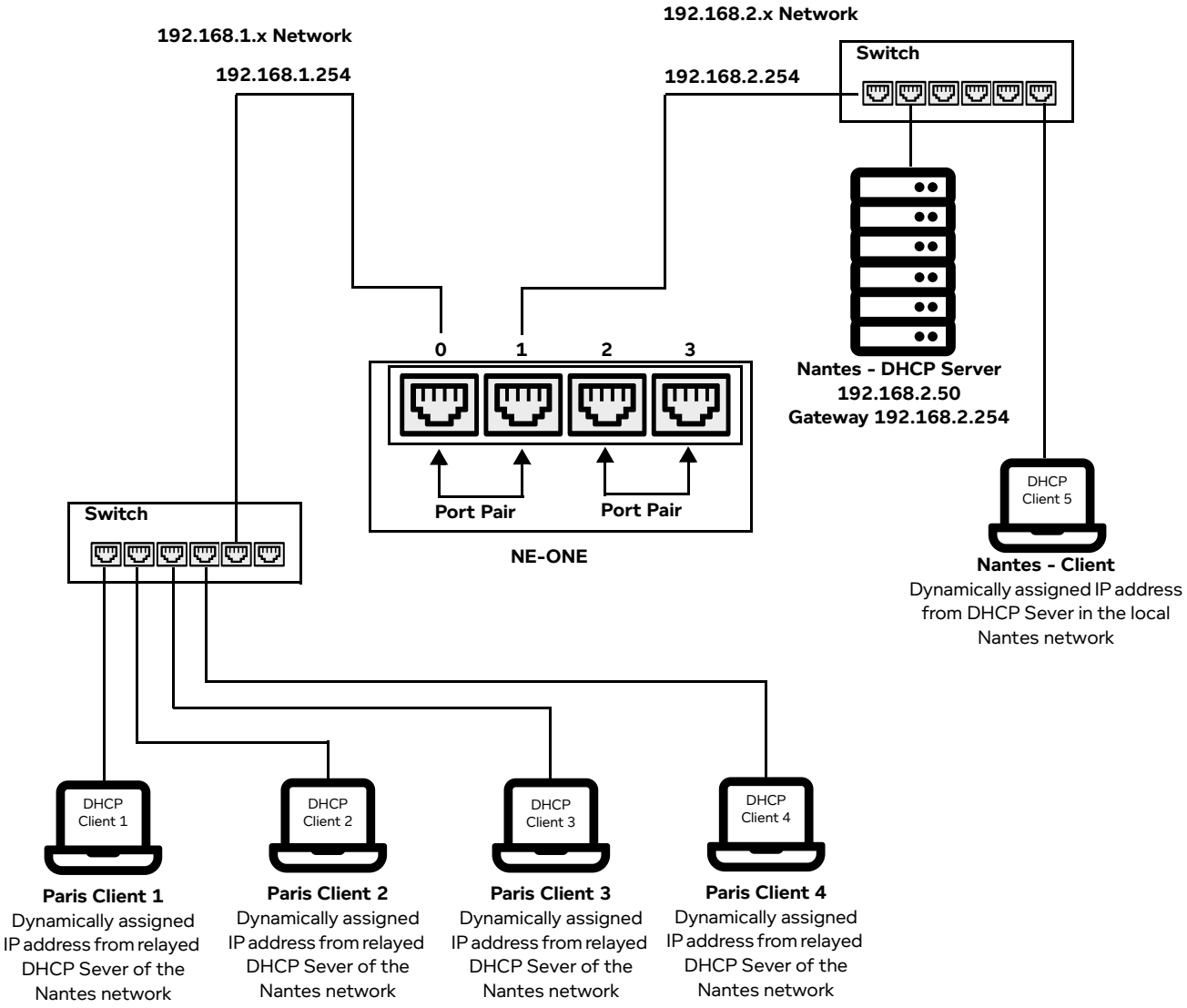
ILLUSTRATION 45 - PORT ADDRESSING IMPACT ON THE STATISTICS PAGE

3-4-1-2. DHCP Server / DHCP Relay

As discussed briefly in *Section 3-4-1-1, Configuring Port Addressing* and in *Table 27* on page 163, the purpose of the **DHCP Server** field is to specify a DHCP Server in the network (subnet) which will provide IP addresses for the DHCP clients in the opposite network (subnet). To explain this further consider the following example.

The example in *Illustration 46* illustrates how the Nantes network connected to Port 1 has a DCHP Server with an IP Address of 192.168.2.50, which provides IP addresses to both DHCP clients in its own Nantes network 192.168.2.x connected to Port 1 and to DHCP clients in the opposite Paris network 192.168.1.x connected to Port 0.

ILLUSTRATION 46 - PORT ADDRESSING WITH DHCP SERVER IN ONE NETWORK RELAYED TO ANOTHER NETWORK



The IP addressing in this example is as follows (no complex Gateways are used) :

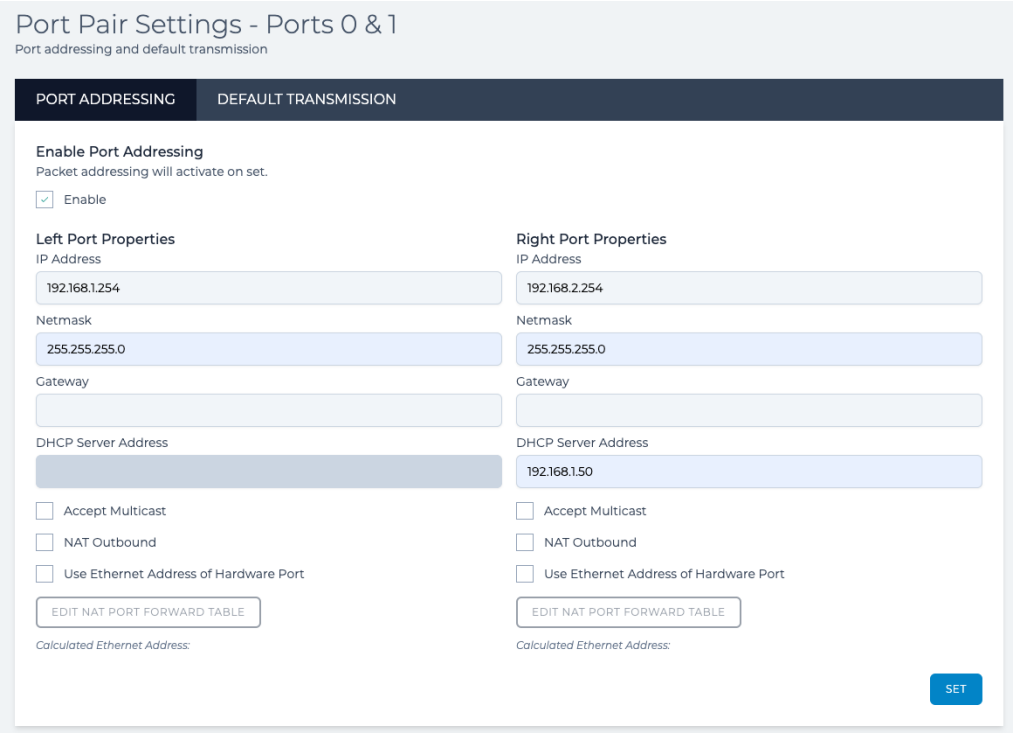
- Port 0 (which is considered the Gateway for network 192.168.1.x) has the IP address 192.168.1.254
- Port 1 (which is considered the Gateway for network 192.168.2.x) has the IP address 192.168.2.254
- DHCP server address is 192.168.2.50.

The Port Pair configuration in this example is as follows:

- The Left Port is assigned to Port 0.
- The Right Port is assigned to Port 1.

Then the corresponding Port Addressing settings for the port pair would be as show in *Illustration 47*.

ILLUSTRATION 47 - PORT ADDRESSING SETTINGS FOR A DHCP SERVER IN ONE NETWORK RELAYED TO ANOTHER NETWORK



Notes:

1. The IP address settings are different to the first example (which used 10.0.0.x network for Port 0 and 192.168.200.x for the Port 1 network), and we have added the address of the DHCP Server to the port to which it is connected.
2. The Gateway is optional as usual, but if the DHCP server was not in the network 192.168.2.0 then it would be required in order to route DHCP requests to it. In our example this is not the case.
3. You are not allowed to configure DHCP servers on both Ports in a Port Pair. Relaying DHCP requests goes in one direction – from Port 0 to Port 1 to the DHCP server in this example.

How it works:

DHCP requests are broadcast messages, and as soon as the DHCP server is defined for Port 1 (and **SET** clicked), then Port 0 (the opposite port in the pair listens for these requests and relays them to Port 1 having first inserted its address (192.168.1.254 in this case) into the DHCP requests Gateway field. This is done so the DHCP server knows which network is requesting addresses, and it can allocate an appropriate one for that subnet.

Port 1 now transmits the request as a DHCP relay directly (no broadcasting) to the DHCP server you specified, either directly (as in our example) or via the Gateway, if required.

The DHCP server responds with a suitable offer of address and sends this back to Port 1's IP address. Port 1 forwards the packets back to Port 0 which sends them to the requesting host.

This meets the DHCP relay standard.

Notes:

1. This process works even if no Point-to-Point network is running – packets are sent directly between the NE-ONE's ports. This means addresses can be obtained as soon as the DHCP setup is completed.
2. DHCP requests are not subject to Link characteristics like Latency, Loss etc. as they do not pass

through the Links.

3. Because the reply from the DHCP server will be directly sent to the address on Port 0 (192.168.1.254) in our example, the DHCP server must have a route defined to the subnet 192.168.1.0 which will go via 192.168.2.254.
4. Suitable DHCP ranges must be defined in the DHCP server for network 192.168.1.0, as by default they only usually allocate addresses for the networks they are in (192.168.2.0 in our example).

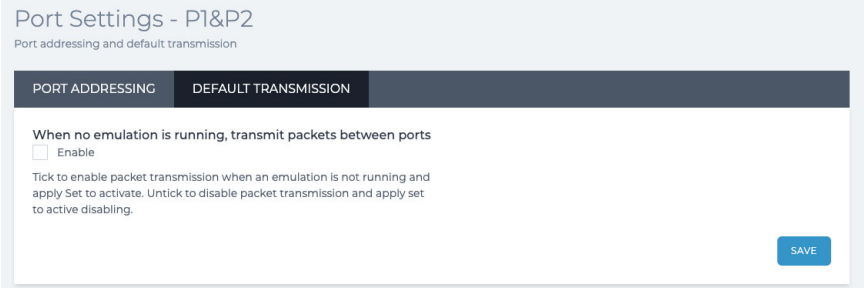
3-4-2. Default Transmission

The NE-ONE's pre-defined port pairs can operate in one of the following ways:

- Default Transmission is disabled: traffic can only pass through the pre-defined port pair when a Point-to-Point network is configured and started on that pre-defined port pair
- Default Transmission is enabled (and running): traffic can still pass through the pre-defined port pair even when a Point-to-Point network is not running on that pre-defined port pair

By default, the Default Transmission service is disabled on a pre-defined port pair.

ILLUSTRATION 48 - PORT SETTINGS PAGE - DEFAULT TRANSMISSION TAB



Default Transmission is configurable per individual pre-defined port pair (either hardware port pairs, or soft port pairs). For example, you can have Default Transmission enabled on one pre-defined port pair (e.g. on hardware ports 0 and 1), and have Default Transmission disabled on another pre-defined port pair (e.g. on hardware ports 2 and 3).

If the Default Transmission service is enabled on a pre-defined port pair it is listed in as a Service type framework object in the Statistics table of the **Statistics** page (*Illustration 160* on page 527). The object name of a pre-defined port pair's Default Transmission service has the format `Default_Transmission_PP_<Port Pair Name>`.

The **DEFAULT TRANSIMISSION** tab of the **Port Settings** page (*Illustration 42* on page 167) contains an **Enable** check box, and a **SAVE** button.

- If the **Enable** check box is ticked, the Default Transmission service is active and running on the pre-defined port par.
- If the **Enable** check box is ticked, the Default Transmission service is inactive and not running on the pre-defined port par.

Note:

Since Default Transmission is a service, if it is enabled for a pre-defined port pair it is also accessible from within the **Service Manager** page (*Illustration 49* on page 177) from where it can be edited (i.e. port pair assignments changed) or deleted (i.e. disabled). If the port assignments of an existing Default Transmission service are modified from within the **Service Manager** page, the **Enable** check box for the original port pair it was assigned to becomes unticked because the Default Transmission service is now assigned to another port pair. Similarly, if an existing Default Transmission service is deleted from within the **Service Manager** page, the **Enable** check box for the original port pair it was assigned to becomes unticked because the Default Transmission service is now deleted.

3-4-2-1. Configuring (Enabling or Disabling) Default Transmission on a Port Pair

Use the following steps to configure (enable or disable) the Default Transmission service on a pre-defined port pair:

1. From the Web Interface, click **Management > Port Pairs**.
1. From the Web Interface, access the **Port Settings** page via one of the following methods:

   Method 1 (quickest method):

   a. Under **Networks** in the menu, click on the appropriate port pair.
   b. From the Network Port Pair page that appears, click **Port Settings**.

   Method 2 (only possible when the Port Manager feature is present):

   a. Click **Management > Port Pairs**.

      A **Port Pairs** page (*Illustration 38* on page 157) appears, containing a tile for each port pair.

      Each port pair tile contains a cog icon ( ) letting you edit it, and a star icon ( ) letting you favorite it.

   b. Click on the cog ( ) corresponding to the port pair on which you want to configure port addressing.

      The right hand side of the **Port Pairs** page updates with a **Port Pair** panel (*Illustration 39* on page 158).

   c. Click on the **PORT SETTINGS** button.

   A **Port Settings** page appears with the **PORT ADDRESSING** tab active (*Illustration 41* on page 166).
2. Click the **DEFAULT TRNASMISSION** tab to show the current Default Transmission settings for the pre-defined port pair (*Illustration 48* on page 175).
3. Configure the Default Transmission service for the selected pre-defined port pair according to your requirements, as follows:
   - If you want the Default Transmission service to be running on the pre-defined port pair, tick the **Enable** check box.
   - If you do not want the Default Transmission service to be running on the pre-defined port pair, untick the **Enable** check box.
4. Click **SAVE** to store the Default Transmission settings for the pre-defined port pair.

   If the Default Transmission service was enabled for the pre-defined port pair, it starts immediately and is listed as a framework object in the **Statistics** page (*Illustration 160* on page 527). Traffic can now only pass through the selected pre-defined port pair when a Point-to-Point network is configured and started on that pre-defined port pair.

   If the Default Transmission service was disabled for the pre-defined port pair, it stops immediately and is no longer listed as a framework object in the **Statistics** page (*Illustration 160* on page 527). Traffic can now still pass through the selected pre-defined port pair even when a Point-to-Point network is not running on that pre-defined port pair.

3-4-2-2. Determining Whether Default Transmission is Active on a Port Pair

To determine whether Default Transmission is active on a pre-defined port pair, you could simply use the steps described in *Section 3-4-2-1, Configuring (Enabling or Disabling) Default Transmission on a Port Pair* on page 176 and observe current state of the **Enable** check box.

Alternatively, you could also use the **Statistics** page (*Illustration 160* on page 527) to apply a **Service** object filter, and look for any Default Transmission services that would be listed with the Service framework objects naming format: `Default_Transmission_PP_<Port Pair Name>`.

4. MANAGING SERVICES

Note:

This section is only applicable to the NE-ONE with the Service Manager feature activated. Depending on your license, the Service Manager feature may be activated or deactivated.

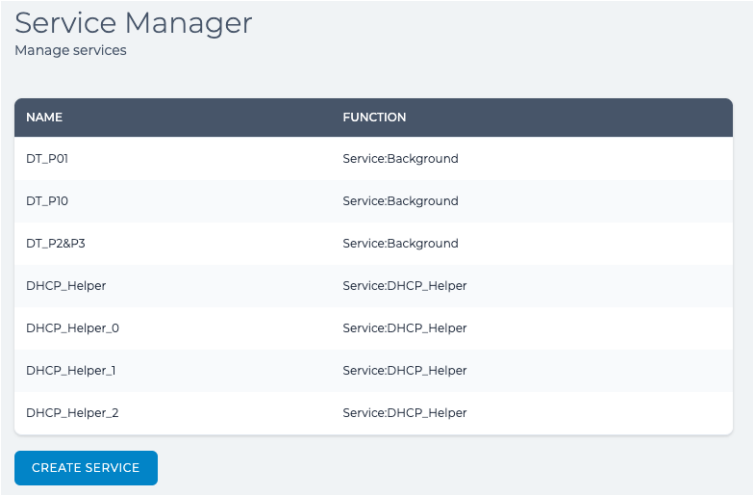
Services are an additional capability that in many ways function like soft ports (see *Available Soft Port Functions* on page 96), in that they are independent of running networks. Unlike soft ports they are not directly associated with any particular hardware.

4-1. The Service Manager Page

Services are centrally managed (i.e. created, deleted, and edited) via the **Service Manager** page (*Illustration 49*).

To launch the **Service Manager** page, select **Management > Service Manager**.

ILLUSTRATION 49 - SERVICE MANAGER PAGE



The **Service Manager** page contains the following elements:

- **CREATE SERVICE** button - clicking this button opens a **Create Service** page, from where you can select an available service (see *Available Services Functions* on page 101) and define it according to your requirements.
- Services table listing all of the services (if any) that have been created on the NE-ONE. Clicking on a service in the table opens an **Edit Service** page, from where you can either edit the service or delete the service.

The following sections describe the service functions that are available to NE-ONE, and how to create services (with examples). By default, no services are created or active on the NE-ONE. You need to decide what services you want to create (see *Creating Services* on page 178).

Once a service is created on the NE-ONE, it runs in the background as a framework object. As described previously within in *Chapter 2*, *NE-ONE Overview*, the NE-ONE uses two types of objects; namely framework objects and network objects. A service is considered a framework object as it creates an underlying networking framework (such as a DHCP helper service, or managed routing between ports, etc.) on which user created networks may operate with, but users cannot themselves select a service when creating their networks (they only select network objects (i.e. nodes and links)).

4-2. Creating Services

Use one of the following sections, according to the type of service function that you want to create. For more information on service functions, see *Available Services Functions* on page 101.

Note:
The sections below provide example networks. Adapt the examples to your actual networking needs.

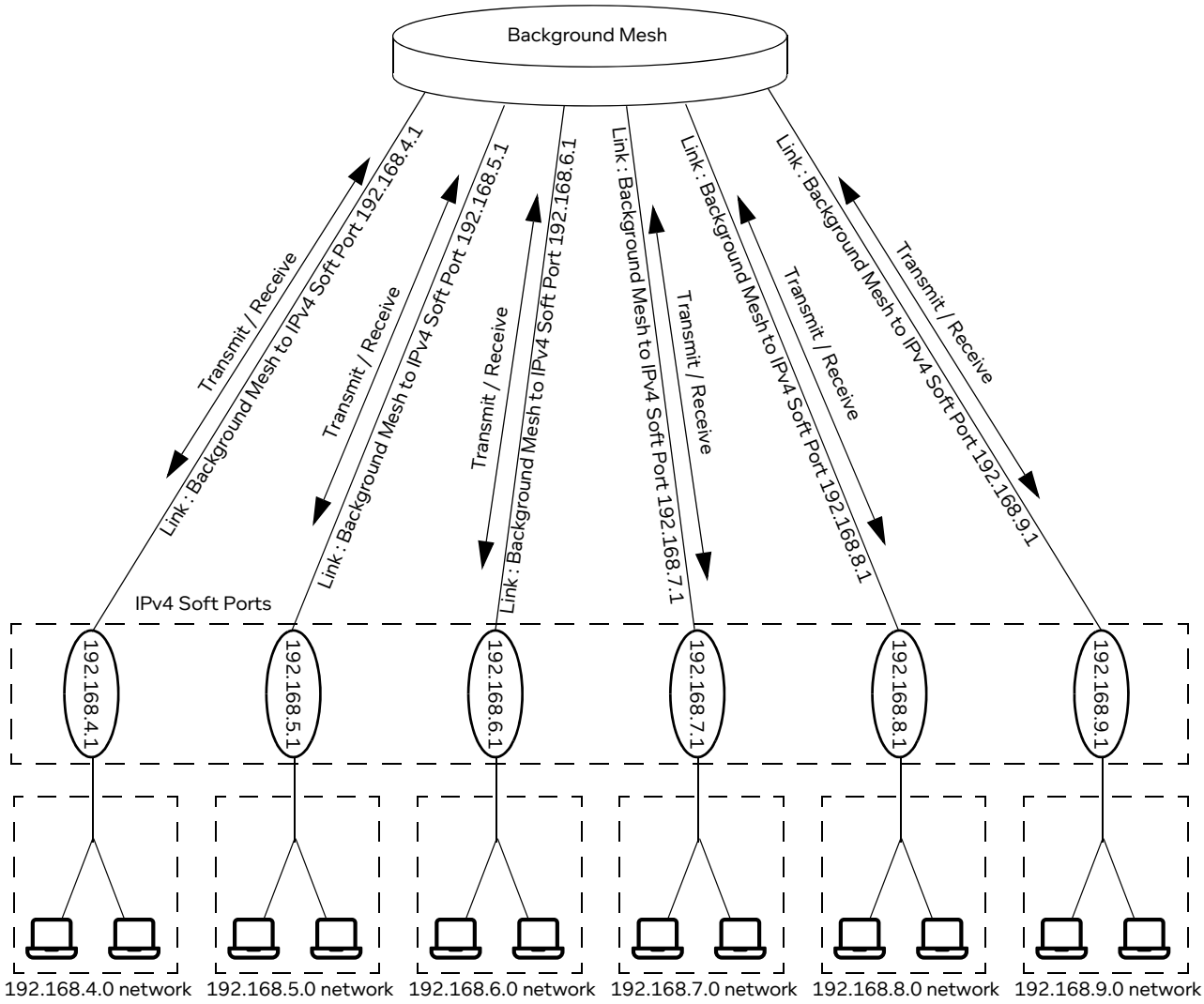
4-2-1. Creating a Background Expression Routed service

The example below shows the use of the Background Expression Routed service to create a mesh transmission between six ports.

Note:
If the requirement is simply to connect ports in pairs (i.e. port pairs) then the simpler and more efficient Background service should be used. This service only operates on pairs of ports (i.e. port pairs), and for the maximum efficiency it is recommended that in this case one service is created per port pair per direction. For more information, see *Creating a Background Service* on page 190.

Suppose that we have six IPv4 soft ports called 192.168.4.1, 192.168.5.1, 192.168.6.1, IPv4_192.168.7.1, 192.168.8.1 and 192.168.9.1 (as per the example described in *Creating an IPv4 Soft Port* on page 114) and we wish to bind them together in a fully meshed background service (where any port in the list can transmit and receive from any other port).

ILLUSTRATION 50 - EXAMPLE BACKGROUND MESH SERVICE WITH SIX IPV4 SOFT PORTS CONNECTED TOGETHER VIA THE SERVICE : BACKGROUND EXPRESSION ROUTED FUNCTION



The procedure below assumes that six IPv4 soft ports have been set up using the Port Manager, with the following names:

- 192.168.4.1 for the IPv4 soft port with IP Address 192.168.4.1
- 192.168.5.1 for the IPv4 soft port with IP Address 192.168.5.1
- 192.168.6.1 for the IPv4 soft port with IP Address 192.168.6.1
- 192.168.7.1 for the IPv4 soft port with IP Address 192.168.7.1
- 192.168.8.1 for the IPv4 soft port with IP Address 192.168.8.1
- 192.168.9.1 for the IPv4 soft port with IP Address 192.168.9.1

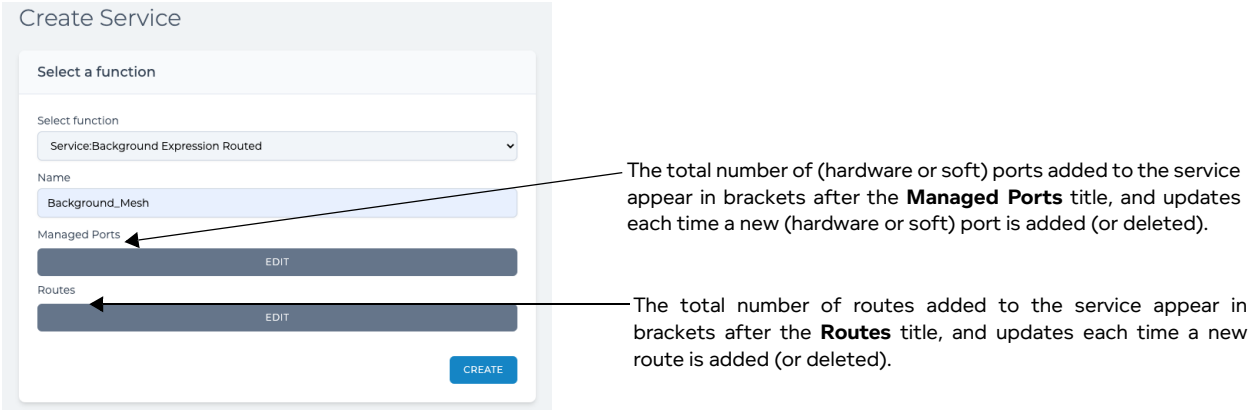
For more example of setting up IPv4 soft ports, see *Creating an IPv4 Soft Port* on page 114.

Use the following steps to create a Background Expression Routed service based on the example above (for your own network, adapt the procedure accordingly):

1. From the Web Interface, click **Management > Service Manager**.
   A **Service Manager** page appears displaying a list of services that have been added (if any exist) to the NE-ONE

2. Click the **CREATE SERVICE** button.
3. From the **Create Service** page that appears, select **Service:Background_Expression_Routed** from the **Select function** field.

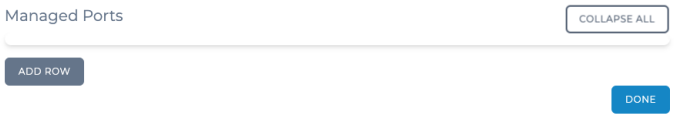
   The **Create Service** page updates with elements associated with configuring Background Expression Routed service.



   Initially, no managed ports or routes exist in the service. As managed (hardware or soft) ports and routes are added to the service, their totals appear in brackets after the **Managed Ports** and **Routes** titles in the **Create Services** page.
4. In the **Name** field, type an appropriate service name to represent the service you are creating (for our example, type **`Background_Mesh`**). The **Name** field accepts alpha-numeric characters, special characters (except \, / and *), and spaces. The name that you specify is also used by the service file that gets created for the service.

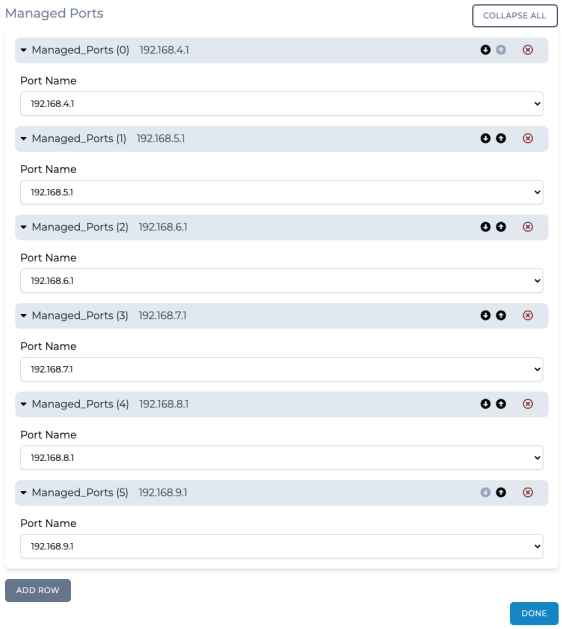
   At this stage we need to add the six IPv4 soft ports to the Background Expression Routed service.
5. Click the **Managed Ports EDIT** button.

   An empty **Managed Ports** dialog box appears, letting you define the ports in the Background Expression Routed service.

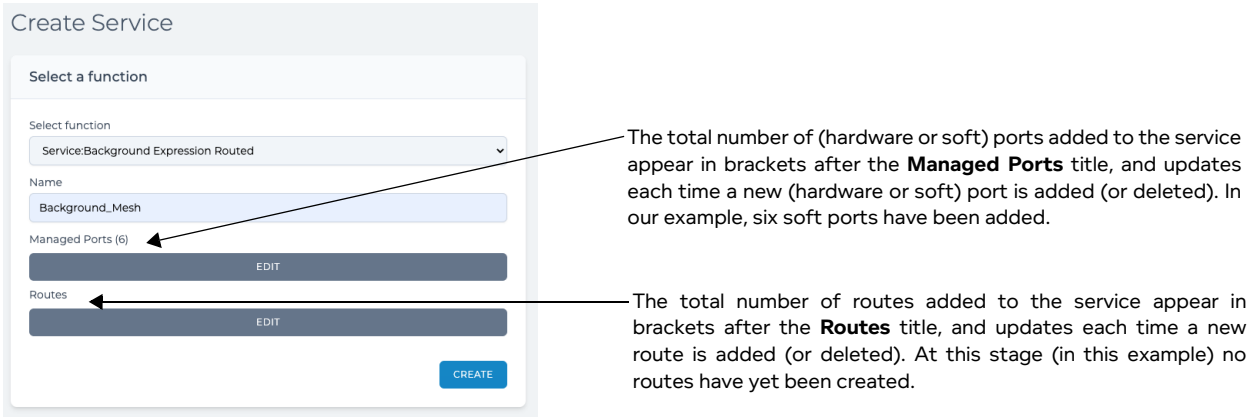


6. From the **Managed Ports** dialog box that appears, do the following:
   a. Click **ADD ROW**.
      A **Managed_Ports (0)** row appears with a Port Name field in the **Managed Ports** dialog box.
   b. In the **Managed_Ports (0)**, select **192.168.4.1** from the **Port Name** drop-down field.
   c. Click **ADD ROW**.
      A **Managed_Ports (1)** row appears with a Port Name field in the **Managed Ports** dialog box.
   d. In the **Managed_Ports (1)**, select **192.168.5.1** from the **Port Name** drop-down field.
   e. Click **ADD ROW**.
      A **Managed_Ports (2)** row appears with a Port Name field in the **Managed Ports** dialog box.
   f. In the **Managed_Ports (2)**, select **192.168.6.1** from the **Port Name** drop-down field.
   g. Click **ADD ROW**.
      A **Managed_Ports (3)** row appears with a Port Name field in the **Managed Ports** dialog box.
   h. In the **Managed_Ports (3)**, select **192.168.7.1** from the **Port Name** drop-down field.

i. Click **ADD ROW**.
   A **Managed_Ports (4)** row appears with a Port Name field in the **Managed Ports** dialog box.
j. In the **Managed_Ports (4)**, select **192.168.8.1** from the **Port Name** drop-down field.
k. Click **ADD ROW**.
   A **Managed_Ports (5)** row appears with a Port Name field in the **Managed Ports** dialog box.
l. In the **Managed_Ports (5)**, select **192.168.9.1** from the **Port Name** drop-down field.
m. Click **ADD ROW**.
   At this stage, all the six soft ports have been added to the Expression : Background Expression Routed service.

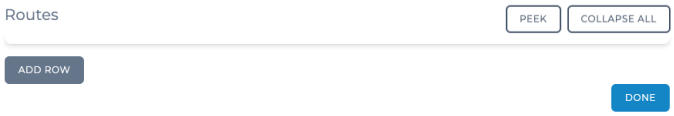


7. Click **DONE** to return to **Create Service** page.
   The **Create Service** page appears, and now contains the six soft ports that you added.



   You now have to define the routing relationship between these soft ports. This is done via the Routes Array (List) Editor, where you now need to add routes which will connect the appropriate soft ports together as required.
8. Click the **Routes EDIT** button.
   An empty **Routes** dialog box appears, letting you define the routes in the Background Expression

Routed service. Initially the **Routes** dialog box is empty as no routes currently exist.

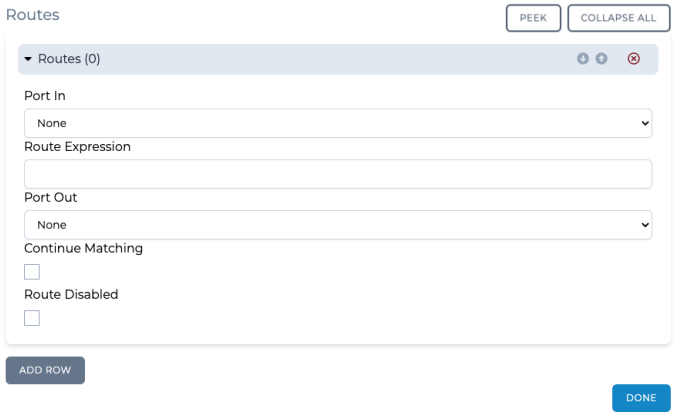


Clicking on the **ADD ROW** button results in creating **Routes (0)** row (*Illustration 51*), letting you add a route, and define its properties (see *Table 29* on page 182).

Note:

When creating services, the **PEEK** button is visible but intentionally inactive.

ILLUSTRATION 51 - ROUTE ROW WITHIN THE ROUTES DIALOG BOX



The **Routes (0)** row contains the elements in *Table 29*.

TABLE 29 - ROUTE PROPERTIES DIALOG BOX ELEMENTS

Route Properties dialog Box Element	Description
Port In drop-down field	Defines the in port for the route (i.e. the port the packet was received on). The list of ports contains at least all the hardware ports (i.e. **0**, **1**, **2**, **3**, etc.) and **None**. If soft ports have been created by an admin user (which is normally the case, and the case in our example), the names given to each of the created soft ports are listed. If **None** is selected, it is the equivalent of selecting all ports, rather than a particular port. Typically (as in our example), you choose **None** for the in port when binding together all ports when creating a fully meshed background service (where any port in the list can transmit and receive from any other port).

Route Properties dialog Box Element	Description
Route Expression field	This field lets you define the routing expression on the route, using Wireshark syntax. Any packets of data matching the route expression will be routed to the selected out port of the route. This field does not support `ip route` syntax, but rather Wireshark style of routing syntax. For example, if we want to create an IPv4 style routing table so that any port could be routed to any port, in `ip route` syntax terms we might want a routes like: `ip route add 192.168.1.0/24 dev eth0` Being more specific if our soft port IPv4_192.168.4.1 had an IP address of the same value (i.e. 192.168.4.1) and a netmask of 255.255.255.0 (/24) then in `ip route` syntax, a suitable route would be: `ip route add 192.168.4.0/24 dev 192.168.4.1` (because our soft port is in effect a device). However, the **Route Expression** field does not support `ip route` syntax, but rather a Wireshark style of syntax. Therefore, we can express this `ip route` with an expression rule in a very similar way, using the Wireshark syntax as follows: `ipv4.dst & 255.255.255.0 = 192.168.4.0` **Note:** Expression syntax is far more powerful than this and can access many packet properties - see *Appendix 1*, *Specifying Expressions* on page 731 for more information on expression syntax.
Port Out drop-down field	Defines the port to send the packet to if it matches the rule defined in the Route Expression field. The list of ports contains at least all the hardware ports (i.e. **0**, **1**, **2**, **3**, etc.) and **None**. If soft ports have been created by an admin user (which is normally the case, and the case in our example), the names given to each of the created soft ports are listed. If **None** is selected, it is the equivalent of selecting all ports, rather than a particular port. Typically (as in our example), you would choose a specific port.
Continue Matching check box	This check box defines whether or not a packet (which matched the route expression) can be sent to more than one route. The default setting is off (unticked). • When unticked (i.e. off), a packet matching the route expression can not be sent to more than one route • When ticked (i.e. on), a packet matching the route expression can be sent to more than one route Normally (like in the case of our example), continue matching is set to off (unticked).
Route Disabled check box	This check box defines whether or not the route is enabled or disabled, and thus lets you disable the route without actually deleting it from the **Routes** dialog box. • When unticked, the route is enabled (i.e. route disabled is off/false) • When ticked, the route is disabled (i.e. route disabled is on/true) Normally (like in the case of our example), route disable is set to off (unticked).

9. From the **Routes** dialog box that appears, click **ADD ROW** to add the first route. From the **Routes (0)** row that appears, do the following:
   a. From the **Port In** drop-down field, select the input port for the first route. In our example, since it is a mesh, leave the **Port In** drop-down field set to **None**.

b. In the **Route Expression** field, type the Wireshark syntax expression for the first route. In our example, type: **`ipv4.dst & 255.255.255.0 = 192.168.4.0`**
c. From the **Port Out** drop-down field, select the output port for the first route. In our example, select **192.168.4.1** (i.e. the first soft port).
d. Leave the **Continue Matching** check box unticked (i.e. continue matching disabled). This is because our example will not allow packets to be sent to more than one route.
e. Leave the **Route Disabled** check box unticked (i.e. the route is enabled). This is because our example wants the first route enabled.

10. From the **Routes** dialog, click **ADD ROW** to add the second route. From the **Routes (1)** row that appears, do the following:
    a. From the **Port In** drop-down field, select the input port for the second route. In our example, since it is a mesh, leave the **Port In** drop-down field set to **None**.
    b. In the **Route Expression** field, type the Wireshark syntax expression for the second route. In our example, type: **`ipv4.dst & 255.255.255.0 = 192.168.5.0`**
    c. From the **Port Out** drop-down field, select the output port for the second route. In our example, select **192.168.5.1** (i.e. the second soft port).
    d. Leave the **Continue Matching** check box unticked (i.e. continue matching disabled). This is because our example will not allow packets to be sent to more than one route.
    e. Leave the **Route Disabled** check box unticked (i.e. the route is enabled). This is because our example wants the second route enabled.
11. From the **Routes** dialog box, click **ADD ROW** to add the third route. From the **Routes (2)** row that appears, do the following:
    a. From the **Port In** drop-down field, select the input port for the third route. In our example, since it is a mesh, leave the **Port In** drop-down field set to **None**.
    b. In the **Route Expression** field, type the Wireshark syntax expression for the third route. In our example, type: **`ipv4.dst & 255.255.255.0 = 192.168.6.0`**
    c. From the **Port Out** drop-down field, select the output port for the first route. In our example, select **192.168.6.1** (i.e. the third soft port).
    d. Leave the **Continue Matching** check box unticked (i.e. continue matching disabled). This is because our example will not allow packets to be sent to more than one route.
    e. Leave the **Route Disabled** check box unticked (i.e. the route is enabled). This is because our example wants the third route enabled.
12. From the **Routes** dialog box, click **ADD ROW** to add the fourth route. From the **Routes (3)** row that appears, do the following:
    a. From the **Port In** drop-down field, select the input port for the fourth route. In our example, since it is a mesh, leave the **Port In** drop-down field set to **None**.
    b. In the **Route Expression** field, type the Wireshark syntax expression for the fourth route. In our example, type: **`ipv4.dst & 255.255.255.0 = 192.168.7.0`**
    c. From the **Port Out** drop-down field, select the output port for the fourth route. In our example, select **192.168.7.1** (i.e. the first soft port).
    d. Leave the **Continue Matching** check box unticked (i.e. continue matching disabled). This is because our example will not allow packets to be sent to more than one route.
    e. Leave the **Route Disabled** check box unticked (i.e. the route is enabled). This is because our example wants the fourth route enabled.
13. From the **Routes** dialog box, click **ADD ROW** to add the fifth route. From the **Routes (4)** dialog box

that appears, do the following:

a. From the **Port In** drop-down field, select the input port for the fifth route. In our example, since it is a mesh, leave the **Port In** drop-down field set to **None**.

b. In the **Route Expression** field, type the Wireshark syntax expression for the fifth route. In our example, type: **`ipv4.dst & 255.255.255.0 = 192.168.8.0`**

c. From the **Port Out** drop-down field, select the output port for the first route. In our example, select **192.168.8.1** (i.e. the fifth soft port).

d. Leave the **Continue Matching** check box unticked (i.e. continue matching disabled). This is because our example will not allow packets to be sent to more than one route.

e. Leave the **Route Disabled** check box unticked (i.e. the route is enabled). This is because our example wants the fifth route enabled.

14. From the **Routes** dialog box that appears, click **ADD ROW** to add the sixth route. From the **Routes (5)** row that appears, do the following:

a. From the **Port In** drop-down field, select the input port for the sixth route. In our example, since it is a mesh, leave the **Port In** drop-down field set to **None**.

b. In the **Route Expression** field, type the Wireshark syntax expression for the sixth route. In our example, type: **`ipv4.dst & 255.255.255.0 = 192.168.9.0`**

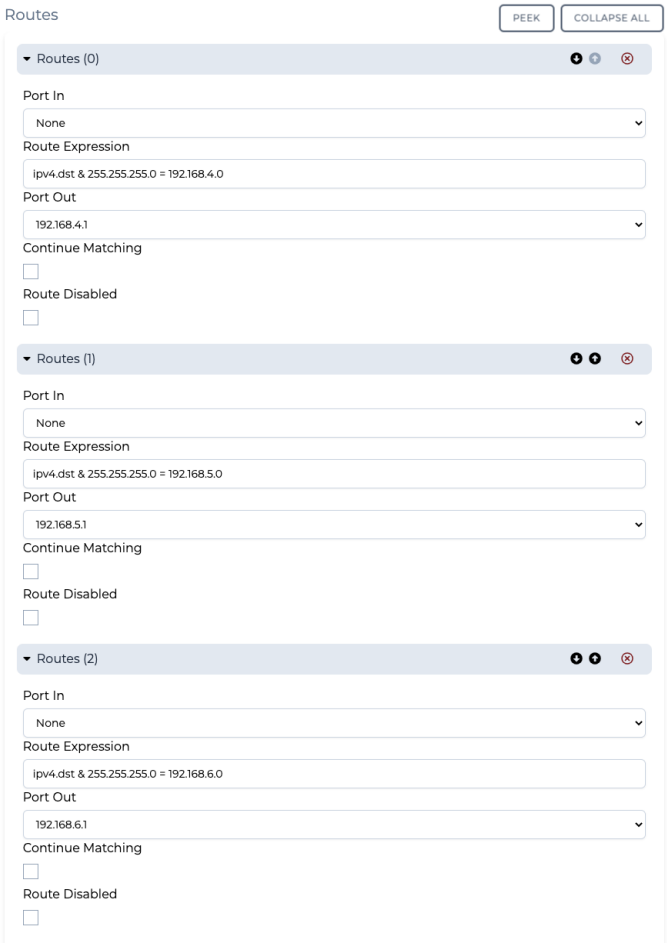
c. From the **Port Out** drop-down field, select the output port for the first route. In our example, select **192.168.9.1** (i.e. the sixth soft port).

d. Leave the **Continue Matching** check box unticked (i.e. continue matching disabled). This is because our example will not allow packets to be sent to more than one route.

e. Leave the **Route Disabled** check box unticked (i.e. the route is enabled). This is because our example wants the sixth route enabled.

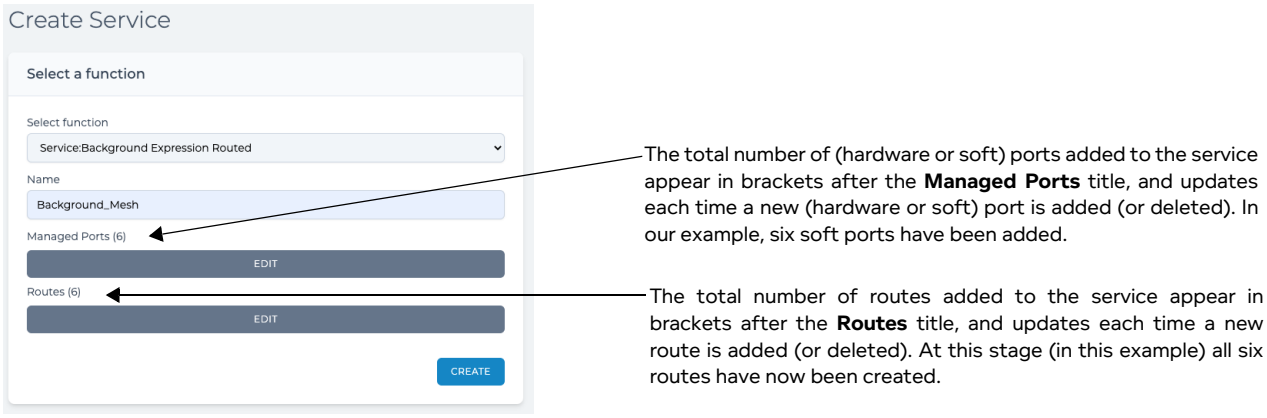
At this stage all of the six routes are added to the Service : Background Expression Routed

service.



15. Click **DONE** to return to **Create Service** page.

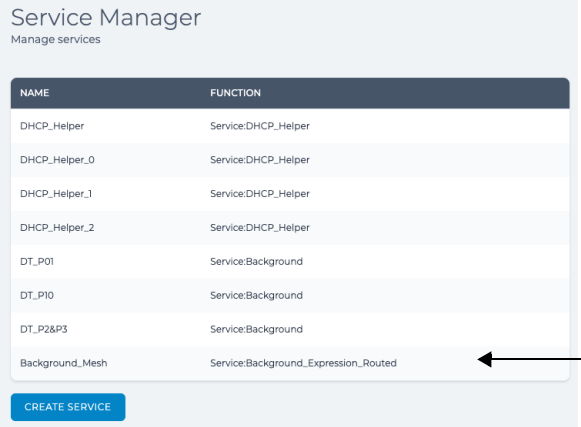
    The **Create Service** page appears, and now contains the six routes that you added and defined.



    The Background Expression Routed service is now fully configured, and can be committed to the system.

16. In the **Create Service** page appears, click **CREATE**.
17. The **Create Service** page closes, and in the **Created service successfully** dialog box that appears, click **OK**.

You are returned to the **Service Manager** page.



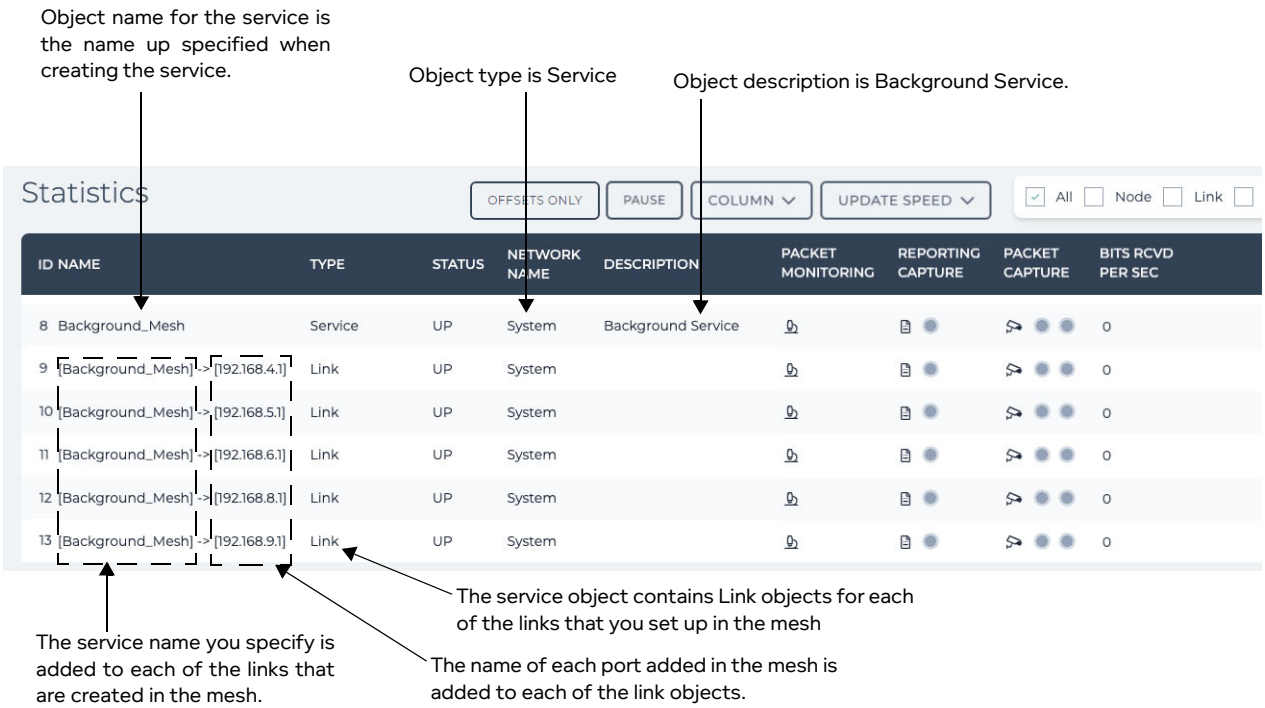
The newly created **Service:Background Expression Routed** service called **Background_Mesh** appears at the bottom of the list of services.

The Background Expression Routed service you configured is committed to the system, and:

- starts immediately on the selected ports with the routing criteria you had defined. The service is now complete and will manage the ports in the Managed Port array whenever they are not used in a running network.
- is listed in the services table on the **Service Manager** page. Clicking on this service from the **Service Manager** page re-opens it in the **Edit Service** page, letting you edit (i.e. change the port selection and route definitions) or delete the service.
- is listed as a service object in objects table of the **Statistics** page (*Illustration 160* on page 527), from where packet capturing and graphing can be launched for the service. For more information, see *Enabling Packet Capture for a PPO Within the Statistics Page* on page 537 in *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing*.

  For the example mesh (*Illustration 50* on page 179) that was created, its service object and associated link objects will appear in the **Statistics**, as shown in *Illustration 52*.

ILLUSTRATION 52 - EXAMPLE SERVICE AND LINK STATISTICS FOR A MESH



4-2-2. Creating Multiple DHCP Helper Services

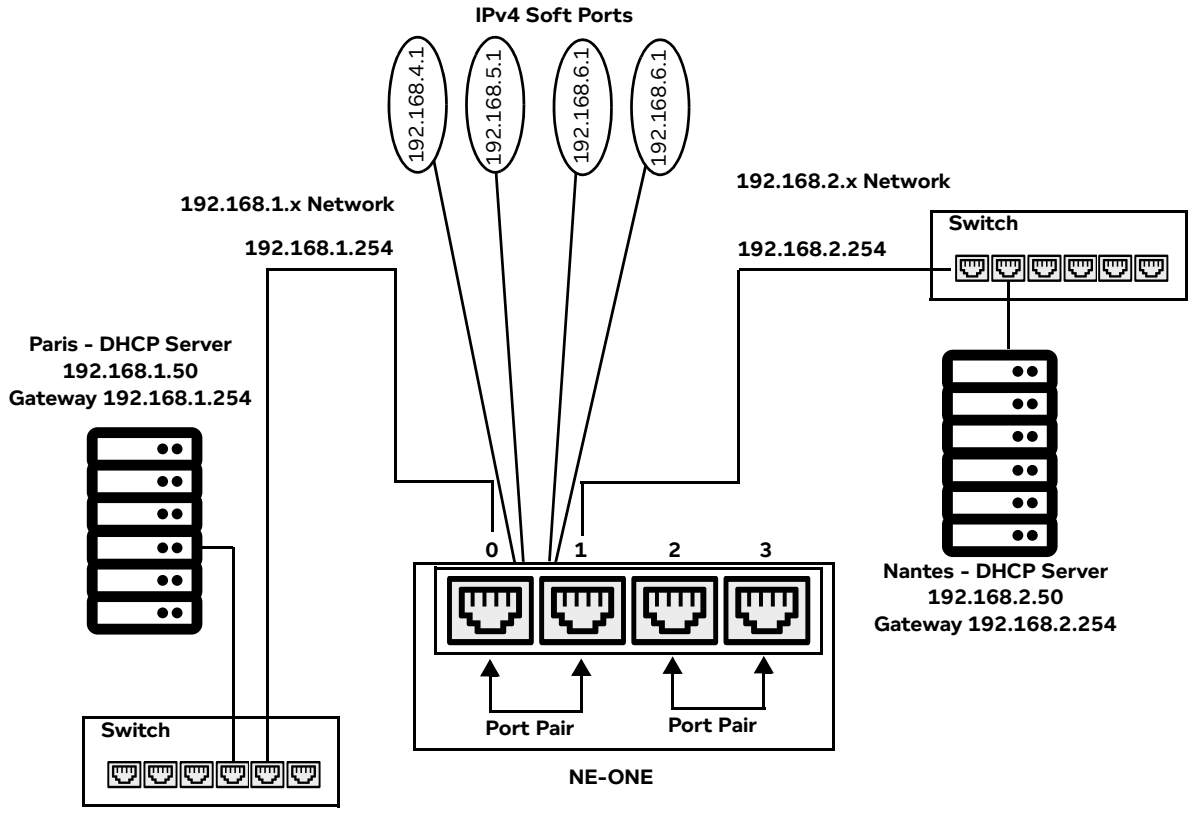
The example below in *Illustration 53* shows the use of the DHCP Helper service to create four DHCP Helper services on the following already created IPv4 soft ports:

- IPv4 soft port (a child on hardware port 0), named **192.168.4.1** will use the service with the name defined as **DHCP_Helper_4_1** (i.e we have used the last octets of the IPv4 soft port's IP address to easily identify it). This name must be the same as the name that you specified in the **DHCP Helper Service Name** field of the **Edit Port** panel when you created the IPv4 soft port **192.168.4.1**.
- IPv4 soft port (a child on hardware port 0), named **192.168.5.1** will use the service with the name defined as **DHCP_Helper_5_1** (i.e we have used the last octets of the IPv4 soft port's IP address to easily identify it). This name must be the same as the name that you specified in the **DHCP Helper Service Name** field of the **Edit Port** panel when you created the IPv4 soft port **192.168.5.1**.
- IPv4 soft port (a child on hardware port 1), named **192.168.6.1** will use the service with the name defined as **DHCP_Helper_6_1** (i.e we have used the last octets of the IPv4 soft port's IP address to easily identify it). This name must be the same as the name that you specified in the **DHCP Helper Service Name** field of the **Edit Port** panel when you created the IPv4 soft port **192.168.6.1**.
- IPv4 soft port (a child on hardware port 1), named **192.168.7.1** will use will use the service with the name defined as **DHCP_Helper_7_1** (i.e we have used the last octets of the IPv4 soft port's IP address to easily identify it). This name must be the same as the name that you specified in the **DHCP Helper Service Name** field of the **Edit Port** panel when you created the IPv4 soft port **192.168.7.1**.

Hardware port 0 is connected in a network which contains a DHCP server with IP address 192.168.1.50.

Hardware port 1 is connected in a network which contains a DHCP server with IP address 192.168.2.50.

ILLUSTRATION 53 - DHCP SERVERS IN TWO DIFFERENT NETWORKS WITH FOUR DHCP HELPER SERVICES RUNNING

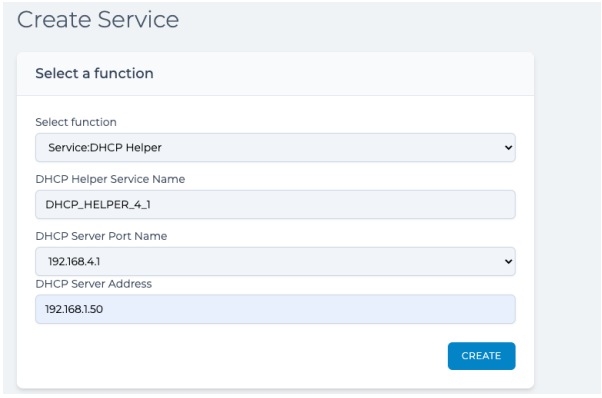


Note:
If you want to create a DHCP Helper service on a IPv4 soft port, the IPv4 soft port must have already been configured with the **Use DHCP Relay** check box ticked. For more information on creating IPv4 soft ports, see *Creating an IPv4 Soft Port* on page 114.

Note:
In some cases you need to create a DHCP Helper service on a pair of ports in order for the DHCP relay to work. Use the steps below for each port on which you want to the DHCP Helper service to be running.

Use the following steps to create a DHCP Helper service on a IPv4 soft port. Repeat these steps for each IPv4 soft port on which you need the DHCP Helper service running.

1. From the Web Interface, click **Management > Service Manager**.
   A **Service Manager** page (*Illustration 49*) appears displaying a list of services that have been added (if any exist) on the NE-ONE.
2. Click the **CREATE SERVICE** button.
3. From the **Create Service** page that appears, select **Service:DHCP Helper** from the **Select function** field.
   The **Create Service** page updates with elements associated with configuring a DHCP Helper service.
4. In the **DHCP Helper Service Name** field, type an appropriate service name.
   In the example in *Illustration 53*, you would do the following:
   - for the first child IPv4 soft port belonging to hardware port 0, type **`DHCP_HELPER_4_1`**.
   - for the second child IPv4 soft port belonging to hardware port 0, type **`DHCP_HELPER_5_1`**.
   - for the first child IPv4 soft port belonging to hardware port 1, type **`DHCP_HELPER_6_1`**.
   - for the second child IPv4 soft port belonging to hardware port 1, type **`DHCP_HELPER_7_1`**.
5. In the **DHCP Server Port Name** field, select the IPv4 or soft port on which you want the DHCP Helper service to be running.



   In the example in *Illustration 53*, you would do the following:
   - for the first child IPv4 soft port belonging to hardware port 0, select **192.168.4.1**.
   - for the second child IPv4 soft port belonging to hardware port 0, select **192.168.5.1**.
   - for the first child IPv4 soft port belonging to hardware port 1, select **192.168.6.1**.
   - for the second child IPv4 soft port belonging to hardware port 1, select **192.168.7.1**.
6. In the **DHCP Server Address** field, type the IP address of the DHCP server that will be used for accepting DHCP requests from DHCP clients connected to the selected port. For the example in *Illustration 53*, you would do the following:
   - for the first child IPv4 soft port belonging to hardware port 0, type **`192.168.1.50`** for the DHCP

server IP address.

- for the second IPv4 soft port belonging to hardware port 0, type **192.168.1.50** for the DHCP server IP address.
- for the first child IPv4 soft port belonging to hardware port 1, type **192.168.2.50** for the DHCP server IP address.
- for the second child IPv4 soft port belonging to hardware port 1, type **192.168.2.50** for the DHCP server IP address.

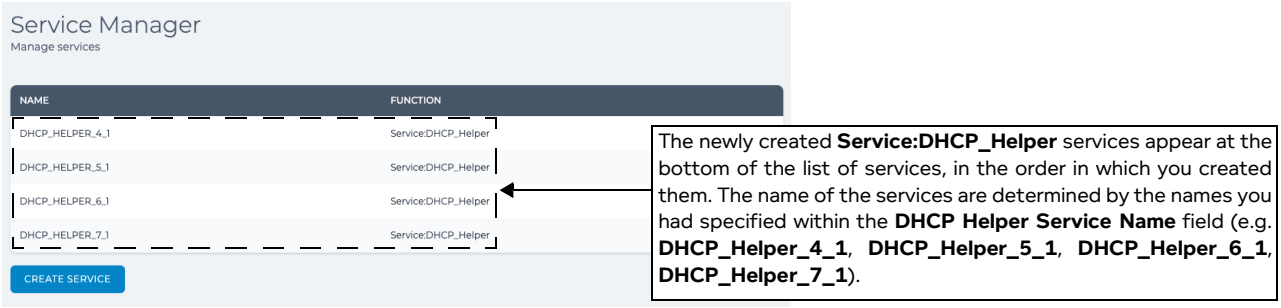
7. Click **CREATE**.
8. The **Create Service** page closes, and in the **Created Service Successfully** dialog box that appears, click **OK**.

   You are returned to the **Service Manager** page.

   The newly created DHCP Helper service:

   - starts immediately on the selected port relaying DHCP requests to the defined DHCP server.
   - is listed in the services table on the **Service Manager** page. Clicking on this service from the **Service Manager** page re-opens it in the **Edit Service** page, letting you edit (i.e. change the port selection or re-define a different DHCP server) or delete the service.
   - is listed as a service object in objects table of the **Statistics** page (*Illustration 160* on page 527), from where packet capturing and graphing can be launched for the service. For more information, see *Enabling Packet Capture for a PPO Within the Statistics Page* on page 537 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
9. Repeat steps 2 to 8 for each of the DHCP Helper services you want to add.

   In our example, four DHCP Helper services were added.



4-2-3. Creating a Background Service

The examples below shows the use of the Background service to create a Default Transmission service between two ports in a port pair.

Note:

This procedure is the equivalent simply enabling Default Transmission on a port pair (see *Default Transmission* on page 175). However, using the Background service to create a Default Transmission service between two ports in a port pair provides the following minor differences compared to simply enabling Default Transmission:

1. It lets you create a Default Transmission service on a pair of ports that are not defined as port pairs.
2. It lets you create a Default Transmission service on a port pair for each port pair direction (i.e. one Default Transmission service for each port pair direction, and thus two Default Transmission services for a port pair).
3. It lets you create a Default Transmission service on a port pair for both port pair directions (i.e.

one Default Transmission service for both port pair directions, and thus one Default Transmission service for a port pair, where the two directions are defined in the Background service).

Note:

For the maximum efficiency it is recommended that case one service is created per port pair per direction.

4-2-3-1. Creating Two Default Transmission Services for a Port Pair (i.e. One Service For Each Traffic Direction)

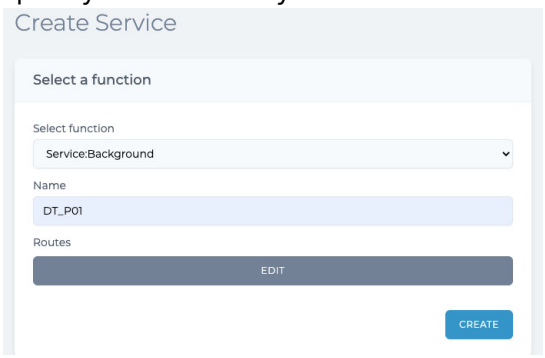
Use the following steps to create two Background services on a port pair, where each service is for the same port pair, but for the opposite port pair directions. In the example below, the two services called DT_P01 and DT_P10 are set up on hardware ports 0 and 1 for the port directions 0 to 1 and 1 to 0, respectively.

Note:

The example below uses port pairs on hardware ports. However, you can also create Background services on port pairs using soft ports.

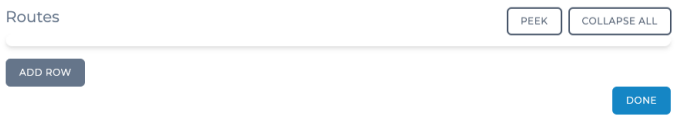
1. From the Web Interface, click **Management > Service Manager**.

   A **Service Manager** page appears displaying a list of services that have been added (if any exist) to the NE-ONE.
2. Click the **CREATE SERVICE** button to create the first service for the first port pair direction.
3. From the **Create Service** page that appears, select **Service:Background** from the **Select function** field.
4. The **Create Service** page updates with elements associated with configuring a Background service.
5. In the **Name** field, type an appropriate service name to represent the service you are creating (for our example, type **`DT_P01`** (where DT is an acronym for Default Transmission, and P01 represents hardware ports 0 and 1 with the port pair direction going from port 0 to 1). The **Name** field accepts alpha-numeric characters, special characters (except \, / and *), and spaces. The name that you specify is also used by the service file that gets created for the service.



6. Click the **Routes EDIT** button.

   An empty **Routes** dialog box appears, letting you define the routes in the Background service. Initially the **Routes** dialog box is empty as no routes currently exist.

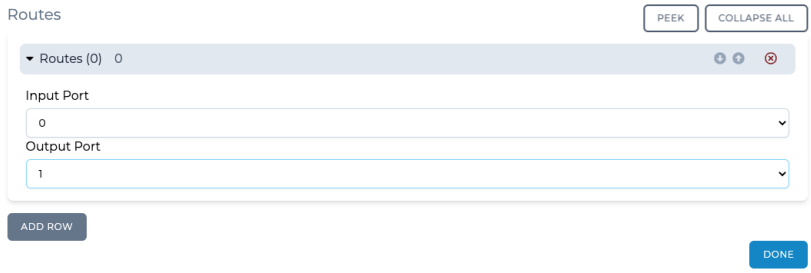


   For this service, you will only configure one route going in the port direction of hardware port 0 to hardware port 1.

Note:

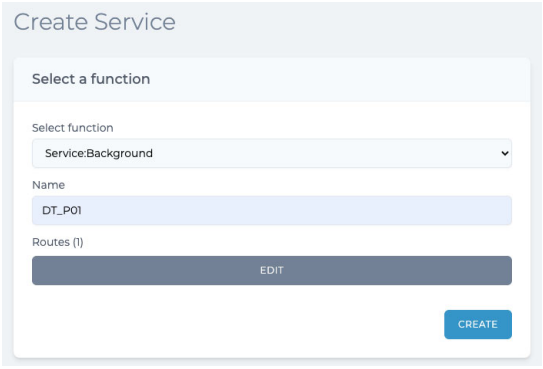
When creating services, the **PEEK** button is visible but intentionally inactive.

7. From the **Routes** dialog box that appears, click **ADD ROW** to add the first (and only) route. From the **Routes (0)** row that appears, do the following:
   a. From the **Input Port** drop-down field, select the input port for the first (and only) route. In our example, select **0** (i.e. hardware port 0).
   b. From the **Output Port** drop-down field, select the output port for the first (and only) route. In our example, select **1** (i.e. hardware port 1).



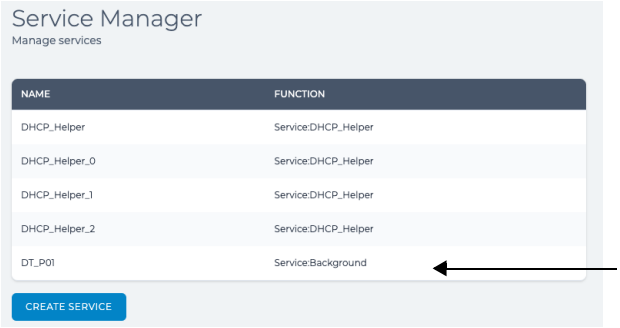
   c. Click **DONE** to return to **Create Service** page.

   The **Create Service** page appears, and now contains the one route that you added and defined.



   The Background service is now fully configured, and can be committed to the system.
8. In the **Create Service** page, click **CREATE**.
9. The **Create Service** page closes, and in the **Created Service Successfully** dialog box that appears, click **OK**.

   You are returned to the **Service Manager** page.



The newly created **Service:Background** service appears at the bottom of the list of services.

   The Background service you configured is committed to the system, and:

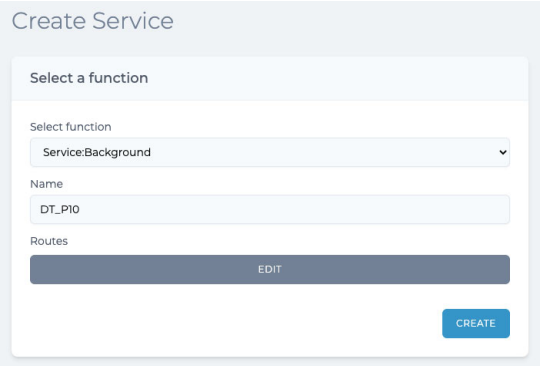
   - starts immediately on the selected ports (in this example, hardware ports 0 and 1 with port pair direction going from 0 to 1).
   - is listed in the services table on the **Service Manager** page. Clicking on this service from the **Service Manager** page re-opens it in the **Edit Service** page, letting you edit (i.e. change the port

selection and port traffic direction) or delete the service.

- is listed as a service object in objects table of the **Statistics** page (*Illustration 160* on page 527), from where packet capturing and graphing can be launched for the service. For more information, see *Enabling Packet Capture for a PPO Within the Statistics Page* on page 537 in *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing*.

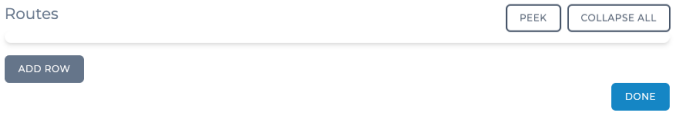
At this stage, since only one service has been created for the port pair direction (in our example 0 to 1), you must now create the second service for the other port pair direction (in our example 1 to 0).

10. Click the **CREATE SERVICE** button to create the second service for the second port pair direction.
11. From the **Create Service** page that appears, select **Service:Background** from the **Select function** field.
12. The **Create Service** page updates with elements associated with configuring a Background service.
13. In the **Name** field, type an appropriate service name to represent the service you are creating (for our example, type **`DT_P10`** (where DT is an acronym for Default Transmission, and P10 represents hardware ports 0 and 1 with the port pair direction going from port 1 to 0). The **Name** field accepts alpha-numeric characters, special characters (except \, / and *), and spaces. The name that you specify is also used by the service file that gets created for the service.



14. Click the **Routes EDIT** button.

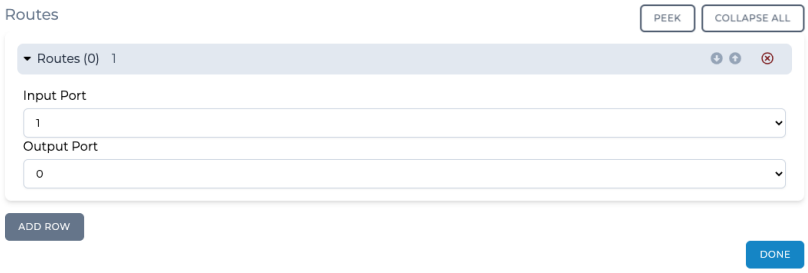
An empty **Routes** dialog box appears, letting you define the routes in the Background service. Initially the **Routes** dialog box is empty as no routes currently exist.



For this service, you will only configure one route going in the port pair direction of hardware port 1 to hardware port 0.

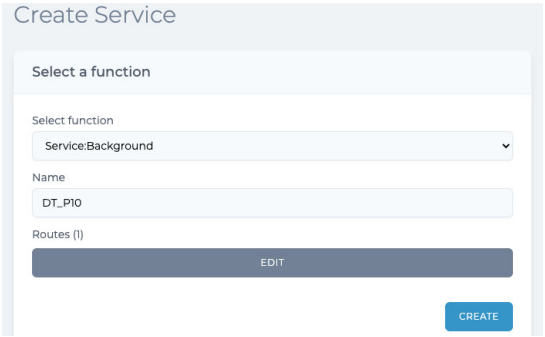
15. From the **Routes** dialog box that appears, click **ADD ROW** to add the first (and only) route. From the **Routes (0)** row that appears, do the following:
    a. From the **Input Port** drop-down field, select the input port for the first (and only) route. In our example, select **1** (i.e. hardware port 1).
    b. From the **Output Port** drop-down field, select the output port for the first (and only) route. In our

example, select **0** (i.e. hardware port 0).



c. Click **DONE** to return to **Create Service** page.

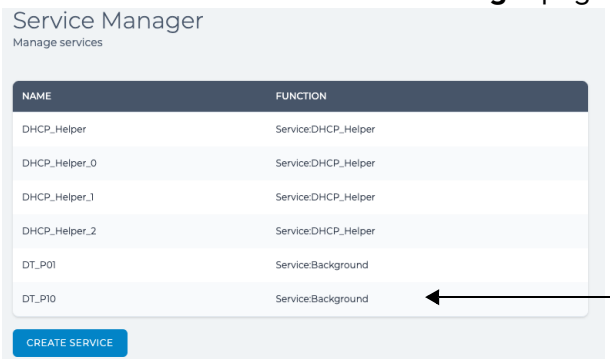
The **Create Service** page appears, and now contains the one route that you added and defined.



The Background service is now fully configured, and can be committed to the system.

16. In the **Create Service** page, click **CREATE**.
17. The **Create Service** page closes, and in the **Created Service Successfully** dialog box that appears, click **OK**.

You are returned to the **Service Manager** page.



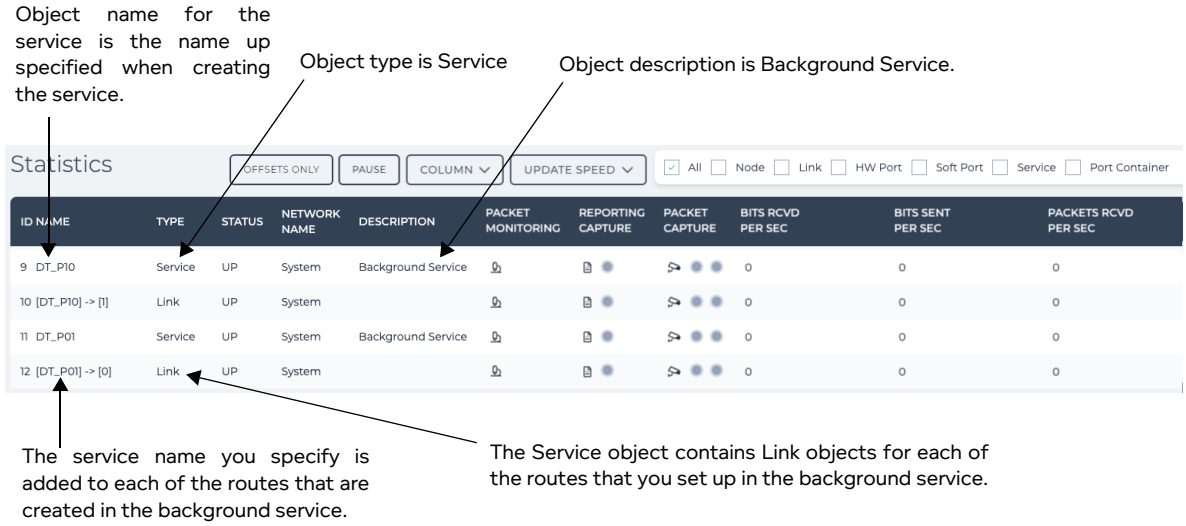
The newly created **Service:Background** service appears at the bottom of the list of services.

The Background service you configured is committed to the system, and:

- starts immediately on the selected ports (in this example, hardware ports 0 and 1 with port pair direction going from 1 to 0).
- is listed in the services table on the **Service Manager** page. Clicking on this service from the **Service Manager** page re-opens it in the **Edit Service** page, letting you edit (i.e. change the port selection and port traffic direction) or delete the service.
- is listed as a service object in objects table of the **Statistics** page (*Illustration 160* on page 527), from where packet capturing and graphing can be launched for the service. For more information, see *Enabling Packet Capture for a PPO Within the Statistics Page* on page 537 in *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing*.

  For the example in this procedure that was created, the service objects and associated link objects will appear in the **Statistics**, as shown in *Illustration 54*.

ILLUSTRATION 54 - EXAMPLE SERVICE AND LINK STATISTICS FOR TWO UNIDIRECTIONAL DEFAULT TRANSMISSION BACKGROUND SERVICES



4-2-3-2. Creating One Default Transmission Service for a Port Pair (i.e. One Service For Both Traffic Directions)

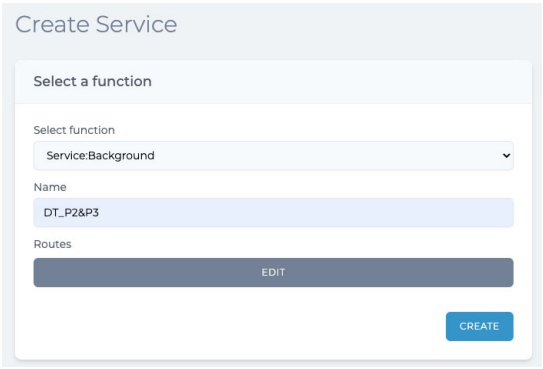
Use the following steps to create one Background service on a port pair, where the service contains two routes for both port pair directions. In the example below, the a service called DT_P2&P3 is set up on hardware ports 2 and 3 for both port directions 2 to 3 and 3 to 2.

Note:

The example below uses port pairs on hardware ports. However, you can also create Background services on port pairs using soft ports.

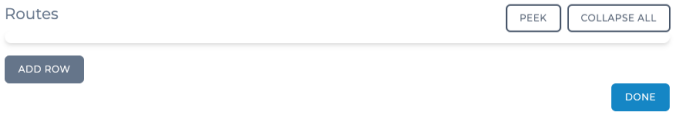
1. From the Web Interface, click **Management > Service Manager**.
   A **Service Manager** page appears displaying a list of services that have been added (if any exist) to the NE-ONE.
2. Click the **CREATE SERVICE** button to create the service for the port pair.
3. From the **Create Service** page that appears, select **Service:Background** from the **Select function** field.
4. The **Create Service** page updates with elements associated with configuring a Background service.
5. In the **Name** field, type an appropriate service name to represent the service you are creating (for our example, type **`DT_P2&P3`** (where DT is an acronym for Default Transmission, and P2&P3 represents hardware ports 2 and 3). The **Name** field accepts alpha-numeric characters, special characters (except \, / and *), and spaces. The name that you specify is also used by the service file that gets

created for the service.



6. Click the **Routes EDIT** button.

   An empty **Routes** dialog box appears, letting you define the routes in the Background service. Initially the **Routes** dialog box is empty as no routes currently exist.



Note:

When creating services, the **PEEK** button is visible but intentionally inactive.

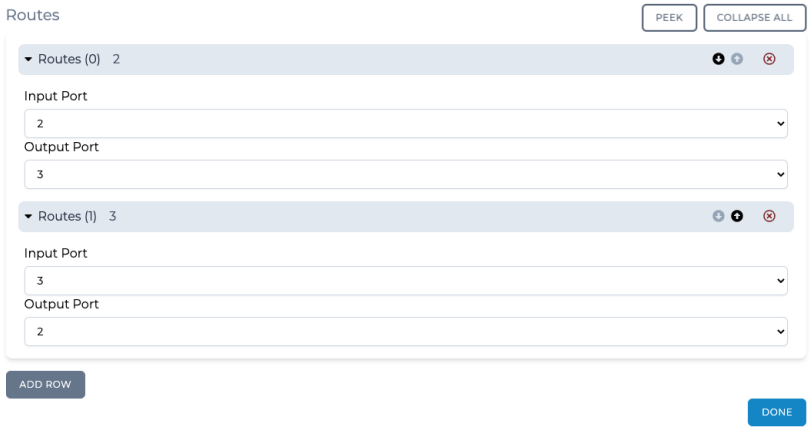
For this service (in our example), you configure the following two routes:

- one route going in the port pair direction of hardware port 2 to hardware port 3
- one route going in the port pair direction of hardware port 3 to hardware port 2

7. From the **Routes** dialog box that appears, click **ADD ROW** to add the first route. From the **Routes (0)** row that appears, do the following:
   a. From the **Input Port** drop-down field, select the input port for the first route. In our example, select **2** (i.e. hardware port 2).
   b. From the **Output Port** drop-down field, select the output port for the first route. In our example, select **3** (i.e. hardware port 3).

8. From the **Routes** dialog box, click **ADD ROW** to add the second route. From the **Routes (1)** dialog box that appears, do the following:
   a. From the **Input Port** drop-down field, select the input port for the second route. In our example, select **3** (i.e. hardware port 3).
   b. From the **Output Port** drop-down field, select the output port for the second route. In our

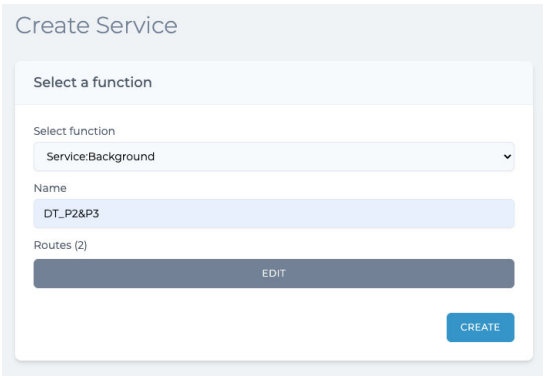
example, select **2** (i.e. hardware port 2).



At this stage both routes for both port pair directions have been created.

9. Click **DONE** to return to **Create Service** page.

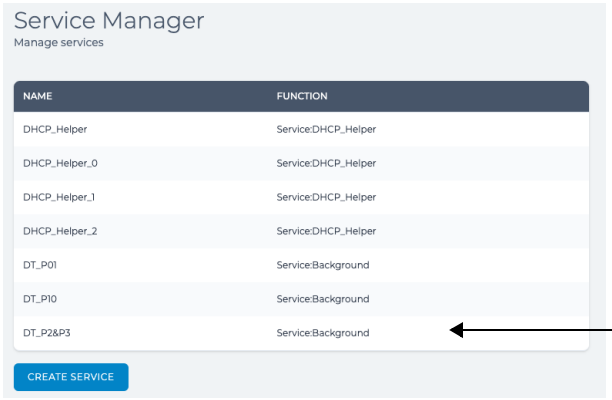
   The **Create Service** page appears, and now contains the two routes that you added and defined.



The Background service is now fully configured, and can be committed to the system.

10. In the **Create Service** page, click **CREATE**.
11. The **Create Service** page closes, and in the **Created Service Successfully** dialog box that appears, click **OK**.

    You are returned to the **Service Manager** page.



The newly created **Service:Background** service appears at the bottom of the list of services.

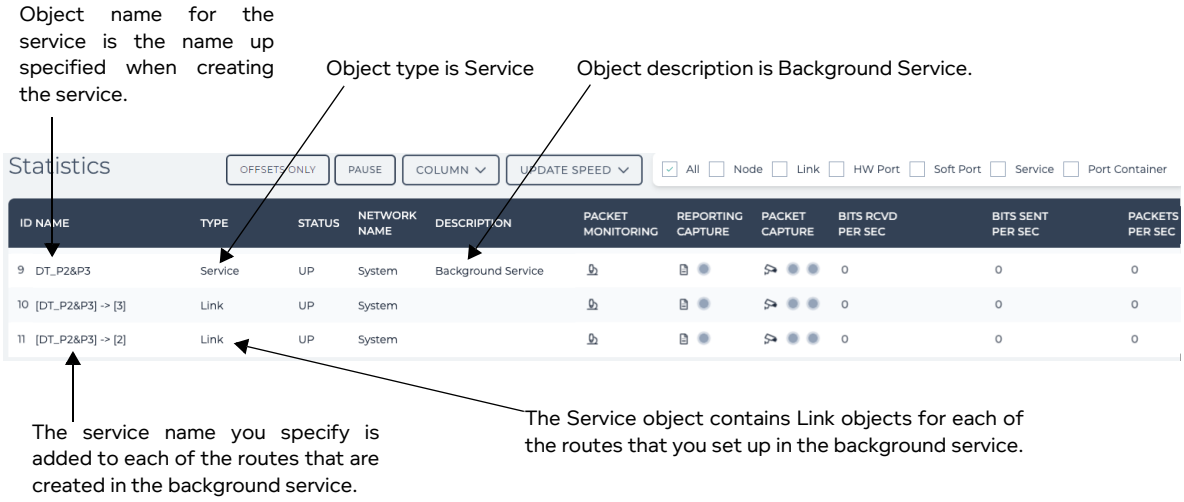
The Background service you configured is committed to the system, and:

- starts immediately on the selected ports (in this example, hardware ports 2 and 3 with port pair directions going from both 2 to 3 and 3 to 2).

- is listed in the services table on the **Service Manager** page. Clicking on this service from the **Service Manager** page re-opens it in the **Edit Service** page, letting you edit (i.e. change the port selection and port traffic direction) or delete the service.
- is listed as a service object in objects table of the **Statistics** page (*Illustration 160* on page 527), from where packet capturing and graphing can be launched for the service. For more information, see *Enabling Packet Capture for a PPO Within the Statistics Page* on page 537 in *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing*.

  For the example in this procedure that was created, the service objects and associated link objects will appear in the **Statistics**, as shown in *Illustration 55*.

ILLUSTRATION 55 - EXAMPLE SERVICE AND LINK STATISTICS FOR ONE BIDIRECTIONAL DEFAULT TRANSMISSION BACKGROUND SERVICE



CHAPTER 6 USER ADMINISTRATION

1. INTRODUCTION

This chapter is applicable to admin users, and describes the procedures that you use to administer users on the NE-ONE.

2. PREREQUISITES

Before administering users on the NE-ONE, ensure the you have already done the steps summarized in *Table 30*.

TABLE 30 - USER ADMINISTRATION PREREQUISITES

Step	Task	Port Manager feature activated ?		Service Manager feature activated ?	
		NO	**YES**	**NO**	**YES**
1	Install and set up the NE-ONE according to the procedures in *Chapter 4*, *Installation and Configuration*	N/A	N/A	N/A	N/A
2	Configure all the necessary soft ports and port pairs, according to *Managing Ports* on page 103 and *Managing Port Pairs* on page 156, respectively within *Chapter 5*, *Ports and Services Management*	NO	YES	NO	NO
3	If necessary, configure services according to *Managing Services* on page 177 within *Chapter 5*, *Ports and Services Management*	NO	NO	NO	YES
4	If necessary, configure Port Addressing according to *Configuring Port Addressing* on page 167 in *Chapter 5*, *Ports and Services Management*	N/A	N/A	N/A	N/A
5	If necessary, configure a DHCP relay according to *DHCP Server / DHCP Relay* on page 172 in *Chapter 5*, *Ports and Services Management*	N/A	N/A	N/A	N/A
Note: The Port Manager feature and Service Manager feature are premium features. Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated. In the cells above N/A indicates that this task is not associated with the premium features and always available to the admin user.					

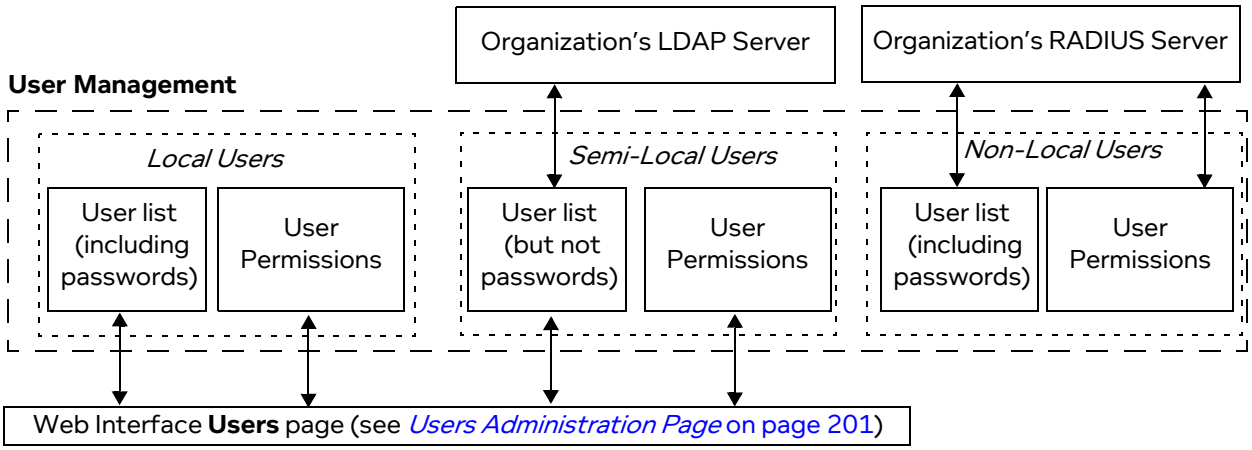
3. LOCAL, SEMI-LOCAL AND NON-LOCAL USERS

It is important to understand the concept of local, semi-local, and non-local users. In addition to built-in authentication, the NE-ONE also supports LDAP and RADIUS authentication methods. *Table 9* on page 77 summarizes the differences between how the built-in, LDAP and RADIUS authentication methods are implemented on the NE-ONE, and how the users are authenticated and managed.

Note:
The LDAP and RADIUS authentication methods are part of the Advanced Authentication feature, which is a premium feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

- If the NE-ONE has been set up to use the built-in authentication method (see *Configuring Built-in Authentication* on page 78), all the "local" users;
  - must be created locally from within the **Users** page (see *Users Administration Page* on page 201).
  - must have their permissions managed on the NE-ONE (see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205),
  - can be locally deleted from the NE-ONE (see *Deleting Local and Semi-Local Users* on page 205).
- If the NE-ONE has been set up to use the LDAP authentication method (see *Configuring LDAP Authentication* on page 78), it will verify the "semi-local" users passwords from the organization's LDAP servers. In this case, however, the semi-local users;
  - must still be created locally from within the **Users** page (see *Adding Local and Semi-Local Users* on page 204), but the password is not defined on the NE-ONE as it is managed by the LDAP server,
  - must still have their permissions managed on the NE-ONE (see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205),
  - can be locally deleted from the NE-ONE (see *Deleting Local and Semi-Local Users* on page 205).
- If the NE-ONE has been set up to use the RADIUS authentication method (see *Configuring RADIUS Authentication* on page 79), it will inherit "non-local" users and their permissions from the organization's RADIUS server. In this case, the non-local users cannot be added or deleted as they are completely inherited from the organization's RADIUS server. However, the non-local users will only be inherited if you also configure your RADIUS server to inter-operate with the NE-ONE according to *Configuring a Radius Server to Inter-operate with the NE-ONE* on page 209.

ILLUSTRATION 56 - COMPARISON BETWEEN LOCAL, SEMI-LOCAL AND NON LOCAL USERS



4. USERS ADMINISTRATION PAGE

This section is only applicable if the NE-ONE uses either built-in authentication or LDAP authentication. If the NE-ONE uses the RADIUS authentication method, refer to *Configuring a Radius Server to Inter-operate with the NE-ONE* on page 209.

The **Users** page (*Illustration 57*) appears after selecting **Management > ··· Platform Settings > Users**, and provides a central area from where you can perform all the user management functions on the NE-ONE. The **Users** page contains a User List Table with a row for each of the NE-ONE users, and an **ADD USER** button.

- Clicking on the **ADD USER** button opens a **Create User** pages, which lets you create a new local or semi-local user (see *Adding Local and Semi-Local Users* on page 204).
- Clicking on a user row within the User List Table opens the **Edit User Details** page (*Illustration 58*), from where you can:
  - Define the permissions associated with that user (see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205). The number of permissions that you can define vary (see *Table 31*) according to whether or not you have the Advanced User Permissions feature activated.
  - Change the user's password (only possible for local users) (see *Changing a User Password* on page 208).
  - Delete a user (only possible for local or semi-local users) (see *Deleting Local and Semi-Local Users* on page 205).

ILLUSTRATION 57 - THE USERS PAGE

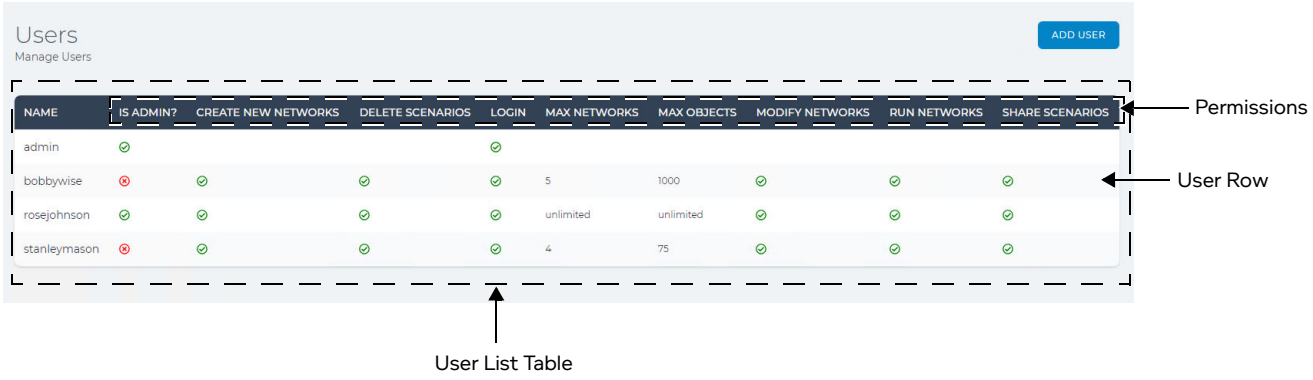
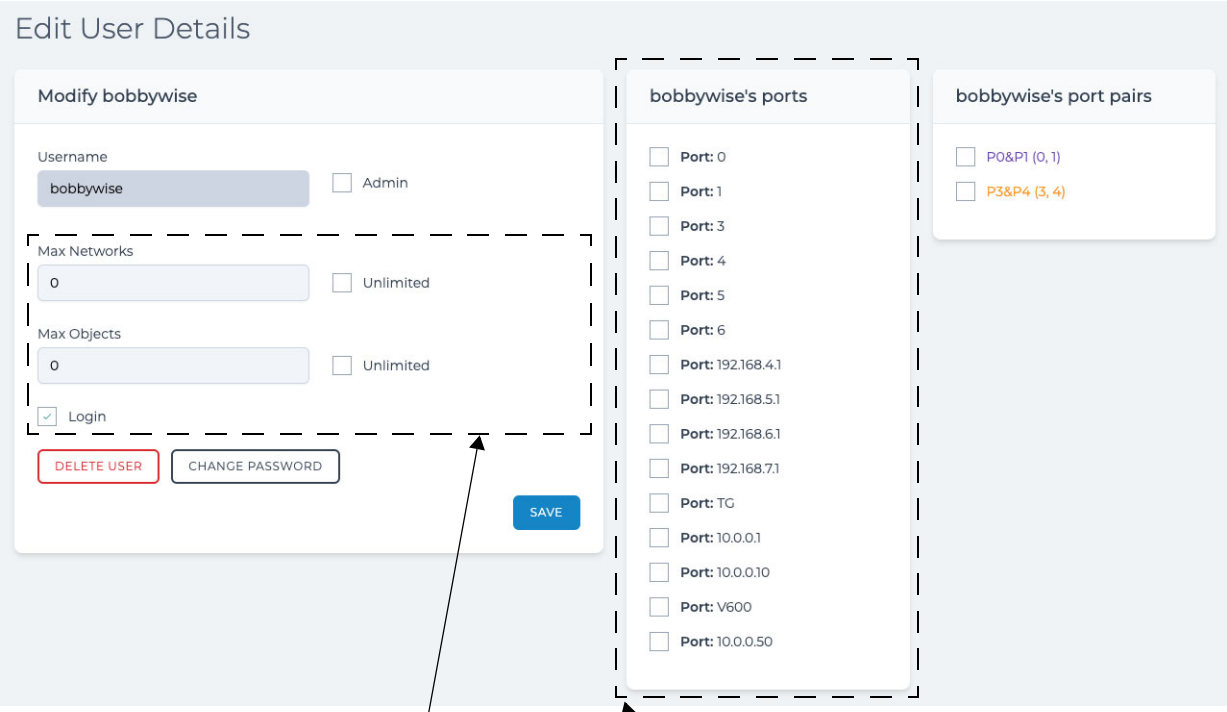


TABLE 31 - DEFINABLE USER PERMISSIONS

Definable User Permission	Advanced User Permissions feature activated	Advanced User Permissions feature deactivated
Determine whether or not the user is an admin user	Yes	Yes
Determine whether or not the user can create new networks	Yes	No
Determine whether or not the user can delete scenarios	Yes	No
Determine whether or not the user can login	Yes	No
Define the maximum number of networks available for the user	Yes	No, all users are assigned an unlimited number of networks

Definable User Permission	Advanced User Permissions feature activated	Advanced User Permissions feature deactivated
Define the maximum number of objects available for the user	Yes	No, all users are assigned an the maximum number of objects that are permissible on the NE-ONE
Define the maximum number of links available for the user	Yes	No, all users are assigned an unlimited number of links
Determine whether or not the user can modify networks	Yes	No
Determine whether or not the user can run networks	Yes	No
Determine whether or not the user can share scenarios	Yes	No

ILLUSTRATION 58 - EDIT USER DETAILS PAGE



The **Max Networks** parameter, **Max Objects** parameter, and **Login** parameter are only available if the Advanced User Permissions feature is activated.

Individual ports (via the **<username>'s** ports area) can only be assigned to a user if the Port Manager feature is active. Depending on your license, the Port Manager feature may either be activated (i.e. you are able to assign ports to a user) or deactivated (i.e. you are unable to assign ports to a user).

Note:

The **Edit User Details** page for the local (built-in) admin user has an additional **Reset password on next login** check box (when logged in as the local admin user), which can be used for resetting the local admin user password back to the default value of admin. For more information, see *Resetting the Local Admin User Password back to the Default Value* on page 227 in *Chapter 7, System Maintenance*.

The **Users** page lets you perform the following user management functions on the NE-ONE:

- view all the users (in the User List Table)
- add a local or semi-local user (see *Adding Local and Semi-Local Users* on page 204)
- delete a local or semi-local user (see *Deleting Local and Semi-Local Users* on page 205)
- configure the following permissions of users (via the User List Table) (see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205), such as:
  - Whether the user is an admin type user or non-admin type user. For more information on the differences between an admin type and non-admin type user, see *User Types and Roles* on page 25 in *Chapter 2*, *NE-ONE Overview*.
  - Whether the user can login to the NE-ONE.
  - Determine the maximum number of networks and scenarios they can create/run.
  - Determine the maximum number of objects they can use within their networks.
  - Assign port pairs to the user.
  - Assign individual ports to the user.

  Note:
  Individual ports can only be assigned to a user if the Port Manager feature is active. Depending on your license, the Port Manager feature may either be activated (i.e. you are able to assign ports to a user) or deactivated (i.e. you are unable to assign ports to a user).
- change a local user's password (see *Changing a User Password* on page 208)

4-1. Adding Local and Semi-Local Users

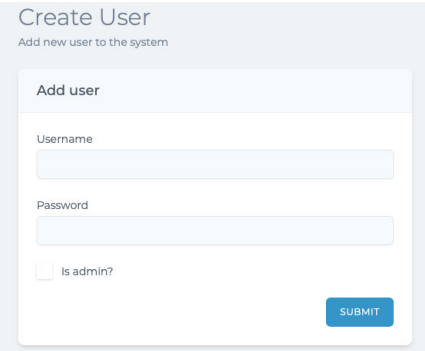
This section is only applicable if the NE-ONE uses either built-in authentication or LDAP authentication. If the NE-ONE uses the RADIUS authentication method, refer to *Configuring a Radius Server to Inter-operate with the NE-ONE* on page 209.

Note:
In order to access the NE-ONE for the first time, a local admin user exists using built-in authentication, which cannot be removed. The local admin user can therefore be used for initial access to the NE-ONE, and if necessary future access if the need arises. Additionally, because the local admin uses built-in authentication on the NE-ONE it would not conflict with an admin user on an LDAP server if one exists.

Note:
The LDAP and RADIUS authentication methods are part of the Advanced Authentication feature, which is a premium feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated. If you do not have the Advanced Authentication feature, then you must use the built-in authentication method for each of your users.

Use the following steps to add a local or semi-local user on the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Users**.
   A **Users** page (see *Illustration 57*) appears.
2. From the **Users** page that appears, click the **ADD USER** button.
   A **Create User** page appears.



3. From the **Create User** page that appears, do the following:
   a. In the **Username** field, type the user name of the new user.
   b. In the **Password** field, type the password for the new user.

Note:
If you have configured the NE-ONE to use LDAP authentication, the **Password** field is intentionally grayed out as the user's password is managed by the primary and secondary LDAP servers.

   c. If you want the new user to be an Admin type user, check (tick) the **Is admin?** check box.
   d. Click **SUBMIT**.
   The **Create User** page closes, and the **Users** page updates with the newly created user listed in the User List Table.

4-2. Deleting Local and Semi-Local Users

This section is only applicable if the NE-ONE uses either built-in authentication or LDAP authentication. If the NE-ONE uses the RADIUS authentication method, refer to *Configuring a Radius Server to Interoperate with the NE-ONE* on page 209.

Note:
The LDAP and RADIUS authentication methods are part of the Advanced Authentication feature, which is a premium feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

Note:
In order to access the NE-ONE for the first time, a local admin user exists using built-in authentication, which cannot be removed. The local admin user can therefore be used for initial access to the NE-ONE, and if necessary future access if the need arises.

Use the following steps to delete a local or semi-local user from the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Users**.
   A **Users** page (similar to *Illustration 57*) appears with a User List Table listing all the users.
2. From the **Users** page that appears, click on the row corresponding to the user that you want to delete.
   An **Edit User Details** page (similar to *Illustration 58*) appears.
3. From the **Edit User Details** page that appears, click the **DELETE USER** button.
4. From the **Delete User** confirmation dialog box that appears, click **OK**.
   The User List Table in the **Users** page updates, and no longer shows the user that you deleted.

4-3. Configuring and Editing User Permissions (for Built-in and LDAP authentication)

This section is only applicable if the NE-ONE uses either built-in authentication or LDAP authentication. If the NE-ONE uses the RADIUS authentication method, refer to *Configuring a Radius Server to Interoperate with the NE-ONE* on page 209.

An admin type user has all permissions on the NE-ONE. Whereas, a non-admin type user can be configured with a certain set of permissions.

When a local or semi-local user is created, all of their permissions are defaulted to the following:

- can login to the NE-ONE
- is not an admin type user
- zero maximum networks allocated
- zero maximum object allocated
- zero links allocated
- no ports allocated
- no port pairs allocated

Note:
If the Advanced User Permissions feature is not activated, the network allocation and object allocation is not configurable for each user. In this case each user will be assigned an unlimited number of networks, and the maximum number of objects that are permissible on the NE-ONE.

You can use the User List Table in the **Users** page (see *Illustration 57*) to quickly identify a user, review their existing permissions, and if necessary edit them as required. Clicking on a user row within the User List Table opens the **Edit User Details** page (see *Illustration 58*), from where you can define the

permissions associated with that user.

Notice:

The permissions of the **Edit User Details** page includes a dynamic list of soft ports and port pairs, which can change as more soft ports are added or deleted. Therefore, before creating users and defining their permissions, Calnex recommends that you complete configuring all the soft ports, port pairs, and services (see *Chapter 5, Ports and Services Management*). If you create additional soft ports or port pairs after creating a user, those new soft ports/port pairs are not enabled by default for those users, and you would have to reconfigure the user's permissions in order to add the new soft ports/port pairs.

Use the following steps to edit the permissions available to a user:

1. From the Web Interface, click **Management > Platform Settings > Users**.

   A **Users** page (similar to *Illustration 57*) appears with a User List Table listing all the users.
2. From the **Users** page that appears, click on the row corresponding to the user whose permissions that you want change.

   An **Edit User Details** page appears (similar to *Illustration 58*) appears.
3. From the **Modify <username>** area of the **Edit User Details** page, do the following:
   a. Check (tick) or uncheck (untick) the **Admin** check box according to whether or not you want to allow the user to have admin privileges.

      If the **Admin** check box is checked (ticked), the user will have admin privileges.

      If the **Admin** check box is unchecked (unticked), the user will not have admin privileges.
   b. In the **Max Networks** field, specify the maximum number of networks that can be run for the user. If you want the user to be able to run an unlimited number of networks, check (tick) the **Unlimited** check box.

      Note: When you enable the **Unlimited** check box, the NE-ONE automatically updates the field with **Unlimited**.

      Note: The **Max Networks** field is only available if the Advanced User Permissions feature is activated. If the Advanced User Permissions feature is not activated, an unlimited number of networks is assigned to the user.
   c. In the **Max Objects** field, specify the maximum number of objects that can be used for the user's networks. If you want the user to be able to use an unlimited number of objects in their networks, check (tick) the **Unlimited** check box.

      Note: When you enable the **Unlimited** check box, the NE-ONE automatically updates the field with **Unlimited**.

      Note: The **Max Objects** field is only available if the Advanced User Permissions feature is activated. If the Advanced User Permissions feature is not activated, the maximum number of objects that are permissible on the NE-ONE are assigned to the user.
   d. Check (tick) or uncheck (untick) the **Login** check box according to whether or not you want to allow the user login to the NE-ONE.

      If the **Login** check box is checked (ticked), the user can login to the NE-ONE.

      If the **Login** check box is unchecked (unticked), the user cannot login to the NE-ONE.

      Note: The **Login** check box is only available if the Advanced User Permissions feature is activated. If the Advanced User Permissions feature is not activated, the user will be automatically configured and always be allowed to login to the NE-ONE.
4. From the **<username>'s ports** area of the **Edit User Details** page, do the following:

a. Check (tick) the corresponding port check boxes according to individual ports that you want to be available to the user. The ports you enable will be available to the user for their networks.
b. Uncheck (untick) the corresponding port check boxes according to individual ports that you do not want to be available to the user. The ports you disable will not be available to the user for their networks.

Note:
Individual ports can only be assigned to a user via the **<username>'s ports** area if the Port Manager feature is active. Depending on your license, the Port Manager feature may either be activated (i.e. you are able to assign ports to a user via the **<username>'s ports** area) or deactivated (i.e. you are unable to assign ports to a user via the **<username>'s ports** area).

5. From the **<username>'s port pairs** area of the **Edit User Details** page, do the following:
   a. Check (tick) the corresponding port pair check boxes according to port pair that you want to be available to the user. The port pair you enable will be available to the user for their Point-to-Point networks.
   b. Uncheck (untick) the corresponding port pair check boxes according to port pair that you do not want to be available to the user. The port pair you disable will not be available to the user for their Point-to-Point networks.
6. Click the **SAVE** button.
   The permissions are applied on the NE-ONE, and you are returned to the **Users** page.

4-4. Changing a User Password

This section is only applicable if the NE-ONE uses built-in authentication.

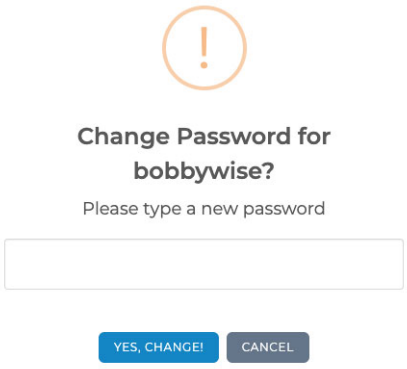
If the NE-ONE uses LDAP authentication, the user's password is managed on the LDAP server. If the NE-ONE uses the RADIUS authentication method, refer to *Configuring a Radius Server to Inter-operate with the NE-ONE* on page 209.

Note:
The LDAP and RADIUS authentication methods are part of the Advanced Authentication feature, which is a premium feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

Note:
The following steps are for an admin user to change an existing user's password. If a user wants to change their own password, they must follow the steps defined in *Changing Your User Password via the Tray User Menu* on page 230 in *Chapter 8*, *General System Procedures*.

Use the following steps to change a local user's password:

1. From the Web Interface, click **Management > Platform Settings > Users**.
   A **Users** page (similar to *Illustration 57*) appears with a User List Table listing all the users.
2. From the **Users** page that appears, click on the row corresponding to the user who's password you want to change.
   An **Edit User Details** page appears (similar to *Illustration 58*) appears.
3. From the **Edit User Details** page that appears, click the **CHANGE PASSWORD** button.
   A **Change Password** confirmation dialog box appears.



4. From the **Change Password** confirmation dialog box that appears, do the following:
   a. In the **Please type a new password** field, type the new password for the user.
   b. Click the **YES, CHANGE!** button.
5. The **Change Password** confirmation dialog box closes, and you are returned to the **Edit User Details** page. The user password is already committed to the system.

Note:
You do not have to click the **SAVE** button in the **Edit User Details** page as is only associated with the committing the **Admin** check box settings on the **Edit User Details** page.

5. CONFIGURING A RADIUS SERVER TO INTER-OPERATE WITH THE NE-ONE

The NE-ONE supports RADIUS authentication, allowing seamlessly integration within the Corporate/ Enterprise networks that use RADIUS servers to verify their users. In this situation, the NE-ONE acts as a RADIUS client.

Once the NE-ONE with is configured with the RADIUS authentication method, no user administration locally on the NE-ONE is required. All of the user administration (i.e. login credentials and permissions) is undertaken on the RADIUS server.

When users login to the NE-ONE, their login credentials are verified against the RADIUS server instead of the local NE-ONE database. The user permissions that are granted to each user vary according to `iTrinegy-NEONE` attributes that are added to the each user (see *Add iTrinegy-NEONE Attributes to New or Existing RADIUS Users* on page 211). If a user does not exist on the NE-ONE, upon the first login a `/Private` folder is created for them.

Note:
In order to access the NE-ONE for the first time, a local admin user exists using built-in authentication, which cannot be removed. The local admin user can therefore be used for initial access to the NE-ONE, and if necessary future access if the need arises. Additionally, because the local admin uses built-in authentication on the NE-ONE it would not conflict with an admin user on an RADIUS server if one exists.

Note:
For legacy purposes, on the current release of the NE-ONE the attributes, dictionary, and vendor use the term iTrinegy/itrinegy. In the future this is subject to change.

To configure a RADIUS server to inter-operate with the NE-ONE, follow sub-sections 5-1 to 5-3 below.

5-1. Configure the NE-ONE Authentication Method with the RADIUS Servers

During the initial configuration of the NE-ONE in *Chapter 4*, *Installation and Configuration*, you should have already configured the NE-ONE to point to the primary and secondary RADIUS servers using *Configuring RADIUS Authentication* on page 79. If not, do this configuration now.

5-2. Import the dictionary.itrinegy file into the RADIUS server

Illustration 59 shows the contents of the `dictionary.itrinegy` file that must be created and imported into the primary and secondary RADIUS servers that were defined in *Configuring RADIUS Authentication* on page 79.

ILLUSTRATION 59 - CONTENTS OF DICTIONARY.ITRINEGY FILE

```
VENDOR      iTrinegy            57621

BEGIN-VENDOR iTrinegy

ATTRIBUTE           iTrinegy-NEONE-Login                1       integer
VALUE       iTrinegy-NEONE-Login        Login-Enabled       1
VALUE       iTrinegy-NEONE-Login        Login-Disabled      2

ATTRIBUTE           iTrinegy-NEONE-Admin                2       integer
VALUE       iTrinegy-NEONE-Admin        Admin-Enabled       1
VALUE       iTrinegy-NEONE-Admin        Admin-Disabled      2

ATTRIBUTE           iTrinegy-NEONE-Ports                3       string
ATTRIBUTE           iTrinegy-NEONE-Networks             4       integer
ATTRIBUTE           iTrinegy-NEONE-Objects              5       integer
ATTRIBUTE           iTrinegy-NEONE-Links                6       integer

END-VENDOR iTrinegy
```

Use the following steps to create the `dictionary.itrinegy` file.

1. Create a text file called `dictionary.itrinegy`.
2. Copy and paste the contents of *Illustration 59* into the `dictionary.itrinegy` file.
3. Save the `dictionary.itrinegy` file.

   The `dictionary.itrinegy` file is now ready to be imported into the primary and secondary RADIUS servers.

The sub-sections below describe how to import the `dictionary.itrinegy` file into the primary and secondary RADIUS servers.

Note:

At the time of writing, only the FreeRADIUS (version 3.0) server solution is described. However, the principles are similar for other RADIUS server solutions. For other RADIUS server solutions, contact your Calnex support representative or Calnex support, if required.

5-2-1. Example Import Procedure Using FreeRADIUS

On both the primary and secondary FreeRADIUS servers, use the following steps to import the `dictionary.itrinegy` file into the server dictionary area:

1. Copy the `dictionary.itrinegy` file into the `/usr/share/freeradius` directory.
2. Edit the `dictionary` located in the `/usr/share/freeradius` directory, by entering:

   `sudo gedit /usr/share/freeradius/dictionary`

   Then add the following line to include the `dictionary.itrinegy` file:

   `$INCLUDE dictionary.itrinegy`

   The example below, shows a `/usr/share/freeradius/dictionary` file, with three include statements to three different dictionaries (including the `dictionary.itrinegy` file):

   `$INCLUDE dictionary.itk`

   `$INCLUDE dictionary.itrinegy`

   `$INCLUDE dictionary.ipunplugged`
3. Restart the FreeRADIUS server for the changes to take effect, by entering:

   `sudo /etc/init.d/freeradius restart`

   During the restart, the `dictionary.itrinegy` file is now included in the RADIUS server's configuration, and is active.

5-3. Add iTrinegy-NEONE Attributes to New or Existing RADIUS Users

If a user on the RADIUS server has no `iTrinegy-NEONE` attributes, it will obviously not able to access the NE-ONE. You may want to edit existing users and/or add new users on your RADIUS servers for use with the NE-ONE.

The `iTrinegy-NEONE` attributes that you add to either a new or existing user on the RADIUS server will determine what permissions that user has on the NE-ONE. Looking at the contents of the `dictionary.itrinegy` file in *Illustration 59* we see that there are six attributes, summarized in *Table 32*.

TABLE 32 - CALNEX-NEONE RADIUS SEVER USER ATTRIBUTES

Attribute	Description
`iTrinegy-NEONE-Login`	This is a mandatory attribute, and determines whether or not the user can login to the NE-ONE. • If set to `Login-Enabled`, the user will be able to login to the NE-ONE. • If set to `Login-Disabled`, the user will not be able to login to the NE-ONE.
`iTrinegy-NEONE-Admin`	This is an optional attribute, and determines whether the user logged in to the NE-ONE is an admin type user or non-admin type user. • If this attribute is not added to the user, the user will be an non-admin type user on the NE-ONE. • If this attribute is added to the user, and set to `Admin-Enabled`, the user will be an admin type user on the NE-ONE. • If this attribute is added to the user, and set to `Admin-Disabled`, the user will be an non-admin type user on the NE-ONE. **Note:** An admin type user is automatically assigned all ports. Therefore, if you set the `iTrinegy-NEONE-Admin` attribute to `Admin-Enabled` for a user, you do not need to add the `iTrinegy-NEONE-Ports` attribute for that user. If you want an admin type user to not be automatically assigned all ports, you would also use the `iTrinegy-NEONE-Ports` attribute for that admin type user to define which ports are available.

Attribute	Description
iTringey-NEONE-Ports	This is an optional attribute, and determines the ports that are assigned to the user for use within their networks. • If this attribute is not added to a non-admin type user (i.e. iTringey-NEONE-Admin set to Admin-Disabled, the non-admin type user will not have any ports available to use within their networks. • If this attribute is not added to an admin type user (i.e. iTringey-NEONE-Admin set to Admin-Enabled, the admin type user will have all ports available to use within their networks. • If this attribute is added to the user, but has no string of values, the user will also not have any ports available to use within their networks. • If this attribute is added to the user, you must list the port names in a comma and spaced separated string surrounded by inverted commas (e.g. "<port name 1>, <port name 2>, <port name 3>"). The ports associated with port names that you listed will be available to the user. Additionally, any child ports belong to those ports will also be available to the user. **Note 1:** Hardware ports already exist on the NE-ONE. However, soft ports are created on the NE-ONE using the Port Manager. If you list any soft ports, you must ensure that they have been created on the NE-ONE using the Port Manager, and that match (including case sensitivity) the port names that were given to them. When specifying soft port names using the Port Manager, do not use spaces in their names if you use RADIUS authentication. **Note 2:** If you specify a hardware port that has child soft ports beneath it, the user will also inherit all the associated child soft ports. This is a useful logic to be aware of as it means that you can optionally avoid specifying individual soft ports, and simply specify the hardware port that they belong to. **Note 3:** You do not need specify port pairs in order for them to be assigned to the user. The NE-ONE will automatically present any port pairs that exist to the user if you have specified the appropriate left port name and right port name of the port pair that was defined within the Port Manager. For example, it a port pair called P0&1 is set up for hardware ports 0 and 1, and you have listed the port names 0 and 1 in the list of port names, the port pair called P0&1 to that user.
iTringey-NEONE-Networks	This is an optional attribute, and determines the maximum number of networks that can be run by the user. • If this attribute is not added to the user, the user is able to run an unlimited number of networks. • If this attribute is added to the user, you must specify an integer value (e.g. 1, 2, 3, etc.) for the maximum number of networks.
iTringey-NEONE-Objects	This is an optional attribute, and determines the maximum number of objects that can be used for the user's networks. • If this optional attribute is not added to the user, the user is able to use an unlimited number of objects within their networks. • If this attribute is added to the user, you must specify an integer value (e.g. 1, 2, 3, etc.) for the maximum number of objects.

Attribute	Description
iTrinegy-NEONE-Links	This is an optional attribute, and determines the maximum number of links that can be used for the user's networks • If this optional attribute is not added to the user, the user is able to use an unlimited number of links within their networks. • If this attribute is added to the user, you must specify an integer value (e.g. 1, 2, 3, etc.) for the maximum number of links.

The sub-sections below describe how to add iTrinegy-NEONE attributes to new or existing RADIUS users on the primary and secondary RADIUS servers.

Note:

At the time of writing, only the FreeRADIUS (version 3.0) server solution is described. However, the principles are similar for other RADIUS server solutions. For other RADIUS server solutions, contact your Calnex support representative or Calnex support, if required.

5-3-1. Defining User Permissions with Calnex-NEONE Attributes on FreeRADIUS

As shown in *Illustration 59* and described in *Table 32*, we see that there are six attributes that can be used to define the permissions of the users that use the NE-ONE. All users on FreeRADIUS are defined within the users file located in the /etc/freeradius/3.0 directory.

Note:

Two types of username format exist for a user on FreeRADIUS. The first format works without the suffix (i.e. without the @) e.g. bob, while the second format other works with the suffix (i.e. with the @) e.g. bob@itrinegy.com. Both username formats can exist in the /etc/freeradius/3.0/users file. If you use the second format, the user belongs to a realm, and that realm must be defined within the /etc/freeradius/3.0/proxy.conf file. It is beyond the scope of this *User and Administration Guide* to go into more detail with regards to the proxy.conf file. For more information, refer to the FreeRADIUS documentation and man pages.

The following example set of steps below, shows how to configure the different users with the different permissions as summarized in *Table 33*.

TABLE 33 - EXAMPLE SET OF USERS ON RADIUS SERVER WITH DIFFERENT NE-ONE PERMISSIONS

User	Password	Permissions					
		Login enabled	Admin user	Assigned Ports	Maximum Networks	Maximum Networks	Maximum Links
bob	bob1234	Yes	No	Hardware Ports 0 Hardware Port 1	5	50	Unlimited
sam	sam1234	Yes	Yes	Hardware Port 1 Hardware Port 2 Hardware Port 3 Hardware Port 4	Unlimited	Unlimited	Unlimited
sue	sue1234	Yes	No	Soft Port VLAN601	5	50	200
tom	tom1234	No	No	Hardware Port 0 Hardware Port 1	5	50	200

1. Open the FreeRADIUS users file in a text editor, by entering:
   sudo gedit /etc/freeradius/3.0/users
2. Add users to the file using the following format:

```
bob     Cleartext-Password := "bob1234"
         iTringey-NEONE-Admin := Admin-Disabled,
         iTringey-NEONE-Login := Login-Enabled,
         iTringey-NEONE-Ports := "0, 1",
         iTringey-NEONE-Networks := 5,
         iTringey-NEONE-Objects := 50

sam     Cleartext-Password := "sam1234"
         iTringey-NEONE-Admin := Admin-Enabled,
         iTringey-NEONE-Login := Login-Enabled,
         iTringey-NEONE-Ports := "0, 1, 3, 4"

sue     Cleartext-Password := "sue1234"
         iTringey-NEONE-Admin := Admin-Disabled,
         iTringey-NEONE-Login := Login-Enabled,
         iTringey-NEONE-Ports := "VLAN_601",
         iTringey-NEONE-Networks := 5,
         iTringey-NEONE-Objects := 50,
         iTringey-NEONE-Links := 200

tom     Cleartext-Password := "tom1234"
         iTringey-NEONE-Admin := Admin-Disabled,
         iTringey-NEONE-Login := Login-Disabled,
         iTringey-NEONE-Ports := "0, 1",
         iTringey-NEONE-Networks := 5,
         iTringey-NEONE-Objects := 50,
         iTringey-NEONE-Links := 200
```

3. Save and close the FreeRADIUS users file.
4. Verify that your changes did not introduce any syntax errors, by entering:
   sudo freeradius -CX

If you did not introduce any syntax errors, a message similar to the following appears:

```
...
Configuration appears to be OK
```

Note:

If you did introduce some syntax errors, an error message will appear. In this case, before proceeding to the next step, re-edit the FreeRADIUS users file to correct the errors, then save and close it.

5. Restart the FreeRADIUS server, by entering:

   `sudo /etc/init.d/freeradius restart`

   After the restart, the changes you made to the `/etc/freeradius/3.0/users` file are applied, and the users permissions are updated according to that changes that you made.

This page is intentionally left blank.

CHAPTER 7 SYSTEM MAINTENANCE

1. INTRODUCTION

This chapter is applicable to admin users, and describes the maintenance procedures that you use on a regular basis after NE-ONE has been installed and configured.

2. UPDATING THE SYSTEM SOFTWARE

The NE-ONE's internal software can be updated via the Web Interface.

2-1. Obtaining Software and Platform Updates

Calnex rigorously provide software updates in order to future proof the NE-ONE, keeping its feature set and functionality up-to-date with current industry standards.

For example, when a new network technology is implemented (e.g. 5G mobile network), its link type and all its link characteristics are added to the NE-ONE's database in the form of a software update.

Software updates are freely available for any NE-ONE that is covered by an active maintenance contract. You can find the renewal date of your NE-ONE's maintenance contract in the **My Model** section of the Web Interface's **Home** page (see *Home Page* on page 40).

For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date.

If you have an active maintenance contract, you can obtain the latest software and platform updates by following the steps below:

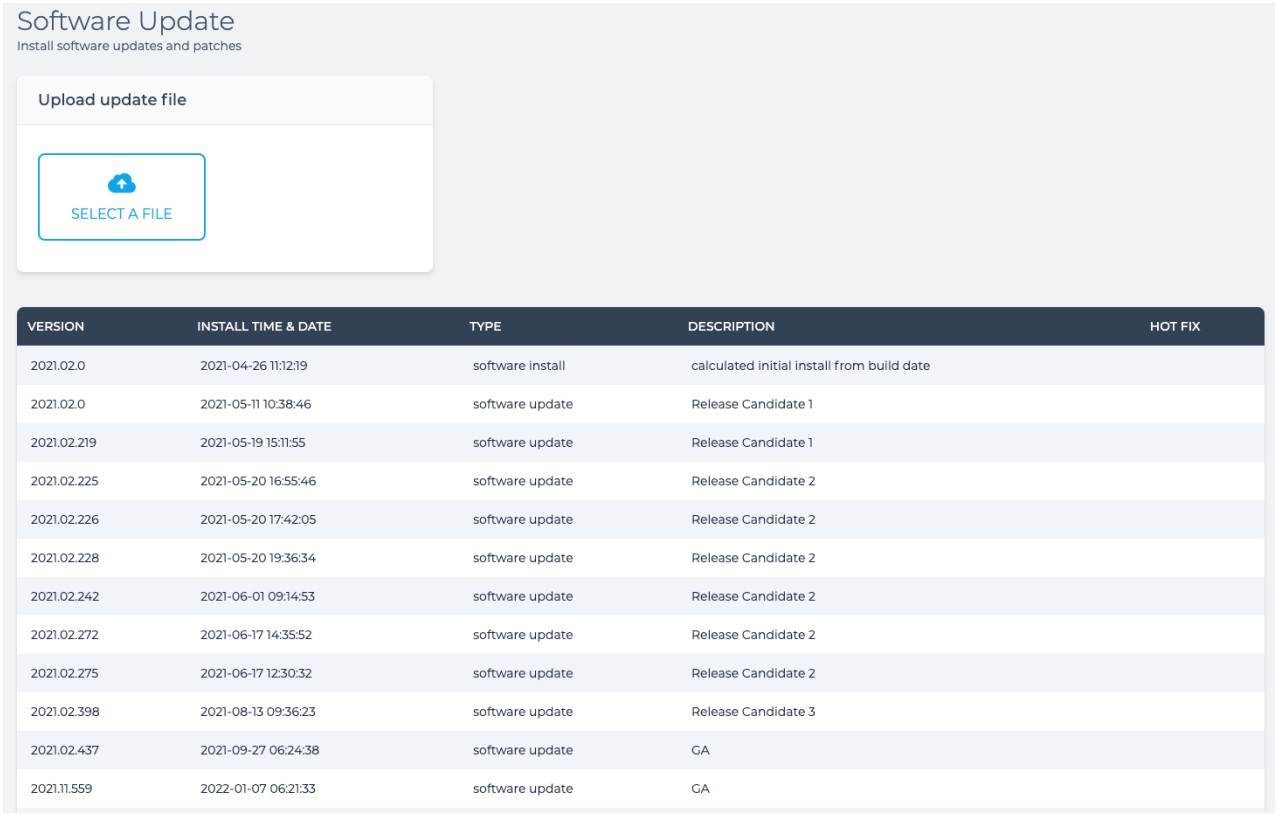
1. Calnex support or your support representative will notify you if a software or platform update is available for your NE-ONE.
2. View the current software versions installed on the NE-ONE (see *Viewing and Updating the System Software* on page 218).

   Make a mental note of the platform and software so you can compare them with what is currently available on the Calnex support site.
3. Go to the Calnex support site at *https://itrinegysupport.force.com* and login with your customer account.
4. Navigate within the Calnex support site, and if necessary download the appropriate software updates to your computer's local filing system.

2-2. Viewing and Updating the System Software

Use the following steps to view and/or update the system software on the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Software Update**.



VERSION	INSTALL TIME & DATE	TYPE	DESCRIPTION	HOT FIX
2021.02.0	2021-04-26 11:12:19	software install	calculated initial install from build date	
2021.02.0	2021-05-11 10:38:46	software update	Release Candidate 1	
2021.02.219	2021-05-19 15:11:55	software update	Release Candidate 1	
2021.02.225	2021-05-20 16:55:46	software update	Release Candidate 2	
2021.02.226	2021-05-20 17:42:05	software update	Release Candidate 2	
2021.02.228	2021-05-20 19:36:34	software update	Release Candidate 2	
2021.02.242	2021-06-01 09:14:53	software update	Release Candidate 2	
2021.02.272	2021-06-17 14:35:52	software update	Release Candidate 2	
2021.02.275	2021-06-17 12:30:32	software update	Release Candidate 2	
2021.02.398	2021-08-13 09:36:23	software update	Release Candidate 3	
2021.02.437	2021-09-27 06:24:38	software update	GA	
2021.11.559	2022-01-07 06:21:33	software update	GA	

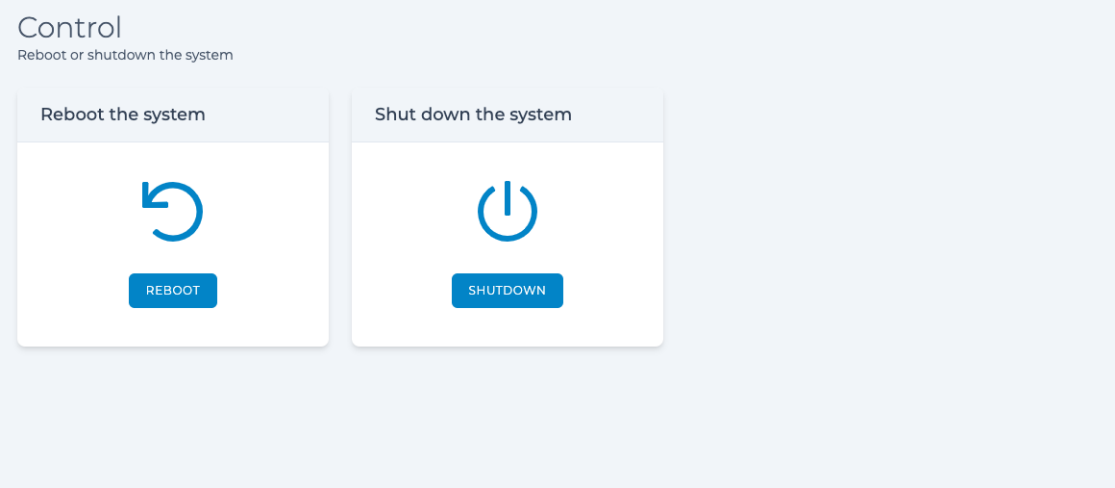
   A **Software Update** page appears, which contains:
   - a table listing the existing software versions installed on the NE-ONE
   - an area with a **SELECT A FILE** button, which lets you upload and apply a software update or software patch
2. View the existing software versions installed on the NE-ONE by reviewing the information in the table.
3. If you want to apply a software update or software patch, do the following:
   a. Obtain the appropriate software update and/or software patch as described in *Obtaining Software and Platform Updates* on page 217.
   b. Click the **SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the software update and/or software patch to upload.
4. From the **Success** confirmation dialog that appears, click **OK**.

3. CONTROLLING THE SYSTEM

On some occasions you may want to reboot or shut down the NE-ONE. For example, if you have applied a software or platform update, Calnex recommends that you reboot the NE-ONE. Similarly, if the NE-ONE needs to be physically moved or it is not being used for a period of time, you would gracefully shut it down.

The Control page (*Illustration 60*) allows you reboot or shut down the NE-ONE.

ILLUSTRATION 60 - CONTROL PAGE



3-1. Rebooting the System

Use the following steps to reboot the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Control**.
2. From the **Control** page that appears, click **Reboot**.
   The hardware version of the NE-ONE takes up to five minutes to reboot.
   The Virtual Machine version of the NE-ONE takes up to one minute to reboot.

3-2. Shutting Down the System

Use the following steps to gracefully shut down the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Control**.
2. From the **Control** page that appears, click **Shutdown**.
   The hardware version of the NE-ONE takes up to three minutes to gracefully shut down.
   The Virtual Machine version of the NE-ONE takes up to 30 seconds to gracefully shut down.

4. BACKING UP AND RESTORING THE SYSTEM

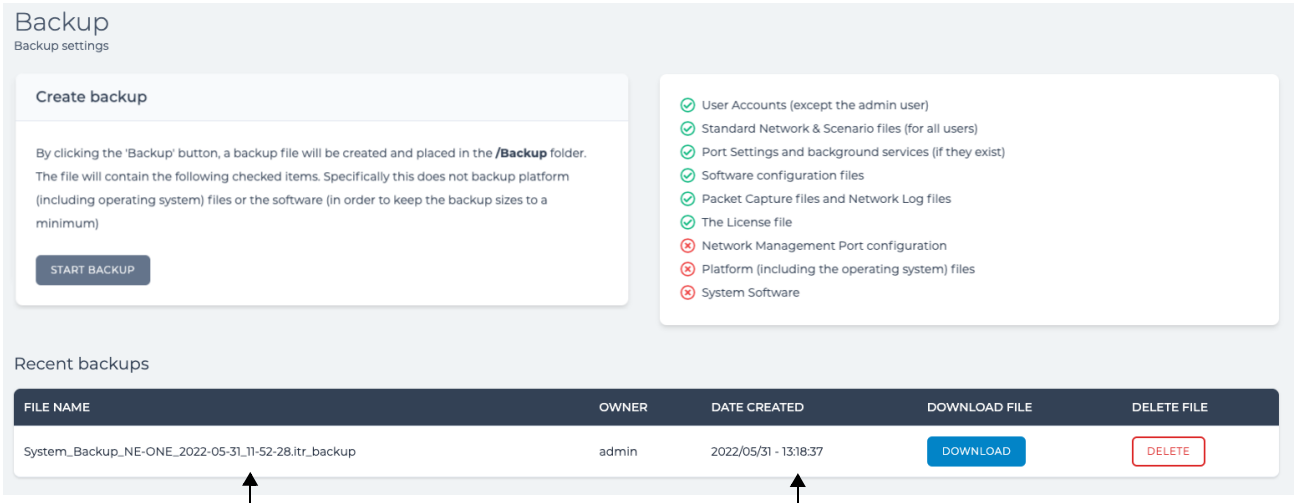
This section describes the principles and procedures associated with backing up, restoring backups, and managing backup files on the NE-ONE.

4-1. Backing up the System

When you create a system backup, the created backup file is stored locally on the NE-ONE in the `/Backup` directory, and can either be downloaded during the time you create the backup, or downloaded at a later date from the **Recent backups** area of the **Backup** page (see *Illustration 61*).

The backup file is of the format `System_Backup_NE-ONE_YYYY-MM-DD_HH-MM-SS.itr_backup` appears, where YYYY-MM-DD_HH-MM-SS is the UTC date and time of the NE-ONE when the backup process was initiated. When the backup process is complete, it is date and time stamped with the timezone defined in the Web Interface.

ILLUSTRATION 61 - BACKUP PAGE



Note: The date and time stamp of the filename and the date created is different. This is normal because the filename includes the UTC date and time of when the backup process was initiated, whereas the date created is the once the backup process has completed and for the timezone defined in the Web Interface management pages.

The backup file contains a backup of the following components of the NE-ONE:

- Built-in user accounts (except for the default admin user)
- Standard network and scenario files (for all users)
- Port settings and background services (if they exist)
- All the system configuration files (except for the network settings)
- Packet capture files and Network Log files
- License file

Note:

The management port settings (see *Configuring the Management Port Settings* on page 60) are not backed up. This is normal, as the design intent assumes that you may want to change the existing network settings after restoring a system backup, because you are either going to:

- restore the backup on another NE-ONE with different network settings

- restore the backup on the same NE-ONE but with different network settings

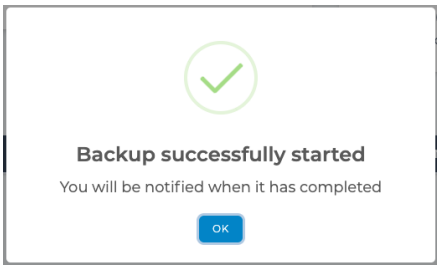
Note:
The platform files and software files are not backed up. This is normal. If you need to update the system platform or system software, you can follow the steps described within *Updating the System Software* on page 217.

The created backup file can be used at a later date to restore the NE-ONE to the level it was (with the exception of the management port settings) at the date of the backup.

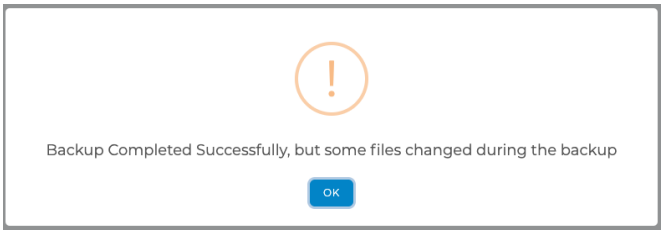
Note:
If over time you create many backups locally on the NE-ONE, and want to perform some general house keeping (i.e. delete older locally stored backup files), you can delete the locally stored backup files by following the steps in *Removing Old Backup Files* on page 224.

Use the following steps to backup the NE-ONE:

1. From the Web Interface, click **Management > ••• Platform Settings > Backup**.
   A **Backup** page (see *Illustration 61*) appears, which contains:
   - a **Recent backups** table listing any recent (if any) backups the NE-ONE
   - a **Create backup** area with a **START BACKUP** button, which lets you create a backup file by starting the backup process
2. Click **START BACKUP**.
3. From the **Backup successfully started** dialog box that appears, click **OK**.

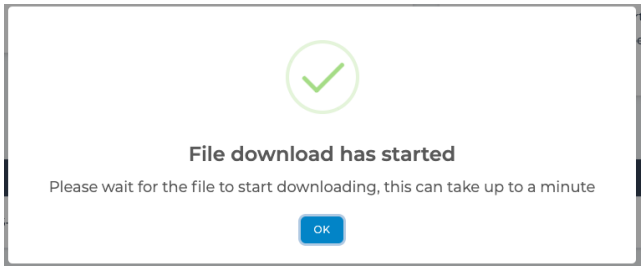


   The backup process runs in the background and can take several minutes to complete. While the backup file is being generated by the backup process, you can continue to the use the NE-ONE.
4. When the backup process is complete, from the **Backup Completed Successfully** dialog box that appears, click **OK**.



   When the backup process is complete, a backup file of the format `System_Backup_NE-ONE_YYYY-MM-DD_HH-MM-SS.itr_backup` appears in the **Recent backups** table of the **Backup** page.

5. Once the backup process is complete, if you want to download the backup file to your local computer, do the following:
   a. Click on the corresponding **DOWNLOAD** button from within the **DOWNLOAD FILE** column.
   b. From the **File download has started** dialog box that appears, click **OK**.



   The `*.itr_backup` automatically starts downloading to the location on your computer defined by the Web Browser you are using. The time it takes to download varies according to the file size and the connection speed with between your computer and the NE-ONE.

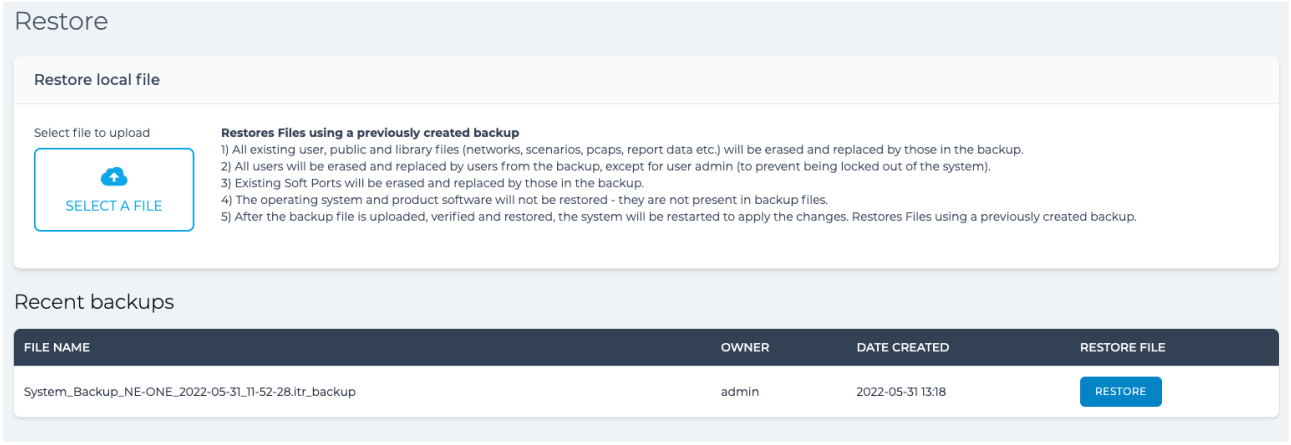
4-2. Restoring a System Backup

You can restore a previous backup on the same NE-ONE or another NE-ONE. You can restore a previous backup from either a:

- a local backup file that is already located on the NE-ONE (if it exists),
- a backup file that you have previously downloaded to your local computer.

Use the following steps to restore a previous backup on the NE-ONE:

1. From the Web Interface, click **Management > Platform Settings > Restore**.



   A **Restore** page appears, which contains:
   - a **Recent backups** table listing any recent (if any) backups the NE-ONE
   - a **Restore local file** area with a **SELECT A FILE** button, which lets you upload and apply a platform update
2. Perform one of the following restore methods:

   If you want to restore from a backup file located locally on your computer:
   a. Click **SELECT A FILE**.
   b. From the dialog box that appears, navigate your local filing system and choose the backup file (`*.itr_backup`) to upload.
   c. Once the backup file has uploaded to the NE-ONE, it appears in the **Recent backups** table from where it can be selected to be restored. Continue with the steps below to restore the backup file.

   If you want to restore from a backup file located locally on the NE-ONE:
   a. In the **Recent backups** table **RESTORE FILE** column, click on the **RESTORE** button corresponding to the backup file that you want to restore on the NE-ONE.
   b. In the **Restore Backup** confirmation dialog box that appears, click **OK**.

   Depending on the number of files that were backed up, the restore process of the NE-ONE takes between 30 seconds and a few minutes to complete. Once completed, a confirmation dialog box appears notifying you that the restore has completed.

4-3. Removing Old Backup Files

When you create a system backup, the associated backup file of the filename format `System_Backup_NE-ONE_YYYY-MM-DD_HH-MM-SS.itr_backup` is stored locally on the NE-ONE within the `/Backup` directory.

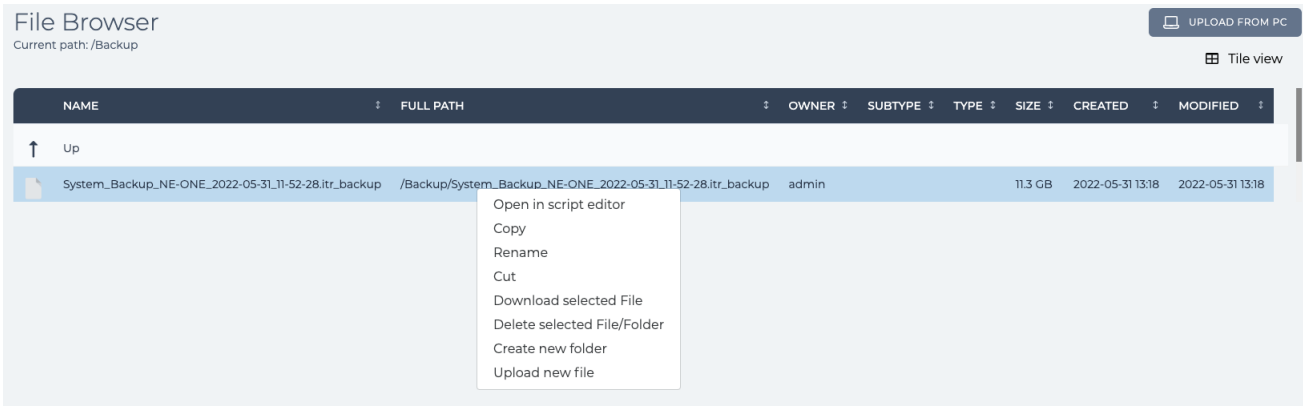
You can remove old backup files that are stored locally on the NE-ONE via either the **Backup** page or the File Browser.

If you want to remove old backup files that are stored locally on the NE-ONE via the **Backup** page, use the steps:

1. From the Web Interface, click **Management > ••• Platform Settings > Backup**.
2. From the **Backup** page (see *Illustration 61* on page 220) that appears, do the following for each of the old backup files you want to delete:
   a. In the **Recent backups** table **DELETE FILE** column, click on the **DELETE** button corresponding to the backup file that you want to delete.
   b. From the **Confirm delete** confirmation dialog box that appears, click **OK**.
   The **Recent backups** table updates, and no longer lists the backup file you deleted.

If you want to remove old backup files that are stored locally on the NE-ONE via the File Browser, use the steps:

1. Click **Management > ••• Platform Settings > File Browser** to launch the File Browser.
2. Navigate to the `/Backup` directory, and identify the backup file you want to delete via its file name (`*.itr_backup`).



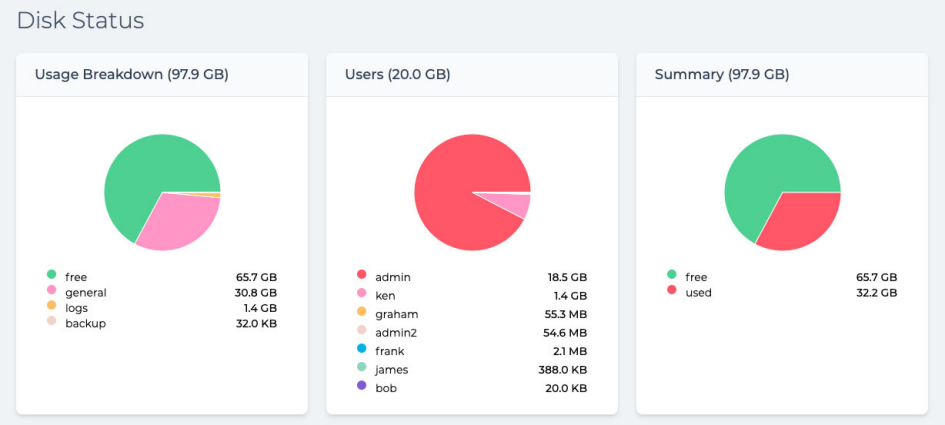
3. Right mouse click on the backup file, and select **Delete selected File/Folder** from the File Browser pop-up menu that appears.
4. From the **Confirm delete** dialog box that appears, click **OK**.

5. MONITORING SYSTEM DISK USAGE

The **Disk Status** page (*Illustration 62*) lets you survey the NE-ONE's disk usage, and details the amount of disk space used by different category tiles, such as:

- used vs remaining
- backup file usage
- **Usage Breakdown** tile, which summarizes the free disk space and the disk space used the following categories:
  - general : the files that are located in the each of the users `/Private` directory plus the files that are located in within the `/Run Data` directory.
  - logs : log files that are located in the `/Support` directory.
  - backup : backup files that are located in the `/Backup` directory.
- **Users** tile, which summarizes the total disk usage for all users, and the disk usage per user.
- **Summary** tile, which summarizes the free vs used disk space.

ILLUSTRATION 62 - DISK STATUS PAGE



Note:

Empty directories are 4 KB in size. Thus, even if no files exist within a directory, the empty directory uses 4 KB of disk space.

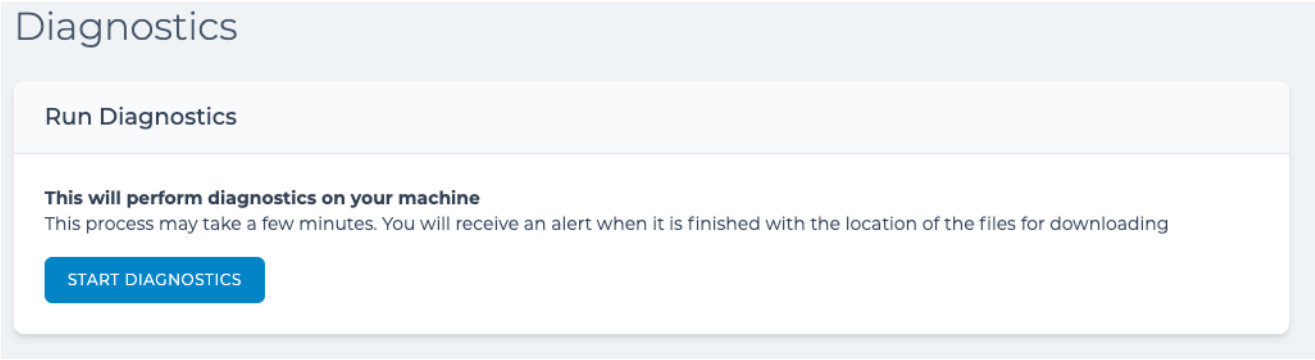
To view the **Disk Status** page, click **Management > ••• Platform Settings > Disk Status** .

You can use the **Disk Status** page in conjunction with the File Browser (see *Chapter 13*, *The File Browser*) it order to review if there is an excessive type of disk usage by a particular user or log files, for example, and if necessary take the appropriate house keeping (i.e. delete un-required file(s)) using the File Manager.

6. RUNNING DIAGNOSTICS

The **Diagnostics** page (*Illustration 63*) lets you run system diagnostics on the NE-ONE. System diagnostics are used in cases when your NE-ONE is not operating as expected, and your support representative or Calnex support has requested that you send them a diagnostics file. Running a system diagnostics results in generating a binary system diagnostics file, located in your `/Private` directory of the following filename format:
`System_Diagnostics_neone_<YYYY>_<MM>_<DD>_<HH>_<MM>_<SS>.itr_diagnostics`

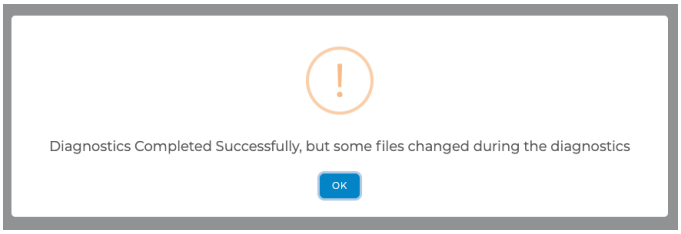
ILLUSTRATION 63 - DIAGNOSTICS PAGE



If you need to send a system diagnostics file to your support representative or Calnex support, use the following steps:

1. From the Web Interface, click **Management > ··· Platform Settings > Diagnostics**.
2. From the **Diagnostics** page that appears, click **START DIAGNOSTICS**.
   A **Diagnostics Started** dialog appears showing you the path of the resultant system diagnostics file.

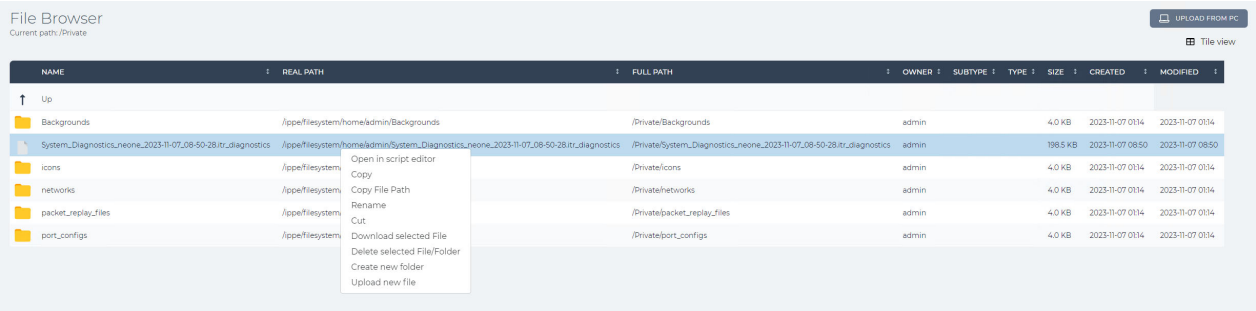
3. From the **Diagnostics Started** dialog that appears, click **OK**.
   The system diagnostics will run very quickly for a period of time.
   Once the system diagnostics have finished a **Diagnostics Completed Successfully** dialog appears, and the system diagnostics file is created in your `/Private` directory.



4. From the **Diagnostics Completed Successfully** dialog that appears, click **OK**.
   The confirmation dialog closes, and you are returned to the **Diagnostics** page.
5. From the Web Interface, click **Management > ··· Platform Settings > File Browser**.
   The **File Browser** page opens already with the path of your `/Private` directory.

Note:

To easily to be able to identify the system diagnostics file that you want to download, ensure that the File Browser is in **List view** mode. For more information, see *File Browser View Modes* on page 585 in *Chapter 13*, *The File Browser*.



6. Right mouse click on the system diagnostics file, and select **Download selected File**.

   The system diagnostics file is downloaded to your computer's local filing system. You can send this diagnostics file to your support representative or Calnex support.

7. RESETTING THE LOCAL ADMIN USER PASSWORD BACK TO THE DEFAULT VALUE

The default password for the local (built-in) admin user on the NE-ONE is admin. Upon connecting to the Web Interface for the first time, the local admin user will be prompted to change the password to another password other than admin. Once the local admin user has changed the default admin password they will be able to access the Web Interface pages.

If after changing the default local admin password, you want to reset it back to the default value admin, use the steps below.

Note:

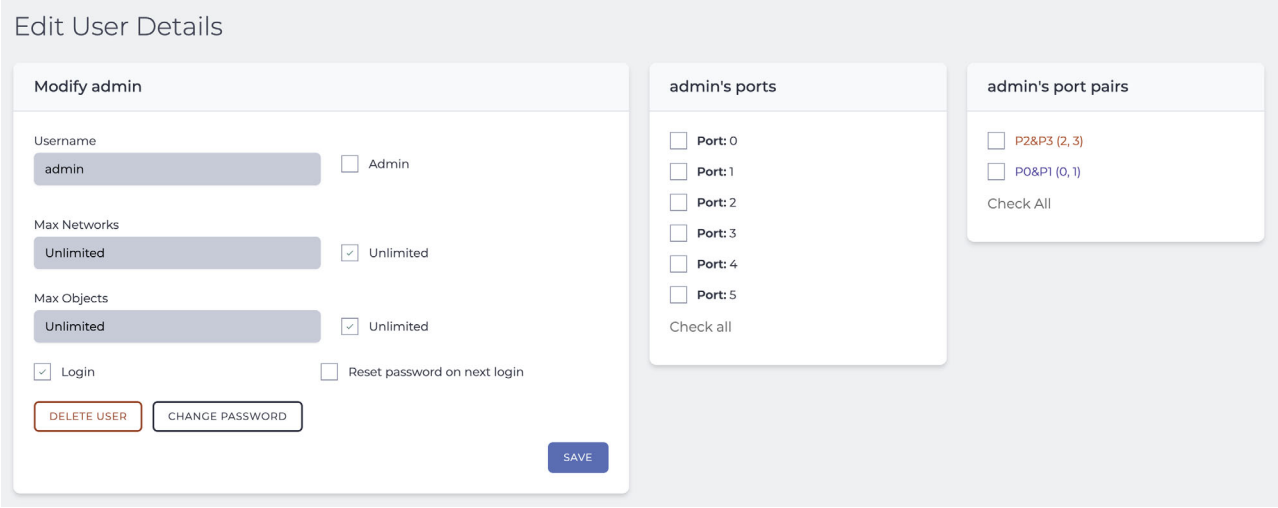
The steps below are only possible if you are logged in to the Web Interface as the local (built-in) admin user. If you login as another admin type, the **Reset password on next login** check box is not present in the **Edit User Details** page.

1. From the Web Interface, click **Management > ••• Platform Settings > Users**.

   A **Users** page (similar to *Illustration 57* on page 201) appears with a User List Table listing all the users.

2. From the **Users** page that appears, click on the row corresponding to the **admin** user.

An **Edit User Details** page appears.



3. From the **Edit User Details** page that appears, check the **Reset password on next login** check box.
4. From the **Success** confirmation dialog box that appears, click **OK**.

   The next time the local admin user logs in to the Web Interface, they will initially have to use the default password admin, and then be prompted to change the default password. For more information, see *Changing the Default Admin Password* on page 62 in *Chapter 4*, *Installation and Configuration*.

CHAPTER 8 GENERAL SYSTEM PROCEDURES

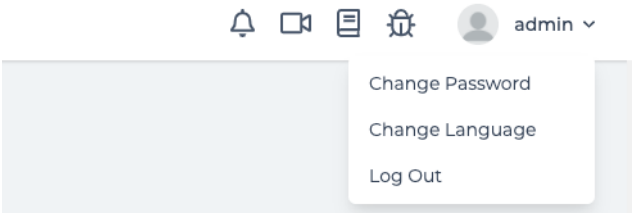
1. INTRODUCTION

This chapter is applicable to non-admin and admin users, and describes the general system related procedures of the NE-ONE.

2. USER RELATED PROCEDURES VIA THE TRAY USER MENU

The user menu in the tray (*Illustration 64*) provides menu items letting you log out of the Web Interface, change your password, or change the language displayed by the Web Interface.

ILLUSTRATION 64 - THE TRAY USER MENU



Note:

The **Change Password** menu item is only visible if the NE-ONE uses the built-in or LDAP authentication method. If the NE-ONE is configured with RADIUS authentication, the **Change Password** menu item will not be visible as the user passwords will be managed by the organization's Directory Access servers.

Note:

The LDAP and RADIUS authentication methods are part of the Advanced Authentication feature, which is a premium feature. Depending on your license, the LDAP and RADIUS authentication methods may be either activated or deactivated.

2-1. Logging Out of the Web Interface

To log out of the Web Interface either select **Log Out** from the tray user menu, or click on **Log Out** in the Menu. Upon logging out, any networks or scenarios that were running will continue to run.

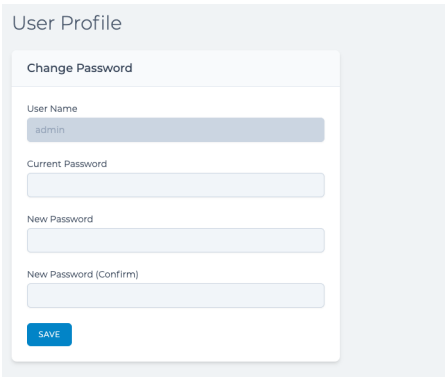
2-2. Changing Your User Password via the Tray User Menu

Note:
The user password can also be set via the **User Preferences** page (see *Illustration 67* on page 235). For more information, see *Changing Your User Password via the User Preferences Page* on page 235.

Selecting the **Change Password** menu item in the tray user menu opens a **User Profile** page.

Use the following steps to change your current user password:

1. In the tray click your username, and select **Change Password**.
   A **User Profile** page appears.



2. From the **User Profile** page that appears, type your existing password in the **Current Password** field, and new password in the **New Password** and **New Password (Confirm)** fields, then click **SAVE**.

2-3. Setting the Web Interface Language via the Tray User Menu

The Web Interface supports multiple languages, and the time of publication supports the languages listed in *Table 34*.

TABLE 34 - WEB INTERFACE SUPPORTED LANGUAGES

Language
English
French
German

By default for the admin user the Web Interface is displayed in English.

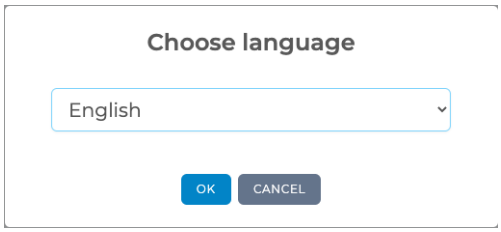
By default for the non-admin user the Web Interface is displayed in the currently chosen language of the admin user when they created the non-admin user. For example, if the admin user has chosen German for the Web Interface language, any users created by the admin use will inherit the German language as their default Web Interface language.

Note:
The Web Interface language can also be set via the **User Preferences** page (see *Illustration 67* on page 235). For more information, see *Setting the Web Interface Language via the User Preferences Page* on page 236.

Use the following steps to change the language displayed by the Web Interface:

1. In the tray click your username, and select **Change Language**.

A **Choose language** dialog box appears.



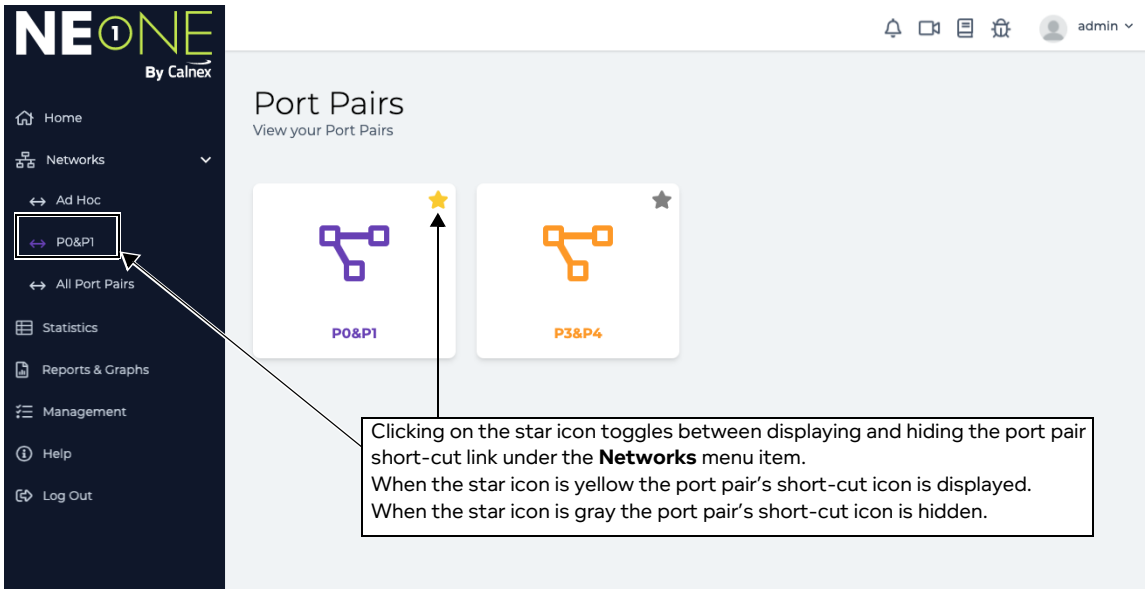
2. From the **Choose language** dialog box that appears, select the appropriate language you want the Web Interface to display, then click **OK**.

   The language you select is immediately applied to the Web Interface and persists for your future login sessions.

2-4. Creating "Starred" Port Pair Favorites

Starred port pairs (or port pair favorites) are port pairs that are assigned to be quickly accessible from under the **Networks** item in the Menu of the Web Interface. *Illustration 65* shows an example of a starred port pair called **P0&P1** appearing under the **Networks** item in the Main area of the Web Interface.

ILLUSTRATION 65 - PORT PAIRS PAGE (VIA ALL PORT PAIRS MENU ITEM)



Starred port pairs are extremely useful as they allow users to quickly choose a frequently used port pair, from where they can quickly create a Point-to-Point network (see *Creating Point-to-Point Networks (Examples)* on page 265 in *Chapter 9*, *Creating and Running Point-to-Point Networks*).

Once an admin user has assigned a port pair to another user (see *Creating Port Pairs* on page 158 and *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205), it can be starred by that user if it is deemed to be used frequently.

Use the following steps to star (favorite) an existing port pair (the following steps show an example of staring port pairs for the hardware ports 0 and 1):

1. From the Web Interface, click **Networks > ↔ All Port Pairs**.

   A **Port Pairs** page appears, containing a tile for each port pair that was assigned to you by the admin user.

   Each port pair tile contains a cog icon (⚙) letting you edit it, and a star icon (★) letting you favorite it.

   - Any port pairs that are assigned as a favorite have unfilled (gray) stars.
   - Any port pairs that are assigned as a favorite have filled (yellow) stars.

2. From the **Port Pairs** page that appears, click on the star (★) for each of the port pairs that you want to favorite, and have appear under the **Networks** menu item.

   Clicking on the star (★) icon toggles between displaying and hiding the port pair short-cut link under the **Networks** menu item. When the star (★) icon is filled (yellow), the port pair's short-cut icon is displayed. When the star (★) icon is gray (unfilled) the port pair's short-cut icon is hidden.

   The **Port Pairs** page updates such that the star corresponding favorited port pair becomes filled, and the favorite port pair also immediately appears under the **Network** menu item of the Web Interface.

3. VIEWING SYSTEM NOTIFICATIONS

To view the **Notifications** page (*Illustration 66*), either click **Management > System Notifications** or click the **Notifications** ( ) icon in the tray.

ILLUSTRATION 66 - SYSTEM NOTIFICATIONS PAGE

The **System Notifications** page chronologically displays events as they occur in different colors according to their event type (see *Table 35*).

TABLE 35 - NOTIFICATION EVENT TYPES

Color	Event Type	Example(s)
Red	Emergency	N/A to date
	Critical	No free disk space
	Error	Network failed to start

Color	Event Type	Example(s)
Yellow	Warning	User session expired Packet capture started Packet capture stopped Packet capture for user exceeded file size limit
Orange	Alert	Disk space low
Green	Notice	Network actions: • Network started • Network stopped Scenario actions: • Scenario started • Scenario stopped **Note:** since networks and scenarios are conceptually the same in terms of their file content, notifications for networks and scenarios will use the same wording (i.e. "Network started..." or "Network stopped..."
Blue	Information	IPPE Runtime started
	Debug	N/A to date

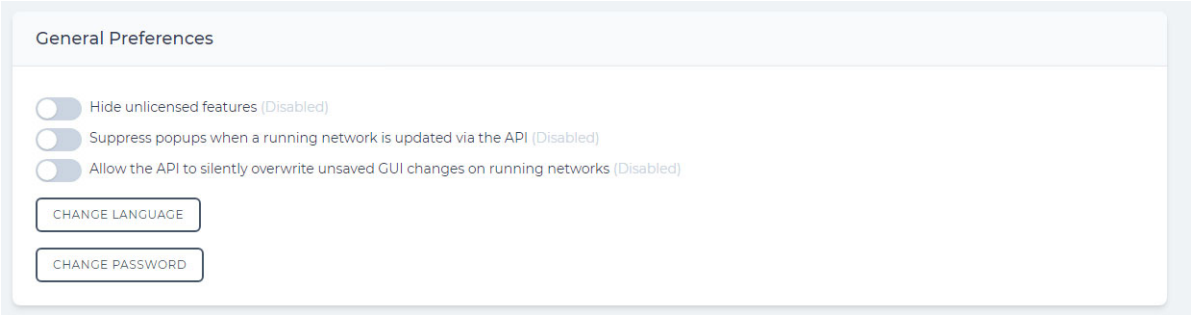
The **System Notifications** page contains the following, letting you customize the notifications that are displayed:

- **VIEW** menu button, with the time-frames **Last 24 hours**, **Last week**, **Last month**, **All**. By default, the **System Notifications** page displays all the notifications. Selecting an appropriate time-frame, updates the notifications accordingly.
- **FILTER** menu button, with check boxes corresponding to the event types listed in *Table 35*. By default, the **System Notifications** page displays all event types for the selected time-frame (and all the event type check boxes are unchecked). Ticking one or more of the event type check boxes, results in displaying only the selected event types that have occurred within the selected time-frame.
- **reset** link, which lets you reset the **System Notifications** page to the default display settings of all time and all event types.

4. USER RELATED PREFERENCES VIA THE USER PREFERENCES PAGE

To view the **User Preferences** page (see *Illustration 67*) click **Management > Preferences**.

ILLUSTRATION 67 - USER PREFERENCES PAGE



The **User Preferences** page contains the following:

- **CHANGE PASSWORD** button, which upon clicking allows the currently logged in user to change their current password. For more information, see *Changing Your User Password via the User Preferences Page* on page 235.
- **CHANGE LANGUAGE** button, which upon clicking allows the currently logged in user to change the language of the Web Interface that is displayed to them. For more information, see *Setting the Web Interface Language via the User Preferences Page* on page 236.
- **Hide unlicensed features** toggle switch, which allows the currently logged in user to show/hide deactivated (i.e. unlicensed) features. For more information, see *Displaying and Hiding Deactivated Features* on page 237.
- **Suppress popups when a running network is updated via the API** toggle switch, which allows the currently logged in user to suppress pop-ups when running networks are updated via the API. For more information, see *Suppressing Pop-Ups on Running Networks Updated via the API* on page 238.
- **Allow the API to silently overwrite unsaved GUI changes on running networks** toggle switch, which allows the currently logged in user to allow the API to silently overwrite unsaved GUI changes on running networks. For more information, see *Allowing the API to Silently Overwrite Unsaved GUI Changes on Running Networks* on page 238.

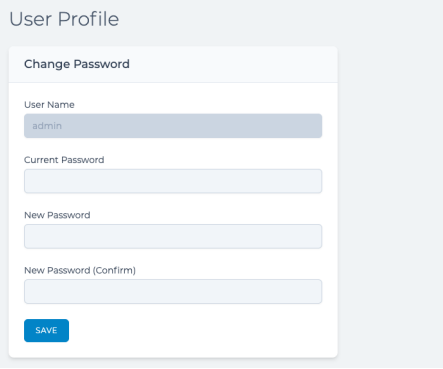
4-1. Changing Your User Password via the User Preferences Page

Note:
The user password can also be set via the tray user menu (see *Illustration 64* on page 229). For more information, see *Changing Your User Password via the Tray User Menu* on page 230.

Use the following steps to change your current user password:

1. From the Web Interface, click **Management > Preferences**.
2. From the **User Preferences** page (*Illustration 67*) that appears, click on the **CHANGE PASSWORD** button.

A **User Profile** page appears.



3. From the **User Profile** page that appears, type your existing password in the **Current Password** field, and new password in the **New Password** and **New Password (Confirm)** fields, then click **SAVE**.

4-2. Setting the Web Interface Language via the User Preferences Page

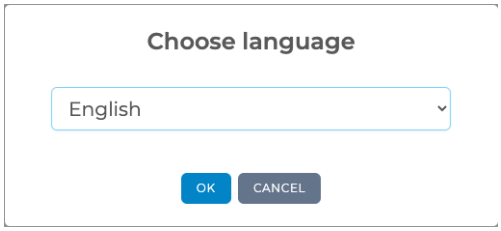
Note:

The Web Interface language can also be set via the tray user menu (see *Illustration 64* on page 229). For more information, see *Setting the Web Interface Language via the Tray User Menu* on page 230.

Use the following steps to change the language displayed by the Web Interface:

1. From the Web Interface, click **Management >** **Preferences**.
2. From the **User Preferences** page (*Illustration 67*) that appears, click on the **CHANGE LANGUAGE** button.

   A **Choose language** dialog box appears.



3. From the **Choose language** dialog box that appears, select the appropriate language you want the Web Interface to display, then click **OK**.

   The language you select is immediately applied to the Web Interface and persists for your future login sessions.

4-3. Displaying and Hiding Deactivated Features

Depending on your license, some of the premium features may be deactivated (i.e. unlicensed). By default, when you log in to the Web Interface, any deactivated features are hidden. The **User Preferences** page (*Illustration 67* on page 235) lets you configure whether the deactivated features are displayed or hidden within the Web Interface.

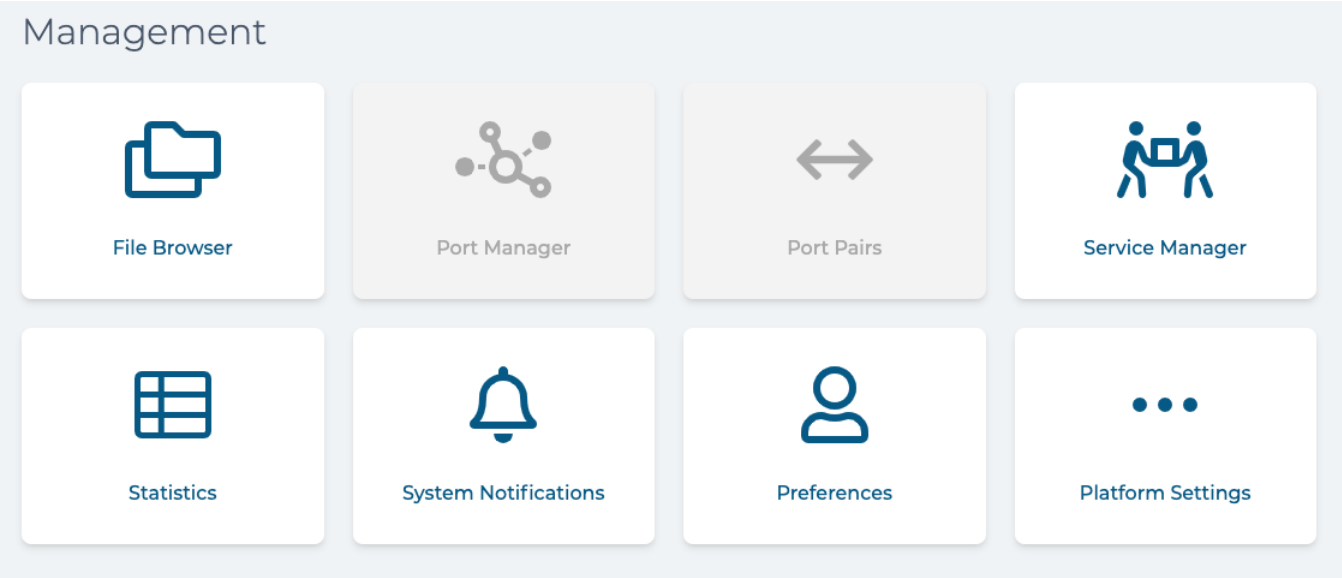
Note:
If the deactivated features are displayed, they are grayed out, and not functional.

Use the following steps set the display preferences for deactivated features:

1. From the Web Interface, click **Management >** **Preferences**.
2. From the **General Preferences** page (*Illustration 67*) that appears, click on the **Hide unlicensed features** switch to toggle between its ON (Enabled) and OFF (Disabled) states.
3. Upon toggling between ON (Enabled) and OFF (Disabled) states, a **Success** dialog box appears. Click **OK**.

   The **Success** dialog box closes, and the new settings take effect. *Illustration 68* shows an example of the **Management** page with settings related to the Port Manager feature grayed out.

ILLUSTRATION 68 - EXAMPLE OF THE MANAGEMENT PAGE WITH DEACTIVATED FEATURES DISPLAYED



4-4. Suppressing Pop-Ups on Running Networks Updated via the API

By default if a running network is updated via the API, a pop-up appears. These pop-ups can be suppressed if required.

Use the following steps to configure whether pop-ups appear for running networks when they are updated via the API:

1. From the Web Interface, click **Management > Preferences**.
2. From the **General Preferences** page (*Illustration 67*) that appears, click on the **Suppress popups when a running network is updated via the API** switch to toggle between its ON (Enabled) and OFF (Disabled) states.
3. Upon toggling between ON (Enabled) and OFF (Disabled) states, a **Success** dialog box appears. Click **OK**.
   - If the **Suppress popups when a running network is updated via the API** switch is set to OFF (Disabled), pop-ups will appear for a running network if it is updated via the API.
   - If the **Suppress popups when a running network is updated via the API** switch is set to ON (Enabled), pop-ups will not appear for a running network if it is updated via the API.

4-5. Allowing the API to Silently Overwrite Unsaved GUI Changes on Running Networks

By default, if network is running the API is not allowed to silently overwrite unsaved GUI changes on the running network. You can modify this default behavior so that the API is allowed to silently overwrite unsaved GUI changes on running networks.

Use the following steps to configure whether unsaved GUI changes on running networks are allowed to be silently overwritten by the API:

1. From the Web Interface, click **Management > Preferences**.
2. From the **General Preferences** page (*Illustration 67*) that appears, click on the **Allow the API to silently overwrite unsaved GUI changes on running networks** switch to toggle between its ON (Enabled) and OFF (Disabled) states.
3. Upon toggling between ON (Enabled) and OFF (Disabled) states, a **Success** dialog box appears. Click **OK**.
   - If the **Allow the API to silently overwrite unsaved GUI changes on running networks** switch is set to OFF (Disabled), the API will not be able to silently overwrite unsaved GUI changes on a running network.
   - If the **Allow the API to silently overwrite unsaved GUI changes on running networks** switch is set to ON (Enabled), the API will be able to silently overwrite unsaved GUI changes on a running network.

CHAPTER 9 CREATING AND RUNNING POINT-TO-POINT NETWORKS

1. INTRODUCTION

This chapter is applicable to non-admin and admin users, and describes:

- the general Web Interface associated with creating Point-to-Point type networks
- example procedures for creating Point-to-Point type networks

Network types can be categorized into two high-level topology types, as follows:

- Point-to-Point, including:
  - Point to Point (single)
  - Point to Point (dual hop)
- Multi-Point, including:
  - Fully Meshed
  - Hub and Spoke
  - Cloud (star)
  - Free Form

Note:

The Multi-Point Designer and associated Multi-Point network topologies (i.e. Fully Meshed, Hub and Spoke, Cloud, and Free Form) are only available with the Multi-Point Designer feature. Depending on your license, the Multi-Point Designer and associated Multi-Point network topologies may be either activated or deactivated.

This chapter is dedicated to creating and running Point-to-Point type networks. For creating and running Multi-Point networks, see *Chapter 10*, *Creating and Running Multi-Point Networks* on page 307.

2. PREREQUISITES

Before creating networks on the NE-ONE, an admin user must have already done the following:

- installed and set up the NE-ONE according to the procedures in *Chapter 4*, *Installation and Configuration*
- configured all the necessary port pairs, soft ports, and services according to *Chapter 5*, *Ports and Services Management*

Note:

The Port Manager feature and Service Manager feature are premium features. Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated.

- administered all users, and assigned appropriate ports and port pairs to the users according to *Chapter 6*, *User Administration* on page 199

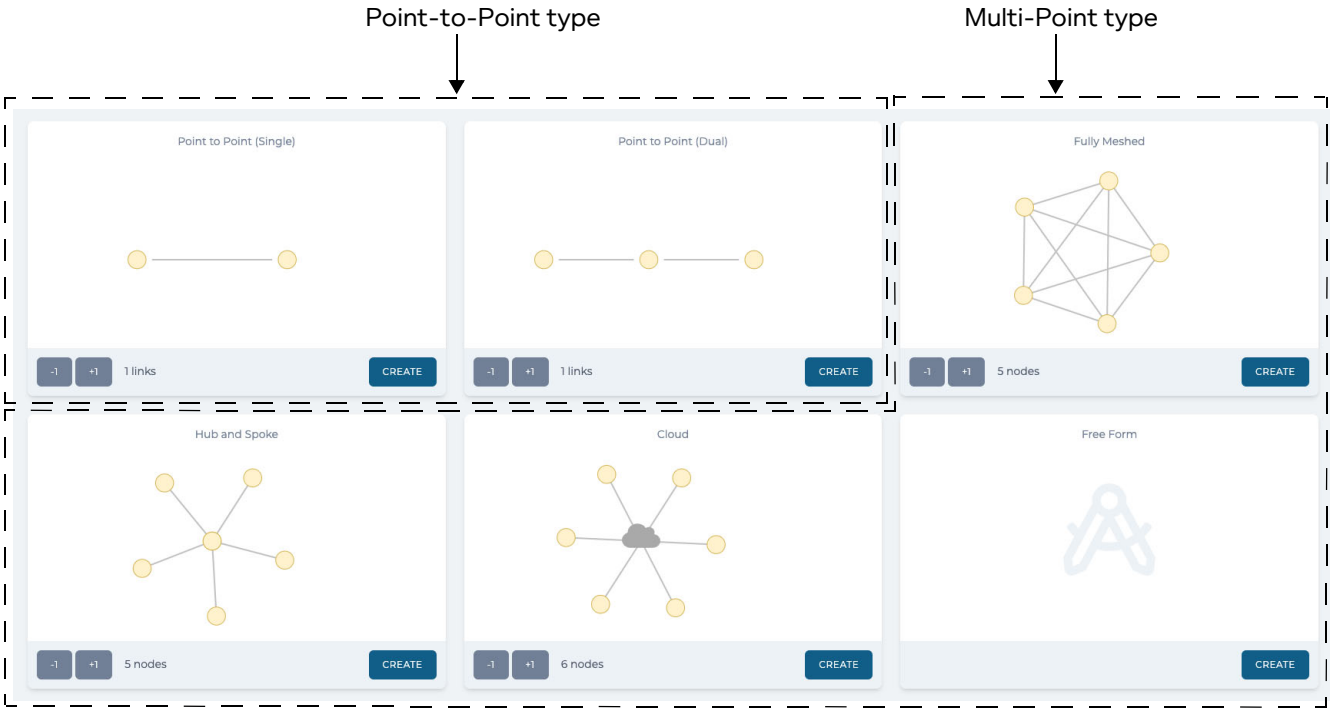
3. WEB INTERFACE NETWORK PAGES (POINT-TO-POINT)

This section contains a description of the Web Interface pages related to creating Point-to-Point type networks.

3-1. The Network Wizard Page (From a Point-to-Point Perspective)

The **Network Wizard** page (see *Illustration 69*) appears after clicking the **+ NEW NETWORK** button from the **Home** page (see *Illustration 3* on page 40), or clicking the **New Network** tile from the **Networks** page (see *Illustration 4* on page 42).

ILLUSTRATION 69 - NETWORK WIZARD PAGE



The **Network Wizard** page contains a network topology template tile for each of the network topology types, from where a network can be created.

The network topology types are categorized into two high-level types, as follows:

- Point-to-Point, including:
  - Point to Point (single)
  - Point to Point (dual hop)
- Multi-Point, including:
  - Fully Meshed
  - Hub and Spoke
  - Cloud
  - Free Form

Note:

The Multi-Point Designer and associated Multi-Point network topologies (i.e. Fully Meshed, Hub and Spoke, Cloud, and Free Form) are only available with the Multi-Point Designer feature. Depending on your license, the Multi-Point Designer and associated Multi-Point network topologies may be either activated or deactivated.

Each of the network topology template tiles (except Free form) contain a **-1** and **+1** button.

The **-1** and **+1** buttons for Point-to-Point network topologies function as follows:

- Clicking on the **+1** button each time for a Point-to-Point network topology increases the number of links between the nodes by one.
- Clicking on the **-1** button each time for a Point-to-Point network topology decreases the number of links between the nodes by one.

Note:
At least one link must exist between two nodes in a Point-to-Point network topology. Therefore, clicking the **-1** button when only one link exists has no effect.

Note:
At least one link must exist between two nodes in a Point-to-Point network topology. Therefore, clicking the **-1** button when only one link exists has no effect.

Note:
If you do not create the correct number of intended links during the Network Wizard stage, you can always add or delete links later on in the **Point To Point Designer** page.

Clicking on the **CREATE** button for either a Single or Dual (hop) Point-to-Point type network topology opens a series of dialog boxes, prompting you to choose the port (hardware or soft) to assign to the left port and then the right port, and then a dialog box prompting you to specify the network name.

Note:
If starred (favorited) port pairs have been set up by an admin user, they can be used instead to launch the network wizard for a Point-to-Point type network. Using a starred (favorited) port pair has the advantage of not needing to chose the left and right port assignments, as they are already specified in the port pair that was created by the admin user. For more information, see *The Port Pair Network Wizard Page* on page 242.

After specifying the network name, a **Point To Point Designer** page appears (*Illustration 71* on page 243 or *Illustration 72* on page 244), from where you can complete the configuration of the network (i.e. configure the nodes and links).

The type of **Point To Point Designer** page that appears varies according to which **CREATE** button you click. If you click the **CREATE** button within the **Point to Point (Single)** tile, the **Point To Point (Single) Designer** page appears (*Illustration 71* on page 243). If you click the **CREATE** button within the **Point to Point (Dual)** tile, the **Point To Point (Dual) Designer** page appears (*Illustration 72* on page 244).

For more information, see *Point To Point Designer Page for Point-to-Point Topologies* on page 242.

Note:
The network name you specify can contain alphanumeric characters, special characters (except /, \, and *), and spaces, and is used for the file name of the network. Once a network is saved, it is located in your `/Private/networks` directory and only accessible to you. You can share your networks with other users by using the File Browser. For more information on sharing networks, see *Sharing Networks via the File Browser* on page 593, in *Chapter 13*, *The File Browser*.

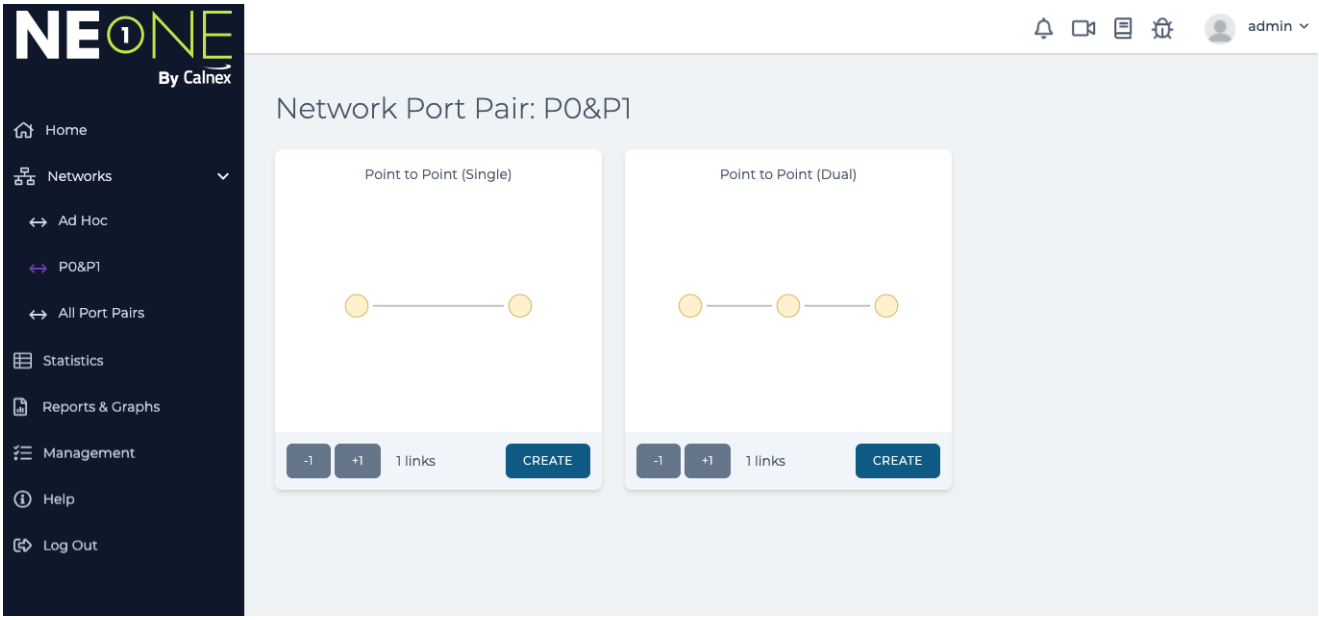
Note:
If creating a network on an NE-ONE Desktop which has an LCD panel, that network can optionally be made accessible from the LCD panel. In order for the network to be accessible to the LCD panel you must use the File Browser to copy the network from your `/Private/networks` directory to the `/Public/networks` directory. Then you must request an admin type user to copy the network from the `/Public/networks` directory to the `/Library/networks/LCD` directory. For more information, see *Making Networks and Scenarios Accessible to the LCD Panel* on page 596 in *Chapter 13*, *The File Browser*.

Note:
If you want a created network on an NE-ONE Desktop to be accessible via the LCD panel, consider the fact that it has two lines of 20 characters. If a network name exceeds 18 characters, it will appear truncated in the LCD panel.

3-2. The Port Pair Network Wizard Page

The **Port Pair Network Wizard** page (see *Illustration 70*) appears after selecting a port pair (↔) from within the expanded **Networks** item in the Menu and after clicking the **New Network** tile from the **Network Port Pair** page for the selected port pair (see *Illustration 5* on page 44).

ILLUSTRATION 70 - PORT PAIR NETWORK WIZARD PAGE



The **Port Pair Network Wizard** page contains a network topology tile for the Point-to-Point (single and dual hop) network topology types, from where a network can be created for the selected port pair.

Each of the Point-to-Point network topology tiles contain a **-1** and **+1** button, which function as follows:

- Clicking on the **+1** button each time increases the number of links between the nodes by one.
- Clicking on the **-1** button each time decreases the number of links between the nodes by one.

Note:
At least one link must exist between two nodes in a Point-to-Point network topology. Therefore, clicking the **-1** button when only one link exists has no effect.

Note:
If you do not create the correct number of intended links during the Network Wizard stage, you can always add or delete links later on in the **Point To Point Designer** page.

Clicking on the **CREATE** button for a Single or Dual (hop) Point-to-Point network topology directly opens the **Network Name** dialog box, letting you specify the network name for the selected port pair. After specifying the network name, a **Point To Point Designer** page appears, from where you can complete the configuration of the network (i.e. configure the nodes and links) for the selected port pair.

3-3. Point To Point Designer Page for Point-to-Point Topologies

Once a Point-to-Point type network has initially been created from either the **Network Wizard** page or **Port Pair Network Wizard** page, it appears in a **Point To Point Designer** page, from where its node and

links configuration can be completed. The type of **Point To Point Designer** page that appears varies according to which **CREATE** button you had clicked. If you had clicked the **CREATE** button within the **Point to Point (Single)** tile, the **Point To Point (Single) Designer** page appears (*Illustration 71*). If you had clicked the **CREATE** button within the **Point to Point (Dual)** tile, the **Point To Point (Dual) Designer** page appears (*Illustration 72*).

During the Network Wizard phase, only the network name is defined. All other aspects (i.e. nodes and links configuration) of the network must be completed from within the **Point To Point Designer** page.

Illustration 71 shows an example of a Single Point-to-Point network that was initially created with one link from the **Network Wizard** page.

ILLUSTRATION 71 - EXAMPLE POINT TO POINT (SINGLE) DESIGNER FOR A POINT-TO-POINT TOPOLOGY INITIALLY CREATED WITH ONE LINK

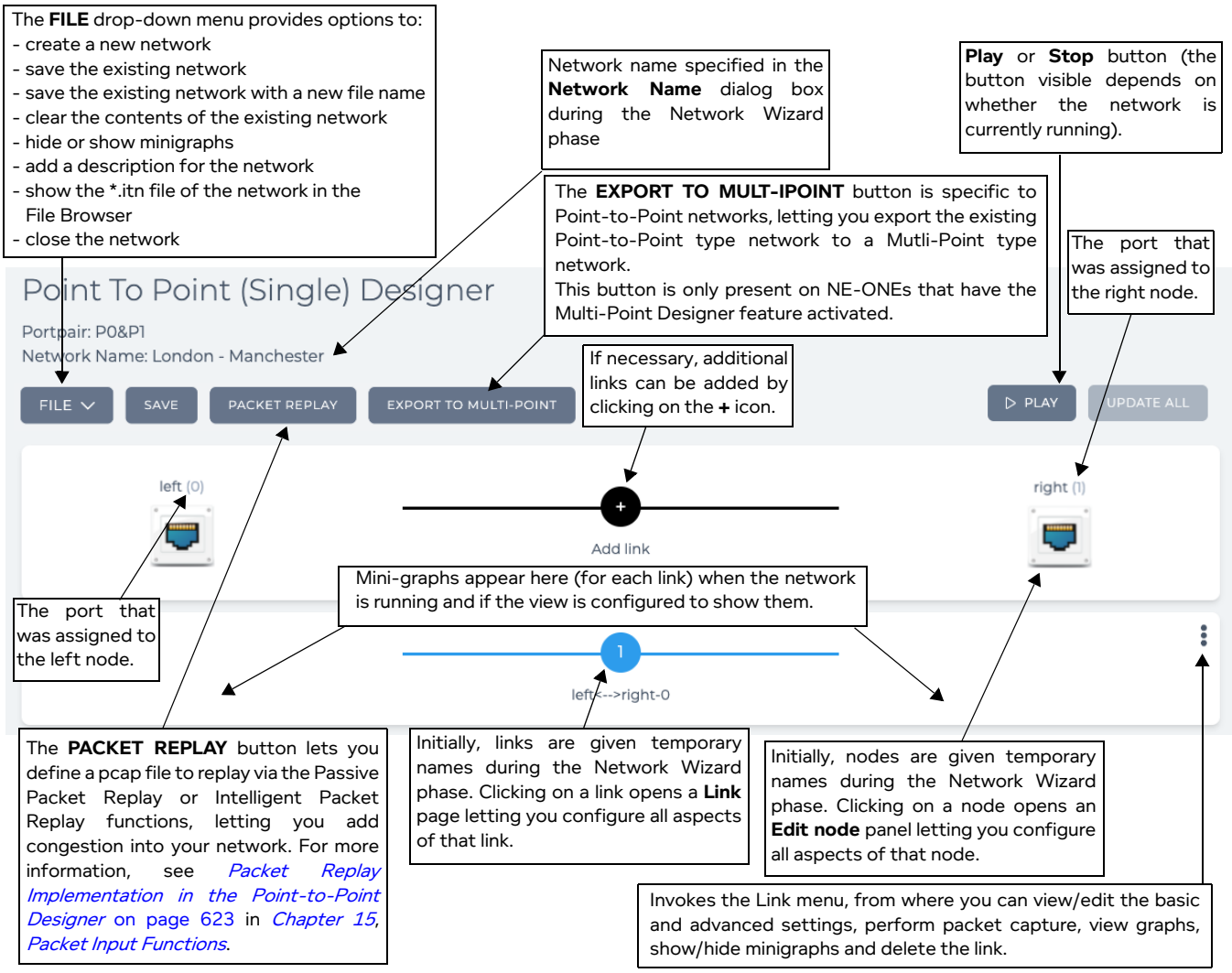
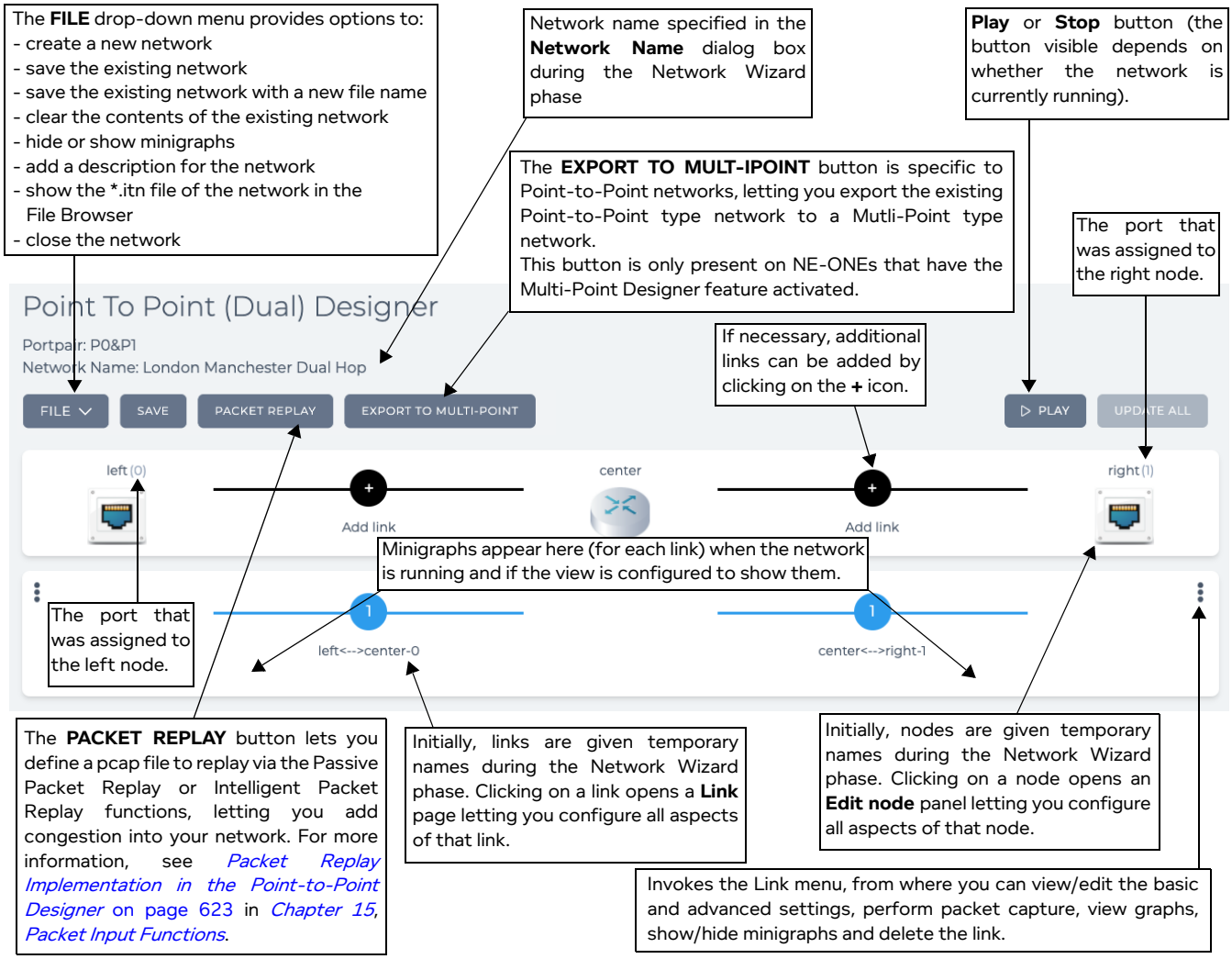


Illustration 72 shows an example of a Dual (hop) Point-to-Point network that was initially created with one link from the **Network Wizard** page.

ILLUSTRATION 72 - EXAMPLE POINT TO POINT (DUAL) DESIGNER FOR A POINT-TO-POINT TOPOLOGY INITIALLY CREATED WITH ONE LINK



The **Point To Point Designer** page contains the elements summarized in *Table 36*, and lets you create point-to-point networks with dual hop/last mile capability.

TABLE 36 - POINT TO POINT DESIGNER ELEMENTS FOR POINT-TO-POINT NETWORKS

Point To Point Designer Element	Description
FILE > New menu option	Selecting this option from the **FILE** drop-down menu keeps the current network open (indicated by either a play ⊙ symbol or edit ✎ symbol in the tray), and returns you to the **Network Wizard** page (see *Illustration 69* on page 240).
FILE > Save menu option	Selecting this option from the **FILE** drop-down menu saves the current network with the same file name in your `/Private/networks` directory.
FILE > Save as menu option	Selecting this option from the **FILE** drop-down menu opens a dialog box letting you save the current network with a different file name in your `/Private/networks` directory. Networks have file names with the `.itn` file extension.

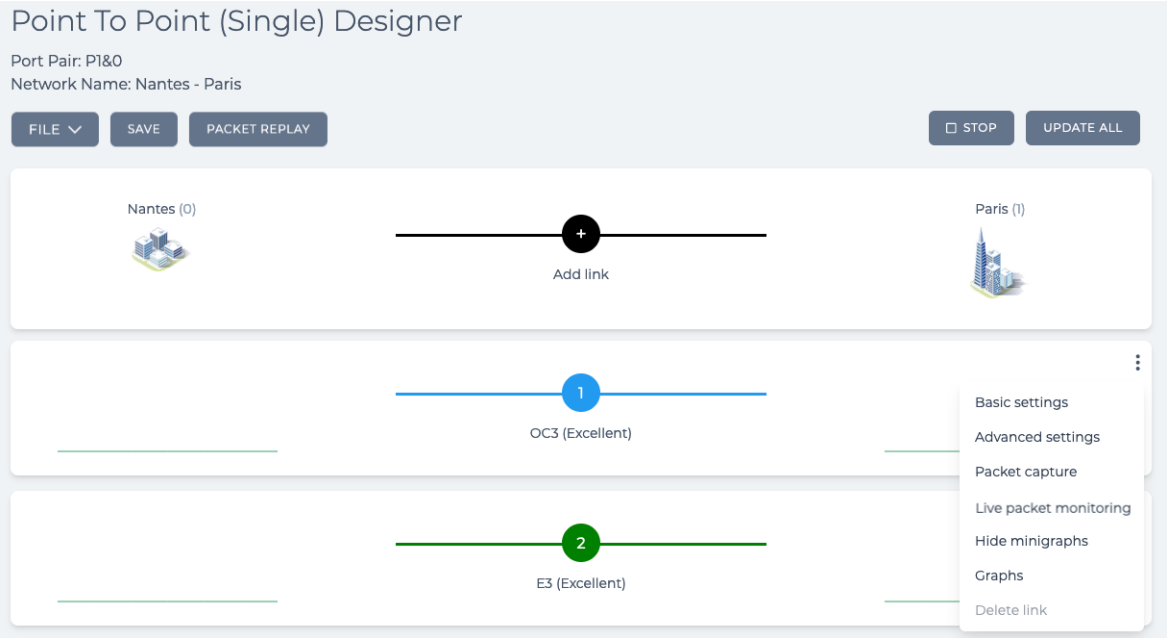
Point To Point Designer Element	Description
FILE > Description menu option	Selecting this option from the **FILE** drop-down menu opens a dialog box with a free field entry letting you write a description of the network, and how it is configured and to be used. Since your network can be complicated and shared with other users, this dialog box lets you describe important items that need to be remembered and communicate with other users.
FILE > Clear menu option	Selecting this option from the **FILE** drop-down menu removes all objects (i.e. node and links) from the Workspace.
FILE > Find in File Browser menu option	This is grayed out until the network has been saved. Selecting this option from the **FILE** drop-down menu opens the File Browser with the `.itn` file of the network selected.
FILE > Close menu option	Selecting this option from the **FILE** drop-down menu closes the network, and removes it from the Tray area of the Web Interface.
FILE > Hide minigraphs check box	By default minigraphs for each link are shown (i.e. this check box is un-ticked), and appear when a network is running. This check box lets you globally hide or show minigraphs for all the links defined in the Point-to-Point network. • Tick this check box to hide the minigraphs for all links in the Point-to-Point network. • Untick this check box to show the minigraphs for all links in the Point-to-Point network. **Note:** To individually hide/show minigraphs for each link in the Point-to-Point network on a per link basis, use the Link menu for each link (see *Link Menu* on page 247).
SAVE button	Clicking on this button saves the current network with the same file name in your `/Private/networks` directory.
EXPORT TO MULTI-POINT button	Clicking on this button opens a confirmation dialog box asking whether you want to export the Point-to-Point type network to Multi-Point type. Clicking **OK** in the confirmation dialog box results in converting and saving the Point-to-Point type network as a Multi-Point type network. Once a Point-to-Point type network is exported to a Multi-Point type network, it can no longer be opened in Point-to-Point mode. The exported network will then act as a Multi-Point type network, from where it can be edited in the Multi-Point Designer. **Note:** This button is only present on NE-ONEs that have the Multi-Point Designer feature activated.
▷ **PLAY** button or ☐ **STOP** button	The state of this button varies according to whether or not the network is running. When the network is not running, a ▷ **PLAY** button is present, and the status icon for the network in the tray is ✎. Clicking on the ▷ **PLAY** button results in: • running the network • changing the network status icon to the play ⏵ symbol • changing the button state to ☐ **STOP** When the network is running, a ☐ **STOP** button is present, and the status icon for the network in the tray is ⏵. Clicking on the ☐ **STOP** button results in: • stopping the network • changing the network status icon to the edit ✎ symbol • changing the button state to ▷ **PLAY**

Point To Point Designer Element	Description
UPDATE ALL button	This button is grayed out when the network is not running. When the network is running, this button is active. When the network is running, you can edit the parameters of the network (i.e. link and node parameters). Clicking this button applies all the changed parameters on the fly to the running network.
Node icons	For Point to Point (Single) networks left and right nodes exist. For Point to Point (Dual) networks left, right and center nodes exist. The port currently assigned to the node appears in brackets next to the node name. Each of the nodes need to be configured. Clicking on a node opens the **Edit node** panel, letting you configure all aspects of the node. For more information, see *Editing a Node via the Edit Node Panel (Point-to-Point Networks)* on page 249.
Links 	An initially created network contains non-configured links, with a default name **tempLink0**, **tempLink1**, etc. Typically, each link must be configured with a link type, link subtype and link quality. If a link is not configured, it acts as a no impedance link. Clicking on a link opens the link opens the **Link** page (see *Editing a Link via the Link Settings Pages (Point-to-Point Networks)* on page 251) from where you can configure the basic settings, link qualifications, and advanced settings (impairments). **Note:** It is normal and advisable, although not compulsory, to configure the links in number order.
Add Link 	Clicking on **Add link** opens a **Link name** dialog box from where you can specify the link name, and create a new link. Clicking **OK** in the **Link name** dialog box adds the new link in the **Point To Point Designer** page. Once a new link is added, typically it must be configured with a link type, link subtype and link quality. If a newly added link is not configured, it acts as a no impedance link. Clicking on a newly added link opens the link opens the **Link** page (see *Editing a Link via the Link Settings Pages (Point-to-Point Networks)* on page 251) from where you can configure the basic settings, link qualifications, and advanced settings (impairments).

3-3-1. Link Menu

Clicking on the ⋮ icon for a link in the **Point Designer To Point Designer** page opens a Link menu (*Illustration 73*).

ILLUSTRATION 73 - LINK MENU



The Link menu remains visible until clicking its ⋮ icon. On clicking a link's ⋮ icon toggles between showing and hiding its Link menu.

The Link menu contains the menu items summarized in *Table 37*

TABLE 37 - LINK MENU ITEMS

Link Menu Item	Description
Basic settings	Selecting this menu item has the same effect as clicking on the link itself, and results in opening the **Link** page with the **LINK PROPERTIES** tab enabled, letting you configure the basic settings for that link. For more information, see *The (Basic Settings) Link Properties Page (Point-to-Point Networks)* on page 251.
Advanced settings	Selecting this menu item has the same effect as clicking on the **ADVANCED SETTINGS** button in the **Link** page, and results in opening the **Advanced Link Settings** page, letting you configure the advanced settings (i.e. impairments) for that link. For more information, see *The Advanced Link Settings Page (Point-to-Point Networks)* on page 256.
Packet Capture	When the network is not running (i.e. when the network is stopped, and being created or edited) this menu item is grayed out. When a network is running, this menu item is enabled. Selecting this menu item opens a **Packet Capture** dialog box (see *Illustration 161* on page 534), from where you can choose what packets to capture (before impairment, after impairment, or all) specific to that link. **Note:** you can also view all network objects (ports/nodes) and launch packet capture for a selected network object (port/node) from within the **Statistics** page. For more information, see *Launching Packet Capture on a PPO* on page 532, in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.

Link Menu Item	Description
Live packet monitoring	When the network is not running (i.e. when the network is stopped, and being created or edited) this menu item is grayed out. When a network is running, this menu item is enabled. Selecting this menu item opens a **Live Packet Monitoring** dialog box (see *Illustration 162* on page 542), from where you can choose which traffic direction to launch the live packet monitoring process on, specific to that link. For more information, see *Launching Live Packet Monitoring on a PPO* on page 540 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
Hide minigraphs / Show minigraphs	When the network is not running (i.e. when the network is stopped, and being created or edited) this menu item is grayed out. When a network is running, this menu item is enabled. Selecting this menu item lets you toggle between hiding and showing minigraphs for that link. Compared to the **FILE > Hide minigraphs** check box (which globally applies either showing or hiding of all minigraphs on all links), this menu item lets you show/hide minigraphs on for each link. If you want to show/hide minigraphs on a per link basis, use this menu item on each link to show/hide minigraphs according to your requirements instead of the **FILE > Hide minigraphs** check box.
Graphs	When the network is not running (i.e. when the network is stopped, and being created or edited) this menu item is grayed out. When a network is running, this menu item is enabled. Selecting this menu item opens a **Select data to monitor** dialog box (*Illustration 161* on page 534), from where you can select which type of data to graph for the node. Once you select which type of data to graph, the graph opens in a separate web browser tab. For more information, see *Launching Live Graphs on a PPO From an Active Network* on page 550 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*. **Note:** you can also view all network objects (ports/nodes) and launch graphs for a selected network object (port/node) from within the **Statistics** page. For more information, see *Launching Graphs for a PPO within the Statistics page* on page 552, in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
Delete link	When a network is running, this menu item is grayed out. Clicking this invokes a **Confirm delete** dialog box, which upon confirming (clicking **OK**) immediately deletes the link from the network.

3-3-2. Editing a Node via the Edit Node Panel (Point-to-Point Networks)

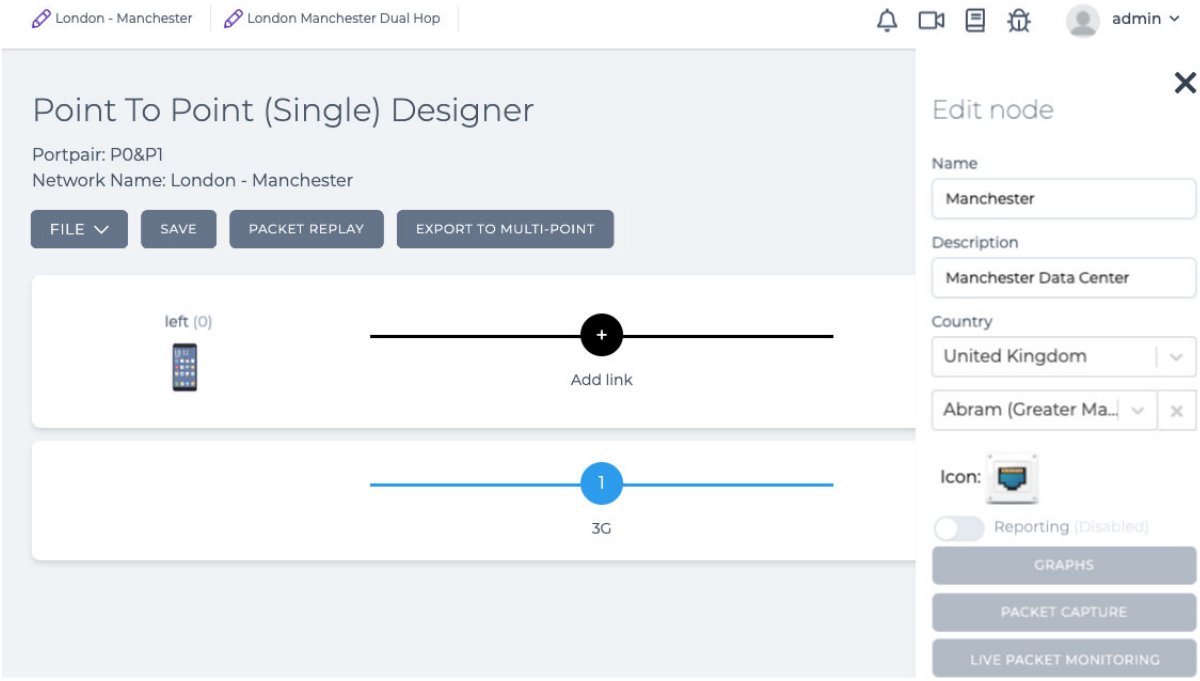
Upon clicking a node, the right hand side of the **Point To Point Designer** page updates with an **Edit node** panel (*Illustration 74*), allowing to you to configure all aspects of that node.

Note:

Any changes (e.g. node name) made in the **Edit node** panel are immediately reflected in the **Point To Point Designer** page, but not committed to the NE-ONE. To commit any node changes to the NE-ONE, either click the **SAVE** button or select **FILE > Save**.

The **Edit node** panel remains visible until clicking its ✕ icon. On clicking the ✕ icon the **Edit node** minimizes so that the **Point To Point Designer** page is fully visible.

ILLUSTRATION 74 - EXAMPLE EDIT NODE PANEL FOR A POINT-TO-POINT TYPE NETWORK



The **Edit node** panel contains the elements summarized in *Table 38*.

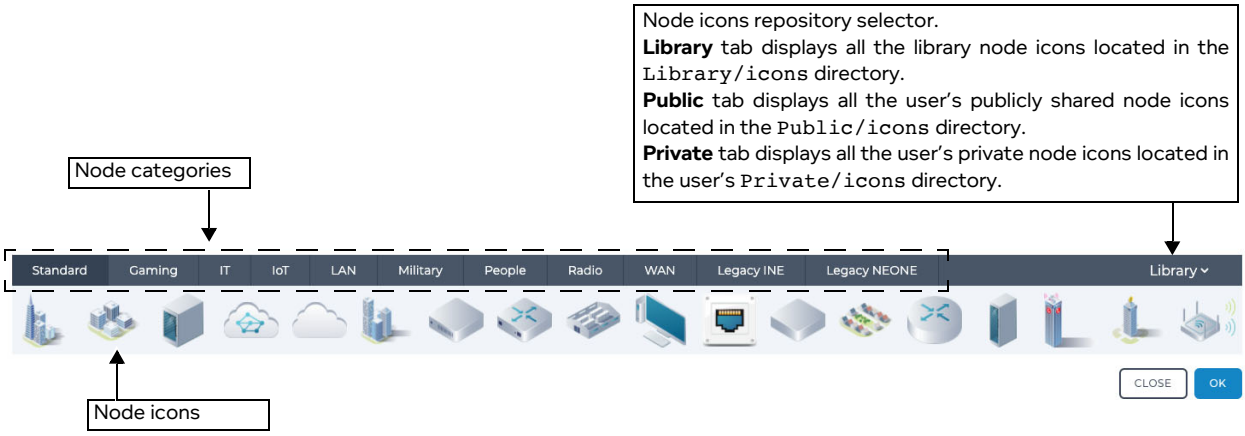
TABLE 38 - EDIT NODE PANEL ELEMENTS FOR POINT-TO-POINT NETWORKS

Edit node element	Description
Name field	Defines the name of the node that appears next to the node's icon in the **Point To Point Designer** page, and can contain alphanumeric characters, special characters, and spaces.
Description field	Defines the description of the node, and can contain alphanumeric characters, special characters, and spaces. The description appears in the mouse over for the node in the **Point-to-Point Designer** page.
Country drop-down field	Defines the country location of the node. Clicking on this drop-down field reveals a list of countries. **Note:** You can also type the name of the country to select it quickly from the list of countries.
Location drop-down field	Defines the location within the country of the node. Clicking on this drop-down field reveals a list of towns and cities associated with the selected country. **Note:** You can start typing the location in order to select it quickly from the list of locations.

Edit node element	Description
Icon graphic	Defines and shows the icon that represents the node. Clicking on this icon opens a dialog box (*Illustration 75*) containing a list of Library icons, Public icons, and Private icons. From this dialog box you can select a new icon to represent the node, and click **OK** to confirm the icon selection. • The Library node icons are standard icons delivered with the NE-ONE, and are located in the `Library/icons` directory. • The Private node icons are custom icons specific to the currently logged in user, and are located in the `Private/icons` directory. A new NE-ONE does not contain any Private node icons. You can use the File Browser to upload custom `*.png` files to your `Private/icons` directory. • The Public node icons are custom icons shared between all users, and are located in the `Public/icons` directory. A new NE-ONE does not contain any Public node icons. You can use the File Browser to upload custom `*.png` files to the publicly accessible `Public/icons` directory. For more information about upload uploading custom `*.png` files, see *Customizing and Sharing Node Icon Files* on page 587 in *Chapter 13*, *The File Browser*.
Reporting switch	By default, Application reporting is disabled for a node. When the network is not running (i.e. when the network is stopped, and being created or edited) this switch is grayed out. Clicking on this switch toggles between enabling and disabling Application reporting on the node. For more information, see *Viewing and Downloading Application Reports* on page 575 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*. **Note:** Applications reporting is a premium reporting feature. If you do not have the premium Applications reporting feature, the associated **Reporting** switch is not present.
GRAPHS button	When the network is not running (i.e. when the network is stopped, and being created or edited) this button is grayed out. When a network is running, this button is enabled. Clicking this button opens a **Select data to monitor** dialog box (*Illustration 161* on page 534), from where you can select which type of data to graph for the node. Once you select which type of data to graph, the graph opens in a separate web browser tab. For more information, see *Launching Live Graphs on a PPO From an Active Network* on page 550, in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*. **Note:** you can also view all network objects (ports/nodes) and launch graphs for a selected network object (port/node) from within the **Statistics** page. For more information, see *Launching Graphs for a PPO within the Statistics page* on page 552, in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
PACKET CAPTURE button	Clicking this button opens a **Packet Capture** dialog box (see *Illustration 161* on page 534), from where you can choose what packets to capture (before impairment, after impairment, or all) specific to that node. **Note:** you can also view all network objects (ports/nodes) and launch packet capture for a selected network object (port/node) from within the **Statistics** page. For more information, see *Launching Packet Capture on a PPO* on page 532, in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.

Edit node element	Description
Live Packet Monitoring button	Clicking this button opens a **Live Packets** dialog box (see *Illustration 163* on page 542), from where you can view the live packet monitoring data specific to that node. For more information, see *Launching Live Packet Monitoring on a PPO* on page 540 in *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing*.

ILLUSTRATION 75 - THE NODE ICON DIALOG BOX



3-3-3. Editing a Link via the Link Settings Pages (Point-to-Point Networks)

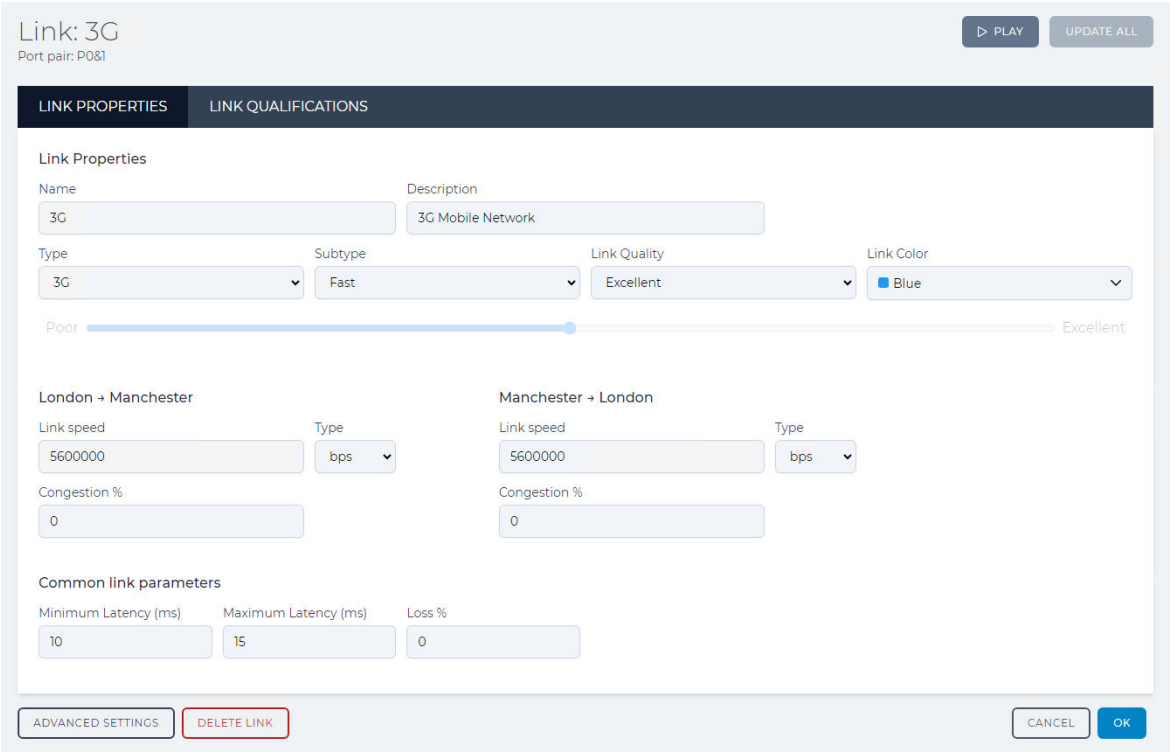
Clicking on a link (or selecting **Basic settings** from the Link menu) from within the **Point To Point Designer** page, opens the **Link** page for that link with the **LINK PROPERTIES** tab enabled (*Illustration 76*). The **Link** page contains the following areas, allowing to you to configure all aspects for the selected link:

- Basic Settings : Link Properties, which is accessed by clicking on the **LINK QUALIFICATIONS** tab (see *The (Basic Settings) Link Properties Page (Point-to-Point Networks)* on page 251)
- Basic Settings : Link Qualifications, which is accessed by clicking on the **LINK QUALIFICATIONS** tab (see *The (Basic Settings) Link Qualifications Page (Point-to-Point Networks)* on page 254)
- Advanced Settings, which is accessed by clicking on the **ADVANCED SETUP** button (see *The Advanced Link Settings Page (Point-to-Point Networks)* on page 256)

3-3-3-1. The (Basic Settings) Link Properties Page (Point-to-Point Networks)

The **LINK PROPERTIES** tab in the **Link** page (*Illustration 76*) lets you configure all the basic properties of the link. Typically the basic properties of a link need to be configured in order for the link to be run by the network. If the basic properties of a link are not configured, the link acts as a zero impedance link.

ILLUSTRATION 76 - EXAMPLE LINK PROPERTIES PAGE (POINT-TO-POINT NETWORKS)



The **Link Properties** page contains the elements summarized in *Table 39*.

TABLE 39 - LINK PROPERTIES PAGE ELEMENTS FOR POINT-TO-POINT NETWORKS

Link page element	Description
LINK QUALIFICATIONS tab	Clicking this tab opens the **LINK QUALIFICATIONS** page for the link, from where you can configure the link qualification criteria. For more information, see *The (Basic Settings) Link Qualifications Page (Point-to-Point Networks)* on page 254.
Name field	Defines the name of the link that appears next to the link in the **Point To Point Designer** page, and can contain alphanumeric characters, special characters, and spaces.
Description field	Defines the description of the link, and can contain alphanumeric characters, special characters, and spaces. The description appears in the mouse over for the link in the **Point-to-Point Designer** page.
Type drop-down field	Defines the link type. The link types available are summarized in *Appendix 3, Available Link Types and Link Sub-Types* on page 765.
Subtype drop-down field	Initially grayed out until the link type is selected from the **Type** drop-down field. The subtypes that are available depend on the link type that was selected from the **Type** drop-down field. The subtypes available for each link type are summarized in *Appendix 3, Available Link Types and Link Sub-Types* on page 765.
Link Quality drop-down field	Initially grayed out until the link subtype is selected from the **Subtype** drop-down field. The link qualities that are available depend on the link subtype that was selected from the **Subtype** drop-down field. The link qualities available for each link subtype are summarized in *Appendix 3, Available Link Types and Link Sub-Types* on page 765.

Link page element	Description
Link Color drop-down field	This defines the color of the link. The initial (default) color is blue. Clicking on this field provides a list of colors to choose from, letting you define the color of the link.
Poor to **Excellent** link quality slider	Once you define the link **Type** and **Subtype**, you can optionally use the **Poor** to **Excellent** link quality slider. When you use the **Poor** to **Excellent** link quality slider the **Link Quality** becomes custom and the **Common link parameters** (**Minimum Latencey (ms)**, **Maximum Latency (ms)**, and **Loss %**) automatically change according to the positioning of the slider.
Right Port to Left Port (initially the same values as Left Port to Right Port direction)	
Link Speed field	This field is initially empty, and automatically updates to a recommended link speed value once the link type, link subtype and link quality have been selected. If required, you can modify this to a different link speed. **Note:** For certain network links it is common to have different Link Speed values in the uplink and downlink directions. The NE-ONE defaults to symmetric values, which may need to be changed manually.
Type drop-down field	Lets you select a different unit so that the **Link Speed** field reformats the value for the selected unit.
Congestion % field	Defines the congestion on the link in percent (the higher the value, the higher the level of congestion). Congestion is usually a temporary state that occurs when the link cannot handle the traffic going through it. This field is initially empty implying no congestion (0% congestion). Because congestion is considered a temporary state, this field intentionally remains empty (0% congestion) once the link type, link subtype and link quality have been selected. If required, you can define a congestion percentage value so that congestion persists on the link.
Left Port to Right Port (initially the same values as Right Port to Left Port direction)	
Link Speed field	This field is initially empty, and automatically updates to a recommended link speed value once the link type, link subtype and link quality have been selected. If required, you can modify this to a different link speed. **Note:** For certain network links it is common to have different Link Speed values in the uplink and downlink directions. The NE-ONE defaults to symmetric values, which may need to be changed manually.
Type drop-down field	Lets you select a different unit so that the **Link Speed** field reformats the value for the selected unit.
Congestion % field	Defines the congestion on the link in percent (the higher the value, the higher the level of congestion). Congestion is usually a temporary state that occurs when the link cannot handle the traffic going through it. This field is initially empty implying no congestion (0% congestion). Because congestion is considered a temporary state, this field intentionally remains empty (0% congestion) once the link type, link subtype and link quality have been selected. If required, you can define a congestion percentage value so that congestion persists on the link.
Common Link Parameters (parameters that persist across the link equally for each port)	

Link page element	Description
Minimum Latency field	Defines the minimum latency in ms that is applied on the link. This field is initially empty, and automatically updates to a recommended minimum latency value once the link type, link subtype and link quality have been selected. If required, you can modify this to a different minimum latency value.
Maximum Latency field	Defines the maximum latency in ms that is applied on the link. This field is initially empty, and automatically updates to a recommended maximum latency value once the link type, link subtype and link quality have been selected. If required, you can modify this to a different maximum latency value.
Congestion % field	Defines the congestion on the link in percent (the higher the value, the higher the level of congestion). Congestion is usually a temporary state that occurs when the link cannot handle the traffic going through it. This field is initially empty implying no congestion (0% congestion). Because congestion is considered a temporary state, this field intentionally remains empty (0% congestion) once the link type, link subtype and link quality have been selected. If required, you can define a congestion percentage value so that congestion persists on the link.
ADVANCED SETTINGS button	Clicking this button opens the **Advanced Settings** page for the link, from where you can customize (i.e. add, remove, and order) the impairments that are applied on the link. For more information, see *The Advanced Link Settings Page (Point-to-Point Networks)* on page 256.
DELETE LINK button	Clicking this button invokes a **Confirm delete** dialog box, which upon confirming (clicking **OK**) immediately deletes the link from the network, and returns you to the **Point To Point Designer** page. **Note:** Clicking outside the **Confirm delete** dialog box cancels the delete operation, and returns you to the **Point To Point Designer** page.

3-3-3-2. The (Basic Settings) Link Qualifications Page (Point-to-Point Networks)

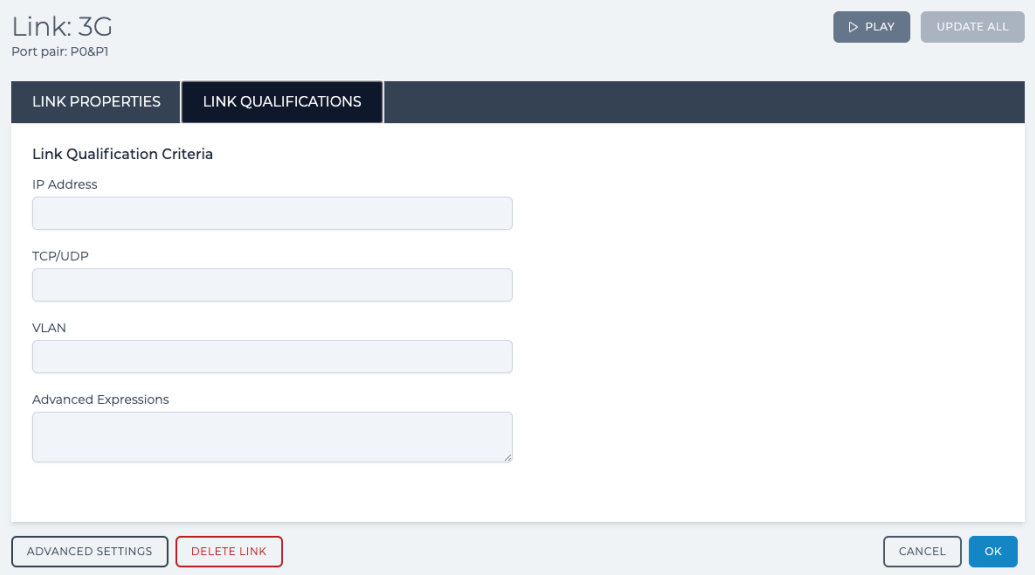
When you configure multiple links (multiple links between the nodes) it is necessary to define criteria specifying what traffic travels over which links. If you do not do this all traffic will go down the first configured link.

The link qualification criteria can also be used as a traffic filter. That is if you select a range of IP addresses for a particular link then only traffic associated with these source and destination IP addresses will traverse this link.

Where no links exist to handle certain traffic, this traffic will be dropped by the network.

Specifying what traffic travels over which link is handled in the **LINK QUALIFICATIONS** area of the **Link** page (*Illustration 77*).

ILLUSTRATION 77 - EXAMPLE LINK QUALIFICATIONS PAGE (POINT-TO-POINT NETWORKS)



The **LINK QUALIFICATIONS** area of the **Link** page contains the fields summarized in *Table 40*, which lets you select the IP addresses, TCP/UDP Ports and the VLAN tags that will be allowed to run over this link.

TABLE 40 - LINK QUALIFICATIONS PARAMETERS (POINT-TO-POINT NETWORKS)

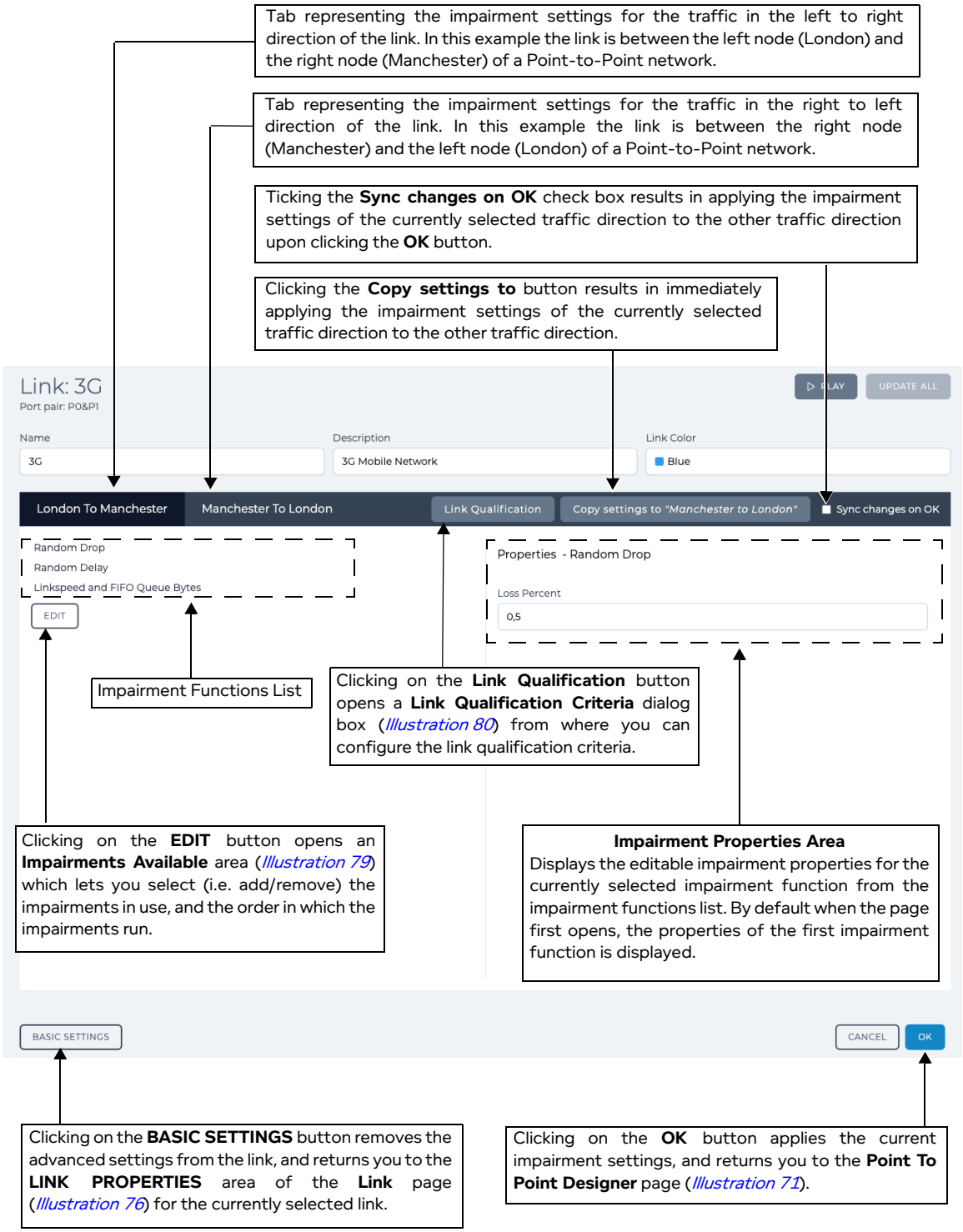
Link Qualification Parameter	Description
IP Address field	Defines the IP address, IP addresses or range of IP addresses that can run over the link, and uses a comma delimiter syntax with dashes. Examples: • To display data only related to IP addresses from 192.168.1.1 to 192.168.1.254, specify: **`192.168.1.1-192.168.1.254`** • To display data only related to IP addresses from 192.168.1.1 to 192.168.1.16 and 192.168.0.1 to 192.168.0.100 and IP address 192.168.1.154, specify: **`192.168.1.1-192.1.68.1.16,192.168.0.1-192.168.0.100,192.168.1.154`** • CIDR (Classless Inter-Domain Routing) notation is also accepted. For example, for the range 192.168.0.0 to 192.168.0.255 specify: **`192.168.0.0/24`**
TCP/UDP field	Defines the TCP and UDP ports that can run over the link, and uses a comma delimiter syntax with dashes. Examples: • To display data only related to ports 80 and 3289 to 3299, specify: **`80,3289-3299`** **Note:** What may assist you is that the port is set to 0 (for matching purposes) for all packets that do not have a port i.e. are (IPv4 and not UDP/TCP) or not IPv4. You can use this fact in packet matching, for example the port range 1-65535 would eliminate ICMP (IPv4 but not TCP/UDP) and ARP (not IPv4 at all) which have no port. Specifying 0 (zero) will match packets that do not have a port number such as ARP and ICMP (ping).
VLAN field	The VLAN field would typically be the VLAN/MPLS tag number. This is the VLAN Tag (ID) applied to Tagged VLAN packets by switches that are tagged VLAN packet aware. The VLAN tag needs to be set according to the 802.1Q standard.

Link Qualification Parameter	Description
Advanced Expressions field	This field lets you define link qualification criteria with more complex expressions. For example, **`ipv4.dst=192.168.100.1 OR ipv4.src=192.168.100.1`**. You must type an expression which describes (in Wireshark like syntax) data that qualifies for this link. For example: • **`eth.dst = 00:1B:21:91:D8:F6 or eth.src = 00:1B:21:91:D8:F6`** would select the single MAC address 00:1B:21:91:D8:F6 • **`ipv4.proto = 17`** would select only UDP packets • **`tcp.Destination_Port = 80 or tcp.source_Port = 80`** would select only port 80 for TCP, not UDP • **`ipv4.tos = x0A`** would select DSCP class AF11 **Note:** Link qualifications are in general symmetric so that both directions use the same link, hence source and destination used in the examples above. These expressions are ANDed with any of the selections that are specified in the **IP Address** field, **TCP/UDP** field and **VLAN** field. For more information, see *Link Qualification Expressions* on page 731 in *Appendix 1*, *Specifying Expressions*.

3-3-3-3. The Advanced Link Settings Page (Point-to-Point Networks)

Whilst the basic link settings are extremely intuitive and quick to use, there are also advanced link settings for the more experienced user that wants to setup more sophisticated network impairment configurations. The **Advanced Settings** area (*Illustration 78*) of the **Link** page lets you configure the impairments that are applied to the traffic on a link.

ILLUSTRATION 78 - ADVANCED SETTINGS AREA OF THE LINK PAGE (POINT-TO-POINT NETWORKS)



The **Advanced Settings** area of the **Link** page contains the elements summarized in *Table 41*.

TABLE 41 - ADVANCED LINK SETTINGS PAGE ELEMENTS FOR POINT-TO-POINT NETWORKS

Advanced Settings element	Description
▷ **PLAY** button or ☐ **STOP** button	The state of this button varies according to whether or not the network is running. When the network is not running, a ▷ **PLAY** button is present, and the status icon for the network in the tray is ✎. Clicking on the ▷ **PLAY** button results in: • running the network • changing the network status icon to the play ⏵ symbol • changing the button state to ☐ **STOP** When the network is running, a ☐ **STOP** button is present, and the status icon for the network in the tray is ⏵. Clicking on the ☐ **STOP** button results in: • stopping the network • changing the network status icon to the edit ✎ symbol • changing the button state to ▷ **PLAY**
UPDATE ALL button	This button is grayed out when the network is not running. When the network is running, this button is active. When the network is running, you can edit the parameters of the network (i.e. link and node parameters). Clicking this button applies all the changed parameters on the fly to the running network.
Left to right traffic direction tab	Tab representing the impairment settings for the traffic in the left to right direction of the link. Clicking on this updates the area below with the impairment configuration (i.e. impairment function properties) for the left to right traffic direction of the link.
Right to left traffic direction tab	Tab representing the impairment settings for the traffic in the right to left direction of the link. Clicking on this updates the area below with the impairment configuration (i.e. impairment function properties) for the right to left traffic direction of the link.
Link Qualification button	Clicking this button opens the **Link Qualification Criteria** dialog box for the link, from where you can configure the link qualification criteria. For more information, see *The (Advanced Settings) Link Qualification Criteria Dialog Box (Point-to-Point Networks)* on page 262.
Copy settings to button	Clicking this button results in immediately applying the impairment settings of the currently selected traffic direction to the other traffic direction.
Sync changes on OK check box	Ticking this check box results in applying the impairment settings of the currently selected traffic direction to the other traffic direction upon clicking the **OK** button. Unticking this check box results in not applying the impairment settings of the currently selected traffic direction to the other traffic direction upon clicking the **OK** button.
Impairment Functions List	Lists the impairment functions that currently apply to the link, and the order in which apply. Clicking on an impairment function updates the right hand side of the page with the properties of the impairment function.
Impairment Properties Area	Contains one or more fields letting you configure the currently selected impairment function.

Advanced Settings element	Description
EDIT button	Clicking this button opens an **Impairments Available** area (*Illustration 79*) which lets you add/remove the impairments in use, and the order in which the impairments run.
BASIC SETTINGS button	Clicking this button, returns you to the **LINK PROPERTIES** area of the **Link** page (*Illustration 76*) for the currently selected link and removing any advanced settings that were made for that link. **NOTICE:** clicking this button results in removing the advanced link settings, and returns the link to the basic settings using the default values of the three functions Random Drop, Random Delay and Linkspeed and FIFO Queue Bytes. The advanced settings for the link are not retained. Only click this button if you want to return the link properties back to the basic settings.
CANCEL button	Clicking this button ignores any changes you made to the current impairment settings, and returns you to the **Point To Point Designer** page (*Illustration 71*).
OK button	Clicking on the **OK** button applies the current impairment settings, and returns you to the **Point To Point Designer** page (*Illustration 71*).

By default, the traffic on a link initially includes the following set of impairment functions, in the following order:

- Random Drop (this is the equivalent of the **Loss %** value from the basic link settings).
- Random Delay (this is the equivalent of the **Minimum Latency (ms)** and **Maximum Latency (ms)** values from the basic link settings).
- Linkspeed and FIFO Queue Bytes (this is the equivalent of the **Link Speed** and **Congestion %** values for both link directions from the basic link settings).

Initially, when no **Type**, **Subtype** or **Link Quality** have been defined for a new link, the properties of these impairments are undefined. Once you defined the **Type**, **Subtype** or **Link Quality** for the link, the properties of these impairments are updated with recommended values.

Before defining the properties of each of the impairment functions associated with a link's traffic, you must update the list of impairment functions associated with that link according to your impairment requirements. The **Impairments Available** area (*Illustration 79*) of the **Link** page lets you define the impairment functions associated with the traffic on a link.

Clicking on the **Edit** button in the **Advanced Settings** area of the **Link** page opens and **Impairments Available** area (*Illustration 79*), which lets you select (i.e. add/remove) and order the impairment functions that are applied on the traffic for the link.

Once you have finalized the list and order of the applied impairment functions in the **Impairments Available** area (*Illustration 79*) of the **Link** page, you must return to the **Advanced Settings** area (*Illustration 78*) of the **Link** page, and configure each of the impairment function properties.

Note:

By default, the **Apply changes to both directions** check box is ticked. When the **Apply changes to both directions** check box is ticked, the properties you define for each of the impairment functions are applied to each of the link's traffic directions (left to right, and right to left).

If you want to apply different impairment function properties to each traffic direction, untick the **Apply changes to both directions** check box, then select the appropriate traffic link tab (left to right or right to left) and configure each of the impairment function properties in the **Advanced Settings** area (*Illustration 78*) of the **Link** page.

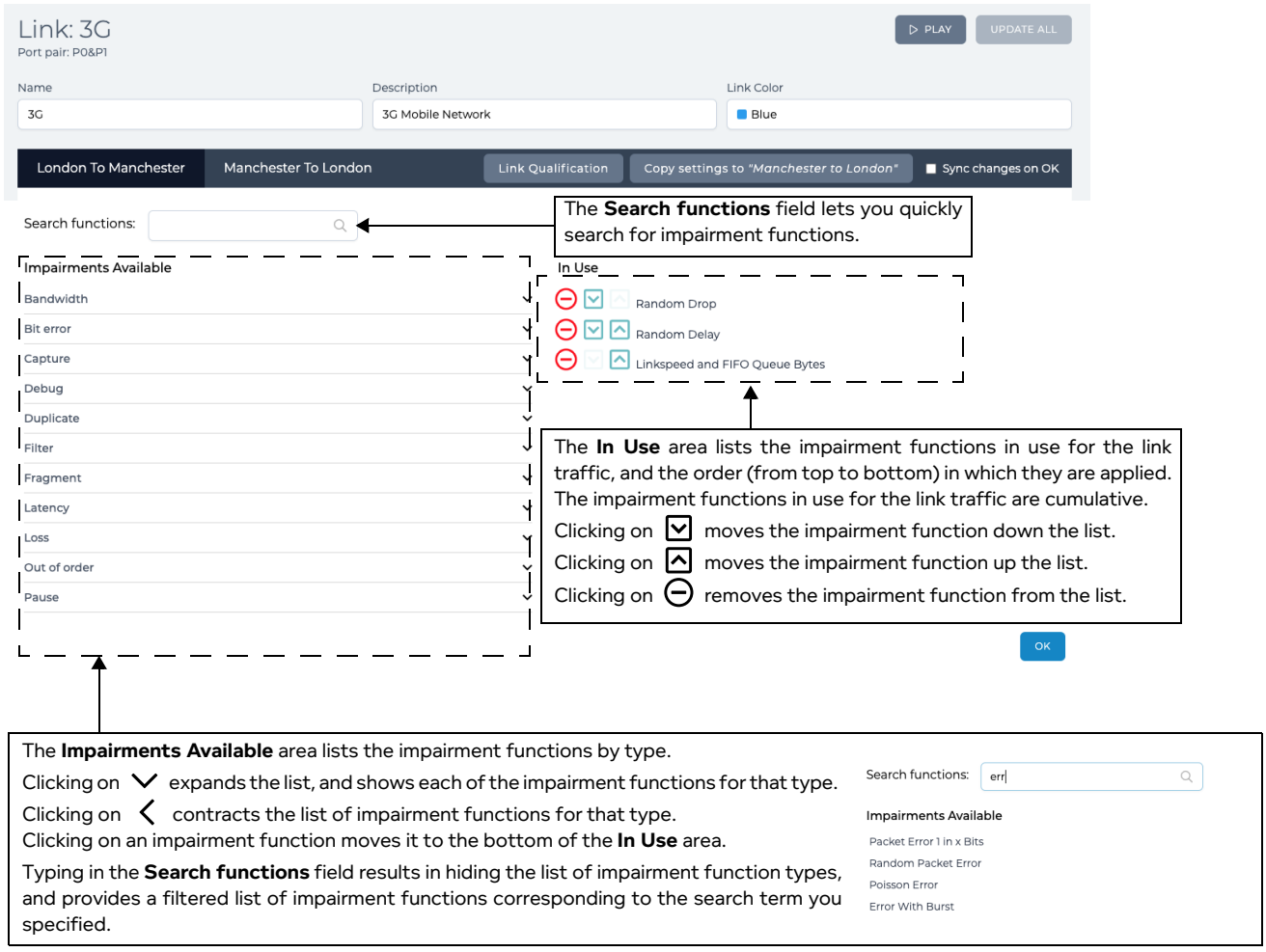
Similarly, if you want to define and order a different list of impairments to each traffic direction, untick the **Apply changes to both directions** check box, then select the appropriate traffic link

tab (left to right or right to left) and then select (i.e. add/remove) and order each of the impairment functions in the **Impairments Available** area (*Illustration 79*) of the **Link** page.

Note:

As network technologies evolve, Calnex keep NE-ONE impairment functions up-to-date via software updates. For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date. An active maintenance contract lets you update the NE-ONE impairment functions when new network technologies become available.

ILLUSTRATION 79 - EXAMPLE IMPAIRMENTS AVAILABLE AREA OF THE ADVANCED PROPERTIES PAGE



The **Impairments Available** area of the **Link** page contains the elements summarized in *Table 41*.

TABLE 42 - ADVANCED LINK AVAILABLE IMPAIRMENTS SETTINGS PAGE ELEMENTS

Impairments Available Element	Description
▷ **PLAY** button or ☐ **STOP** button	The state of this button varies according to whether or not the network is running. When the network is not running, a ▷ **PLAY** button is present, and the status icon for the network in the tray is ✎. Clicking on the ▷ **PLAY** button results in: • running the network • changing the network status icon to the play ⏵ symbol • changing the button state to ☐ **STOP** When the network is running, a ☐ **STOP** button is present, and the status icon for the network in the tray is ⏵. Clicking on the ☐ **STOP** button results in: • stopping the network • changing the network status icon to the edit ✎ symbol • changing the button state to ▷ **PLAY**
UPDATE ALL button	This button is grayed out when the network is not running. When the network is running, this button is active. When the network is running, you can edit the parameters of the network (i.e. link and node parameters). Clicking this button applies all the changed parameters on the fly to the running network.
Left to right traffic direction tab	Tab representing the impairment settings for the traffic in the left to right direction of the link. Clicking on this updates the area below with the impairment configuration for the left to right traffic direction of the link.
Right to left traffic direction tab	Tab representing the impairment settings for the traffic in the right to left direction of the link. Clicking on this updates the area below with the impairment configuration for the right to left traffic direction of the link.
Copy settings to button	Clicking this button results in immediately applying the impairment settings of the currently selected traffic direction to the other traffic direction.
Sync changes on OK check box	Ticking this check box results in applying the impairment settings of the currently selected traffic direction to the other traffic direction upon clicking the **OK** button. Unticking this check box results in not applying the impairment settings of the currently selected traffic direction to the other traffic direction upon clicking the **OK** button.
Search functions field	The **Search functions** field lets you quickly search for impairment functions.
Impairments Available area	The **Impairments Available** area lists the impairment functions by type. • Clicking on ⌄ expands the list, and shows each of the impairment functions for that type. • Clicking on ‹ contracts the list of impairment functions for that type. • Clicking on an impairment function moves it to the bottom of the **In Use** area. Typing in the **Search functions** field results in hiding the list of impairment function types, and provides a filtered list of impairment functions corresponding to the search term you specified.

Impairments Available Element	Description
In Use area	The **In Use** area lists the impairment functions in use for the link traffic, and the order (from top to bottom) in which they are applied. The impairment functions in use for the link traffic are cumulative. • Clicking on ☑ moves the impairment function down the list. • Clicking on ☒ moves the impairment function up the list. • Clicking on ⊖ removes the impairment function from the list.
OK button	Clicking on the **OK** button applies the current impairment settings, and returns you to the **Advanced Settings** area of the **Link** page (*Illustration 78*).

The work flow in *Illustration 81* summarizes the typical steps you perform when configuring the impairments that are applied to the traffic on a link.

3-3-3-4. The (Advanced Settings) Link Qualification Criteria Dialog Box (Point-to-Point Networks)

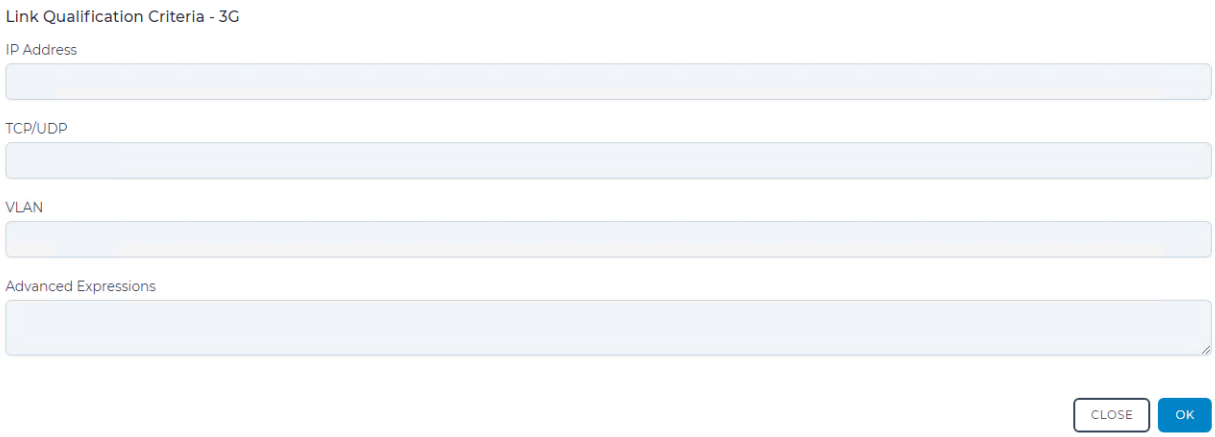
When you configure multiple links (multiple links between the nodes) it is necessary to define criteria specifying what traffic travels over which links. If you do not do this all traffic will go down the first configured link.

The link qualification criteria can also be used as a traffic filter. That is if you select a range of IP addresses for a particular link then only traffic associated with these source and destination IP addresses will traverse this link.

Where no links exist to handle certain traffic, this traffic will be dropped by the network.

Specifying what traffic travels over which link is handled in the **Link Qualification Criteria** dialog box (*Illustration 80*).

ILLUSTRATION 80 - EXAMPLE LINK QUALIFICATION CRITERIA DIALOG BOX (POINT-TO-POINT NETWORKS)



The **Link Qualification Criteria** dialog box contains the fields summarized in *Table 43*, which lets you select the IP addresses, TCP/UDP Ports and the VLAN tags that will be allowed to run over this link.

TABLE 43 - LINK QUALIFICATION CRITERIA PARAMETERS (POINT-TO-POINT NETWORKS)

Link Qualification Parameter	Description
IP Address field	Defines the IP address, IP addresses or range of IP addresses that can run over the link, and uses a comma delimiter syntax with dashes. Examples: • To display data only related to IP addresses from 192.168.1.1 to 192.168.1.254, specify: **`192.168.1.1-192.168.1.254`** • To display data only related to IP addresses from 192.168.1.1 to 192.168.1.16 and 192.168.0.1 to 192.168.0.100 and IP address 192.168.1.154, specify: **`192.168.1.1-192.1.68.1.16,192.168.0.1-192.168.0.100,192.168.1.154`** • CIDR (Classless Inter-Domain Routing) notation is also accepted. For example, for the range 192.168.0.0 to 192.168.0.255 specify: **`192.168.0.0/24`**
TCP/UDP field	Defines the TCP and UDP ports that can run over the link, and uses a comma delimiter syntax with dashes. Examples: • To display data only related to ports 80 and 3289 to 3299, specify: **`80,3289-3299`** **Note:** What may assist you is that the port is set to 0 (for matching purposes) for all packets that do not have a port i.e. are (IPv4 and not UDP/TCP) or not IPv4. You can use this fact in packet matching, for example the port range 1-65535 would eliminate ICMP (IPv4 but not TCP/UDP) and ARP (not IPv4 at all) which have no port. Specifying 0 (zero) will match packets that do not have a port number such as ARP and ICMP (ping).
VLAN field	The VLAN field would typically be the VLAN/MPLS tag number. This is the VLAN Tag (ID) applied to Tagged VLAN packets by switches that are tagged VLAN packet aware. The VLAN tag needs to be set according to the 802.1Q standard.
Advanced Expressions field	This field lets you define link qualification criteria with more complex expressions. For example, **`ipv4.dst=192.168.100.1 OR ipv4.src=192.168.100.1`**. You must type an expression which describes (in Wireshark like syntax) data that qualifies for this link. For example: • **`eth.dst = 00:1B:21:91:D8:F6 or eth.src = 00:1B:21:91:D8:F6`** would select the single MAC address 00:1B:21:91:D8:F6 • **`ipv4.proto = 17`** would select only UDP packets • **`tcp.Destination_Port = 80 or tcp.source_Port = 80`** would select only port 80 for TCP, not UDP • **`ipv4.tos = x0A`** would select DSCP class AF11 **Note:** Link qualifications are in general symmetric so that both directions use the same link, hence source and destination used in the examples above. These expressions are ANDed with any of the selections that are specified in the **IP Address** field, **TCP/UDP** field and **VLAN** field. For more information, see *Link Qualification Expressions* on page 731 in *Appendix 1*, *Specifying Expressions*.

ILLUSTRATION 81 - TYPICAL WORK FLOW OF ADVANCED LINK (IMPAIRMENTS) CONFIGURATION

Point To Point Designer page (*Illustration 71*)

1. Click on a link to edit its properties.

↓

Basic Link Properties page

1. Within the **LINK PROPERTIES** tab (*Illustration 76*), define all basic link properties (*Table 39*).
   Note: If you do not define the **Type**, **Subtype** or **Link Quality** for the link, the **Advanced Settings** area will auto populate the properties of each of the impairment functions with zero values. Ensure you define the **Type**, **Subtype** or **Link Quality** for the link before continuing.
2. If necessary, within the **LINK QUALIFICATIONS** tab (*Illustration 77*) to define the link qualifications (*Table 40*).
3. Click **ADVANCED SETTINGS** button to configure advanced link properties (impairments).

↓

Advanced Settings area (*Illustration 78*) of **Link** page.

1. Decide if the impairment functions apply to both traffic directions.
   - If yes, leave the **Sync changes on OK** check box ticked.
   - If no, untick the **Sync changes on OK** check box.
2. Click the **EDIT** button to select and order the impairment functions from within the **Impairments Available** area (*Illustration 79*) of the **Link** page.

↓

Impairments Available area (*Illustration 79*) of the **Link** page.

1. If **Sync changes on OK** check box is ticked, select (add/remove) and order the impairment functions according to your requirements.
   If **Sync changes on OK** check box is unticked,
   - Select the tab for the left to right traffic direction, then select (add/remove) and order the impairment functions according to your requirements for the left to right traffic direction.
   - Select the tab for the right to left traffic direction, then select (add/remove) and order the impairment functions according to your requirements for the left to right traffic direction.
2. Click **OK** to return to the **Advanced Settings** area (*Illustration 78*) of **Link** page.

↓

Advanced Settings area (*Illustration 78*) of **Link** page.

1. If **Sync changes on OK** check box is ticked, for each of the impairment function in the Impairment Functions List, configure its properties in the Impairment Properties Area.
   If **Sync changes on OK** check box is unticked,
   - Select the tab for the left to right traffic direction, then for each of the impairment function in the Impairment Functions List, configure its properties in the Impairment Properties Area.
   - Select the tab for the right to left traffic direction, then for each of the impairment function in the Impairment Functions List, configure its properties in the Impairment Properties Area.
2. Click on the **OK** button to apply the current impairment settings, and return to the **Point To Point Designer** page (*Illustration 71*).

4. CREATING POINT-TO-POINT NETWORKS (EXAMPLES)

This section provides example procedures for creating Point-to-Point type networks. It assumes that you understand how the network related Web Interface pages operate (as described above in *Section 3*, *Web Interface Network Pages (Point-to-Point)*).

The following sub-sections describe examples of creating Point-to-Point type networks.

4-1. Creating Point-to-Point Networks (Single)

Using more than one link lets you set different network conditions for a single or group of IP Addresses, Applications or VLANs. For example, you may need one client computer to experience a 2G network whilst another experiences a 3G, 4G, or 5G network.

In the following example, five links are configured with different mobile network types:

- Computer with IP Address 10.0.0.2 (Netmask 255.255.255.0, Gateway 10.0.0.1) will use the 2G link (link1).
- Computer 10.0.0.3 (Netmask 255.255.255.0, Gateway 10.0.0.1) will use the 3G link (link2).
- Computer 10.0.0.4 (Netmask 255.255.255.0, Gateway 10.0.0.1) will use the 4G link (link3).
- Computer 10.0.0.5 (Netmask 255.255.255.0, Gateway 10.0.0.1) will use the 5G link (link4).
- Packets that do not qualify for 2G, 3G, 4G or 5G will traverse the 'No impedance' (link 5).

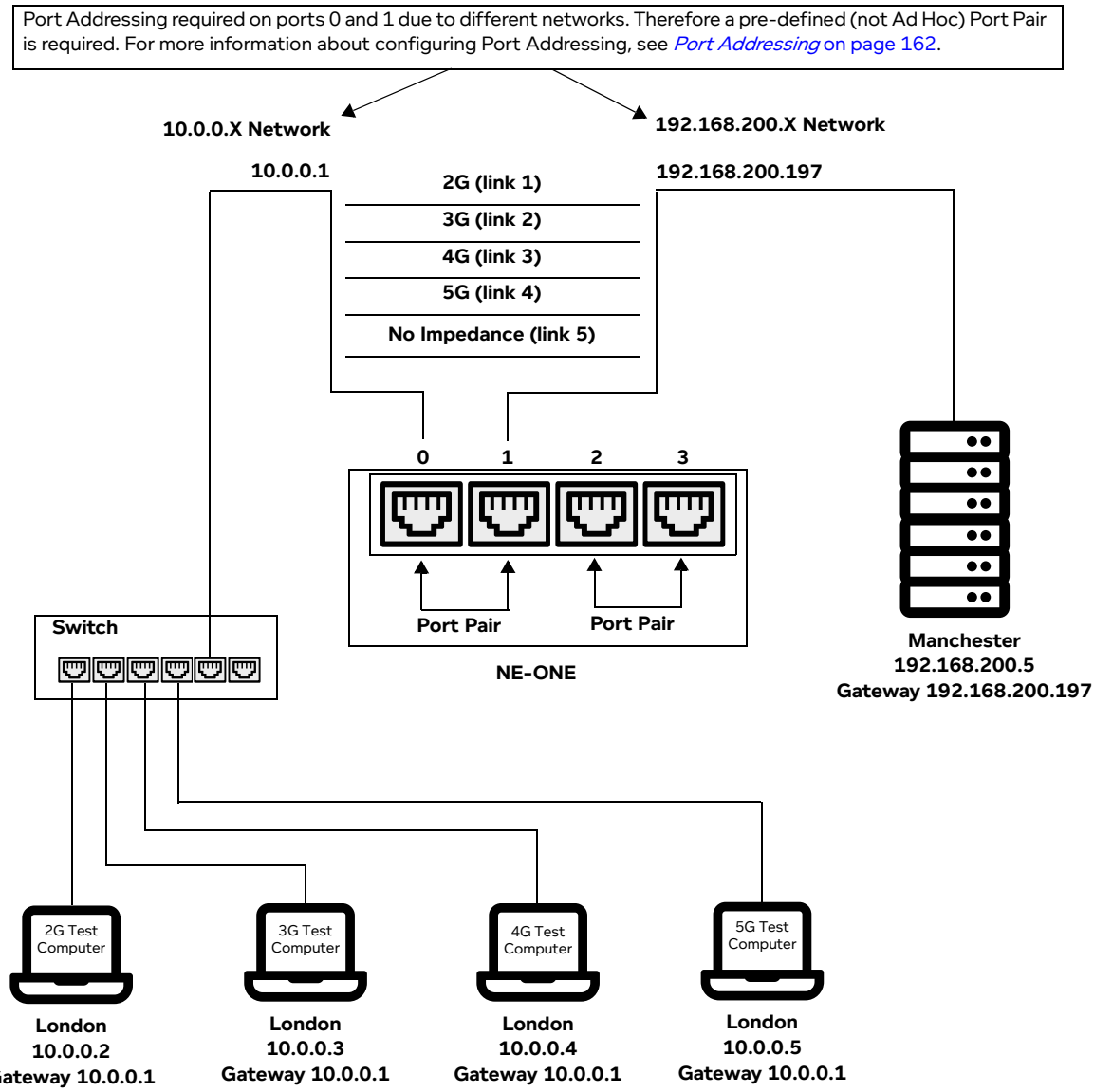
Note:

The example described below is similar to the SDTN1 example shown in *Illustration 9* on page 53 in *Chapter 4*. The minor difference compared to the SDTN1 example is that the example below includes multiple test computers behind a switch on hardware port 0, whereas the SDTN1 has one test computer directly connected to hardware port 0.

Note:

The example described below is similar to the SDTN3 example shown in *Illustration 9* on page 53 in *Chapter 4*. The minor differences compared to the SDTN3 example is that the example below is on hardware ports 0 and 1 instead of hardware ports 4 and 5, the IP addresses of the hardware ports are different, and the IP address of the test server is different.

ILLUSTRATION 82 - EXAMPLE POINT-TO-POINT NETWORK - 5 LINKS WITH PORT ADDRESSING



Links 1 to 4 apply different network conditions for the four computers. Link 5 will forward all other traffic across a link which is not impeded. If link 5 is not defined then all other traffic would be dropped.

Link Qualification Criteria can be specified as a single item, range or combination of both and the criteria can be specified separately (i.e. IP Addressing only) or together (i.e. A combination of IP Addressing, Ports and VLANs).

Note:

Link Qualification criteria is applied in both directions. For example, when specifying an IP Address, it would use the link if its in the packet's source or destination IP Address fields. The same applies to the TCP/UDP Port.

The following example procedure assumes that you are using a pre-defined port pair called **P0&P1** with port 0 for the left port, and port 1 for the right port. Also, in the following example procedure, you must use a predefined port pair and not an Ad Hoc port pair, because Ad Hoc port pairs do not support specific port addressing criteria. The following example procedure assumes that a pre-defined port pair

called **P0&P1** has Port Addressing enabled, and configured according to the example in *Configuring Port Addressing* on page 167, in *Chapter 5*, *Ports and Services Management*.

Also, in addition to the three default impairments (Random Drop, Random Delay, Linkspeed and FIFO Queue Bytes) that are applied to the traffic on each of the links, the example below also shows the following:

- adding a Fixed Delay Milliseconds latency impairment function for each of the links
- positioning the Fixed Delay Milliseconds latency impairment function so that it is first in the list of impairment functions for both traffic directions for each of the links
- keeping the default settings for the default impairments (Random Drop, Random Delay, Linkspeed and FIFO Queue Bytes) for both traffic directions for each of the links
- applying a different Fixed Delay Milliseconds latency to each of the traffic directions on each of the links (5.0 ms in the London to Manchester direction, and 2.5 ms in the Manchester to London direction)

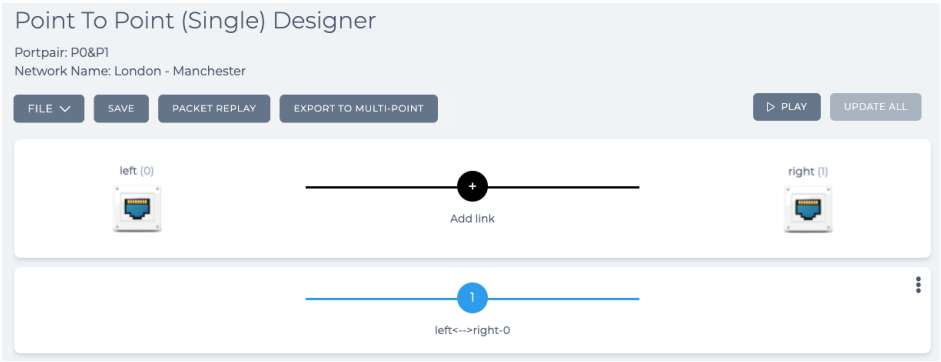
1. Launch the **Point-to-Point Designer** page, using one of the following methods:
   Method 1 (not possible if the ports use Port Addressing):
   a. Select **Networks > ↔ Ad Hoc**.
   b. From the **Choose Left Port** dialog box that appears, select **0** then click **OK**.
   c. From the **Choose Right Port** dialog box that appears, select **1** then click **OK**.
   d. From the **Network Wizard** page (see *Illustration 69*) that appears, click **New Network**.
   e. In the **Point to Point (Single)** tile, click **CREATE**.
   f. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London – Manchester`**), then click **OK**.
   Method 2 (not possible if the ports use Port Addressing):
   a. Select **Networks**.
   b. From the **Network Wizard** page (see *Illustration 69*) that appears, click **New Network**.
   c. In the **Point to Point (Single)** tile, click **CREATE**.
   d. From the **Choose Port Pair** dialog box that appears, select **Ad Hoc**, then click **OK**.
   e. From the **Choose Left Port** dialog box that appears, select **0** then click **OK**.
   f. From the **Choose Right Port** dialog box that appears, select **1** then click **OK**.
   g. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London – Manchester`**), then click **OK**.
   Method 3:
   a. Select **Networks**.
   b. From the **Network Wizard** page (see *Illustration 69*) that appears, click **New Network**.
   c. In the **Point to Point (Single)** tile, click **CREATE**.
   d. From the **Choose Port Pair** dialog box that appears, select the pre-defined **P0&P1** then click **OK**.
   e. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London – Manchester`**), then click **OK**.
   Method 4:
   a. Select **Networks > ↔ P0&P1**.

b. From the **Port Pair Network Wizard** page (see *Illustration 70*) that appears, click **New Network**.
c. In the **Point to Point (Single)** tile, click **CREATE**.
d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London – Manchester`**), then click **OK**.

Method 5 (on a non-favorited (non-starred), pre-defined port pair):

a. Select **Networks > ↔ All Port Pairs**.
The **Port Pairs** page (see *Example Port Pairs page* on page 157) appears.
b. From the **Port Pairs** page that appears, click on the **<Port Pair Name>** tile where <Port Pair Name> is the name of the pre-defined port pair (e.g. **P0&P1**) that you want to select.
The **Port Pair Network Wizard** page associated to the selected pre-defined port pair appears.
c. From the **Port Pair Network Wizard** page (see *Illustration 70* on page 242) that appears, click **New Network**.
d. In the **Point to Point (Single)** tile, click **CREATE**.
e. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London – Manchester`**), then click **OK**.

A **Point To Point (Single) Designer** page appears with generic node definitions and one temporary link called **left<-->right-0**.

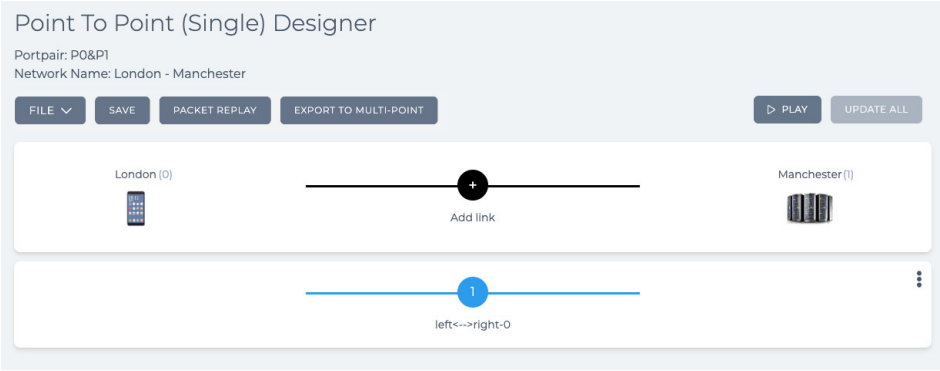


At this point a network file `London – Manchester.itn` has been created in your `/Private/networks` folder.

2. Click on the **left** node, and from the **Edit node** panel that appears, do the following to define a London based pedestrian:
   a. In the **Name** field, type **`London`**.
   b. In the **Description** field, type **`London Pedestrian`**.
   c. From the **Country** drop-down field, select **United Kingdom**.
   Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.
   d. From the **Choose a location** drop-down field, select and appropriate area for the location.
   Note: You can start typing the location in order to select it quickly from the list of locations.
   e. Click on the icon, and from the dialog box that appears click on the phone icon from within the **Legacy NEONE** tab, and then click **OK**.
   f. Click to ✕ close the **Edit node** panel.
3. Click on the **right** node, and from the **Edit node** panel that appears, do the following to define a Manchester based data center:

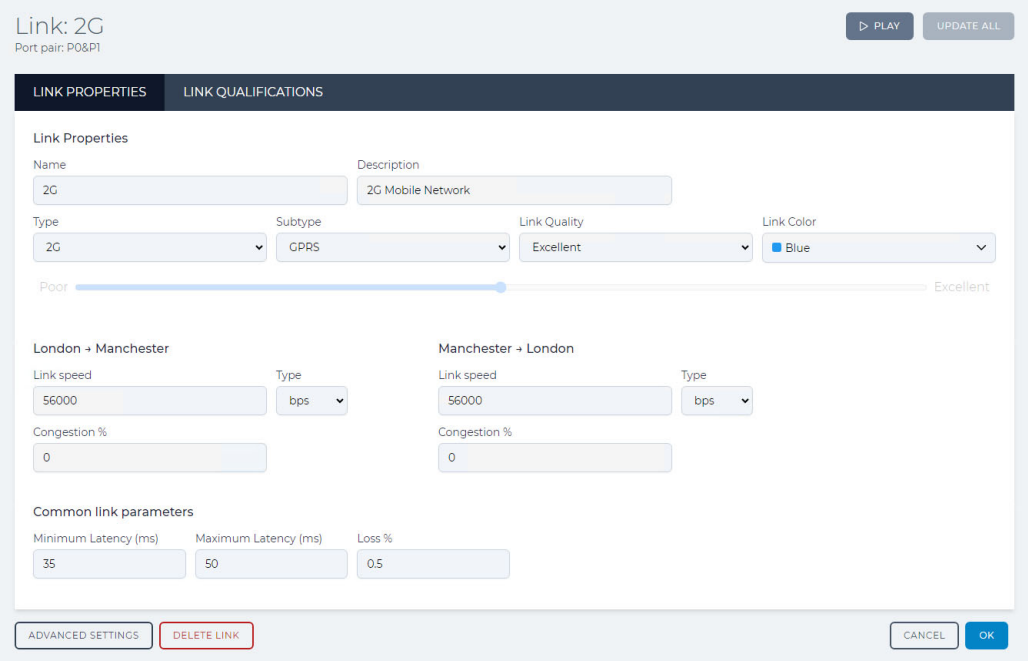
a. In the **Name** field, type **`Manchester`**.
b. In the **Description** field, type **`Manchester Data Center`**.
c. From the **Country** drop-down field, select **United Kingdom**.
Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.
d. From the **Choose a location** drop-down field, select and appropriate area for the location.
Note: You can start typing the location in order to select it quickly from the list of locations.
e. Click on the icon, and from the dialog box that appears click on the data center icon from within the **Legacy NEONE** tab, and then click **OK**.
f. Click to ✕ close the **Edit node** panel.

The **Point To Point (Single) Designer** page now appears as follows.

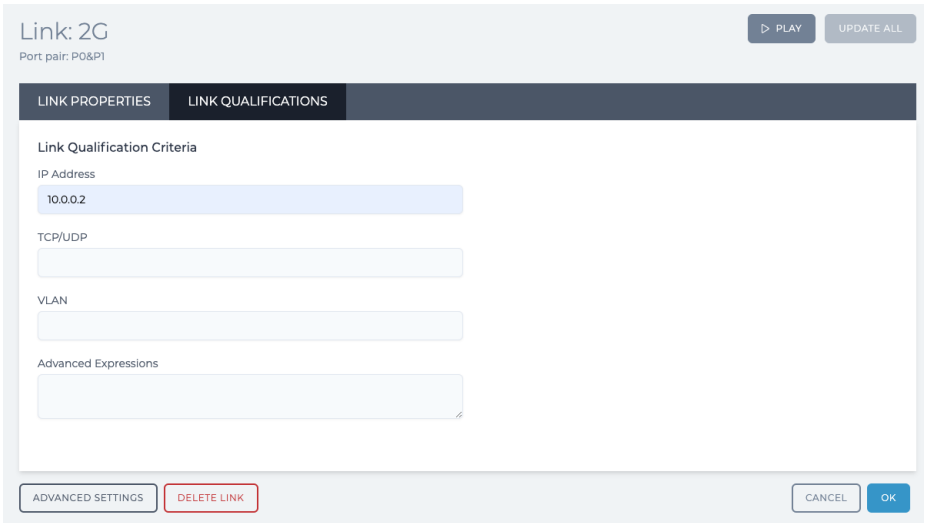


4. The initial link **left<-->right-0** will be assigned to the 2G link for the computer with IP address 10.0.0.2. Click on the **left<-->right-0** link to define its settings (link properties and link qualifications).
5. From the **Link: left<-->right-0** page that appears, do the following in the **LINK PROPERTIES** tab:
   a. In the **Name** field, type **2G**.
   The title of the page changes to **Link: 2G**.
   b. In the **Description** field, type **`2G Mobile Network`**.
   c. From the **Type** drop-down field, select **2G**.
   d. From the **Subtype** drop-down field, select **GPRS**.
   e. From the **Link Quality** drop-down field, select **Excellent**.
   The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.

f. Leave the **Link Color** field set to Blue.



6. From the **Link: 2G** page, click the **LINK QUALIFICATIONS** tab.
7. In the **IP Address** field, type **`10.0.0.2`**.

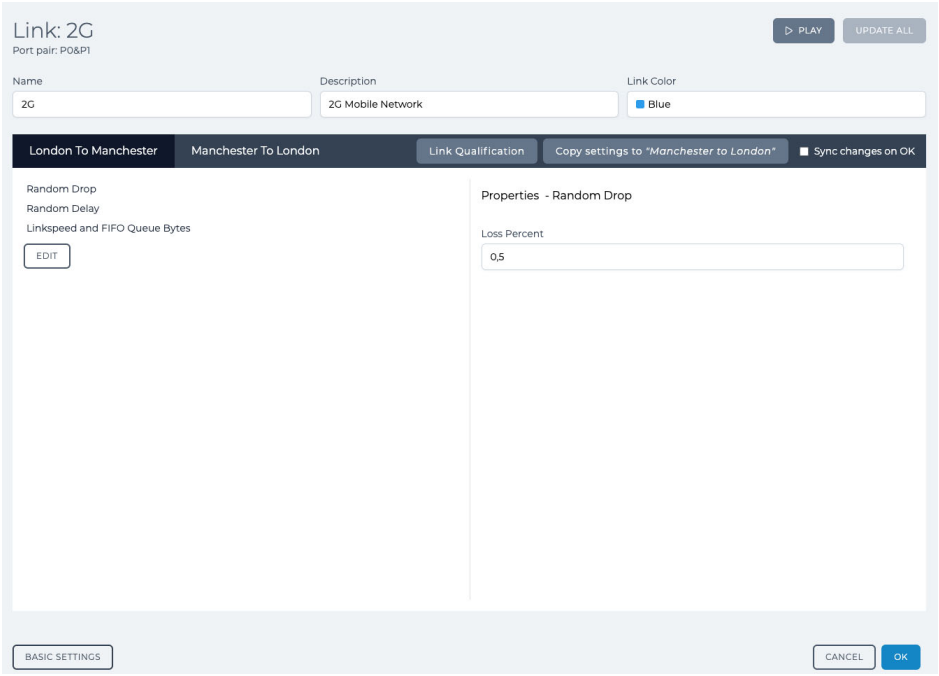


At this stage only the three default impairments (**Random Drop**, **Random Delay**, **Linkspeed and FIFO Queue Bytes**) apply to the link traffic.

8. From the **Link: 2G** page, click the **ADVANCED SETTINGS** button.

   The **Advanced Settings** area of the **Link:2G** page appears with the three default impairment

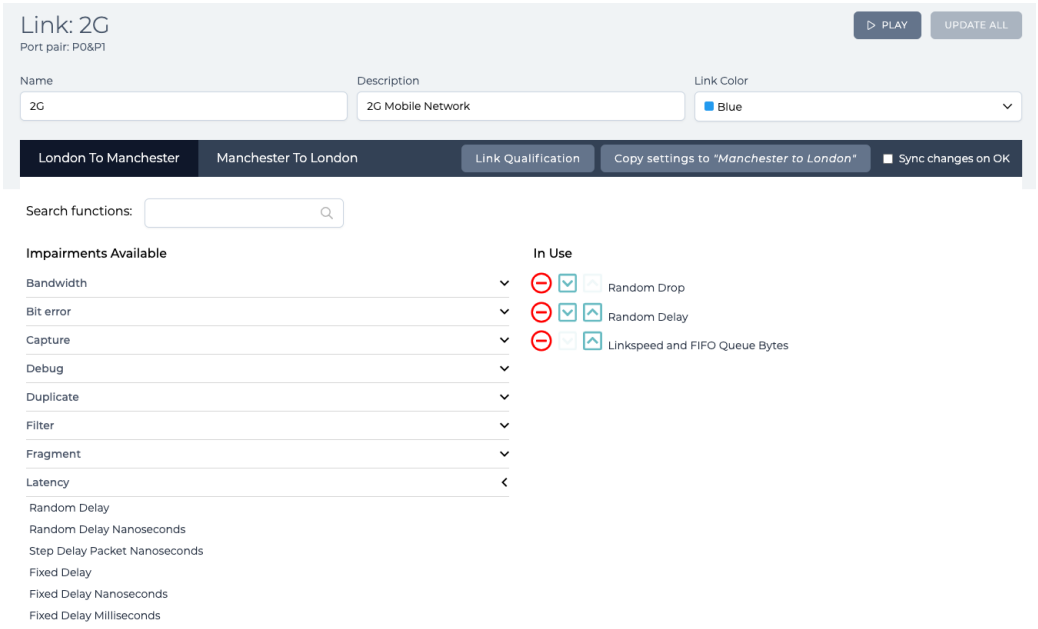
functions.



Note: By default, the **Sync changes on OK** check box is not ticked. Ensure that **Sync changes on OK** check box remains not ticked as you are going to create an asynchronous link.

9. Leaving the **London To Manchester** tab selected, click the **EDIT** button to display the **Impairments Available** area.

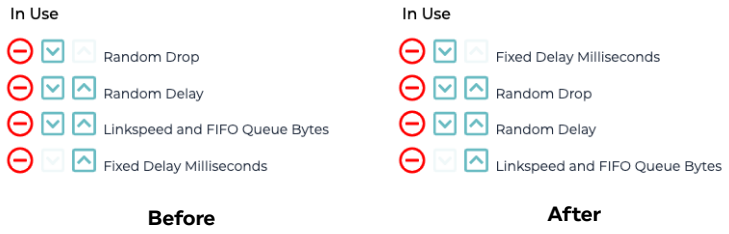
   In the **Impairments Available** area, click the **Latency** ⌄ icon to expand the list of latency type impairment functions.



10. From the list of latency type impairment functions, click on **Fixed Delay Milliseconds**.

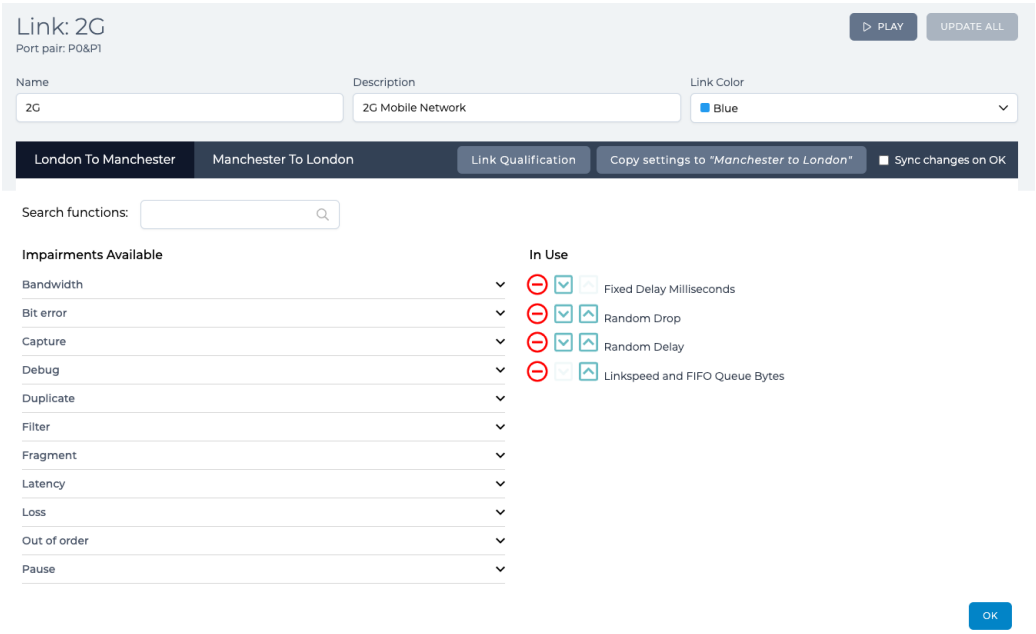
    The list of **In Use** impairment functions updates with **Fixed Delay Milliseconds** getting added to the

bottom.



Before **After**

11. Keep clicking on the **Fixed Delay Milliseconds** icon until it moves above the **Random Drop** impairment function.



12. Click on the **OK** button to return to the **Advanced Settings** area of the **Link:2G** page.

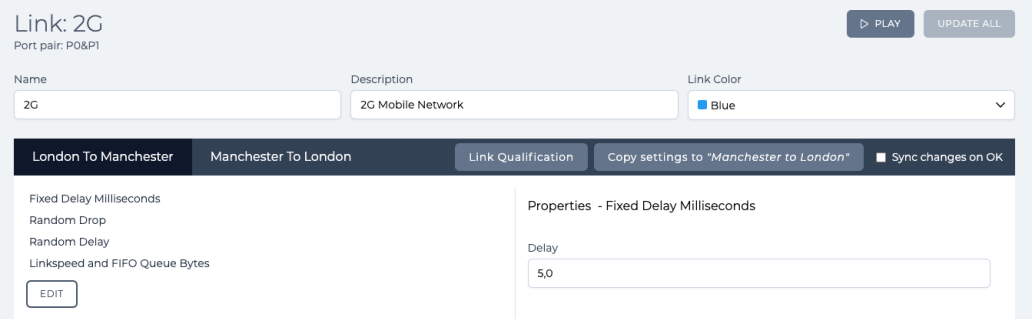
    At this stage, the **Fixed Delay Milliseconds** impairment function is only added to the London To Manchester direction, and none of the other impairment functions have not yet been modified.

13. Click the **Copy settings to "Manchester to London"** button to copy the settings from the London to Manchester direction to the Manchester to London direction. This action has the effect of copying all of the impairment settings, including that of the newly added **Fixed Delay Milliseconds** impairment function to the Manchester to London direction.

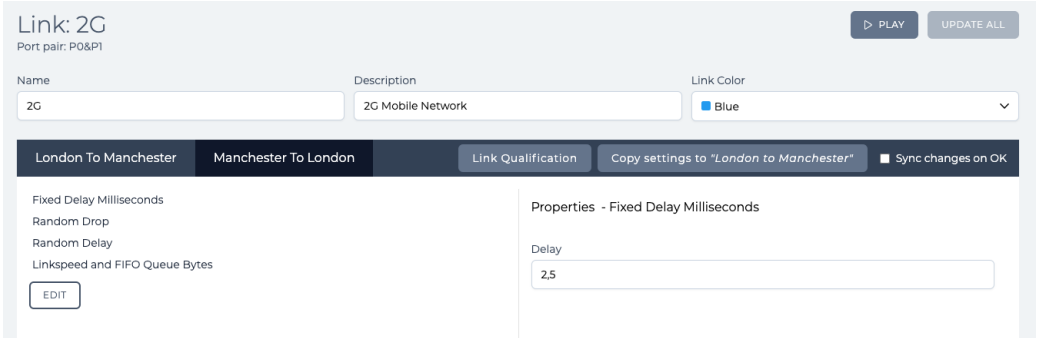
14. With the **London To Manchester** tab still selected, click **Fixed Delay Milliseconds** from the Impairment Functions list.

15. In the Impairment Properties Area, specify **5 , 0** in the **Delay** field to define a latency of 5.0 ms in the

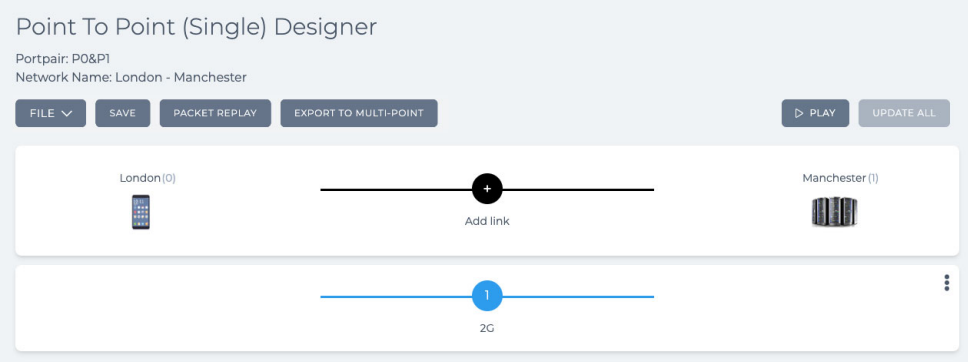
London to Manchester traffic direction.



16. Click the **Manchester To London** tab, and click **Fixed Delay Milliseconds** from the Impairment Functions list.
17. In the Impairment Properties Area, specify **2,5** in the **Delay** field to define a latency of 2.5 ms in the Manchester to London traffic direction.

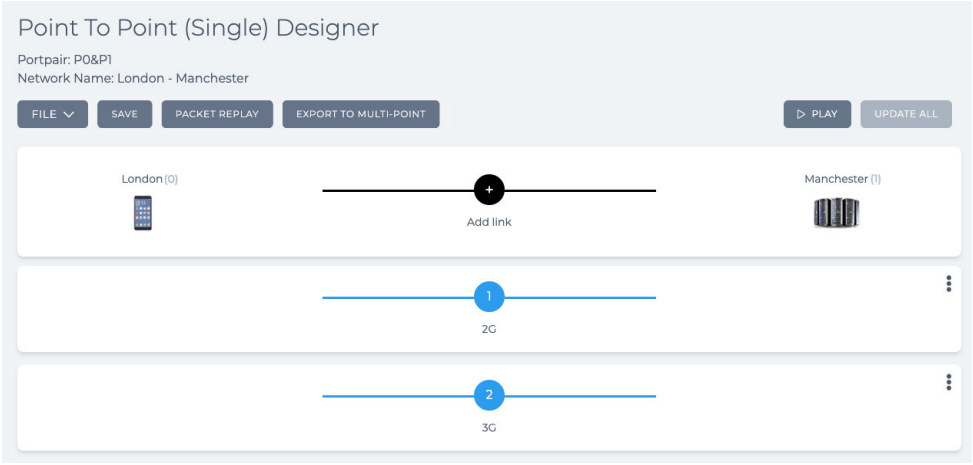


18. Click the **OK** button to return to the The **Point To Point (Single) Designer** page.
    The **Point To Point (Single) Designer** page now appears as follows.

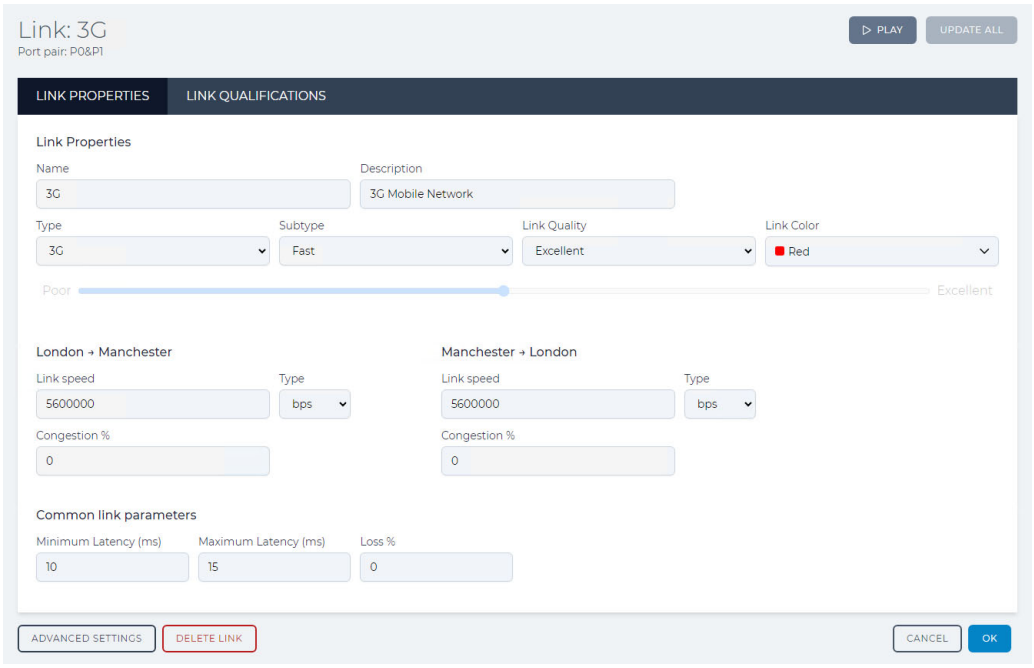


19. At this stage it is prudent to save the progress. To do this, select **FILE > SAVE** or click **SAVE**.
20. Click the **Add link**  icon.
21. From the **Link name** dialog box that appears, type **3G** and click **OK**.

The **Point To Point (Single) Designer** page updates with the newly created 3G link as follows.

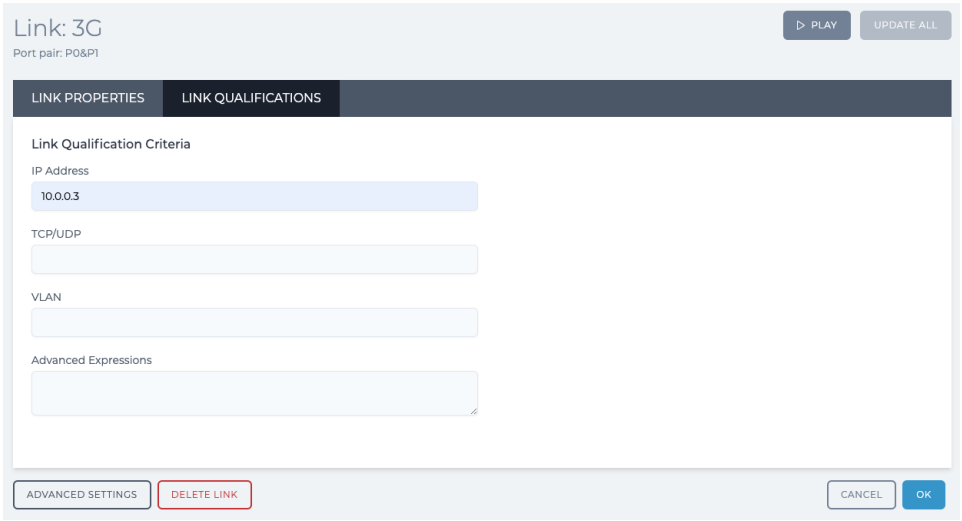


22. The link **3G** will be assigned to the 3G link for the computer with IP address 10.0.0.3. Click on the **3G** link to define its settings (link properties and link qualifications).
23. From the **Link: 3G** page that appears, do the following in the **LINK PROPERTIES** tab:
    a. In the **Name** field, no changes are required (3G already appears as it was defined when you added the new link).
    b. In the **Description** field, type **`3G Mobile Network`**.
    c. From the **Type** drop-down field, select **3G**.
    d. From the **Subtype** drop-down field, select **Fast**.
    e. From the **Link Quality** drop-down field, select **Excellent**.
    The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.
    f. Click the **Link Color** field, and select **Red**.



24. From the **Link: 3G** page, click the **LINK QUALIFICATIONS** tab.

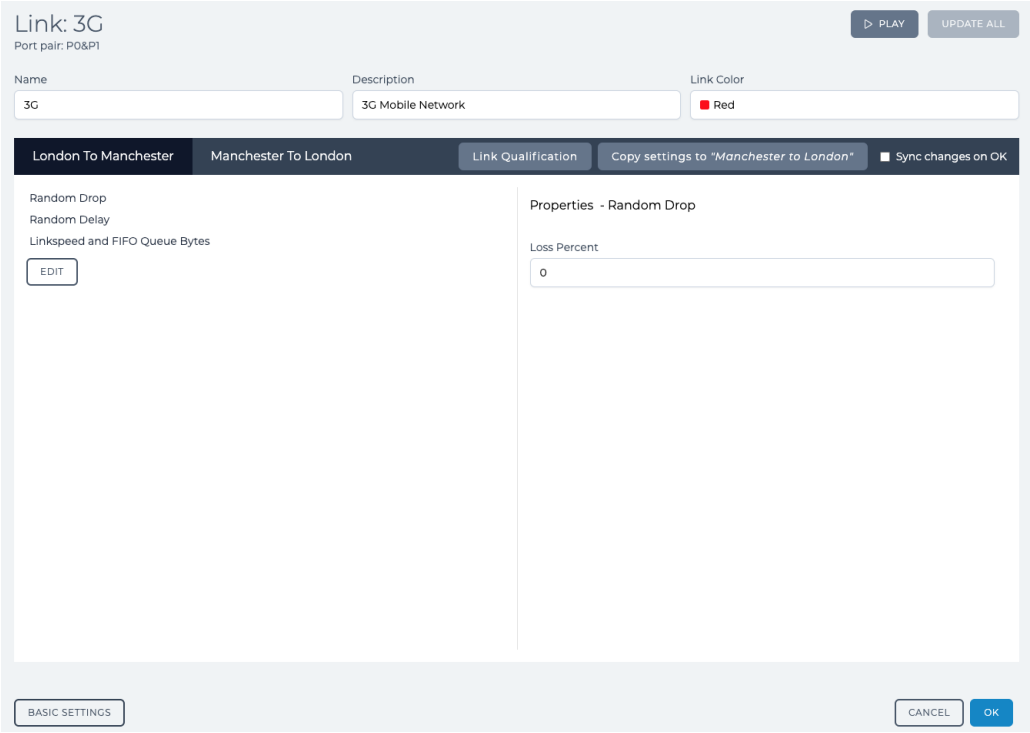
25. In the **IP Address** field, type **`10.0.0.3`**.



At this stage only the three default impairments (**Random Drop**, **Random Delay**, **Linkspeed and FIFO Queue Bytes**) apply to the link traffic.

26. From the **Link: 3G** page, click the **ADVANCED SETTINGS** button.

The **Advanced Settings** area of the **Link:3G** page appears with the three default impairment functions.

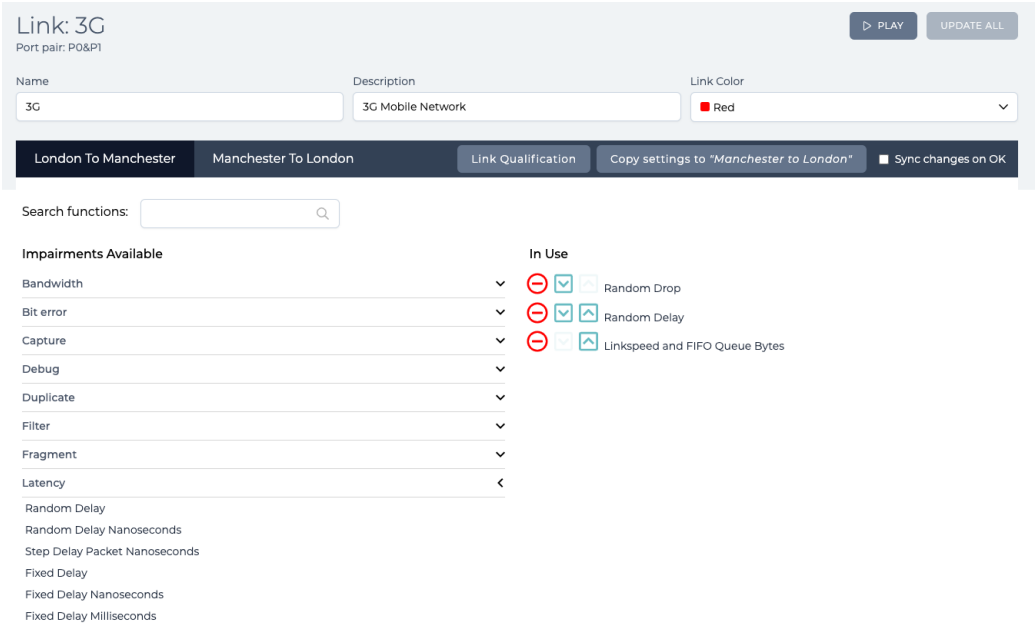


Note: By default, the **Sync changes on OK** check box is not ticked. Ensure that **Sync changes on OK** check box remains not ticked as you are going to create an asynchronous link.

27. Leaving the **London To Manchester** tab selected, click the **EDIT** button to display the **Impairments Available** area.

In the **Impairments Available** area, click the **Latency** ⌄ icon to expand the list of latency type

impairment functions.



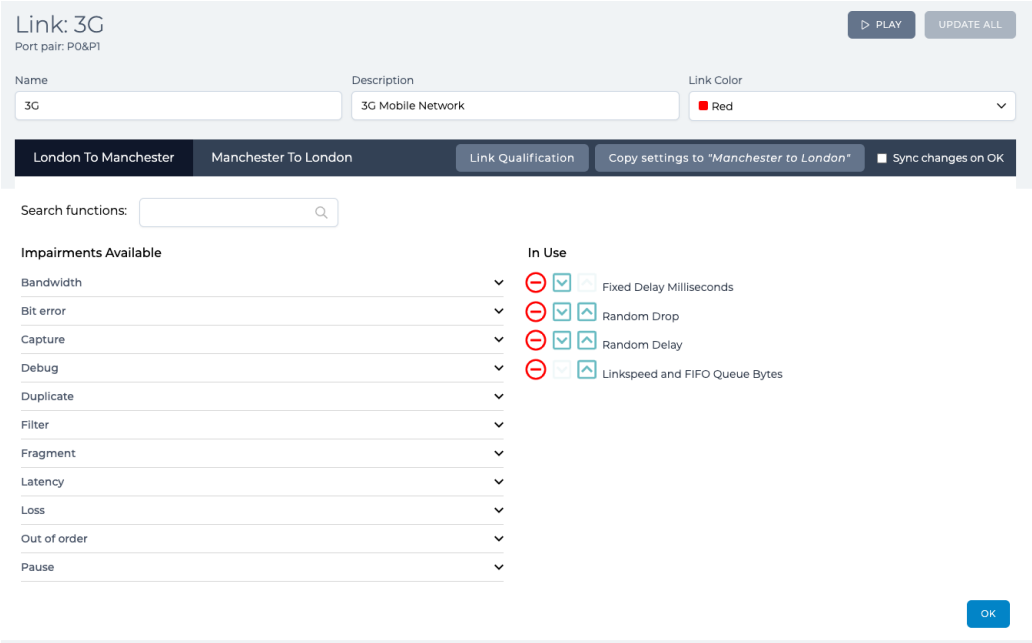
28. From the list of latency type impairment functions, click on **Fixed Delay Milliseconds**.

    The list of **In Use** impairment functions updates with **Fixed Delay Milliseconds** getting added to the bottom.

Before **After**

29. Keep clicking on the **Fixed Delay Milliseconds** icon until it moves above the **Random Drop**

impairment function.



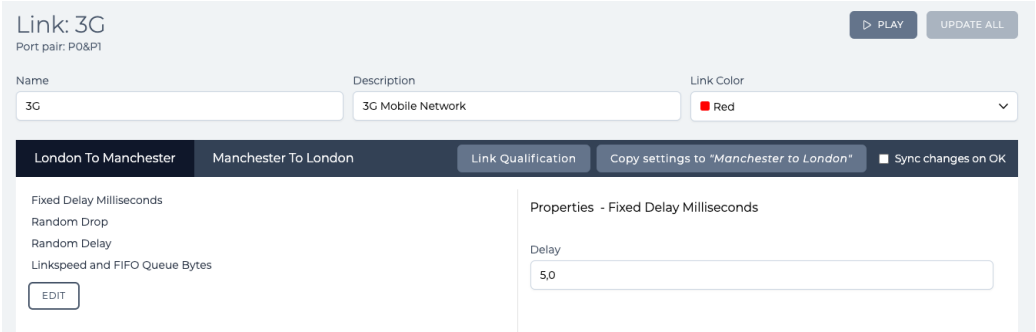
30. Click on the **OK** button to return to the **Advanced Settings** area of the **Link:3G** page.

    At this stage, the **Fixed Delay Milliseconds** impairment function is only added to the London To Manchester direction, and none of the other impairment functions have not yet been modified.

31. Click the **Copy settings to "Manchester to London"** button to copy the settings from the London to Manchester direction to the Manchester to London direction. This action has the effect of copying all of the impairment settings, including that of the newly added **Fixed Delay Milliseconds** impairment function to the Manchester to London direction.

32. With the **London To Manchester** tab still selected, click **Fixed Delay Milliseconds** from the Impairment Functions list.

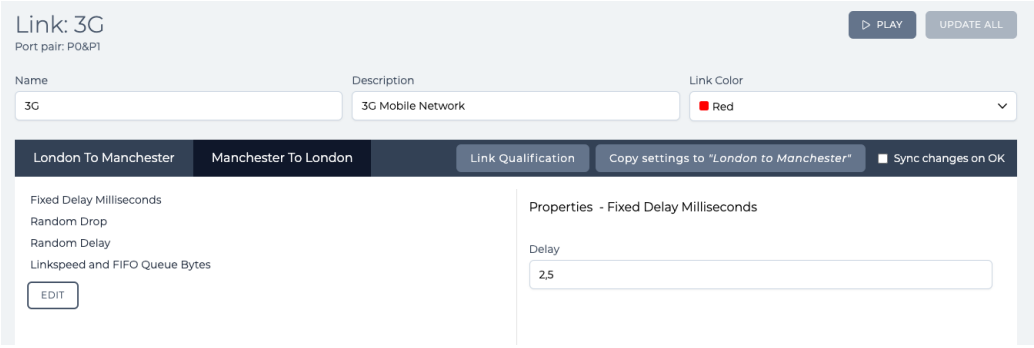
33. In the Impairment Properties Area, specify **5,0** in the **Delay** field to define a latency of 5.0 ms in the London to Manchester traffic direction.



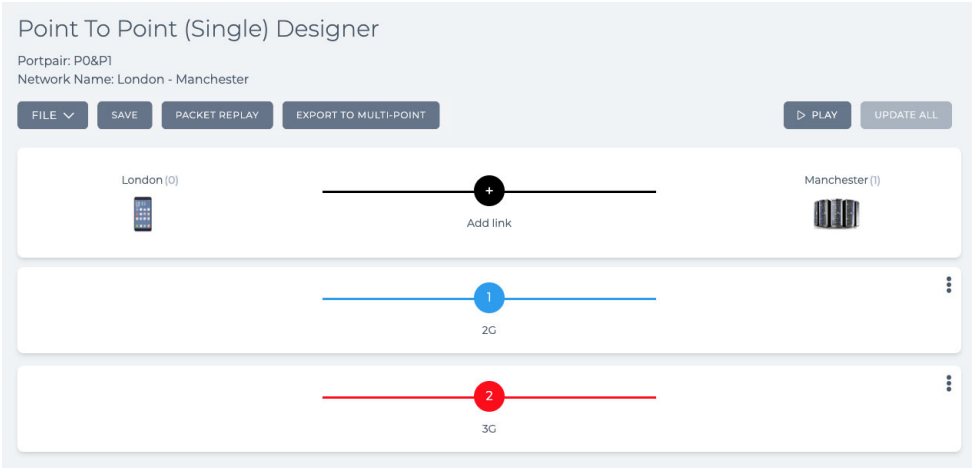
34. Click the **Manchester To London** tab, and click **Fixed Delay Milliseconds** from the Impairment Functions list.

35. In the Impairment Properties Area, specify **2,5** in the **Delay** field to define a latency of 2.5 ms in the

Manchester to London traffic direction.

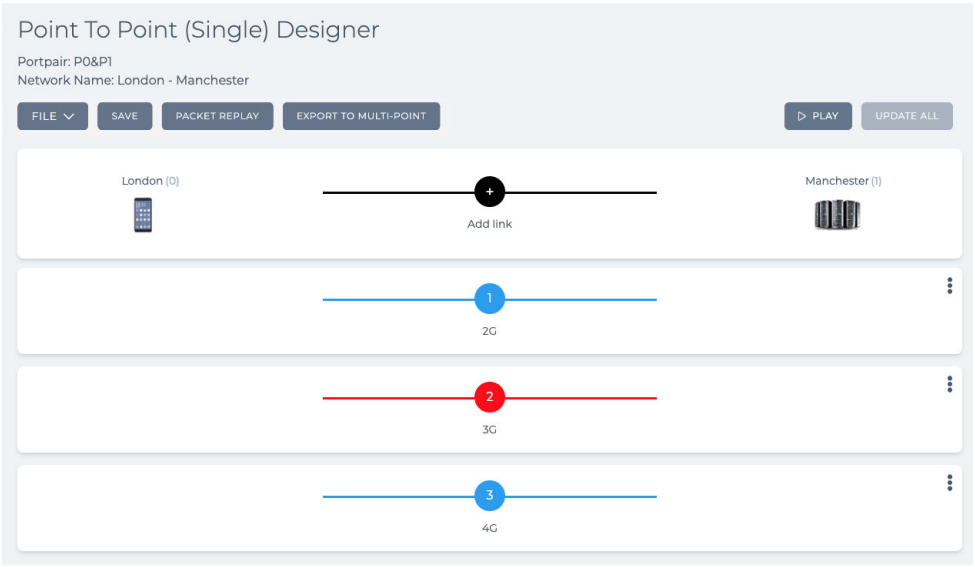


36. Click the **OK** button to return to the The **Point To Point (Single) Designer** page.
    The **Point To Point (Single) Designer** page now appears as follows.

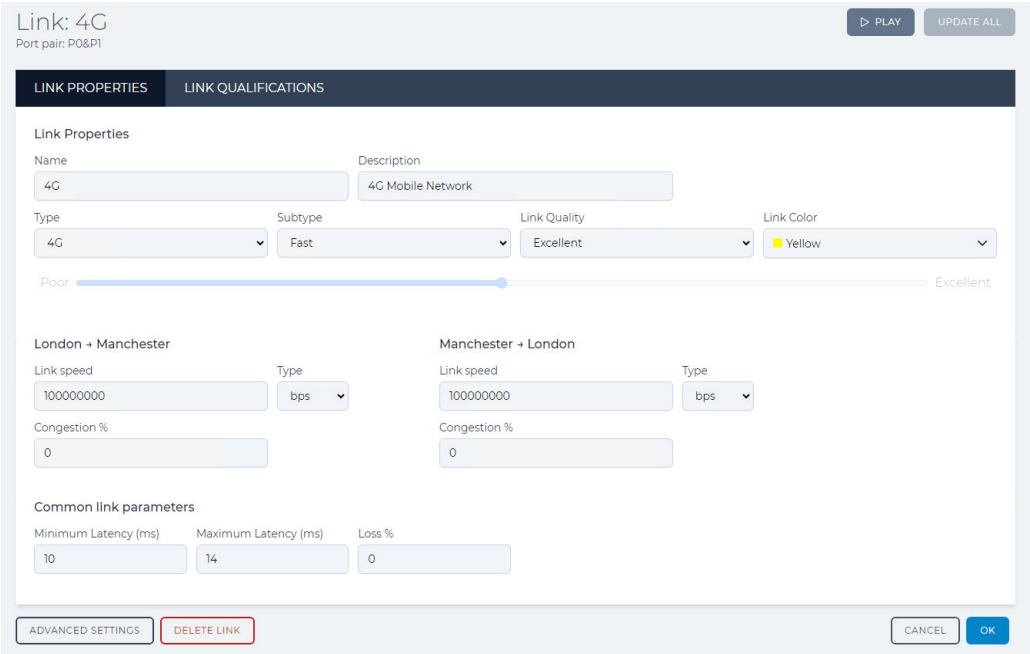


37. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click **SAVE**.
38. Click the **Add link**  icon.

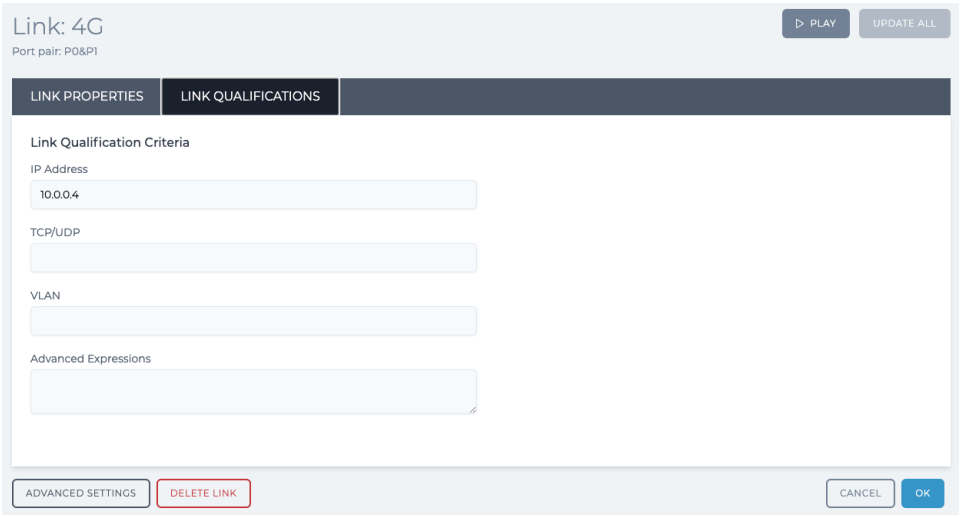
39. From the **Link name** dialog box that appears, type **4G** and click **OK**.
    The **Point To Point (Single) Designer** page updates with the newly created 4G link as follows.



40. The link **4G** will be assigned to the 4G link for the computer with IP address 10.0.0.4. Click on the **4G** link to define its settings (link properties and link qualifications).
41. From the **Link: 4G** page that appears, do the following in the **LINK PROPERTIES** tab:
    a. In the **Name** field, no changes are required (4G already appears as it was defined when you added the new link).
    b. In the **Description** field, type **`4G Mobile Network`**.
    c. From the **Type** drop-down field, select **4G**.
    d. From the **Subtype** drop-down field, select **Fast**.
    e. From the **Link Quality** drop-down field, select **Excellent**.
    The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.
    f. Click the **Link Color** field, and select **Yellow**.



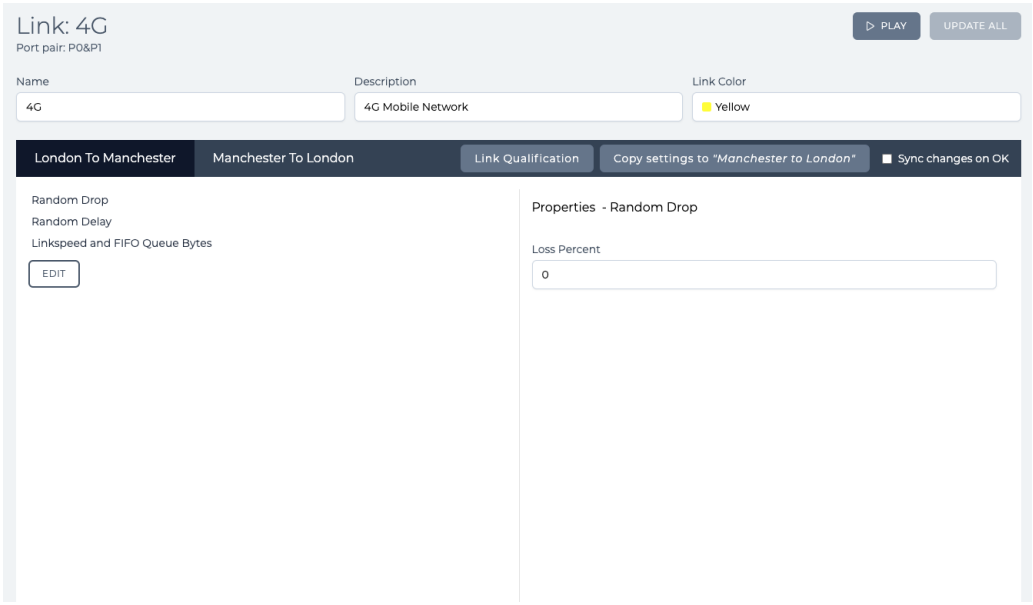
42. From the **Link: 4G** page, click the **LINK QUALIFICATIONS** tab.
43. In the **IP Address** field, type **`10.0.0.4`**.



At this stage only the three default impairments (**Random Drop**, **Random Delay**, **Linkspeed and FIFO Queue Bytes**) apply to the link traffic.

44. From the **Link: 4G** page, click the **ADVANCED SETTINGS** button.

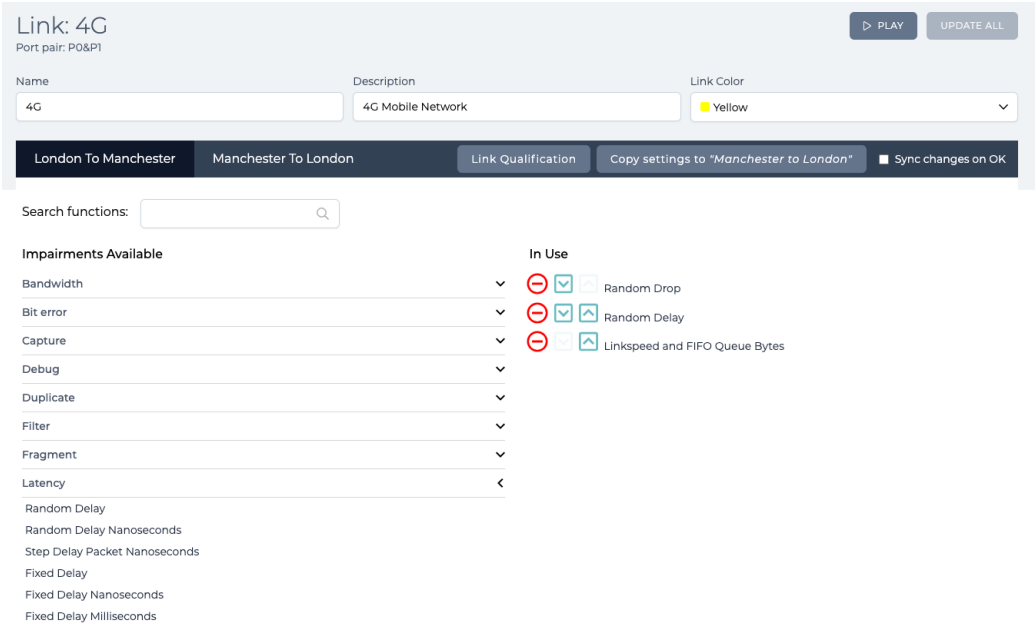
    The **Advanced Settings** area of the **Link:4G** page appears with the three default impairment functions.



Note: By default, the **Sync changes on OK** check box is not ticked. Ensure that **Sync changes on OK** check box remains not ticked as you are going to create an asynchronous link.

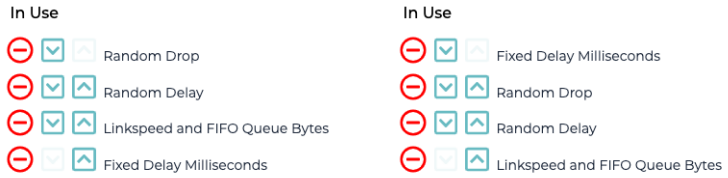
45. Leaving the **London To Manchester** tab selected, click the **EDIT** button to display the **Impairments Available** area.

    In the **Impairments Available** area, click the **Latency** ⌄ icon to expand the list of latency type impairment functions.



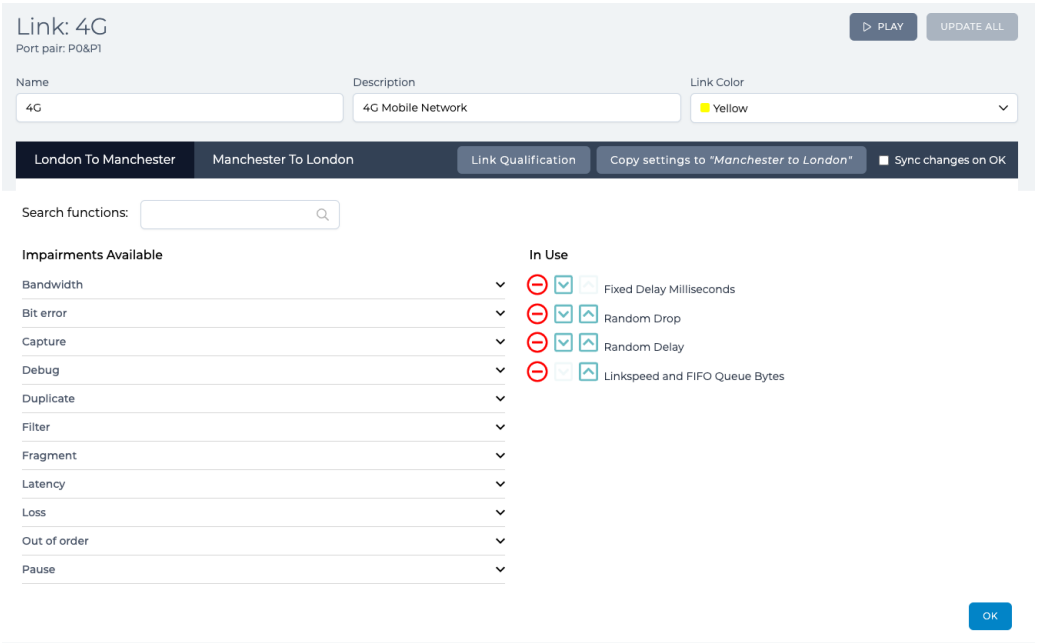
46. From the list of latency type impairment functions, click on **Fixed Delay Milliseconds**.

The list of **In Use** impairment functions updates with **Fixed Delay Milliseconds** getting added to the bottom.



Before **After**

47. Keep clicking on the **Fixed Delay Milliseconds** icon until it moves above the **Random Drop** impairment function.



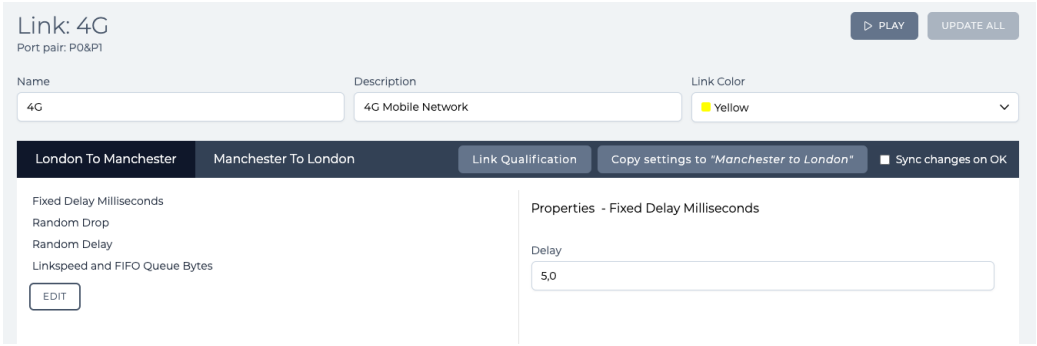
48. Click on the **OK** button to return to the **Advanced Settings** area of the **Link:4G** page.

    At this stage, the **Fixed Delay Milliseconds** impairment function is only added to the London To Manchester direction, and none of the other impairment functions have not yet been modified.

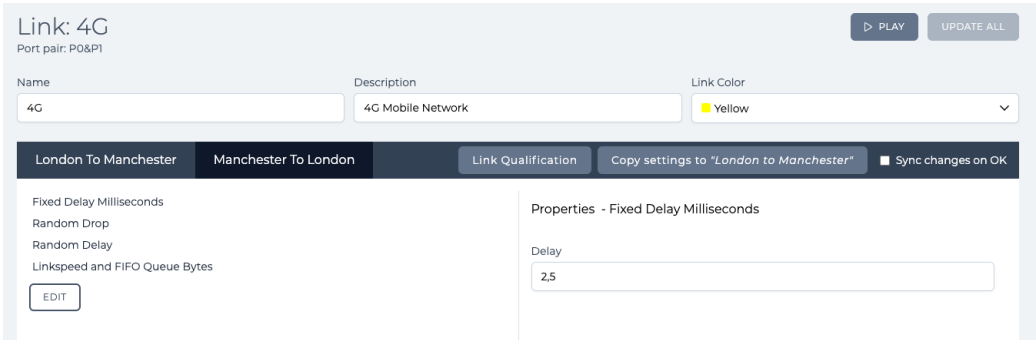
49. Click the **Copy settings to "Manchester to London"** button to copy the settings from the London to Manchester direction to the Manchester to London direction. This action has the effect of copying all of the impairment settings, including that of the newly added **Fixed Delay Milliseconds** impairment function to the Manchester to London direction.

50. With the **London To Manchester** tab still selected, click **Fixed Delay Milliseconds** from the Impairment Functions list.

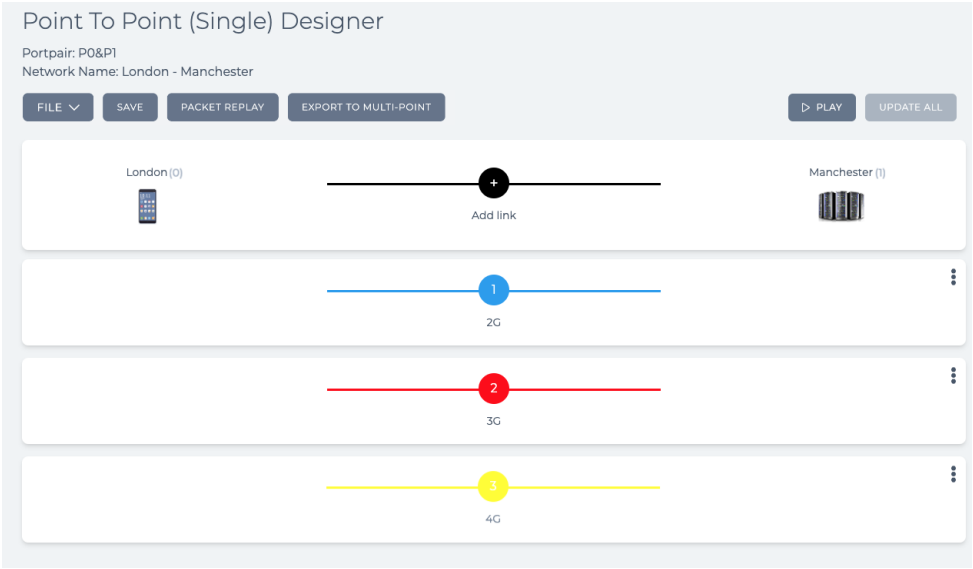
51. In the Impairment Properties Area, specify **5 , 0** in the **Delay** field to define a latency of 5.0 ms in the London to Manchester traffic direction.



52. Click the **Manchester To London** tab, and click **Fixed Delay Milliseconds** from the Impairment Functions list.
53. In the Impairment Properties Area, specify **2 , 5** in the **Delay** field to define a latency of 2.5 ms in the Manchester to London traffic direction.

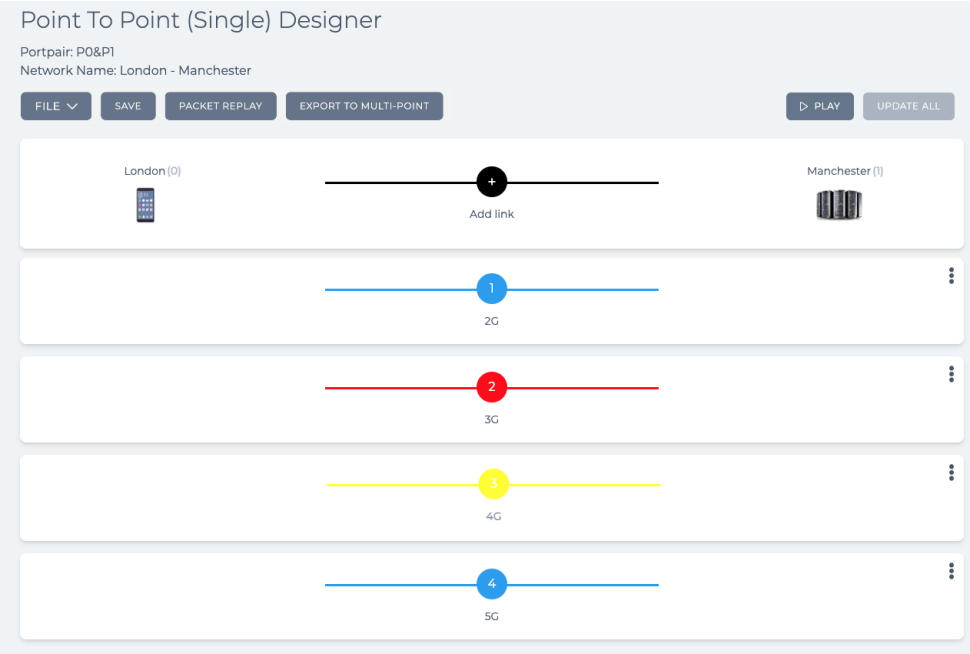


54. Click the **OK** button to return to the The **Point To Point (Single) Designer** page.
    The **Point To Point (Single) Designer** page now appears as follows.



55. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click **SAVE**.
56. Click the **Add link**  icon.
57. From the **Link name** dialog box that appears, type **5G** and click **OK**.

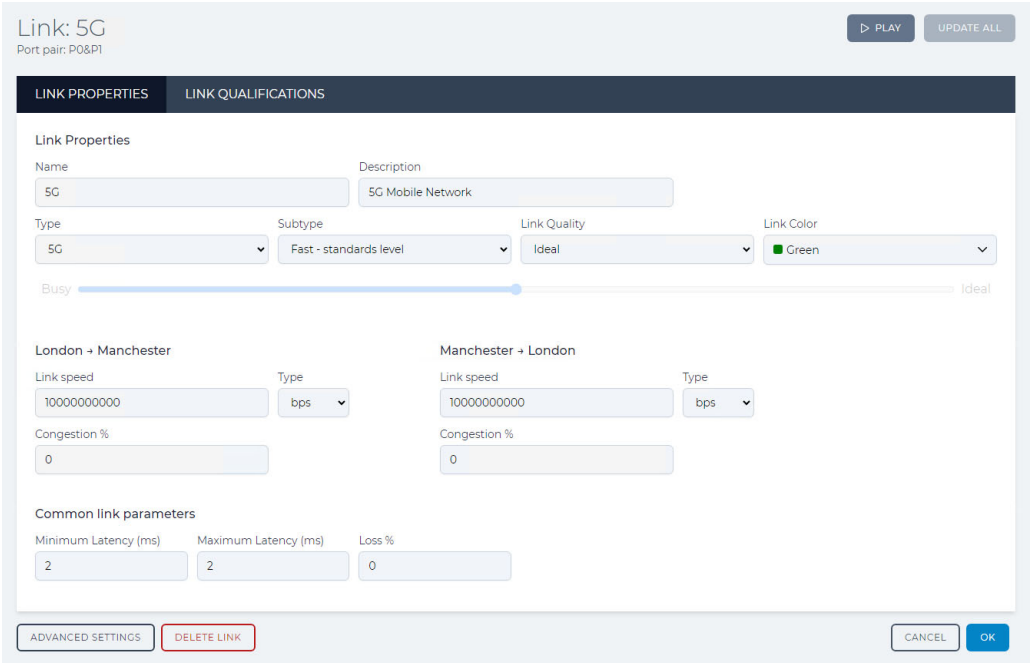
The **Point To Point (Single) Designer** page updates with the newly created 5G link as follows.



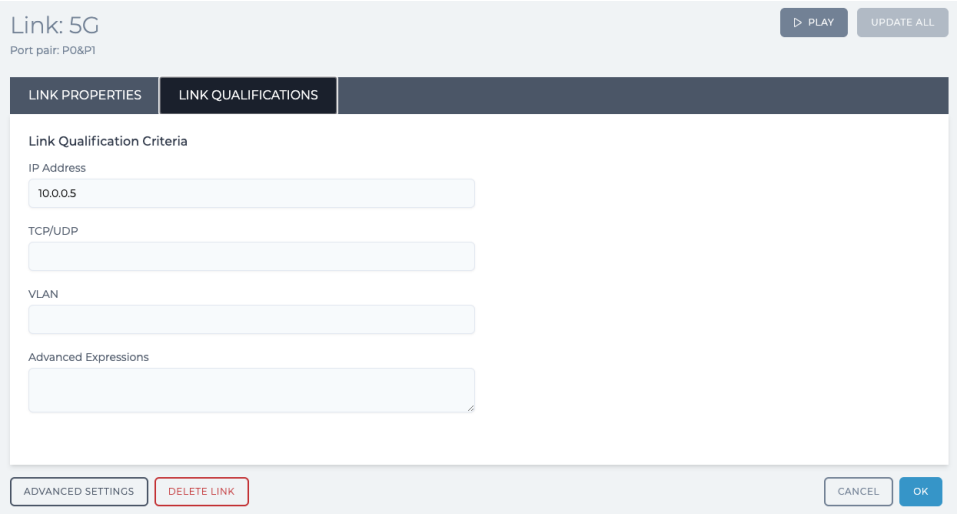
58. The link **5G** will be assigned to the 5G link for the computer with IP address 10.0.0.5. Click on the **5G** link to define its settings (link properties and link qualifications).
59. From the **Link: 5G** page that appears, do the following in the **LINK PROPERTIES** tab:
    a. In the **Name** field, no changes are required (5G already appears as it was defined when you added the new link).
    b. In the **Description** field, type **`5G Mobile Network`**.
    c. From the **Type** drop-down field, select **5G**.
    d. From the **Subtype** drop-down field, select **Fast - standards level**.
    e. From the **Link Quality** drop-down field, select **Ideal**.

    The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.

f. Click the **Link Color** field, and select **Green**.



60. From the **Link: 5G** page, click the **LINK QUALIFICATIONS** tab.
61. In the **IP Address** field, type **`10.0.0.5`**.

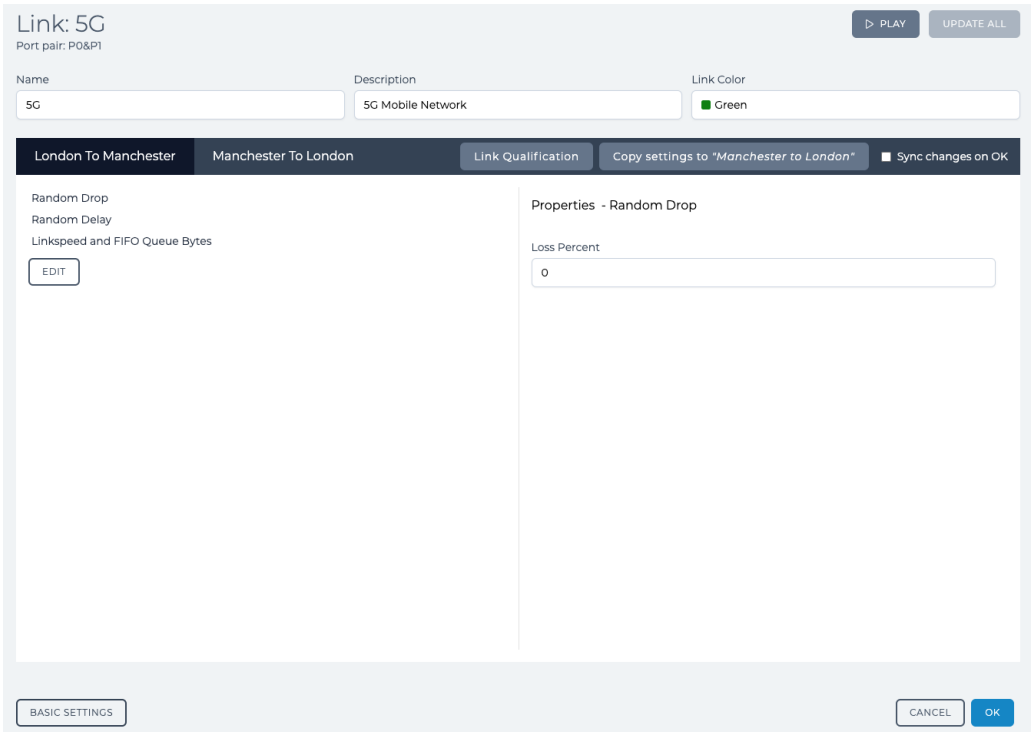


At this stage only the three default impairments (**Random Drop**, **Random Delay**, **Linkspeed and FIFO Queue Bytes**) apply to the link traffic.

62. From the **Link: 5G** page, click the **ADVANCED SETTINGS** button.

The **Advanced Settings** area of the **Link:5G** page appears with the three default impairment

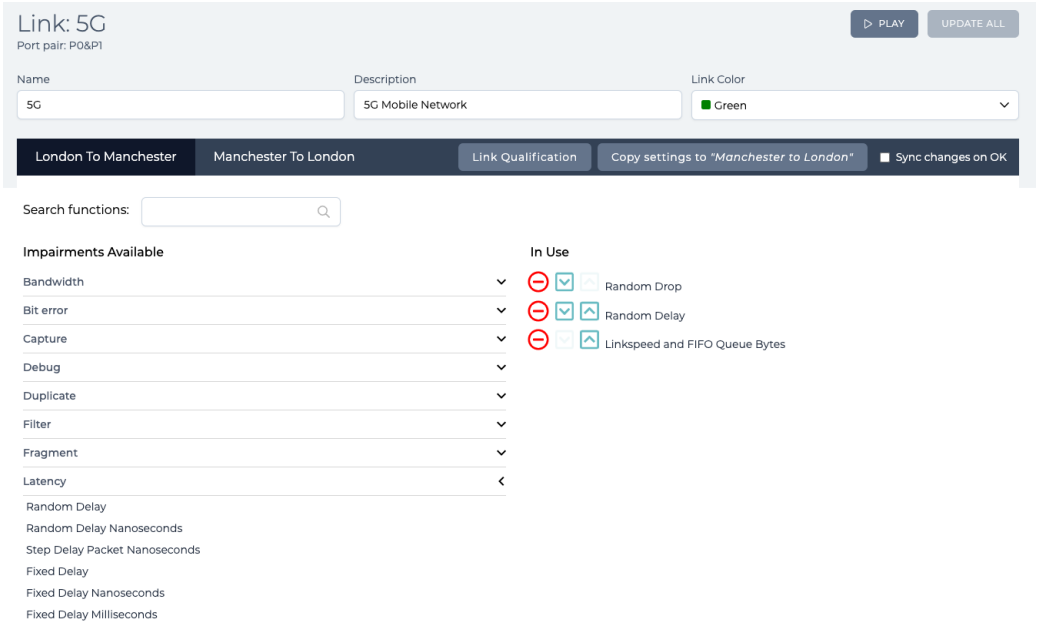
functions.



Note: By default, the **Sync changes on OK** check box is not ticked. Ensure that **Sync changes on OK** check box remains not ticked as you are going to create an asynchronous link.

63. Leaving the **London To Manchester** tab selected, click the **EDIT** button to display the **Impairments Available** area.

    In the **Impairments Available** area, click the **Latency** ⌄ icon to expand the list of latency type impairment functions.

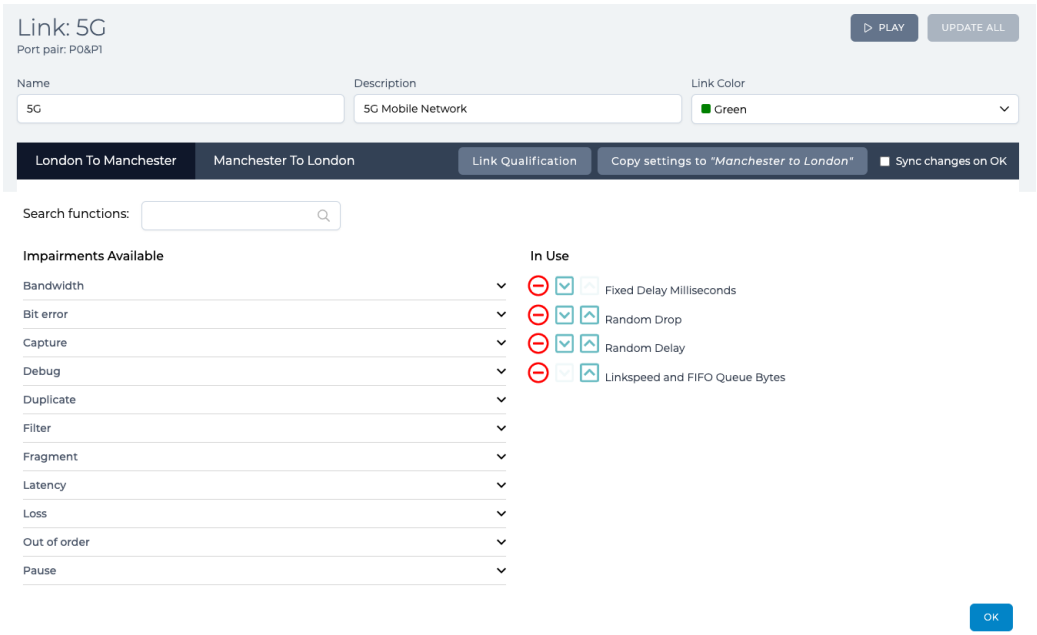


64. From the list of latency type impairment functions, click on **Fixed Delay Milliseconds**.

The list of **In Use** impairment functions updates with **Fixed Delay Milliseconds Latency** getting added to the bottom.

Before **After**

65. Keep clicking on the **Fixed Delay Milliseconds** icon until it moves above the **Random Drop** impairment function.



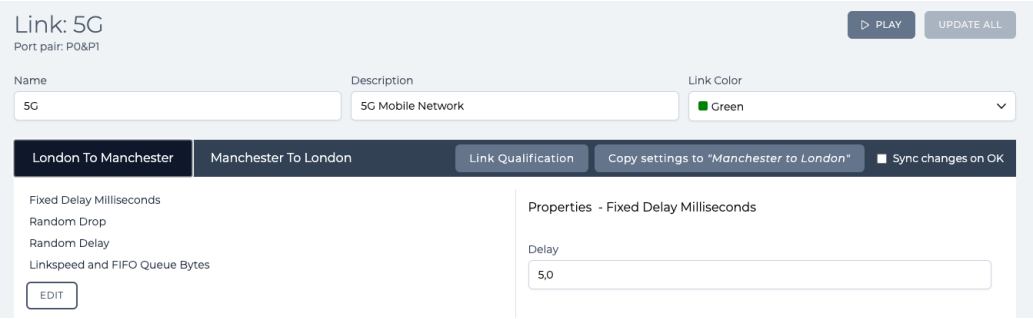
66. Click on the **OK** button to return to the **Advanced Settings** area of the **Link:5G** page.

    At this stage, the **Fixed Delay Milliseconds** impairment function is only added to the London To Manchester direction, and none of the other impairment functions have not yet been modified.

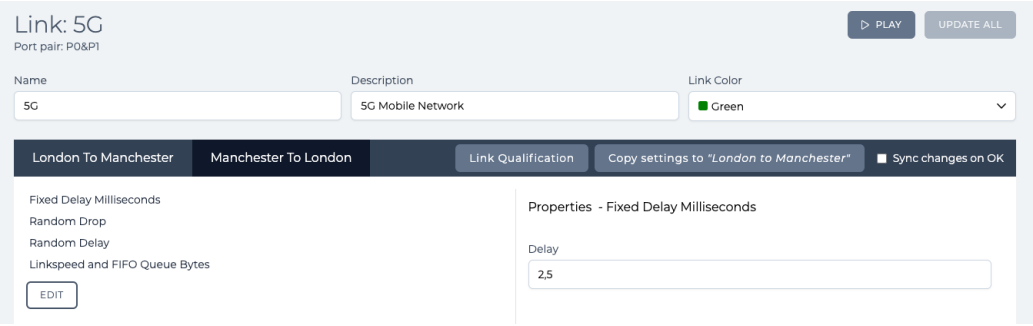
67. Click the **Copy settings to "Manchester to London"** button to copy the settings from the London to Manchester direction to the Manchester to London direction. This action has the effect of copying all of the impairment settings, including that of the newly added **Fixed Delay Milliseconds** impairment function to the Manchester to London direction.

68. With the **London To Manchester** tab still selected, click **Fixed Delay Milliseconds** from the Impairment Functions list.

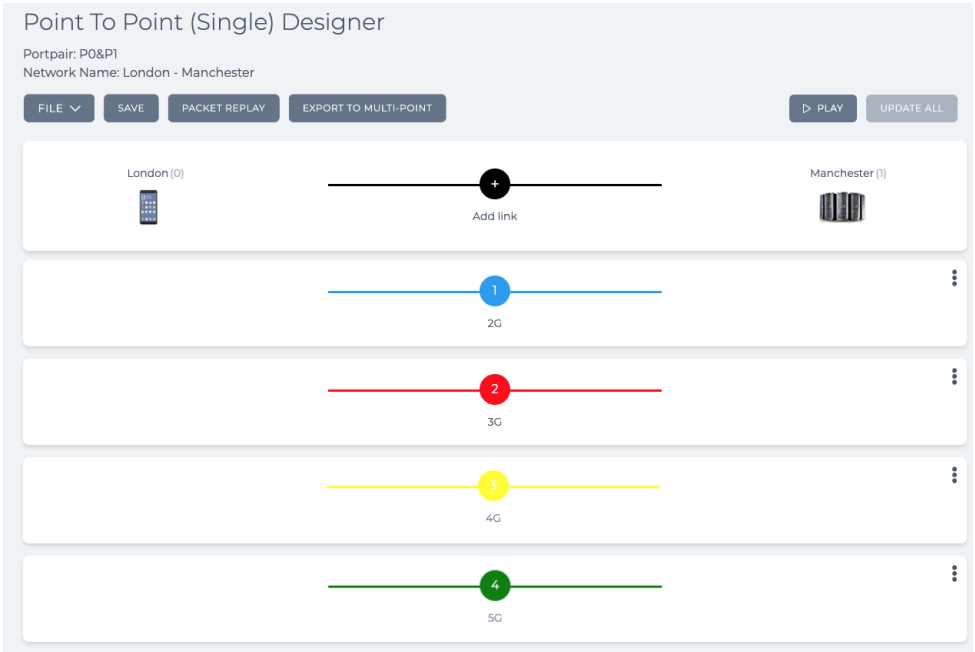
69. In the Impairment Properties Area, specify **5,0** in the **Delay** field to define a latency of 5.0 ms in the London to Manchester traffic direction.



70. Click the **Manchester To London** tab, and click **Fixed Delay Milliseconds** from the Impairment Functions list.
71. In the Impairment Properties Area, specify **2,5** in the **Delay** field to define a latency of 2.5 ms in the Manchester to London traffic direction.



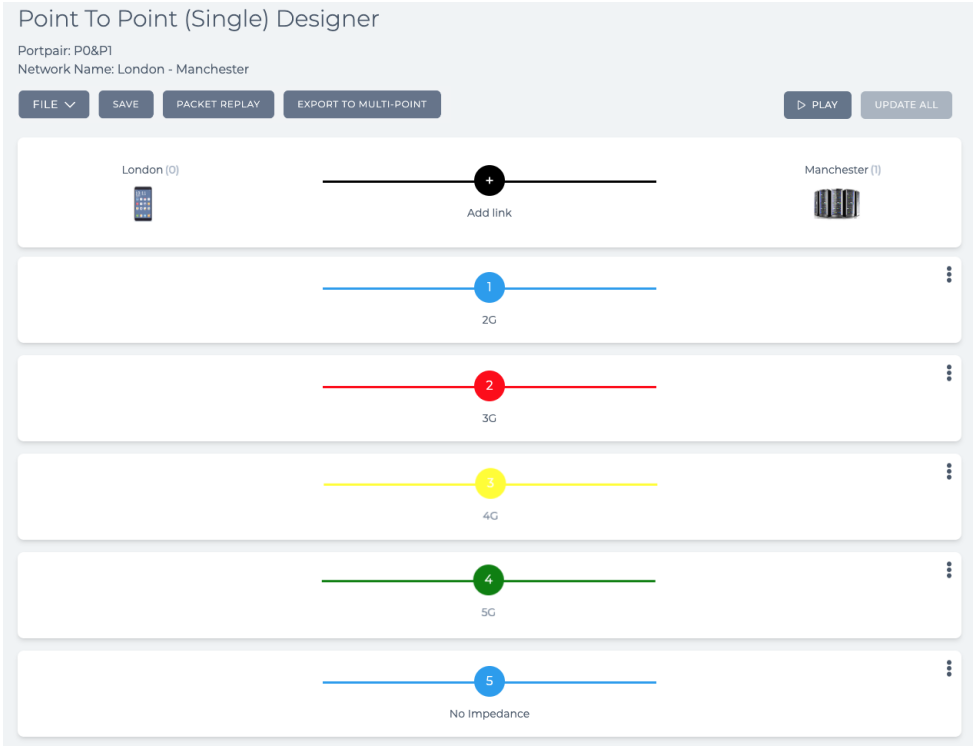
72. Click the **DONE** button to return to the The **Point To Point (Single) Designer** page.
The **Point To Point (Single) Designer** page now appears as follows.



73. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click **SAVE**.
74. Click the **Add link**  icon.

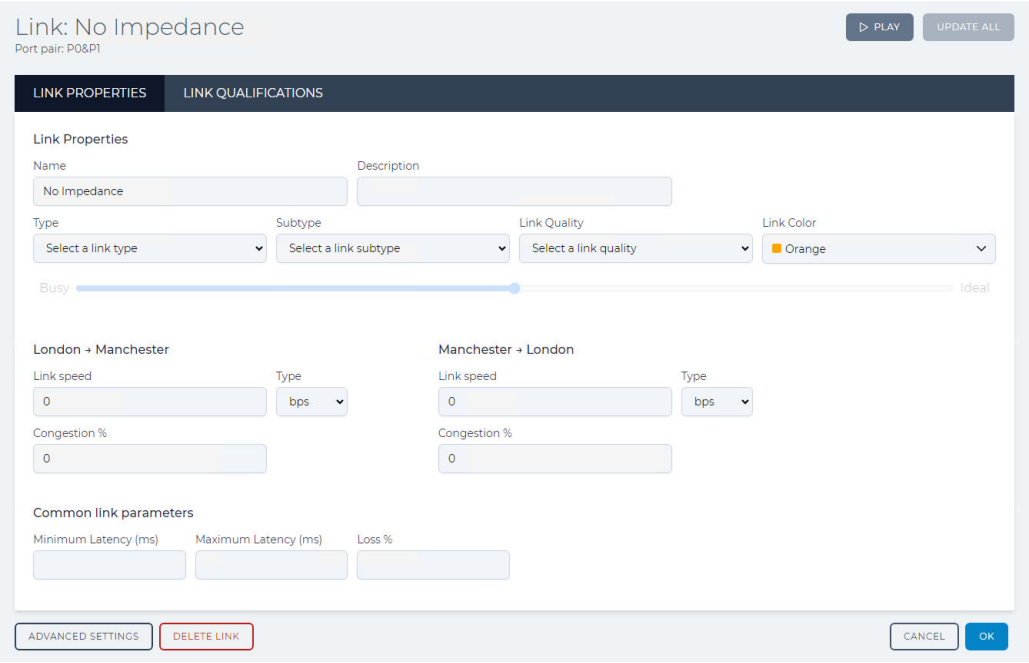
75. From the **Link name** dialog box that appears, type **`No Impedance`** and click **OK**.

    The **Point To Point (Single) Designer** page updates with the newly created No Impedance link as follows.



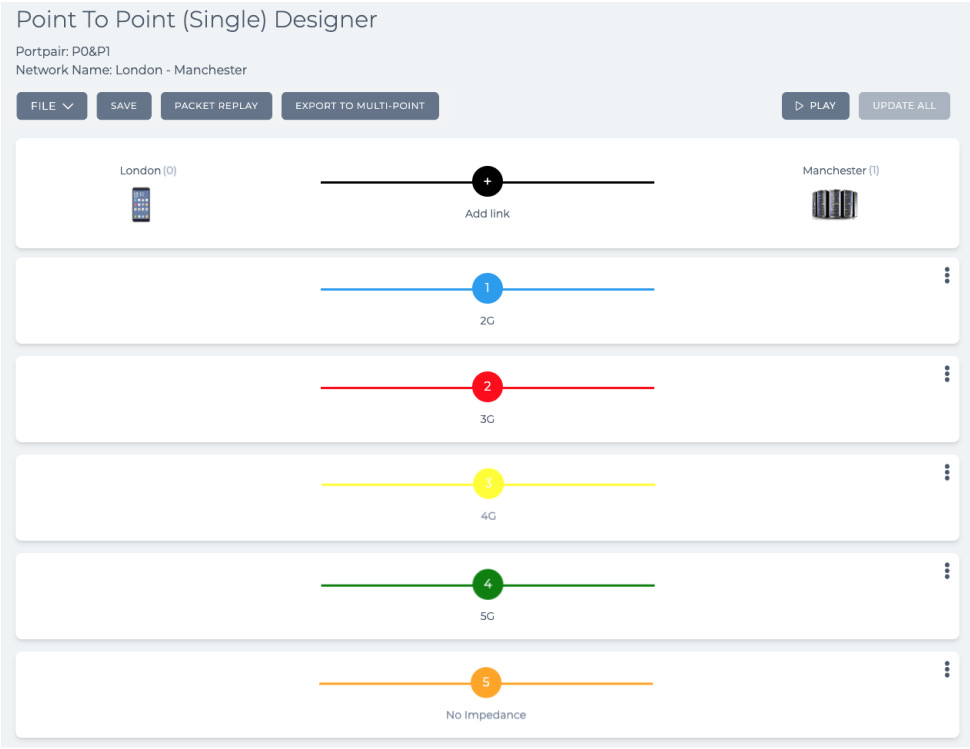
76. The link **No Impedance** will be assigned to the no impedance link for all other computers. Click on the **No Impedance** link to define its settings (link properties and link qualifications).
77. From the **Link: No Impedance** page that appears, do the following in the **LINK PROPERTIES** tab:
    a. In the **Name** field, no changes are required (No Impedance already appears as it was defined when you added the new link).
    b. In the **Description** field, type **`No Impedance`**.
    c. Leave the **Type** drop-down field with no settings.
    d. Leave the **Subtype** drop-down field with no settings.
    e. Leave the **Link Quality** drop-down field with no settings.

f. Click the **Link Color** field, and select **Orange**.



Note: No link qualifications need to be defined. All other clients will use this No Impedance link.

78. Click the **OK** button to return to the The **Point To Point (Single) Designer** page.
    The **Point To Point (Single) Designer** page now appears as follows.



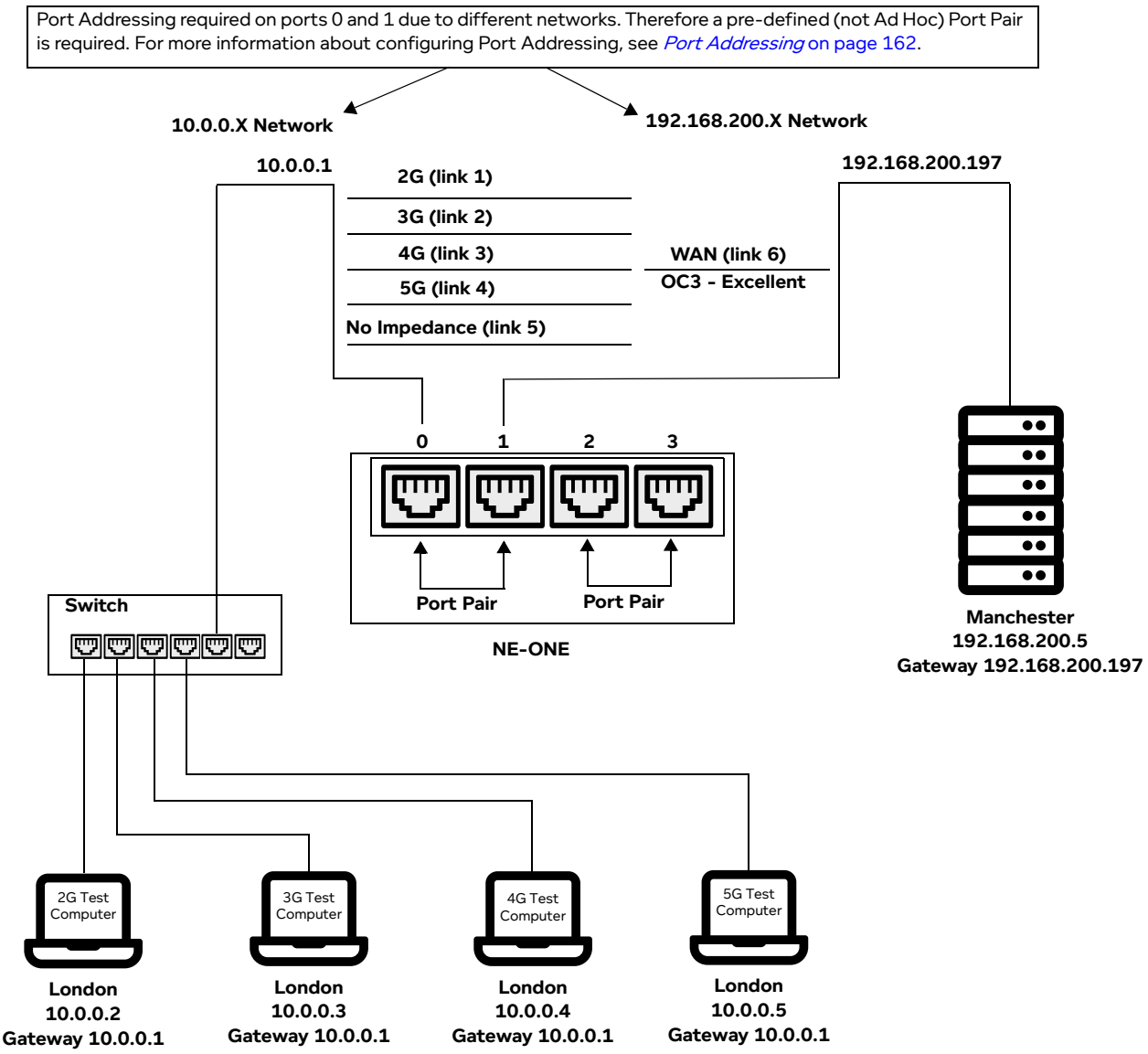
79. Save the finalized Point-to-Point network. To do this, select **FILE > Save** click **SAVE**.
    The network is complete, and ready to be run (played).

4-2. Creating Point-to-Point Networks (Dual)

As discussed in *Creating Point-to-Point Networks (Single)* on page 265, using more than two links lets you set different network conditions for a single or group of IP Addresses, Applications or VLANs. Using our previous example, we now have two locations with five links (2G, 3G, 4G, 5G and No impedance) combining into one WAN (OC3, Excellent) link. In the following example, five links are configured with different mobile network types, and are combined into a sixth WAN (OC3, Excellent) link:

- Computer with IP Address 10.0.0.2 (Netmask 255.255.255.0, Gateway 10.0.0.1) will use the 2G link (link1).
- Computer 10.0.0.3 (Netmask 255.255.255.0, Gateway 10.0.0.1) will use the 3G link (link2).
- Computer 10.0.0.4 (Netmask 255.255.255.0, Gateway 10.0.0.1) will use the 4G link (link3).
- Computer 10.0.0.5 (Netmask 255.255.255.0, Gateway 10.0.0.1) will use the 5G link (link4).
- Packets that do not qualify for 2G, 3G, 4G or 5G will traverse the 'No impedance' (link 5).

ILLUSTRATION 83 - EXAMPLE POINT-TO-POINT DUAL HOP NETWORK - 5 LINKS WITH PORT ADDRESSING INTO WAN LINK



Links 1 to 4 apply different network conditions for the four computers. Link 5 will forward all other traffic across a link which is not impeded. If link 5 is not defined then all other traffic would be dropped.

Link Qualification Criteria can be specified as a single item, range or combination of both and the criteria can be specified separately (i.e. IP Addressing only) or together (i.e. A combination of IP Addressing, Ports and VLANs).

Note:

Link Qualification criteria is applied in both directions. For example, when specifying an IP Address, it would use the link if its in the packet's source or destination IP Address fields. The same applies to the TCP/UDP Port.

The following example procedure assumes that you are using a pre-defined port pair called **P0&P1** with port 0 for the left port, and port 1 for the right port. Also, in the following example procedure, you must use a predefined port pair and not an Ad Hoc port pair, because Ad Hoc port pairs do not support specific port addressing criteria. The following example procedure assumes that a pre-defined port pair called **P0&P1** has Port Addressing enabled, and configured according to the example in *Configuring Port Addressing* on page 167, in *Chapter 5*, *Ports and Services Management*.

Note:

For simplicity, compared to the example in *Creating Point-to-Point Networks (Single)* on page 265, no advanced link settings are set (i.e. the default impairment functions remain unchanged). This is intentional as the example procedure below is intended to show the general differences in terms of the number of links and nodes allowed between single and dual hop Point-to-Point networks. If advanced link settings are required, you can set them as described in *Creating Point-to-Point Networks (Single)* on page 265.

1. Launch the **Point-to-Point Designer** page, using one of the following methods:

   Method 1 (not possible if the ports use Port Addressing):

   a. Select **Networks > ↔ Ad Hoc**.
   b. From the **Choose Left Port** dialog box that appears, select **0** then click **OK**.
   c. From the **Choose Right Port** dialog box that appears, select **1** then click **OK**.
   d. From the **Network Wizard** page (see *Illustration 69*) that appears, click **New Network**.
   e. In the **Point to Point (Dual)** tile, click **CREATE**.
   f. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London Manchester Dual Hop`**), then click **OK**.

   Method 2 (not possible if the ports use Port Addressing):

   a. Select **Networks**.
   b. From the **Network Wizard** page (see *Illustration 69*) that appears, click **New Network**.
   c. In the **Point to Point (Dual)** tile, click **CREATE**.
   d. From the **Choose Port Pair** dialog box that appears, select **Ad Hoc**, then click **OK**.
   e. From the **Choose Left Port** dialog box that appears, select **0** then click **OK**.
   f. From the **Choose Right Port** dialog box that appears, select **1** then click **OK**.
   g. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London Manchester Dual Hop`**), then click **OK**.

   Method 3:

   a. Select **Networks**.
   b. From the **Network Wizard** page (see *Illustration 69*) that appears, click **New Network**.

c. In the **Point to Point (Dual)** tile, click **CREATE**.
d. From the **Choose Port Pair** dialog box that appears, select the pre-defined **P0&P1** then click **OK**.
e. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London Manchester Dual Hop`**), then click **OK**.

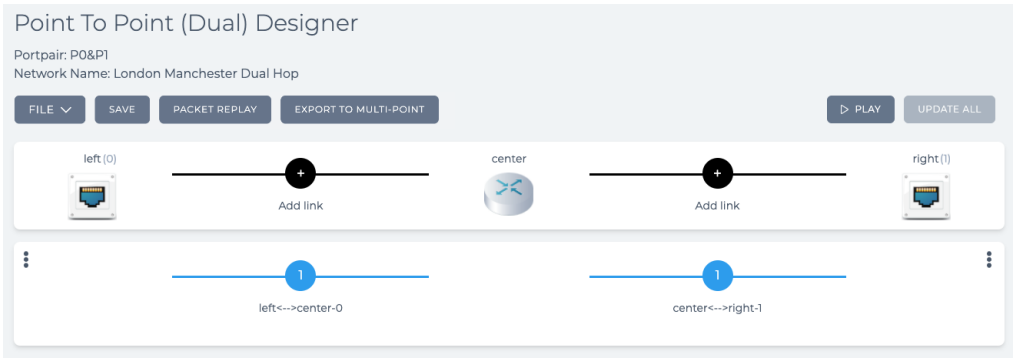
Method 4:

a. Select **Networks > ↔ P0&P1**.
b. From the **Port Pair Network Wizard** page (see *Illustration 70*) that appears, click **New Network**.
c. In the **Point to Point (Dual)** tile, click **CREATE**.
d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London Manchester Dual Hop`**), then click **OK**.

Method 5 (on a non-favorited (non-starred), pre-defined port pair):

a. Select **Networks > ↔ All Port Pairs**.
   The **Port Pairs** page (see *Example Port Pairs page* on page 157) appears.
b. From the **Port Pairs** page that appears, click on the **<Port Pair Name>** tile where <Port Pair Name> is the name of the pre-defined port pair (e.g. **P0&P1**) that you want to select.
   The **Port Pair Network Wizard** page associated to the selected pre-defined port pair appears.
c. From the **Port Pair Network Wizard** page (see *Illustration 70* on page 242) that appears, click **New Network**.
d. In the **Point to Point (Dual)** tile, click **CREATE**.
e. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London Manchester Dual Hop`**), then click **OK**.

A **Point To Point (Dual) Designer** page appears with generic node definitions and two temporary links called **left<-->center-0** and **center <-->right-1**.



At this point a network file `London Manchester Dual Hop.itn` has been created in your `/Private/networks` folder.

2. Click on the **left** node, and from the **Edit node** panel that appears, do the following to define a London based pedestrian:
   a. In the **Name** field, type **`London`**.
   b. In the **Description** field, type **`London Pedestrian`**.
   c. From the **Country** drop-down field, select **United Kingdom**.
      Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

d. From the **Choose a location** drop-down field, select and appropriate area for the location.
Note: You can start typing the location in order to select it quickly from the list of locations.

e. Click on the icon, and from the dialog box that appears click on the phone icon from within the **IoT** category, and then click **OK**.

f. Click to ✕ close the **Edit node** panel.

3. Click on the **center** node, and from the **Edit node** panel that appears, do the following to define a London based pedestrian:

a. In the **Name** field, type **`London DS`**.

b. In the **Description** field, type **`London Data Center`**.

c. From the **Country** drop-down field, select **United Kingdom**.
Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

d. From the **Choose a location** drop-down field, select and appropriate area for the location.
Note: You can start typing the location in order to select it quickly from the list of locations.

e. Leave the icon unchanged, and set to the router icon.

f. Click to ✕ close the **Edit node** panel.

4. Click on the **right** node, and from the **Edit node** panel that appears, do the following to define a Manchester based data center:

a. In the **Name** field, type **`Manchester`**.

b. In the **Description** field, type **`Manchester Data Center`**.

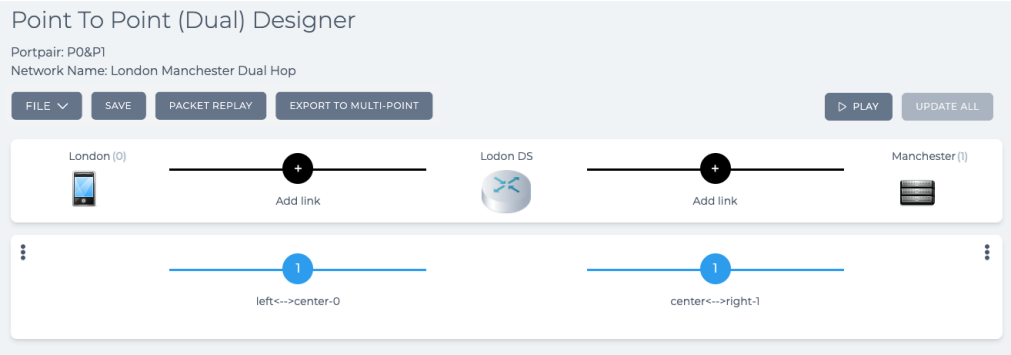
c. From the **Country** drop-down field, select **United Kingdom**.
Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

d. From the **Choose a location** drop-down field, select and appropriate area for the location.
Note: You can start typing the location in order to select it quickly from the list of locations.

e. Click on the icon, and from the dialog box that appears click on the server rack icon from within the **IT** category, and then click **OK**.

f. Click to ✕ close the **Edit node** panel.

The **Point To Point (Dual) Designer** page now appears as follows.



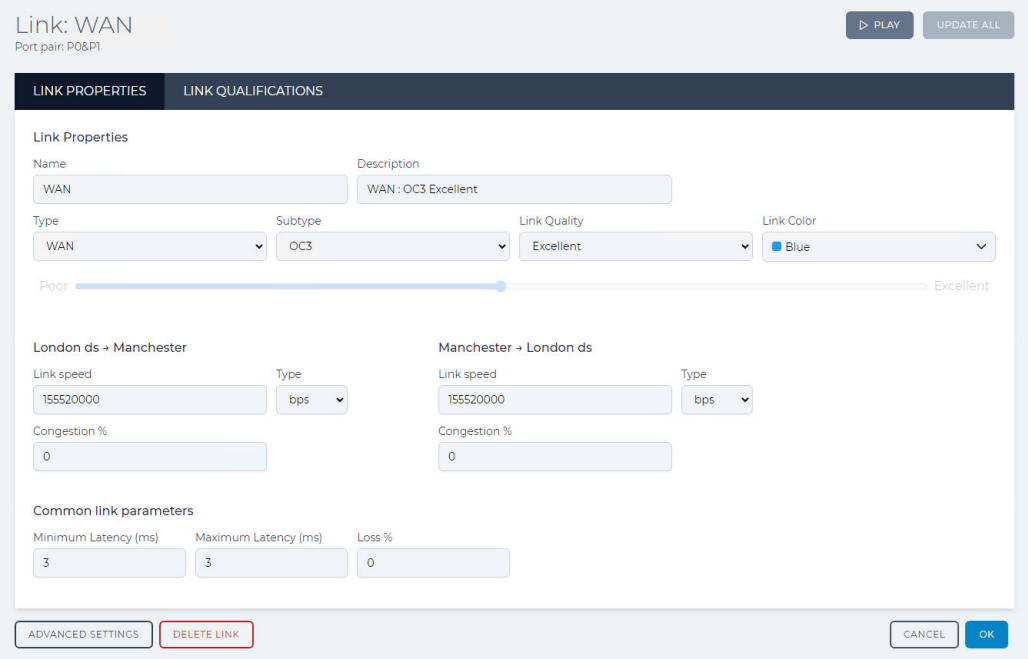
At this stage, all three nodes are configured. Next you need to define all the links, staring with the two initial links (i.e. **left<-->center-0** and **center<-->right-1**) that were automatically created.

5. The link **center<-->right-1** will be assigned to the WAN (OC3, Excellent) link. Click on the **center<-->right-1** link to define its settings (link properties).

6. From the **Link: center<-->right-1** page that appears, do the following in the **LINK PROPERTIES**

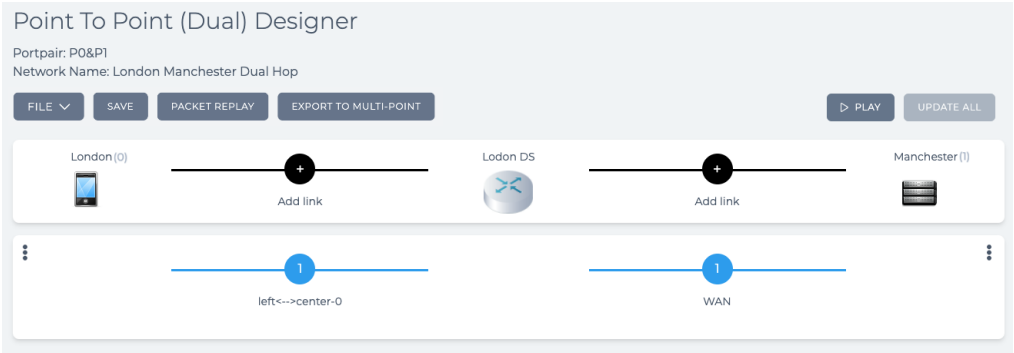
tab:

a. In the **Name** field, type **`WAN`**.
   The title of the page changes to **Link: WAN**.
b. In the **Description** field, type **`WAN : OC3 – Excellent`**.
c. From the **Type** drop-down field, select **WAN**.
d. From the **Subtype** drop-down field, select **OC3**.
e. From the **Link Quality** drop-down field, select **Excellent**.
   The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.
f. Leave the **Link Color** field set to Blue.



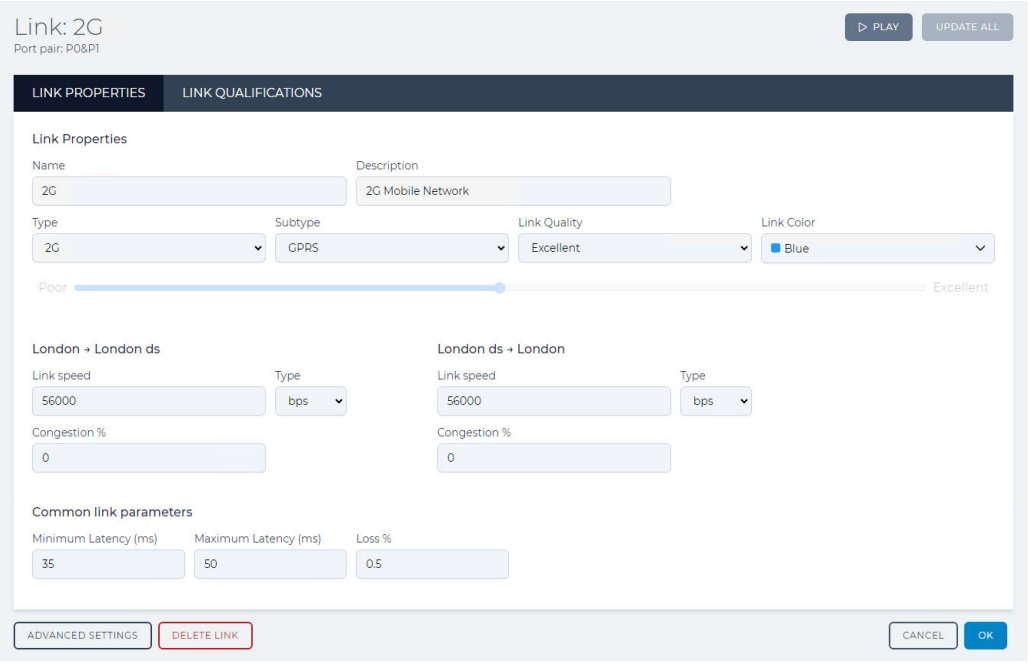
Note: Since traffic from all the 5 links (2G, 3G, 4G, 5G, and No Impedance) are merged into this last hop WAN link, no link qualifications are set.

7. Click the **OK** button to return to the The **Point To Point (Dual) Designer** page.
   The **Point To Point (Dual) Designer** page now appears as follows.

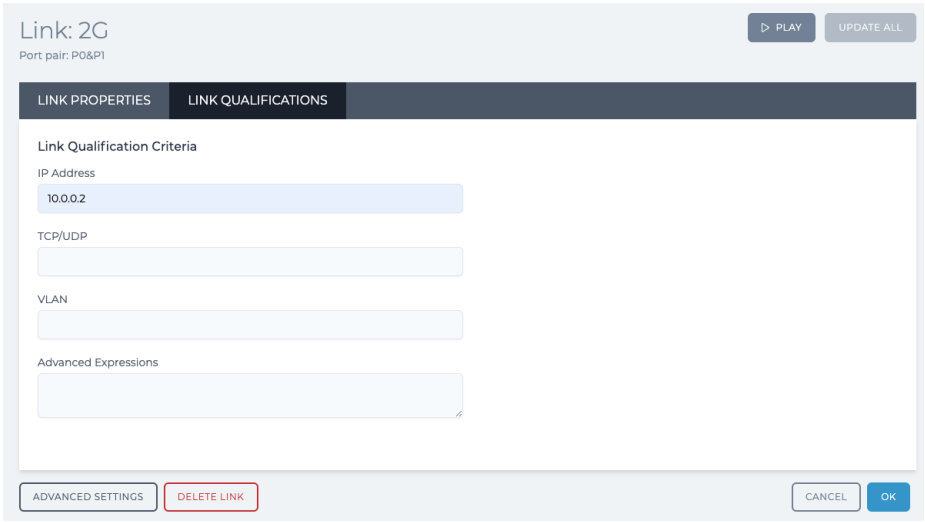


8. The initial link **left<-->center-0** will be assigned to the 2G link for the computer with IP address 10.0.0.2. Click on the **left<-->center-0** link to define its settings (link properties and link qualifications).

9. From the **Link: left<-->center-0** page that appears, do the following in the **LINK PROPERTIES** tab:
   a. In the **Name** field, type **2G**.
      The title of the page changes to **Link: 2G**.
   b. In the **Description** field, type **`2G Mobile Network`**.
   c. From the **Type** drop-down field, select **2G**.
   d. From the **Subtype** drop-down field, select **GPRS**.
   e. From the **Link Quality** drop-down field, select **Excellent**.
      The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.
   f. Leave the **Link Color** field set to Blue.

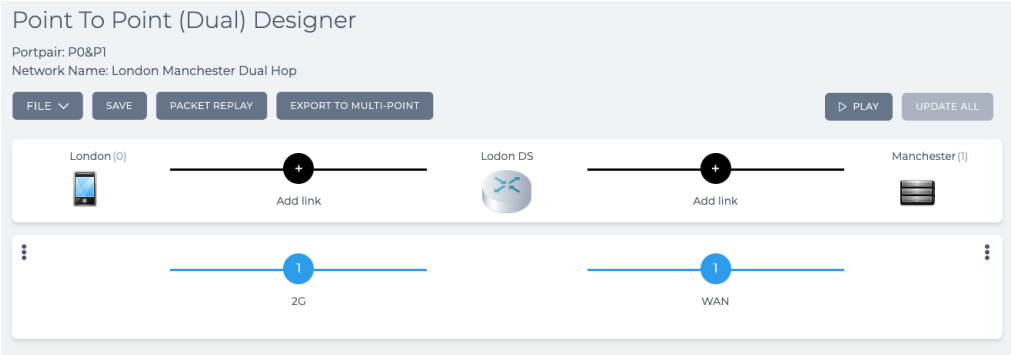


10. From the **Link: 2G** page, click the **LINK QUALIFICATIONS** tab.
11. In the **IP Address** field, type **`10.0.0.2`**.



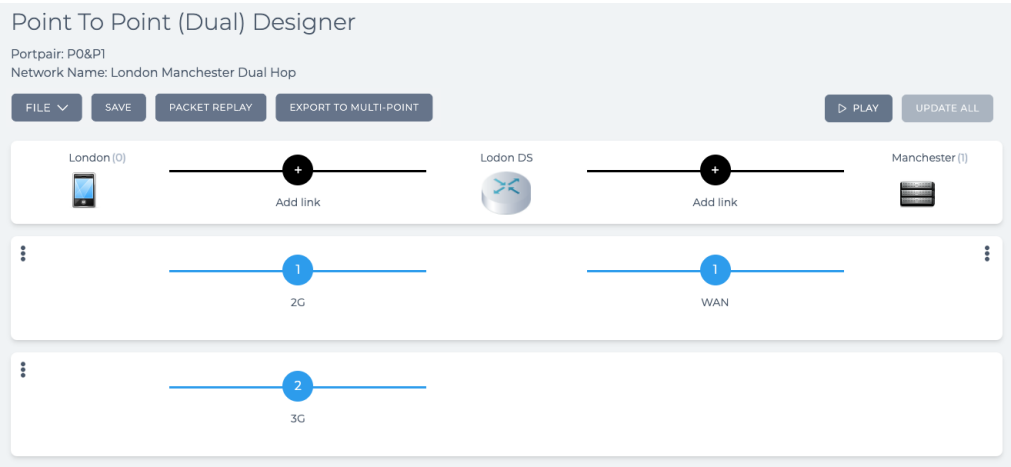
12. Click the **OK** button to return to the The **Point To Point (Dual) Designer** page.

The **Point To Point (Dual) Designer** page now appears as follows.



13. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click **SAVE**.
14. Click the left hand side **Add link**  icon between the two London nodes.
15. From the **Link name** dialog box that appears, type **3G** and click **OK**.

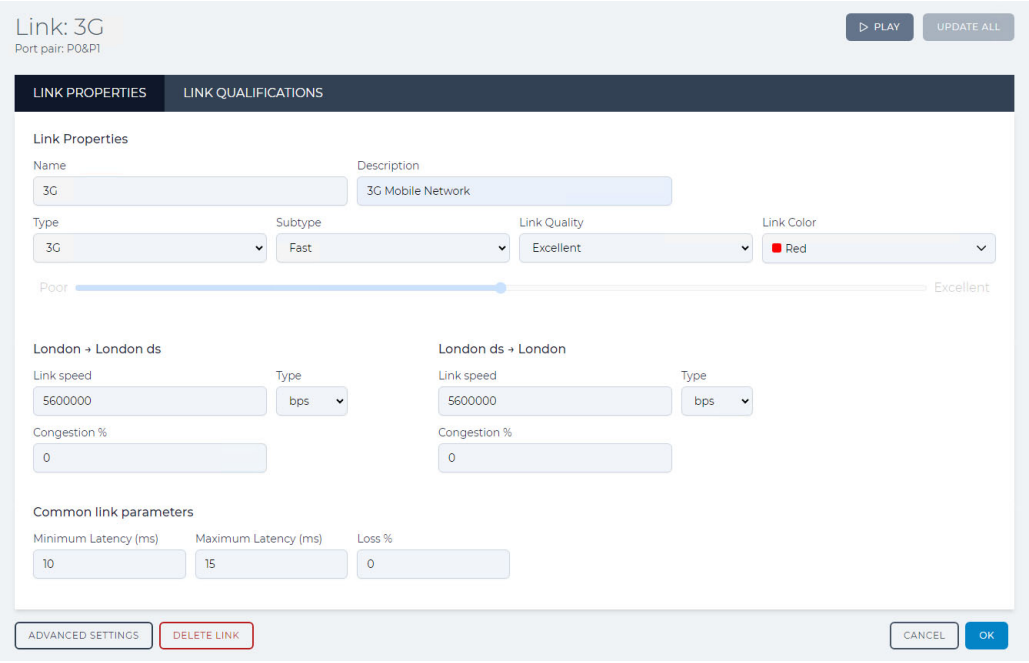
    The **Point To Point (Dual) Designer** page updates with the newly created 3G link as follows.



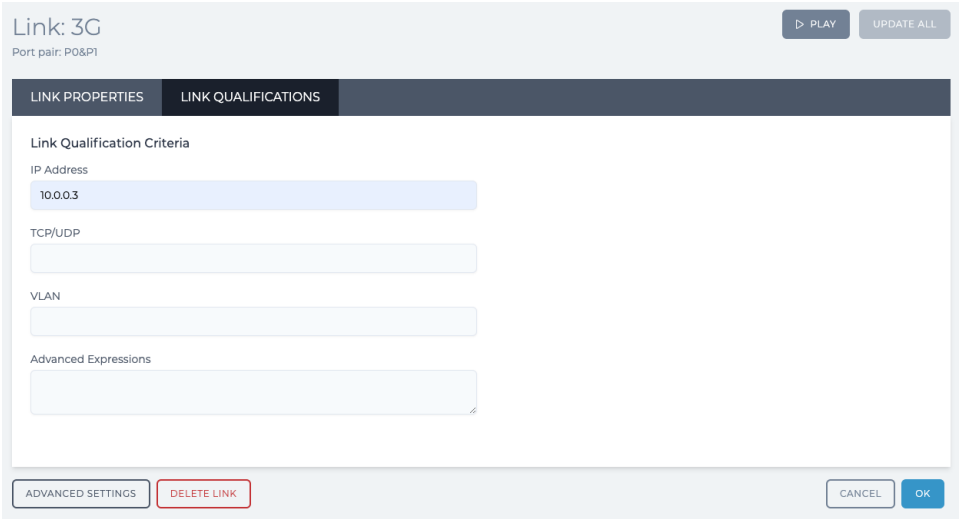
16. The link **3G** will be assigned to the 3G link for the computer with IP address 10.0.0.3. Click on the **3G** link to define its settings (link properties and link qualifications).
17. From the **Link: 3G** page that appears, do the following in the **LINK PROPERTIES** tab:
    a. In the **Name** field, no changes are required (3G already appears as it was defined when you added the new link).
    b. In the **Description** field, type **`3G Mobile Network`**.
    c. From the **Type** drop-down field, select **3G**.
    d. From the **Subtype** drop-down field, select **Fast**.
    e. From the **Link Quality** drop-down field, select **Excellent**.

    The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.

f. Click the **Link Color** field, and select **Red**.

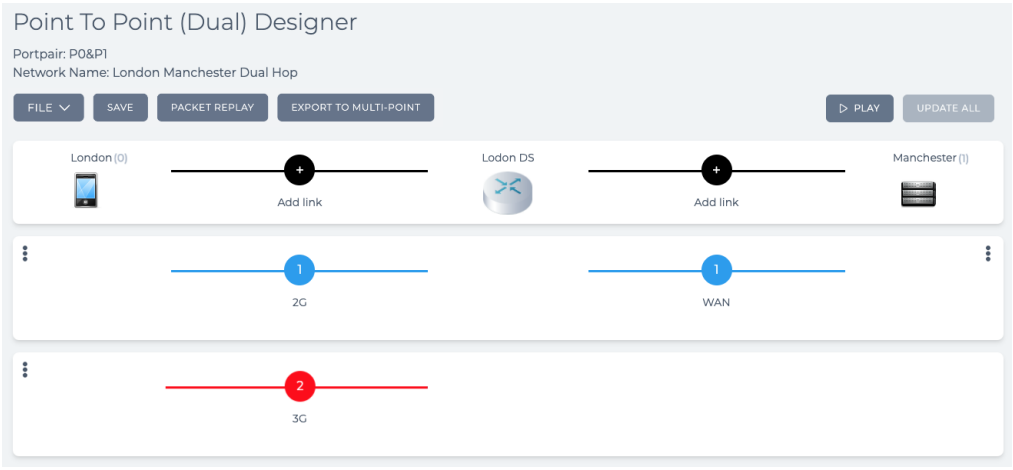


18. From the **Link: 3G** page, click the **LINK QUALIFICATIONS** tab.
19. In the **IP Address** field, type **`10.0.0.3`**.



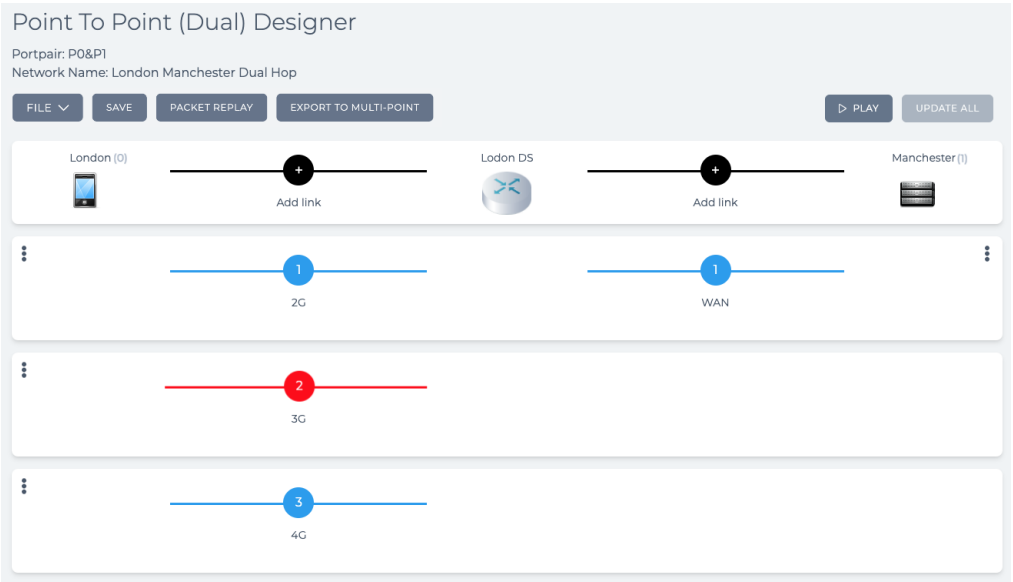
20. Click the **OK** button to return to the The **Point To Point (Dual) Designer** page.

The **Point To Point (Dual) Designer** page now appears as follows.



21. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click **SAVE**.
22. Click the left hand side **Add link**  icon between the two London nodes.
23. From the **Link name** dialog box that appears, type **`4G`** and click **OK**.

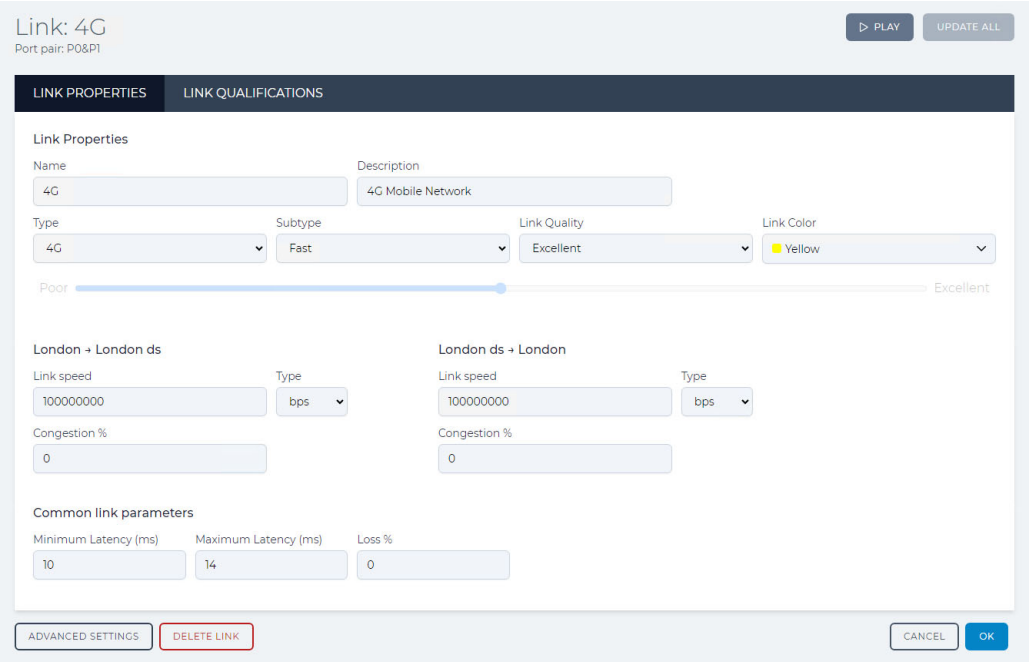
    The **Point To Point (Dual) Designer** page updates with the newly created 4G link as follows.



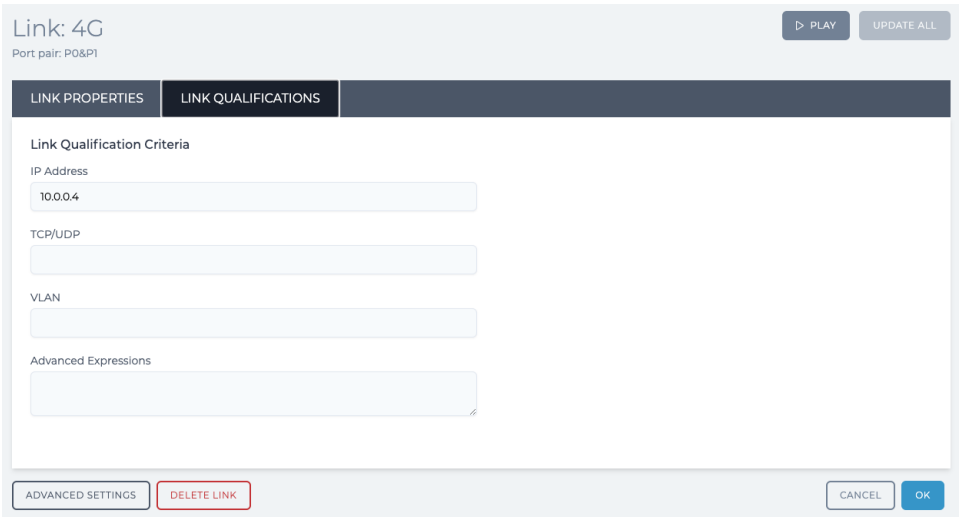
24. The link **4G** will be assigned to the 4G link for the computer with IP address 10.0.0.4. Click on the **4G** link to define its settings (link properties and link qualifications).
25. From the **Link: 4G** page that appears, do the following in the **LINK PROPERTIES** tab:
    a. In the **Name** field, no changes are required (4G already appears as it was defined when you added the new link).
    b. In the **Description** field, type **`4G Mobile Network`**.
    c. From the **Type** drop-down field, select **4G**.
    d. From the **Subtype** drop-down field, select **Fast**.
    e. From the **Link Quality** drop-down field, select **Excellent**.

    The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.

f. Click the **Link Color** field, and select **Yellow**.

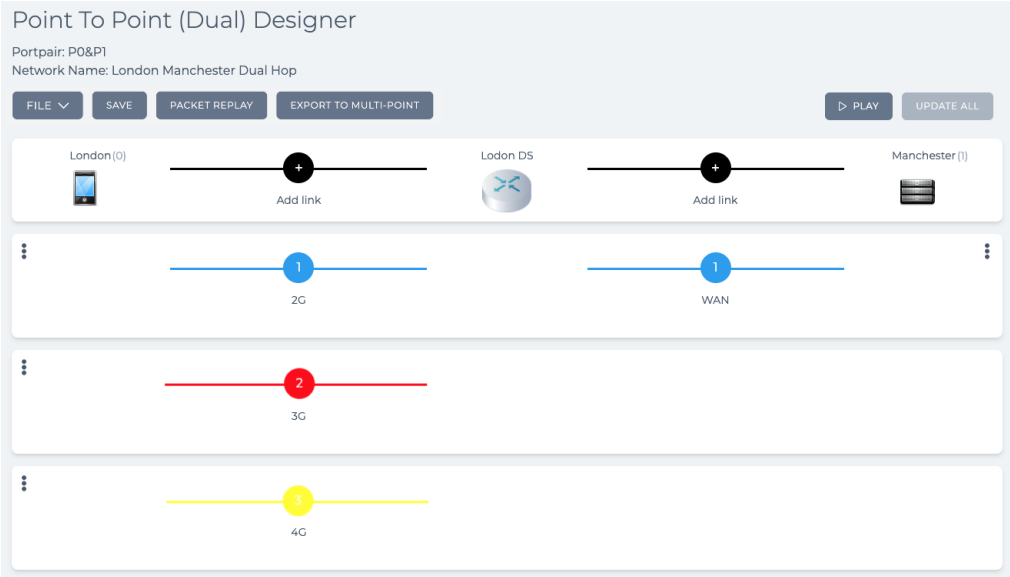


26. From the **Link: 4G** page, click the **LINK QUALIFICATIONS** tab.
27. In the **IP Address** field, type **`10.0.0.4`**.



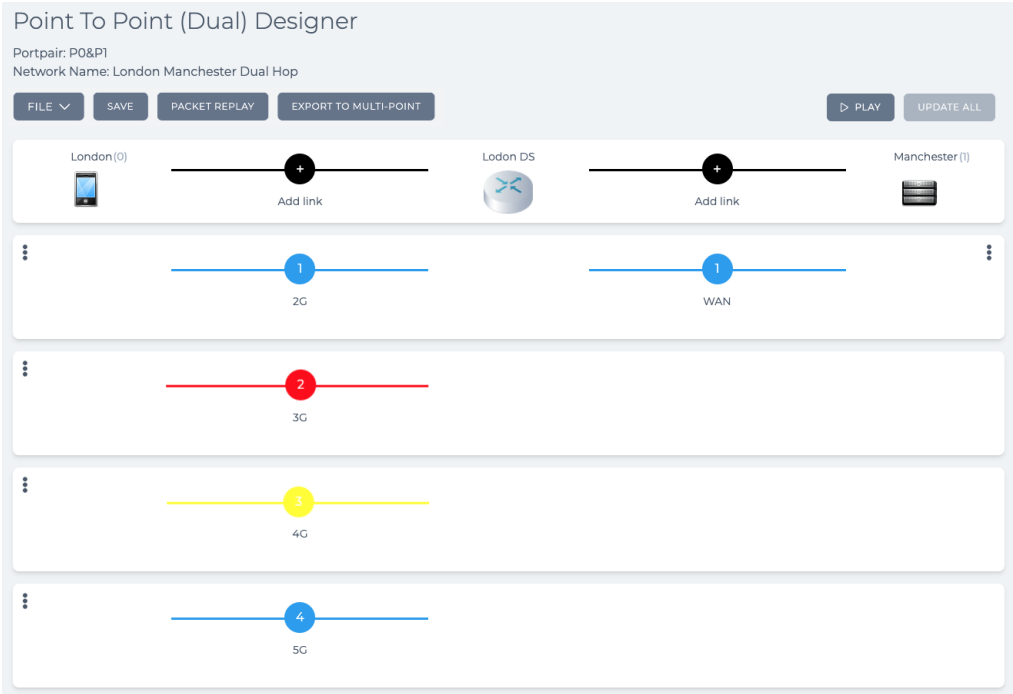
28. Click the **OK** button to return to the The **Point To Point (Dual) Designer** page.

The **Point To Point (Dual) Designer** page now appears as follows.



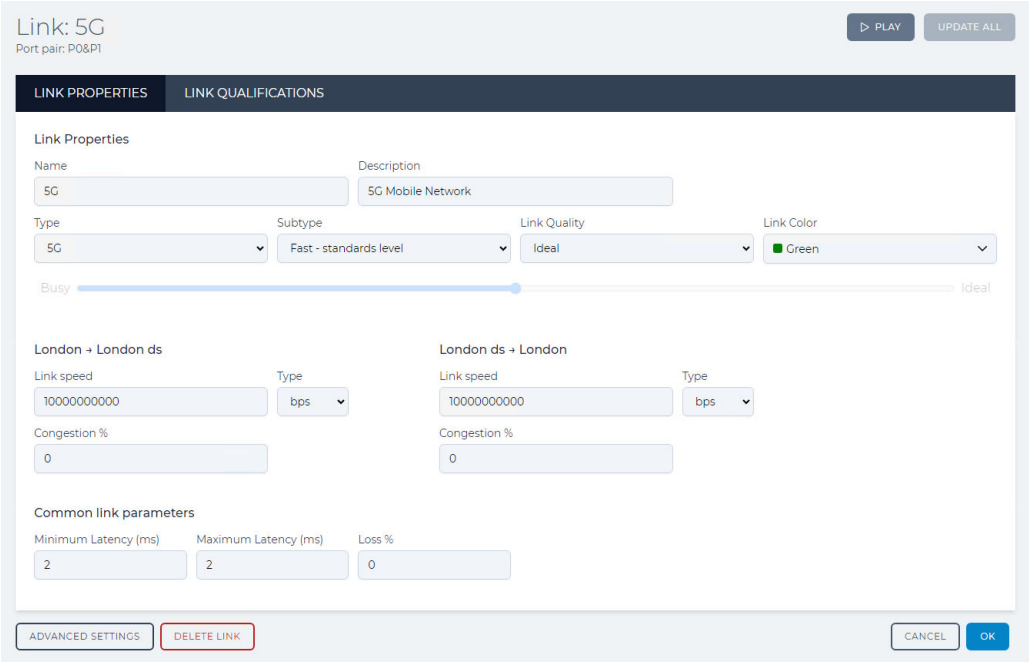
29. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click **SAVE**.
30. Click the left hand side **Add link**  icon between the two London nodes.
31. From the **Link name** dialog box that appears, type **5G** and click **OK**.

    The **Point To Point (Dual) Designer** page updates with the newly created 5G link as follows.

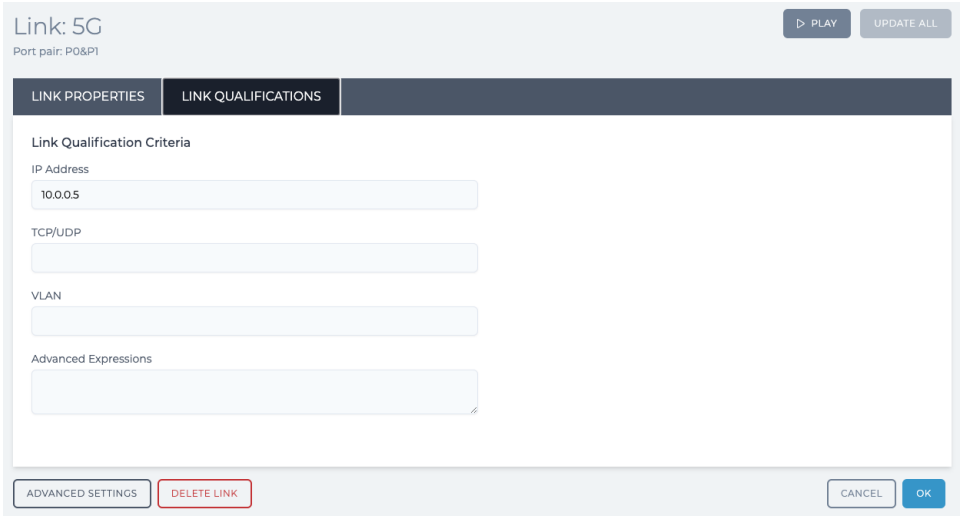


32. The link **5G** will be assigned to the 5G link for the computer with IP address 10.0.0.5. Click on the **5G** link to define its settings (link properties and link qualifications).
33. From the **Link: 5G** page that appears, do the following in the **LINK PROPERTIES** tab:
    a. In the **Name** field, no changes are required (5G already appears as it was defined when you added the new link).

b. In the **Description** field, type **`5G Mobile Network`**.
c. From the **Type** drop-down field, select **5G**.
d. From the **Subtype** drop-down field, select **Fast - standards level**.
e. From the **Link Quality** drop-down field, select **Ideal**.
The right port to left port and left port to right port parameters, and common link parameters automatically update. For this example, leave these parameters unchanged.
f. Click the **Link Color** field, and select **Green**.

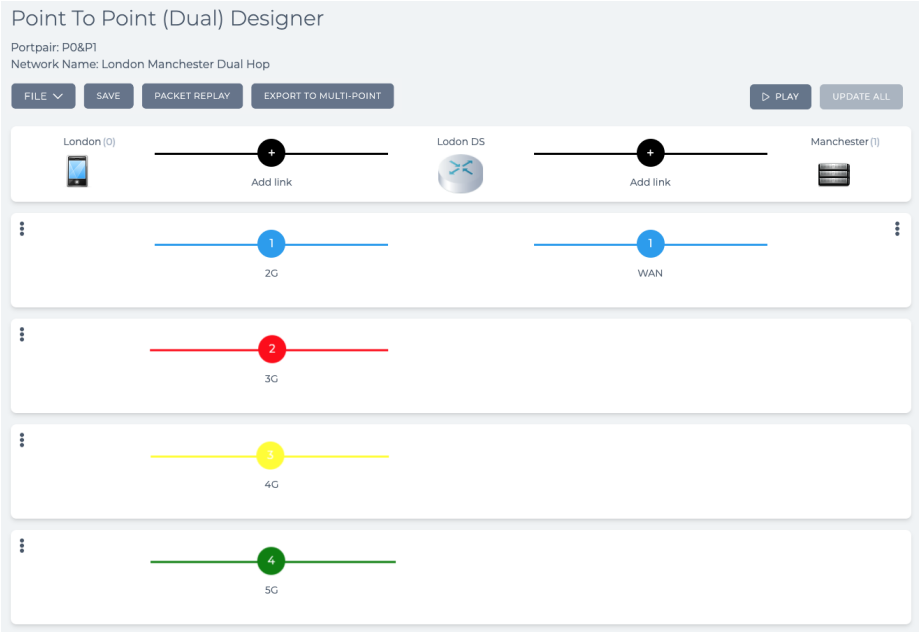


34. From the **Link: 5G** page, click the **LINK QUALIFICATIONS** tab.
35. In the **IP Address** field, type **`10.0.0.5`**.



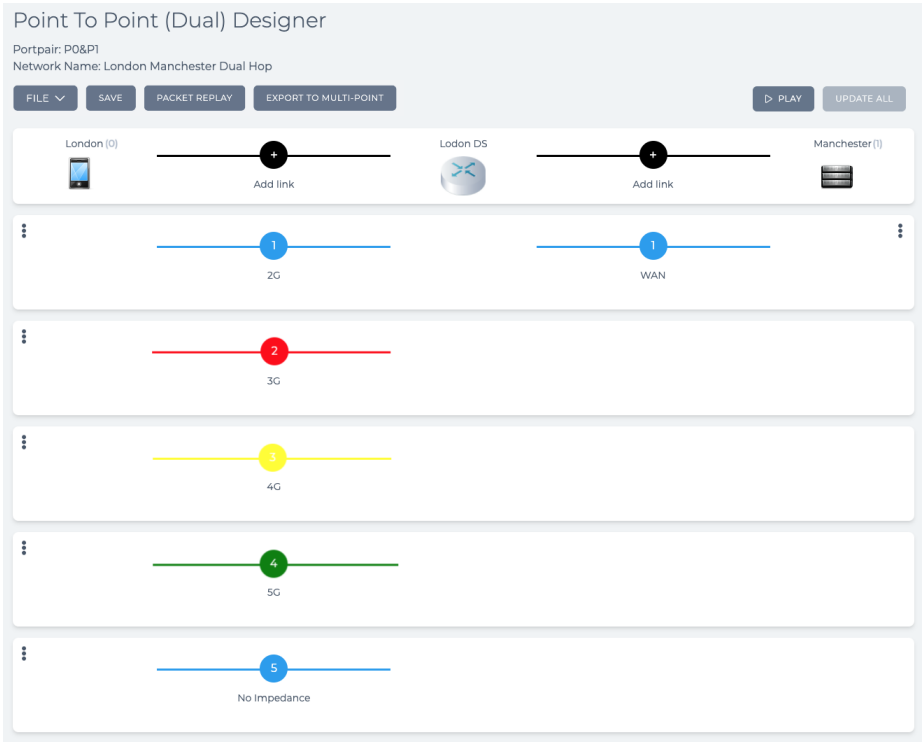
36. Click the **OK** button to return to the The **Point To Point (Dual) Designer** page.

The **Point To Point (Dual) Designer** page now appears as follows.



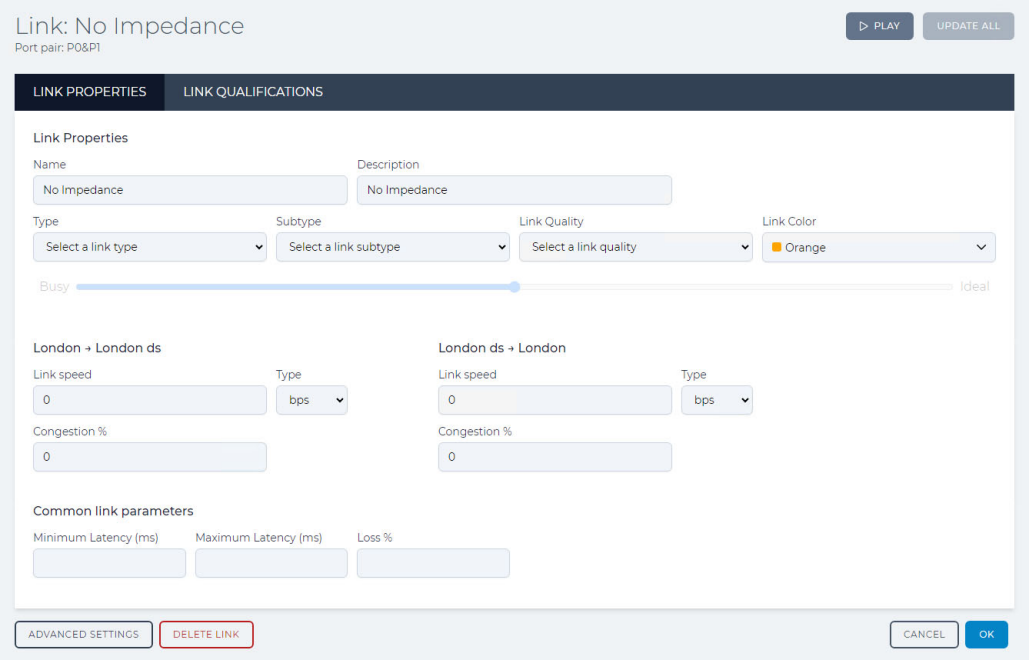
37. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click **SAVE**.
38. Click the left hand side **Add link**  icon between the two London nodes.
39. From the **Link name** dialog box that appears, type **`No Impedance`** and click **OK**.

    The **Point To Point (Dual) Designer** page updates with the newly created No Impedance link as follows.



40. The link **No Impedance** will be assigned to the no impedance link for all other computers. Click on the **No Impedance** link to define its settings (link properties and link qualifications).

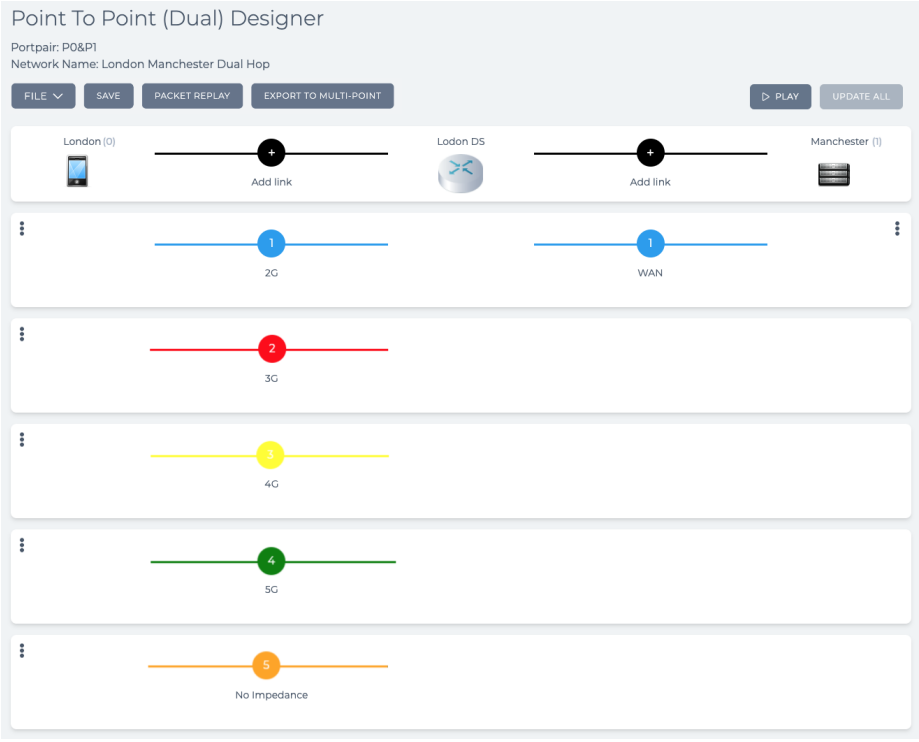
41. From the **Link: No Impedance** page that appears, do the following in the **LINK PROPERTIES** tab:
    a. In the **Name** field, no changes are required (No Impedance already appears as it was defined when you added the new link).
    b. In the **Description** field, type **`No Impedance`**.
    c. Leave the **Type** drop-down field with no settings.
    d. Leave the **Subtype** drop-down field with no settings.
    e. Leave the **Link Quality** drop-down field with no settings.
    f. Click the **Link Color** field, and select **Orange**.



Note: No link qualifications need to be defined. All other clients will use this No Impedance link.

42. Click the **OK** button to return to the The **Point To Point (Dual) Designer** page.

The **Point To Point (Dual) Designer** page now appears as follows.



43. Save the finalized Point-to-Point network. To do this, select **FILE > Save** or click **SAVE**.
    The Point-to-Point network is complete, and ready to be run (played).

5. OPENING AND PLAYING POINT-TO-POINT NETWORKS

Point-to-Point networks can be opened via two ways. Once opened, a Point-to-Point network can be either edited or played.

- Via the Home Page.
- Via the File Browser. For more information, see *Opening a Point-to-Point Type Network From the File Browser* on page 589 in *Chapter 13*, *The File Browser*.

Note:
Once a Point-to-Point network is playing it is attached to the user who run it, and the ports that it is using cannot be used by any other networks until the currently playing network is stopped. Currently playing networks are listed in the **Active** tab of the **Home** page.

Note:
You can also directly play a Point-to-Point network from within the File Browser, without needing to open it. For more information, see *Directly Playing a Point-to-Point Type Network From the File Browser* on page 591 in *Chapter 13*, *The File Browser*.

6. DELETING POINT-TO-POINT NETWORKS

If a Point-to-Point network is no longer needed, it can be deleted from the NE-ONE using the File Browser. Point-to-Point networks have a file name extension `*.itn`, are located in your `/Private/networks` directory with the ↔ icon, and use the network name that you had specified for the file name. To delete a no longer required Point-to-Point network, use the following steps:

1. Click **Management > ••• Platform Settings > File Browser** to launch the File Browser.
2. Navigate to the `/Private/networks` directory, and identify the Point-to-Point network you want to delete via its icon ↔ and its file name (`*.itn`).
3. Right mouse click on the Point-to-Point network file, and select **Delete selected File/Folder** from the File Browser pop-up menu that appears.
4. From the **Confirm delete** dialog box that appears, click **OK**.

This page is intentionally left blank.

CHAPTER 10 CREATING AND RUNNING MULTI-POINT NETWORKS

1. INTRODUCTION

This chapter is applicable to non-admin and admin users, and describes:

- the general Web Interface associated with creating Multi-Point type networks
- example procedures for creating Multi-Point type networks

Network types can be categorized into two high-level network topology types, as follows:

- Point-to-Point, including:
  - Point to Point (single)
  - Point to Point (dual hop)
- Multi-Point, including:
  - Fully Meshed
  - Hub and Spoke
  - Cloud (star)
  - Free Form

Note:

The Multi-Point Designer and associated Multi-Point network topologies (i.e. Fully Meshed, Hub and Spoke, Cloud, and Free Form) are only available with the Multi-Point Designer feature. Depending on your license, the Multi-Point Designer and associated Multi-Point network topologies may be either activated or deactivated.

This chapter is dedicated to creating and running Multi-Point type networks. For creating and running Point-to-Point networks, see *Chapter 9*, *Creating and Running Point-to-Point Networks* on page 239.

2. PREREQUISITES

Before creating networks on the NE-ONE, an admin user must have already done the following:

- installed and set up the NE-ONE according to the procedures in *Chapter 4*, *Installation and Configuration*
- configured all the necessary port pairs, soft ports, and services according to *Chapter 5*, *Ports and Services Management*

Note:

The Port Manager feature and Service Manager feature are premium features. Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated.

- administered all users, and assigned appropriate ports and port pairs to the users according to *Chapter 6*, *User Administration* on page 199

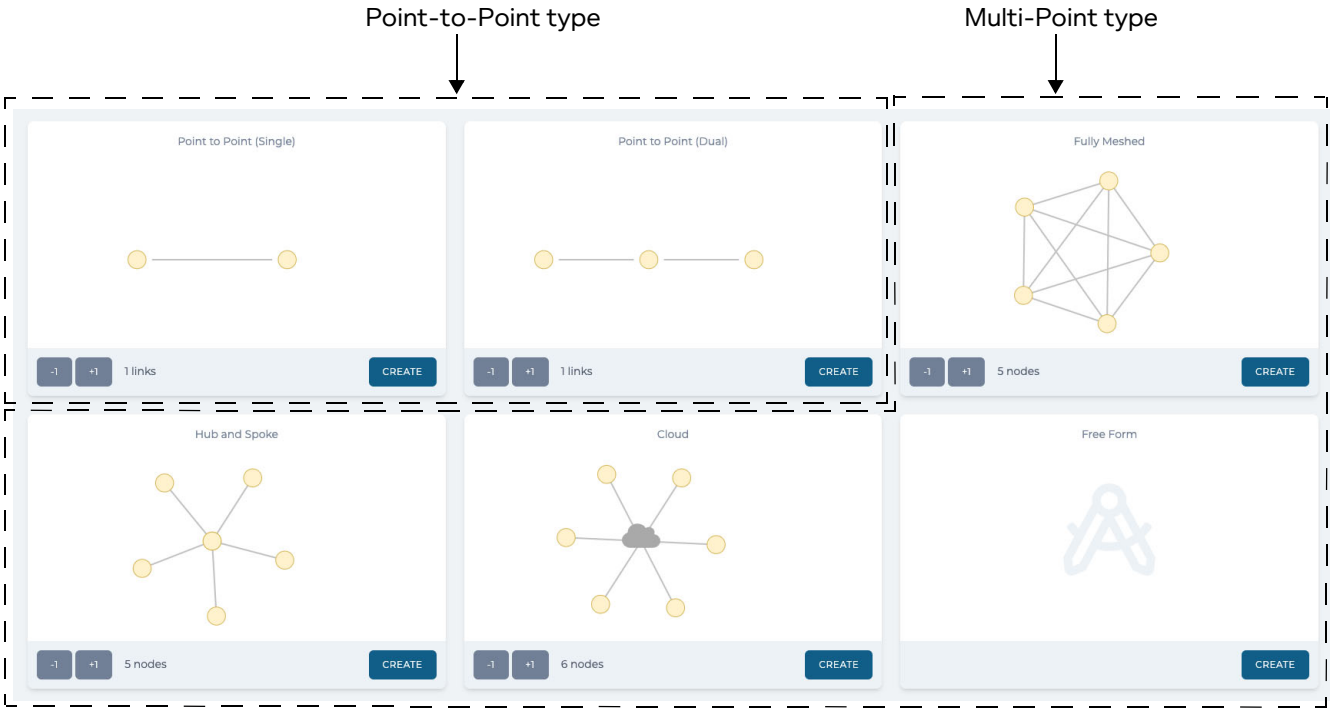
3. WEB INTERFACE NETWORK PAGES (MULTI-POINT)

This section contains a description of the Web Interface pages related to creating Multi-Point type networks.

3-1. The Network Wizard Page (from a Multi-Point Perspective)

The **Network Wizard** page (see *Illustration 84*) appears after clicking the **+ NEW NETWORK** button from the **Home** page (see *Illustration 3* on page 40), or clicking the **New Network** tile from the **Networks** page (see *Illustration 4* on page 42).

ILLUSTRATION 84 - NETWORK WIZARD PAGE



The **Network Wizard** page contains a network topology template panel for each of the network topology types, from where a network can be created.

The network topology types are categorized into two high-level types, as follows:

- Point-to-Point, including:
  - Point to Point (single)
  - Point to Point (dual hop)
- Multi-Point, including:
  - Fully Meshed
  - Hub and Spoke
  - Cloud
  - Free Form

Note:

The Multi-Point Designer and associated Multi-Point network topologies (i.e. Fully Meshed, Hub and Spoke, Cloud, and Free Form) are only available with the Multi-Point Designer feature. Depending on your license, the Multi-Point Designer and associated Multi-Point network topologies may be either activated or deactivated.

Each of the network template topology panels (except Free form) contain a **-1** and **+1** button.

The **-1** and **+1** buttons for Multi-Point network topologies function as follows:

- Clicking on the **+1** button each time for a Multi-Point network topology increases the number of nodes by one. The number of links between each node is set to one, but this can be modified after in the **Multi-Point Designer** page.
- Clicking on the **-1** button each time for a Multi-Point network topology decreases the number of nodes by one. The number of links between each node is set to one, but this can be modified after in the **Multi-Point Designer** page.

Clicking on the **CREATE** button for a Multi-Point type network topology directly opens the **Network Name** dialog box prompting you to specify the network name. After specifying the network name, a **Multi-Point Designer** page appears, from where you can complete the configuration of the network (i.e. configure the nodes and links). For more information, see *Multi-Point Designer Page for Multi-Point Topologies* on page 309.

Note:

The network name you specify can contain alphanumeric characters, special characters (except /, \, and *), and spaces, and is used for the file name of the network. Once a network is saved, it is located in your `/Private/networks` directory and only accessible to you. You can share your networks with other users by using the File Browser. For more information on sharing networks, see *Sharing Networks via the File Browser* on page 593, in *Chapter 13*, *The File Browser*.

Note:

If creating a network on an NE-ONE Desktop which has an LCD panel, that network can optionally be made accessible from the LCD panel. In order for the network to be accessible to the LCD panel you must use the File Browser to copy the network from your `/Private/networks` directory to the `/Public/networks` directory. Then you must request an admin type user to copy the network from the `/Public/networks` directory to the `/Library/networks/LCD` directory. For more information, see *Making Networks and Scenarios Accessible to the LCD Panel* on page 596 in *Chapter 13*, *The File Browser*.

Note:

If you want a created network on an NE-ONE Desktop to be accessible via the LCD panel, consider the fact that it has two lines of 20 characters. If a network name exceeds 18 characters, it will appear truncated in the LCD panel.

3-2. Multi-Point Designer Page for Multi-Point Topologies

Once a Multi-Point type network has initially been created from the **Network Wizard** page, it appears in a **Multi-Point Designer** page (*Illustration 85* on page 310), from where its node and link configuration can be completed.

The initial contents (i.e. links and nodes) that appear in the **Multi-Point Designer** page depend on the type of Multi-Point network you have chosen from within the **Network Wizard** page.

Note:

If you have chosen a Free-Form type of Multi-Point network, the Workspace area of the **Multi-Point Designer** page is empty - this is normal. As the name implies, the Free Form template lets you create a Multi-Point network from scratch without any "starting" template (i.e. Fully Meshed, Cloud or Hub and Spoke). The Free Form template lets you create both very simple and very complicated network topologies.

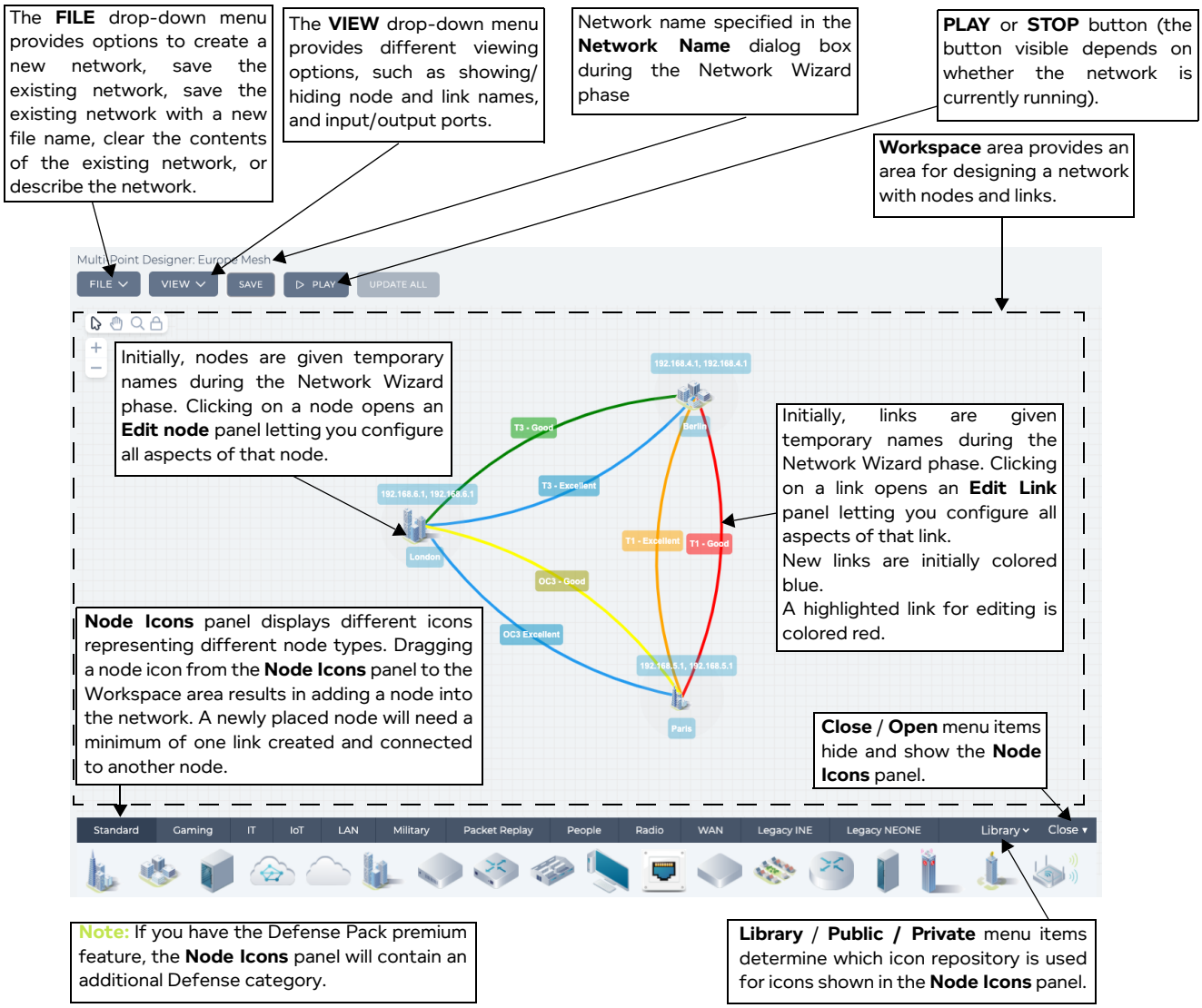
Conceptually speaking, the Multi-Point **Multi-Point Designer** page has exactly the same functionally for the Free Form, Fully Meshed, Cloud, and Hub and Spoke network topology templates. The only difference is the "starting point" provided by the templates in the Workspace.

The Free Form template provides an empty Workspace, whereas the Fully Meshed, Cloud or Hub and Spoke provide an initial network topology on the Workspace, with certain routing functions already applied to their nodes (see *Table 50* on page 336).
Therefore, you can consider that when you adapt a Multi-Point network that was based initially on Fully Meshed, Cloud or Hub and Spoke, you are in Free Form mode going forward when modifying the already existing Multi-Point network.

During the Network Wizard phase, only the network name is defined. All other aspects (i.e. nodes and links configuration) of the network must be completed from within the **Multi-Point Designer** page.

Illustration 85 shows an example of a simple Multi-Point network that was initially created from the **Network Wizard** page for a Fully Meshed topology with three nodes.

ILLUSTRATION 85 - EXAMPLE MULTI-POINT DESIGNER FOR A MULTI-POINT TOPOLOGY



The **Multi-Point Designer** page contains the elements summarized in *Table 44*.

TABLE 44 - MULTI-POINT DESIGNER ELEMENTS FOR MULTI-POINT NETWORKS

Multi-Point Designer Element	Description
FILE > New menu option	Selecting this option from the **FILE** drop-down menu keeps the current network open (indicated by either a play symbol or edit symbol in the tray), and returns you to the **Network Wizard** page (see *Illustration 84* on page 308).
FILE > Save menu option	Selecting this option from the **FILE** drop-down menu saves the current network with the same file name in your `/Private/networks` directory.
FILE > Save as menu option	Selecting this option from the **FILE** drop-down menu opens a dialog box letting you save the current network with a different file name in your `/Private/networks` directory. Networks have file names with the `.itn` file extension.
FILE > Description menu option	Selecting this option from the **FILE** drop-down menu opens a dialog box with a free field entry letting you write a description of the network, and how it is configured and to be used. Since your network can be complicated and shared with other users, this dialog box lets you describe important items that need to be remembered and communicate with other users.
FILE > Clear menu option	Selecting this option from the **FILE** drop-down menu removes all objects (i.e. node and links) from the Workspace.
FILE > Find in File Browser menu option	This is grayed out until the network has been saved. Selecting this option from the **FILE** drop-down menu opens the File Browser with the `.itn` file of the network selected.
FILE > Close menu option	Selecting this option from the **FILE** drop-down menu closes the network, and removes it from the Tray area of the Web Interface.
VIEW > Frame all menu option	Selecting this option from the **VIEW** drop-down menu results in resetting the Workspace to show all the nodes at the extreme edges of the Workspace.
VIEW > Background menu option	Selecting this option from the **VIEW** drop-down menu invokes a dialog box letting you select a background image to use for the Workspace. Once selected, the background image replaces the grid of the Workspace. The NE-ONE has one background image by default. Additional background images can be uploaded to the NE-ONE according to *Customizing and Sharing Background Files* on page 587 in *Chapter 13, The File Browser*.
VIEW > Keyboard Shortcuts menu option	Selecting this option from the **VIEW** drop-down menu invokes a temporary dialog box, which describes the following keyboard shortcut information: • Pressing the **P** or **S** key enables the object select mode (i.e. the same action as clicking on the icon). • Pressing the **G**, **M** or **Spacebar** key enables the Workspace pan mode (i.e. the same action as clicking on the icon). • Pressing the **Z** key enables the Workspace zoom mode (i.e. the same action as clicking on the icon).
VIEW > Show node names check box	This check box determines whether the node names are displayed on the Workspace. • Ticking this check box results in showing the node names on the Workspace. • Unticking this check box results in hiding the node names on the Workspace.
VIEW > Show link names check box	This check box determines whether the link names are displayed on the Workspace. • Ticking this check box results in showing the link names on the Workspace. • Unticking this check box results in hiding the link names on the Workspace.

Multi-Point Designer Element	Description
VIEW > Show node ports check box	Each node has an input port and output port. The input port and output port of each node of nodes can be displayed on the Workspace. This check box determines whether the node ports (both input and output) are displayed on the Workspace. • Ticking this check box results in showing the node names on the Workspace. • Unticking this check box results in hiding the node names on the Workspace. **Note:** if after ticking this check box a node does not display the input or output port next to the node, it is because the input or output port has not yet been set for the node.
VIEW > Lock backgrounds check box	This check box determines whether one or more imported backgrounds are locked by position within the Workspace. • Ticking this check box results in locking the imported backgrounds on the Workspace. • Unticking this check box results in unlocking the imported backgrounds on the Workspace, thus allowing them to be moved around.
VIEW > Visualize traffic flow check box	This check box determines whether or not the traffic flow is visualized on the links within the Multi-Point network while it is playing. The default setting is enabled. • Ticking this check box results in visualizing the traffic flow when the Multi-Point network is playing. In this case, when the Multi-Point network is playing, the color of all the links in the Multi-Point network change to gray, and when traffic is passing over a link it changes to either green (for traffic passing in both directions) or dotted orange (for traffic passing in one direction). • Unticking this check box results in not visualizing the traffic flow when the Multi-Point network is playing. In this case, when the Multi-Point network is playing, the links remain the color that are assigned to them from within the **Link Properties** page.
VIEW > Link Spacing slider	If the nodes within the Workspace have more than one link going between them, you can modify the distance between those links. • Moving the **VIEW > Link Spacing** slider to the left reduces the space between the links. • Moving the **VIEW > Link Spacing** slider to the right increases the space between the links.
SAVE button	Clicking on this button saves the current network with the same file name in your `/Private/networks` directory.
▷ **PLAY** button or ☐ **STOP** button	The state of this button varies according to whether or not the network is running. When the network is not running, a ▷ **PLAY** button is present, and the status icon for the network in the tray is ✎. Clicking on the ▷ **PLAY** button results in: • running the network • changing the network status icon to the play ⊙ symbol • changing the button state to ☐ **STOP** When the network is running, a ☐ **STOP** button is present, and the status icon for the network in the tray is ⊙. Clicking on the ☐ **STOP** button results in: • stopping the network • changing the network status icon to the edit ✎ symbol • changing the button state to ▷ **PLAY**

Multi-Point Designer Element	Description
UPDATE ALL button	This button is grayed out when the network is not running. When the network is running, this button is active. When the network is running, you can edit the parameters of the network (i.e. link and node parameters). Clicking this button applies all the changed parameters on the fly to the running network.
 Workspace navigation icon	When you arrive in the **Multi-Point Designer** page, this icon (object selection) is selected by default. Clicking on this icon enables object (i.e. nodes, links, and backgrounds) selection mode. When object selection mode is enabled you can do the following: • Click on existing nodes within the Workspace in order to select them for editing or deleting, or moving their existing position. • Click on existing links within the Workspace in order to select them for editing or deleting. • Click on a background (if one has been loaded into the Workspace) in order to move, rotate, and/or resize the background within the Workspace. For more information, see *Positioning, Rotating and Resizing a Background Image in the Workspace* on page 315 • Create links between nodes by clicking in the node perimeter area, and dragging the mouse point inside the node perimeter area of another node. For more information, see *Creating Links Between Nodes in the Workspace* on page 317. • Create additional nodes within the Workspace, by dragging an appropriate node icon from the **Node Icons** panel into the Workspace. A newly created node will need to be edited, and have a link or links added to it. For more information, see *Creating Nodes in the Workspace* on page 318.
 Workspace navigation icon	Clicking on this icon enables Workspace pan mode. When Workspace pan mode is enabled, you can do the following: • Move the Workspace in all directions by moving the mouse when the left mouse button is clicked. • Move the Workspace up by rolling the middle mouse roller button down. • Move the Workspace down by rolling the middle mouse roller button up. • Move the Workspace left by rolling the middle mouse roller button down while the **Shift** key is pressed. • Move the Workspace right by rolling the middle mouse roller button up while the **Shift** key is pressed. • Zoom in on the Workspace by rolling the middle mouse roller button down while the **Ctrl** key is pressed. • Zoom out on the Workspace right by rolling the middle mouse roller button up while the **Ctrl** key is pressed.
 Workspace navigation icon	Clicking on this icon enables Workspace zoom mode. When Workspace zoom mode is enabled, you can zoom in and out, as follows: • Zoom in on the Workspace by clicking mouse button and moving the mouse to the right. • Zoom out on the Workspace right by clicking mouse button and moving the mouse to the left.

Multi-Point Designer Element	Description
🔒 / 🔓	The padlock open (🔓) and padlock closed (🔒) icons determine whether you can move or not move the position of the nodes within the **Multi-Point Designer** page, respectively. When you arrive in the **Multi-Point Designer** page, the padlock closed icon (🔒) is active by default. Clicking on the padlock icons toggles between their open and closed states. • When the padlock closed icon (🔒) is active, the node positions are locked, and cannot be moved. • When the padlock open icon (🔓) is active, the node positions are unlocked, and can be moved. To move a node, do the following: 1. While left mouse clicking on the node drag the mouse to the desired location. 2. Once the node is at the desired position let go of the left mouse button.
+ and **-** Workspace navigation icon	Clicking on the **+** icon results in zooming in within the Workspace. Clicking on the **-** icon results in zooming out within the Workspace.
🗑 Workspace navigation icon	If a background image present, and selected, the trash icon is visible. Clicking on the trash icon removes the selected background image from the Workspace.
Node icons	Each of the nodes need to be configured. Clicking on a node opens the **Edit node** panel, letting you configure all aspects of the node. For more information, see *Editing a Node via the Edit Node Panel (Multi-Point Networks)* on page 319.
Links	An initially created network contains non-configured links, with a default name **Node0<-->Node1**, **Node0<-->Node2**, **Node1<-->Node2**, etc. Typically, each link must be configured with a link type, link subtype and link quality. If a link is not configured, it acts as a no impedance link. Clicking on a link opens the link opens the **Link** page (see *The Link Settings Page (Multi-Point Networks)* on page 324) from where you can configure the basic settings, link qualifications, and advanced settings (impairments). **Note:** It is normal and advisable, although not compulsory, to configure the links in number order. You can add new links according to the steps described in *Creating Links Between Nodes in the Workspace* on page 317. Once a new link is added, typically it must be configured with a link type, link subtype and link quality. If a newly added link is not configured, it acts as a no impedance link. Clicking on a newly added link opens the link opens the **Link** page (see *The Link Settings Page (Multi-Point Networks)* on page 324) from where you can configure the basic settings, link qualifications, and advanced settings (impairments).

3-2-1. The Workspace Background Image

The Workspace in the **Multi-Point Designer** page can contain a background image. A background image can be useful in helping you visualize your Multi-Point network in the real world. You can use background images to represent the entire world, a continent, a country, a region, or an office layout for example. The NE-ONE comes with some build in background images. However, you can add additional background images for use with the **Multi-Point Designer** page by uploading them using the File Browser. For more information, see *Customizing and Sharing Background Files* on page 587 in *Chapter 13*, *The File Browser*.

3-2-1-1. Loading a Background Image into the Workspace

Use the following steps to load a background image into the Workspace of the **Multi-Point Designer** page:

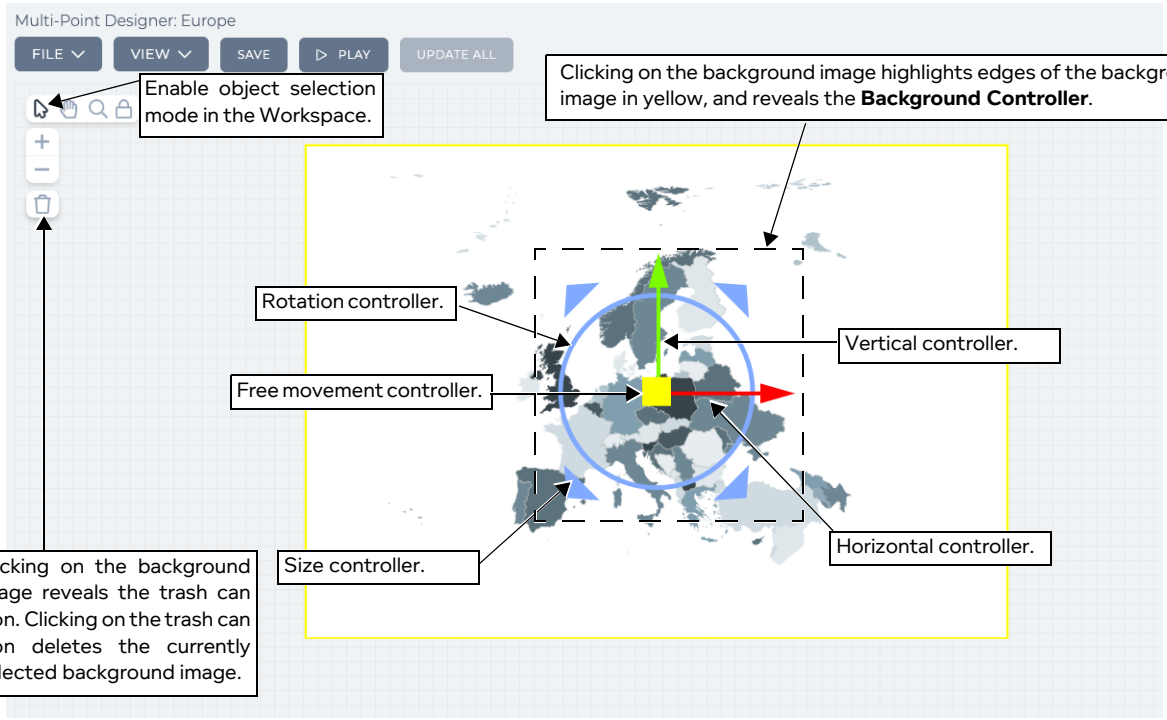
1. From the **Multi-Point Designer** page, select **VIEW** > **Background**.
   A **Select Background** dialog box appears with a list of available background images.
2. From the dialog box that appears, select the image that you want to use as a background, and click **OK**.
   The selected background image is loaded into the Workspace, and can be positioned and resized according to the steps described in *Section 3-2-1-2, Positioning, Rotating and Resizing a Background Image in the Workspace*.

3-2-1-2. Positioning, Rotating and Resizing a Background Image in the Workspace

Illustration 86 shows an example of loading a background image into the Workspace area of the **Multi-Point Designer** page.

Note:
For simplicity and clarity within *Illustration 86*, the nodes and links of a Multi-Point network are intentionally omitted.

ILLUSTRATION 86 - EXAMPLE BACKGROUND IMAGE LOADED INTO THE WORKSPACE



Use the following steps to position, rotate, and resize a background image with the Workspace:

1. To position, rotate, and resize a background image, you must be in object selection mode. To be in object selection mode, click the object selection Workspace navigation icon .
2. Once in object selection mode, click on the background image to show the Background Controller. The Background Controller has the following control functions:
   - **Free movement controller** : yellow box - clicking on this lets you move the background image freely in all directions.
   - **Horizontal controller** : red horizontal control arrow - clicking on this lets you move the

background image in only the horizontal direction

- **Vertical controller** : green vertical control icons arrow - clicking on this lets you move the background image in only the vertical direction.
- **Rotation controller** : white circle - clicking on this lets you rotate the background image around its center point.
- **Size controllers** : horizontal and vertical control triangles (in each corner) - clicking on these triangles lets you change the size of the background.

3. Change the background position, size, and orientation, according to your needs as follows:
   - To freely move the background image, click on the **Free movement controller** (the mouse pointer changes to a hand), and drag the mouse in the direction in which you want to move the background.
   - To move the background image horizontally, click on the **Horizontal controller** (the mouse pointer changes to a hand), and drag the mouse in the direction (i.e. left or right) in which you want to move the background.
   - To move the background image vertically, click on the **Vertical controller** (the mouse pointer changes to a hand), and drag the mouse in the direction (i.e. up or down) in which you want to move the background.
   - To rotate the background image on its center point, click on the **Rotation controller** (the mouse pointer changes to a hand), and drag the mouse in the direction (i.e. up for clockwise or down for anti-clockwise) in which you want to rotate the background.
   - To resize the background image, click on one of the four the **Size controllers** (the mouse pointer changes to a diagonal double sided arrow), and drag the mouse in the an appropriate direction to increase or decrease the background image size.

     Moving the mouse towards the top, right of the background image results in increasing the size of the background image.

     Moving the mouse towards the bottom, left of the background image results in decreasing the size of the background image.

Note:

When the background image is selected, the trash can icon is visible. Clicking on the trash can icon removes the selected background image from the Workspace.

4. Once you have finished, click outside the background image.

   The Background Controller closes.

3-2-2. Creating Links Between Nodes in the Workspace

If you initially created the Multi-Point network from either the Fully Meshed, Hub and Spoke, or Cloud topology template on the **Network Wizard** page (see *Illustration 84*), the Workspace on the **Multi-Point Designer** page will already contain the nodes with one link between each of the nodes based on those network topology templates.

If you initially created the Multi-Point network from the Free Form topology template on the **Network Wizard** page (see *Illustration 84*), the Workspace on the **Multi-Point Designer** page will be blank, letting you flexibly create a free form network topology of your desire.

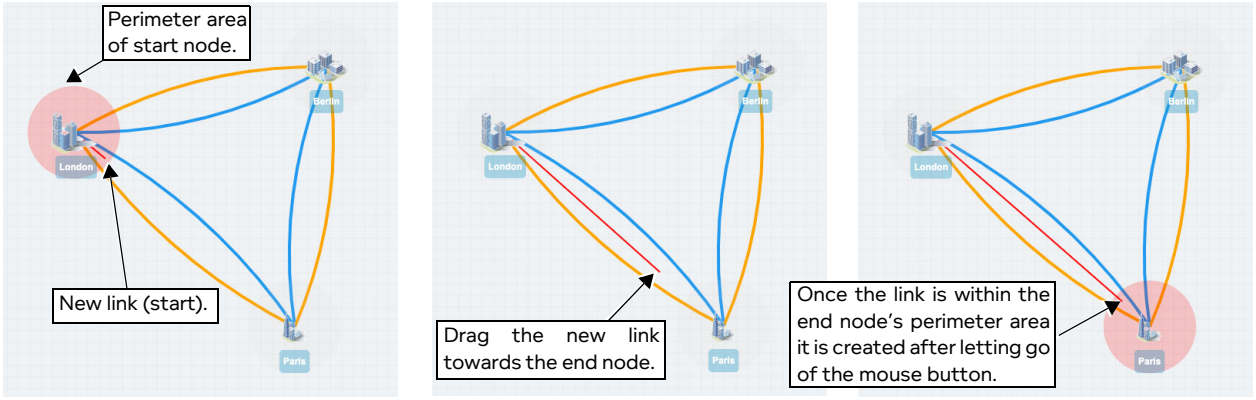
The Workspace lets you quickly and easily create additional links between two nodes (if they exist on the Workspace) within your Multi-Point network.

Note:
In order to be able to create a link, at least two nodes need to be present on the Workspace.

Note:
The Basic and Advanced link settings of the Web Interface (*Illustration 91* on page 325 and *Illustration 92* on page 328) uses the concept of Left node and Right node for traffic direction on a link. When creating a link, the first node that you choose is considered to be the Left node. Therefore, when creating multiple links between the same two nodes, it is recommended that you make them in the same direction (i.e. choose the same node for the start point of the link).

Use the following steps for each additional link that you want to create between two nodes:

1. On the start node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).
   A red line representing the new link appears within the perimeter area of the start node.



2. Continue dragging the link into the perimeter area of the end node (considered the right node).
3. Once the end of the link is in the perimeter area of the end node, let go of the mouse button.
   A **Link Name** dialog box appears.
4. From the **Link Name** dialog box that appears, type an appropriate name for the link, then click **OK**.
   The new link is created, and initially colored blue. The new link is now ready for editing via the **Edit link** panel so that its link parameters can be configured. For more information, see *The Link Settings Page (Multi-Point Networks)* on page 324.
   In the example shown in the steps above, the Left node is London and the Right node is Paris. This is because London was chosen as the start node for the start of the link, and not because it is positioned to the left of the Paris node.

3-2-3. Creating Nodes in the Workspace

If you initially created the Multi-Point network from either the Fully Meshed, Hub and Spoke, or Cloud topology template on the **Network Wizard** page (see *Illustration 84*), the Workspace on the **Multi-Point Designer** page will already contain the nodes with one link between each of the nodes based on those network topology templates.

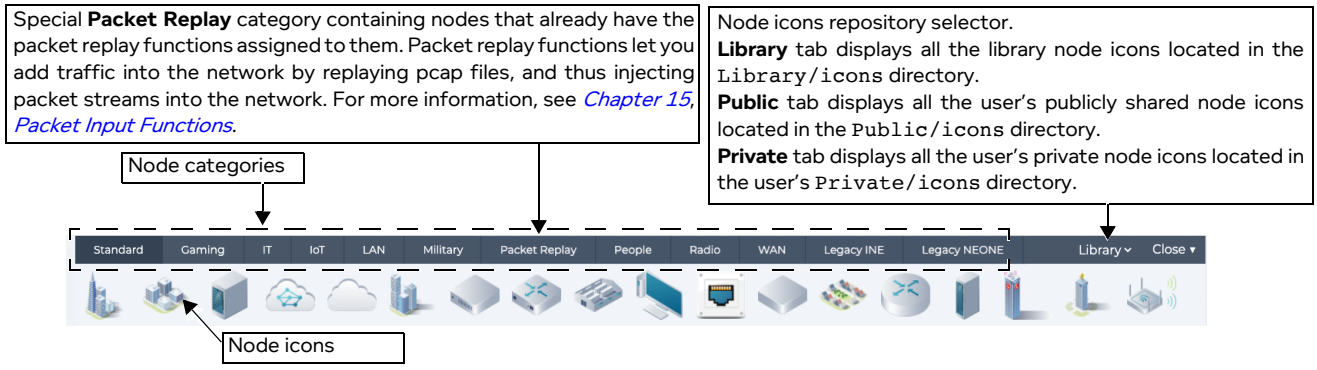
If you initially created the Multi-Point network from the Free Form topology template on the **Network Wizard** page (see *Illustration 84*), the Workspace on the **Multi-Point Designer** page will be blank, letting you flexibly create a free form network topology of your desire.

The Workspace lets you quickly and easily create additional nodes to your Multi-Point network. You may want to create additional nodes in the Workspace in the following cases:

- When you want to modify the original node topology provided by the Fully Meshed, Hub and Spoke, or Cloud topology template.
- When you start with an empty Workspace after initially selecting the Free Form node topology on the **Multi-Point Designer** page.
- When you want to modify an existing node topology of an existing network based on the Free Form node topology template.

The **Node Icons** panel (see *Illustration 87*) located at the bottom of the **Multi-Point Designer** page provides a convenient area from where you can simply select a node from an appropriate category, and drag it to the Workspace in order to create a new node. The NE-ONE comes with some built in node icons within. However, you can add additional node icons for use with the **Multi-Point Designer** page by uploading them using the File Browser. For more information, see *Customizing and Sharing Node Icon Files* on page 587 in *Chapter 13*, *The File Browser*.

ILLUSTRATION 87 - THE NODE ICONS PANEL



Note:

If you have the Defense Pack premium feature, the **Node Icons** panel will contain an additional Defense category.

Use the following steps for each additional node that you want to create in your Multi-Point network:

1. In the **Node Icons** panel, select the appropriate node category tab.
2. Click on the desired node icon, and while holding down the mouse button drag the node icon into the desired location on the Workspace.

   The newly created node appears in the Workspace and is ready for the following configuration actions:

   - Creation of links between other nodes (see *Creating Links Between Nodes in the Workspace* on page 317).
   - Configuration of the node (see *Editing a Node via the Edit Node Panel (Multi-Point Networks)* on page 319).

Note:

A special **Packet Replay** category exists, containing nodes that already have the packet replay functions assigned to them. Packet replay functions let you add congestion into the network by replaying pcap files, and thus injecting packet streams into the network. For more information, see *Chapter 15*, *Packet Input Functions*.

3-2-4. Editing a Node via the Edit Node Panel (Multi-Point Networks)

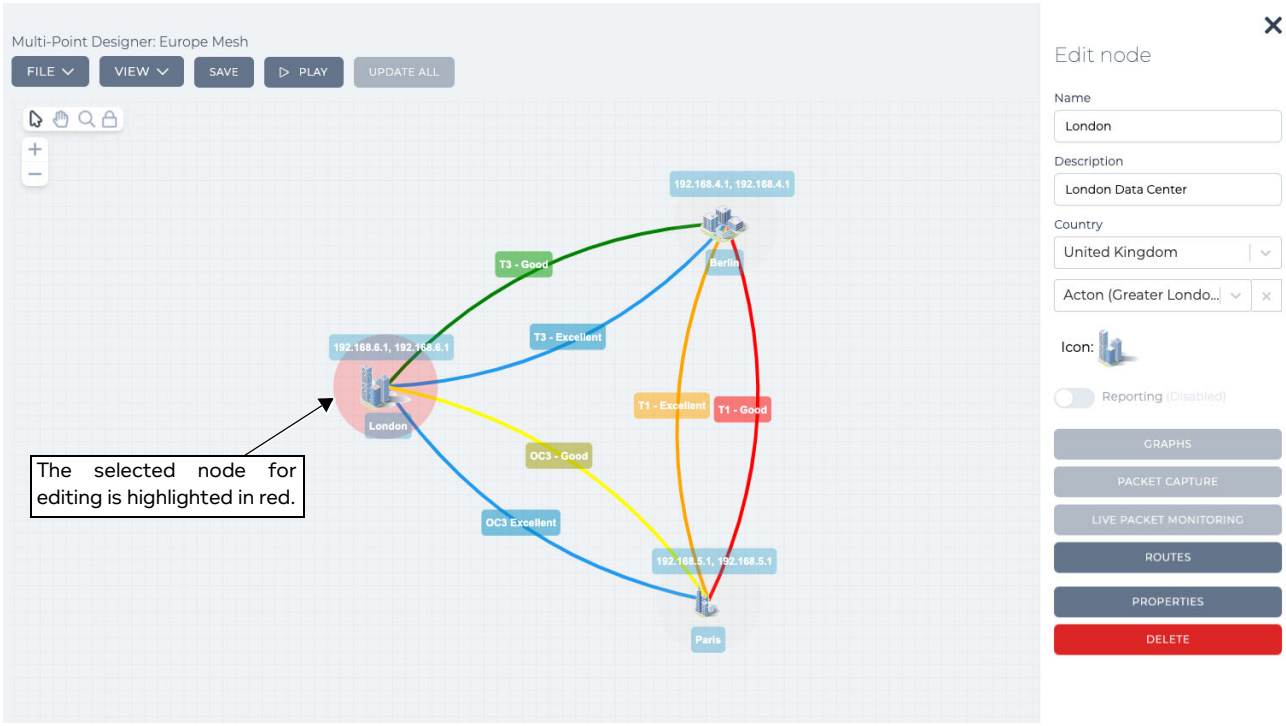
Upon clicking a node within the Workspace, the node becomes highlighted by a red circle, and the right hand side of the **Multi-Point Designer** page updates with an **Edit node** panel (*Illustration 88*), letting you configure all aspects of that node.

Note:

Any changes (e.g. node name) made in the **Edit node** panel are immediately reflected in the **Multi-Point Designer** page, but not committed to the NE-ONE. To commit any node changes to the NE-ONE, either click the **SAVE** button or select **FILE > Save**.

The **Edit node** panel remains visible until clicking its ✕ icon. On clicking the ✕ icon the **Edit node** minimizes so that the **Multi-Point Designer** page is fully visible.

ILLUSTRATION 88 - EXAMPLE EDIT NODE PANEL FOR A MULTI-POINT TYPE NETWORK



The **Edit node** panel contains the elements summarized in *Table 45* on page 320.

Note:

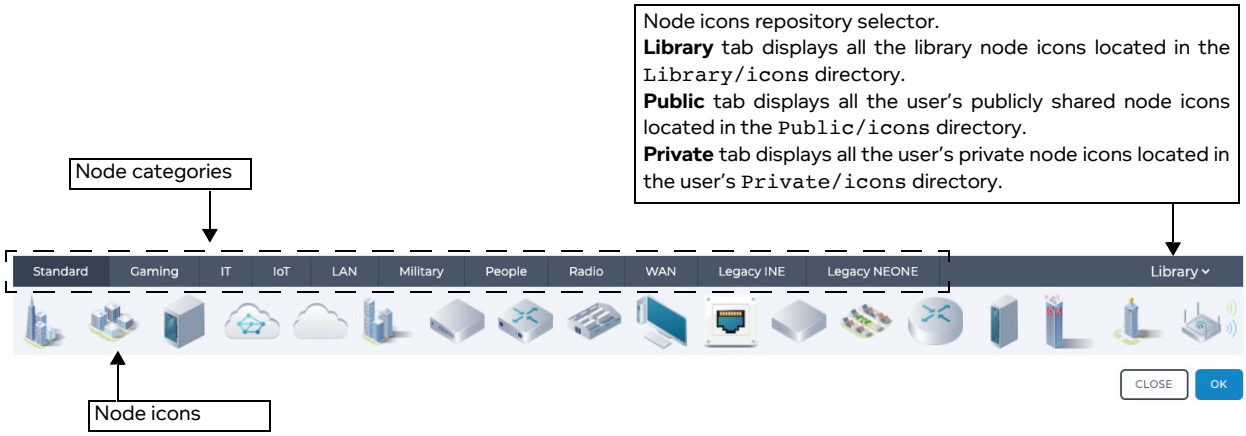
The **Edit node** panel for a node from the **Packet Replay** category is different to that of the regular node category types (see *Illustration 201* on page 630), and intentionally only contains the **PROPERTIES** and **DELETE** buttons. For more information about using dedicated packet replay nodes, see *Chapter 15*, *Packet Input Functions*.

TABLE 45 - EDIT NODE PANEL ELEMENTS FOR MULTI-POINT NETWORKS

Edit node element	Description
Name field	Defines the name of the node that appears next to the node's icon in the **Multi-Point Designer** page, and can contain alphanumeric characters, special characters, and spaces.
Description field	Defines the description of the node, and can contain alphanumeric characters, special characters, and spaces. The description appears in the mouse over for the node in the **Multi-Point Designer** page.
Country drop-down field	Defines the country location of the node. Clicking on this drop-down field reveals a list of countries. **Note:** You can also type the name of the country to select it quickly from the list of countries.
Location drop-down field	Defines the location within the country of the node. Clicking on this drop-down field reveals a list of towns and cities associated with the selected country. **Note:** You can start typing the location in order to select it quickly from the list of locations.
Icon graphic	Defines and shows the icon that represents the node. Clicking on this icon opens a dialog box (*Illustration 89*) containing a list of Library icons, Public icons, and Private icons. From this dialog box you can select a new icon to represent the node, and click **OK** to confirm the icon selection. • The Library node icons are standard icons delivered with the NE-ONE, and are located in the `Library/icons` directory. • The Private node icons are custom icons specific to the currently logged in user, and are located in the `Private/icons` directory. A new NE-ONE does not contain any Private node icons. You can use the File Browser to upload custom `*.png` files to your `Private/icons` directory. • The Public node icons are custom icons shared between all users, and are located in the `Public/icons` directory. A new NE-ONE does not contain any Public node icons. You can use the File Browser to upload custom `*.png` files to the publicly accessible `Public/icons` directory. For more information about upload uploading custom `*.png` files, see *Customizing and Sharing Node Icon Files* on page 587 in *Chapter 13*, *The File Browser*.
Reporting switch	By default, Application reporting is disabled for a node. When the network is not running (i.e. when the network is stopped, and being created or edited) this switch is grayed out. Clicking on this switch toggles between enabling and disabling Application reporting on the node. For more information, see *Viewing and Downloading Application Reports* on page 575 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*. **Note:** Applications reporting is a premium reporting feature. If you do not have the premium Applications reporting feature, the associated **Reporting** switch is not present.

Edit node element	Description
GRAPHS button	When the network is not running (i.e. when the network is stopped, and being created or edited) this button is grayed out. When a network is running, this button is enabled. Clicking this button opens a **Select data to monitor** dialog box (*Illustration 161* on page 534), from where you can select which type of data to graph for the node. Once you select which type of data to graph, the graph opens in a separate web browser tab. For more information, see *Launching Live Graphs on a PPO From an Active Network* on page 550, in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*. **Note:** you can also view all network objects (ports/nodes) and launch graphs for a selected network object (port/node) from within the **Statistics** page. For more information, see *Launching Graphs for a PPO within the Statistics page* on page 552, in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
PACKET CAPTURE button	When the network is not running (i.e. when the network is stopped, and being created or edited) this button is grayed out. When a network is running, this button is enabled. Clicking this button opens a **Packet Capture** dialog box (see *Illustration 161* on page 534), from where you can choose what packets to capture (before impairment, after impairment, or all) specific to that node. **Note:** you can also view all network objects (ports/nodes) and launch packet capture for a selected network object (port/node) from within the **Statistics** page. For more information, see *Launching Packet Capture on a PPO* on page 532 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
LIVE PACKET MONITORING button	Clicking this button opens a **Live Packets** dialog box (see *Illustration 163* on page 542), from where you can view the live packet monitoring data specific to that node. For more information, see *Launching Live Packet Monitoring on a PPO* on page 540 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
ROUTES button	Clicking this button opens a **Node Routes** window (*Illustration 95* on page 335), letting you define all the routing properties of the node. For more information, see *Editing the Properties of a Node via the Node Properties Window (Multi-Point Networks)* on page 345.
PROPERTIES button	Clicking this button opens a **Node Properties** window (*Illustration 98* on page 345), letting you define all the properties (routing, advanced routing, and cloud routing) of the node. For more information, see *Editing the Properties of a Node via the Node Properties Window (Multi-Point Networks)* on page 345.
DELETE button	Clicking this button invokes a **Confirm delete** dialog box, which upon confirming (clicking **OK**) immediately deletes the node from the network, and returns you to the **Multi-Point Designer** page. **Note:** Clicking outside the **Confirm delete** dialog box cancels the delete operation, and returns you to the **Multi-Point Designer** page.

ILLUSTRATION 89 - THE NODE ICON DIALOG BOX



Note:

If you have the Defense Pack premium feature, the **Node Icons** panel will contain an additional Defense category.

3-2-5. Editing a Link via the Edit Link Panel (Multi-Point Networks)

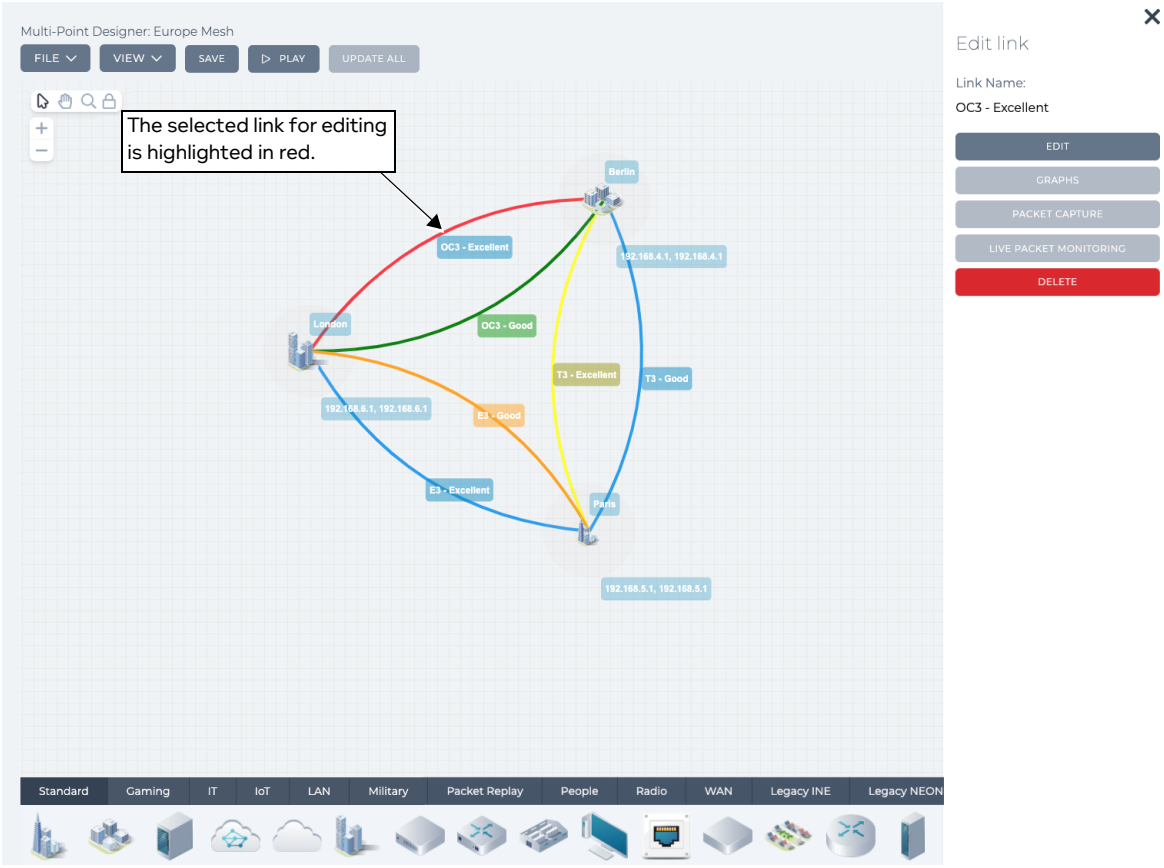
Upon clicking a link, the selected link becomes highlighted in red, and the right hand side of the **Multi-Point Designer** page updates with an **Edit link** panel (*Illustration 90*), letting you configure all aspects of that link.

Note:

Any changes (e.g. link name) made in the **Edit link** panel are immediately reflected in the **Multi-Point Designer** page, but not committed to the NE-ONE. To commit any node changes to the NE-ONE, either click the **SAVE** button or select **FILE > Save**.

The **Edit link** panel remains visible until clicking its ✕ icon. On clicking the ✕ icon the **Edit link** minimizes so that the **Multi-Point Designer** page is fully visible.

ILLUSTRATION 90 - EXAMPLE EDIT LINK PANEL FOR A MULTI-POINT TYPE NETWORK



The **Edit link** panel contains the elements summarized in *Table 45*.

TABLE 46 - LINK NODE PANEL ELEMENTS FOR MULTI-POINT NETWORKS

Edit node element	Description
Name field	Show the name of the link that appears next to the link in the **Multi-Point Designer** page. **Note:** This field is not editable. The link name is defined in the **Link Settings** page after clicking the **EDIT** button.
EDIT button	Opens a **Link** page, letting you edit all aspects (i.e. link type, link quality, and impairment functions) of the link. For more information, see *The Link Settings Page (Multi-Point Networks)* on page 324.
GRAPHS button	When the network is not running (i.e. when the network is stopped, and being created or edited) this button is grayed out. When a network is running, this button is enabled. Clicking this button opens a **Select data to monitor** dialog box (*Illustration 161* on page 534), from where you can select which type of data to graph for the link. Once you select which type of data to graph, the graph opens in a separate web browser tab. For more information, see *Launching Live Graphs on a PPO From an Active Network* on page 550 in *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing*. **Note:** you can also view all network objects (ports/nodes) and launch graphs for a selected network object (port/node) from within the **Statistics** page. For more information, see *Launching Graphs for a PPO within the Statistics page* on page 552, in *Chapter 12, Statistics, Graphing, Reporting and Packet Capturing*.

Edit node element	Description
PACKET CAPTURE button	Clicking this button opens a **Packet Capture** dialog box (see *Illustration 161* on page 534), from where you can choose what packets to capture (before impairment, after impairment, or all) specific to that link. **Note:** you can also view all network objects (ports/nodes) and launch packet capture for a selected network object (port/node) from within the **Statistics** page. For more information, see *Launching Packet Capture on a PPO* on page 532, in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
LIVE PACKET MONITORING button	When the network is not running (i.e. when the network is stopped, and being created or edited) this menu item is grayed out. When a network is running, this menu item is enabled. Selecting this menu item opens a **Live Packet Monitoring** dialog box (see *Illustration 162* on page 542), from where you can choose which traffic direction to launch the live packet monitoring process on, specific to that link. For more information, see *Launching Packet Capture on a PPO* on page 532 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.
DELETE LINK button	Clicking this button invokes a **Confirm delete** dialog box, which upon confirming (clicking **OK**) immediately deletes the link from the network, and returns you to the **Multi-Point Designer** page. **Note:** Clicking outside the **Confirm delete** dialog box cancels the delete operation, and returns you to the **Multi-Point Designer** page.

3-2-6. The Link Settings Page (Multi-Point Networks)

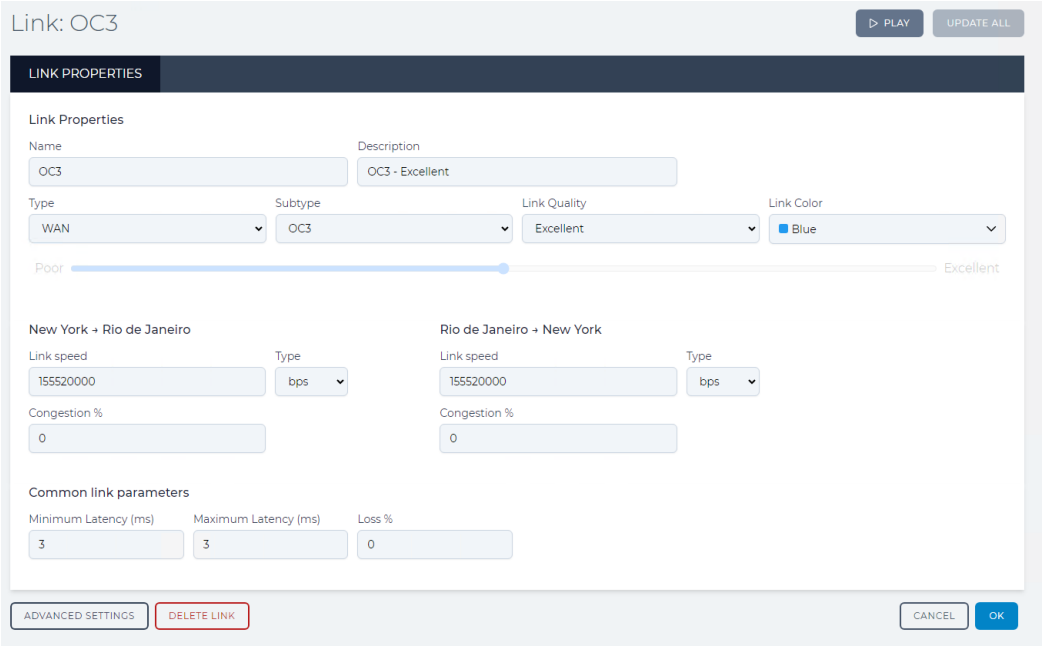
Clicking on a link from within the **Multi-Point Designer** page opens an **Edit link** panel for that link. Then clicking on the **EDIT** button in the **Edit link** panel opens the **Link** page for that link with the **LINK PROPERTIES** tab enabled (*Illustration 91*). The **Link** page contains the following areas, letting you configure all aspects for the selected link:

- Basic Settings : Link Properties, which is accessed by clicking on the **LINK QUALIFICATIONS** tab (see *The (Basic Settings) Link Properties page (Multi-Point Networks)* on page 324).
- Advanced Settings, which is accessed by clicking on the **ADVANCED SETUP** button (see *The Advanced Link Settings Page (Multi-Point Networks)* on page 327).

3-2-6-1. The (Basic Settings) Link Properties page (Multi-Point Networks)

The **LINK PROPERTIES** tab in the **Link** page (*Illustration 91*) lets you configure all the basic properties of the link. Typically the basic properties of a link need to be configured in order for the link to be run by the network. If the basic properties of a link are not configured, the link acts a a zero impedance link.

ILLUSTRATION 91 - EXAMPLE LINK PROPERTIES PAGE (MULTI-POINT NETWORKS)



The **Link** page contains the elements summarized in *Table 47*.

Note:

Compared with Point-to-Point type networks, the **Link** page does not contain a **LINK QUALIFICATIONS** tab. This is normal as link qualifications are a form of basic routing, which is specific to Point-to-Point type networks. For Multi-Point type networks, complex routing functions are available. For more information on complex routing functions, see *Editing the Routing of a Node via the Node Routing Window (Multi-Point Networks)* on page 335.

TABLE 47 - LINK PROPERTIES PAGE ELEMENTS FOR MULTI-POINT NETWORKS

Link page element	Description
Name field	Defines the name of the link that appears next to the link in the **Multi-Point Designer** page, and can contain alphanumeric characters, special characters, and spaces.
Description field	Defines the description of the link, and can contain alphanumeric characters, special characters, and spaces. The description appears in the mouse over for the link in the **Multi-Point Designer** page.
Type drop-down field	Defines the link type. The link types available are summarized in *Appendix 3, Available Link Types and Link Sub-Types* on page 765.
Subtype drop-down field	Initially grayed out until the link type is selected from the **Type** drop-down field. The subtypes that are available depend on the link type that was selected from the **Type** drop-down field. The subtypes available for each link type are summarized in *Appendix 3, Available Link Types and Link Sub-Types* on page 765.
Link Quality drop-down field	Initially grayed out until the link subtype is selected from the **Subtype** drop-down field. The link qualities that are available depend on the link subtype that was selected from the **Subtype** drop-down field. The link qualities available for each link subtype are summarized in *Appendix 3, Available Link Types and Link Sub-Types* on page 765.

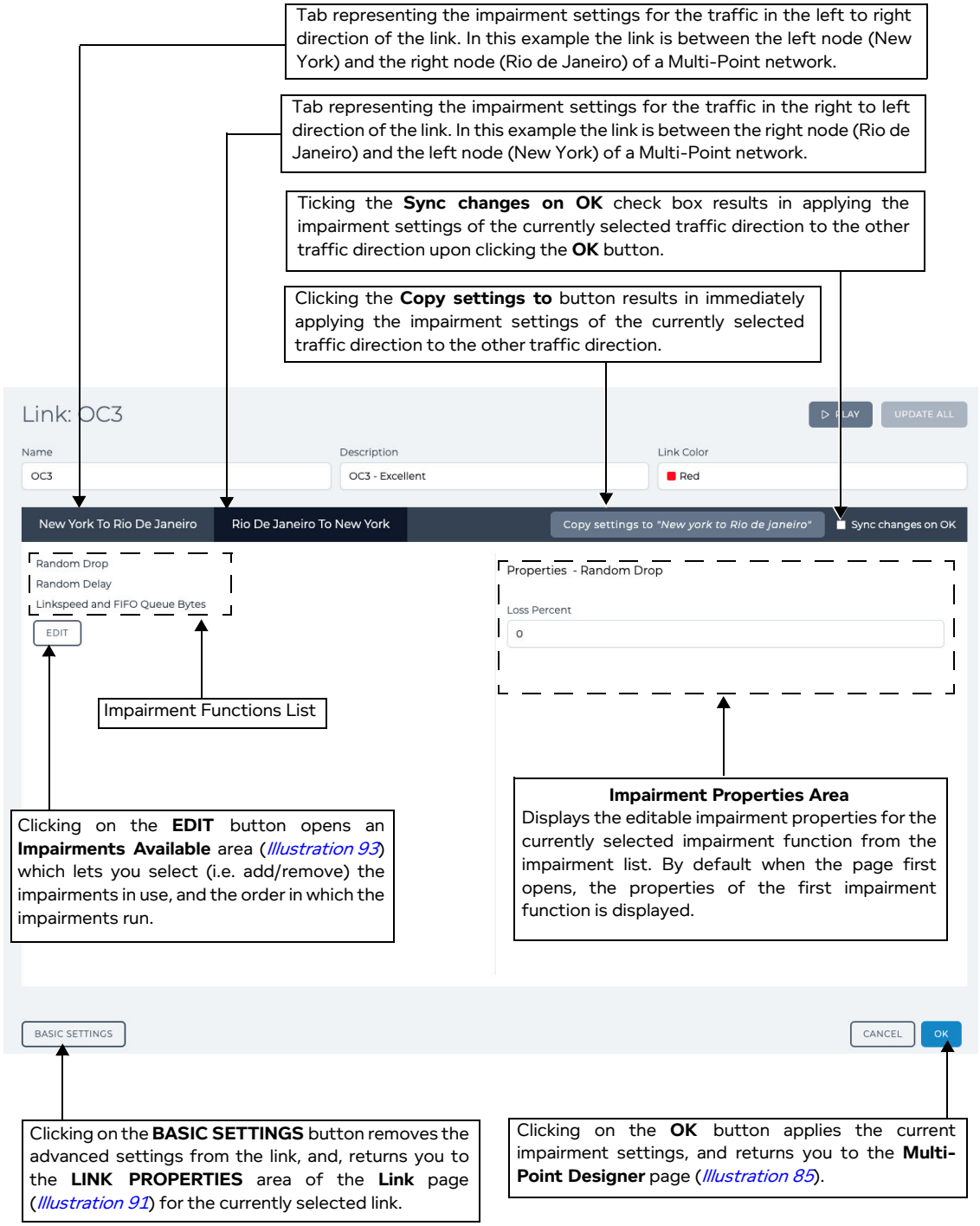
Link page element	Description
Link Color drop-down field	This defines the color of the link. The initial (default) color is blue. Clicking on this field provides a list of colors to choose from, letting you define the color of the link.
Poor to **Excellent** link quality slider	Once you define the link **Type** and **Subtype**, you can optionally use the **Poor** to **Excellent** link quality slider. When you use the **Poor** to **Excellent** link quality slider the **Link Quality** becomes custom and the **Common link parameters** (**Minimum Latencey (ms)**, **Maximum Latency (ms)**, and **Loss %**) automatically change according to the positioning of the slider.
Right Port to Left Port (initially the same values as Left Port to Right Port direction)	
Link Speed field	This field is initially empty, and automatically updates to a recommended link speed value once the link type, link subtype and link quality have been selected. If required, you can modify this to a different link speed. **Note:** For certain network links it is common to have different Link Speed values in the uplink and downlink directions. The NE-ONE defaults to symmetric values, which may need to be changed manually.
Type drop-down field	Lets you select a different unit so that the **Link Speed** field reformats the value for the selected unit.
Congestion % field	Defines the congestion on the link in percent (the higher the value, the higher the level of congestion). Congestion is usually a temporary state that occurs when the link cannot handle the traffic going through it. This field is initially empty implying no congestion (0% congestion). Because congestion is considered a temporary state, this field intentionally remains empty (0% congestion) once the link type, link subtype and link quality have been selected. If required, you can define a congestion percentage value so that congestion persists on the link.
Left Port to Right Port (initially the same values as Right Port to Left Port direction)	
Link Speed field	This field is initially empty, and automatically updates to a recommended link speed value once the link type, link subtype and link quality have been selected. If required, you can modify this to a different link speed. **Note:** For certain network links it is common to have different Link Speed values in the uplink and downlink directions. The NE-ONE defaults to symmetric values, which may need to be changed manually.
Type drop-down field	Lets you select a different unit so that the **Link Speed** field reformats the value for the selected unit.
Congestion % field	Defines the congestion on the link in percent (the higher the value, the higher the level of congestion). Congestion is usually a temporary state that occurs when the link cannot handle the traffic going through it. This field is initially empty implying no congestion (0% congestion). Because congestion is considered a temporary state, this field intentionally remains empty (0% congestion) once the link type, link subtype and link quality have been selected. If required, you can define a congestion percentage value so that congestion persists on the link.
Common Link Parameters (parameters that persist across the link equally for each port)	

Link page element	Description
Minimum Latency field	Defines the minimum latency in ms that is applied on the link. This field is initially empty, and automatically updates to a recommended minimum latency value once the link type, link subtype and link quality have been selected. If required, you can modify this to a different minimum latency value.
Maximum Latency field	Defines the maximum latency in ms that is applied on the link. This field is initially empty, and automatically updates to a recommended maximum latency value once the link type, link subtype and link quality have been selected. If required, you can modify this to a different maximum latency value.
Congestion % field	Defines the congestion on the link in percent (the higher the value, the higher the level of congestion). Congestion is usually a temporary state that occurs when the link cannot handle the traffic going through it. This field is initially empty implying no congestion (0% congestion). Because congestion is considered a temporary state, this field intentionally remains empty (0% congestion) once the link type, link subtype and link quality have been selected. If required, you can define a congestion percentage value so that congestion persists on the link.
ADVANCED SETTINGS button	Clicking this button opens the **Advanced Settings** page for the link, from where you can customize (i.e. add, remove, and order) the impairments that are applied on the link. For more information, see *The Advanced Link Settings Page (Multi-Point Networks)* on page 327.
DELETE LINK button	Clicking this button invokes a **Confirm delete** dialog box, which upon confirming (clicking **OK**) immediately deletes the link from the network, and returns you to the **Multi-Point Designer** page. **Note:** Clicking outside the **Confirm delete** dialog box cancels the delete operation, and returns you to the **Multi-Point Designer** page.

3-2-6-2. The Advanced Link Settings Page (Multi-Point Networks)

Whilst the basic link settings are extremely intuitive and quick to use, there are also advanced link settings for the more experienced user that wants to setup more sophisticated network impairment configurations. The **Advanced Settings** area (*Illustration 92*) of the **Link** page lets you configure the impairments that are applied to the traffic on a link.

ILLUSTRATION 92 - ADVANCED SETTINGS AREA OF THE LINK PAGE (MULTI-POINT NETWORKS)



The **Advanced Settings** area of the **Link** page contains the elements summarized in *Table 48*.

TABLE 48 - ADVANCED LINK SETTINGS PAGE ELEMENTS FOR MULTI-POINT NETWORKS

Advanced Settings element	Description
▷ **PLAY** button or ☐ **STOP** button	The state of this button varies according to whether or not the network is running. When the network is not running, a ▷ **PLAY** button is present, and the status icon for the network in the tray is ✎. Clicking on the ▷ **PLAY** button results in: • running the network • changing the network status icon to the play ⏵ symbol • changing the button state to ☐ **STOP** When the network is running, a ☐ **STOP** button is present, and the status icon for the network in the tray is ⏵. Clicking on the ☐ **STOP** button results in: • stopping the network • changing the network status icon to the edit ✎ symbol • changing the button state to ▷ **PLAY**
UPDATE ALL button	This button is grayed out when the network is not running. When the network is running, this button is active. When the network is running, you can edit the parameters of the network (i.e. link and node parameters). Clicking this button applies all the changed parameters on the fly to the running network.
Left to right traffic direction tab	Tab representing the impairment settings for the traffic in the left to right direction of the link. Clicking on this updates the area below with the impairment configuration (i.e. impairment function properties) for the left to right traffic direction of the link.
Right to left traffic direction tab	Tab representing the impairment settings for the traffic in the right to left direction of the link. Clicking on this updates the area below with the impairment configuration (i.e. impairment function properties) for the right to left traffic direction of the link.
Copy settings to button	Clicking this button results in immediately applying the impairment settings of the currently selected traffic direction to the other traffic direction.
Sync changes on OK check box	Ticking this check box results in applying the impairment settings of the currently selected traffic direction to the other traffic direction upon clicking the **OK** button. Unticking this check box results in not applying the impairment settings of the currently selected traffic direction to the other traffic direction upon clicking the **OK** button.
Impairment Functions List	Lists the impairment functions that currently apply to the link, and the order in which apply. Clicking on an impairment function updates the right hand side of the page with the properties of the impairment function.
Impairment Properties Area	Contains one or more fields letting you configure the currently selected impairment function.
EDIT button	Clicking this button opens an **Impairments Available** area (*Illustration 93*) which lets you add/remove the impairments in use, and the order in which the impairments run.

Advanced Settings element	Description
BASIC SETTINGS button	Clicking this button, returns you to the **LINK PROPERTIES** area of the **Link** page (*Illustration 91*) for the currently selected link and removing any advanced settings that were made for that link. **NOTICE:** clicking this button results in removing the advanced link settings, and returns the link to the basic settings using the default values of the three functions Random Drop, Random Delay and Linkspeed and FIFO Queue Bytes. The advanced settings for the link are not retained. Only click this button if you want to return the link properties back to the basic settings.
CANCEL button	Clicking this button ignores any changes you made to the current impairment settings, and returns you to the **Multi-Point Designer** page (*Illustration 85*).
OK button	Clicking on the **OK** button applies the current impairment settings, and returns you to the **Multi-Point Designer** page (*Illustration 85*).

By default, the traffic on a link initially includes the following set of impairment functions, in the following order:

- Random Drop (this is the equivalent of the **Loss %** value from the basic link settings).
- Random Delay (this is the equivalent of the **Minimum Latency (ms)** and **Maximum Latency (ms)** values from the basic link settings).
- Linkspeed and FIFO Queue Bytes (this is the equivalent of the **Link Speed** and **Congestion %** values for both link directions from the basic link settings).

Initially, when no **Type**, **Subtype** or **Link Quality** have been defined for a new link, the properties of these impairments are undefined. Once you defined the **Type**, **Subtype** or **Link Quality** for the link, the properties of these impairments are updated with recommended values.

Before defining the properties of each of the impairment functions associated with a link's traffic, you must update the list of impairment functions associated with that link according to your impairment requirements. The **Impairments Available** area (*Illustration 93*) of the **Link** page lets you define the impairment functions associated with the traffic on a link. The

Clicking on the **Edit** button in the **Advanced Settings** area of the **Link** page opens and **Impairments Available** area (*Illustration 93*), which lets you select (i.e. add/remove) and order the impairment functions that are applied on the traffic for the link.

Once you have finalized the list and order of the applied impairment functions in the **Impairments Available** area (*Illustration 93*) of the **Link** page, you must return to the **Advanced Settings** area (*Illustration 92*) of the **Link** page, and configure each of the impairment function properties.

Note:

By default, the **Sync changes on OK** check box is unticked. When the **Sync changes on OK** check box is ticked, the properties you define for each of the impairment functions in the currently selected traffic direction are applied to each of the other link traffic direction upon clicking the **OK** button.

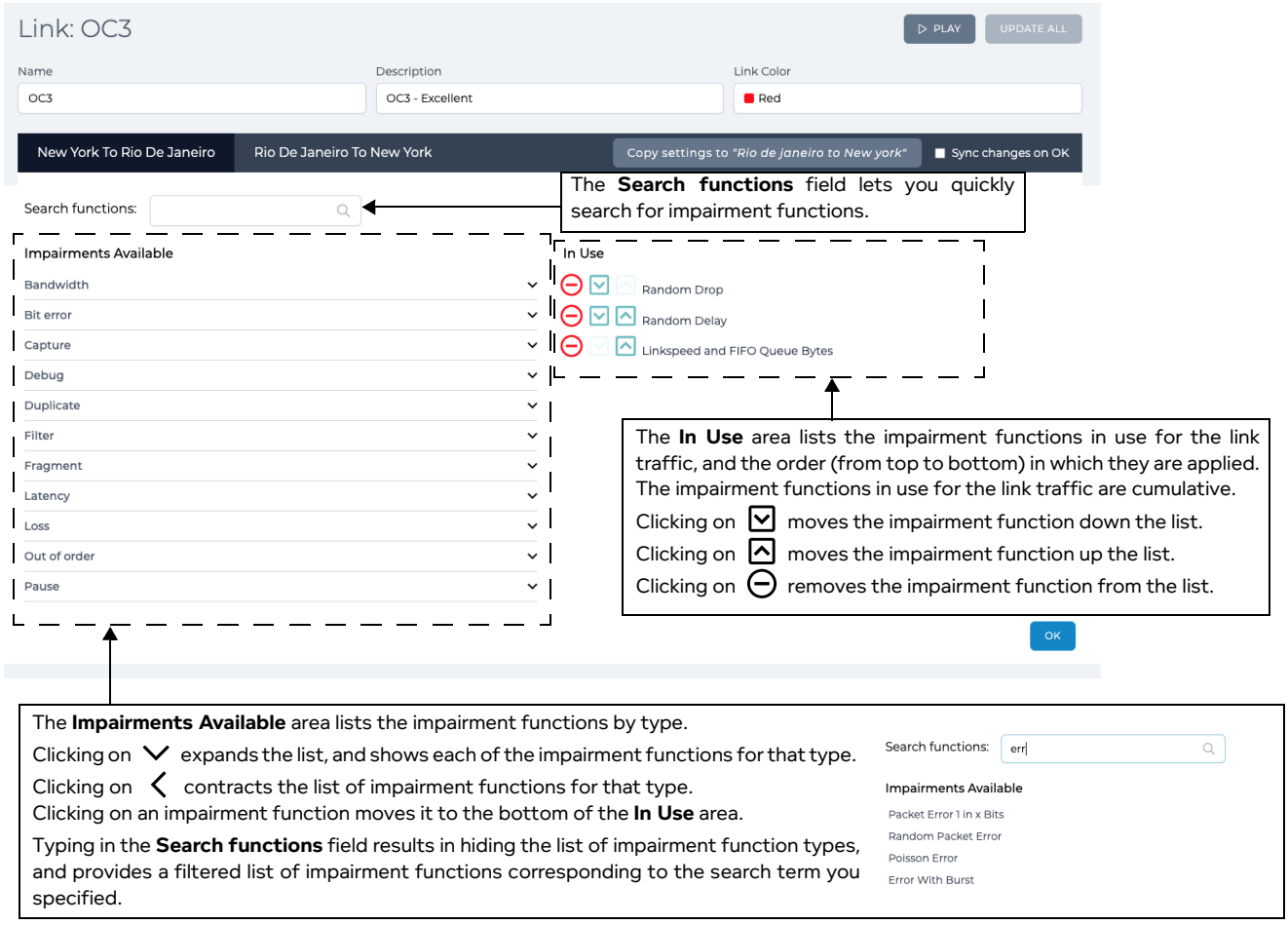
If you want to apply different impairment function properties to each traffic direction, keep the **Sync changes on OK** check box unticked, then select the appropriate traffic link tab (left to right or right to left) and configure each of the impairment function properties in the **Advanced Settings** area (*Illustration 92*) of the **Link** page.

Similarly, if you want to define and order a different list of impairments to each traffic direction, keep the **Sync changes on OK** check box unticked, then select the appropriate traffic link tab (left to right or right to left) and then select (i.e. add/remove) and order each of the impairment functions in the **Impairments Available** area (*Illustration 93*) of the **Link** page.

Note:

As network technologies evolve, Calnex keep NE-ONE impairment functions up-to-date via software updates. For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date. An active maintenance contract lets you update the NE-ONE impairment functions when new network technologies become available.

ILLUSTRATION 93 - EXAMPLE IMPAIRMENTS AVAILABLE AREA OF THE ADVANCED PROPERTIES PAGE



The **Impairments Available** area of the **Link** page contains the elements summarized in *Table 48*.

TABLE 49 - ADVANCED LINK AVAILABLE IMPAIRMENTS SETTINGS PAGE ELEMENTS

Impairments Available Element	Description
▷ **PLAY** button or ☐ **STOP** button	The state of this button varies according to whether or not the network is running. When the network is not running, a ▷ **PLAY** button is present, and the status icon for the network in the tray is ✎. Clicking on the ▷ **PLAY** button results in: • running the network • changing the network status icon to the play ⏵ symbol • changing the button state to ☐ **STOP** When the network is running, a ☐ **STOP** button is present, and the status icon for the network in the tray is ⏵. Clicking on the ☐ **STOP** button results in: • stopping the network • changing the network status icon to the edit ✎ symbol • changing the button state to ▷ **PLAY**
UPDATE ALL button	This button is grayed out when the network is not running. When the network is running, this button is active. When the network is running, you can edit the parameters of the network (i.e. link and node parameters). Clicking this button applies all the changed parameters on the fly to the running network.
Left to right traffic direction tab	Tab representing the impairment settings for the traffic in the left to right direction of the link. Clicking on this updates the area below with the impairment configuration for the left to right traffic direction of the link.
Right to left traffic direction tab	Tab representing the impairment settings for the traffic in the right to left direction of the link. Clicking on this updates the area below with the impairment configuration for the right to left traffic direction of the link.
Copy settings to button	Clicking this button results in immediately applying the impairment settings of the currently selected traffic direction to the other traffic direction.
Sync changes on OK check box	Ticking this check box results in applying the impairment settings of the currently selected traffic direction to the other traffic direction upon clicking the **OK** button. Unticking this check box results in not applying the impairment settings of the currently selected traffic direction to the other traffic direction upon clicking the **OK** button.
Search functions field	The **Search functions** field lets you quickly search for impairment functions.
Impairments Available area	The **Impairments Available** area lists the impairment functions by type. • Clicking on ⌄ expands the list, and shows each of the impairment functions for that type. • Clicking on ‹ contracts the list of impairment functions for that type. • Clicking on an impairment function moves it to the bottom of the **In Use** area. Typing in the **Search functions** field results in hiding the list of impairment function types, and provides a filtered list of impairment functions corresponding to the search term you specified. The current list of impairment functions that are available to the NE-ONE are summarized in *Available Impairment Functions* on page 743 in *Appendix 2, Available Functions*.

Impairments Available Element	Description
In Use area	The **In Use** area lists the impairment functions in use for the link traffic, and the order (from top to bottom) in which they are applied. The impairment functions in use for the link traffic are cumulative. • Clicking on ⊡ moves the impairment function down the list. • Clicking on ⊡ moves the impairment function up the list. • Clicking on ⊖ removes the impairment function from the list.
DONE button	Clicking on the **DONE** button applies the current impairment settings, and returns you to the **Advanced Settings** area of the **Link** page (*Illustration 92*).

The work flow in *Illustration 94* summarizes the typical steps you perform when configuring the impairments that are applied to the traffic on a link.

ILLUSTRATION 94 - TYPICAL WORK FLOW OF ADVANCED LINK (IMPAIRMENTS) CONFIGURATION

Multi-Point Designer page (*Illustration 85*)

1. Click on a link in the Workspace, and from the **Edit link** panel that appears click **EDIT** to edit the link properties.

↓

Basic Link Properties page

1. Within the **LINK PROPERTIES** tab (*Illustration 91*), define all basic link properties (*Table 47*).
   Note: If you do not define the **Type**, **Subtype** or **Link Quality** for the link, the **Advanced Settings** area will auto populate the properties of each of the impairment functions with zero values. Ensure you define the **Type**, **Subtype** or **Link Quality** for the link before continuing.
2. Click **ADVANCED SETTINGS** button to configure advanced link properties (impairments).

↓

Advanced Settings area (*Illustration 92*) of **Link** page.

1. Decide if the impairment functions apply to both traffic directions.
   - If yes, leave the **Sync changes on OK** check box ticked.
   - If no, untick the **Sync changes on OK** check box.
2. Click the **EDIT** button to select and order the impairment functions from within the **Impairments Available** area (*Illustration 93*) of the **Link** page.

↓

Impairments Available area (*Illustration 93*) of the **Link** page.

1. If **Sync changes on OK** check box is ticked, select (add/remove) and order the impairment functions according to your requirements.
   If **Sync changes on OK** check box is unticked,
   - Select the tab for the left to right traffic direction, then select (add/remove) and order the impairment functions according to your requirements for the left to right traffic direction.
   - Select the tab for the right to left traffic direction, then select (add/remove) and order the impairment functions according to your requirements for the left to right traffic direction.
2. Click **OK** to return to the **Advanced Settings** area (*Illustration 92*) of **Link** page.

↓

Advanced Settings area (*Illustration 92*) of **Link** page.

1. If **Sync changes on OK** check box is ticked, for each of the impairment function in the Impairment Functions List, configure its properties in the Impairment Properties Area.
   If **Sync changes on OK** check box is unticked,
   - Select the tab for the left to right traffic direction, then for each of the impairment function in the Impairment Functions List, configure its properties in the Impairment Properties Area.
   - Select the tab for the right to left traffic direction, then for each of the impairment function in the Impairment Functions List, configure its properties in the Impairment Properties Area.
2. Click on the **OK** button to apply the current impairment settings, and return to the **Multi-Point Designer** page (*Illustration 85*).

3-2-7. Editing the Routing of a Node via the Node Routing Window (Multi-Point Networks)

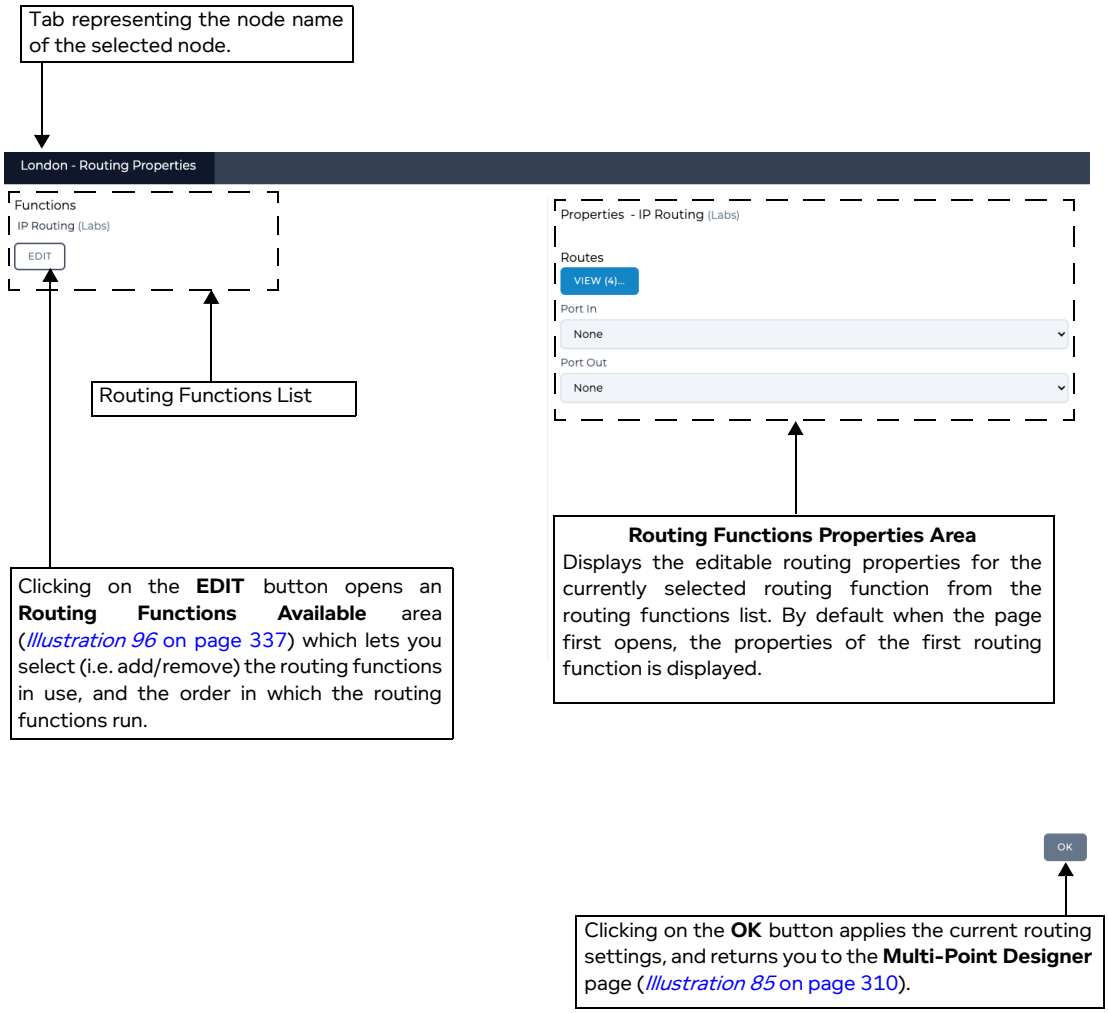
The **Routing Properties** window (*Illustration 95*) lets you define the routing properties for a node. When a new Multi-Point network is created from the **Network Wizard** page (*Illustration 84* on page 308), each of the nodes have no ports assigned to them, nor their routing configured.

In order for the Multi-Point network to run, each node within the Workspace must have its routing properties defined.

To open the **Routing Properties** window for a node, click on the node whose routing properties that you want to edit, then do the following from the **Edit node** panel that appears:

- click the **ROUTES** button
- click the **PROPERTIES** button, and from the **Node Properties** window (*Illustration 98*) that appears, click the **Routing** button

ILLUSTRATION 95 - NODE ROUTING PROPERTIES WINDOW



The routing function (and advanced function) that is initially applied to the node depends on the following (see *Table 50*):

- the network topology template type that was chosen for the Multi-Point network from the **Network Wizard** page
- the type of node (i.e. end node, hub node, cloud node)

TABLE 50 - DEFAULT ROUTING AND ADVANCED FUNCTIONS THAT ARE INITIALLY APPLIED TO A NODE

Network Topology Template Type	Node Type	Default Routing Function	Default Advanced Function
Fully Meshed	End node	IP Routing (Labs)	None
Hub and Spoke	Hub	IP Routing (Labs)	None
	End node	Composite Routing (Labs)	None
Cloud	Cloud	IP Routing (Labs)	Cloud Object (Labs)
	End node	Composite Routing (Labs)	None
Free Form	End node	IP Routing (Labs)	None

Note:
Using multiple routing functions on a node is possible, but not recommended.

The **Routing Properties** window contains the following:

- Routing Functions List area, which contains:
  - The list of routing functions that are currently applied to the node. If more than one routing function exists (this in not recommended), clicking on the routing function selects it for configuring from within the Routing Function Properties area.
  - **EDIT** button. Clicking this button invokes the **Routing Functions Available** window (*Illustration 96* on page 337) letting you add, remove, and order the routing functions that are applied on the node. For more information, see *Assigning Routing Functions to a Node* on page 337.
- Routing Function Properties area, which contains the following for the selected routing function:
  - **VIEW** button. Clicking this button opens a **Routes** window (*Illustration 97* on page 343), which lets you define the routing table for the selected routing function of the node. For more information, see *Creating and Editing a Routing Table for a Routing Function on a Node* on page 343.
  - **Port In** drop-down field, which lets you define the input port for the selected routing function of the node. To assist you with the creation of the routing table, the selected input port is also applied to the routing table (from where it can be overridden, if necessary).
  - **Port Out** drop-down field, which lets you define the output port for the selected routing function of the node. This is the out-put port of any packets that were not treated by the routing table. Typically, you leave this as the same as the input port that was defined in the **Port In** drop-down menu. The selected output port is intentionally not applied to the routing table, as the routing table inherits the link connected to the node.
- **OK** button. Clicking this button applies the current routing settings, and returns you to the **Multi-Point Designer** page (*Illustration 85* on page 310).

3-2-7-1. Assigning Routing Functions to a Node

The **Routing Functions Available** window (*Illustration 96*) lets you select (i.e. add/remove) and order the routing functions that are applied to the traffic for the node, and contains the elements summarized in *Table 51*.

Note:
Using multiple routing functions on a node is possible, but not recommended.

ILLUSTRATION 96 - ROUTING FUNCTIONS AVAILABLE AREA OF THE ROUTING PROPERTIES WINDOW

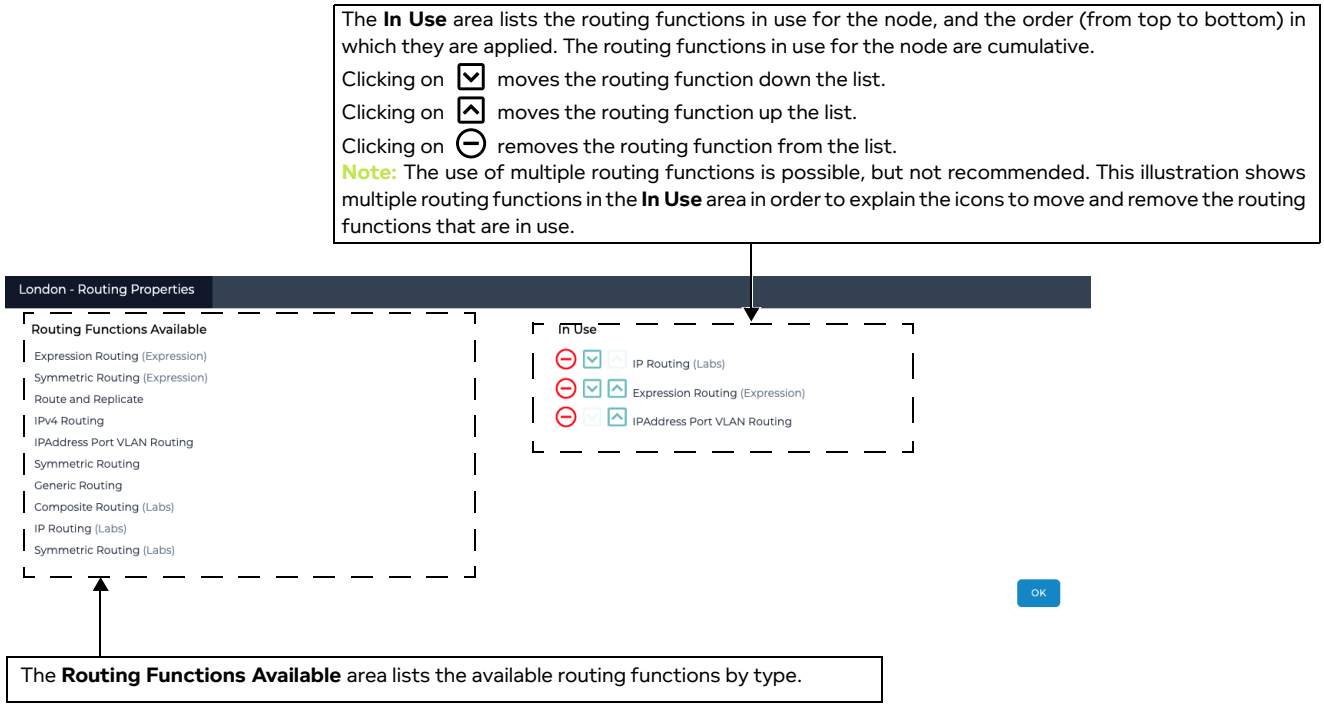


TABLE 51 - ROUTING FUNCTIONS AVAILABLE WINDOW ELEMENTS

Routing Functions Available Element	Description
Routing Functions Available area	The **Routing Functions Available** area lists the routing functions by type. • Clicking on ⌄ expands the list, and shows each of the routing functions for that type. • Clicking on ⌃ contracts the list of routing functions for that type. • Clicking on a routing function moves it to the bottom of the **In Use** area.
In Use area	The **In Use** area lists the routing functions in use for the node, and the order (from top to bottom) in which they are applied. The routing functions in use for the node are cumulative. • Clicking on ☑ moves the routing function down the list. • Clicking on ☑ moves the routing function up the list. • Clicking on ⊖ removes the routing function from the list.
OK button	Clicking on the **OK** button applies the current routing settings, and returns you to the **Routing Properties** window (*Illustration 95*).

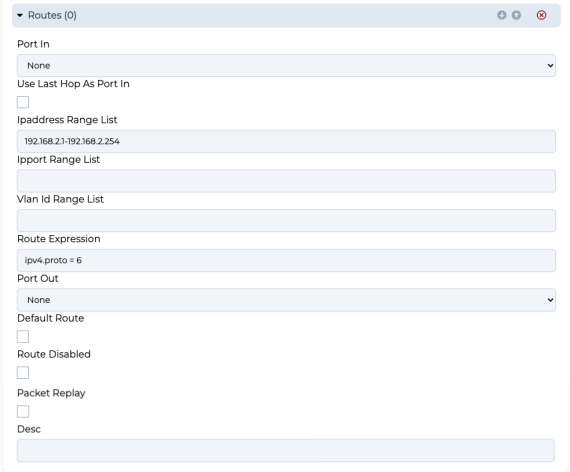
At the time of writing (i.e. the current release), the routing functions summarized in *Table 51* are available.

TABLE 52 - AVAILABLE ROUTING FUNCTIONS FOR MULTI-POINT NETWORKS

Routing Function	Description
Generic Routing	This is the fastest routing function available – it has no routing table to consider and so does not have a routes option – use this when creating very simple network structures that need to be fast.
IPAddress Port VLAN Routing	Route by a selection of packet properties: Source and/or Destination IP Addresses, Source and/or Destination TCP/UDP Ports and/or VLAN IDs. This function allows routing by lists, ranges or list of ranges of: • **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE. • **Use Last Hop as Port In** – modifies **Port In** to be the name of the immediately previous network object (i.e. link or node) or port (hardware or soft) the packet just came from. • **Source IP Address** – where the packet has come from e.g. for TCP/IP 192.168.1.1-192.168.1.255. • **Dest IP Address** - where the packet is going to e.g. 192.168.2.10 • **Source Port** – which port the packet has come from e.g. for TCP/IP 6000, 6001. • **Dest Port** – which port the packet is going to e.g. 80 (HTTP), 443 (HTTPS), 25 (smtp), 21 (ftp), 110 (pop3), 445 (Microsoft-ds – Network File Access). • **VLAN Id** – 802.1Q VLAN label (tag), if the packet is VLAN tagged. • **Port Out** – A network object (i.e. link or node) or a port (hardware or soft) to which the traffic will be routed if it matches this rule. • **Default Route** – Tick (check) to specify that this route is the default for all traffic not otherwise matching a route. Only the first route marked default will be used as the default. • **Route Disabled** - If ticked (checked) then this route is disabled i.e. not in use.
IPv4 Routing	Route specifying Network Address and Network Mask – a conventional routing approach. This function allows routing by lists, ranges or list of ranges of: • **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE. • **Network Address** – Any IPv4 address in the subnet that is being Routed e.g. 192.168.1.1 and 192.168.1.254 are equivalent is network mask (below) is set to 255.255.255.0. For clarity it's often good (but not required) to use the network base address e.g. 192.168.1.0. • **Network Mask** – The network mask to use with the Network Address above e.g. 255.255.255.0 for a standard "class c" style network. As usual, the mask is "ANDed" with both the Network Address specified above and the Destination IP Address in the network packet. If the results of these ANDing processes match then the packet is deemed to match the network and therefore match the routing rule. • **Port Out** – A network object (i.e. link or node) or a port (hardware or soft) to which the Traffic will be Routed if it matches this rule. • **Route Disabled** - If ticked (checked) then this Route is disabled i.e. not in use.

Routing Function	Description
Symmetric Routing	Specify IP Address, TCP/UDP Port and VLAN Id as text strings of lists and ranges. The IP addresses and TCP/UDP ports can apply to either the source or the destination for ease of use. Care must be taken when using symmetric routing not to create routing loops (by always specifying the **Port In** field in the routing rules). This function has the following fields: • **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE. • **Use Last Hop as Port In** – modifies **Port In** to be the name of the immediately previous network object (i.e. link or node) or port (hardware or soft) the packet just came from. • **IP Address Range List** – a list of individual IPv4 addresses or ranges of IP addresses, which will be matched against the packet's Source IP Address or Destination IP address e.g. a Range List would be like: 192.168.1.1- 192.168.1.255,192.168.5.34,8.8.8.8. • **IPPort Range List** – a list of individual TCP/UDP Ports or ranges of Ports, which will be matched against the Packet's Source Port or Destination Port e.g. source ports similar to 6000, 6001 or destination ports e.g. 80 (HTTP), 443 (HTTPS), 25 (smtp), 21 (ftp), 110 (pop3), 445 (Microsoft-ds – Network File Access). The port Range List is specified like this: 6000-7000,80,8080-8082 • **VLANId Range List** – 802.1Q VLAN label (tag), if the packet is VLAN tagged. The VLANId range list is specified as follows: 600-630,701,705-709. • **Port Out** – A network object (i.e. link or node) or a port (hardware or soft) to which the Traffic will be Routed if it matches this rule • **Default Route** – Tick (check) to specify that this Route is the default for all traffic not otherwise matching a route. Only the first Route marked default will be used as the default • **Route Disabled** - If ticked (checked) then this Route is disabled i.e. not in use
Symmetric Routing (Labs)	This function is identical in operation to *Symmetric Routing* described above with the exception that it also handles IPv6 as well as IPv4 addresses. This means that the parameter IP Address Range List can now accept ranges of IPv4, IPv6 and mixtures of these e.g. 192.168.1.1-192.168.1.255,fe80::612d:7669:d879:1302- fe80::612d:7669:d879:1400.

Routing Function	Description

Symmetric Routing (Expression)	**Note:** This routing function is applied by default on any nodes that were exported from a Point-to-Point network to a Multi-Point network.
	This function has the same concept as the *Symmetric Routing* function. It supports all the fields that the *Symmetric Routing* function does. That is IP Address range lists, IP Port range Lists and VLAN Range lists, but adds to these an Expression field, which it adds to your selection. So if you use the IP address range 192.168.2.1-192.168.2.254 it will automatically (without you needing to know) generate the expression:
	`(ipv4.dst >= 192.168.2.1 and ipv4.dst <= 192.168.2.254) or (ipv4.src >= 192.168.2.1 and ipv4.src <= 192.168.2.254)`
	Why? Because this exactly what symmetric routing does (routes by either source or destination property. So now if you add your own expression as well as specifying this range it will automatically generate the required expression.
	As an example, let's assume you fill out the fields as follows, in your symmetric route:
	 
	Then it needs to make sure your IP addresses are in the correct ranges and the expression is true to match the route. To do this behind the scenes it creates the following expression:
	`((ipv4.dst >= 192.168.2.1 and ipv4.dst <= 192.168.2.254) or (ipv4.src >= 192.168.2.1 and ipv4.src <= 192.168.2.254)) and (ipv4.proto = 6)`
	Again, you don't see this process, as it happens in the background.
	From the resulting expression (part generated and part input by you) it evaluated whether the route matches (i.e. when the expression is True).
	This leads to a caveat. Suppose instead of `ipv4.proto = 6` you entered the Route Expression: `eth.dst = 00:11:22:33:44:01` (for example). Then the resulting combined expression would be:
	`((ipv4.dst >= 192.168.2.1 and ipv4.dst <= 192.168.2.254) or (ipv4.src >= 192.168.2.1 and ipv4.src <= 192.168.2.254)) and (eth.dst = 00:11:22:33:44:01)`
	which is of course no longer symmetric because `eth.dst = 00:11:22:33:44:01` is itself not symmetric in the mac address. If you want to keep it symmetric (you don't have to, but then why are you using symmetric routing?) you need to make sure that your expressions are symmetric e.g. set your expression to be:
	`eth.dst = 00:11:22:33:44:01 or eth.src = 00:11:22:33:44:01`
	Now the resulting auto generated expression is:
	`((ipv4.dst >= 192.168.2.1 and ipv4.dst <= 192.168.2.254) or (ipv4.src >= 192.168.2.1 and ipv4.src <= 192.168.2.254)) and (eth.dst = 00:11:22:33:44:01 or eth.src = 00:11:22:33:44:01)`
	This is quite an expression, but the hard work is automatically done for you and it is also compiled to machine code by the just in time (JIT) compiler and so evaluated quickly.

Routing Function	Description
Route and Replicate	This is a very specialist function and should not be used generally, but is very useful in testing broadcast and multicast scenarios. This function routes a packet to ALL the matching routes, not just the first match, as is done in other routing functions (and in regular routers). The effect is to replicate (clone) the packet and send it to all routes. Specify the "routing" table using routes as follows: • **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE. • **Use Last Hop as Port In** – modifies **Port In** to be the name of the immediately previous network object (i.e. link or node) or port (hardware or soft) the packet just came from. • **Port Out** – A network object (i.e. link or node) or a port (hardware or soft) to which the Traffic will be Routed if it matches this rule. • **Route Disabled** - If ticked (checked) then this route is disabled i.e. not in use. **Note:** This function copies the contents of entire packets which is a considerable overhead, so it should not be used unless packet duplication and routing is exactly what is required.
Composite Routing (Labs)	**Note:** This routing function is applied by default on end nodes for Cloud and Hub and Spoke network topology templates. This function is a super-set of IP Address Port VLAN Routing. Route by a selection of packet properties: Source and/or Destination IP Addresses, Source and/or Destination TCP/UDP Ports and/or VLAN IDs. This function allows routing by lists, ranges or list of ranges of: • **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE. • **Use Last Hop as Port In** – modifies **Port In** to be the name of the immediately previous network object (i.e. link or node) or port (hardware or soft) the packet just came from. • **Source IP Address** – where the packet has come from e.g. for TCP/IP 192.168.1.1-192.168.1.255. • **Dest IP Address** - where the packet is going to e.g. 192.168.2.10 • **Source Port** – which port the packet has come from e.g. for TCP/IP 6000, 6001 • **Dest Port** – which port the packet is going to e.g. 80 (HTTP), 443 (HTTPS), 25 (smtp), 21 (ftp), 110 (pop3), 445 (Microsoft-ds – Network File Access) • **IP Protocol** – the IP protocol of the packet e.g. 0 (Not IP) 1 (ICMP), 6 (TCP), 17 (UDP), 47 (GRE) etc. • **VLAN Id** – 802.1Q VLAN label (tag), if the packet is VLAN tagged. • **DPI** – (Deep Packet Inspection) select a packet for routing based on one or more bytes or bits in the header or data part of the packet. • **Port Out** – A network object (i.e. link or node) or a port (hardware or soft) to which the Traffic will be Routed if it matches this rule. • **Default Route** – Tick (check) to specify that this route is the default for all traffic not otherwise matching a route. Only the first route marked default will be used as the default. • **Continue Matching** – If ticked (checked) then if this route is matched the packet will be cloned and sent to the next routes for further matching. This implies the ability to duplicate the packet. **Note:** If **Continue Matching** is checked the function copies the contents of entire packets which is a considerable overhead, so it should not be used unless packet duplication and routing is exactly what is required. • **Route Disabled** - If ticked (checked) then this route is disabled i.e. not in use.

Routing Function	Description
Expression Routing (Expression)	This function is the most powerful routing function. It is the expression version of *Composite Routing (Labs)* (described above) – equivalent to that function but using our "Wireshark like" expressions for classification instead of ranges and lists of IP Addresses, IP Ports,IP protocols, VLAN Ids etc. For more on expressions, see *Expression Library Functions* on page 734 in *Appendix 1*, *Specifying Expressions*. Like *Composite Routing (Labs)* it supports Continue Matching (and therefore packet duplication and Route disablement).
IP Routing (Labs)	**Note:** This routing function is applied by default on end nodes for Fully Meshed and Free Form network topology templates, and the hub node in the Hub and Spoke network topology template. Route specifying either an IPv4 Network Address and IPv4 Network Mask or an IPv6 Address/network bits, or both IPv4 and IPv6. This function allows routing by lists, ranges or list of ranges of: • **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE. • **IPv4 Network Address** – Any IPv4 address in the subnet that is being Routed e.g. 192.168.1.1 and 192.168.1.254 are equivalent is network mask (below) is set to 255.255.255.0. For clarity it's often good (but not required) to use the network base address e.g. 192.168.1.0 in this example. • **IPv4 Network Mask** – The network mask to use with the Network Address above e.g. 255.255.255.0 for a standard "class c" style network. As usual, the mask is "ANDed" with both the Network Address specified above and the Destination IP Address in the network packet. If the results of these ANDing processes match then the packet is deemed to match the network and therefore match the routing rule. • **IPv6 Address** – The IPv6 address in standard form with the number of bits representing the network portion of the address following the "/" character e.g. fe80::612d:7669:d879:1302/64. • **Port Out** – A network object (i.e. link or node) or a port (hardware or soft) to which the Traffic will be routed if it matches this rule. • **Continue Matching** – If ticked (checked) then if this route is matched the packet will be cloned and sent to the next routes for further matching. This implies the ability to duplicate the packet. **Note:** If **Continue Matching** is checked the function copies the contents of entire packets which is a considerable overhead, so it should not be used unless packet duplication and routing is exactly what is required. • **Route Disabled** - If ticked (checked) then this route is disabled i.e. not in use.
Note: The Composite Routing (Labs), Symmetric Routing (Expression) or IP Routing (Labs) have a **Packet Replay** check box, which must usually be unticked. The a **Packet Replay** check box is only for use with the Packet Replay function, and applied on the last route in the route table on any endpoint nodes connected to a Packet Replay node. For more information, see *Chapter 15, Packet Input Functions*.	

For each node in the Workspace, if necessary you can change default routing functions used according to your routing needs. Once you are happy with the routing function(s) that apply to a node, click the **OK** button to return to the **Routing Properties** window (*Illustration 95* on page 335), from where you can define the routing table for each of the routing function applied on the node. For more information on defining a node's routing table, see *Creating and Editing a Routing Table for a Routing Function on a Node* on page 343.

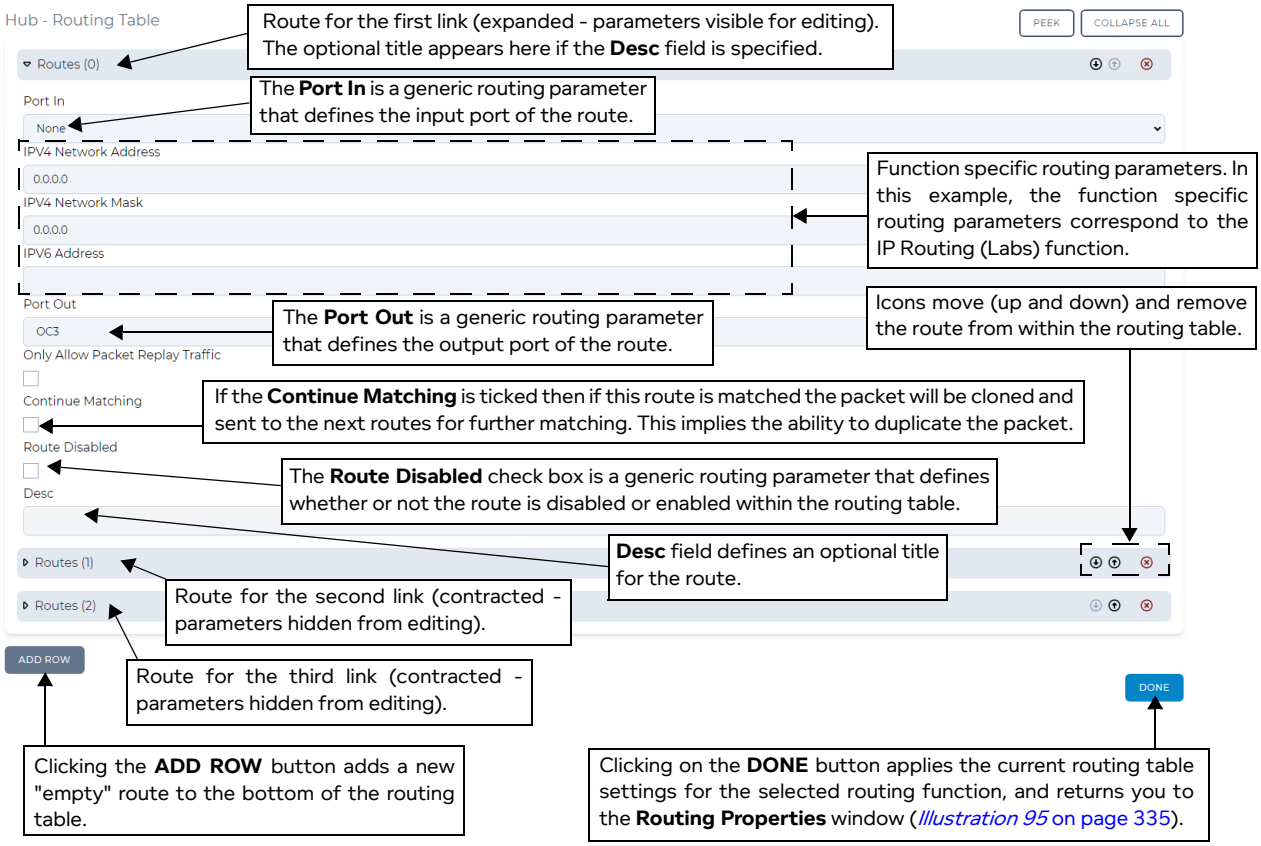
3-2-7-2. Creating and Editing a Routing Table for a Routing Function on a Node

Initially each node within the Workspace needs its routing table defined. The **Routing Table** window (*Illustration 97*) lets you define routing table for the node. The parameters that appear in the Routes window depend on the routing function that you selected in the **Routing Properties** window (*Illustration 95* on page 335).

By default, the **Routing Table** window contains one route for each link that is connected to the node, and the output port (**Port Out** drop-down menu) will automatically select the connected link. Also, if the input port was already defined from within the **Routing Properties** window (*Illustration 95* on page 335), the **Routing Table** window inherits this input port in the **Port In** drop-down field. However, if necessary, the input port defined in the **Port In** drop-down field can be changed to override the input port that is inherited from the **Routing Properties** window (*Illustration 95* on page 335).

The example in **Routing Table** window in *Illustration 97* is for a hub node that has three end nodes connected to it, each with one link, and where the IP Routing (Labs) routing function is used on the hub node.

ILLUSTRATION 97 - ROUTES WINDOW (EXAMPLE OF HUB, INITIALLY UNDEFINED WITH THREE LINKS)



The **Routing Table** window contains the elements summarized in *Table 53*.

TABLE 53 - ROUTING TABLE WINDOW ELEMENTS

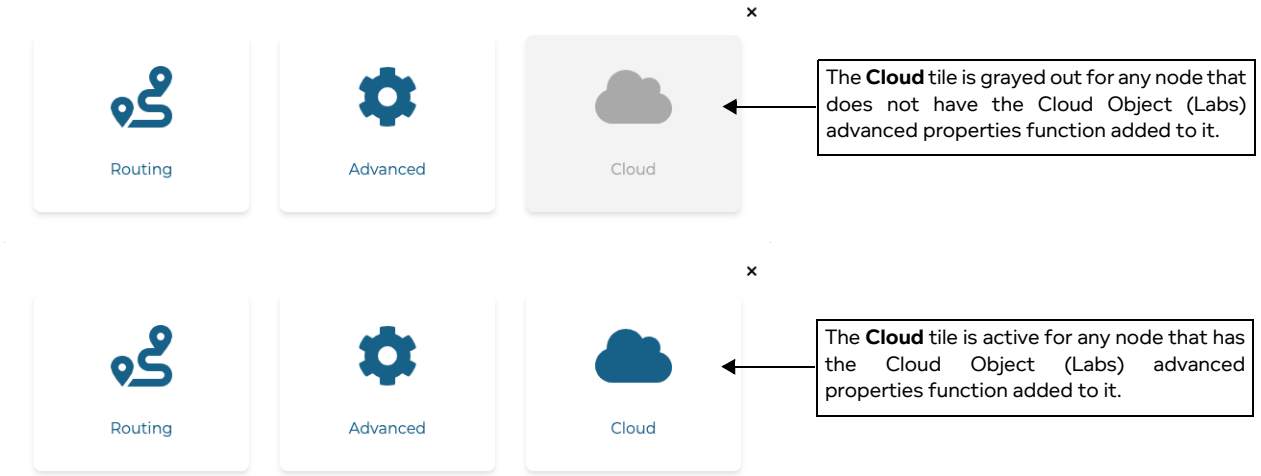
Routes Window Element	Description
ADD ROW button	Clicking this button adds a new "empty" route to the bottom of the routing table. The newly added route intentionally does not inherit any existing link or input port parameters. Once a new route is added, it needs defining.
COLLAPSE ALL button	Clicking this button collapses all (if any) of the routes whose properties are expanded.

Routes Window Element	Description
PEEK button	Hovering over this button hides the **Routing Table** window so you can examine the Multi-Point network. Moving the mouse away from this button re-displays the **Routing Table** window. This is useful when building a routing table and lets you quickly view the routes of the Multi-Point network without leaving the **Routing Table** window.
A route (row) for each route in the routing table, each with the following route manipulation icons: ▼ ▶ ⬇ ⬆ ⊗	Each route (i.e. row) has the following manipulation icons: • Clicking on ▶ expands the route letting you configure the route's parameters. The route parameters that vary according to the routing function that was selected. The route parameters that appear are split into two types, as follows: Generic route parameters (i.e. **Port In** drop-down field, **Port Out** drop-down field, and **Route Disabled** check box). Function specific route parameters. • Clicking on ▼ contracts the route's parameters. • Clicking on ⬇ moves the route function down the routing. • Clicking on ⬆ moves the route up the routing table. • Clicking on ⊗ removes the routing function from the routing table.
DONE button	Clicking on the **DONE** button applies the current routing settings, and returns you to the **Routing Properties** window (*Illustration 95*).

3-2-8. Editing the Properties of a Node via the Node Properties Window (Multi-Point Networks)

The **Node Properties** window (*Illustration 98*) lets you define all the networking properties (i.e. routing, advanced properties, and cloud properties) for a node. Each node within the Workspace may have its networking properties defined (if required, as discussed below).

ILLUSTRATION 98 - NODE PROPERTIES WINDOW (WITH AND WITHOUT CLOUD TILE ENABLED)



To open the **Node Properties** window for a node, click on the node whose routing properties that you want to edit, then click the **PROPERTIES** button from the **Edit node** panel that appears.

The **Node Properties** window contains the following tiles:

- **Routing** - clicking on this tile opens a **Routing Properties** window (*Illustration 95* on page 335), which lets you define the routing properties of the node. You must define the routing properties for the node in order for the Multi-Point network to run correctly. For more information, see *Editing the Routing of a Node via the Node Routing Window (Multi-Point Networks)* on page 335.
- **Advanced** - clicking on this tile opens an **Advanced Node Properties** window (*Illustration 101* on page 348), from where you can add one or more advanced property functions on the node. Configuring advanced node properties for a node is optional, and depends on your testing needs. For more information, see *Editing the Advanced Properties of a Node via the Advanced Node Properties Window (Multi-Point Networks)* on page 346.
- **Cloud** - clicking on this tile opens an **Cloud Node Properties** window (*Illustration 102* on page 351), from where you can configure the cloud properties of the node. Configuring cloud node properties for a node is optional, and depends on your testing needs. For more information, see *Editing the Cloud Properties of a Node via the Cloud Node Properties Window (Multi-Point Networks)* on page 351.

Note:

The **Cloud** tile may initially be grayed out, which is normal. The **Cloud** tile is initially grayed out on any nodes in a Free-Form, Fully Meshed, and Hub and Spoke network topology.

The **Cloud** tile is active on any node that has the Cloud Object (Labs) advanced properties function added to it. Thus, the **Cloud** tile is or becomes active in the following two cases:

1. Is already active for the middle cloud node in a Cloud network topology type (as when this network topology type was initially chosen in the **Network Wizard** window, the Cloud Object (Labs) advanced properties function is automatically added to the middle cloud node).
2. When the Cloud Object (Labs) advanced properties function is manually added to a node.

3-2-9. Editing the Advanced Properties of a Node via the Advanced Node Properties Window (Multi-Point Networks)

Whilst the basic node properties are extremely intuitive and quick to use, there are also advanced node properties for the more experienced user that wants to setup more sophisticated node configurations. The **Advanced Node Properties** window (*Illustration 100* on page 347) lets you add and configure different functions that are applied to the traffic on a node.

Note:

By default, a node initially includes no advanced functions (which is normal), and contains only an **Add new property** tile (*Illustration 99*). Clicking the **Add new property** tile opens an **Advanced Node Properties Available** window (*Illustration 101* on page 348) which lets you add/remove the functions in use on the node, and the order in which the functions run on the node. Once, one or more functions have been added from the **Advanced Node Properties Available** window, the **Advanced Node Properties** window becomes populated with functions similar to that shown in *Illustration 100* on page 347.

ILLUSTRATION 99 - ADVANCED NODE PROPERTIES WINDOWS (BEFORE ANY FUNCTIONS HAVE BEEN ADDED TO THE NODE)

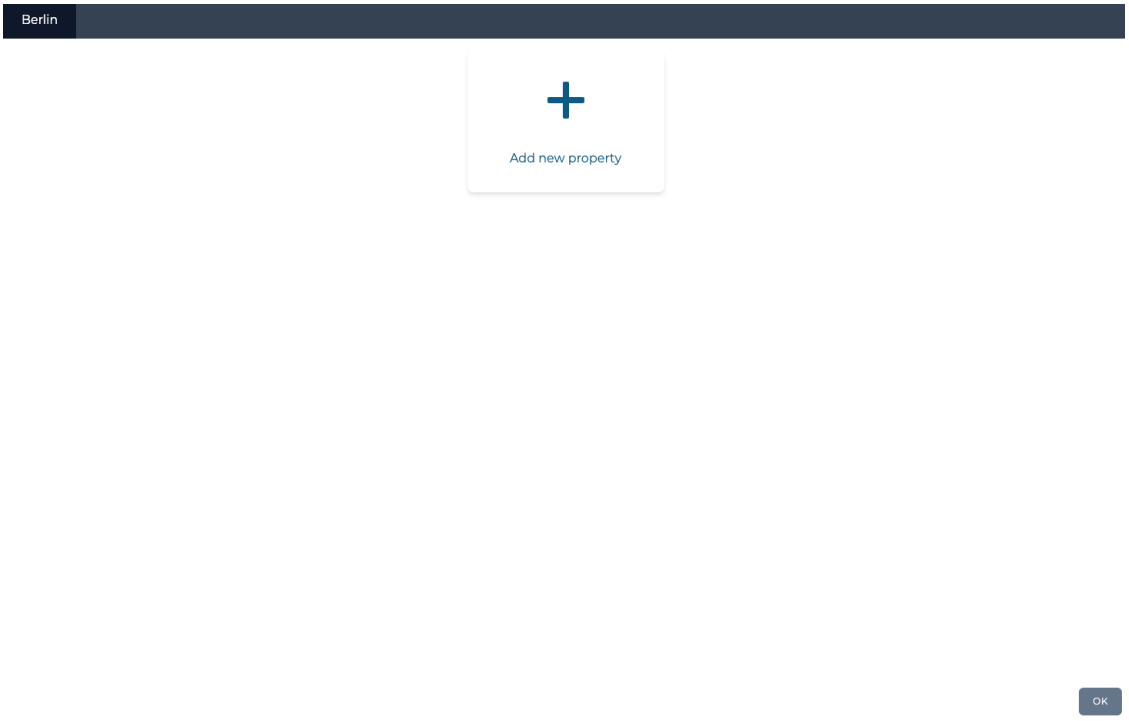
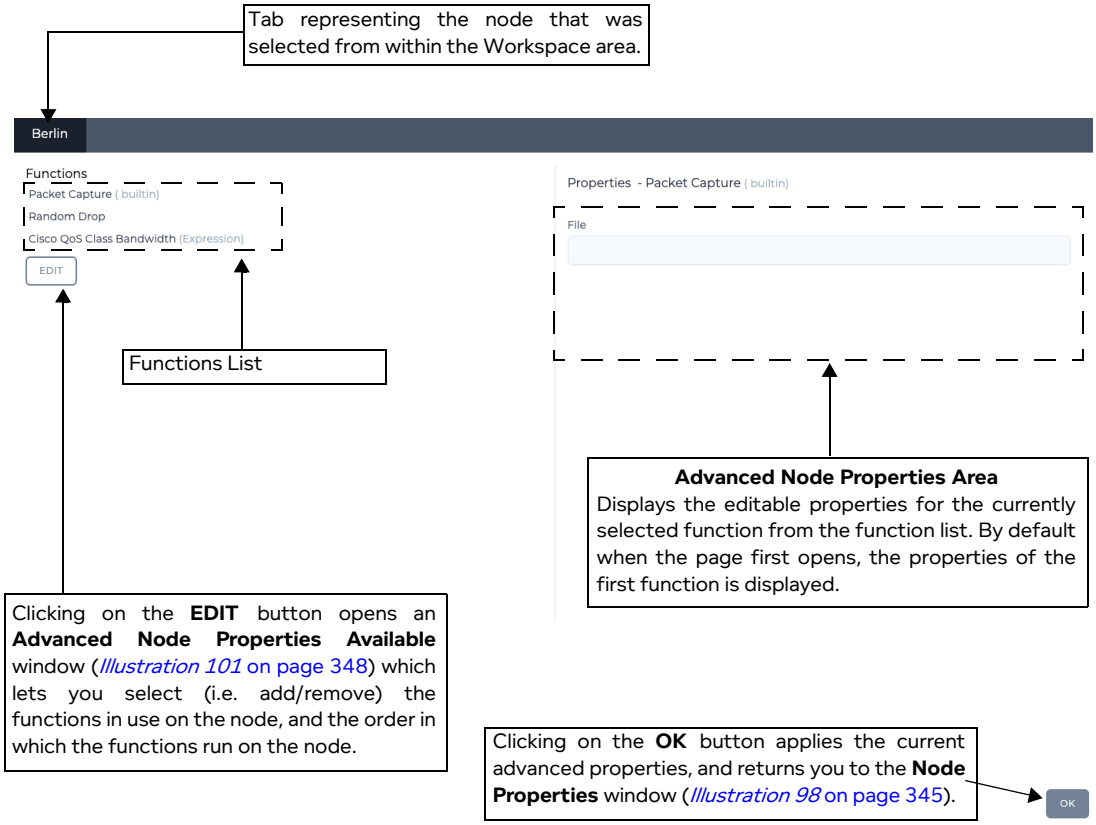


ILLUSTRATION 100 - ADVANCED NODE PROPERTIES WINDOW (ONCE ONE OR MORE FUNCTIONS HAVE BEEN ADDED TO THE NODE)



The **Advanced Node Properties** window contains the elements summarized in *Table 54*.

TABLE 54 - ADVANCED NODE PROPERTIES WINDOW ELEMENTS FOR MULTI-POINT NETWORKS

Advanced Node Settings element	Description
EDIT button	Clicking this button opens an **Advanced Node Properties Available** window (*Illustration 101*) which lets you add/remove the functions in use on the node, and the order in which the functions run on the node.
Advanced Node Properties Area	Contains one or more fields letting you configure the currently selected function. The different node functions that are available, and their parameters are summarized in *Available Node Functions* on page 759 in *Appendix 2*, *Available Functions*.
OK button	Clicking on the **OK** button applies the current impairment settings, and returns you to the **Node Properties** window (*Illustration 99* on page 346).

The **Advanced Properties Available** window (*Illustration 101* on page 348) lets you select (i.e. add/remove) and order the advanced properties functions that are applied to the traffic for the node, and contains the elements summarized in *Table 55*.

ILLUSTRATION 101 - ADVANCED NODE PROPERTIES AVAILABLE WINDOW

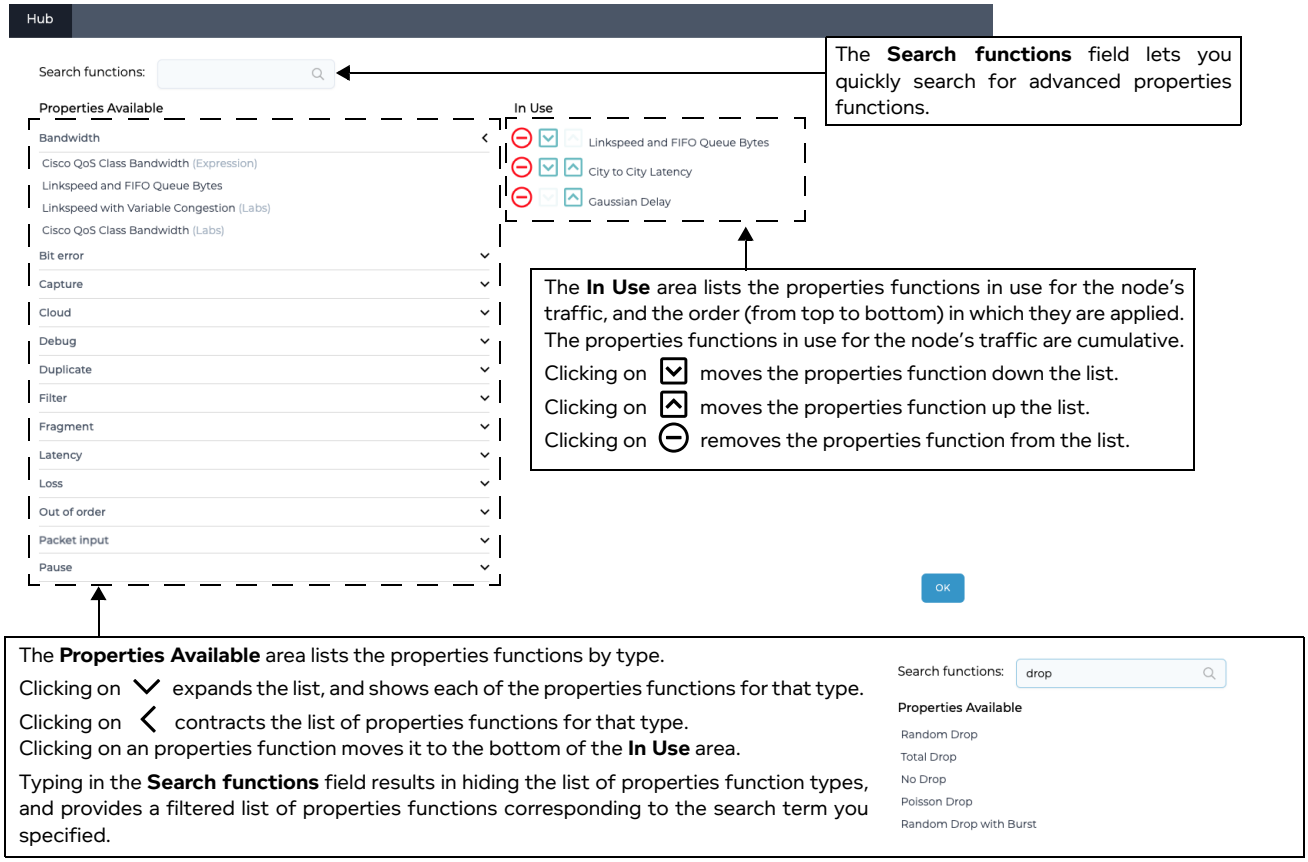


TABLE 55 - ADVANCED NODE PROPERTIES FUNCTIONS AVAILABLE WINDOW ELEMENTS

Advanced Properties Functions Available Element	Description
Search functions field	The **Search functions** field lets you quickly search for properties functions.
Properties Available area	The **Properties Available** area lists the properties functions by type. • Clicking on expands the list, and shows each of the properties functions for that type. • Clicking on contracts the list of properties functions for that type. • Clicking on a properties function moves it to the bottom of the **In Use** area. Typing in the **Search functions** field results in hiding the list of properties function types, and provides a filtered list of properties functions corresponding to the search term you specified.
In Use area	The **In Use** area lists the properties functions in use for the node, and the order (from top to bottom) in which they are applied. The properties functions in use for the node are cumulative. • Clicking on moves the properties function down the list. • Clicking on moves the properties function up the list. • Clicking on removes the properties function from the list.
OK button	Clicking on the **OK** button applies the current properties settings, and returns you to the **Advanced Node Properties** window (*Illustration 100* on page 347).

For each node in the Workspace, if necessary you can optionally add one or more advanced properties functions used on the node according to your testing needs. Once you are happy with the advanced properties function(s) that apply to a node, click the **OK** button to return to the **Advanced Node Properties** window (*Illustration 100* on page 347), from where you can define the parameters for each of the advanced properties function(s) applied on the node.

The different node functions that are available, and their parameters are summarized in *Available Node Functions* on page 759 in *Appendix 2*, *Available Functions*.

3-2-9-1. Adding Advanced Functions to a Node

It is beyond the scope of this document to discuss all of the node functions in detail. However, it is interesting to briefly discuss adding the Cloud Object (Labs) function to a node, for the following reasons:

- to illustrate the general steps of adding any function to a node,
- to highlight the fact that you do not necessarily need to start with the Cloud network topology type from the **Multi-Point Designer** page (*Illustration 84* on page 308) in order to create a Cloud network. For example, a cloud network can also be created in via a Free-Form network template, where you would simply add the Cloud Object (Labs) function to the central node in the network that you create, and then configure the parameters of the Cloud Object (Labs) function.

Note:

Typically, if you want a Cloud network topology, you would simply choose the Cloud network topology type template from the **Multi-Point Designer** page as a starting point as the Cloud Object (Labs) function is automatically applied to the Cloud node by the template.

Use the following steps to add a function (in this example, the Cloud Object (Labs) function) to a Node from within the Workspace.

1. From the **Multi-Point Designer** page, click on the node to which you intend add the function.

   An **Edit node** panel (*Illustration 88* on page 319) appears.
2. From the **Edit node** panel that appears, click the **PROPERTIES** button.

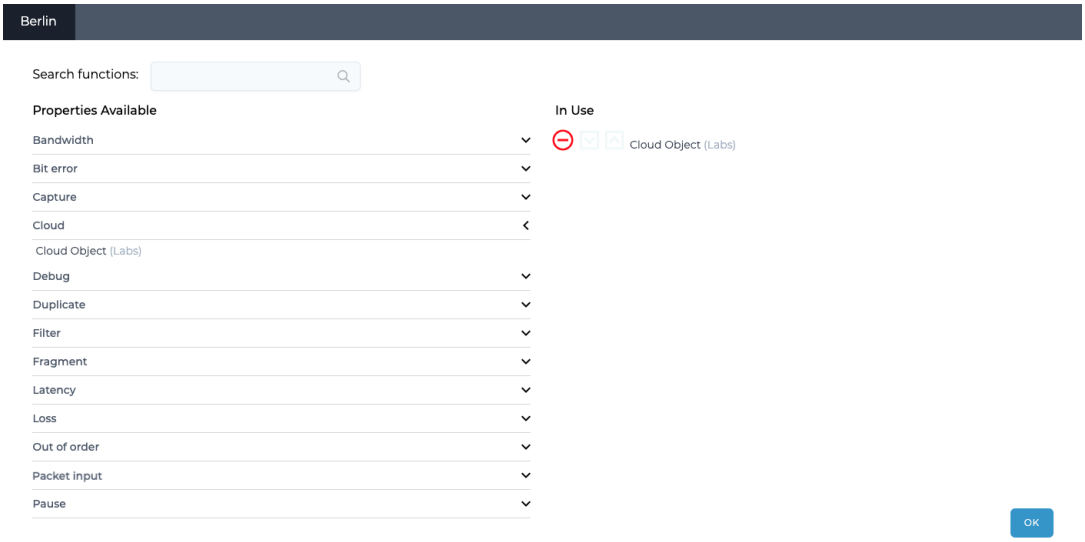
   A **Node Properties** window (*Illustration 98* on page 345) appears.
3. From the **Node Properties** window that appears, click the **ADVANCED** button.

   A **Advanced Node Properties** window appears.
   - If no functions are already applied to the node, the **Advanced Node Properties** window is unpopulated (*Illustration 99* on page 346), and an **Add new property** tile is present.
   - If one or more functions are already applied to the node, the **Advanced Node Properties** window is populated (*Illustration 100* on page 347), and an **EDIT** button is present.
4. From the **Advanced Node Properties** window (*Illustration 101* on page 348) that appears, click either the **Add new property** tile or **EDIT** button.

   The **Advanced Properties Available** window (*Illustration 101* on page 348) appears.
5. From the **Advanced Properties Available** window, do the following for each of the functions that you want to add to the node:
   a. In the **Properties Available** area, search for and select the appropriate function you want to add.

      In our example (for the Cloud Object (Labs) function, click on the ⌄ icon next to the **Cloud**

function category, then click on the **Cloud Objects (Labs)** function to select it.



The selected function moves over to the **In Use** area.

b. If necessary, move the function up or down relative to other function by clicking on either the ⬒ icon or ⬓ icon, respectively.
   In our example, only the Cloud Object (Labs) function is added to the **In Use** area.
c. Click **OK**.
d. You are returned to **Advanced Node Properties** window from where you can now define the parameters of the added function.
   In our example, only the Cloud Object (Labs) function is added to the node, and the **Advanced Node Properties** window looks like that shown in *Illustration 102* on page 351 of which is described in *Editing the Cloud Properties of a Node via the Cloud Node Properties Window (Multi-Point Networks)* on page 351.

3-2-10. Editing the Cloud Properties of a Node via the Cloud Node Properties Window (Multi-Point Networks)

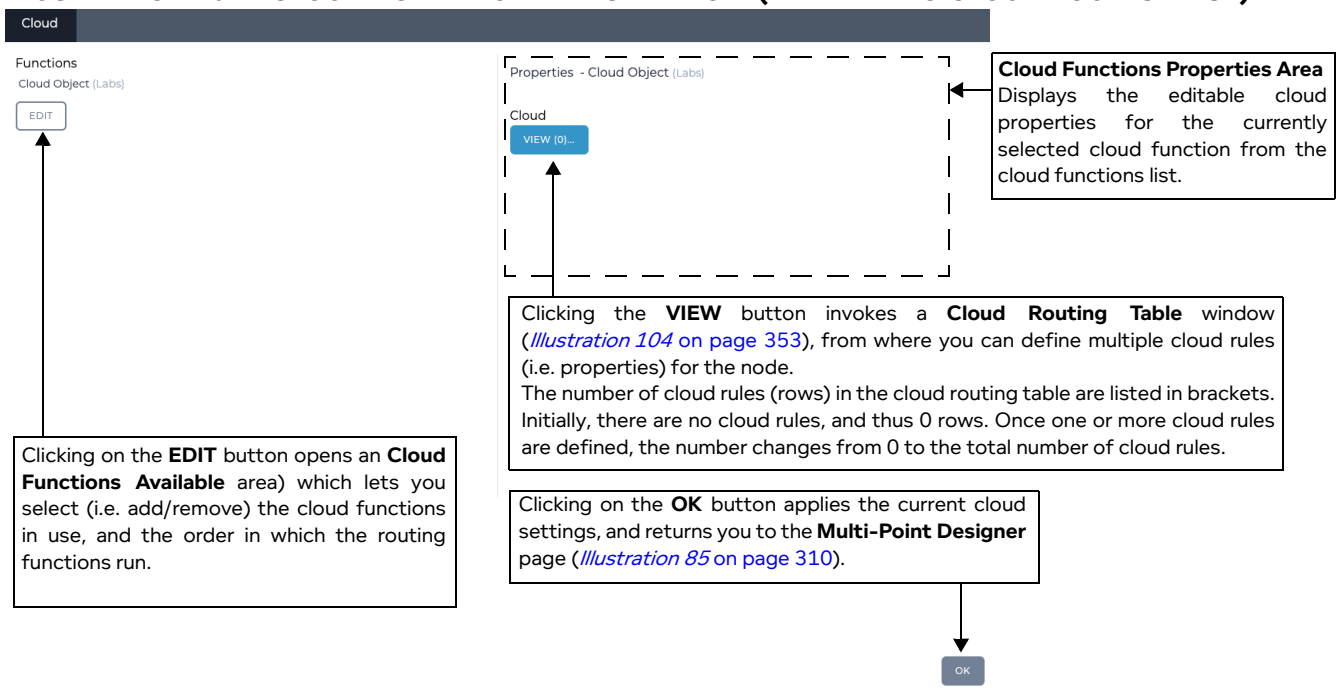
If a node already has Cloud Object (Labs) advanced properties function added to it (which is automatically the case for a cloud node in the Cloud network topology type), the cloud properties can be defined for the node.

Note:

If you want a node to act as a cloud object, then it must have the Cloud Object (Labs) advanced properties function added to it. For more information about adding advanced properties to a node, see *Editing the Advanced Properties of a Node via the Advanced Node Properties Window (Multi-Point Networks)* on page 346.

The **Cloud Node Properties** window (*Illustration 102*) lets you define all of the cloud properties for a node.

ILLUSTRATION 102 - CLOUD NODE PROPERTIES WINDOW (INITIALLY NO CLOUD ROUTES EXIST)



The **Cloud Node Properties** window contains the following:

- Cloud Functions List area, which contains:
  - The list of cloud functions that are currently applied to the node. If more than one cloud function exists (this in not recommended), clicking on the cloud function selects it for configuring from within the Routing Cloud Properties area.
  - **EDIT** button. Clicking this button invokes the **Cloud Functions Available** window (*Illustration 103* on page 352) letting you add, remove, and order the cloud functions that are applied on the node. For more information, see *Assigning Cloud Functions to a Node* on page 352.
- Cloud Function Properties area, which contains a **VIEW** button for the selected cloud function. Clicking this button opens a **Cloud Routing Table** window (*Illustration 104*), which lets you define the cloud function for the selected cloud function of the node. For more information, see *Creating and Editing Cloud Rules for a Cloud Function* on page 353.
- **OK** button. Clicking this button applies the current cloud settings, and returns you to the **Multi-Point Designer** page (*Illustration 85* on page 310).

3-2-10-1.Assigning Cloud Functions to a Node

The **Cloud Functions Available** window (*Illustration 103*) lets you select (i.e. add/remove) and order the cloud functions that are applied on the traffic for the node, and contains the elements summarized in *Table 56*.

Note:
Using multiple cloud functions on a node is possible, but not recommended.

Note:
At the current release, only one cloud function (i.e. Cloud Object (Labs)) exists. Future product releases will contain additional cloud functions. If the NE-ONE is licensed with the Defense Pack, a second TDMA Mesh (Labs) function exists. For more information, see *Editing the TDMA Mesh Properties of a Node via the Mesh Properties Window (Multi-Point Networks)* on page 360.

ILLUSTRATION 103 - CLOUD FUNCTIONS AVAILABLE AREA OF THE CLOUD NODE PROPERTIES PAGE

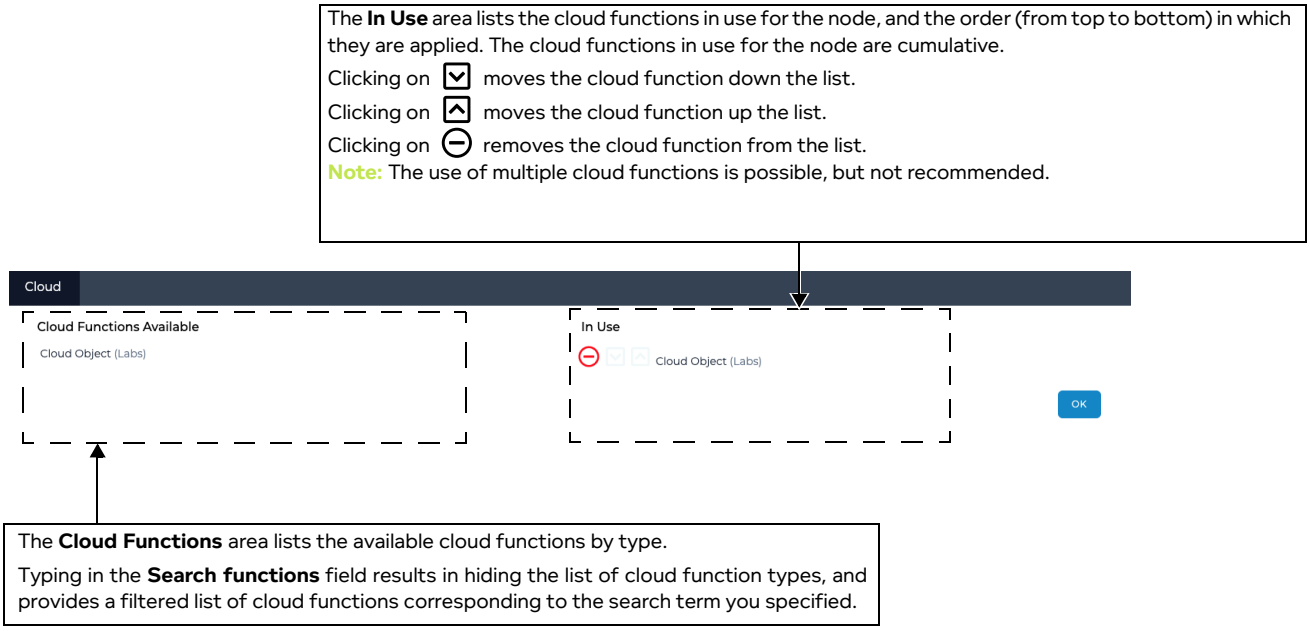


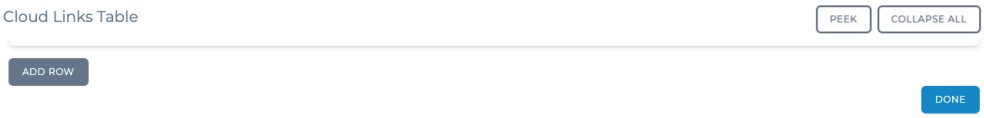
TABLE 56 - CLOUD FUNCTIONS AVAILABLE WINDOW ELEMENTS

Cloud Functions Available Element	Description
Cloud Functions Available area	The **Cloud Functions Available** area lists the cloud functions by type. • Clicking on ⌄ expands the list, and shows each of the cloud functions for that type. • Clicking on ‹ contracts the list of cloud functions for that type. • Clicking on an cloud function moves it to the bottom of the **In Use** area.
In Use area	The **In Use** area lists the cloud functions in use for the node, and the order (from top to bottom) in which they are applied. The cloud functions in use for the node are cumulative. • Clicking on moves the cloud function down the list. • Clicking on moves the cloud function up the list. • Clicking on removes the cloud function from the list.
OK button	Clicking on the **OK** button applies the current cloud settings, and returns you to the **Cloud Node Properties** window (*Illustration 102*).

3-2-10-2.Creating and Editing Cloud Rules for a Cloud Function

Initially a node with the Cloud Object (Labs) function has no cloud link rules added to it (*Illustration 104*). The **Cloud Links Table** window (*Illustration 104*) lets you add cloud link rules. Each cloud link rule that you add, appears as a row in the **Cloud Links Table** window.

ILLUSTRATION 104 - CLOUD LINKS TABLE WINDOW (INITIALLY NO CLOUD RULES EXIST)



Clicking on the **ADD ROW** button, creates an new cloud link rule row, which is initially expanded (*Illustration 105*). Within the cloud link rule row, exist all the appropriate elements (i.e. fields, and buttons invoking the definition of ranges - see *Table 57* on page 354), letting you define all aspects of the cloud link rule.

Conceptually, a cloud link can be considered as having two sets of parameters (described in *Table 57* on page 354):

- Cloud link quality parameters (i.e. bandwidth, latency, jitter, TTL cost, loss, queue length), which are optional parameters that let you define the general quality of the cloud link.
- Cloud link filter parameters (i.e. input port, source/destination IP addresses, source/destination ports, IPv4 protocols, VLAN Ids, deep packet inspection (DPI) criteria), which are optional parameters that let you define the traffic on which you want to filter for the cloud link.

Each cloud link can also be configured to be enabled/disabled within the cloud node, and to generate or not generate packet capture and tracing data (these parameters are also described in *Table 57* on page 354).

In order for a Cloud type Multi-Point network to run properly and transfer data packets, at least one cloud link must be set up using a valid cloud link rule. You can set up many cloud links (each with a cloud link rule) within the **Cloud Links Table** window.

ILLUSTRATION 105 - CLOUD LINKS TABLE WINDOW (WITH ONE EXAMPLE RULE)

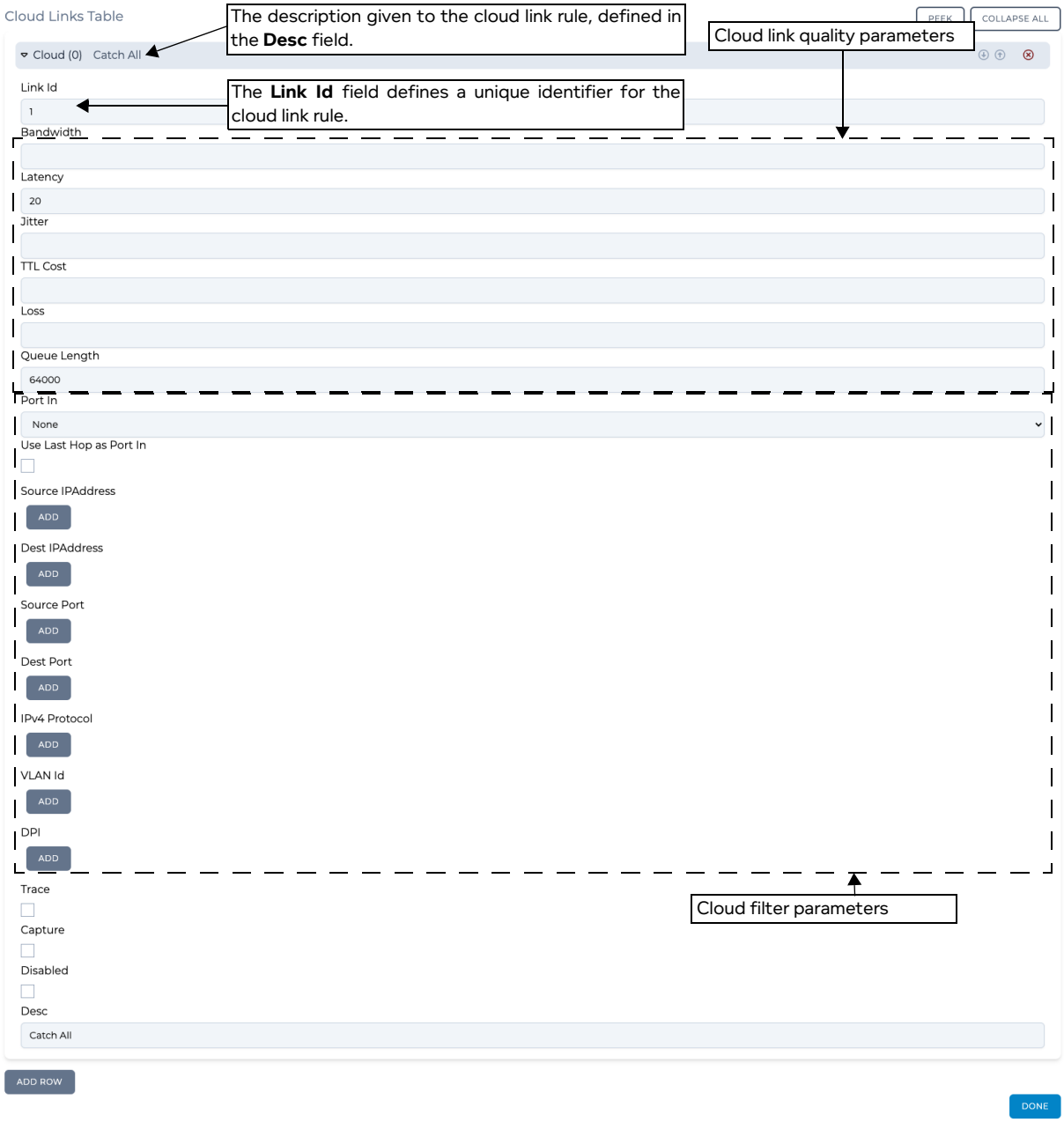


TABLE 57 - CLOUD LINK RULE ROW ELEMENTS

Cloud Link Rule Element	Description
Link Id field	This is a mandatory parameter, needs to be set to a unique value per cloud row to enable the NE-ONE to locate rows that have been updated, deleted and reordered, preserving currently queued packets, where appropriate. Link Ids do not need to be consecutive but must be greater than 0 and less than 1,000,000.

Cloud Link Rule Element	Description
Bandwidth field	This defines the bandwidth applied to the cloud's link. The maximum bandwidth (in bps) that this traffic can have (0 means unregulated – effectively infinity, not no bandwidth – if no bandwidth is required please use 100% Loss instead) **Note:** This can be left undefined. If left undefined, no bandwidth impairment is applied to the cloud link.
Latency field	This defines the latency applied to the cloud's link. This is the base delay in (decimal) milliseconds to apply to the packet. **Note:** This can be left undefined. If left undefined, no latency is applied to the cloud link.
Jitter field	This defines the jitter applied to the cloud's link. This is a random additional delay (in milliseconds) to be added to the Latency. For each packet a value between 0 and Jitter is randomly added to Latency and the packet is delayed by the combined delay value. **Note:** This can be left undefined. If left undefined, no jitter is applied to the cloud link.
TTL Cost field	This defines the TTL cost applied to the cloud's link. This value is subtracted from the Packet's IP Time-to-Live (TTL) value and the packet's IP checksum is recomputed to be valid. If the packet's checksum is <= 0 after the subtraction the packet is dropped. **Note:** This can be left undefined. If left undefined, no TTL cost is applied to the cloud link.
Loss field	This defines the packet loss applied to the cloud's link. This is a (decimal) percentage loss (between 0 and 100) which is applied to each packet at random. It represents a loss probability e.g. if it was 10 then 10 in every 100 (10%) of packets would be lost at random. **Note:** This can be left undefined. If left undefined, no packet lost is applied to the cloud link.
Queue Length field	This defines the queue length (i.e. cloud user waiting time) applied to the cloud's link. This sets the queue size for bandwidth purposes for this cloud row. If a packet cannot be immediately transmitted it is queued in this queue. Eventually if there is no space in the queue the packet is dropped. The default queue size is 64000 bytes. **Note:** The queue length must be defined with a non-zero value. If left undefined, no queue length is applied to the cloud link which is an unrealistic test scenario (i.e. each cloud user must cloud wait their turn for a defined queue length for the previous cloud user to have finished their task).
Port In drop-down field	This defines the input port in (i.e. the inward bound links) coming into the cloud to filter on. If you want to filter traffic from a particular inbound link, select the name of the link from this drop-down field. **Note 1:** By default **None** (i.e. undefined - all inbound links) is set. If this is left set to **None** (i.e. undefined), traffic from all inbound links is selected by the cloud rule. If only one inbound link is selected, then only traffic from the selected inbound link is selected by the cloud rule. **Note 2:** If you are creating a general cloud rule that catches all traffic from all inbound links, you do not define an input port filter, and would leave the **Port In** drop-down field set to **None**.

Cloud Link Rule Element	Description
Use Last Hop As Port In check box	This check box determines whether or not the **Port In** is modified to be the name of the immediately previous network object (i.e. link or node) or port (hardware or soft) the packet just came from. • If this check box is unticked, the **Port In** is not modified. • If this check box is ticked, the **Port In** is modified. **Note 1:** by default, when a cloud link rule is created, this check box is unticked. **Note 2:** If you are creating a general cloud rule that catches all traffic from all inbound links, you do not define an input port filter, and would leave the **Use Last Hop As Port In** check box unticked.
Source IP Address ADD button	Clicking this button opens a **Source IP Address Range** dialog box with **Maximum** and **Minimum** fields, letting you define a source IP Address range to filter on for the cloud rule. **Note:** If you are creating a general cloud rule that catches all traffic, you do not define a source IP address filter.
Destination IP Address ADD button	Clicking this button opens a **Destination IP Address Range** dialog box with **Maximum** and **Minimum** fields, letting you define a destination IP Address range to filter on for the cloud rule. **Note:** If you are creating a general cloud rule that catches all traffic, you do not define a destination IP address filter.
Source Port ADD button	Clicking this button opens a **Source Port** dialog box with **Maximum** and **Minimum** fields, letting you define a source UDP/TCP port range to filter on for the cloud rule. Port filtering is applied for both UDP and TCP. **Note:** If you are creating a general cloud rule that catches all traffic, you do not define a source port filter.
Destination Port ADD button	Clicking this button opens a **Destination Port** dialog box with **Maximum** and **Minimum** fields, letting you define a destination UDP/TCP port range to filter on for the cloud rule. Port filtering is applied for both UDP and TCP. **Note:** If you are creating a general cloud rule that catches all traffic, you do not define a destination port filter.
IPv4 Protocol ADD button	Clicking this button opens a **Destination Port** dialog box with **Maximum** and **Minimum** fields, letting you define a destination UDP/TCP port range to filter on for the cloud rule. Port filtering is applied for both UDP and TCP. **Note:** If you are creating a general cloud rule that catches all traffic, you do not define a destination port filter.
VLAN Id ADD button	Clicking this button opens a **VLAN Id** dialog box with **Maximum** and **Minimum** fields, letting you define a VLAN Id range to filter on for the cloud rule. **Note:** If you are creating a general cloud rule that catches all traffic, you do not define a VLAN Id filter.
DPI ADD button	Clicking this button opens a **DPI** dialog box with **Byte Offset**, **Byte Mask**, and **Byte Value** fields, letting you define a Deep Packet Inspection filter for the cloud rule. **Note:** If you are creating a general cloud rule that catches all traffic, you do not define a Deep Packet Inspection filter.

Cloud Link Rule Element	Description
Trace check box	This check box determines whether or not the tracing is enabled or disabled for the cloud link rule. • If this check box is unticked, tracing is disabled for the cloud link rule. • If this check box is ticked, tracing is enabled for the cloud link rule. **Note:** by default, when a cloud link rule is created, this check box is unticked (i.e. tracing of the cloud link rule is disabled).
Capture check box	By default, a cloud node network object contains packet capture data for all enable cloud link rules that are defined in the **Cloud Link Rules Array** table window. If necessary, you can determine whether some or all of the cloud link rules packet capture data exists in the packet capture file (`*.pcap`) of the cloud network object. This check box determines whether or not the packet capture is enabled or disabled for the cloud link rule. • If this check box is unticked, packet capture is disabled for the cloud link rule. • If this check box is ticked, packet capture is enabled for the cloud link rule. **Note:** by default, when a cloud link rule is created, this check box is unticked (i.e. packet capture of the cloud link rule is disabled).
Disabled check box	This check box determines whether or not the cloud link rule is enabled or disabled on the cloud node. • If this check box is unticked, the cloud link rule is enabled on the cloud node. • If this check box is ticked, the cloud link rule is disabled on the cloud node. **Note 1:** by default, when a cloud link rule is created, this check box is unticked (i.e. the cloud link rule is enabled by default). **Note 2:** In order for a cloud node to function (i.e. transfer packets of data) within a Multi-Point network, at least one valid cloud link rule must be configured and enabled.
Desc field	This defines the description given to the cloud link rule (which appears in the row for the cloud link rule within the **Cloud Routing Table** window). The description is optional, but Calnex recommends that you specify something meaningful so multiple cloud link rules can easily be distinguished from one another. The description can contain alpha-numeric characters and spaces.

After defining the cloud link rule's parameters, and clicking **DONE**, the new cloud rule will be listed in the **Cloud Node Properties** window (see *Illustration 107* on page 359).

Illustration 106 on page 358 shows an example of a **Cloud Links Table** window with multiple cloud link rules defined (and all minimized). Outside of each rows, the **Cloud Links Table** window contains the elements summarized in *Table 57*.

TABLE 58 - CLOUD LINKS WINDOW ELEMENTS

Cloud Links Table Window Element	Description
ADD ROW button	Clicking this button adds a new "empty" cloud link rule to the bottom of the cloud link rules array table. The newly added cloud link rule intentionally does not inherit any existing link or input port parameters. Once a new cloud link rule is added, it needs defining.
A route (row) for each route in the routing table, each with the following route manipulation icons: ▾ ▸ ⬇ ⬆ ⊗	Each cloud link rule (i.e. row) has the following manipulation icons: • Clicking on ▸ expands the cloud link rule letting you configure the cloud link rule's parameters. • Clicking on ▾ contracts the cloud link rule's parameters. • Clicking on ⬇ moves the cloud link rule down the cloud link rules array table. • Clicking on ⬆ moves the cloud link rule up the cloud link rules array table. • Clicking on ⊗ removes the cloud link rule function from the cloud link rules array table.
DONE button	Clicking on the **DONE** button applies the current cloud link rule settings, and returns you to the **Cloud Node Properties** window (*Illustration 102*).

ILLUSTRATION 106 - CLOUD LINKS TABLE WINDOW (WITH MULTIPLE RULES)

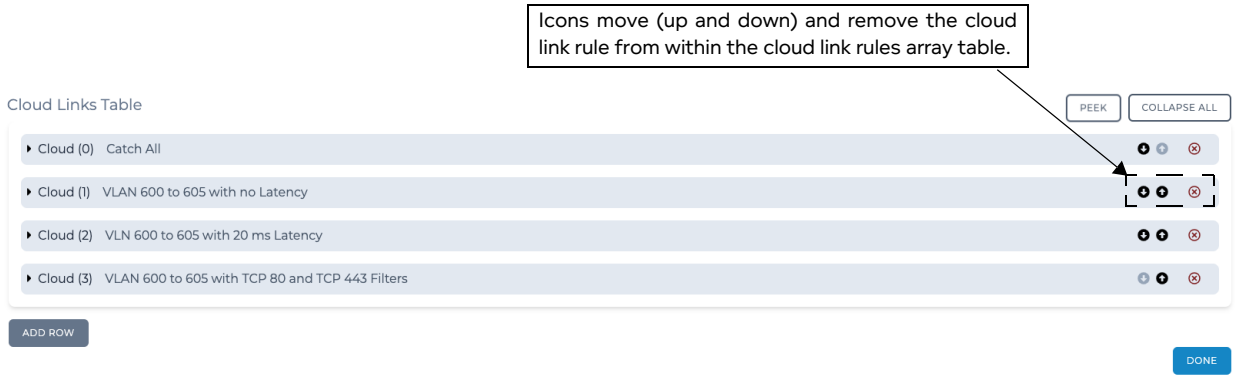
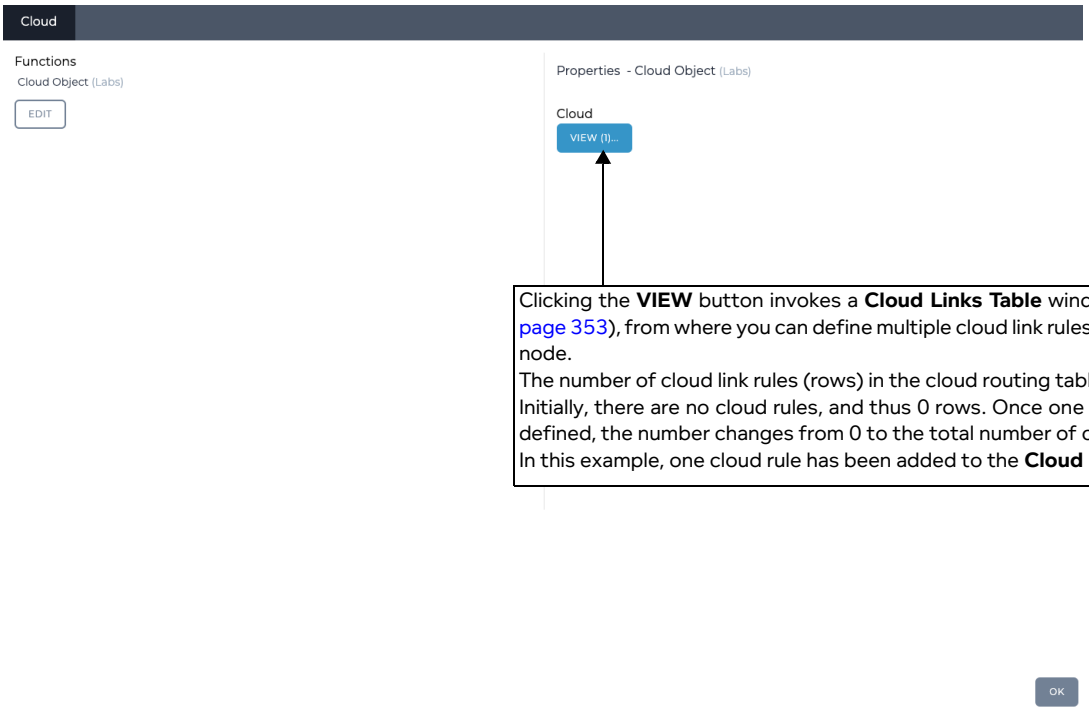


ILLUSTRATION 107 - CLOUD NODE PROPERTIES WINDOW (WITH ONE CLOUD RULE)



Clicking the **VIEW** button invokes a **Cloud Links Table** window (*Illustration 104* on page 353), from where you can define multiple cloud link rules (i.e. properties) for the node.
The number of cloud link rules (rows) in the cloud routing table are listed in brackets. Initially, there are no cloud rules, and thus 0 rows. Once one or more cloud rules are defined, the number changes from 0 to the total number of cloud rules.
In this example, one cloud rule has been added to the **Cloud Links Table** window.

3-2-11. Editing the TDMA Mesh Properties of a Node via the Mesh Properties Window (Multi-Point Networks)

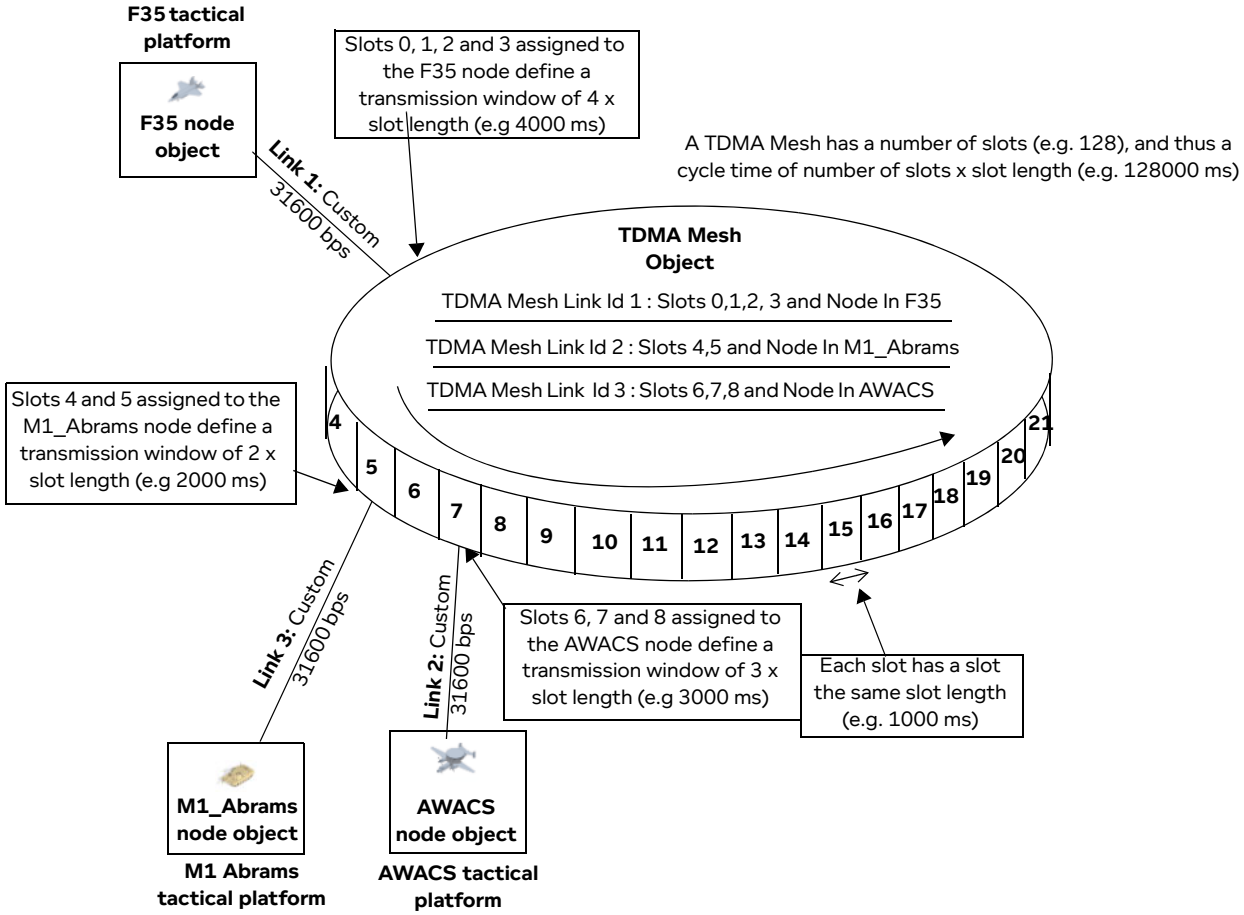
Note:

This section is only applicable if the NE-ONE is licensed with the Defense Pack.

To understand how the TDMA Mesh (Labs) function works, we briefly discuss how a Time Division Multiple Access (TDMA) network functions.

Tactical platforms communicate (i.e transmit and receive data) via a TDMA Mesh (see *Illustration 108*). A TDMA Mesh contains a number of slots (e.g. 128), each with the same slot length (e.g. 1000 ms (1s)), and thus a cycle time of number of slots x slot length (e.g. 128000 ms (12s)).

ILLUSTRATION 108 - EXAMPLE TDMA NETWORK



The TDMA Mesh can be conceptually considered as a "wall" during its cycle time for data transmitted by tactical platforms. The "wall" does not exist for nodes receiving data that has already been transmitted into the TDMA Mesh.

Each tactical platform can only transmit data into the TDMA Mesh when their allocated slots are available (i.e. when their allocated slots "pass by" during the cycle time). A tactical platform can be allocated one or more unique slots (i.e. the same slot number cannot be used for more than one tactical platform). Multiple slots can be allocated in a contiguous manner (i.e. 0, 1, 2, and 3), in which case there is no break in the ability for the tactical platform to transmit into the TDMA Mesh between those contiguous slots. The transmission window (i.e. the number of contiguous slots) into the TDMA Mesh can be different for different tactical platforms. The more contiguous slots that are defined for a tactical platform, the larger its transmission window into the TDMA Mesh is.

The tactical platforms can always receive data via the TDMA Mesh (i.e. the reception of the data is not impacted by their allocated slots). When a "source" tactical platform transmits data into the TDMA Mesh (i.e. when its allocated slots are "passing by" during the slot cycle time) the transmitted data passes via the TDMA Mesh onto the "destination" platform, which can always receive data.

The NE-ONE lets you simulate a TDMA network with a Multi-Point Free Form network as follows:

- Apply a TDMA Mesh (Labs) function on a central TDMA Mesh node. The TDMA Mesh (Labs) function has the following parameters:
  - Slot Length - defines the slot length (in ms) for the TDMA Mesh.
  - Number of Slots - defines the number of slots for the TDMA Mesh. The cycle time of the TDMA Mesh = number of slots x slot length.

  Note:
  It is recommended to set a maximum number of slots to "future proof" the capacity (i.e. cycle time (slot length x number of slots) of your TDMA configuration without the need to change it later on. The NE-ONE will implement the same cycle time and the unused slots are still present in the cycle. This lets you add additional end nodes at a later time on the unused slots, and thus future proof your TDMA implementation on the NE-ONE.
  - A manually created TDMA Mesh link with a unique Link Id per tactical platform. This defines the allocated slots for the selected tactical platform (**Node In**).
- Create tactical platforms using end nodes, and connect those end nodes to the central TDMA Mesh using a link.

The example TDMA Network in *Illustration 108* illustrates how the NE-ONE lets you simulate the TDMA Network. In this example, there are the three tactical platforms (i.e. Airborne Warning and Control System (AWACS), M1 Abrams Tank, and F35 combat aircraft) which are defined as end nodes in a Free Form Multi-Point network.

The three tactical platforms (end nodes) are connected by links to the central TDMA Mesh node which has the TDMA Mesh (Labs) function. The three tactical platforms (end nodes) communicate (transmit and receive data) via the TDMA Mesh.

The three tactical platforms (end nodes) can always receive data via the TDMA Mesh. The three tactical platforms (end nodes) can only transmit data into the TDMA Mesh when their allocated slots "pass by" during the cycle time. The allocated slots (i.e. transmission window) for each tactical platform (end node) is defined by a unique TDMA Mesh Link (with a unique Link Id) within the TDMA Mesh (Labs) function on the TDMA Mesh.

In the example in *Illustration 108* we see that the F35 combat aircraft has a transmission window of 4000 ms (contiguous slots 0, 1, 2, and 3), the M1 Abrams battle tank has transmission window of 2000 ms (contiguous slots 4, and 5), and the AWACS has transmission window of 3000 ms (contiguous slots 6, 7 and 8).

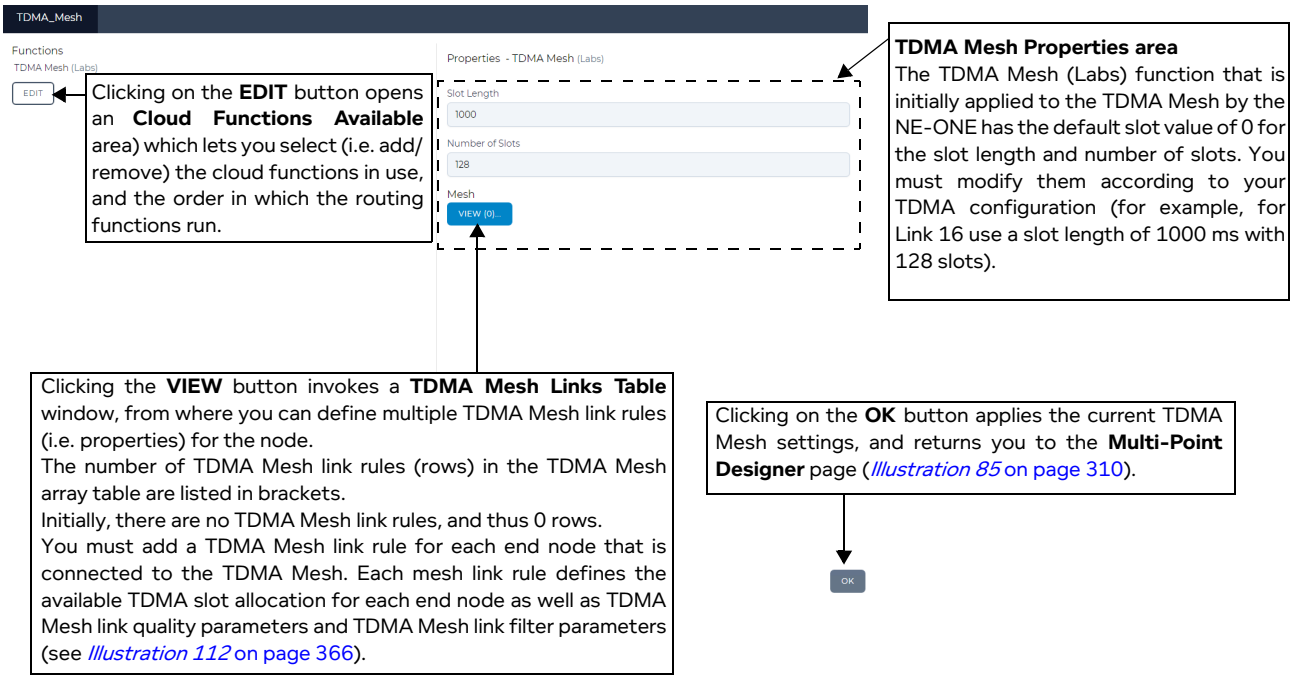
In the example in *Illustration 108* we see that the three tactical platforms transmit immediately after each other during the cycle time because they are on slots 0,1,2,3, slots 4,5 and slots 6,7,8, respectively. They could however be configured to transmit not after each other during the cycle time, for example slots 55,56,57,59, slots 10,11, and slots 20,21,21, respectively.

When you drag the TDMA Mesh icon from the **Defense** category on to the Multi-Point Workspace it already has TDMA Mesh (Labs) advanced properties function added to it, and the TDMA properties can be defined for the TDMA Mesh node directly without needing to manually add the TDMA Mesh (Labs) advanced properties function.

Note:
If you want another node (i.e. not the TDMA Mesh node) to act as a TDMA Mesh object, then it must have the TDMA Mesh (Labs) advanced properties function added to it. For more information about adding advanced properties to a node, see *Editing the Advanced Properties of a Node via the Advanced Node Properties Window (Multi-Point Networks)* on page 346.

The **TDMA Mesh Properties** window (*Illustration 109*) lets you define all of the properties for a TDMA Mesh node.

ILLUSTRATION 109 - TDMA MESH NODE PROPERTIES WINDOW (INITIALLY NO TDMA LINKS EXIST)



The **TDMA Mesh Properties** window contains the following:

- Functions List area, which contains:
  - The list of cloud functions that are currently applied to the node. If more than one cloud function exists (this in not recommended), clicking on the cloud function selects it for configuring from within the TDMA Mesh Properties area.
  - **EDIT** button. Clicking this button invokes the **Cloud Functions Available** window (*Illustration 110* on page 364) letting you add, remove, and order the cloud functions that are applied on the node. For more information, see *Assigning TDMA Functions to a Node* on page 364.
- TDMA Mesh Function Properties area, which contains the following:
  - **Slot Length** field. This defines the slot length (in ms) for the TDMA Mesh.
  - **Number of Slots** field. This defines the number of slots in the TDMA Mesh. The cycle time of the TDMA Mesh = number of slots x slot length.

Note:
It is recommended to set a maximum number of slots to "future proof" the capacity (i.e. cycle time (slot length x number of slots) of your TDMA configuration without the need to change it later on. The NE-ONE will implement the same cycle time and the unused slots are still present in the cycle.

This lets you add additional end nodes at a later time on the unused slots, and thus future proof your TDMA implementation on the NE-ONE.

Note:

The number of slots you define impact the number of valid slots that can be listed for each TDMA Mesh link. For example, if you define the number of slots as 128, then the valid slots available to define in the **Slot List** field for the TDMA Mesh Link rule (see *Illustration 112* on page 366) will be between 0 and 127.

- A **VIEW** button for the selected TDMA Mesh (Labs) function. Clicking this button opens a **TDMA Mesh Links Table** window (*Illustration 111*), which lets you define mesh link rules for each end node connected to the TDMA Mesh. You must add a mesh link rule for each end node that is connected to the TDMA Mesh. Each mesh link rule defines the available TDMA slot allocation for each end node as well as TDMA Mesh link quality parameters and TDMA Mesh link filter parameters (see *Illustration 112* on page 366).

- **OK** button. Clicking this button applies the current TDMA Mesh settings, and returns you to the **Multi-Point Designer** page (*Illustration 85* on page 310).

3-2-11-1.Assigning TDMA Functions to a Node

If you have the Defense Pack, the **Cloud Functions Available** window (*Illustration 110*) contains an additional TDMA Mesh (Labs) function as well as the Cloud Object (Labs) function. The **Cloud Functions Available** window (*Illustration 110*) lets you select (i.e. add/remove) and order the cloud functions that are applied on the traffic for the node, and contains the elements summarized in *Table 59*.

Note:
Using multiple cloud functions on a node is possible, but not recommended. If you are creating a network with a TDMA Mesh, only use the TDMA Mesh (Labs) function for the TDMA Mesh.

ILLUSTRATION 110 - CLOUD FUNCTIONS AVAILABLE AREA OF THE TDMA MESH NODE PROPERTIES PAGE (FOR AN NE-ONE LICENSED WITH THE DEFENSE PACK)

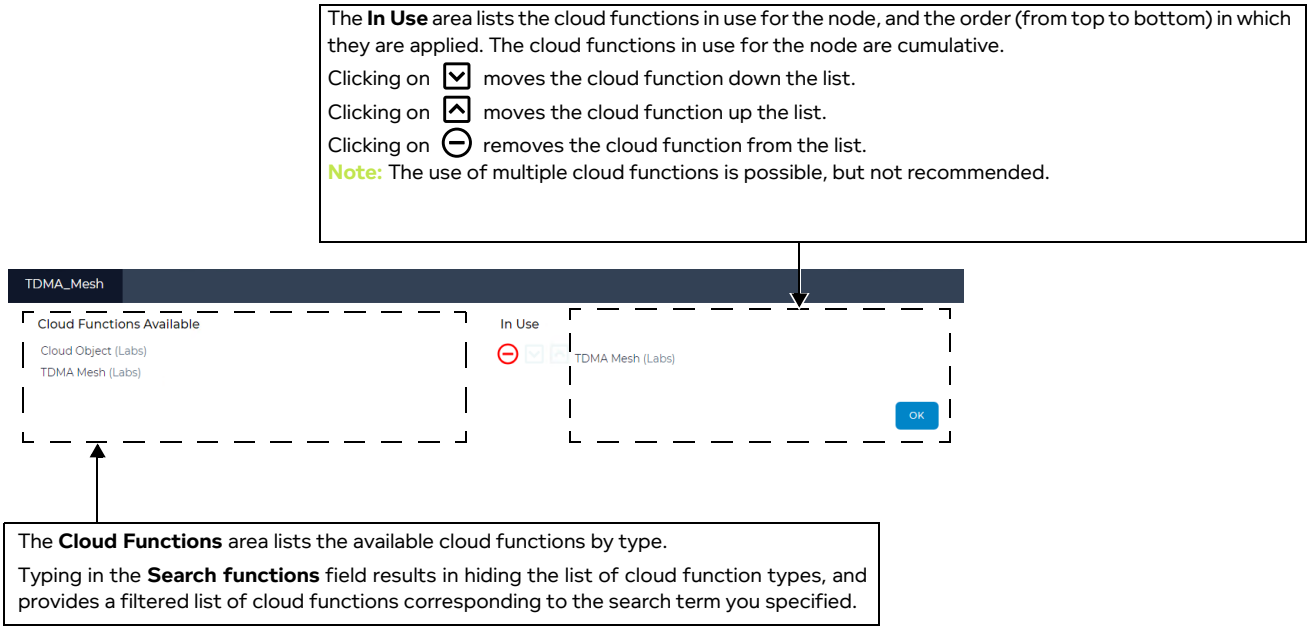


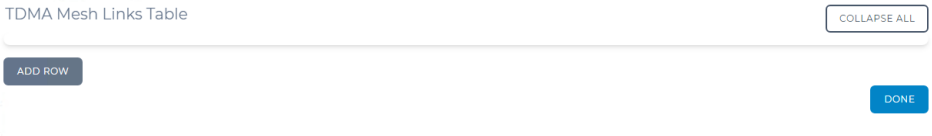
TABLE 59 - CLOUD FUNCTIONS AVAILABLE WINDOW ELEMENTS

Cloud Functions Available Element	Description
Cloud Functions Available area	The **Cloud Functions Available** area lists the cloud functions by type. • Clicking on ⌄ expands the list, and shows each of the cloud functions for that type. • Clicking on ‹ contracts the list of cloud functions for that type. • Clicking on an cloud function moves it to the bottom of the **In Use** area.
In Use area	The **In Use** area lists the cloud functions in use for the node, and the order (from top to bottom) in which they are applied. The cloud functions in use for the node are cumulative. • Clicking on moves the cloud function down the list. • Clicking on moves the cloud function up the list. • Clicking on removes the cloud function from the list.
OK button	Clicking on the **OK** button applies the current cloud settings, and returns you to the **TDMA Mesh Node Properties** window (*Illustration 109*).

3-2-11-2.Creating and Editing TDMA Link Rules for a TDMA Mesh Function

Initially a node with the TDMA Mesh (Labs) function has no TDMA Mesh link rules added to it (*Illustration 111*). The **TDMA Mesh Links Table** window (*Illustration 111*) lets you add TDMA Mesh link rules. Each TDMA Mesh link rule that you add, appears as a row in the **TDMA Mesh Links Table** window.

ILLUSTRATION 111 - TDMA MESH LINKS TABLE WINDOW (INITIALLY NO TDMA MESH LINK RULES EXIST)



Clicking on the **ADD ROW** button, creates an new TDMA Mesh link rule row, which is initially expanded (*Illustration 112*). Within the TDMA Mesh link rule row, exist all the appropriate elements (i.e. fields, and buttons invoking the definition of ranges - see *Table 60* on page 366), letting you define all aspects of the TDMA Mesh link rule.

Conceptually, a TDMA Mesh link can be considered as having four sets of parameters (described in *Table 60* on page 366):

- **Slot List** - This is a mandatory parameter, and defines the slots allocated to the selected end node (**Node In**). Each end node uses a unique slot list (i.e. you cannot use the same slot number for a different end node). The more slots you list for the selected end node (Node In), the larger their "transmission window" into the TDMA Mesh is.
- TDMA Mesh link quality parameters (i.e. bandwidth, latency, jitter, TTL cost, loss, queue length), which are optional parameters that let you define the general quality of the TDMA Mesh link.
- TDMA Mesh link filter parameters (i.e. source/destination IP addresses, source/destination ports, IPv4 protocols, VLAN Ids, deep packet inspection (DPI) criteria), which are optional parameters that let you define the traffic on which you want to filter for the TDMA Mesh link.
- **Node In** link filter parameter - This is a mandatory parameter and selects the end node for which you want the defined **Slot List** apply.

Each TDMA Mesh link can also be configured to be enabled/disabled within the TDMA Mesh node, and to generate or not generate packet capture and tracing data (these parameters are also described in *Table 60* on page 366).

In order for a TDMA Mesh type Multi-Point network to run properly and transfer data packets, one TDMA Mesh link must be set up for each end node connected to the TDMA Mesh.

ILLUSTRATION 112 - TDMA MESH LINKS TABLE WINDOW (WITH ONE EXAMPLE RULE)

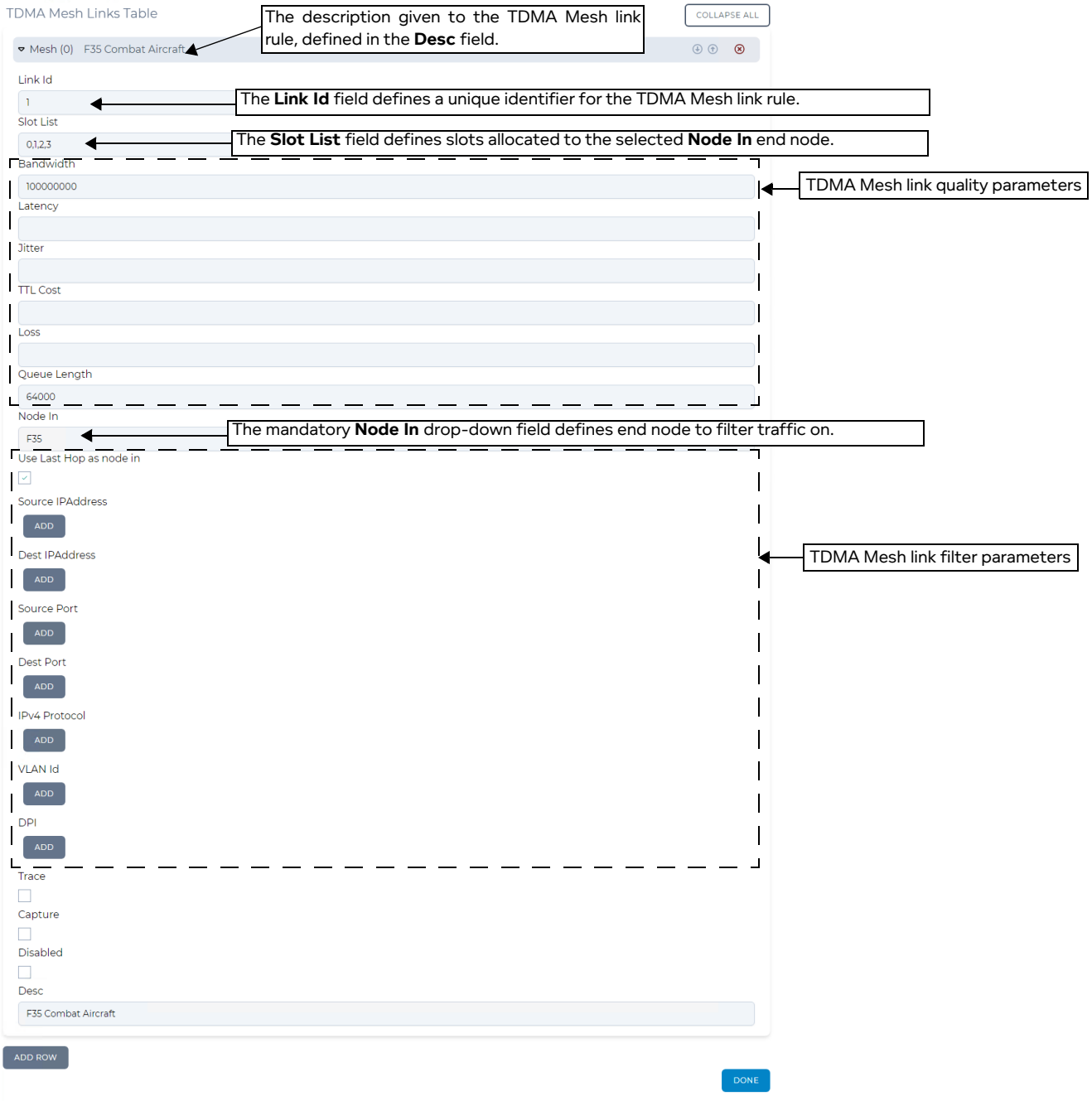


TABLE 60 - TDMA MESH LINK RULE ROW ELEMENTS

TDMA Mesh Link Rule Element	Description
Link Id field	This is a mandatory parameter, needs to be set to a unique value per TDMA Mesh link row to enable the NE-ONE to locate rows that have been updated, deleted and reordered, preserving currently queued packets, where appropriate. Link Ids do not need to be consecutive but must be greater than 0 and less than 1,000,000.

TDMA Mesh Link Rule Element	Description
Slot List field	This is a mandatory parameter, and defines the slots allocated to the selected end node (**Node In**). Each end node uses a unique slot list (i.e. you cannot use the same slot number for a different end node). You must use valid slot numbers. For example if the **Number of Slots** field in the **TDMA Mesh Node Properties** window (*Illustration 109* on page 362) is 128, then the valid slot numbers are 0 - 127. The more slots you list for the selected end node (**Node In**), the larger their "transmission window" into the TDMA Mesh is. For example, if you assign four slots 0,1,2,3 to an end node, its transmission window will be 4 x the slot length (in ms), where the slot length is defined by the **Slot Length** field in the **TDMA Mesh Node Properties** window (*Illustration 109* on page 362).
Bandwidth field	This defines the bandwidth applied to the TDMA Mesh's link. The maximum bandwidth (in bps) that this traffic can have (0 means unregulated – effectively infinity, not no bandwidth – if no bandwidth is required please use 100% Loss instead) **Note:** This can be left undefined. If left undefined, no bandwidth impairment is applied to the TDMA Mesh link.
Latency field	This defines the latency applied to the TDMA Mesh's link. This is the base delay in (decimal) milliseconds to apply to the packet. **Note:** This can be left undefined. If left undefined, no latency is applied to the cloud link.
Jitter field	This defines the jitter applied to the TDMA Mesh's link. This is a random additional delay (in milliseconds) to be added to the Latency. For each packet a value between 0 and Jitter is randomly added to Latency and the packet is delayed by the combined delay value. **Note:** This can be left undefined. If left undefined, no jitter is applied to the TDMA Mesh link.
TTL Cost field	This defines the TTL cost applied to the TDMA Mesh's link. This value is subtracted from the Packet's IP Time-to-Live (TTL) value and the packet's IP checksum is recomputed to be valid. If the packet's checksum is <= 0 after the subtraction the packet is dropped. **Note:** This can be left undefined. If left undefined, no TTL cost is applied to the TDMA Mesh link.
Loss field	This defines the packet loss applied to the TDMA Mesh's link. This is a (decimal) percentage loss (between 0 and 100) which is applied to each packet at random. It represents a loss probability e.g. if it was 10 then 10 in every 100 (10%) of packets would be lost at random. **Note:** This can be left undefined. If left undefined, no packet lost is applied to the TDMA Mesh link.

TDMA Mesh Link Rule Element	Description
Queue Length field	This defines the queue length (i.e. end node (defense platform) waiting time) applied to the TDMA Mesh's link. This sets the queue size for bandwidth purposes for this TDMA Mesh link row. If a packet cannot be immediately transmitted it is queued in this queue. Eventually if there is no space in the queue the packet is dropped. The default queue size is 64000 bytes. **Note:** The queue length must be defined with a non-zero value. If left undefined, no queue length is applied to the TDMA Mesh link which is an unrealistic test scenario (i.e. each end node (defense platform) user must wait their turn for a defined queue length for the previous end node (defense platform) user to have finished their task).
Node In drop-down field	This is a mandatory parameter and selects the end node for which you want the defined **Slot List** apply. This defines the end node coming into the TDMA Mesh to filter on. For each end node connected to the TDMA Mesh, you must create a TDMA Mesh link, and select that end node from the **Node In** drop-down field.
Use Last Hop As Node In check box	This check box determines whether or not the **Node In** is modified to be the name of the immediately previous network object (i.e. link or node) or port (hardware or soft) the packet just came from. • If this check box is unticked, the **Node In** is not modified. • If this check box is ticked, the **Node In** is modified. **Note:** by default, when a TDMA Mesh link rule is created, this check box is unticked.
Source IP Address ADD button	Clicking this button opens a **Source IP Address Range** dialog box with **Maximum** and **Minimum** fields, letting you define a source IP Address range to filter on for the TDMA Mesh rule.
Destination IP Address ADD button	Clicking this button opens a **Destination IP Address Range** dialog box with **Maximum** and **Minimum** fields, letting you define a destination IP Address range to filter on for the TDMA Mesh rule.
Source Port ADD button	Clicking this button opens a **Source Port** dialog box with **Maximum** and **Minimum** fields, letting you define a source UDP/TCP port range to filter on for the TDMA Mesh rule. Port filtering is applied for both UDP and TCP.
Destination Port ADD button	Clicking this button opens a **Destination Port** dialog box with **Maximum** and **Minimum** fields, letting you define a destination UDP/TCP port range to filter on for the TDMA Mesh rule. Port filtering is applied for both UDP and TCP.
IPv4 Protocol ADD button	Clicking this button opens a **Destination Port** dialog box with **Maximum** and **Minimum** fields, letting you define a destination UDP/TCP port range to filter on for the TDMA Mesh rule. Port filtering is applied for both UDP and TCP.
VLAN Id ADD button	Clicking this button opens a **VLAN Id** dialog box with **Maximum** and **Minimum** fields, letting you define a VLAN Id range to filter on for the TDMA Mesh rule.
DPI ADD button	Clicking this button opens a **DPI** dialog box with **Byte Offset**, **Byte Mask**, and **Byte Value** fields, letting you define a Deep Packet Inspection filter for the TDMA Mesh rule.

TDMA Mesh Link Rule Element	Description
Trace check box	This check box determines whether or not the tracing is enabled or disabled for the TDMA Mesh link rule. • If this check box is unticked, tracing is disabled for the TDMA Mesh link rule. • If this check box is ticked, tracing is enabled for the TDMA Mesh link rule. **Note:** by default, when a TDMA Mesh link rule is created, this check box is unticked (i.e. tracing of the TDMA Mesh link rule is disabled).
Capture check box	By default, a TDMA Mesh node network object contains packet capture data for all enable TDMA Mesh link rules that are defined in the **Cloud Link Rules Array** table window. If necessary, you can determine whether some or all of the TDMA Mesh link rules packet capture data exists in the packet capture file (`*.pcap`) of the cloud network object. This check box determines whether or not the packet capture is enabled or disabled for the TDMA Mesh link rule. • If this check box is unticked, packet capture is disabled for the TDMA Mesh link rule. • If this check box is ticked, packet capture is enabled for the TDMA Mesh link rule. **Note:** by default, when a cloud link rule is created, this check box is unticked (i.e. packet capture of the TDMA Mesh link rule is disabled).
Disabled check box	This check box determines whether or not the TDMA Mesh link rule is enabled or disabled on the TDMA Mesh node. • If this check box is unticked, the TDMA Mesh link rule is enabled on the cloud node. • If this check box is ticked, the TDMA Mesh link rule is disabled on the cloud node. **Note 1:** by default, when a TDMA Mesh link rule is created, this check box is unticked (i.e. the TDMA Mesh link rule is enabled by default). **Note 2:** In order for a TDMA Mesh node to function (i.e. transfer packets of data) within a Multi-Point network, one valid TDMA Mesh link rule must be configured and enabled for each end node connected to the TDMA Mesh. If you disable the TDMA Mesh link for the selected **Node In** end node, you effective cut the communication link between the end node and the TDMA Mesh.
Desc field	This defines the description given to the TDMA Mesh link rule (which appears in the row for the TDMA Mesh link rule within the **Cloud Routing Table** window). The description is optional, but Calnex recommends that you specify something meaningful so multiple TDMA Mesh link rules can easily be distinguished from one another. The description can contain alpha-numeric characters and spaces.

After defining the TDMA Mesh link rule's parameters, and clicking **DONE**, the new TDMA Mesh link rule will be listed in the **TDMA Mesh Node Properties** window (see *Illustration 114* on page 372).

Illustration 113 on page 371 shows an example of a **TDMA Mesh Links Table** window with multiple TDME Mesh link rules defined. Outside of each rows, the **TDMA Mesh Links Table** window contains the elements summarized in *Table 61*.

TABLE 61 - TDMA MESH LINKS WINDOW ELEMENTS

TDMA Mesh Links Table Window Element	Description
ADD ROW button	Clicking this button adds a new "empty" TDMA Mesh link rule to the bottom of the TDMA Mesh link rules array table. The newly added TDMA Mesh link rule intentionally does not inherit any existing link or input port parameters. Once a new TDMA Mesh link rule is added, it needs defining.
A route (row) for each route in the routing table, each with the following route manipulation icons: ▼ ▶ ⬇ ⬆ ⊗	Each cloud link rule (i.e. row) has the following manipulation icons: • Clicking on ▶ expands the TDMA Mesh link rule letting you configure the TDMA Mesh link rule's parameters. • Clicking on ▼ contracts the TDMA Mesh link rule's parameters. • Clicking on ⬇ moves the TDMA Mesh link rule down the TDMA Mesh link rules array table. • Clicking on ⬆ moves the TDMA Mesh link rule up the TDMA Mesh link rules array table. • Clicking on ⊗ removes the TDMA Mesh link rule function from the TDMA Mesh link rules array table.
DONE button	Clicking on the **DONE** button applies the current TDMA Mesh link rule settings, and returns you to the **Cloud Node Properties** window (*Illustration 109*).

ILLUSTRATION 113 - TDMA MESH LINKS TABLE WINDOW (WITH MULTIPLE RULES)

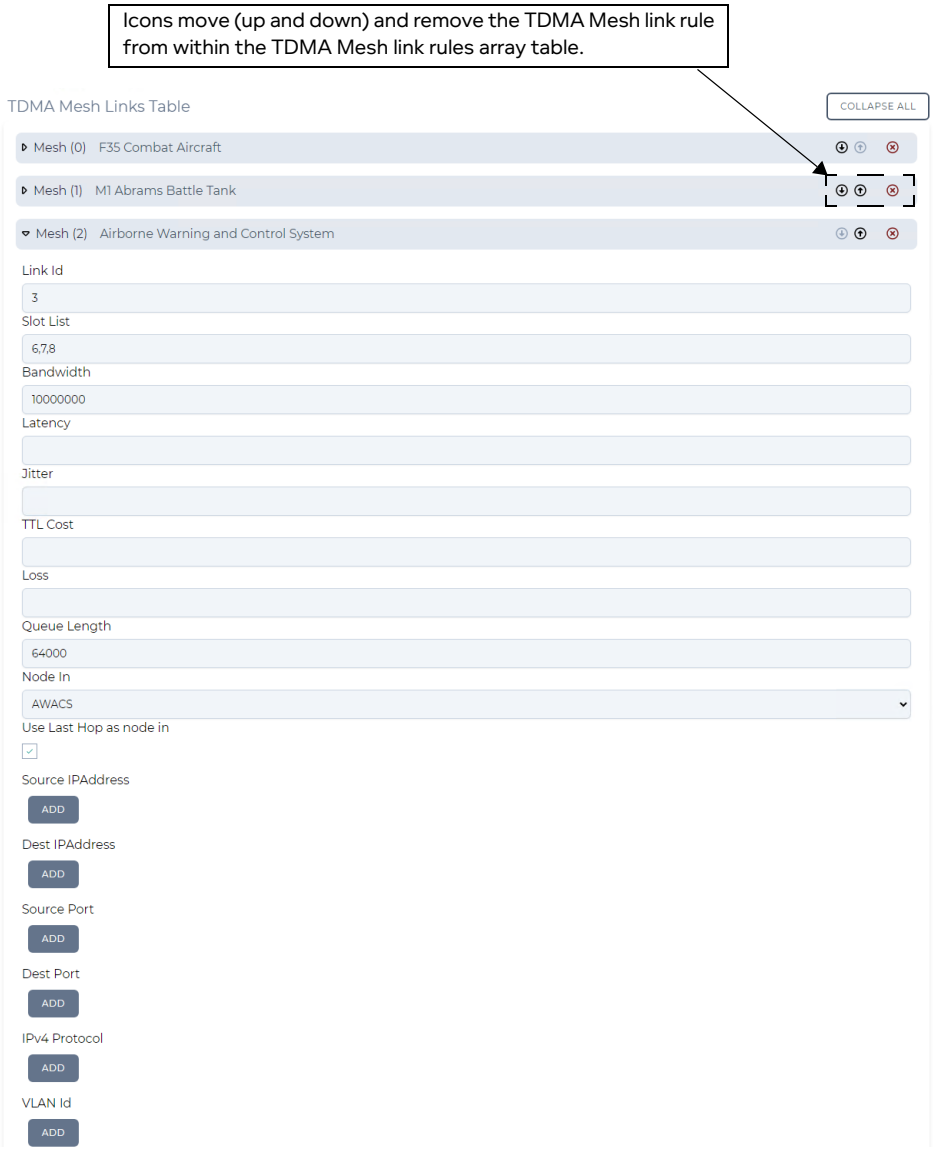
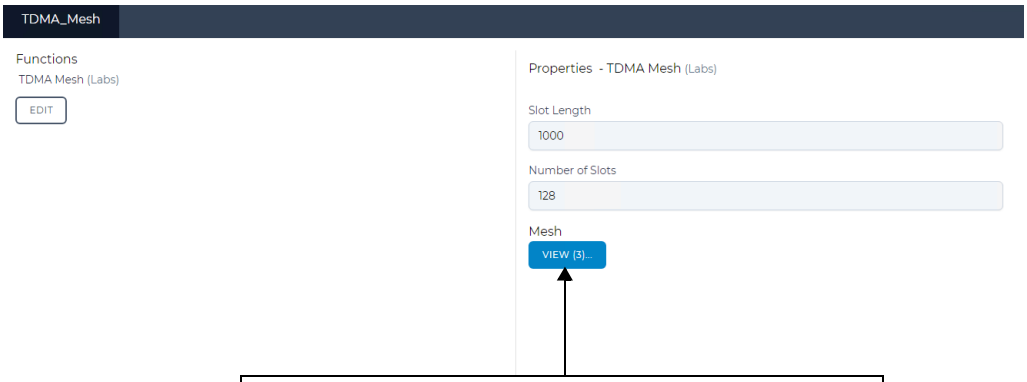


ILLUSTRATION 114 - TDMA MESH NODE PROPERTIES WINDOW (WITH THREE TDMA MESH LINK RULES)



Clicking the **VIEW** button invokes a **TDMA Mesh Links Table** window, from where you can define multiple TDMA Mesh link rules (i.e. properties) for the node.
The number of TDMA Mesh link rules (rows) in the TDMA Mesh array table are listed in brackets.
Initially, there are no TDMA Mesh link rules, and thus 0 rows.
You must add a TDMA Mesh link rule for each end node that is connected to the TDMA Mesh. Each mesh link rule defines the available TDMA slot allocation for each end node as well as TDMA Mesh link quality parameters and TDMA Mesh link filter parameters (see *Illustration 112* on page 366).

4. CREATING MULTI-POINT NETWORKS (EXAMPLES)

This section provides example procedures for creating Multi-Point networks. It assumes that you understand how the network related Web Interface pages operate (as described above in *Section 3*, *Web Interface Network Pages (Multi-Point)*).

Note:

The procedures in this section provide simplistic small networks with a small number of nodes and links. This is intentional in order to describe the general concepts of using the **Multi-Point Designer** page to create a Multi-Point network. The principles described in these procedures equally extend further for much larger number of nodes and links. These procedures aim to provide the type of work flow you would follow in order to rapidly create Multi-Point network.

4-1. Creating Free Form Networks

The **Multi-Point Designer** page Free Form template lets you create a Multi-Point network from scratch without any "starting" template (i.e. Fully Meshed, Cloud or Hub and Spoke). The Free Form template lets you create both very simple and very complicated network topologies.

Conceptually speaking, the **Multi-Point Designer** page has exactly the same functionally for the Free Form, Fully Meshed, Cloud, and Hub and Spoke network topology templates. The only difference is the "starting point" provided by the templates in the Workspace. The Free Form template provides an empty Workspace, whereas the Fully Meshed, Cloud or Hub and Spoke provide an initial network topology on the Workspace, with certain routing functions already applied to their nodes (see *Table 50* on page 336).

Therefore, you can consider that when you adapt a Multi-Point network that was based initially on Fully Meshed, Cloud or Hub and Spoke, you are in Free Form mode going forward when modifying the already existing Multi-Point network.

If you want to create a simple Point-to-Point network, you typically use the **Point To Point Designer** page (see *Creating Point-to-Point Networks (Examples)* on page 265 in *Chapter 9*, *Creating and Running Point-to-Point Networks*). However, Point-to-Point type networks have a simplified type of routing (called Link Qualifications). If you require a simple Point-to-Point network topology to be emulated with more complex routing (i.e. not using the more basic Link Qualifications), you could do either one of the following:

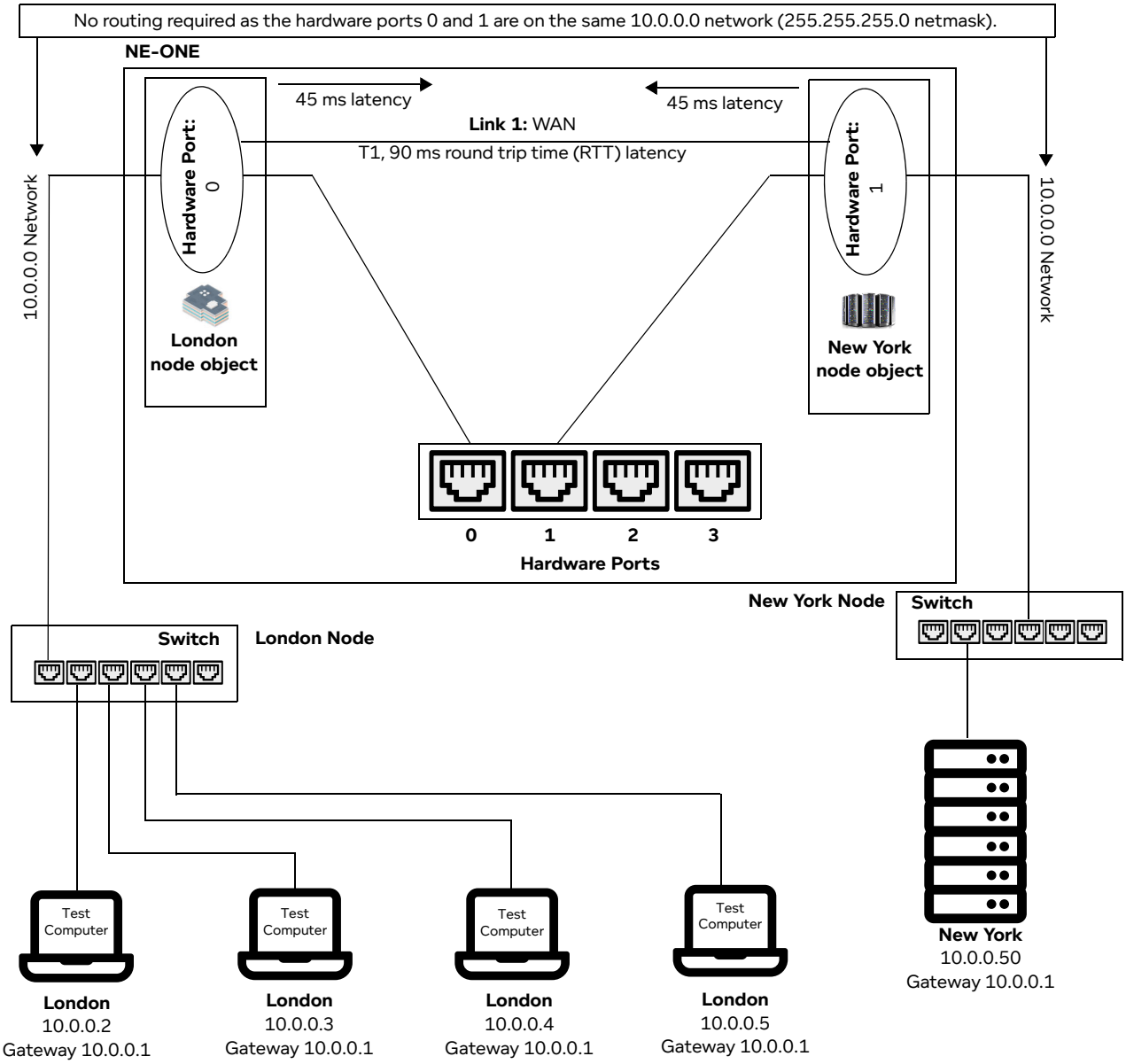
- Initially use the **Point To Point Designer** page to create a Point-to-Point type network. Then use the **EXPORT TO MULTI-POINT** button in the **Point To Point Designer** page to convert the Point-to-Point type network to a Multi-Point type network. From this point on, the network only can be opened in the **Multi-Point Designer** page, where it can be adapted with more complex routing functions, etc.
- Immediately use the **Multi-Point Designer** page, choosing the Free Form template, and building the Point-to-Point network topology from scratch.

The following sub-sections describe creating a simple impaired wire (bridge) network; one with two nodes (with no routing), and one with three nodes (with no routing), and two interface routed network, using IPv4 soft ports.

4-1-1. Building a Simple Impaired Wire (Bridged) Network (no routing)

In this example we look at the simplest single hop Point-to-Point network with no routing. We call this a 2 Interface Simple Impaired Wire Network (i.e. in network speak a two port "Bridged" network), as it behaves just like a piece of Ethernet Cable or Fiber with the addition of impairments or restrictions. In this configuration the rest of the network does not "know" that the NE-ONE is present, as we show no IP addresses or Ethernet addresses (except for the management port). This is the easiest way to insert the NE-ONE into an existing environment, but does require it to be placed in-line at some point in the test network, which will require the network to be re-plugged, at that time.

ILLUSTRATION 115 - SIMPLE IMPAIRED WIRE (BRIDGED) WAN LINK ON THE SAME NETWORK



In our example (see *Illustration 115*) we assume that the servers are in New York, the clients in London and a T1 (1.544 Mbps) symmetric link between the two with 90 ms round trip latency (RTT).

Note:
For this example, an admin user must have assigned the hardware ports 0 and 1 to the account of the non-admin user creating the Multi-Point network. For more information on hardware port to a non-admin user, see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205 in *Chapter 10,User Administration*.

Use the following steps to create a Free Form based Multi-Point network based on the Simple Impaired Wire example described above:

1. Launch the **Multi-Point Designer** page, and choose the Free Form network topology template, using the following sub-steps:
   a. Select **Networks** from the Menu.
   b. From the **Networks** page (see *Illustration 4* on page 42) that appears, click **New Network**.
   c. From the **Network Wizard** page (see *Illustration 84*) that appears, in the **Free Form** panel, click **CREATE**.
   d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`New York - London (Simple Impaired Wire)`**), then click **OK**.

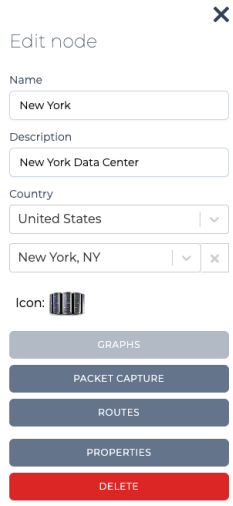
   A new (i.e. undefined) Multi-Node network appears based on the selected Free Form network topology template you selected. At this stage, the Workspace is empty, and nothing is configured in the network.
2. From the **Multi-Point Designer** page, optionally tick the **Show node names**, **Show link names**, and **Show node ports** check boxes from the **VIEW** drop-down menu.

   Note: This optional step is useful in letting you identify what still needs configuring in the Multi-Point network. Undefined nodes have the generic names **node0**, **node1**, etc. Undefined links have the format **node0<-->node1**, etc. End nodes with undefined input and output ports show nothing.
3. Create the New York node on the Workspace. To do this, from the **Node Icons** panel, drag an appropriate icon (for example a data center icon from within the **Legacy NEONE** tab) into the right hand side area of the Workspace. For more information, see *Creating Nodes in the Workspace* on page 318.
4. Define the New York node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:
   a. In the **Name** field, type **`New York`**.
   b. In the **Description** field, type **`New York Data Center`**.
   c. From the **Country** drop-down field, select **United States**.

      Note: You can start typing the word `united` in order to select **United States** quickly from the list of countries.
   d. From the **Choose a location** drop-down field, select **New York, NY**.

      Note: You can start typing the location in order to select it quickly from the list of locations.

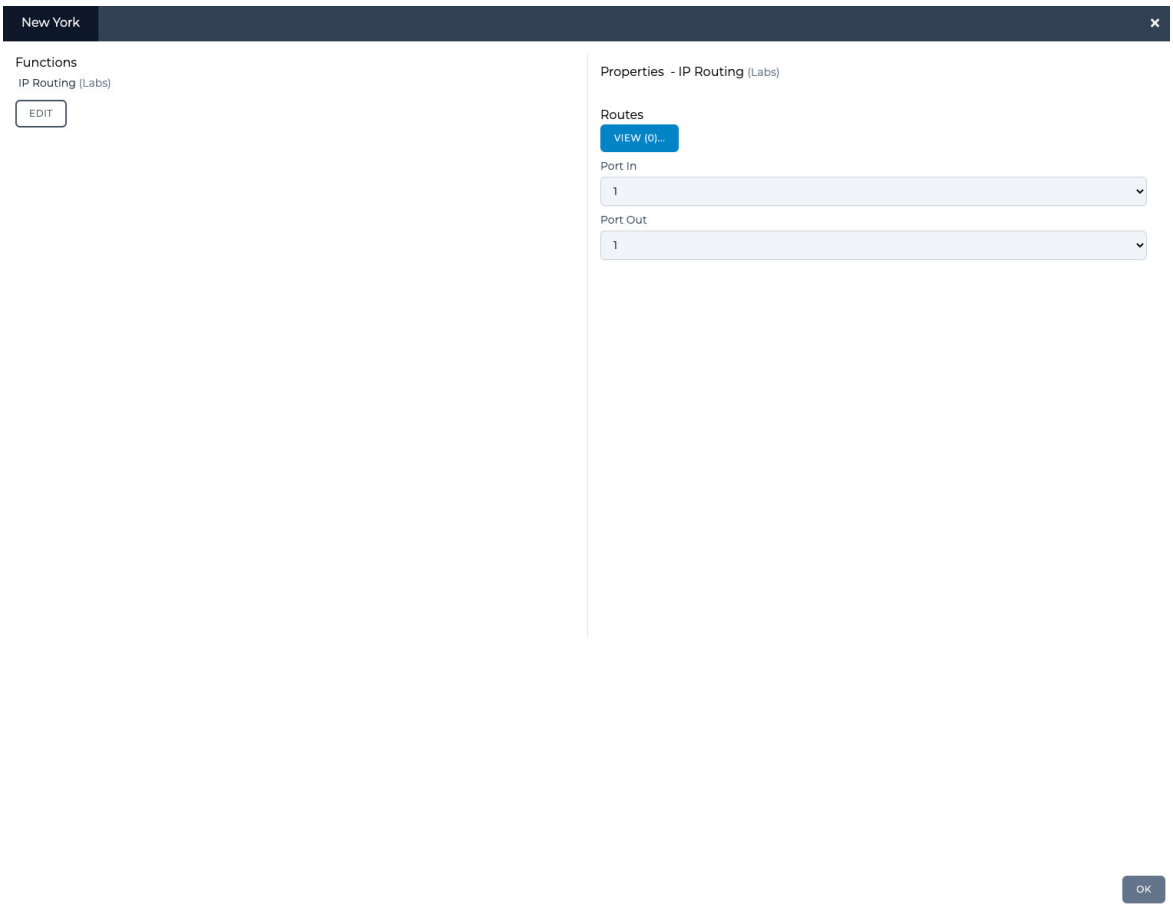
The **Edit node** panel now looks as follows.



At this stage you now need to assign hardware port 1 to the New York node.

e. Click on the **Routes** button.

A **New York - Routing Properties** window appears, letting you define the New York node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down field is set to **None**.



f. In **Port In** drop-down field of the **New York - Routing Properties** window, select an appropriate

input port for the New York node. In our example, select **1**, which represents the hardware port 1 of the NE-ONE.

g. In **Port Out** drop-down field of the **New York - Routing Properties** window, select an appropriate output port for the New York node. In our example, select **1**, which represents the hardware port 1 of the NE-ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

i. Click to ✕ close the **Edit node** panel.

5. Create the London node on the Workspace. To do this, from the **Node Icons** panel, drag an appropriate icon (for example a building icon from within the **Legacy NEONE** tab) into the left hand side area of the Workspace. For more information, see *Creating Nodes in the Workspace* on page 318.

6. Define the London node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:

a. In the **Name** field, type **`London`**.

b. In the **Description** field, type **`London Test Center`**.

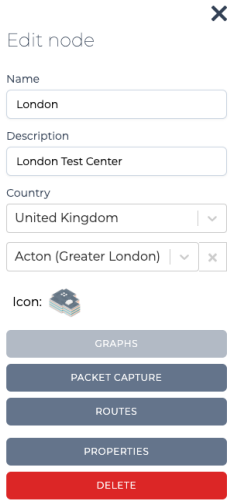
c. From the **Country** drop-down field, select **United Kingdom**.

Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

d. From the **Choose a location** drop-down field, select **Acton (Greater London)**.

Note: You can start typing the location in order to select it quickly from the list of locations.

The **Edit node** panel now looks as follows.

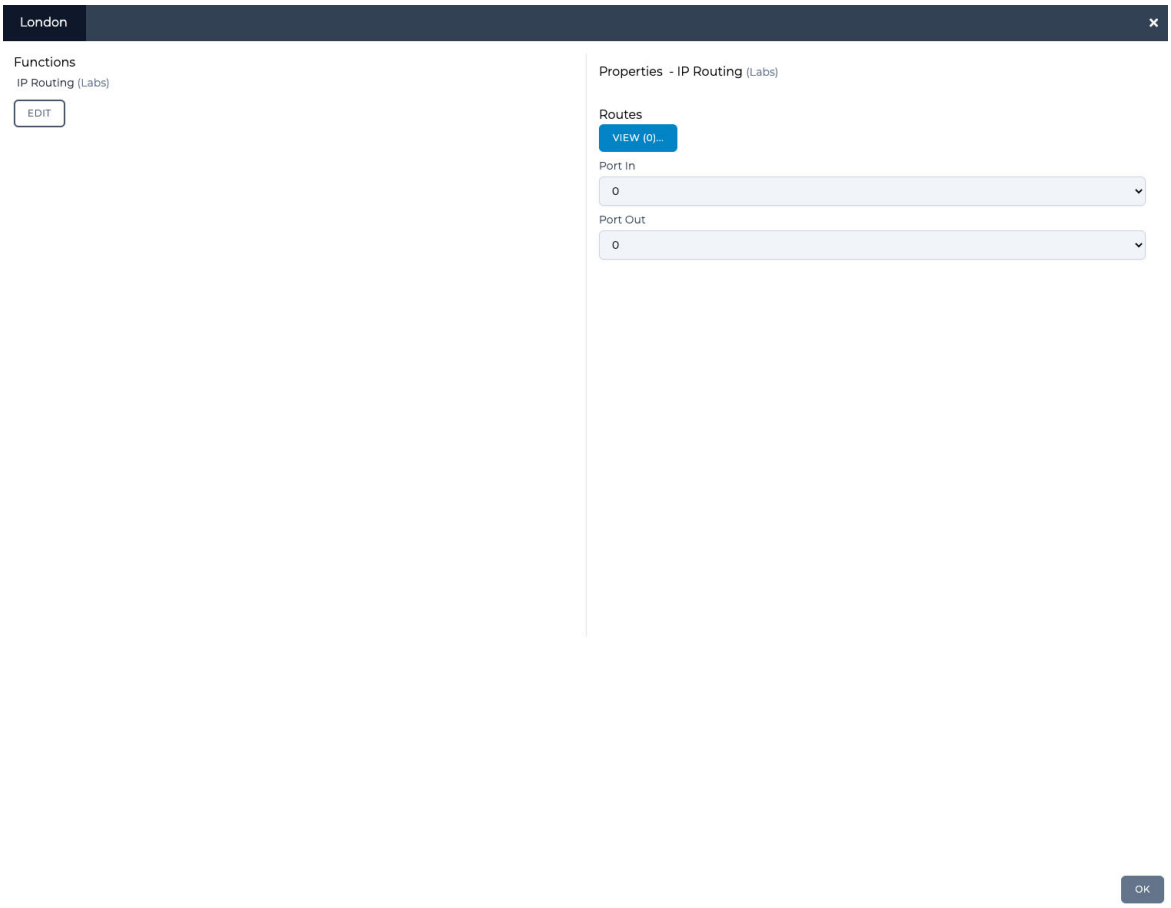


At this stage you now need to assign hardware port 0 to the London node.

e. Click on the **Routes** button.

A **London** routing properties window appears, letting you define the New York node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down

field is set to **None**.



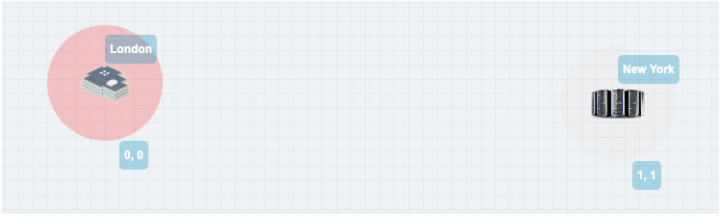
f. In **Port In** drop-down field of the **London** routing properties window, select an appropriate input port for the New York node. In our example, select **0**, which represents the hardware port 0 of the NE-ONE.

g. In **Port Out** drop-down field of the **London** routing properties window, select an appropriate input port for the New York node. In our example, select **0**, which represents the hardware port 0 of the NE-ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

i. Click to ✕ close the **Edit node** panel.

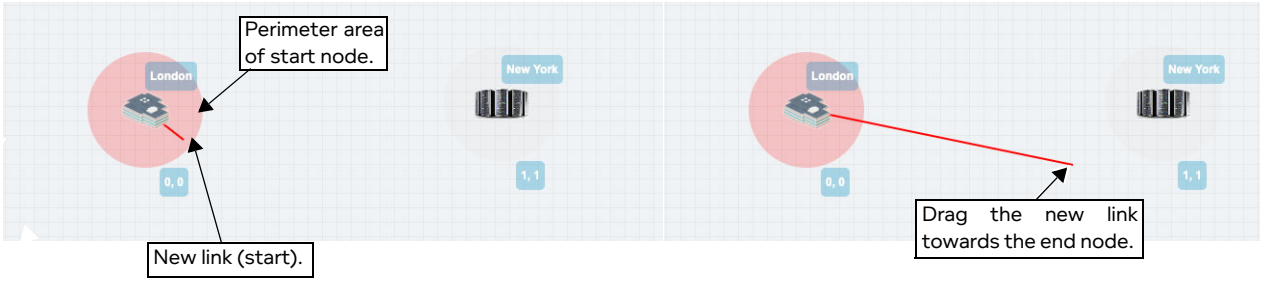
At this stage, the two nodes London and New York exist on the Work Space with no link.



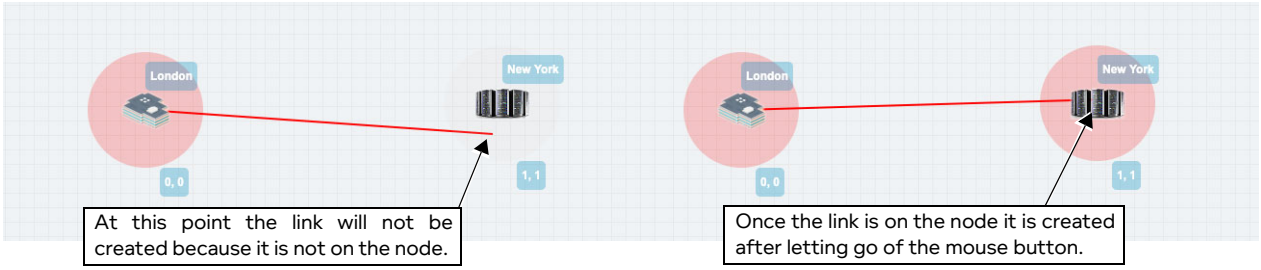
7. Create a link between the London and New York nodes, going from starting from the London (left side) to New York (right side). To do this, do the following:

   a. On the London node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).

A red line representing the new link appears within the perimeter area of the London node.



b. Continue dragging the link into the perimeter area of the New York node (considered the right node), and position the end of the link onto the icon of the New York node.



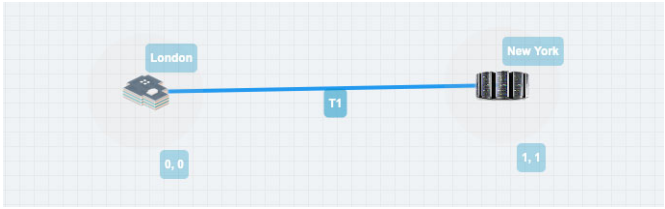
Note: If you do not position the end of the link on the icon of the New York node, the link is not created. Ensure that you position the end of the link on the icon of the New York node before letting go of the mouse button.

c. Once the end of the link is on the icon of the New York node, let go of the mouse button.

A **Link Name** dialog box appears.

d. From the **Link Name** dialog box that appears, type **`T1`**, then click **OK**.

At this stage the newly created and named **T1** link appears between the London and New York nodes.



The newly created **T1** link now needs configuring.

8. In the Workspace, click on the **T1** link, and from the **Edit link** panel that appears click the **EDIT** button.

A **Link** page appears.

9. From the **Link** page that appears, do the following:

a. Leave the **Name** field unchanged as it inherits the name you originally specified when you created the link.

b. In the **Description** field, type a **`T1 - Poor`**.

c. From the **Type** drop-down field, select **WAN**.

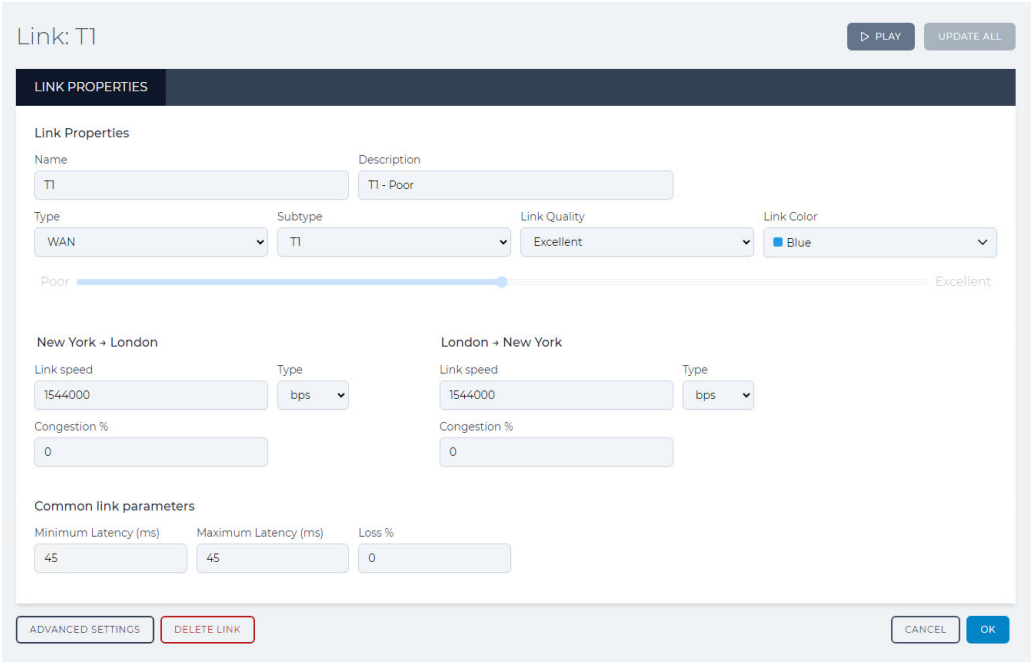
d. From the **Subtype** drop-down field, select **T1**.

e. From the **Link Quality** drop-down field, select **Excellent**. This setting automatically updates the **Minimum Latency (ms)** field to 7, the **Maximum Latency (ms)** field to 12, and the **Loss %** field to 0. This is a useful setting to select, as the **Loss %** field is set to 0, which will not change. You will only modify the values of the **Minimum Latency (ms)** field and **Maximum Latency (ms)** field.

f. From the **Link Color** drop-down field, leave the color set to **Blue**.

g. In the **Minimum Latency (ms)** field specify **45** (this will create the 90 ms round trip latency).

h. In the **Maximum Latency (ms)** field specify **45** (this will create the 90 ms round trip latency).



i. Click **OK** to submit the link properties.

You are returned to the Workspace in the **Multi-Point Designer** page.

10. Save the finalized Free Form Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

The Free Form Multi-Point network is ready to be run (i.e. played). You now have a Multi-Point network that does the following:

- On London node object, take data from hardware port 0 to hardware port 1 and apply a link speed limit of 1544000 bps and a latency (fixed of 45 ms).
- On New York node object, take data from hardware port 1 to hardware port 0 and apply a link speed limit of 1544000 bps and a latency (fixed of 45 ms).

When connecting equipment to the NE-ONE connect the London equipment to port #0 and the New York equipment to port #1 (ports 0 and 1 in the example in *Illustration 115* on page 374).

4-1-2. Building a Simple Impaired Wire (Bridged) Network (with Routing and Map)

In this example we expand upon the original example of *Section 4-1-1*, where an additional test center node exists in Rio de Janeiro, connected to the New York data center. The New York data center node now requires routing to support the traffic to/from the links of London and Rio de Janeiro nodes.

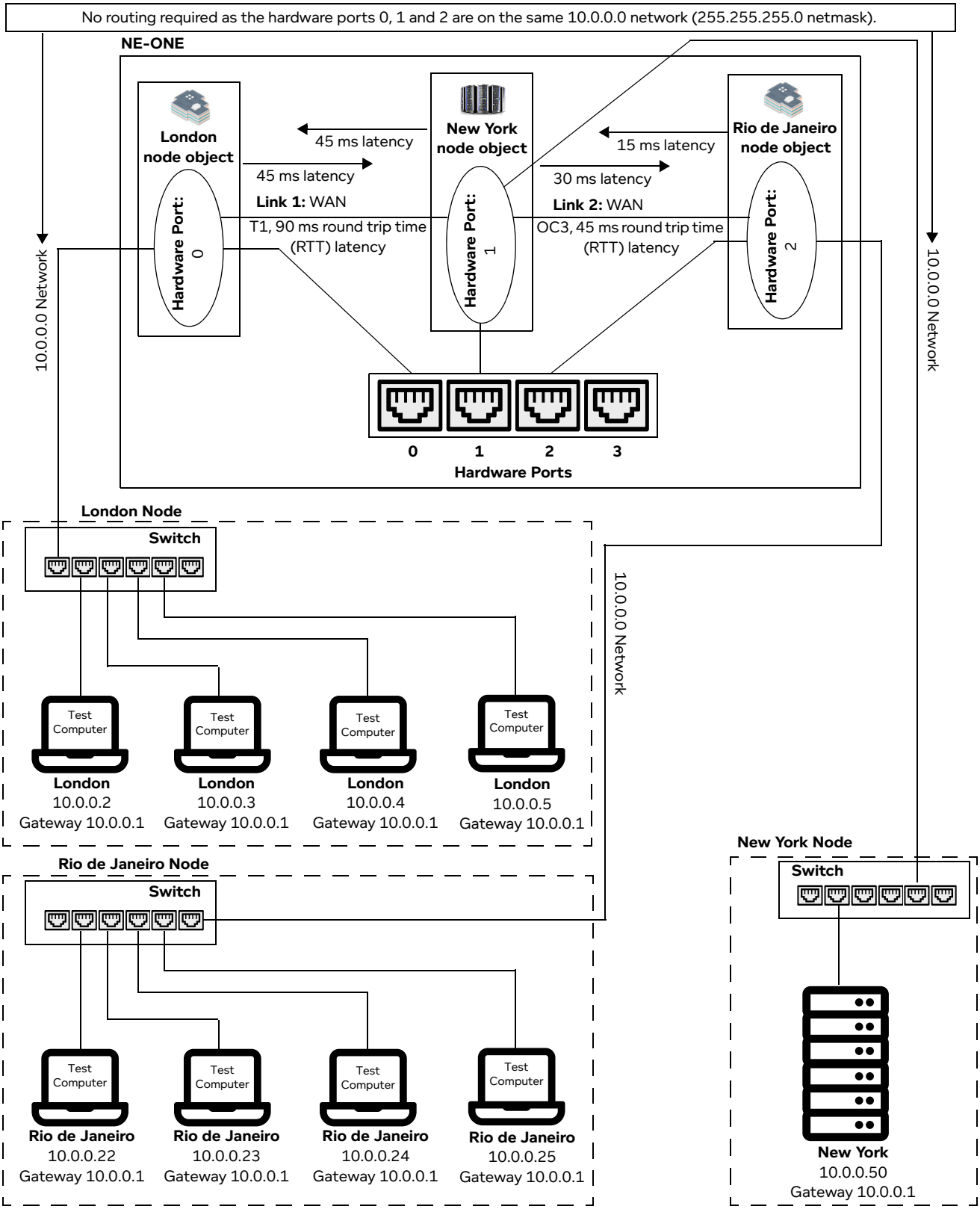
In our example (see *Illustration 116* on page 382) we assume that the servers are in New York, and the clients from:

- London are on a T1 (1.544 Mbps) symmetric link between the two with 90 ms round trip latency time (RTT).
- Rio de Janeiro are on an OC3 (155.52 Mbps) asymmetric link with different latencies 45 ms round trip latency time (RTT) (15 ms in the Rio de Janeiro to New York traffic direction, and 30 ms in the New York to Rio de Janeiro traffic direction)

Note:

For this example, an admin user must have assigned the hardware ports 0, 1, and 2 to the account of the non-admin user creating the Multi-Point network. For more information on assigning hardware ports to a non-admin user, see *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205 in *Chapter 10*,*User Administration*.

ILLUSTRATION 116 - SIMPLE IMPAIRED WIRE (BRIDGED) WAN LINK ON THE SAME NETWORK



Use the following steps to create a Free Form based Multi-Point network based on the Simple Impaired Wire example described above (*Illustration 116* on page 382):

1. Launch the **Multi-Point Designer** page, and choose the Free Form network topology template, using the following sub-steps:
   a. Select **Networks** from the Menu.
   b. From the **Networks** page (see *Illustration 4* on page 42) that appears, click **New Network**.
   c. From the **Network Wizard** page (see *Illustration 84*) that appears, in the **Free Form** panel, click **CREATE**.
   d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London – New York (Simple Impaired Wire)`**), then click **OK**.

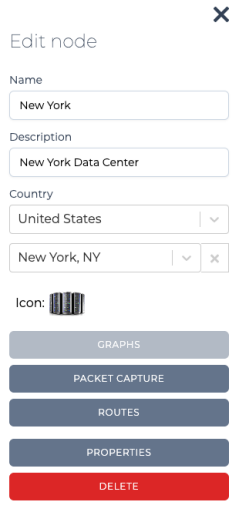
   A new (i.e. undefined) Multi-Node network appears based on the selected Free Form network topology template you selected. At this stage, the Workspace is empty, and nothing is configured in the network.
2. Load the world map in to the Workspace, as follows:
   a. Select **VIEW > Background**.
   b. From the window that appears, select the **world_map_blue_grey.png** file, and click **OK**.
   c. Manipulate the size and position of the map according to your needs (for more detailed information on how to do this, see *The Workspace Background Image* on page 314).
3. From the **Multi-Point Designer** page, optionally tick the **Show node names**, **Show link names**, and **Show node ports** check boxes from the **VIEW** drop-down menu.

   Note: This optional step is useful in letting you identify what still needs configuring in the Multi-Point network. Undefined nodes have the generic names **node0**, **node1**, etc. Undefined links have the format **node0<-->node1**, etc. End nodes with undefined input and output ports show nothing.
4. Create the New York node on the Workspace. To do this, from the **Node Icons** panel, drag an appropriate icon (for example a data center icon from within the **Legacy NEONE** tab) into the left hand side area of the Workspace, on the United States part of the world map. For more information, see *Creating Nodes in the Workspace* on page 318.
5. Define the New York node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:
   a. In the **Name** field, type **`New York`**.
   b. In the **Description** field, type **`New York Data Center`**.
   c. From the **Country** drop-down field, select **United States**.

      Note: You can start typing the word `united` in order to select **United States** quickly from the list of countries.
   d. From the **Choose a location** drop-down field, select **New York, NY**.

      Note: You can start typing the location in order to select it quickly from the list of locations.

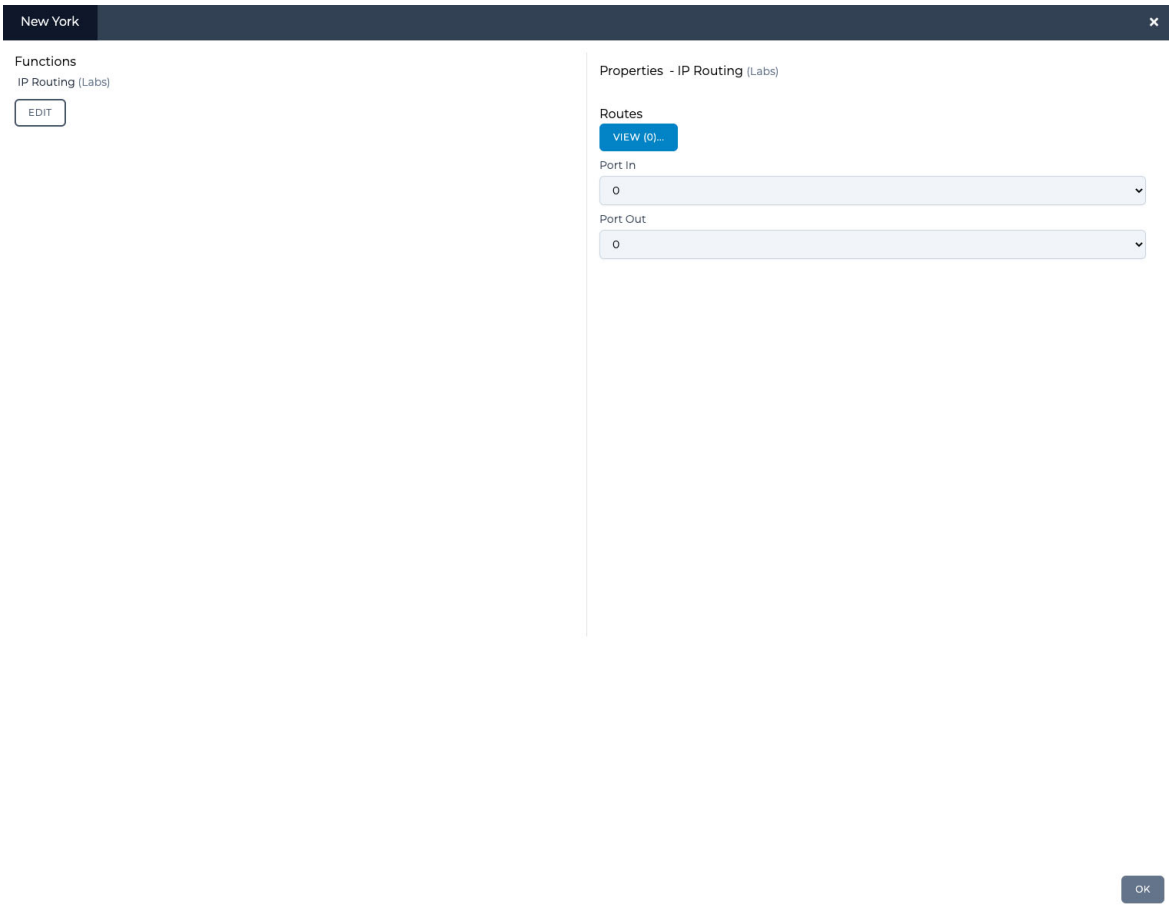
The **Edit node** panel now looks as follows.



At this stage you now need to assign hardware port 0 to the New York node.

e. Click on the **Routes** button.

A **New York - Routing Properties** window appears, letting you define the New York node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down field is set to **None**.



f. In **Port In** drop-down field of the **New York - Routing Properties** window, select an appropriate

input port for the New York node. In our example, select **0**, which represents the hardware port 0 of the NE-ONE.

g. In **Port Out** drop-down field of the **New York - Routing Properties** window, select an appropriate output port for the New York node. In our example, select **0**, which represents the hardware port 0 of the NE-ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

i. Click to ✕ close the **Edit node** panel.

6. Create the London node on the Workspace. To do this, from the **Node Icons** panel, drag an appropriate icon (for example a building icon from within the **Legacy NEONE** tab) into the right hand side area of the Workspace on the United Kingdom part of the world map. For more information, see *Creating Nodes in the Workspace* on page 318.

7. Define the London node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:

a. In the **Name** field, type **`London`**.

b. In the **Description** field, type **`London Test Center`**.

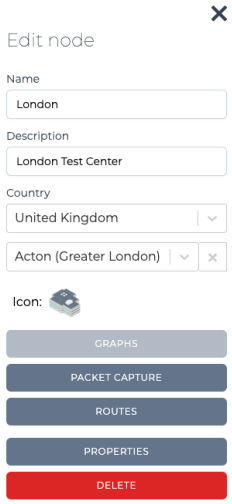
c. From the **Country** drop-down field, select **United Kingdom**.

Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

d. From the **Choose a location** drop-down field, select **Acton (Greater London)**.

Note: You can start typing the location in order to select it quickly from the list of locations.

The **Edit node** panel now looks as follows.

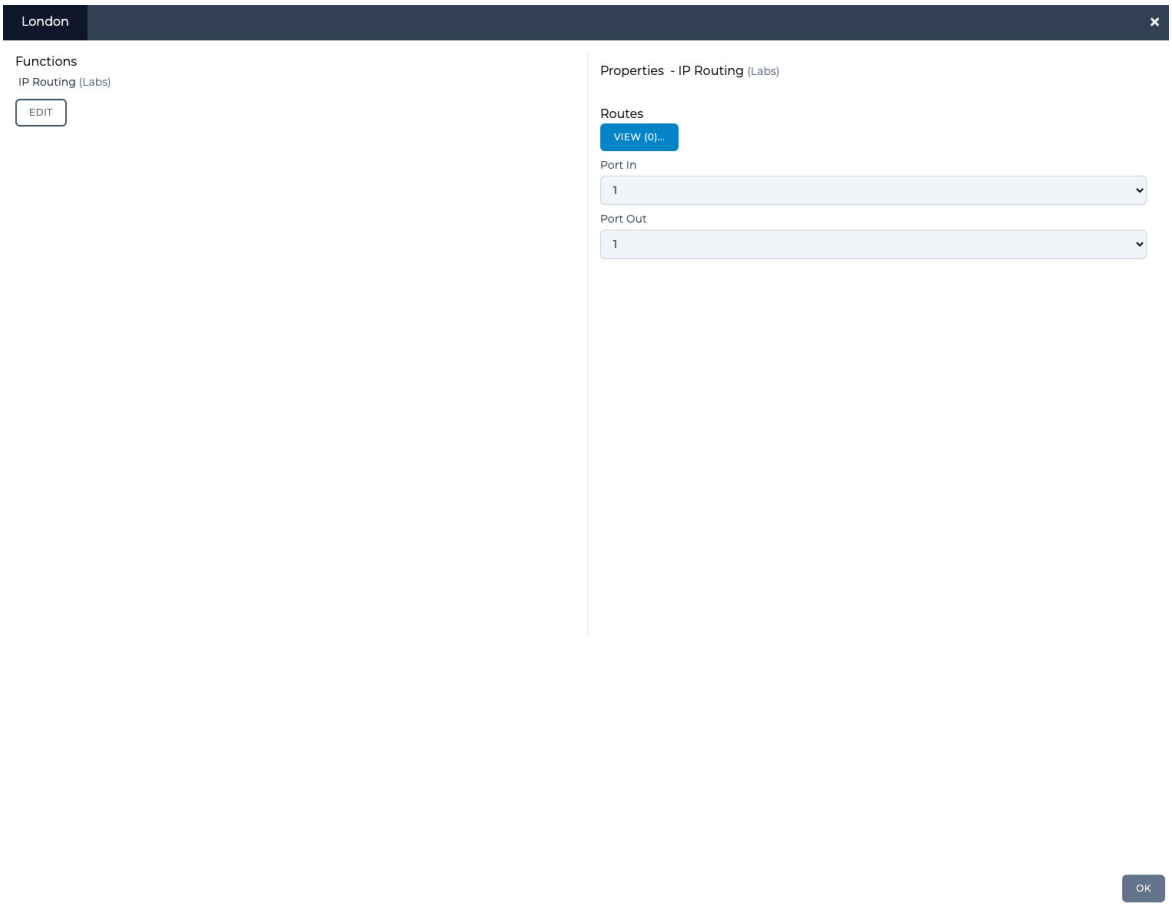


At this stage you now need to assign hardware port 1 to the London node.

e. Click on the **Routes** button.

A **London** routing properties window appears, letting you define the New York node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down

field is set to **None**.



f. In **Port In** drop-down field of the **London** routing properties window, select an appropriate input port for the New York node. In our example, select **1**, which represents the hardware port 1 of the NE-ONE.

g. In **Port Out** drop-down field of the **London** routing properties window, select an appropriate input port for the New York node. In our example, select **1**, which represents the hardware port 1 of the NE-ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

i. Click to ✕ close the **Edit node** panel.

8. Create the Rio de Janeiro node on the Workspace. To do this, from the **Node Icons** panel, drag an appropriate icon (for example a building icon from within the **Legacy NEONE** tab) into the left hand side area of the Workspace on the Brazil part of the world map. For more information, see *Creating Nodes in the Workspace* on page 318.

9. Define the Rio de Janeiro node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:

a. In the **Name** field, type **`Rio de Janeiro`**.

b. In the **Description** field, type **`Rio de Janeiro Center`**.

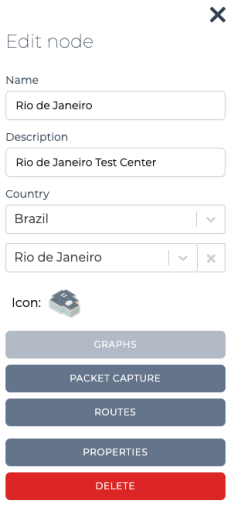
c. From the **Country** drop-down field, select **Brazil**.

Note: You can start typing the word `brazil` in order to select **Brazil** quickly from the list of countries.

d. From the **Choose a location** drop-down field, select **Rio de Janeiro**.

Note: You can start typing the location in order to select it quickly from the list of locations.

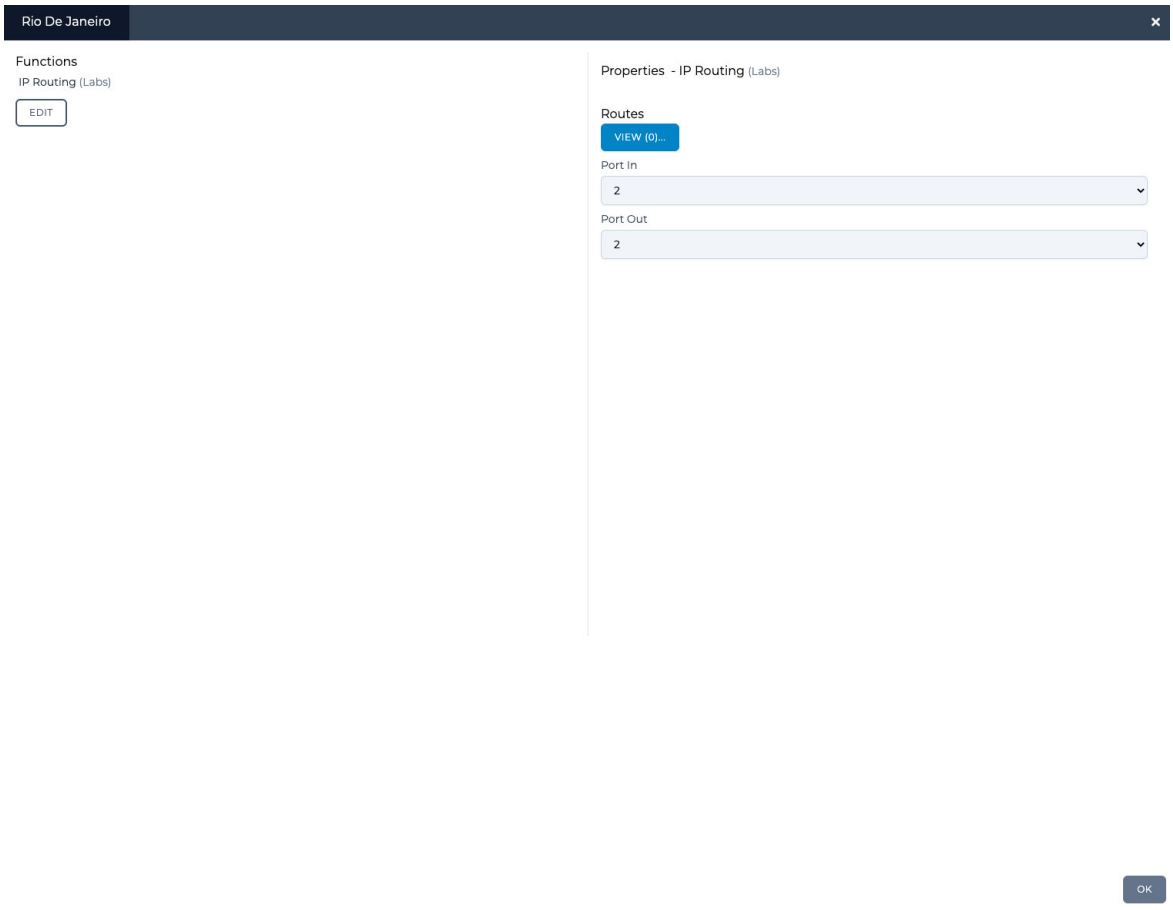
The **Edit node** panel now looks as follows.



At this stage you now need to assign hardware port 2 to the Rio de Janeiro node.

e. Click on the **Routes** button.

A **Rio De Janeiro** routing properties window appears, letting you define the New York node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down field is set to **None**.



f. In **Port In** drop-down field of the **Rio de Janeiro** routing properties window, select an appropriate input port for the New York node. In our example, select **2**, which represents the hardware port 2 of the NE-ONE.

g. In **Port Out** drop-down field of the **Rio de Janeiro** routing properties window, select an appropriate input port for the New York node. In our example, select **2**, which represents the hardware port 2 of the NE-ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

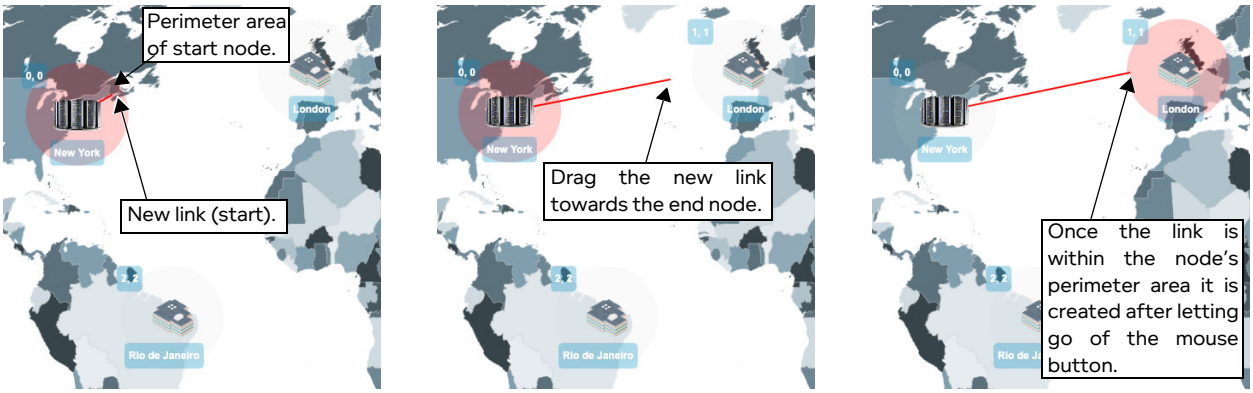
i. Click to ✕ close the **Edit node** panel.

At this stage, the three nodes London, New York and Rio de Janeiro exist on the Work Space with no links.

10. Create a link between the New York and London nodes, going from starting from the New York (left side) to London (right side). To do this, do the following:

a. On the New York node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).

A red line representing the new link appears within the perimeter area of the New York node.



b. Continue dragging the link into the perimeter area of the London node (considered the right node).

c. Once the end of the link is in the perimeter area of the London node, let go of the mouse button.

A **Link Name** dialog box appears.

d. From the **Link Name** dialog box that appears, type **`T1`**, then click **OK**.

At this stage the newly created and named **T1** link appears between the New York and London nodes.

The newly created **T1** link now needs configuring.

11. In the Workspace, click on the **T1** link, and from the **Edit link** panel that appears click the **EDIT** button.

    A **Link:T1** page appears.

12. From the **Link:T1** page that appears, do the following:

    a. Leave the **Name** field unchanged as it inherits the name you originally specified when you created the link.

    b. In the **Description** field, type a **`T1 - Poor`**.

    c. From the **Type** drop-down field, select **WAN**.

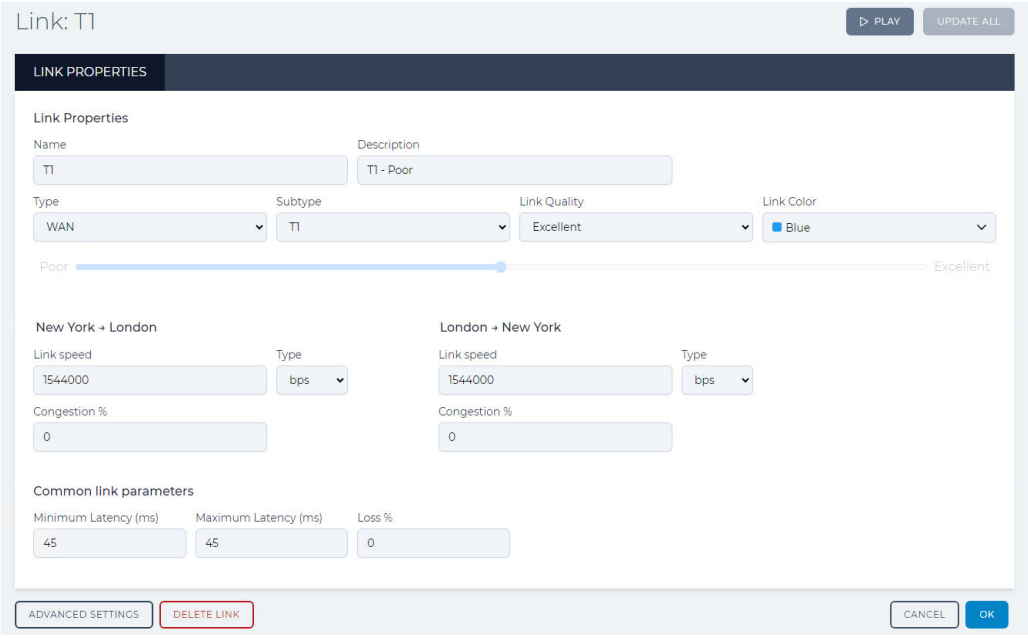
    d. From the **Subtype** drop-down field, select **T1**.

    e. From the **Link Quality** drop-down field, select **Excellent**. This setting automatically updates the **Minimum Latency (ms)** field to 7, the **Maximum Latency (ms)** field to 12, and the **Loss %** field to 0. This is a useful setting to select, as the **Loss %** field is set to 0, which will not change. You will only modify the values of the **Minimum Latency (ms)** field and **Maximum Latency (ms)** field.

    f. From the **Link Color** drop-down field, leave the color set to **Blue**.

    g. In the **Minimum Latency (ms)** field specify **`45`** (this will create the 90 ms round trip latency).

    h. In the **Maximum Latency (ms)** field specify **`45`** (this will create the 90 ms round trip latency).



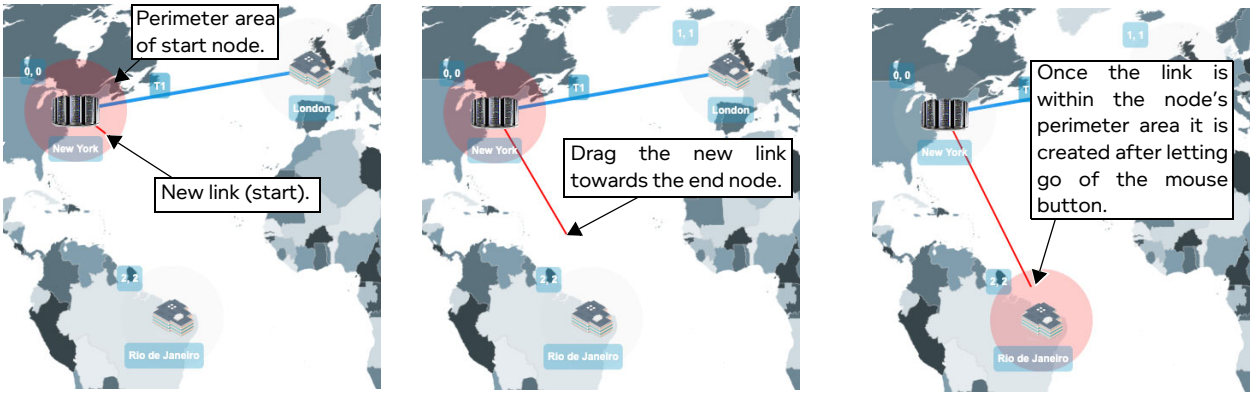
i. Click **OK** to submit the link properties.

You are returned to the Workspace in the **Multi-Point Designer** page.

13. Create a link between the New York and Rio de Janeiro nodes, going from starting from the New York (left side) to Rio de Janeiro (right side). To do this, do the following:

a. On the New York node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).

A red line representing the new link appears within the perimeter area of the New York node.



b. Continue dragging the link into the perimeter area of the Rio de Janeiro node (considered the right node).

c. Once the end of the link is in the perimeter area of the Rio de Janeiro node, let go of the mouse button.

A **Link Name** dialog box appears.

d. From the **Link Name** dialog box that appears, type **OC3**, then click **OK**.

At this stage the newly created and named **OC3** link appears between the New York and Rio de Janeiro nodes.

The newly created **OC3** link now needs configuring.

14. In the Workspace, click on the **OC3** link, and from the **Edit link** panel that appears click the **EDIT** button.

A **Link:OC3** page appears.

15. From the **Link:OC3** page that appears, do the following:

a. Leave the **Name** field unchanged as it inherits the name you originally specified when you created the link.

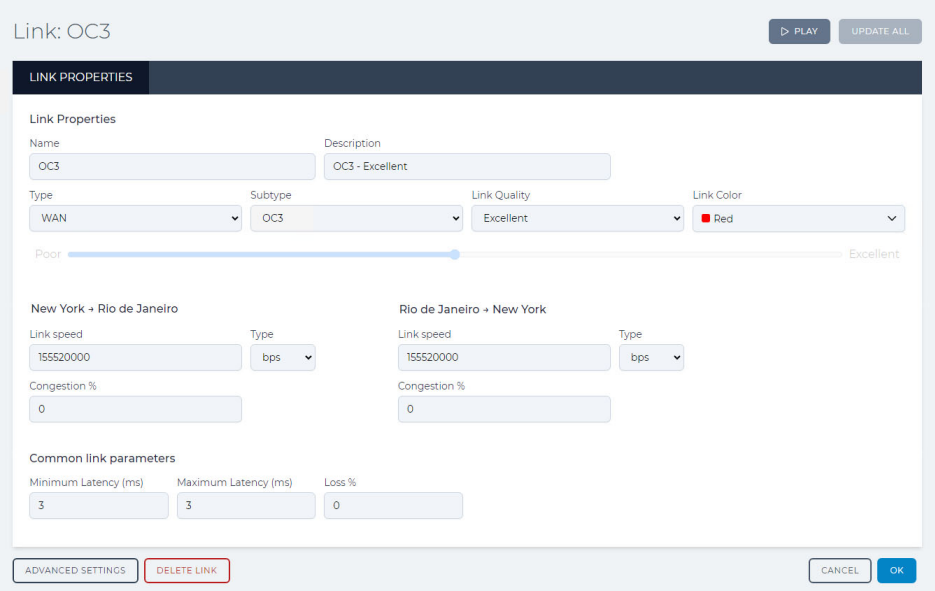
b. In the **Description** field, type a **`OC3 - Excellent`**.

c. From the **Type** drop-down field, select **WAN**.

d. From the **Subtype** drop-down field, select **OC3**.

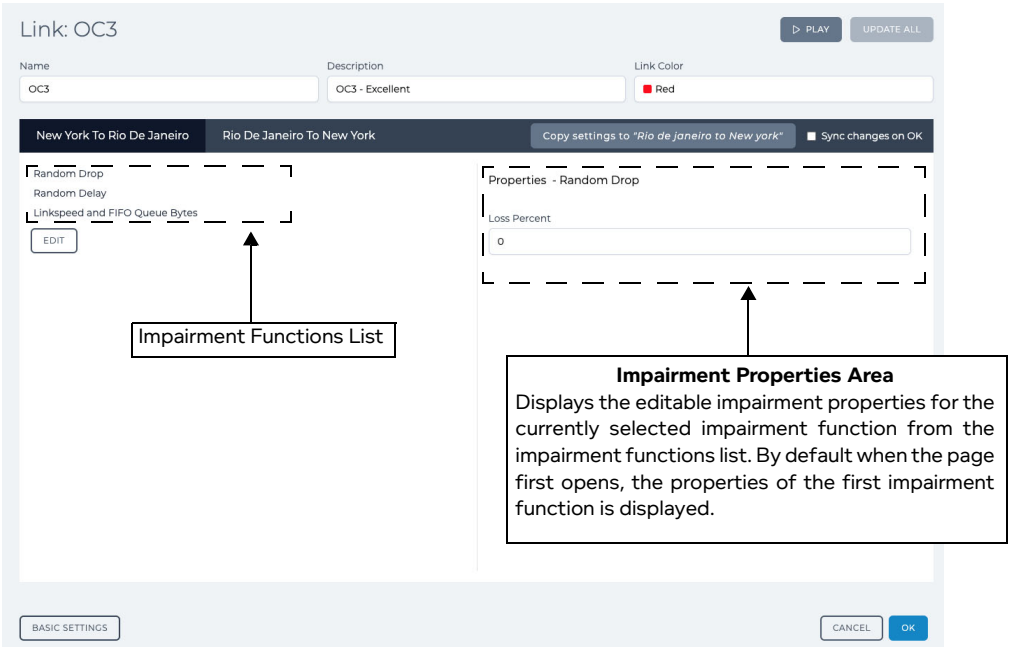
e. From the **Link Quality** drop-down field, select **Excellent**. This setting automatically updates the **Minimum Latency (ms)** field to 3, the **Maximum Latency (ms)** field to 3, and the **Loss %** field to 0. This is a useful setting to select, as the **Loss %** field is set to 0, which will not change. You will only modify the values of the **Minimum Latency (ms)** field and **Maximum Latency (ms)** field, but since these latency values will be asymmetrically applied, you will change them in the advanced settings of the link (which overrides the basic settings).

f. From the **Link Color** drop-down field, select the color **Red**.



g. Click the **ADVANCED SETTINGS** button.

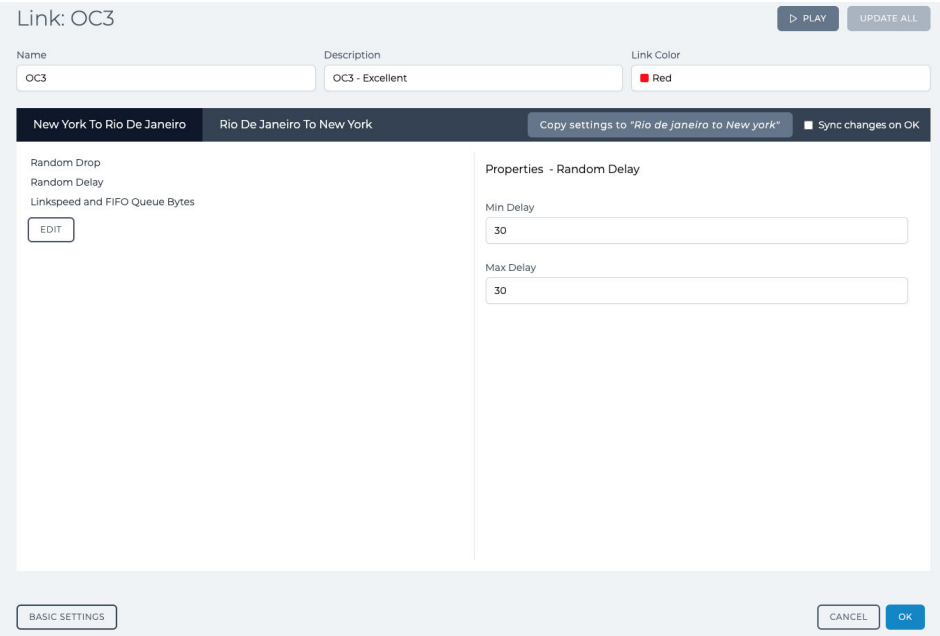
The **Advanced Settings** area of the **Link:OC3** page appears with the three default impairment functions for the New York to Rio de Janeiro direction, initially with the Random Drop value displayed (for our example, this remains unchanged with a value of 0%).



h. In the Impairment Functions List area, click on the **Random Delay** function from the list.

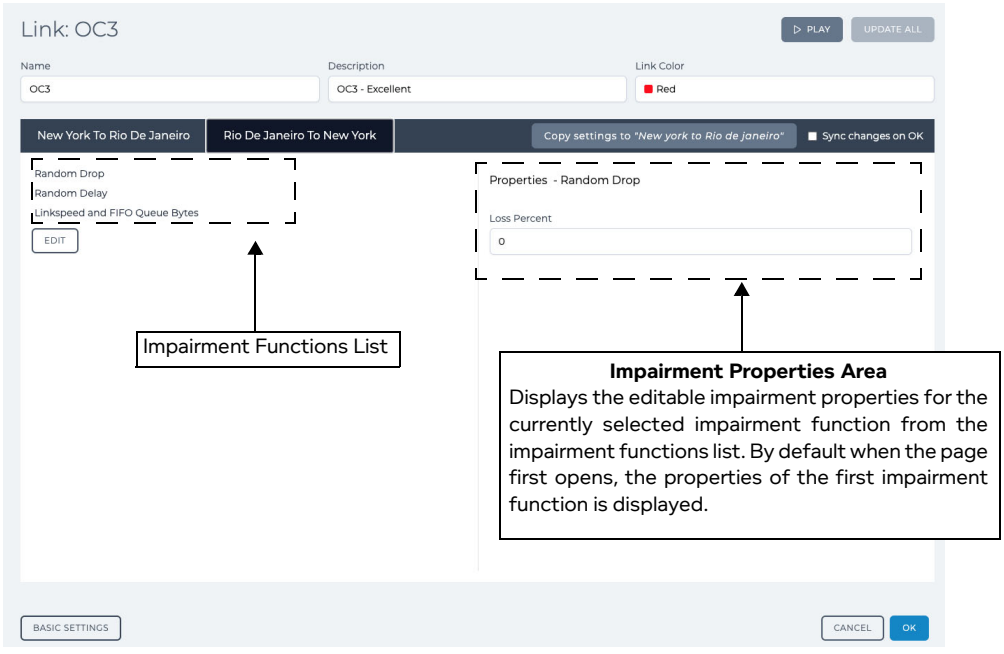
The Impairment Properties area updates with the parameter fields related to the Random Delay function (with default values of 3 ms for both maximum and minimum).

i. In the Impairment Properties area, specify **30** in the **Min Delay** field and specify in **30** in the **Min Delay** field. This will set a latency of 30 ms for the New York to Rio de Janerio traffic direction, as required in our example.



j. Click the **Rio De Janeiro To New York** tab to display the advanced properties for the Rio de Janeiro To New York Tab traffic direction.

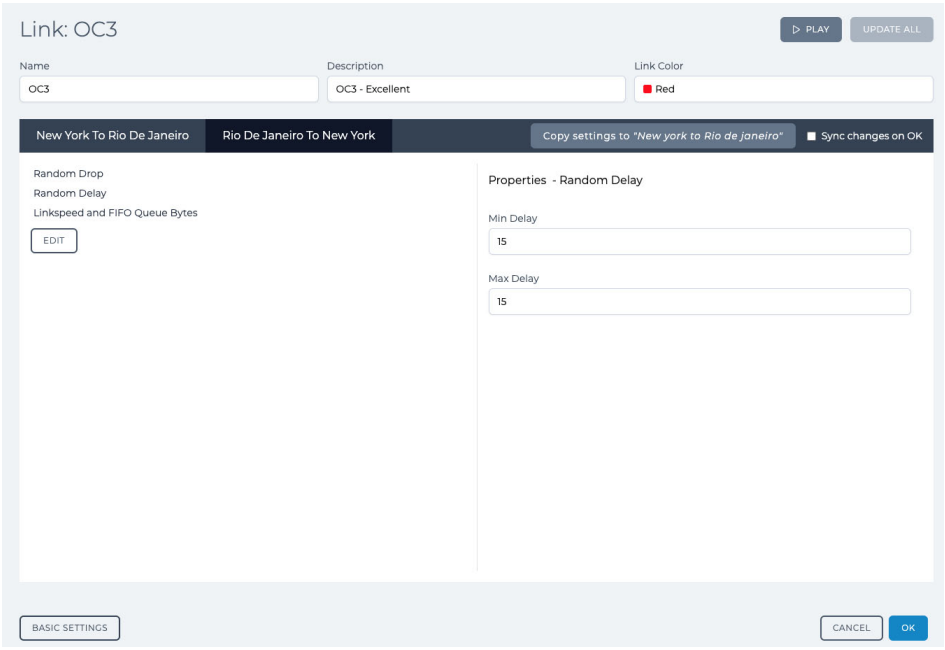
The **Advanced Settings** area of the **Link:OC3** page appears with the three default impairment functions for the New York to Rio de Janeiro direction, initially with the Random Drop value displayed (for our example, this remains unchanged with a value of 0%).



k. In the Impairment Functions List area, click on the **Random Delay** function from the list.

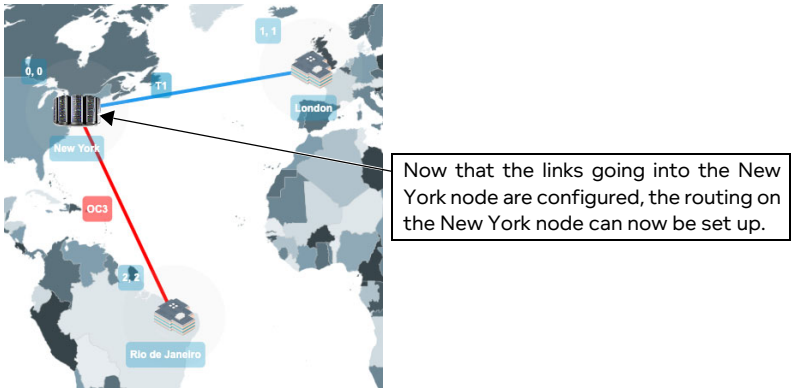
The Impairment Properties area updates with the parameter fields related to the Random Delay function (with default values of 3 ms for both maximum and minimum).

l. In the Impairment Properties area, specify **15** in the **Min Delay** field and specify in **15** in the **Min Delay** field. This will set a latency of 15 ms for the Rio de Janeiro to New York traffic direction, as required in our example.



m. Click **OK** to submit the link properties.

You are returned to the Workspace in the **Multi-Point Designer** page.



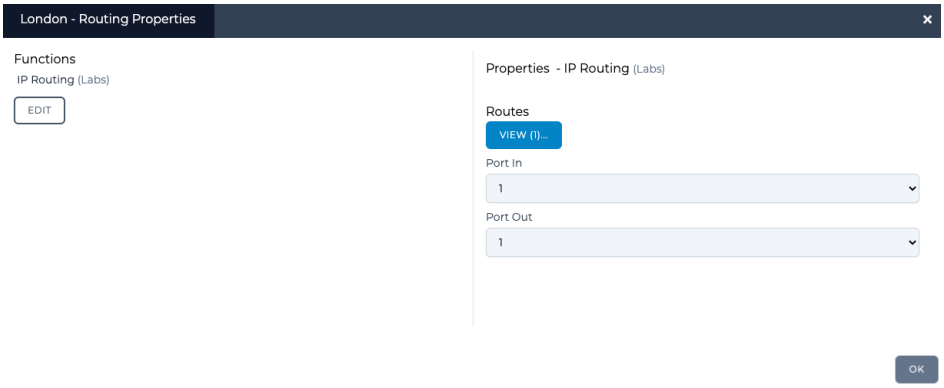
At this point, everything is configured, except for the routing on the New York node to support the traffic to/from the links of London and Rio de Janeiro nodes. Now that all the links exist, additional routing on the New York node can be configured, if required. In our example, no additional routing needs to be set up. When creating the links between New York and London, and New York and Rio de Janeiro, the NE-ONE intelligently created all the necessary default routing tables for each of the nodes.

In order to illustrate the routing tables automatically generated by the NE-ONE, the optional steps below describe how to view (but not modify) the routing tables that were automatically generated on each of the nodes.

16. Optionally view the London node's auto-generated routing table, as follows:

a. In the Workspace, click on the London node, then from the **Edit node** panel that appears, click the **ROUTES** button.

A **London - Routing Properties** window appears.



Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**1**), but the **Port Out** value is only used if no route is matched in the Routing table. You can examine the routing table by clicking on the **VIEW** button.

b. Click the **VIEW** button.

A **London - Routing Table** window appears.

We see that the NE-ONE intelligently and helpfully created a route (during the act of creating the link between New York and London in step 10). The routing works as follows:

If the packet originated on port 1 and matches the other conditions which, as they are all blank, it treats as wild cards so anything will do, then the packet is sent to the link object **T1** (London to New York direction). This is what we want – packets originating on port 1 the input port are sent down the link **T1**, any other packets do not match the routing rule and so are output on port 1. This means that packet coming down the link in the other direction i.e. from the link object **T1** (New York to London direction) will be output on port 1, as it originated on port 0 – again exactly what we want.

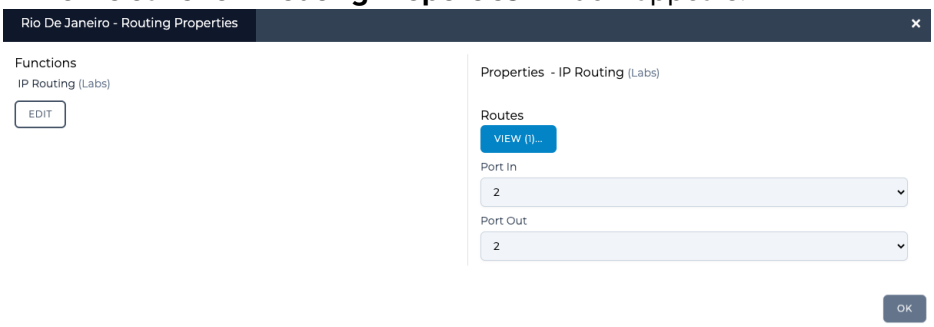
c. Click **DONE** to return to the **London - Routing Properties** window.

d. In the **London - Routing Properties** window, click **OK** to return to **Multi-Point Designer** page.

17. Optionally view the Rio de Janeiro node's auto-generated routing table, as follows:

a. In the Workspace, click on the Rio de Janeiro node, then from the **Edit node** panel that appears, click the **ROUTES** button.

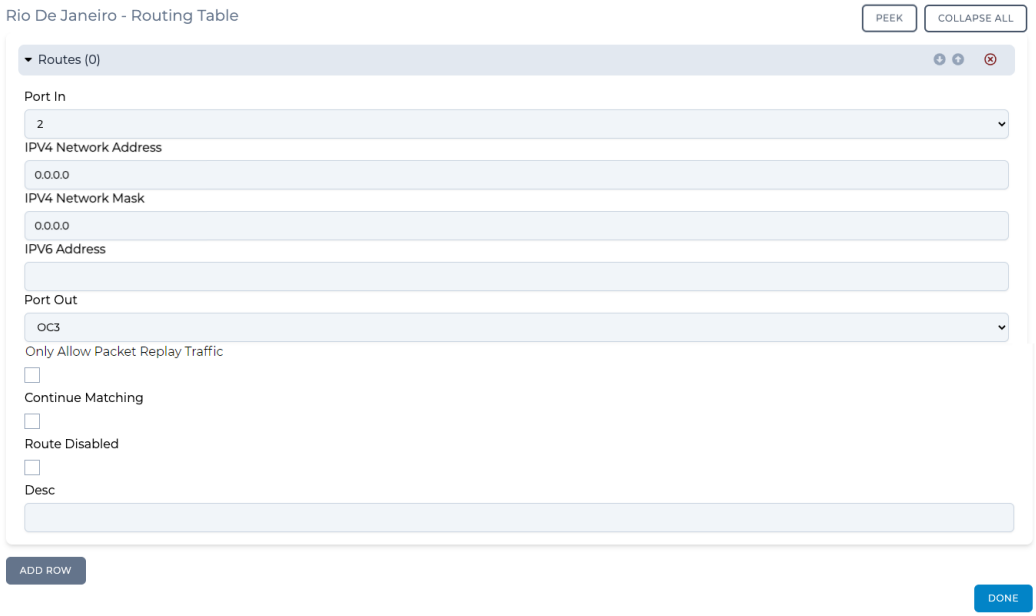
A **Rio De Janeiro - Routing Properties** window appears.



Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**2**), but the **Port Out** value is only used if no route is matched in the Routing table. You can examine the routing table by clicking on the **VIEW** button.

b. Click the **VIEW** button.

A **Rio De Janeiro - Routing Table** window appears.



We see that the NE-ONE intelligently and helpfully created a route (during the act of creating the link between New York and Rio de Janeiro in step 13). The routing works as follows:

If the packet originated on port 2 and matches the other conditions which, as they are all blank, it treats as wild cards so anything will do, then the packet is sent to the link object **OC3** (Rio de Janeiro to New York direction). This is what we want – packets originating on port 2 the input port are sent down the link **OC3**, any other packets do not match the routing rule and so are output on port 2. This means that packet coming down the link in the other direction i.e. from the link object **OC3** (New York to Rio de Janeiro direction) will be output on port 2, as it originated on port 0 – again exactly what we want.

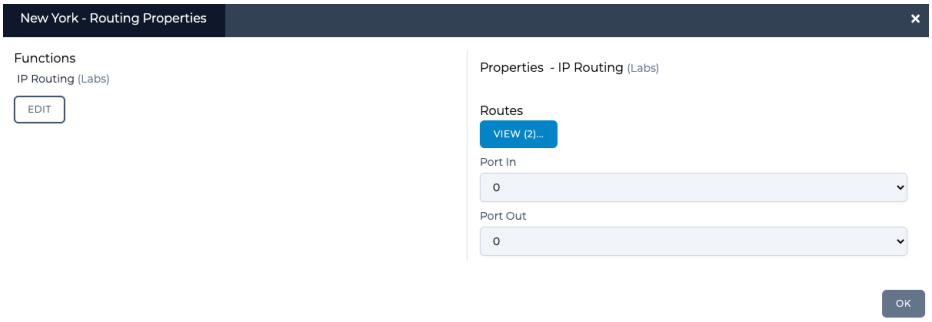
c. Click **DONE** to return to the **Rio De Janeiro - Routing Properties** window.

d. In the **Rio De Janeiro - Routing Properties** window, click **OK** to return to **Multi-Point Designer** page.

18. Optionally view the New York node's auto-generated routing table, as follows:

a. In the Workspace, click on the New York node, then from the **Edit node** panel that appears, click the **ROUTES** button.

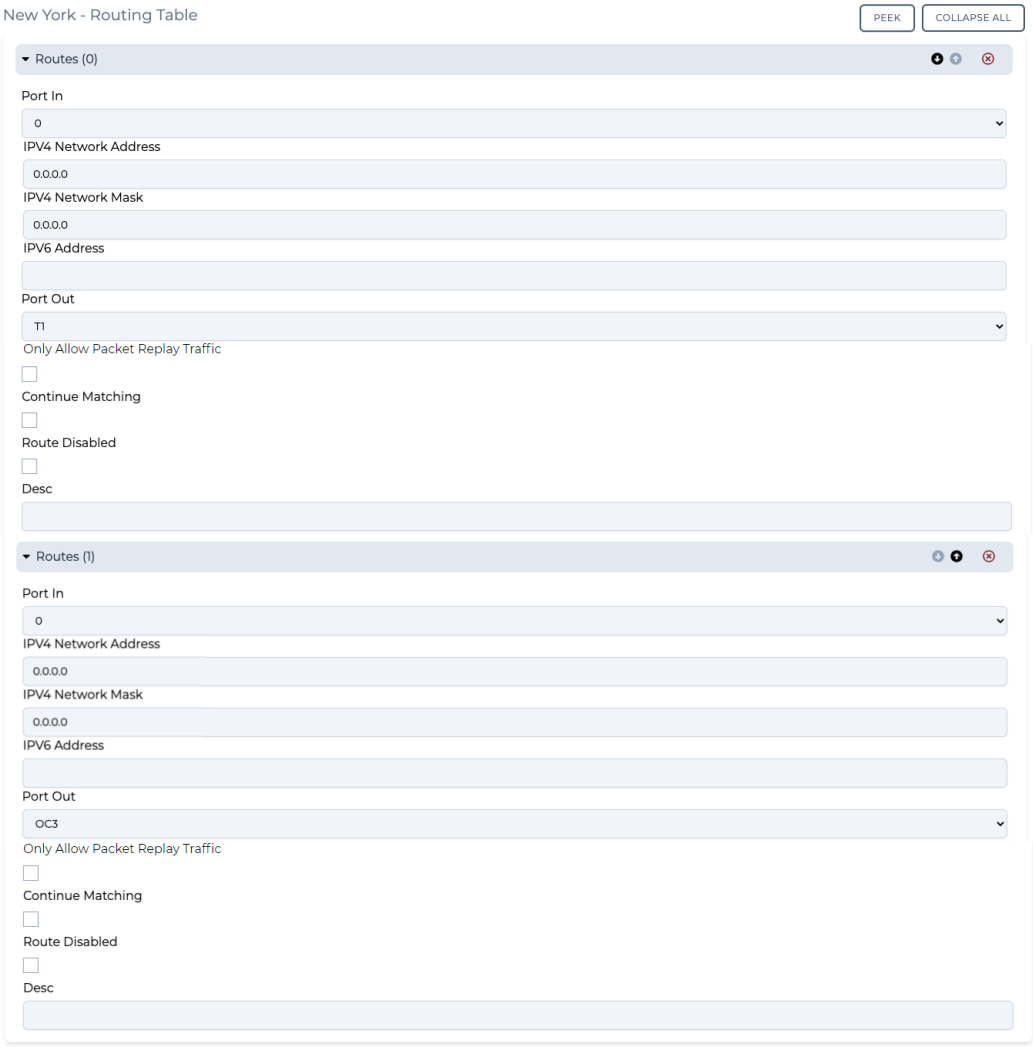
A **New York - Routing Properties** window appears.



Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**0**), but the **Port Out** value is only used if no route is matched in the Routing table. You can examine the routing table by clicking on the **VIEW** button.

b. Click the **VIEW** button.

A **New York - Routing Table** window appears.



We see that the NE-ONE intelligently and helpfully created a route (during the act of creating the links between New York and London in step 10 and New York and Rio de Janeiro in step 13). The routing works as follows:

If the packet originated on port 0 and matches the other conditions which, as they are all blank, it treats as wild cards so anything will do, then the packet is sent to the link object **T1** (New York to London direction). This is what we want – packets originating on port 0 the input port are sent up the link **T1**, any other packets do not match the routing rule and so are output on port 0. This means that packet coming up the link in the other direction i.e. from the link object **T1** (London to New York direction) will be output on port 0, as it originated on port 1 – again exactly what we want.

If the packet originated on port 0 and matches the other conditions which, as they are all blank, it treats as wild cards so anything will do, then the packet is sent to the link object **OC3** (New York to Rio de Janeiro direction). This is what we want – packets originating on port 0 the input port are sent up the link T1, any other packets do not match the routing rule and so are output on port 0. This means that packet coming up the link in the other direction i.e. from the link object **OC3** (Rio de Janeiro to New York direction) will be output on port 0, as it originated on port 2 – again exactly what we want.

c. Click **DONE** to return to the **New York - Routing Properties** window.

d. In the **New York - Routing Properties** window, click **OK** to return to **Multi-Point Designer** page.

19. Save the finalized Free Form Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

    The Free Form Multi-Point network is ready to be run (i.e. played). You now have a Multi-Point network that does the following:

    - On London node object, take data from hardware port 1 to hardware port 0 and apply a link speed limit of 1544000 bps and a latency (fixed of 45 ms).
    - On New York node object, take data from hardware port 0 to hardware port 1 and apply a link speed limit of 1544000 bps and a latency (fixed of 45 ms).
    - On New York node object, take data from hardware port 0 to hardware port 2 and apply a link speed limit of 155520000 bps and a latency (fixed of 30 ms).
    - On Rio de Janeiro node object, take data from hardware port 2 to hardware port 1 and apply a link speed limit of 155520000 bps and a latency (fixed of 15 ms).

    When connecting equipment to the NE-ONE connect the London equipment to port #0, the New York equipment to port #1, and the Rio de Janeiro equipment to port #2 (ports 0, 1 and 2 in the example in *Illustration 116* on page 382).

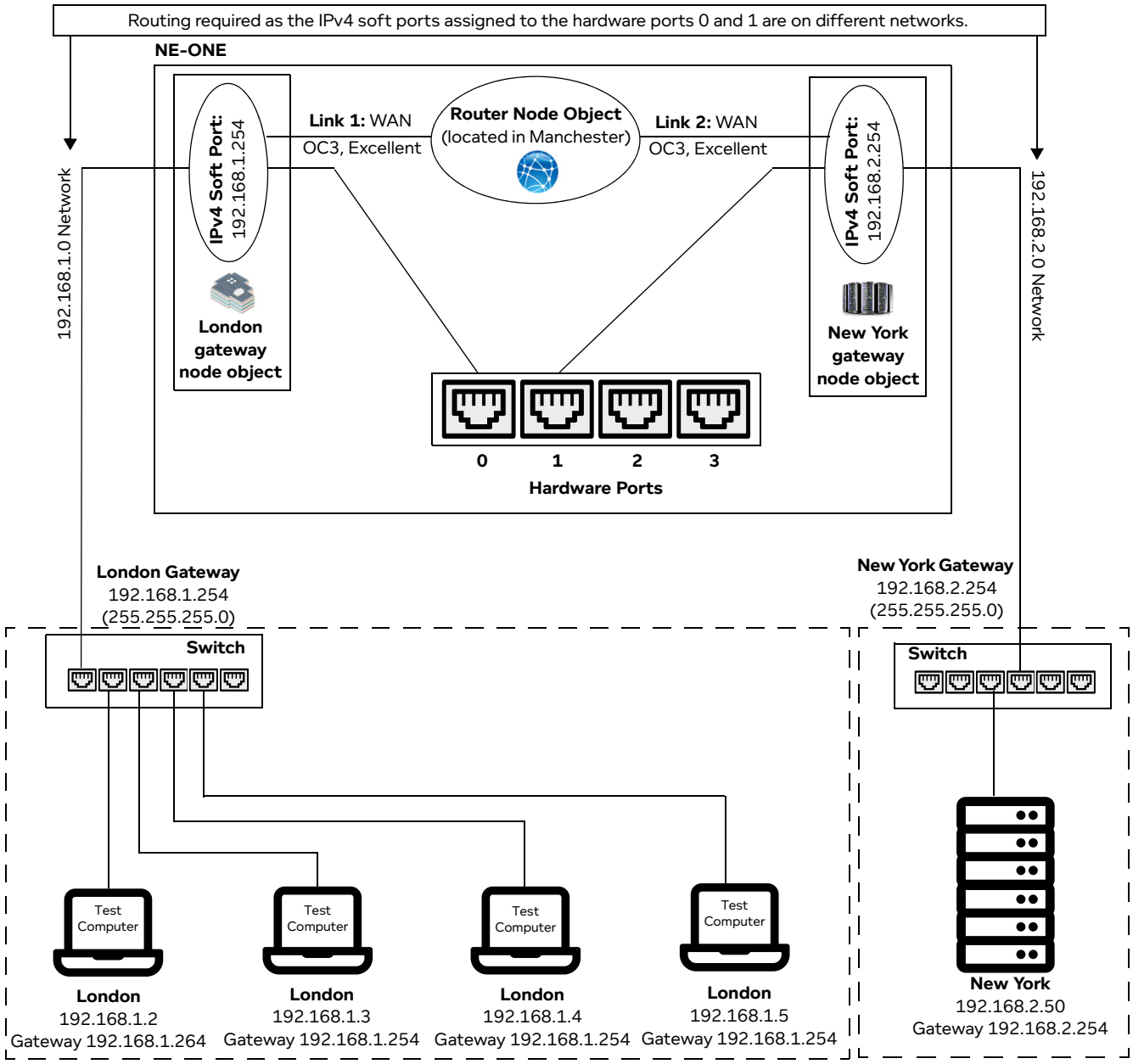
    The Multi-Point network is ready to be run (i.e. played).

4-1-3. Two Interface Routed Network, using IPv4 Soft Ports

In this example we will build a Free Form Multi-Point network which routes between two different networks. It is possible to extend the previous examples (in *Section 4-1-1* and *Section 4-1-2*) to do this by simply creating IPv4 soft ports, and then using IPv4 soft ports instead of the hardware ports 0 and 1, but this is not extensible to more than two networks.

Here we will build a classic 2 Interface Routed network which is the starting point for all Hub and Spoke networks. To concentrate on the routing aspects we will not be changing the default impairments on the links (this can be done later, and there are examples of this in examples of *Section 4-1-1* and *Section 4-1-2* above). Also we will not use a background for clarity (*Section 4-1-2* above explains the use of backgrounds).

ILLUSTRATION 117 - 2 INTERFACED ROUTED EXAMPLE



In our example (*Illustration 117* on page 399), we assume the following:

- The end users (represented by a building icon), based in London have a network 192.168.1.0 (netmask 255.255.255.0) with a Default Gateway of 192.168.1.254 – the NE-ONE will act as that gateway.
- The data center (represented by a data center icon), located in New York has a network 192.168.2.0 (mask 255.255.255.0) with a Default Gateway of 192.168.2.254 – the NE-ONE will act as that gateway too.
- The Router node is located in Manchester (in the United Kingdom).
- The link going between the London and Router node is an OC3, excellent quality WAN link (to concentrate on the routing aspects we will not be changing the default impairments).
- The link going between the New York and Router node is an OC3, excellent quality WAN link (to concentrate on the routing aspects we will not be changing the default impairments).

4-1-3-1. Prerequisite Steps Performed by an Admin User

In order for a non-admin user to create a 2 Interface Routed network based on this example, an admin user needs to do the following prerequisite steps:

1. Connect NE-ONE hardware port 0 to the switch with the London test computers, and hardware port 1 to the switch with the New York data center computers.
2. Create and assign IPv4 soft ports to the hardware ports 0 and 1. To do this, create an IPv4 soft port according the steps described in *Creating an IPv4 Soft Port* on page 114 in *Chapter 5*, *Ports and Services Management*, with the following settings (*Illustration 118* on page 401).
   - IPv4 soft port called 192.168.1.254, with IP address 192.168.1.254, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway) on hardware port 0. There is no gateway defined for this IPv4 soft port as there are no other routers in the network 192.168.1.0, only the NE-ONE itself which is acting as the gateway.

     This IPv4 soft port is represented as a child port of hardware port 0. This IPv4 soft port is semi-permanent and will survive reboots. It is pingable from the 192.168.1.0 network and will respond to ARP requests (“Tell ???? who is 192.168.1.254”).
   - IPv4 soft port called 192.168.2.254, with IP address 192.168.2.254, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway) on hardware port 1. There is no gateway defined for this IPv4 soft port as there are no other routers in the network 192.168.2.254, only the NE-ONE itself which is acting as the gateway.

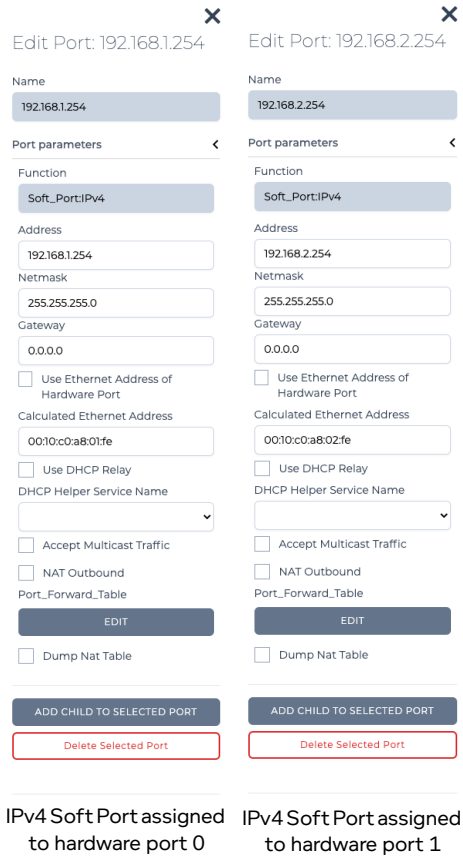
     This IPv4 soft port is represented as a child port of hardware port 1. This IPv4 soft port is semi-permanent and will survive reboots. It is pingable from the 192.168.2.0 network and will respond to ARP requests (“Tell ???? who is 192.168.2.254”).

   Note: Notice that there is only one IPv4 soft port in each hardware port, as we only require one IP address in each network. For clarity, the name given to each of the IPv4 soft ports is the same name as its IP address.

   The resulting soft port layout for this example is shown in *Illustration 118* on page 401, which give a non-admin user all the soft ports they need to create a 2 Interface Routed network based on our example described above.

   Note: Our example is for two nodes, and two links with two IPv4 soft ports. This is easily extensible to much larger networks with many more nodes, links, and IPv4 soft ports.
3. Assign the created IPv4 soft ports (192.168.1.254 and 192.168.2.254) to the intended non-admin user who will create the 2 Interface Routed network according to the steps described in *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205 in *Chapter 6*, *User Administration*.

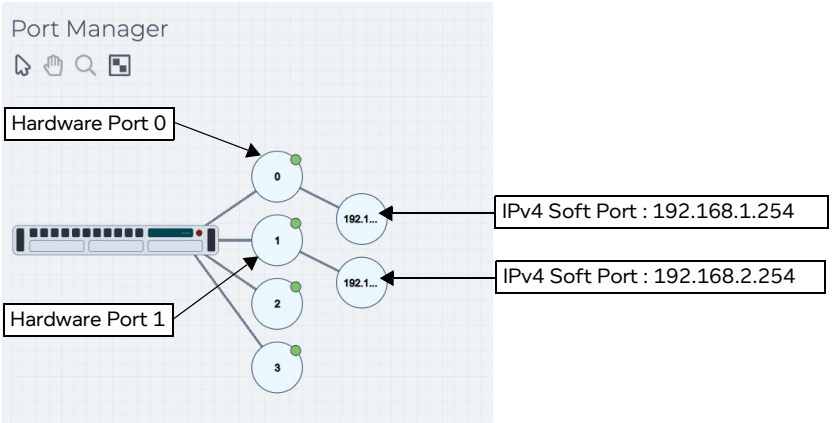
ILLUSTRATION 118 - IPV4 SOFT PORT CONFIGURATIONS FOR 2 INTERFACE ROUTED EXAMPLE



IPv4 Soft Port assigned to hardware port 0

IPv4 Soft Port assigned to hardware port 1

ILLUSTRATION 119 - RESULTING IPV4 SOFT PORT LAYOUT FOR 2 INTERFACE ROUTED EXAMPLE



4-1-3-2. 2 Interface Routed Network Steps Performed by a Non Admin User

Once the NE-ONE has been configured by an admin user according to *Section 4-1-3-1*, a non-admin user (or admin user) can create a 2 Interface Routed network for the example described above (*Illustration 117* on page 399), using the following steps:

1. Launch the **Multi-Point Designer** page, and choose the Free Form network topology template, using the following sub-steps:
   a. Select **Networks** from the Menu.
   b. From the **Networks** page (see *Illustration 4* on page 42) that appears, click **New Network**.

c. From the **Network Wizard** page (see *Illustration 84*) that appears, in the **Free Form** panel, click **CREATE**.

d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`London - New York (Routed)`**), then click **OK**.

A new (i.e. undefined) Multi-Node network appears based on the selected Free Form network topology template you selected. At this stage, the Workspace is empty, and nothing is configured in the network.

2. From the **Multi-Point Designer** page, optionally tick the **Show node names**, **Show link names**, and **Show node ports** check boxes from the **VIEW** drop-down menu.

   Note: This optional step is useful in letting you identify what still needs configuring in the Multi-Point network. Undefined nodes have the generic names **node0**, **node1**, etc. Undefined links have the format **node0<-->node1**, etc. End nodes with undefined input and output ports show nothing.

3. Create the New York node on the Workspace. To do this, from the **Node Icons** panel, drag an appropriate icon (for example a data center icon from within the **Legacy NEONE** tab) into the right hand side area of the Workspace. For more information, see *Creating Nodes in the Workspace* on page 318.

4. Define the New York node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:

   a. In the **Name** field, type **`New York`**.

   b. In the **Description** field, type **`New York Data Center`**.

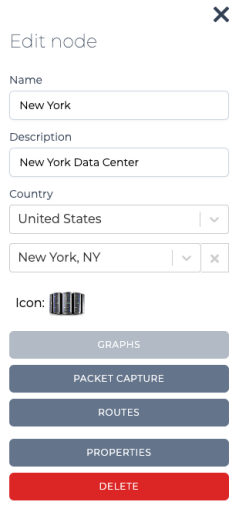
   c. From the **Country** drop-down field, select **United States**.

   Note: You can start typing the word `united` in order to select **United States** quickly from the list of countries.

   d. From the **Choose a location** drop-down field, select **New York, NY**.

   Note: You can start typing the location in order to select it quickly from the list of locations.

   The **Edit node** panel now looks as follows.

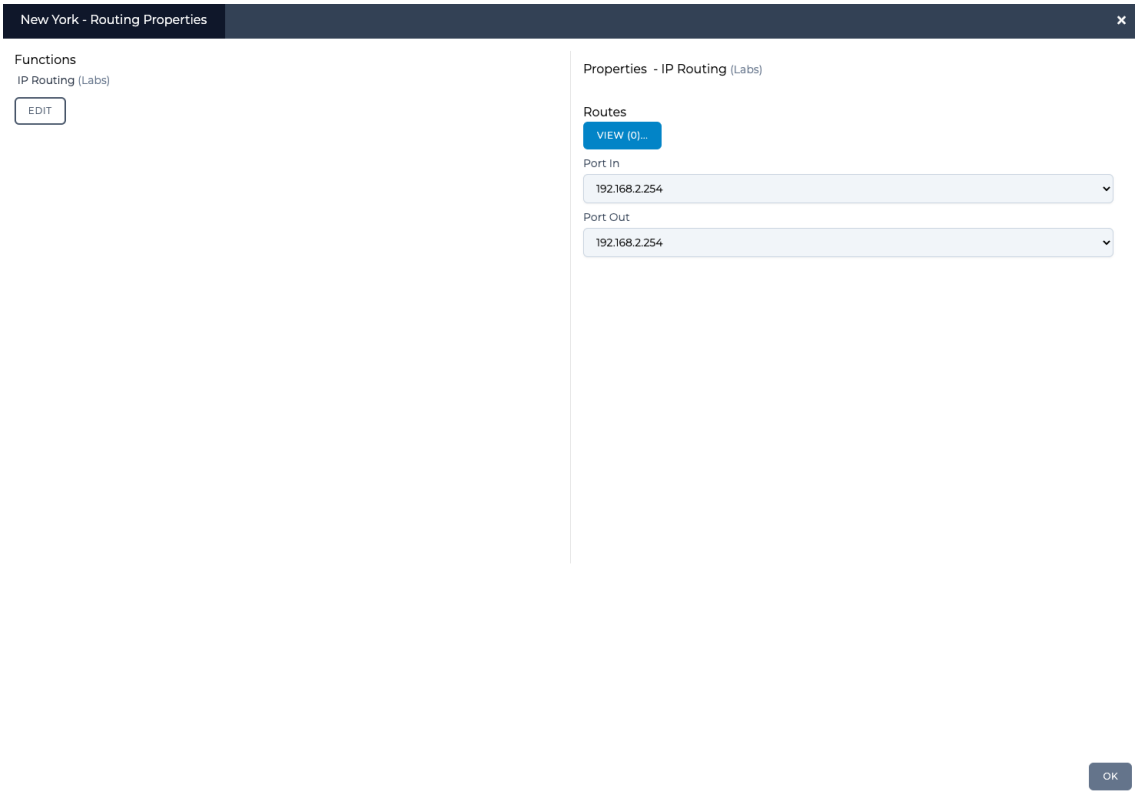


   At this stage you now need to assign the IPv4 soft port 192.168.2.254 to the New York node.

   e. Click on the **Routes** button.

   A **New York - Routing Properties** window appears, letting you define the New York node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out**

drop-down field is set to **None**.



f. In **Port In** drop-down field of the **New York - Routing Properties** window, select an appropriate input port for the New York node. In our example, select **192.168.2.254**, which represents the IPv4 soft port with IP address 192.168.2.254 that was created within hardware port 1 of the NE-ONE.

g. In **Port Out** drop-down field of the **New York - Routing Properties** window, select an appropriate out port for the New York node. In our example, select **192.168.2.254**, which represents the IPv4 soft port with IP address 192.168.2.254 that was created within hardware port 1 of the NE-ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

i. Click to ✕ close the **Edit node** panel.

5. Create the London node on the Workspace. To do this, from the **Node Icons** panel, drag an appropriate icon (for example a building icon from within the **Legacy NEONE** tab) into the left hand side area of the Workspace. For more information, see *Creating Nodes in the Workspace* on page 318.

6. Define the London node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:

a. In the **Name** field, type **`London`**.

b. In the **Description** field, type **`London Test Center`**.

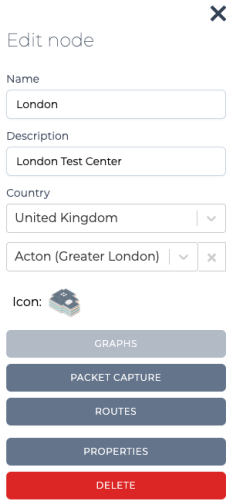
c. From the **Country** drop-down field, select **United Kingdom**.

Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

d. From the **Choose a location** drop-down field, select **Acton (Greater London)**.

Note: You can start typing the location in order to select it quickly from the list of locations.

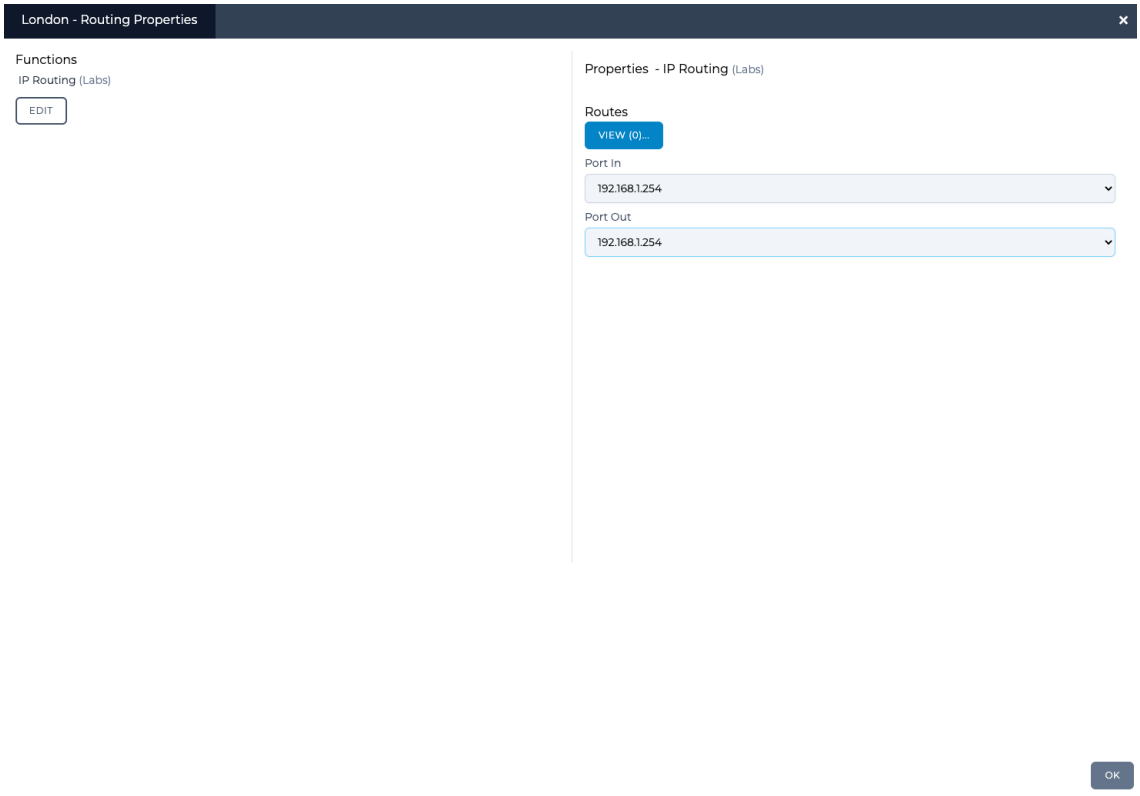
The **Edit node** panel now looks as follows.



At this stage you now need to assign the IPv4 soft port 192.168.1.254 to the London node.

e. Click on the **Routes** button.

A **London - Routing Properties** window appears, letting you define the London node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down field is set to **None**.



f. In **Port In** drop-down field of the **London - Routing Properties** window, select an appropriate input port for the London node. In our example, select **192.168.1.254**, which represents the IPv4 soft port with IP address 192.168.1.254 that was created within hardware port 0 of the NE-ONE.

g. In **Port Out** drop-down field of the **London - Routing Properties** window, select an appropriate

input port for the London node. In our example, select **192.168.1.254**, which represents the IPv4 soft port with IP address 192.168.1.254 that was created within hardware port 0 of the NE-ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

i. Click to ✕ close the **Edit node** panel.

7. Create the Router node on the Workspace. To do this, from the **Node Icons** panel, drag an appropriate icon (for example a globe icon from within the **Legacy NEONE** tab) into the middle area of the Workspace (i.e. between the London and New York nodes). For more information, see *Creating Nodes in the Workspace* on page 318.

   Note: bear in mind that any node object is capable of routing) e.g. a building or cloud is capable of routing. However, in our example we use the globe icon.

8. Define the Router node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:

   a. In the **Name** field, type **`Router`**.

   b. In the **Description** field, type **`Router in Manchester`**.

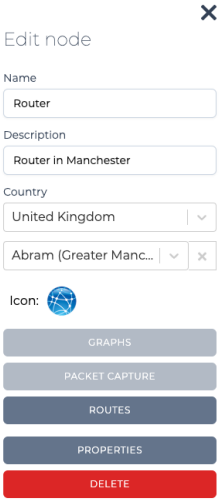
   c. From the **Country** drop-down field, select **United Kingdom**.

   Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

   d. From the **Choose a location** drop-down field, select **Abram (Greater Manchester)**.

   Note: You can start typing the location in order to select it quickly from the list of locations.

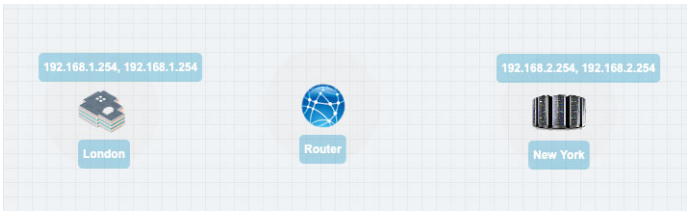
   The **Edit node** panel now looks as follows.



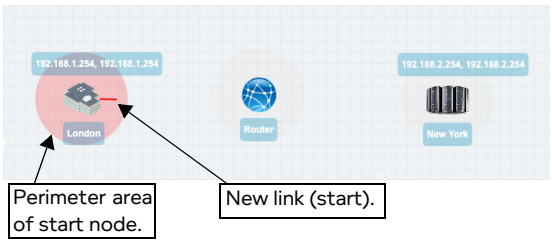
   At this stage you do not do anything further in terms of routing configuration. You will configure the routing once the links have been created between the London and New York nodes, and the router node.

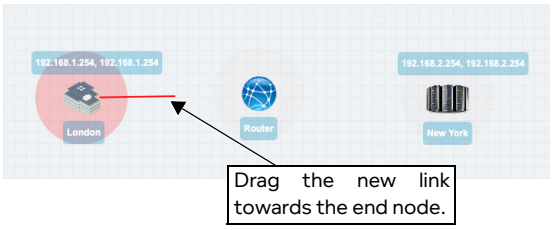
   e. Click to ✕ close the **Edit node** panel.

At this stage, the three nodes London, New York and Router exist on the Work Space with no link.

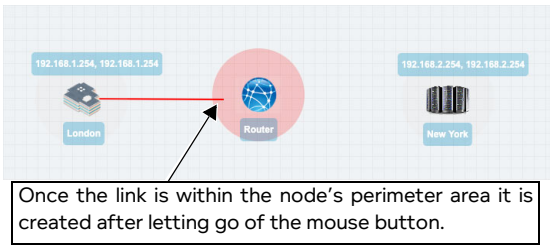


9. Create a link between the London and Router nodes, going from starting from the London (left side) to Router (right side). To do this, do the following:
   a. On the London node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).
      A red line representing the new link appears within the perimeter area of the London node.



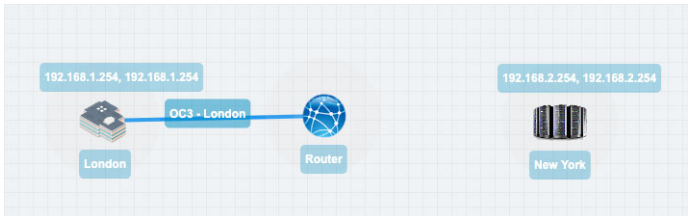


   b. Continue dragging the link into the perimeter area of the Router node (considered the right node).



   c. Once the end of the link is in the perimeter area of the Router node, let go of the mouse button.
      A **Link Name** dialog box appears.
   d. From the **Link Name** dialog box that appears, type **`OC3 - London`**, then click **OK**.

   At this stage the newly created and named **OC3 - London** link appears between the London and Router nodes.



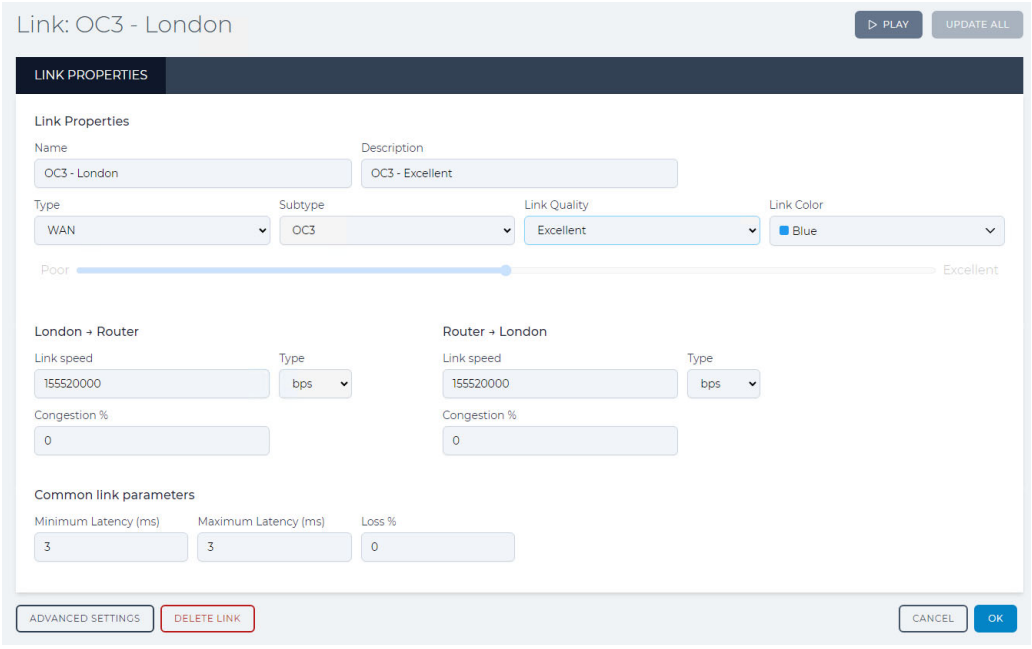
   The newly created **OC3 - London** link now needs configuring.
10. In the Workspace, click on the **OC3 - London** link, and from the **Edit link** panel that appears click the **EDIT** button.
    A **Link** page appears.
11. From the **Link** page that appears, do the following:
    a. Leave the **Name** field unchanged as it inherits the name you originally specified when you created the link.
    b. In the **Description** field, type **`OC3 - Excellent`**.

c. From the **Type** drop-down field, select **WAN**.

d. From the **Subtype** drop-down field, select **OC3**.

e. From the **Link Quality** drop-down field, select **Excellent**. This setting automatically updates the **Minimum Latency (ms)** field to 3, the **Maximum Latency (ms)** field to 3, and the **Loss %** field to 0. This is a useful setting to select, as the **Loss %** field is set to 0, which will not change. You will not modify the values of the **Minimum Latency (ms)** field and **Maximum Latency (ms)** field.

f. From the **Link Color** drop-down field, leave the color set to **Blue**.



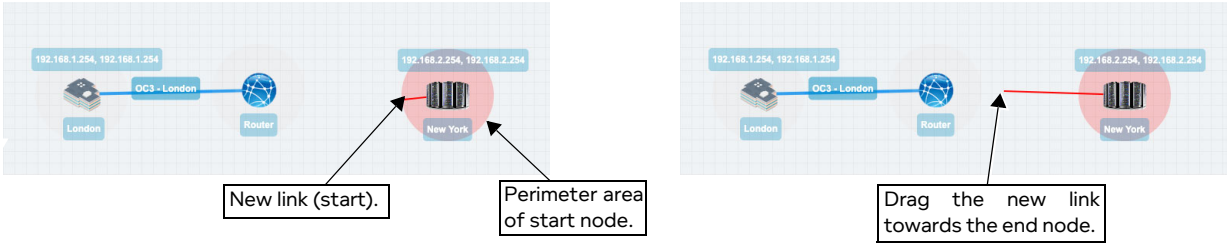
g. Click **OK** to submit the link properties.

You are returned to the Workspace in the **Multi-Point Designer** page.

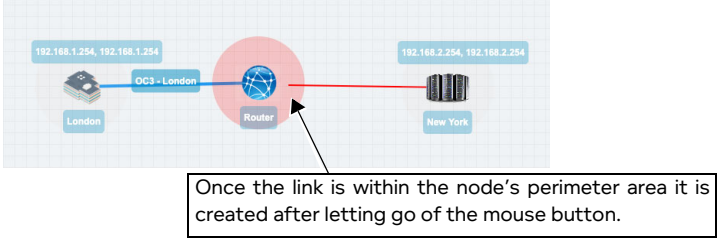
12. Create a link between the New York and Router nodes, going from starting from the New York (left side) to Router (right side). To do this, do the following:

a. On the New York node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).

A red line representing the new link appears within the perimeter area of the New York node.



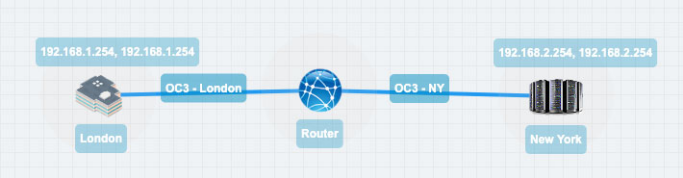
b. Continue dragging the link into the perimeter area of the Router node (considered the right node).



c. Once the end of the link is in the perimeter area of the Router node, let go of the mouse button.
A **Link Name** dialog box appears.

d. From the **Link Name** dialog box that appears, type **`OC3 - NY`**, then click **OK**.

At this stage the newly created and named **OC3 - NY** link appears between the London and Router nodes.



The newly created **OC3 - NY** link now needs configuring.

13. In the Workspace, click on the **OC3 - NY** link, and from the **Edit link** panel that appears click the **EDIT** button.
A **Link** page appears.

14. From the **Link** page that appears, do the following:

a. Leave the **Name** field unchanged as it inherits the name you originally specified when you created the link.

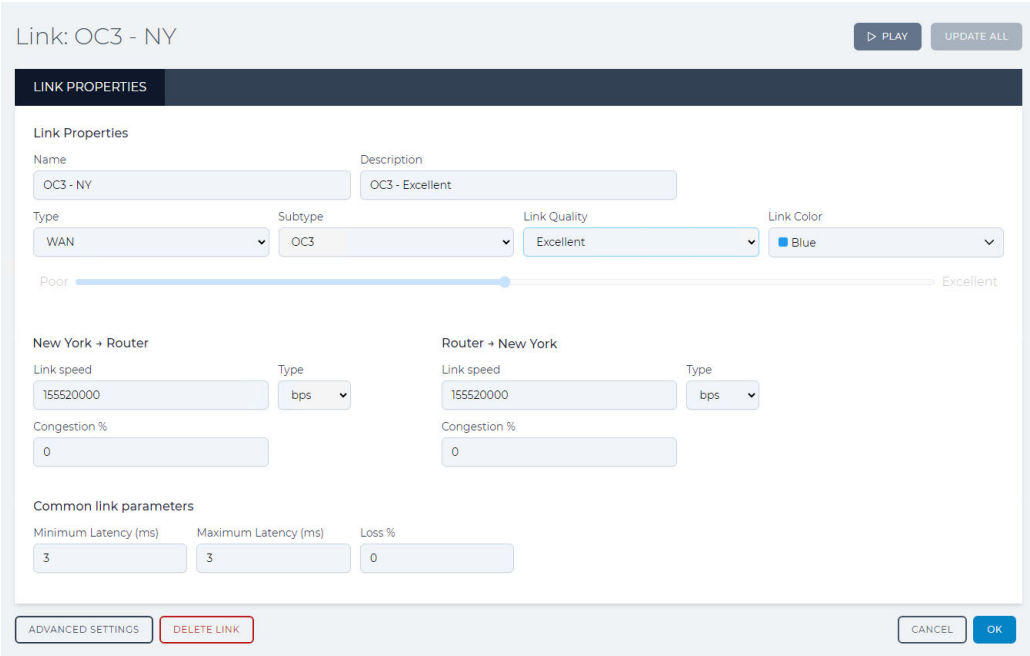
b. In the **Description** field, type a **`OC3 - Excellent`**.

c. From the **Type** drop-down field, select **WAN**.

d. From the **Subtype** drop-down field, select **OC3**.

e. From the **Link Quality** drop-down field, select **Excellent**. This setting automatically updates the **Minimum Latency (ms)** field to 3, the **Maximum Latency (ms)** field to 3, and the **Loss %** field to 0. This is a useful setting to select, as the **Loss %** field is set to 0, which will not change. You will not modify the values of the **Minimum Latency (ms)** field and **Maximum Latency (ms)** field.

f. From the **Link Color** drop-down field, leave the color set to **Blue**.



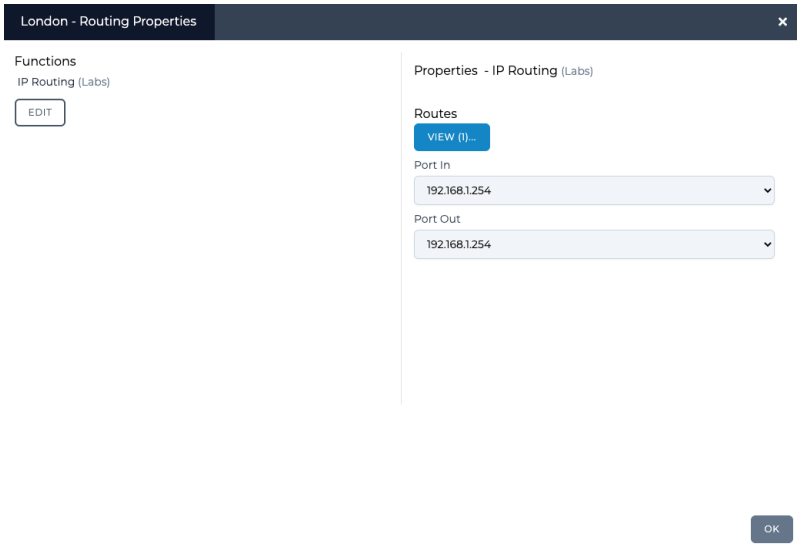
g. Click **OK** to submit the link properties.
You are returned to the Workspace in the **Multi-Point Designer** page.

At this point, everything is configured, except for the routing table on the Router node to support the traffic to/from the links of London and New York nodes (because they are from different networks). Now that all the links exist, the routing table on the Router node can be configured to route traffic between the different London (192.168.1.0) and New York (192.168.2.0) networks.

When creating the links between London and the Router, and New York and the Router, the NE-ONE intelligently created all the necessary default routing tables for each of the London and New York nodes. In order to illustrate that the routing tables automatically generated by the NE-ONE for the London and New York nodes, the optional steps below describe how to view (but not modify) the routing tables that were automatically generated.

15. Optionally view the London node's auto-generated routing table, as follows:
    a. In the Workspace, click on the London node, then from the **Edit node** panel that appears, click the **ROUTES** button.

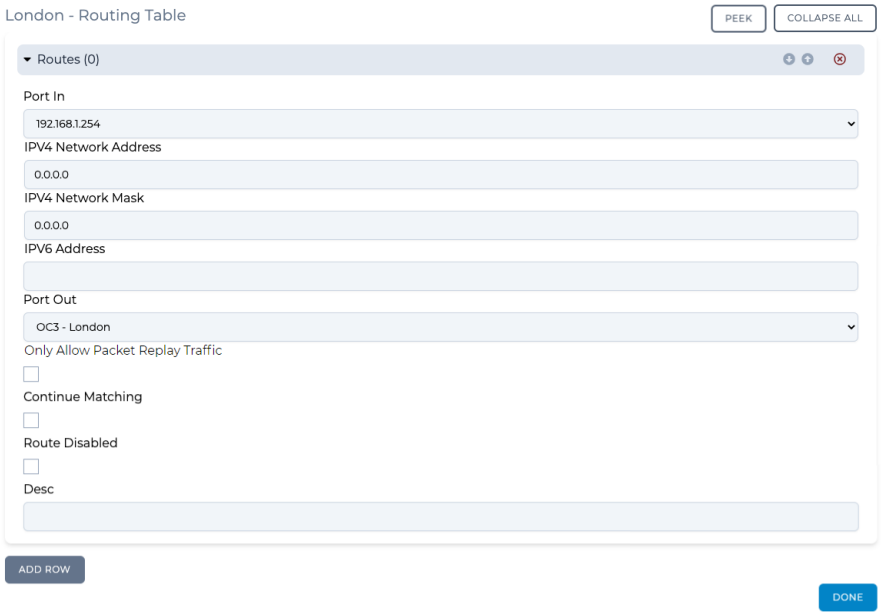
    A **London - Routing Properties** window appears.



    Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**192.168.1.254**), but the **Port Out** value is only used if no route is matched in the Routing table. You can examine the routing table by clicking on the **VIEW** button.

    b. Click the **VIEW** button.

A **London - Routing Table** window appears.



We see that the NE-ONE intelligently and helpfully created a route (during the act of creating the link between London and the Router in step 9). The routing works as follows:

If the packet originated on IPv4 soft port 192.168.1.254 and matches the other conditions which, as they are all blank, it treats as wild cards so anything will do, then the packet is sent to the link object **OC3 - London** (London to Router direction). This is what we want – packets originating on IPv4 soft port 192.168.1.254 the input port are sent down the link **OC3 - London**, any other packets do not match the routing rule and so are output on IPv4 soft port 192.168.1.254. This means that packet coming down the link in the other direction i.e. from the link object **OC3 - London** (Router to London direction) will be output on IPv4 soft port 192.168.1.254, as it originated on the Router – again exactly what we want.

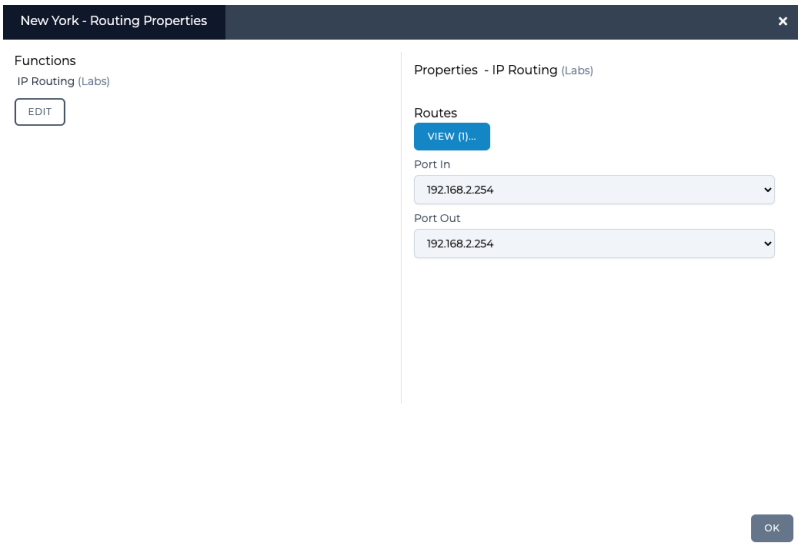
c. Click **DONE** to return to the **London - Routing Properties** window.

d. In the **London - Routing Properties** window, click **OK** to return to **Multi-Point Designer** page.

16. Optionally view the New York node's auto-generated routing table, as follows:

a. In the Workspace, click on the New York node, then from the **Edit node** panel that appears, click the **ROUTES** button.

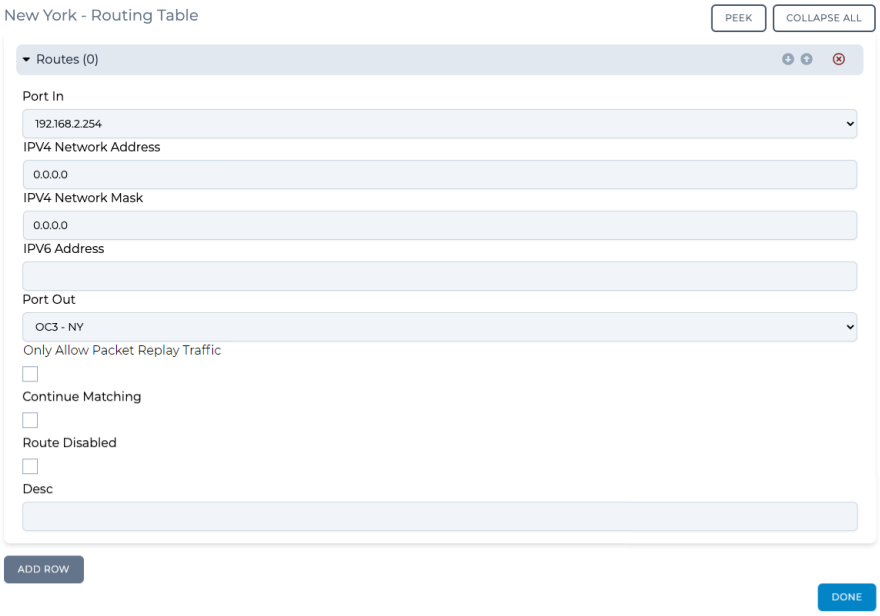
A **New York - Routing Properties** window appears.



Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**192.168.2.254**), but the **Port Out** value is only used if no route is matched in the Routing table. You can examine the routing table by clicking on the **VIEW** button.

b. Click the **VIEW** button.

A **New York - Routing Table** window appears.



We see that the NE-ONE intelligently and helpfully created a route (during the act of creating the link between New York and the Router in step 12). The routing works as follows:

If the packet originated on IPv4 soft port 192.168.2.254 and matches the other conditions which, as they are all blank, it treats as wild cards so anything will do, then the packet is sent to the link object **OC3 - New York** (New York to Router direction). This is what we want – packets originating on IPv4 soft port 192.168.2.254 the input port are sent down the link **OC3 - New York** link, any other packets do not match the routing rule and so are output on IPv4 soft port 192.168.2.254. This means that packet coming down the link in the other direction i.e. from the

link object **OC3 - New York** (Router to New York direction) will be output on IPv4 soft port 192.168.2.254, as it originated on the Router – again exactly what we want.

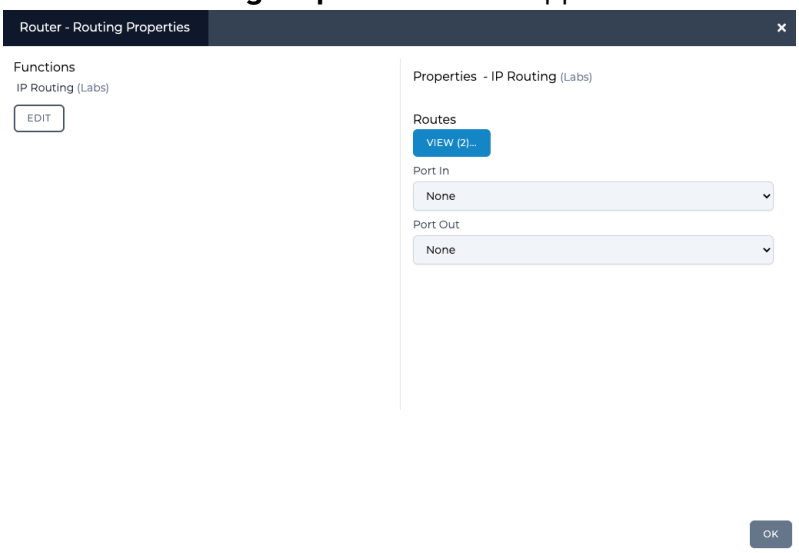
c. Click **DONE** to return to the **Rio De Janeiro - Routing Properties** window.

d. In the **New York - Routing Properties** window, click **OK** to return to **Multi-Point Designer** page.

17. View and edit the Router node's auto-generated routing table, as follows:

a. In the Workspace, click on the Router node, then from the **Edit node** panel that appears, click the **ROUTES** button.

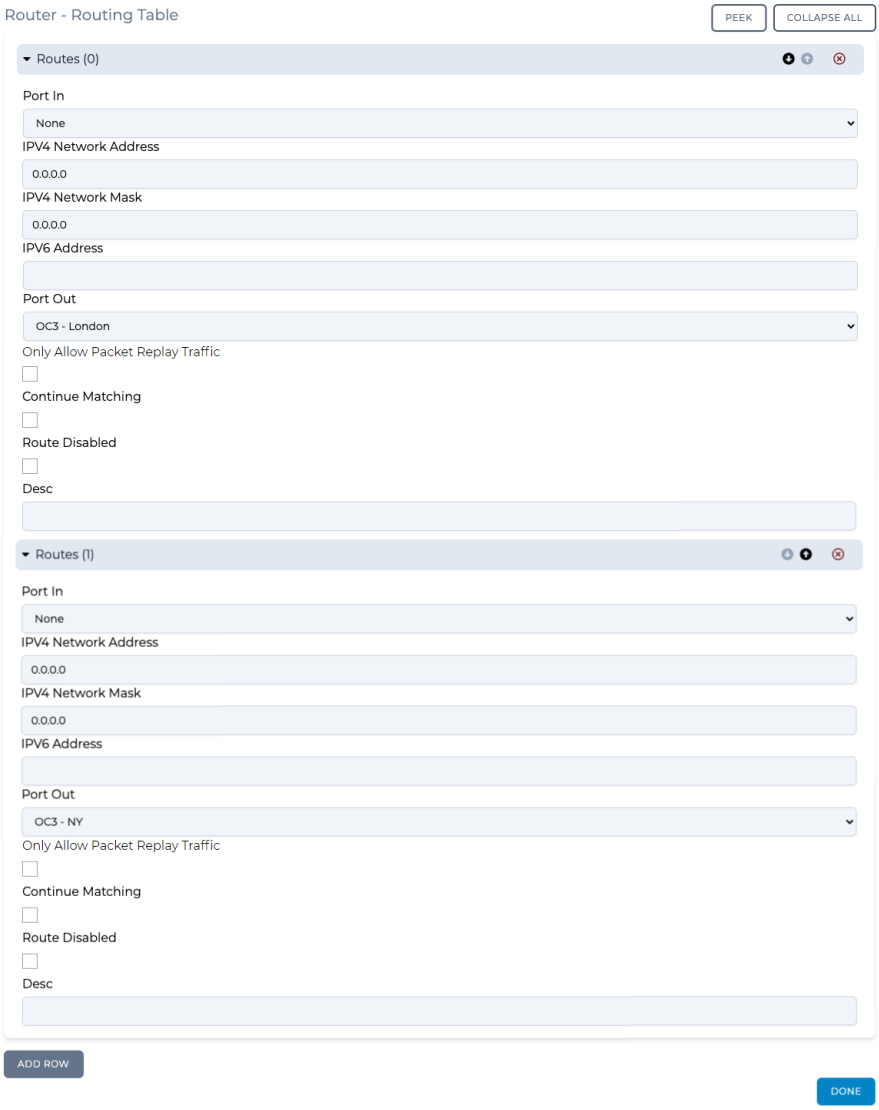
A **Router - Routing Properties** window appears.



Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**None**), but the **Port Out** value is only used if no route is matched in the Routing table. In this case however, because the node is performing purely a routing function, you will rely purely on the routing table, and leave the **Port In** and **Port Out** set to the same value of **None** (i.e. no filtering on any ports, and the routing table (which you will define) performs all of the routing.

b. Click the **VIEW** button.

A **Router - Routing Table** window appears.



We see that the NE-ONE intelligently and helpfully started to create two routes in the routing table (during the act of creating the links between London and the Router in step 9 and New York and the Router in step 12). The two initial routes in the routing table (that need to be manually completed) correspond to the following two incoming links:

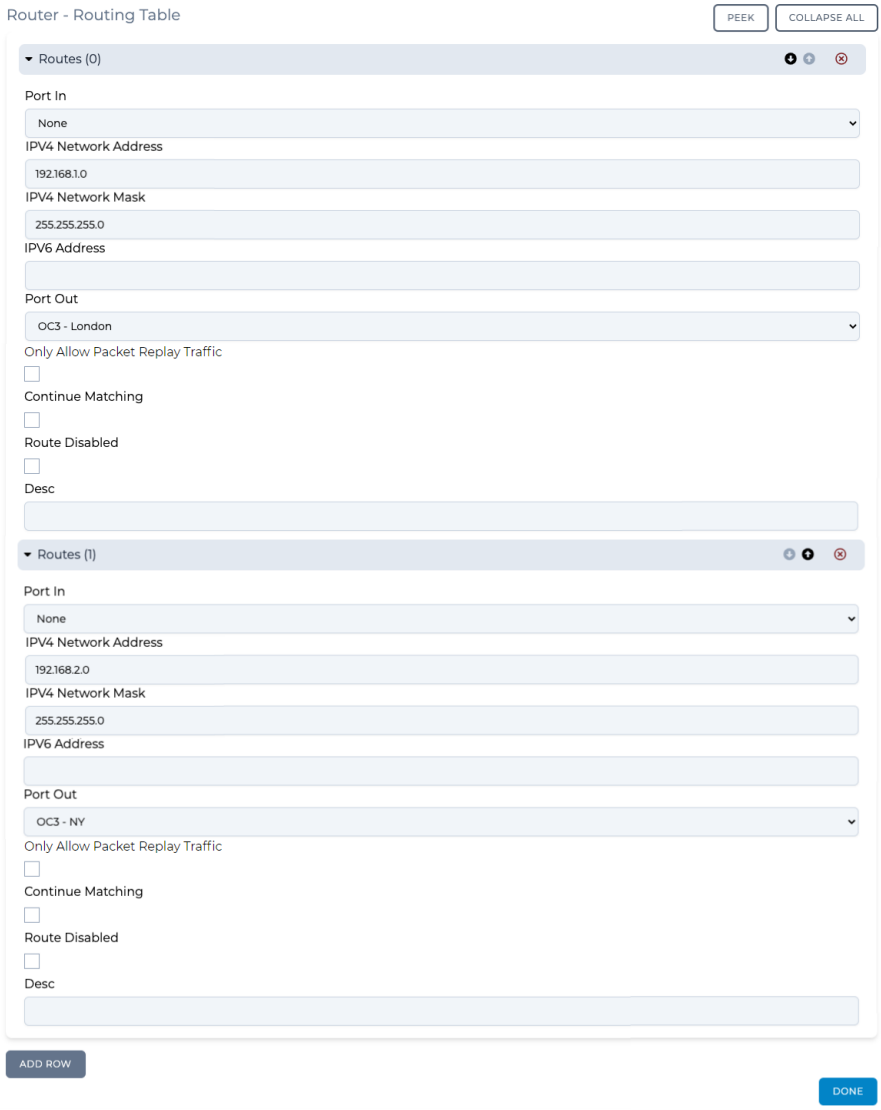
Link object **OC3 - London** from the London node (which is defined to be acting as a gateway on IP address 192.168.1.254, netmask 255.255.255.0 (i.e. network 192.168.1.0)). By default the NE-ONE does not define the IP address or netmask for this route. For this route you will need to define the IP address and netmask. Since the London node at the end of the **OC3 - London** link is acting as a gateway, you will define the IP address as the network address (i.e. 192.168.1.0) for the entire network behind the London gateway node, and also define the netmask (i.e. the same netmask as that of the London gateway node).

Link object **OC3 - New York** from the New York node (which is defined to be acting as a gateway on IP address 192.168.2.254, netmask 255.255.255.0 (i.e. network 192.168.2.0)). By default the NE-ONE does not define the IP address or netmask for this route. For this route you will need to define the IP address and netmask. Since the New York node at the end of the **OC3 - New York**

link is acting as a gateway, you will define the IP address as the network address (i.e. 192.168.2.0) for the entire network behind the New York gateway node, and also define the netmask (i.e. the same netmask as that of the New York gateway node).

c. In the first route (called **Routes(0)**, with **Port Out** already set to **OC3 - London**), do the following to complete the route configuration:
In the **IPv4 Network Address** field, type: **`192.168.1.0`**
In the **IPv4 Network Mask** field, type: **`255.255.255.0`**

Note: As with normal IPv4 routing the Network address you use could be any in the subnet i.e. 192.168.1.0-192.168.1.255, as the value used for matching purposes is taken after masking the address you give with the network mask, so, for example 192.168.1.45 masked with 255.255.255.0 is 192.168.1.0 and that is the value used in route matching.



d. In the second route (called **Routes(1)**, with **Port Out** already set to **OC3 - NY**), do the following to complete the route configuration:
In the **IPv4 Network Address** field, type: **`192.168.2.0`**
In the **IPv4 Network Mask** field, type: **`255.255.255.0`**

Note: As with normal IPv4 routing the Network address you use could be any in the subnet i.e.

192.168.2.0-192.168.2.255, as the value used for matching purposes is taken after masking the address you give with the network mask, so, for example 192.168.2.45 masked with 255.255.255.0 is 192.168.2.0 and that is the value used in route matching.

e. Click **DONE** to return to the **Router - Routing Properties** window.

f. In the **Router - Routing Properties** window, click **OK** to return to **Multi-Point Designer** page.

18. Save the finalized Free Form Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

    The Free Form Multi-Point network is ready to be run (i.e. played). You now have a Multi-Point network that does the following:

    - On London node object, take data from IPv4 soft port 192.168.1.254 to the Router node and apply a link speed limit of 155520000 bps and a latency (fixed of 3 ms).
    - On Router node object, take data from link OC3 - London and apply a link speed limit of 1544000 bps and a latency (fixed of 3 ms).
    - On Router node object, take data from link OC3 - New York and apply a link speed limit of 1544000 bps and a latency (fixed of 3 ms).
    - On New York node object, take data from IPv4 soft port 192.168.2.254 to the Router node and apply a link speed limit of 155520000 bps and a latency (fixed of 3 ms).

    When connecting equipment to the NE-ONE connect the London equipment to port #0 and the New York equipment to port #1 (ports 0 and 1 in the example in *Illustration 117* on page 399).

    Make sure that the equipment at the client (London) and server (New York) ends knows that its default gateways are 192.168.1.254 and 192.168.2.254, respectively by setting their routing/gateway to these addresses.

4-2. Creating Fully Meshed Networks

In this example, we need to connect three private (sub) networks e.g. 192.168.4.0/24, 192.168.5.0/24 and 192.168.6.0/24 to each other. The structure for connection is a Fully Meshed network.

These subnets are connected to a VLAN (802.1Q) capable switch which has up to now been routing (it is a layer 3 switch) between these subnets.

Unfortunately, the switch cannot create WAN conditions between these subnets and in the “real world”. That is, in the non-test environment these subnets will be in geographically dispersed locations (for example, London, Berlin, and Paris.

The requirement is to connect the NE-ONE to the VLAN switch in Berlin, and produce a Fully Meshed WAN between these subnets with the minimum amount of changes.

We are told that:

- The Berlin site has Network 192.168.4.0 is on VLAN 601 with gateway 192.168.4.254.
- The Paris site has Network 192.168.6.0 is on VLAN 602 with gateway 192.168.6.1.
- The London site has Network 192.168.5.0 is on VLAN 603 with gateway 192.168.5.1.
- The IP address for the NE-ONE to have in the Berlin network is 192.168.4.100.

In the following example (*Illustration 130* on page 436), the Fully Meshed network topology template is used to create a Multi-Point network, with the following configuration:

- Berlin (end node):
  - Input port : 192.168.4.1
  - Output port : 192.168.4.1
  - Two links :
    Link to London node: Type : WAN, T3 - Good, with link name T3 - Good.
    Link to Paris node: Type : WAN, T1 - Excellent, with link name T1 - Excellent.
  - Routing table, with the following auto-generated routes (i.e. nothing needs changing):
    One route with input port as 192.168.4.1, output port as T3 - Good : this routes all traffic to/from the Berlin and London nodes, with no packet filtering.
    One route with input port as 192.168.4.1, output port as T1 - Excellent : this routes all traffic to/from the Berlin and Paris nodes, with no packet filtering.
- London (end node):
  - Input port : 192.168.5.1
  - Output port : 192.168.5.1
  - Two links :
    Link to Paris node: Type : WAN, OC3 - Excellent, with link name OC3 - Excellent.
    Link to Berlin node: Type : WAN, T3 - Good, with link name T3 - Good.
  - Routing table, with the following auto-generated routes (i.e. nothing needs changing):
    One route with input port as 192.168.5.1, output port as OC3 - Excellent : this routes all traffic to/from the London and Paris nodes, with no packet filtering.
    One route with input port as 192.168.5.1, output port as T3 - Good : this routes all traffic to/from the Berlin and London nodes, with no packet filtering.
- Paris (end node):
  - Input port : 192.168.6.1
  - Output port : 192.168.6.1
  - Two links :
    Link to Berlin node: Type : WAN, T1 - Excellent, with link name T1 - Excellent.
    Link to London node: Type : WAN, OC3 - Excellent, with link name OC3 - Excellent.

- Routing table, with the following auto-generated routes (i.e. nothing needs changing):
  One route with input port as 192.168.6.1, output port as T1 - Excellent : this routes all traffic from the Paris and Berlin nodes, with no packet filtering.
  One route with input port as 192.168.6.1, output port as OC3 - Excellent : this routes all traffic to/from the London and Paris nodes, with no packet filtering.

Note:
An assumption is made that the total I/O we are handling can be covered in total by one of the NE-ONE's hardware ports, if this is not true then a modified version of this example can be produced by using more than one NE-ONE hardware ports.

ILLUSTRATION 120 - EXAMPLE SIMPLE FULLY MESHED NETWORK (MULTI-POINT WORKSPACE)

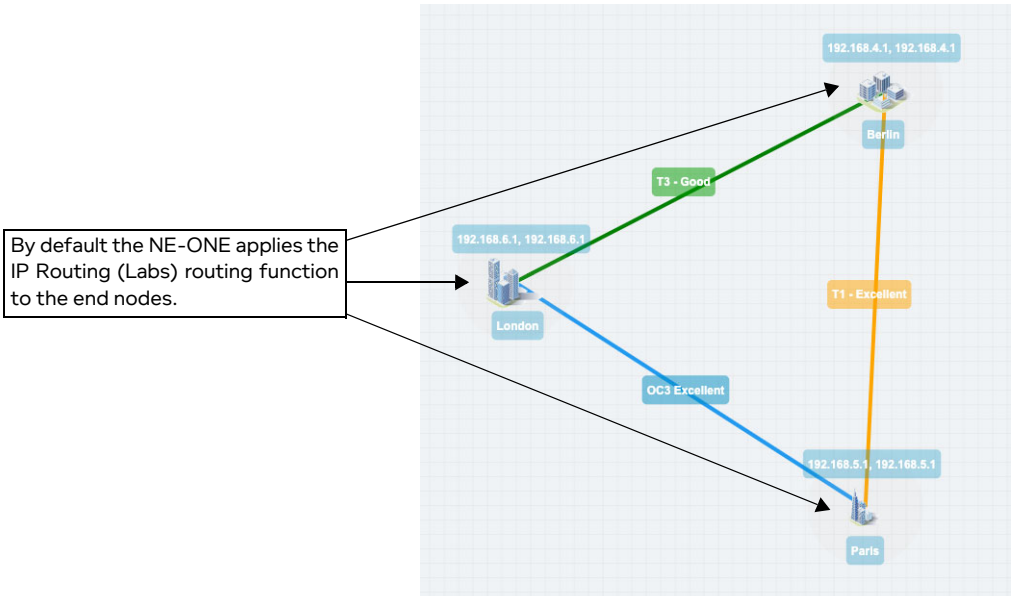
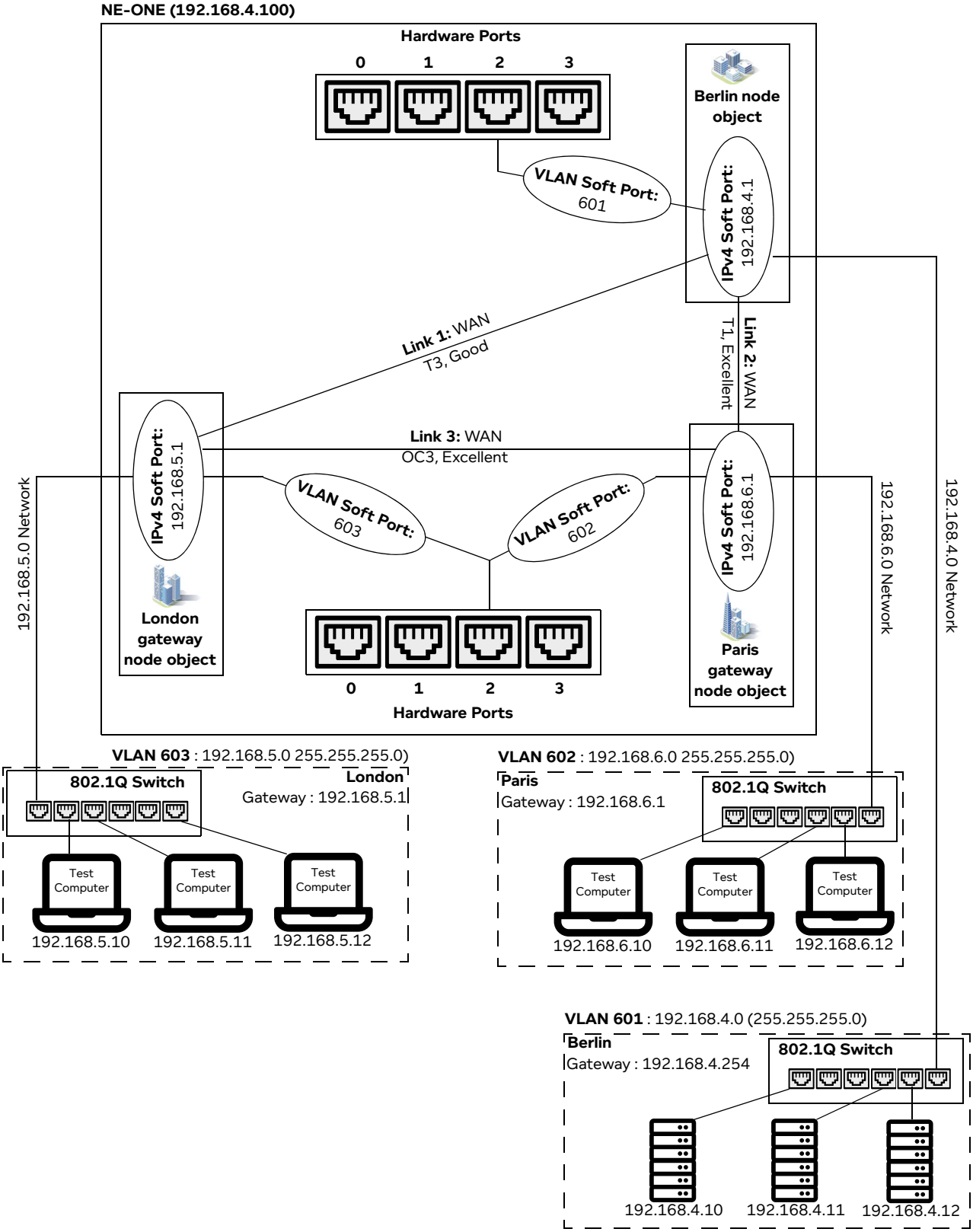


ILLUSTRATION 121 - EXAMPLE FULLY MESHED NETWORK (WITH VLAN AND IPV4 SOFT PORTS)

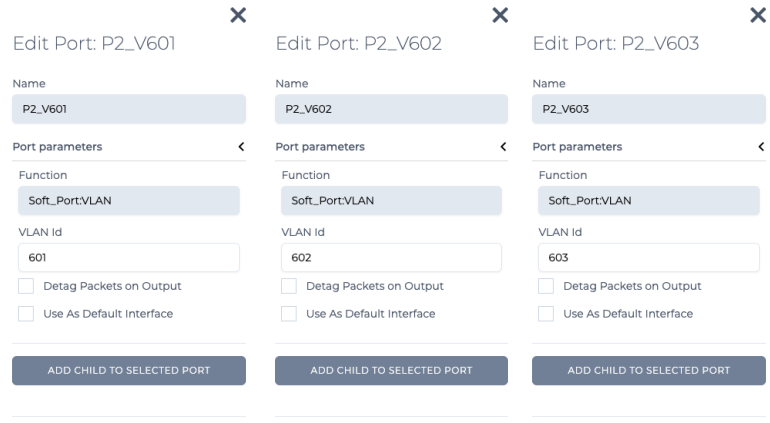


4-2-1. Prerequisite Steps Performed by an Admin User

In order for a non-admin user to create a Fully Meshed network based on this example, an admin user needs to do the following prerequisite steps:

1. Configure the NE-ONE with a static IP address of 192.168.4.100 according to the steps described in *Configuring the Management Port Settings* on page 60 of *Chapter 4*, *Installation and Configuration*.
2. Request to the Berlin network administrator that a VLAN (802.1Q) Trunk port is set up on the switch, trunking at least VLANs 601, 602, and 603.
3. Request to the Berlin network administrator that the switch's routing addresses 192.168.5.1 and 192.168.6.1 are removed from its routing tables, as the NE-ONE will take over that function.
4. Connect NE-ONE hardware port (in our example, hardware port 2) to that Trunk port with a suitable cable.
5. Create one VLAN soft port for each required VLANs (601, 602, and 603) on the NE-ONE's hardware port (in our example, hardware port 2) according the steps described in *Creating a VLAN Soft Port* on page 107 in *Chapter 5*, *Ports and Services Management*, with each VLAN soft port having **Detag Packets** on **Output and Default Interface** settings disabled (unticked), as shown in *Illustration 107*.

ILLUSTRATION 122 - VLAN SOFT PORT CONFIGURATIONS



VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2

Note: The naming convention of the VLAN soft ports uses the P2 prefix to indicate that these ports are children of hardware port 2, where VNNN denotes a VLAN port with that ID (tag). You can use any soft port names you want, but they should be meaningful.

6. Create and assign IPv4 soft ports to the VLAN soft ports. To do this, within each of the VLAN soft ports, create an IPv4 soft port according the steps described in *Creating an IPv4 Soft Port* on page 114 in *Chapter 5*, *Ports and Services Management*, with the following settings (*Illustration 140* on page 455).
   - VLAN 601 soft port contains IPv4 soft port called 192.168.4.1, with IP address 192.168.4.1, netmask 255.255.255.0, and gateway 192.168.4.254.
   - VLAN 602 soft port contains IPv4 soft port called 192.168.6.1, with IP address 192.168.6.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway as there are no other routers in the network 192.168.6.0, only the NE-ONE itself which is acting as the gateway.
   - VLAN 603 soft port contains IPv4 soft port called 192.168.5.1, with IP address 192.168.5.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway as there are no other routers in the network 192.168.6.0, only the NE-ONE itself which is acting as the gateway.

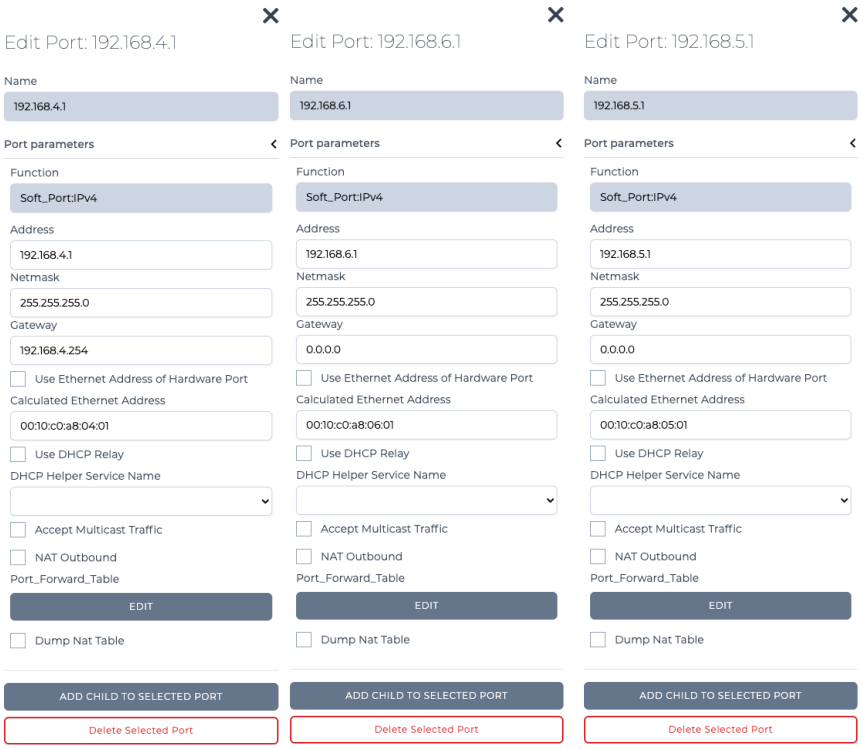
Note: Notice that there is only one IPv4 soft port in each VLAN soft port, as we only require one IP address in each VLAN network. Also, again for clarity, name given to each of the IPv4 soft ports is the same name as its IP address.

The resulting soft port layout for this example is shown in *Illustration 124* on page 421, which give a non-admin user all the soft ports they need to create a Fully Meshed type Multi-Point network based on our example described above.

Note: Our example is for three end nodes, and three links with three VLAN soft ports and three IPv4 soft ports. This is easily extensible to much larger networks with many more end nodes, links, VLAN soft ports and IPv4 soft ports.

7. Assign the created IPv4 soft ports (192.168.4.1, 192.168.5.1, and 192.168.6.1) to the intended non-admin user who will create the Fully Meshed network according to the steps described in *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205 in *Chapter 6*, *User Administration*.

ILLUSTRATION 123 - IPV4 SOFT PORT CONFIGURATIONS FOR FULLY MESHED EXAMPLE

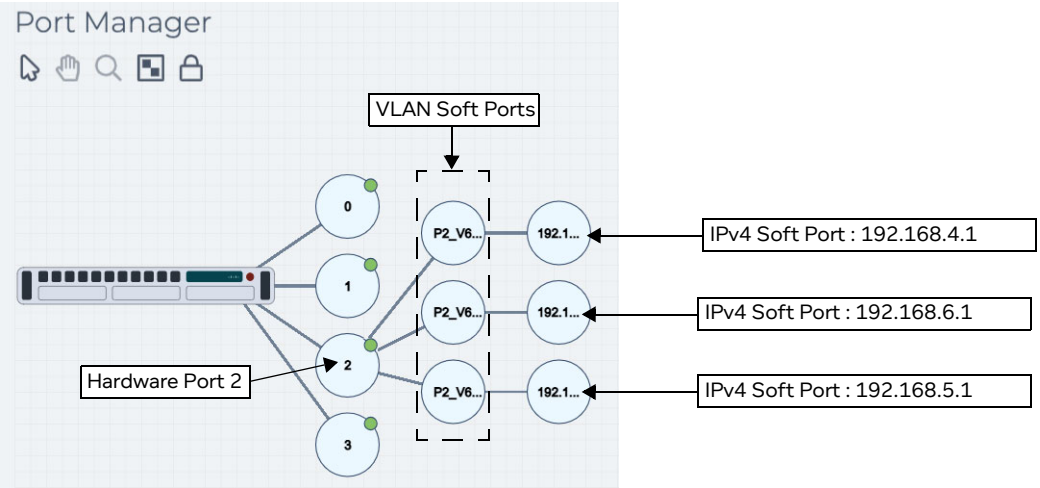


IPv4 Soft Port assigned to VLAN Soft Port 601

IPv4 Soft Port assigned to VLAN Soft Port 602

IPv4 Soft Port assigned to VLAN Soft Port 603

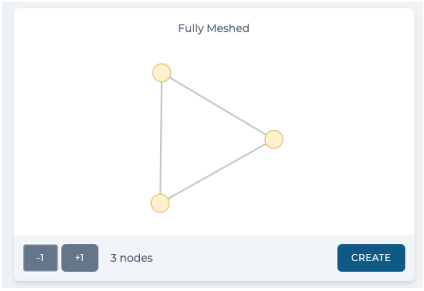
ILLUSTRATION 124 - RESULTING VLAN AND IPV4 SOFT PORT LAYOUT FOR FULLY MESHED EXAMPLE



4-2-2. Fully Meshed Network Creation Steps Performed by a Non Admin User

Once the NE-ONE has been configured by an admin user according to *Section 4-2-1*, a non-admin user (or admin user) can create a Fully Meshed Multi-Point network for the example described above, using the following steps:

1. Launch the **Multi-Point Designer** page, and choose the Cloud network topology template, using the following sub-steps:
   a. Select **Networks** from the Menu.
   b. From the **Networks** page (see *Illustration 4* on page 42) that appears, click **New Network**.
   c. From the **Network Wizard** page (see *Illustration 84*) that appears, in the **Fully Meshed** panel, click the **+1** or **-1** icon to increase or decrease the total number of end nodes used by the Fully Meshed network topology template, then click **CREATE**.

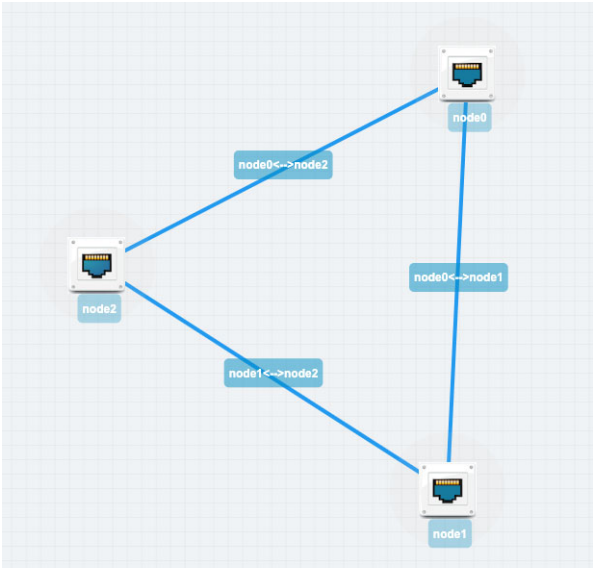


   In our example we want three nodes, so click the **-1** button two times until only three nodes are shown in the **Fully Meshed** panel, then click **CREATE**.
   d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`Europe Mesh`**), then click **OK**.

A new (i.e. undefined) Multi-Node network appears based on the selected Fully Meshed network topology template you selected. At this stage, nothing is configured in the Fully Meshed network. You will need to configure the:

- routing for each of the nodes (i.e. assign input and output ports),
- links between each of the nodes
- routing table of the nodes (i.e. so that traffic can pass between the nodes (as each of the nodes

are on different networks)



2. From the **Multi-Point Designer** page, optionally tick the **Show node names**, **Show link names**, and **Show node ports** check boxes from the **VIEW** drop-down menu.

   Note: This optional step is useful in letting you identify what still needs configuring in the Multi-Point network. Undefined nodes have the generic names **node0**, **node1**, and **node2**, etc. Undefined links have the format **node0<-->node2**, **node0<-->node1**, **node1<-->node2**, etc. End nodes with undefined input and output ports show nothing.

3. For each of the end nodes and cloud node in the Workspace, click on the end node/cloud node, and from the **Edit node** panel that appears do the following to define the node's basic properties.

   a. In the **Name** field, type an appropriate node name. The node name can contain alpha-numeric characters and spaces. In our example, do the following:

      For the first end node (which was initially called node0), type **`Berlin`**.

      For the second end node (which was initially called node1), type **`Paris`**

      For the third end node (which was initially called node2), type **`London`**.

   b. In the **Description** field, optionally type an appropriate description.The node description can contain alpha-numeric characters and spaces.

   c. From the **Country** drop-down field, select an appropriate country to define the country where the node is located. In our example, do the following:

      For the first end node, select **Germany**.

      For the second end node, select **France**.

      For the third end node, select **United Kingdom**.

      Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

   d. From the **Choose a location** drop-down field, select and appropriate area for the location. In our example, do the following:

      For the first end node, select a location within **Berlin**.

      For the second end node, select a location within **Paris**.

      For the third end node, select a location within **London**.

      Note: You can start typing the location in order to select it quickly from the list of locations. The

list of locations proposed depend on the string you specified in the **Name** field. In this case for example, locations in an around London are proposed.

e. Click on the icon, and from the dialog box that appears click on the an appropriate icon, and then click **OK**.

In our example, from the **Standard** category in the **Node** Icons panel do the following:

For the first end node, select the four low buildings icon .

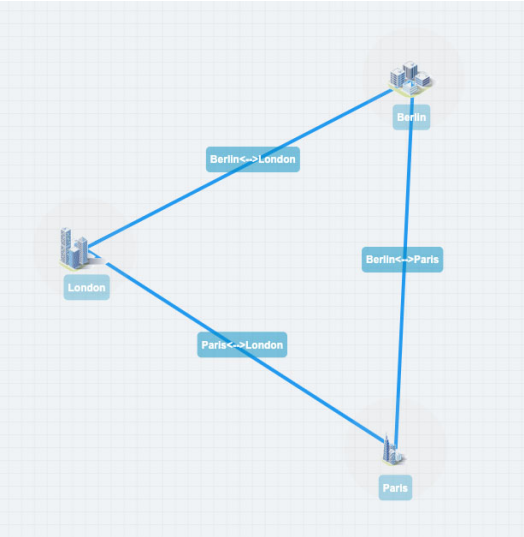
For the second end node, select the four buildings point icon .

For the third end node, select the commercial center icon .

f. Click to ✕ close the **Edit node** panel.

At this stage the basic properties of each of the end nodes are defined. Since the node names were changed, the link names automatically update to include the node names, such that:

- **node0<-->node1** becomes **Berlin<-->Paris**
- **node0<-->node2** becomes **Berlin<-->London**
- **node1<-->node2** becomes **Paris<-->London**



Next, define the properties of links between each of the end nodes. In the example below, the automatically assigned link names are changed, however this is purely optional.

4. For each of the links in the Workspace, click on the link, and from the **Edit link** panel that appears, click the **EDIT** button. Then from the **Link** page that appears, do the following to define the link's properties.

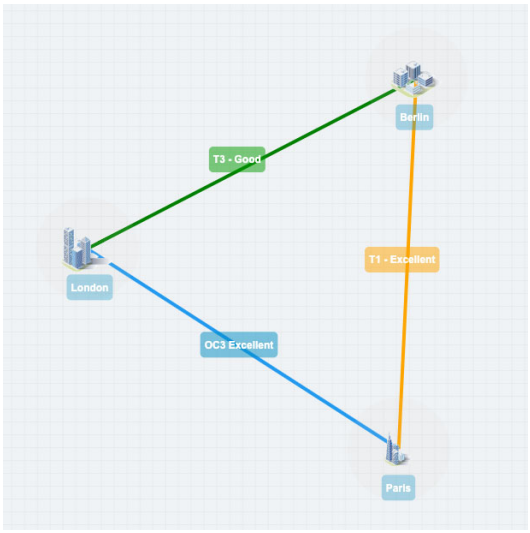
a. In the **Name** field, type an appropriate link name. The link name can contain alpha-numeric characters and spaces. In our example, do the following:
For the link going between the first node and the third node (which is currently called **Berlin<-->London**), type **`T3 - Good`**.
For the link going between the first node and the second node (which is currently called **Berlin<-->Paris**), type **`T1 - Excellent`**.
For the link going between the second node and the third cloud node (which is currently called **Paris<-->London**), type **`OC3 - Excellent`**.

b. In the **Description** field, type a description. The link name can contain alpha-numeric characters and spaces.

c. From the **Type** drop-down field, select an appropriate link type. In our example, do the following:
   For the link going between the first end node and the central cloud node (which is now called **T3 - Good**), select **WAN**.
   For the link going between the second node and the third node (which is now called **T1 - Excellent**), select **WAN**.
   For the link going between the third end node and the third node (which is now called **OC3 - Excellent**), select **WAN**.
d. From the **Subtype** drop-down field, an appropriate link type. In our example, do the following:
   For the link going between the first node and the third node (which is now called **T3 - Good**), select **T3/DS3**.
   For the link going between the second end node and the third node (which is now called **T1 - Excellent**), select **T1**.
   For the link going between the third end node and the third node (which is now called **OC3 - Excellent**), select **OC3**.
e. From the **Link Quality** drop-down field, select an appropriate link quality. In our example, do the following:
   For the link going between the first node and the third node (which is now called **T3 - Good**), select **Good**.
   For the link going between the second end node and the third node (which is now called **T1 - Excellent**), select **Excellent**.
   For the link going between the third end node and the third node (which is now called **OC3 - Excellent**), select **Excellent**.
f. From the **Link Color** drop-down field, select an appropriate link color. In our example, do the following:
   For the link going between the first end node and the third node (which is now called **T3 - Good**), select **Green**.
   For the link going between the second end node and the third node (which is now called **T1 - Excellent**), select **Orange**.
   For the link going between the third end node and the third node (which is now called **OC3 - Excellent**), leave the color set to **Blue**.
g. Click **OK** to submit the link properties.

At this point, everything is configured, except for the ports and routing table on the each node to

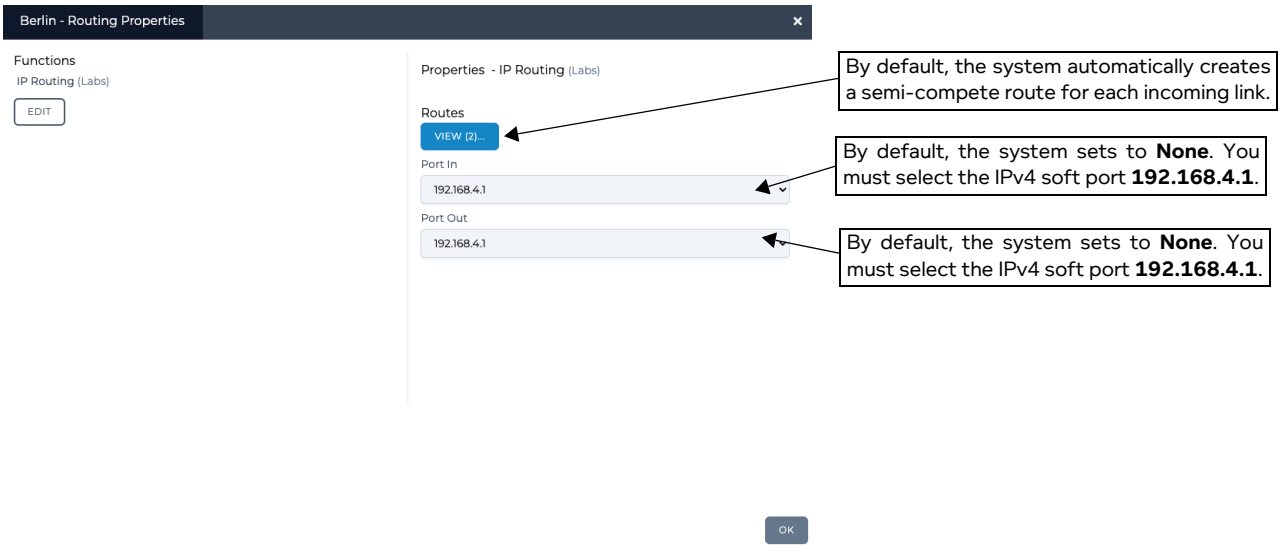
support the traffic between them (because they are from different networks).



The routing tables on each node must now be configured to route traffic between the different them, as follows:

- London node, two routes to support the traffic between the Berlin network (192.168.4.0) and Paris network (192.168.6.0), via the T3 - Good link and OC3 - Excellent link, respectively.
- Berlin node, two routes to support the traffic between the London network (192.168.5.0) and Paris network (192.168.6.0), via the T3 - Good link and T1 - Excellent link, respectively.
- Paris node, two routes to support the traffic between the London network (192.168.5.0) and Berlin network (192.168.6.0), via the T1 - Excellent link and OC3 - Excellent link, respectively.

5. Click on the Berlin node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button.
6. A **Berlin - Routing Properties** window appears, initially with the **Port In** and **Port Out** values set to **None**.



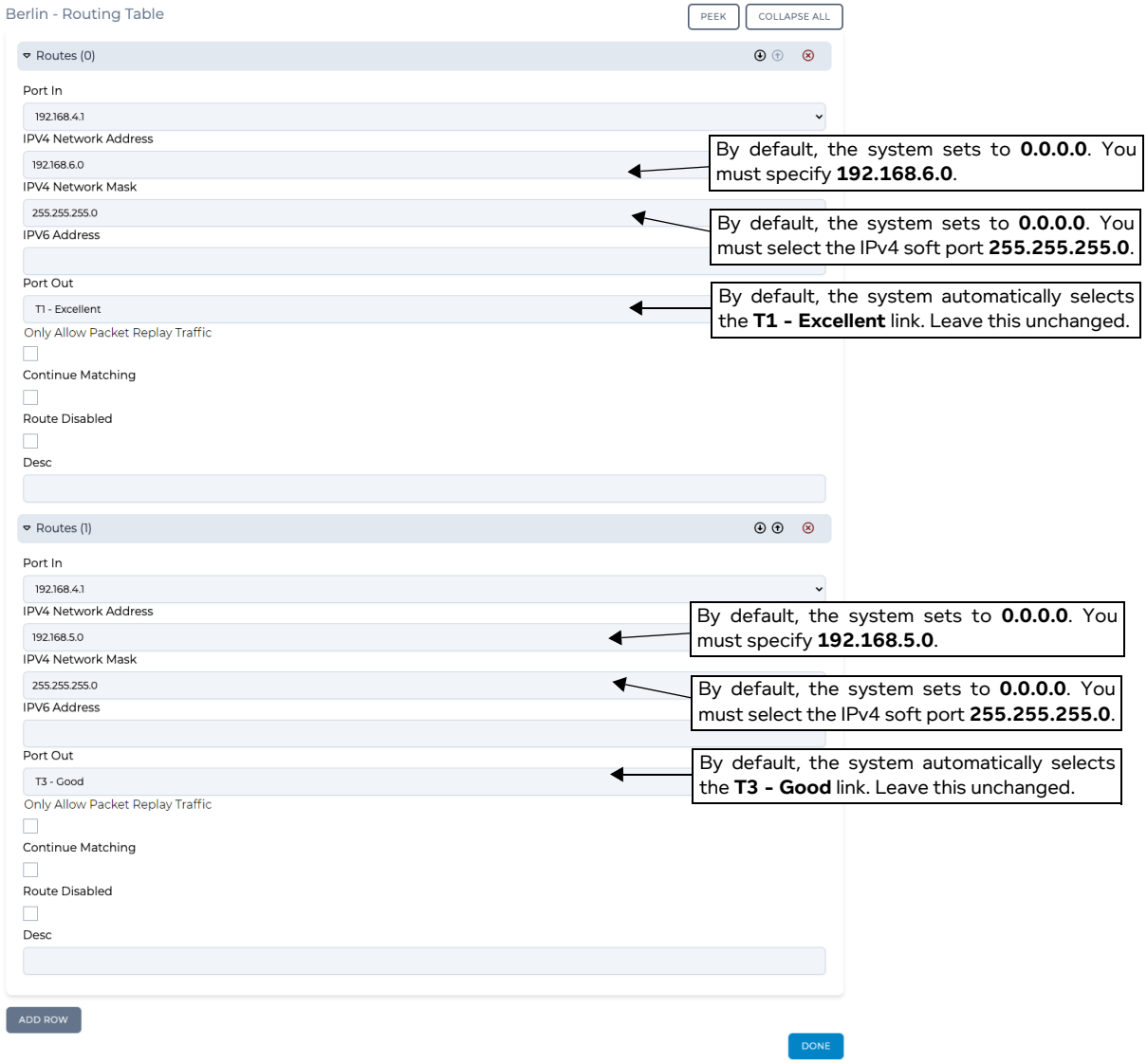
7. Do the following in the **Berlin - Routing Properties** window that appears to define the Berlin node's routing properties.
   a. In the **Port In** drop-down field, select an appropriate input port for the node. In our example, select **192.168.4.1**.

b. In the **Port Out** drop-down field, select an appropriate out port for the node. In our example, select **192.168.4.1**.

Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**192.168.4.1**), but the **Port Out** value is only used if no route is matched in the routing table.

c. Examine and edit the Berlin node's routing table by clicking on the **VIEW** button.

ILLUSTRATION 125 - EXAMPLE OF A SEMI-AUTO GENERATED ROUTE RULES FOR BERLIN NODE



We see that the NE-ONE intelligently and helpfully started to create two routes in the routing table (see *Illustration 125*). The NE-ONE automatically selects **Port In** value you specified in the **Berlin - Routing Properties** window, and automatically selects the connected link for the **Port Out**. The two initial routes in the routing table (that need to be manually completed) correspond to the following two incoming links:

Link object **T1 - Excellent** from the Paris node (which is defined to be acting as a gateway on IP address 192.168.6.1, netmask 255.255.255.0 (i.e. network 192.168.6.0)). By default the NE-ONE does not define the IP address or netmask for this route. For this route you will need to define the IP address and netmask. Since the Paris node at the end of the **T1 - Excellent** link is

acting as a gateway, you will define the IP address as the network address (i.e. 192.168.6.0) for the entire network behind the Paris gateway node, and also define the netmask (i.e. the same netmask as that of the Paris gateway node).

Link object **T3 - Good** from the London node (which is defined to be acting as a gateway on IP address 192.168.5.1, netmask 255.255.255.0 (i.e. network 192.168.5.0)). By default the NE-ONE does not define the IP address or netmask for this route. For this route you will need to define the IP address and netmask. Since the London node at the end of the **T3 - Good** link is acting as a gateway, you will define the IP address as the network address (i.e. 192.168.5.0) for the entire network behind the London gateway node, and also define the netmask (i.e. the same netmask as that of the London gateway node).

d. In the first route (called **Routes(0)**, with **Port Out** already set to **T1 - Excellent**), do the following to complete the route configuration going to the Paris node:
In the **IPv4 Network Address** field, type: **`192.168.6.0`**
In the **IPv4 Network Mask** field, type: **`255.255.255.0`**

Note: As with normal IPv4 routing the Network address you use could be any in the subnet i.e. 192.168.6.0-192.168.6.255, as the value used for matching purposes is taken after masking the address you give with the network mask, so, for example 192.168.6.45 masked with 255.255.255.0 is 192.168.1.0 and that is the value used in route matching.

e. In the second route (called **Routes(1)**, with **Port Out** already set to **T3 - Good**), do the following to complete the route configuration going to the London node:
In the **IPv4 Network Address** field, type: **`192.168.5.0`**
In the **IPv4 Network Mask** field, type: **`255.255.255.0`**

Note: As with normal IPv4 routing the Network address you use could be any in the subnet i.e. 192.168.5.0-192.168.5.255, as the value used for matching purposes is taken after masking the address you give with the network mask, so, for example 192.168.5.45 masked with 255.255.255.0 is 192.168.5.0 and that is the value used in route matching.

If necessary, to create additional routing rules within the routing table for the end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes are set up.

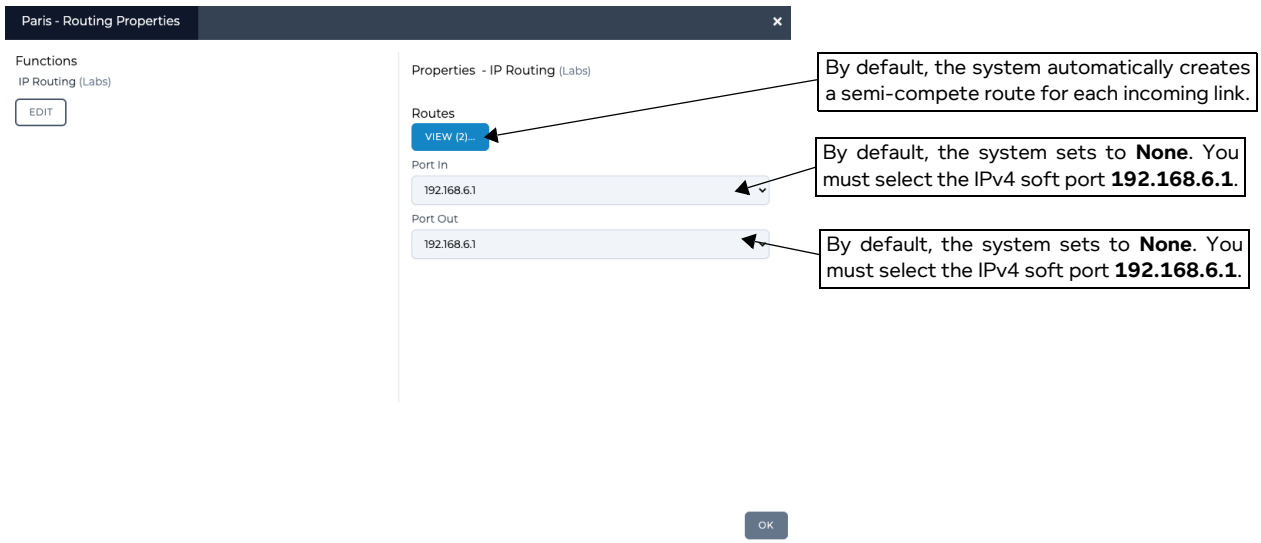
f. Click **DONE** to return to the **Berlin - Routing Properties** window.

g. In the **Berlin - Routing Properties** window, click **OK**.

You are returned to the **Multi-Point Designer** page.

8. Click on the Paris node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button.
9. A **Paris - Routing Properties** window appears, initially with the **Port In** and **Port Out** values set to

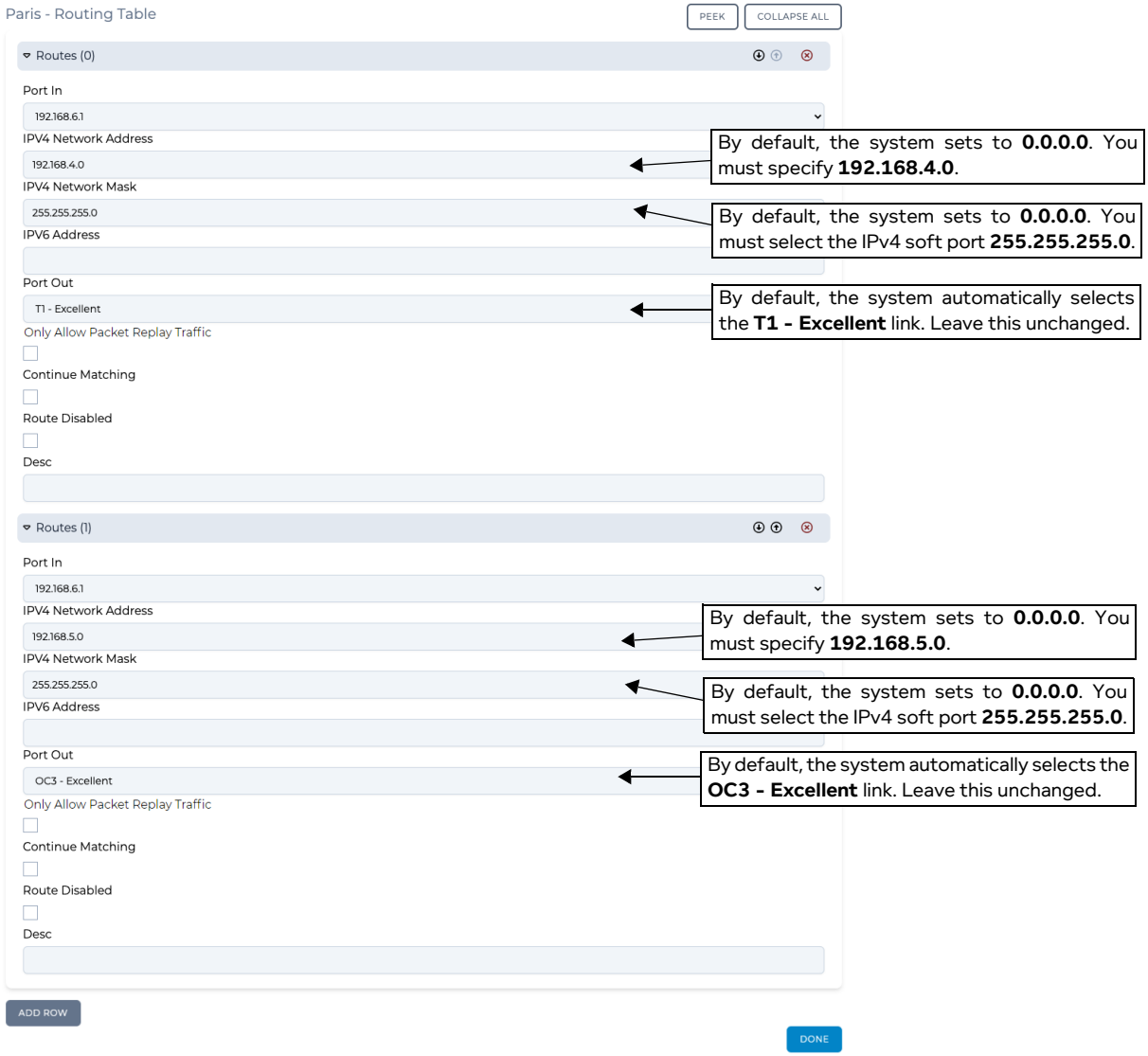
None.



10. Do the following in the **Paris - Routing Properties** window that appears to define the Paris node's routing properties.
    a. In the **Port In** drop-down field, select an appropriate input port for the node. In our example, select **192.168.6.1**.
    b. In the **Port Out** drop-down field, select an appropriate out port for the node. In our example, select **192.168.6.1**.

       Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**192.168.6.1**), but the **Port Out** value is only used if no route is matched in the routing table.
    c. Examine and edit the Paris node's routing table by clicking on the **VIEW** button.

ILLUSTRATION 126 - EXAMPLE OF SEMI-AUTO GENERATED ROUTE RULES FOR PARIS NODE



We see that the NE-ONE intelligently and helpfully started to create two routes in the routing table (see *Illustration 126*). The NE-ONE automatically selects **Port In** value you specified in the **Paris - Routing Properties** window, and automatically selects the connected link for the **Port Out**. The two initial routes in the routing table (that need to be manually completed) correspond to the following two incoming links:

Link object **T1 - Excellent** from the Berlin node (which has IP address 192.168.4.1, netmask 255.255.255.0 (i.e. network 192.168.4.0)). By default the NE-ONE does not define the IP address or netmask for this route. For this route you will need to define the IP address and netmask. Since the Berlin node at the end of the **T1 - Excellent** link is in the same network as the gateway (192.168.4.254), you will define the IP address as the network address (i.e. 192.168.4.0) and netmask (i.e. 255.255.255.0) for the entire network that the Berlin node belongs to.

Link object **T3 - Good** from the London node (which is defined to be acting as a gateway on IP address 192.168.5.1, netmask 255.255.255.0 (i.e. network 192.168.5.0)). By default the NE-ONE does not define the IP address or netmask for this route. For this route you will need to define the IP address and netmask. Since the London node at the end of the **T3 - Good** link is

acting as a gateway, you will define the IP address as the network address (i.e. 192.168.5.0) for the entire network behind the London gateway node, and also define the netmask (i.e. the same netmask as that of the London gateway node).

d. In the first route (called **Routes(0)**, with **Port Out** already set to **T1 - Excellent**), do the following to complete the route configuration going to the Berlin node:
In the **IPv4 Network Address** field, type: **192.168.4.0**
In the **IPv4 Network Mask** field, type: **255.255.255.0**

Note: As with normal IPv4 routing the Network address you use could be any in the subnet i.e. 192.168.4.0-192.168.4.255, as the value used for matching purposes is taken after masking the address you give with the network mask, so, for example 192.168.4.45 masked with 255.255.255.0 is 192.168.4.0 and that is the value used in route matching.

e. In the second route (called **Routes(1)**, with **Port Out** already set to **T3 - Good**), do the following to complete the route configuration going to the London node:
In the **IPv4 Network Address** field, type: **192.168.5.0**
In the **IPv4 Network Mask** field, type: **255.255.255.0**

Note: As with normal IPv4 routing the Network address you use could be any in the subnet i.e. 192.168.5.0-192.168.5.255, as the value used for matching purposes is taken after masking the address you give with the network mask, so, for example 192.168.5.45 masked with 255.255.255.0 is 192.168.5.0 and that is the value used in route matching.

If necessary, to create additional routing rules within the routing table for the end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes are set up.

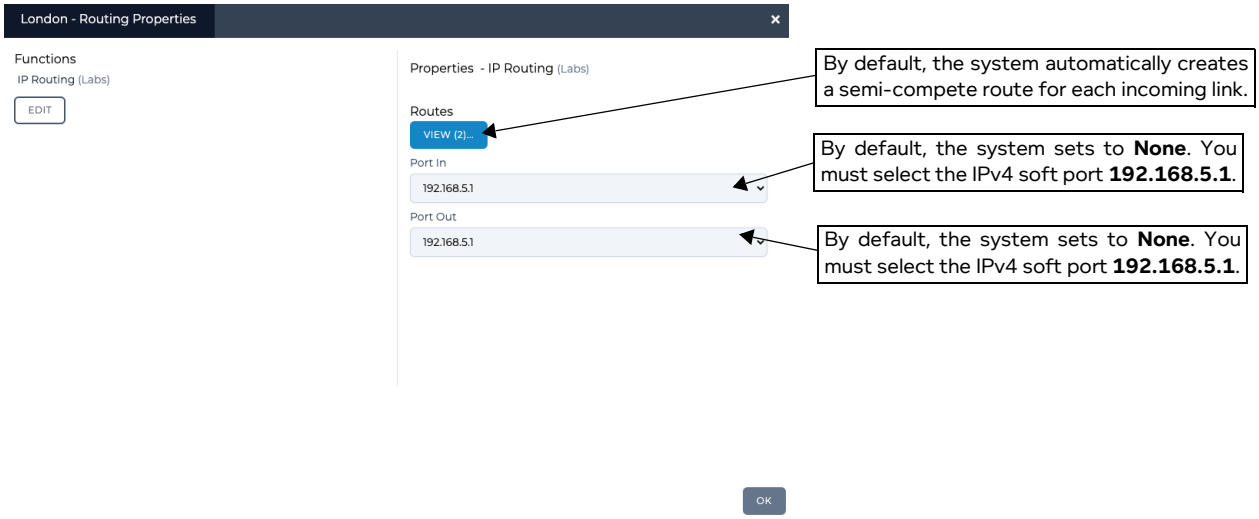
f. Click **DONE** to return to the **Paris - Routing Properties** window.

g. In the **Paris - Routing Properties** window, click **OK**.

You are returned to the **Multi-Point Designer** page.

11. Click on the London node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button.

12. A **London - Routing Properties** window appears, initially with the **Port In** and **Port Out** values set to **None**.



13. Do the following in the **London - Routing Properties** window that appears to define the Paris node's routing properties.

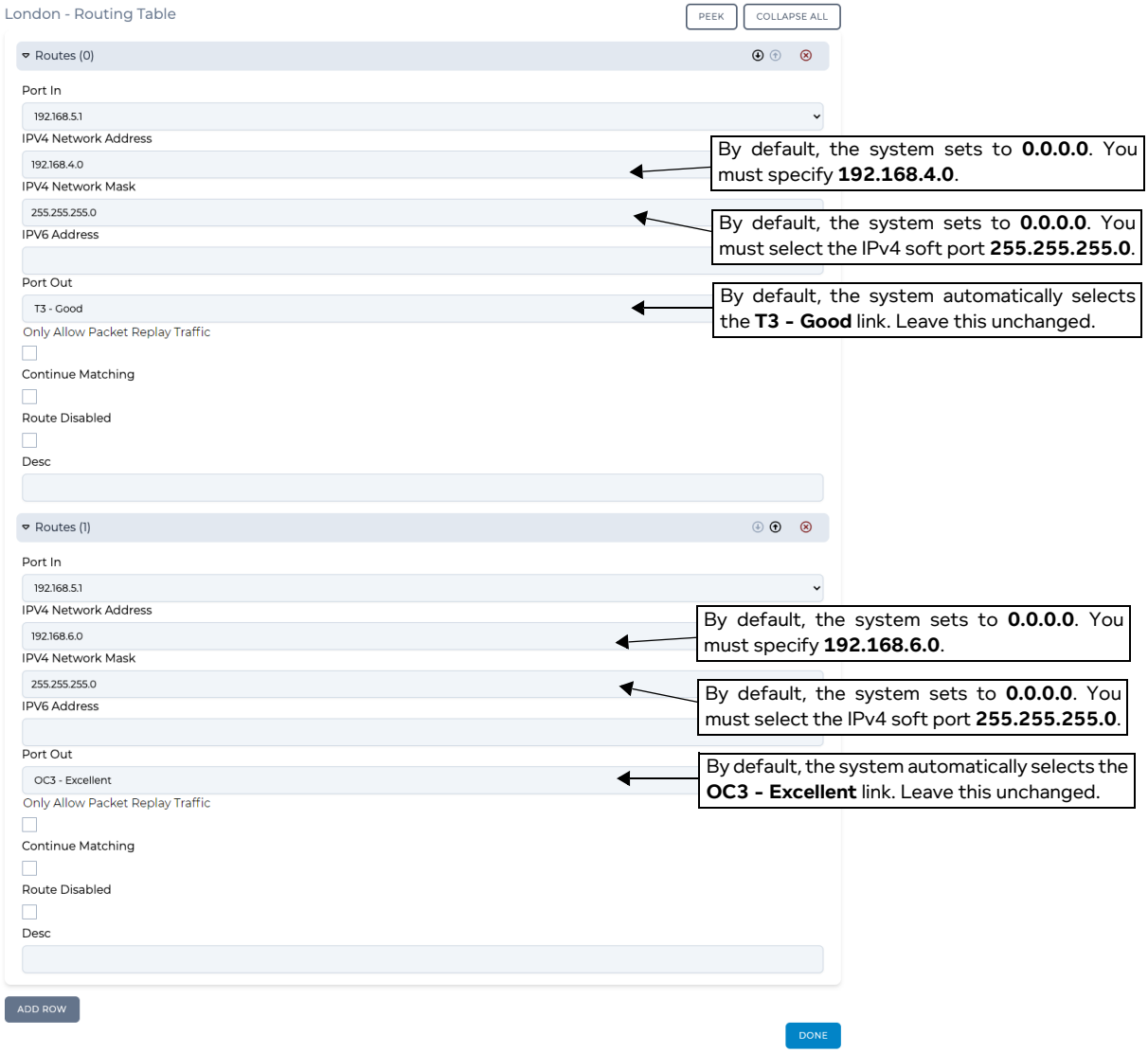
a. In the **Port In** drop-down field, select an appropriate input port for the node. In our example, select **192.168.5.1**.

b. In the **Port Out** drop-down field, select an appropriate out port for the node. In our example, select **192.168.5.1**.

Note: It may seem very strange at first, that the **Port In** and **Port Out** have the same value (**192.168.5.1**), but the **Port Out** value is only used if no route is matched in the routing table.

c. Examine and edit the London node's routing table by clicking on the **VIEW** button.

ILLUSTRATION 127 - EXAMPLE OF SEMI-AUTO GENERATED ROUTE RULES FOR LONDON NODE



We see that the NE-ONE intelligently and helpfully started to create two routes in the routing table (see *Illustration 127*). The NE-ONE automatically selects **Port In** value you specified in the **London - Routing Properties** window, and automatically selects the connected link for the **Port Out**. The two initial routes in the routing table (that need to be manually completed) correspond to the following two incoming links:

Link object **T3 - Good** from the Berlin node (which has IP address 192.168.4.1, netmask 255.255.255.0 (i.e. network 192.168.4.0)). By default the NE-ONE does not define the IP

address or netmask for this route. For this route you will need to define the IP address and netmask. Since the Berlin node at the end of the **T3 - Good** link is in the same network as the gateway (192.168.4.254), you will define the IP address as the network address (i.e. 192.168.4.0) and netmask (i.e. 255.255.255.0) for the entire network that the Berlin node belongs to.

Link object **OC - Excellent** from the Paris node (which is defined to be acting as a gateway on IP address 192.168.6.1, netmask 255.255.255.0 (i.e. network 192.168.6.0)). By default the NE-ONE does not define the IP address or netmask for this route. For this route you will need to define the IP address and netmask. Since the Paris node at the end of the **OC3 - Excellent** link is acting as a gateway, you will define the IP address as the network address (i.e. 192.168.6.0) for the entire network behind the London gateway node, and also define the netmask (i.e. the same netmask as that of the London gateway node).

d. In the first route (called **Routes(0)**, with **Port Out** already set to **T3 - Good**), do the following to complete the route configuration going to the Berlin node:
In the **IPv4 Network Address** field, type: **192.168.4.0**
In the **IPv4 Network Mask** field, type: **255.255.255.0**

Note: As with normal IPv4 routing the Network address you use could be any in the subnet i.e. 192.168.4.0-192.168.4.255, as the value used for matching purposes is taken after masking the address you give with the network mask, so, for example 192.168.4.45 masked with 255.255.255.0 is 192.168.4.0 and that is the value used in route matching.

e. In the second route (called **Routes(1)**, with **Port Out** already set to **O3 - Excellent**), do the following to complete the route configuration going to the Paris node:
In the **IPv4 Network Address** field, type: **192.168.6.0**
In the **IPv4 Network Mask** field, type: **255.255.255.0**

Note: As with normal IPv4 routing the Network address you use could be any in the subnet i.e. 192.168.6.0-192.168.6.255, as the value used for matching purposes is taken after masking the address you give with the network mask, so, for example 192.168.6.45 masked with 255.255.255.0 is 192.168.6.0 and that is the value used in route matching.

If necessary, to create additional routing rules within the routing table for the end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes are set up.

f. Click **DONE** to return to the **London - Routing Properties** window.

g. In the **London - Routing Properties** window, click **OK**.

You are returned to the **Multi-Point Designer** page.

At this stage the routing configuration is now complete for each of the nodes.

14. Save the finalized Fully Meshed Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

The Fully Meshed Multi-Point network will appear in the **Multi-Point Designer** page as shown in *Illustration 120* on page 417, and is ready to be run (i.e. played).

If you click the **PLAY** button in the **Multi-Point Designer** page, the Cloud Multi-Point network starts running and its associated objects appear in the **Statistics** page (see *Illustration 128*).

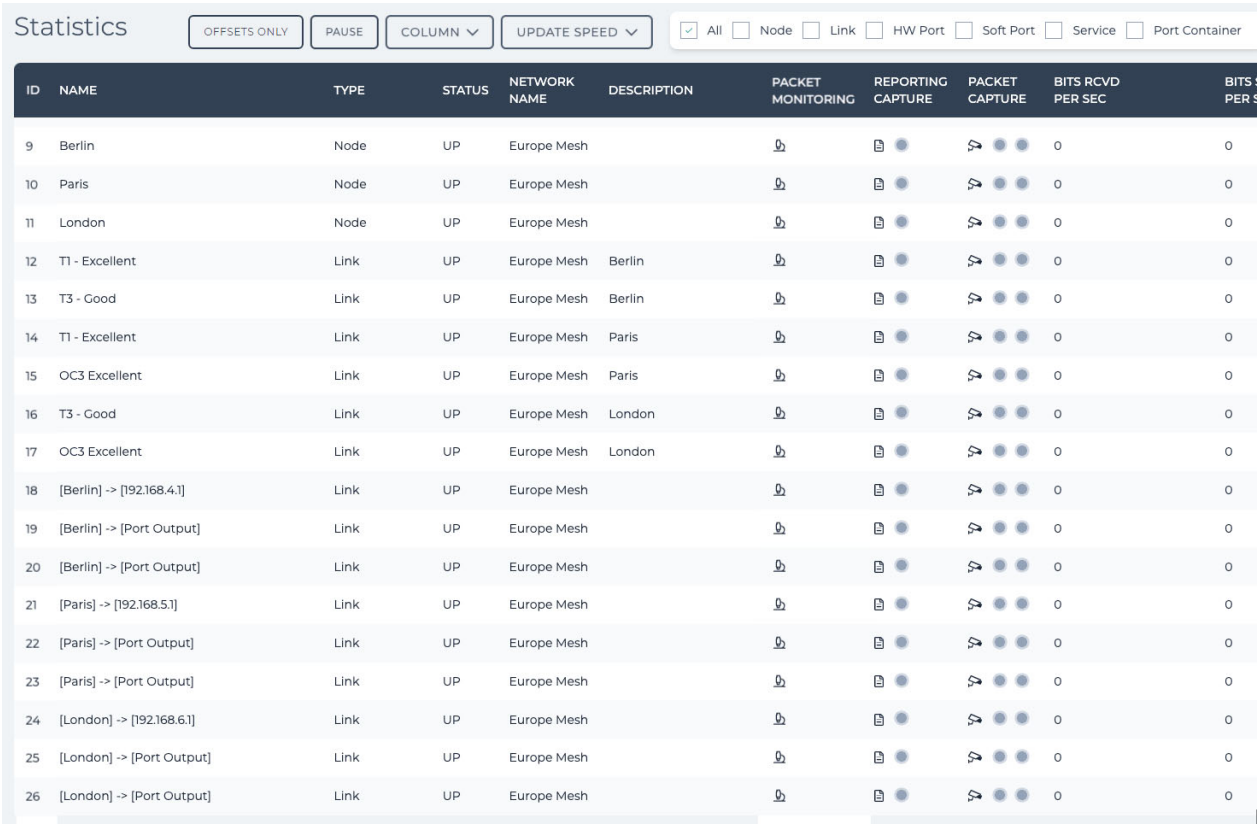
The nice thing about fully meshed networks is that they often represent the real world, where connections from one location to another do not go via some central hub location or cloud. However, what is not so nice is the complexity. We witnessed with our example (simple three nodes, with one link between each node) that there was still some routing to configure to get traffic between the nodes. 3 nodes gives 3 full duplex circuits, 4 nodes gives 6 full duplex lines, etc. In full generality N

nodes, gives (N2-N)/2 full duplex lines and that could be a lot of lines and a lot of complexity.

So, to make that much simpler, the NE-ONE provides the ability to create such networks out as though they were either on of the following network topology types:

- Hub and Spoke (as the example in *Creating Hub and Spoke Networks* on page 451), but then define the central point (i.e. the hub) as having varying properties depending on addresses, ports etc. of incoming and outgoing traffic.
- Cloud (as the example in *Creating Cloud Networks* on page 434), but then define the central Cloud node as having varying properties depending on addresses, ports etc. of incoming and outgoing traffic.

ILLUSTRATION 128 - EXAMPLE FULLY MESHED NETWORK ASSOCIATED OBJECTS VISIBLE IN THE STATISTICS PAGE



ID	NAME	TYPE	STATUS	NETWORK NAME	DESCRIPTION	PACKET MONITORING	REPORTING CAPTURE	PACKET CAPTURE	BITS RCVD PER SEC	BITS PER S
9	Berlin	Node	UP	Europe Mesh					0	0
10	Paris	Node	UP	Europe Mesh					0	0
11	London	Node	UP	Europe Mesh					0	0
12	T1 - Excellent	Link	UP	Europe Mesh	Berlin				0	0
13	T3 - Good	Link	UP	Europe Mesh	Berlin				0	0
14	T1 - Excellent	Link	UP	Europe Mesh	Paris				0	0
15	OC3 Excellent	Link	UP	Europe Mesh	Paris				0	0
16	T3 - Good	Link	UP	Europe Mesh	London				0	0
17	OC3 Excellent	Link	UP	Europe Mesh	London				0	0
18	[Berlin] -> [192.168.4.1]	Link	UP	Europe Mesh					0	0
19	[Berlin] -> [Port Output]	Link	UP	Europe Mesh					0	0
20	[Berlin] -> [Port Output]	Link	UP	Europe Mesh					0	0
21	[Paris] -> [192.168.5.1]	Link	UP	Europe Mesh					0	0
22	[Paris] -> [Port Output]	Link	UP	Europe Mesh					0	0
23	[Paris] -> [Port Output]	Link	UP	Europe Mesh					0	0
24	[London] -> [192.168.6.1]	Link	UP	Europe Mesh					0	0
25	[London] -> [Port Output]	Link	UP	Europe Mesh					0	0
26	[London] -> [Port Output]	Link	UP	Europe Mesh					0	0

4-3. Creating Cloud Networks

In this example, we need to connect two private (sub) networks e.g. 192.168.5.0/24 and 192.168.6.0/24 to each other and also out to the corporate network and thus to the Internet. The structure for connection is a Cloud network.

These subnets are connected to a VLAN (802.1Q) capable switch which has up to now been routing (it is a layer 3 switch) between these subnets and the main corporate network.

Unfortunately, the switch cannot create WAN conditions between these subnets and in the “real world”. That is, in the non-test environment these subnets will be in geographically dispersed locations (for example, London, Berlin, and Paris).

The requirement is to connect the NE-ONE to the VLAN corporate switch and produce a Cloud WAN between these subnets with the minimum amount of changes.

We are told that:

- The corporate network in Berlin has Network 192.168.4.0 is on VLAN 601 with gateway 192.168.4.254.
- The Paris test site has Network 192.168.6.0 is on VLAN 602 with gateway 192.168.6.1.
- The London test site has Network 192.168.5.0 is on VLAN 603 with gateway 192.168.5.1.
- The IP address for the NE-ONE to have in the corporate network is 192.168.4.100.

In the following example (*Illustration 130* on page 436), the Cloud network topology template is used to create a cloud based Multi-Point network, with the following configuration:

- Berlin (end node):
  - Input port : 192.168.4.1
  - Output port : 192.168.4.1
  - One link : Type : WAN, T3 - Good, with link name T3 - Good
  - Routing table : one route with input port as 192.168.4.1, output port as T3 - Good : this routes all traffic to/from the Berlin end node into the cloud, with no packet filtering.
- London (end node):
  - Input port : 192.168.5.1
  - Output port : 192.168.5.1
  - One link : Type : WAN, OC3 - Excellent, with link name OC3 - Excellent
  - Routing table : one route with input port as 192.168.5.1, output port as OC3 - Excellent : this routes all traffic to/from the London end node into the cloud, with no packet filtering.
- Paris (end node):
  - Input port : 192.168.6.1
  - Output port : 192.168.6.1
  - One link : Type : WAN, T1 - Excellent, with link name T1 - Excellent
  - Routing table : one route with input port as 192.168.6.1, output port as T1 - Excellent : this routes all traffic from the Paris end node into the cloud, with no packet filtering.
- Cloud node (using the automatically system applied Cloud Object (Labs) function)

  With the following cloud link rule:
  - Catch All : this cloud link rule accepts traffic from all three inbound links (i.e. no input port defined), with no packet filtering.

  With the following routing table rules (i.e. one for each inbound link):
  - Input port as None, output port as T3 - Good, IP address 192.168.4.1 and netmask 255.255.255.0 : this routes all traffic to/from the Berlin end node into the cloud, with no packet

filtering.

- Input port as None, output port as OC3 - Excellent, IP address 192.168.5.1 and netmask 255.255.255.0 : this routes all traffic to/from the London end node into the cloud, with no packet filtering.
- Input port as None, output port as T1 - Excellent, IP address 192.168.6.1 and netmask 255.255.255.0 : this routes all traffic from the Paris end node into the cloud, with no packet filtering.

Note:

An assumption is made that the total I/O we are handling can be covered in total by one of the NE-ONE's hardware ports, if this is not true then a modified version of this example can be produced by using more than one NE-ONE hardware ports.

ILLUSTRATION 129 - EXAMPLE SIMPLE CLOUD NETWORK (MULTI-POINT WORKSPACE)

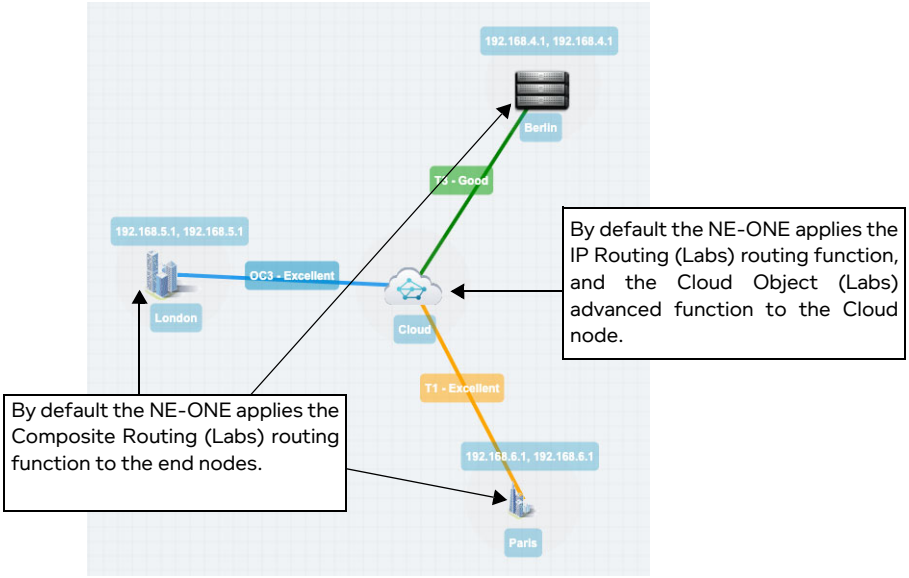
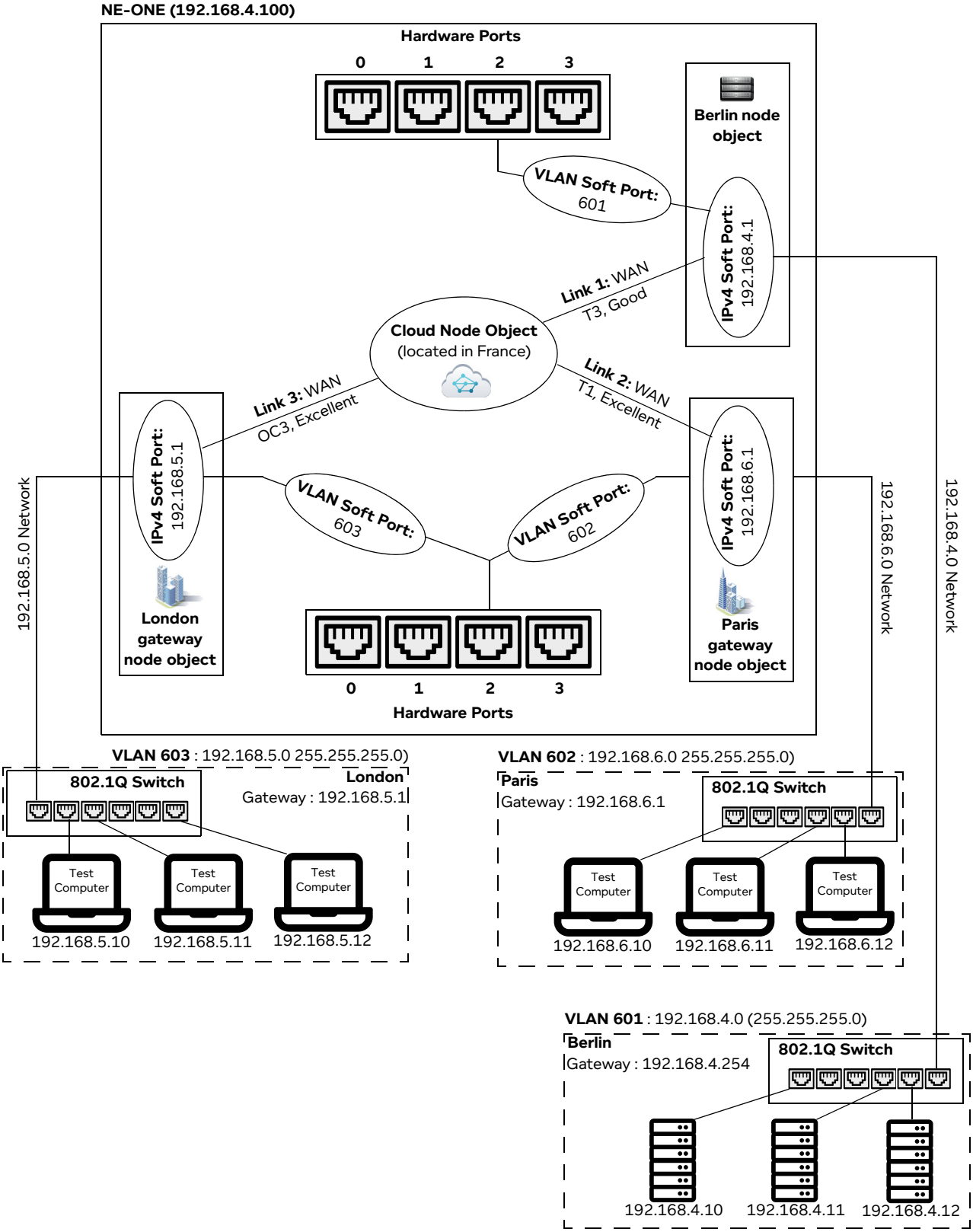


ILLUSTRATION 130 - EXAMPLE CLOUD NETWORK (WITH VLAN AND IPV4 SOFT PORTS)

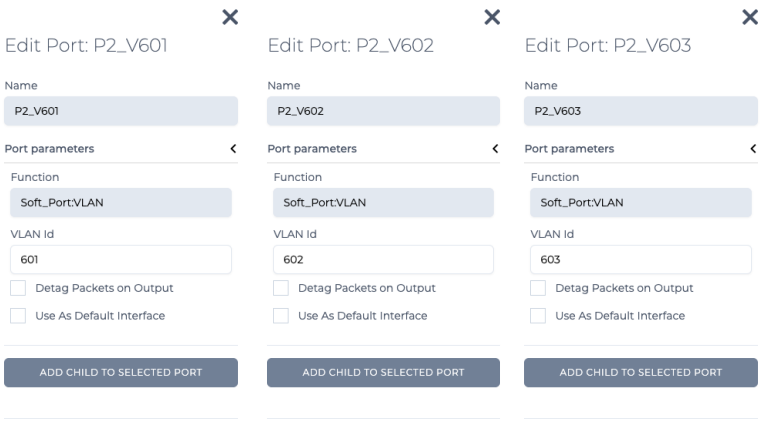


4-3-1. Prerequisite Steps Performed by an Admin User

In order for a non-admin user to create a Cloud network based on this example, an admin user needs to do the following prerequisite steps:

1. Configure the NE-ONE with a static IP address of 192.168.4.50 according to the steps described in *Configuring the Management Port Settings* on page 60 of *Chapter 4*, *Installation and Configuration*.
2. Request to the corporate network administrator that a VLAN (802.1Q) Trunk port is set up on the switch, trunking at least VLANs 601, 602, and 603.
3. Request to the corporate network administrator that the corporate switch's routing addresses 192.168.5.1 and 192.168.6.1 are removed from its routing tables, as the NE-ONE will take over that function.
4. Connect NE-ONE hardware port (in our example, hardware port 2) to that Trunk port with a suitable cable.
5. Create one VLAN soft port for each required VLANs (601, 602, and 603) on the NE-ONE's hardware port (in our example, hardware port 2) according the steps described in *Creating a VLAN Soft Port* on page 107 in *Chapter 5*, *Ports and Services Management*, with each VLAN soft port having **Detag Packets** on **Output and Default Interface** settings disabled (unticked), as shown in *Illustration 107*.

ILLUSTRATION 131 - VLAN SOFT PORT CONFIGURATIONS



VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2

Note: The naming convention of the VLAN soft ports uses the P2 prefix to indicate that these ports are children of hardware port 2, where VNNN denotes a VLAN port with that ID (tag). You can use any soft port names you want, but they should be meaningful.

6. Create and assign IPv4 soft ports to the VLAN soft ports. To do this, within each of the VLAN soft ports, create an IPv4 soft port according the steps described in *Creating an IPv4 Soft Port* on page 114 in *Chapter 5*, *Ports and Services Management*, with the following settings (*Illustration 140* on page 455).
   - VLAN 601 soft port contains IPv4 soft port called 192.168.4.1, with IP address 192.168.4.1, netmask 255.255.255.0, and gateway 192.168.4.254.
   - VLAN 602 soft port contains IPv4 soft port called 192.168.6.1, with IP address 192.168.6.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway as there are no other routers in the network 192.168.6.0, only the NE-ONE itself which is acting as the gateway.
   - VLAN 603 soft port contains IPv4 soft port called 192.168.5.1, with IP address 192.168.5.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway

as there are no other routers in the network 192.168.6.0, only the NE-ONE itself which is acting as the gateway.

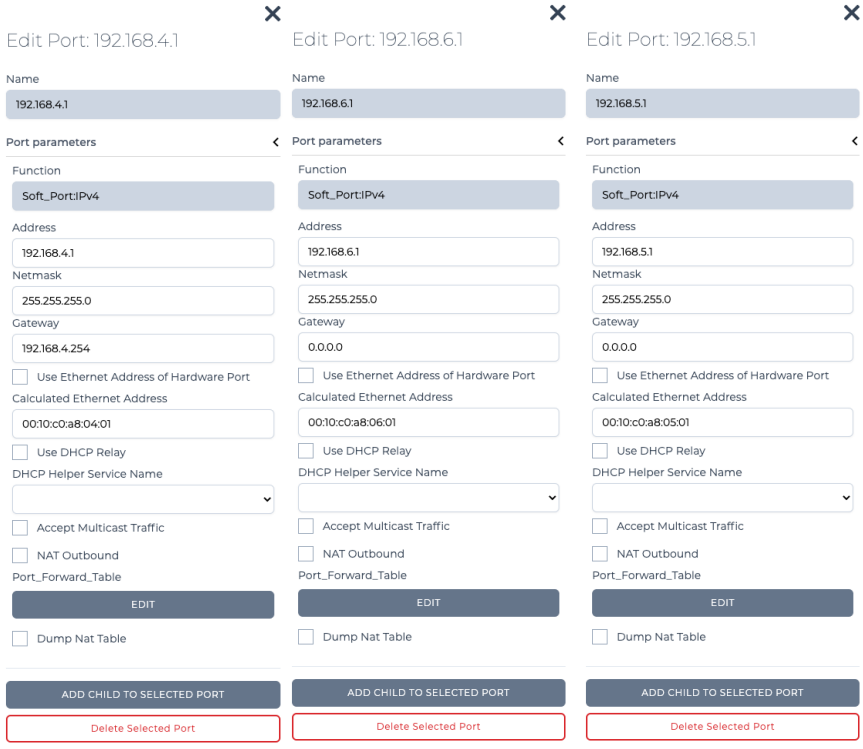
Note: Notice that there is only one IPv4 soft port in each VLAN soft port, as we only require one IP address in each VLAN network. Also, again for clarity, name given to each of the IPv4 soft ports is the same name as its IP address.

The resulting soft port layout for this example is shown in *Illustration 141* on page 456, which give a non-admin user all the soft ports they need to create a Cloud type Multi-Point network based on our example described above.

Note: Our example is for three end nodes, a cloud node, and three links with three VLAN soft ports and three IPv4 soft ports. This is easily extensible to much larger networks with many more end nodes, links, VLAN soft ports and IPv4 soft ports.

7. Assign the created IPv4 soft ports (192.168.4.1, 192.168.5.1, and 192.168.6.1) to the intended non-admin user who will create the Cloud Multi-Type network according to the steps described in *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205 in *Chapter 6*, *User Administration*.

ILLUSTRATION 132 - IPV4 SOFT PORT CONFIGURATIONS FOR CLOUD SPOKE EXAMPLE

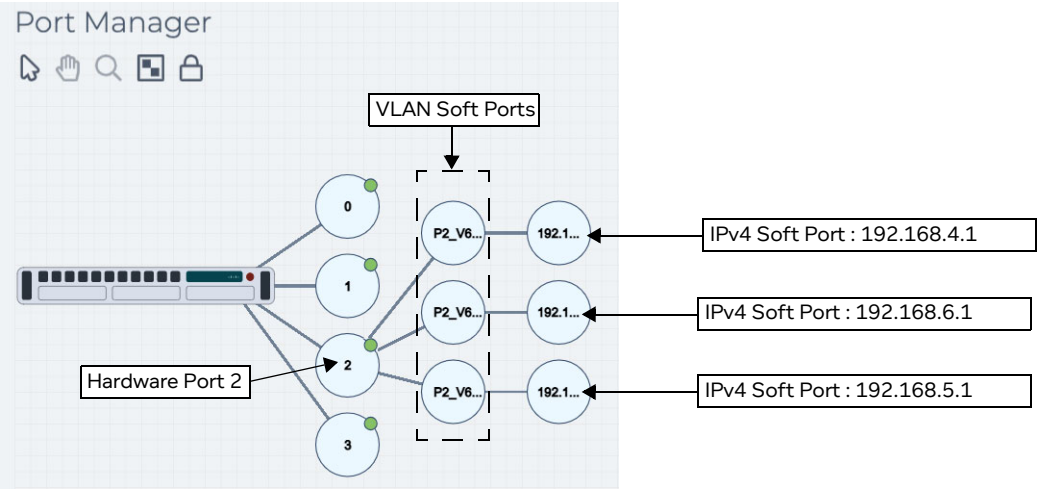


IPv4 Soft Port assigned to VLAN Soft Port 601

IPv4 Soft Port assigned to VLAN Soft Port 602

IPv4 Soft Port assigned to VLAN Soft Port 603

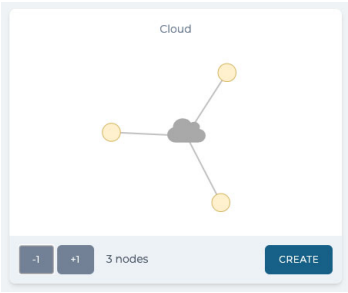
ILLUSTRATION 133 - RESULTING VLAN AND IPV4 SOFT PORT LAYOUT FOR CLOUD EXAMPLE



4-3-2. Cloud Network Creation Steps Performed by a Non Admin User

Once the NE-ONE has been configured by an admin user according to *Section 4-3-1*, a non-admin user (or admin user) can create a Cloud Multi-Point network for the example described above, using the following steps:

1. Launch the **Multi-Point Designer** page, and choose the Cloud network topology template, using the following sub-steps:
   a. Select **Networks** from the Menu.
   b. From the **Networks** page (see *Illustration 4* on page 42) that appears, click **New Network**.
   c. From the **Network Wizard** page (see *Illustration 84*) that appears, in the **Cloud** panel, click the **+1** or **-1** icon to increase or decrease the total number of end nodes used by the Cloud network topology template, then click **CREATE**.



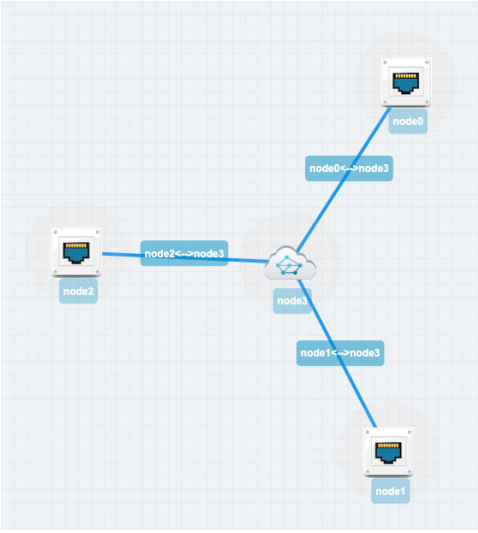
   In our example we want three nodes, so click the **-1** button three times until only three nodes are shown in the Cloud panel, then click **CREATE**.
   d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`Europe Cloud`**), then click **OK**.

A new (i.e. undefined) Multi-Node network appears based on the selected Cloud network topology template you selected. At this stage, nothing is configured in the cloud network. You will need to configure the:

- routing for each of the nodes (i.e. assign input and output ports, and optionally define routing rules),
- links between each of the end nodes and the central cloud node
- routing table of the cloud node (i.e. at least three routes for each of the end nodes going into the

cloud node)

- at least one cloud link rule for the cloud node



2. From the **Multi-Point Designer** page, optionally tick the **Show node names**, **Show link names**, and **Show node ports** check boxes from the **VIEW** drop-down menu.

   Note: This optional step is useful in letting you identify what still needs configuring in the Multi-Point network. Undefined nodes have the generic names **node0**, **node1**, **node2**, **node3**, etc. Undefined links have the format **node0<-->node3**, **node1<-->node3**, **node2<-->node3**, etc. End nodes with undefined input and output ports show nothing.

3. For each of the end nodes and cloud node in the Workspace, click on the end node/cloud node, and from the **Edit node** panel that appears do the following to define the node's basic properties.

   a. In the **Name** field, type an appropriate node name. The node name can contain alpha-numeric characters and spaces. In our example, do the following:

   For the first end node (which was initially called node0), type **`Berlin`**.

   For the second end node (which was initially called node1), type **`Paris`**

   For the third end node (which was initially called node2), type **`London`**.

   For the central cloud node (which was initially called node3), type **`Cloud`**.

   b. In the **Description** field, optionally type an appropriate description.The node description can contain alpha-numeric characters and spaces.

   c. From the **Country** drop-down field, select an appropriate country to define the country where the node is located. In our example, do the following:

   For the first end node, select **Germany**.

   For the second end node, select **France**.

   For the third end node, select **United Kingdom**.

   For the central cloud node, select **France**.

   Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

   d. From the **Choose a location** drop-down field, select and appropriate area for the location. In our example, do the following:

   For the first end node, select a location within **Berlin**.

   For the second end node, select a location within **Paris**.

For the third end node, select a location within **London**.

For the central cloud node, select a location somewhere within **France**.

Note: You can start typing the location in order to select it quickly from the list of locations. The list of locations proposed depend on the string you specified in the **Name** field. In this case for example, locations in an around London are proposed.

e. Click on the icon, and from the dialog box that appears click on the an appropriate icon, and then click **OK**.

In our example, do the following:

For the first end node, select the rack servers icon from the **IT** category in the **Node Icons** panel.

For the second end node, select the four buildings point icon from the **Standard** category in the **Node Icons** panel.

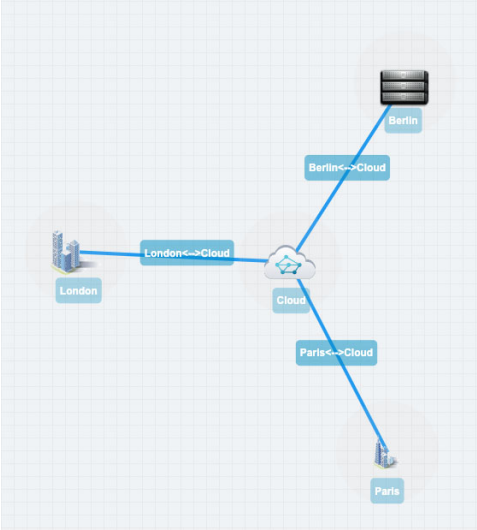
For the third end node, select the commercial center icon from the **Standard** category in the **Node Icons** panel.

For the central cloud node, leave it set to the cloud icon.

f. Click to ✕ close the **Edit node** panel.

At this stage the basic properties of each of the end nodes and cloud node are defined. Since the node names were changed, the link names automatically update to include the node names, such that:

- **node0<-->node3** becomes **Berlin<-->Cloud**
- **node1<-->node3** becomes **Paris<-->Cloud**
- **node2<-->node3** becomes **London<-->Cloud**



Next, define the properties of links between each of the end nodes. In the example below, the automatically assigned link names are changed, however this is purely optional.

4. For each of the links in the Workspace, click on the link, and from the **Edit link** panel that appears, click the **EDIT** button. Then from the **Link** page that appears, do the following to define the link's properties.

a. In the **Name** field, type an appropriate link name. The link name can contain alpha-numeric characters and spaces. In our example, do the following:

For the link going between the first end node and the central cloud node (which is currently called **Berlin<-->Cloud**), type **`T3 – Good`**.
For the link going between the second end node and the central cloud node (which is currently called **Paris<-->Cloud**), type **`T1 – Excellent`**.
For the link going between the third end node and the central cloud node (which is currently called **London<-->Cloud**), type **`OC3 – Excellent`**.

b. In the **Description** field, type a description. The link name can contain alpha-numeric characters and spaces.

c. From the **Type** drop-down field, select an appropriate link type. In our example, do the following:
For the link going between the first end node and the central cloud node (which is now called **T3 - Good**), select **WAN**.
For the link going between the second end node and the central cloud node (which is now called **T1 - Excellent**), select **WAN**.
For the link going between the third end node and the central cloud node (which is now called **OC3 - Excellent**), select **WAN**.

d. From the **Subtype** drop-down field, an appropriate link type. In our example, do the following:
For the link going between the first end node and the central cloud node (which is now called **T3 - Good**), select **T3/DS3**.
For the link going between the second end node and the central cloud node (which is now called **T1 - Excellent**), select **T1**.
For the link going between the third end node and the central cloud node (which is now called **OC3 - Excellent**), select **OC3**.

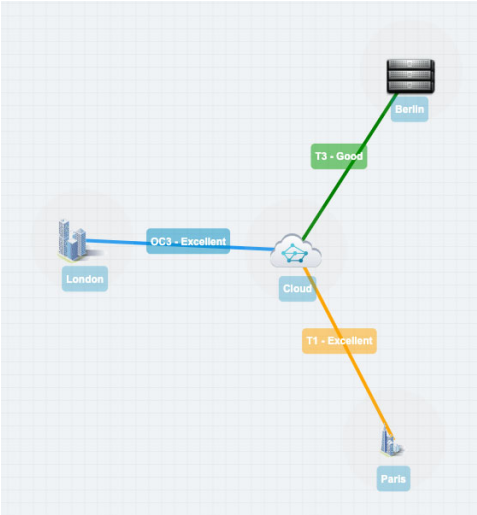
e. From the **Link Quality** drop-down field, select an appropriate link quality. In our example, do the following:
For the link going between the first end node and the central cloud node (which is now called **T3 - Good**), select **Good**.
For the link going between the second end node and the central cloud node (which is now called **T1 - Excellent**), select **Excellent**.
For the link going between the third end node and the central cloud node (which is now called **OC3 - Excellent**), select **Excellent**.

f. From the **Link Color** drop-down field, select an appropriate link color. In our example, do the following:
For the link going between the first end node and the central cloud node (which is now called **T3 - Good**), select **Green**.
For the link going between the second end node and the central cloud node (which is now called **T1 - Excellent**), select **Orange**.
For the link going between the third end node and the central cloud node (which is now called **OC3 - Excellent**), leave the color set to **Blue**.

g. Click **OK** to submit the link properties.

At this stage the link names are now defined to something meaningful within your Cloud Multi-Point

network.



The link names you defined will appear as selectable output ports within the routing table you define for the central cloud node.

5. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click the **SAVE** button.
6. For each of the end nodes in the Workspace, click on the end node, and from the **Edit node** panel that appears, click the **ROUTES** button, then do the following in the **Routing Properties** window that appears to define the end node's routing properties.
   a. In the **Port In** drop-down field, select an appropriate input port for the end node. In our example, do the following:

      For the first end node (i.e. Berlin), select **192.168.4.1**.

      For the second end node (i.e. Paris), select **192.168.5.1**.

      For the third end node (i.e. London), select **192.168.6.1**.
   b. In the **Port Out** drop-down field, select an appropriate out port for the end node. In our example, do the following:

      For the first end node (i.e. Berlin), select **192.168.4.1**.

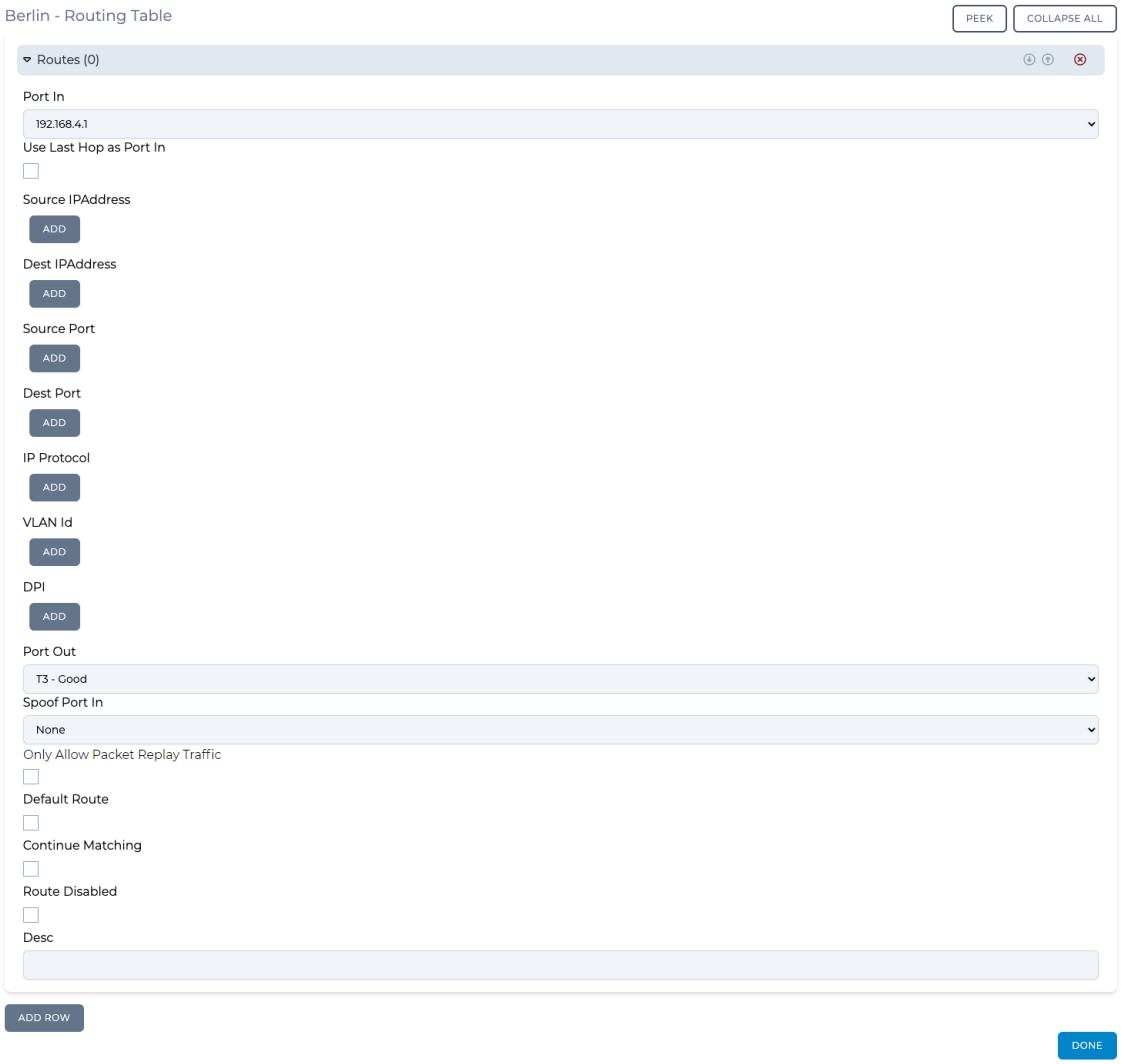
      For the second end node (i.e. Paris), select **192.168.5.1**.

      For the third end node (i.e. London), select **192.168.6.1**.

      By default, the NE-ONE automatically creates one working (all traffic, no filtering) route in the end node's routing table (see *Illustration 134* on page 444). That is, the NE-ONE automatically selects **Port In** value you specified in the **Routing Properties** window, and automatically selects the connected link for the **Port Out**.

      If necessary, to create additional routing rules within the routing table for the end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes with filtering are set up.

ILLUSTRATION 134 - EXAMPLE OF AN AUTO GENERATED ROUTE RULE



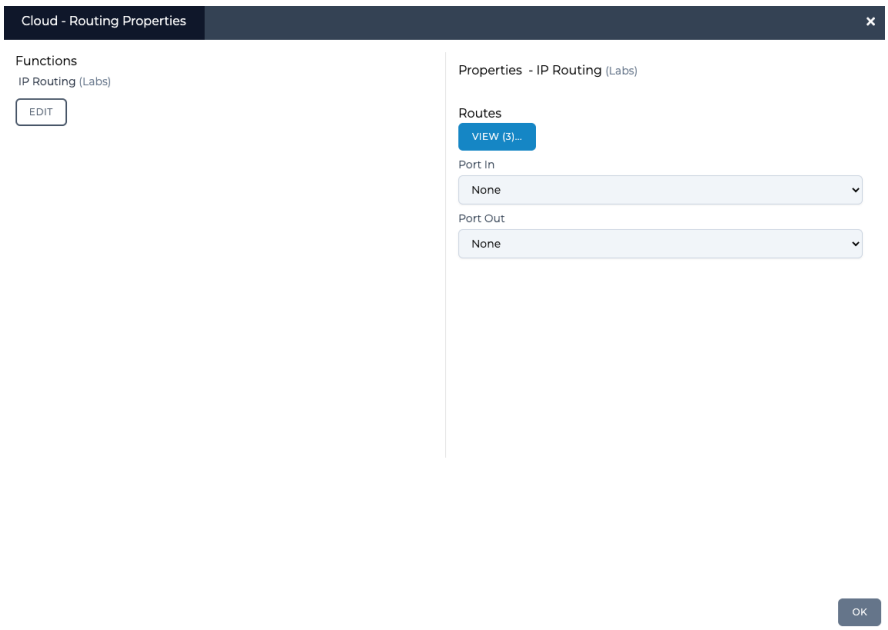
c. In the **Routing Properties** window, click **OK**.

You are returned to the **Multi-Point Designer** page.

At this stage the routing configuration is now complete for each of the end nodes. You are now ready to define the routing table of the central cloud node, and the cloud link rule(s) for the central cloud node.

7. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click the **SAVE** button.
8. Now define the routing table for the cloud node. To do this, click on the cloud node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button, then do the following in the **Cloud - Routing Properties** window that appears to define the central cloud node's routing properties:
   a. Leave the **Port In** drop-down field set to **None** (as traffic is coming in to the cloud from all inbound links (in our example, three inbound links)).
   b. Leave the **Port Out** drop-down field set to **None** (as traffic is coming out from the cloud to all

inbound links (in our example, three inbound links)).



By default, the central cloud node's routing table inherits an empty (undefined) route rule for each of the inbound links. Each of the empty (undefined) route rule corresponding to each of the inbound links must be defined. In our example, three route rules for the three inbound links going into the central cloud node need to be defined.

c. Click the **VIEW** button, and from the **Routes** window that appears, do the following for each of the route rules:

Leave the **Port In** drop-down field set to **None**.

In the **IPv4 Network Address** field, type the IP address of the end node. In our example, do the following:

For the first end node (i.e. Berlin), type **`192.168.4.1`**

For the second end node (i.e. Paris), type **`192.168.5.1`**

For the third end node (i.e. London), type **`192.168.6.1`**

In the **IPv4 Netmask** field, type the netmask of the end node. In our example, do the following:

For the first end node (i.e. Berlin), type **`255.255.255.0`**

For the second end node (i.e. Paris), type **`255.255.255.0`**

For the third end node (i.e. London), type **`255.255.255.0`**

Leave the **IPv6 Address** drop-down field blank.

In the **Port Out** field, select the link name corresponding to the end node whose IP address and network you define. In our example, do the following:

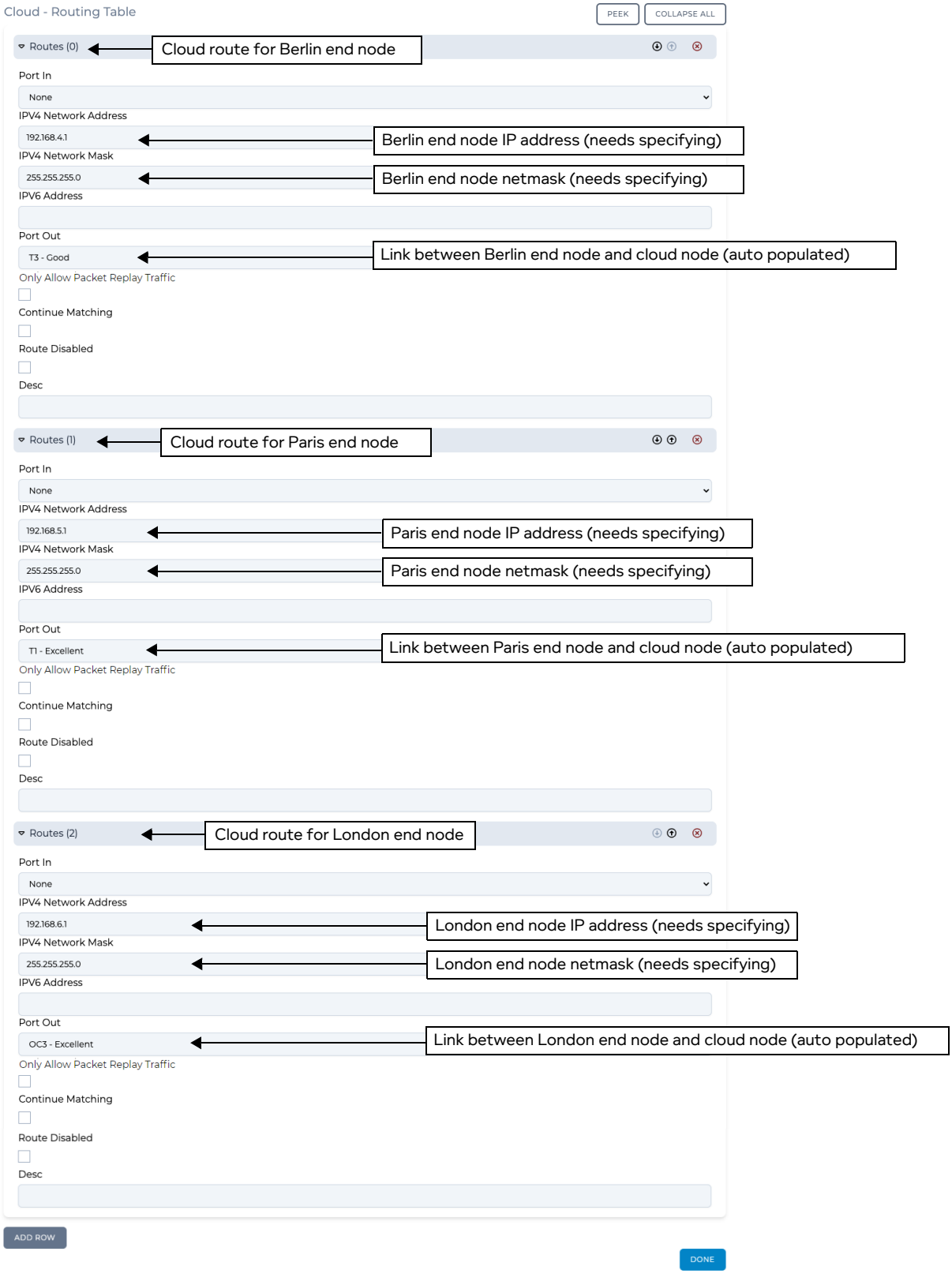
For the first end node (i.e. Berlin), select **T3 - Good** link.

For the second end node (i.e. Paris), select **T1 - Excellent** link.

For the third end node (i.e. London), select **OC3 - Excellent** link.

The **Cloud - Routing Table** window shown in *Illustration 135* on page 446 shows the three rules defined for our example.

ILLUSTRATION 135 - EXAMPLE ROUTES WINDOW (CLOUD EXAMPLE)



Click **DONE** to return to the **Cloud - Route Properties** window.

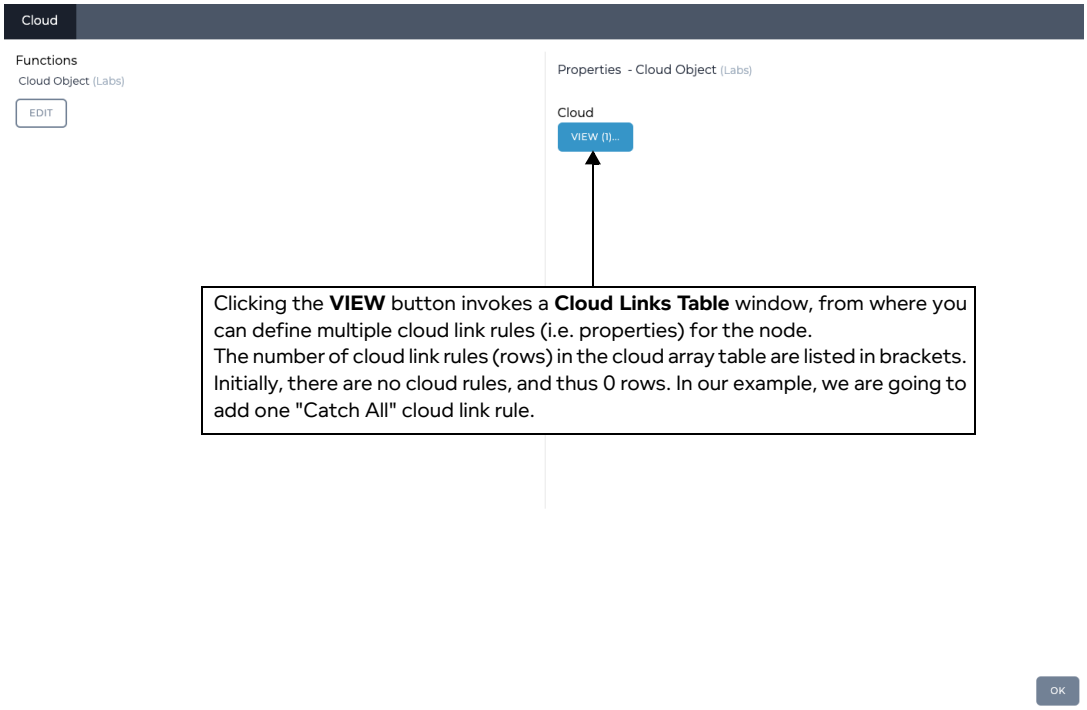
If necessary, to create additional routing rules within the routing table for the central cloud node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table.

d. From the **Cloud - Route Properties** window, click **OK**.

You are returned to the **Multi-Point Designer** page.

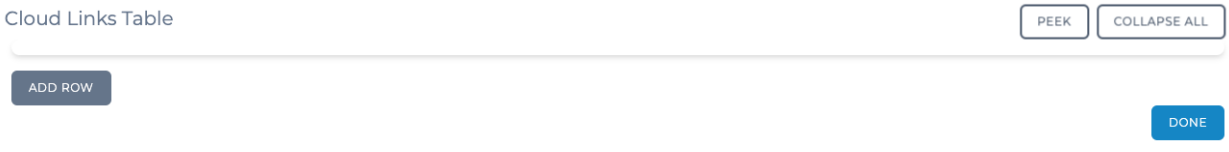
9. At this stage the routing configuration is now complete for the central cloud node. Now the central node's Cloud Object (Labs) function needs configuring with at least one cloud link rule so that traffic can pass through the cloud.To do this, click on the central cloud node in the Workspace, and from the **Edit node** panel that appears, click the **PROPERTIES** button, then from the **Node Properties Window** that appears (see *Illustration 98* on page 345), click on the **Cloud** button.

   A **Cloud** window appears with one empty (undefined) cloud link rule.



10. Click the **VIEW** button, to open the **Cloud Routing Table** window.

    The **Cloud Links Table** window appears. Initially a node with the Cloud Object (Labs) function has no cloud link rules added to it. The **Cloud Links Table** window lets you add cloud link rules. Each cloud link rule that you add, appears as a row in the **Cloud Links Table** table window.



11. Click on the **ADD ROW** button.

A new cloud link rule row is created, and initially expanded.

Within the cloud link rule row, exist all the appropriate elements (i.e. fields, and buttons invoking the definition of ranges - see *Table 57* on page 354), letting you define all aspects of the cloud link rule. You can set up many cloud links (each with a cloud link rule) within the **Cloud Routing Table** window.

12. For our example, set up a catch all cloud link rule (i.e. no filters), with the following parameters:
    - In the **Link Id** field, type **1**.
    - Leave the **Bandwidth** field blank.
    - In the **Latency** field, type **20**.
    - Leave the **Jitter** field blank.
    - Leave the **TTL Cost** field blank.
    - Leave the **Loss** field blank.

- Leave the **Queue Length** field value set to **64000**.
- Leave the **Port In field** set to **None** (as in our example, we want to catch all traffic from all inbound links).
- Leave the **Use Last Hop As Port In** check box unticked.
- Do not define any filters (i.e. leave the **Source IP Address**, **Destination IP Address**, **Source Port**, **Destination Port**, **IPv4 Protocol**, and **VLAN Id** filters to their default (undefined) ranges).
- Leave the **Trace** check box unticked.
- Leave the **Capture** check box unticked.
- Leave the **Disabled** check box unticked.
- In the **Description** field, type an appropriate description for the rule (e.g. **`Catch All`**).

  Click **DONE** to return to the **Cloud** window.

  All the necessary parameters have now been configured for the example Cloud Multi-Point network (*Illustration 129* on page 435).

13. From the **Cloud** window, click **OK**.

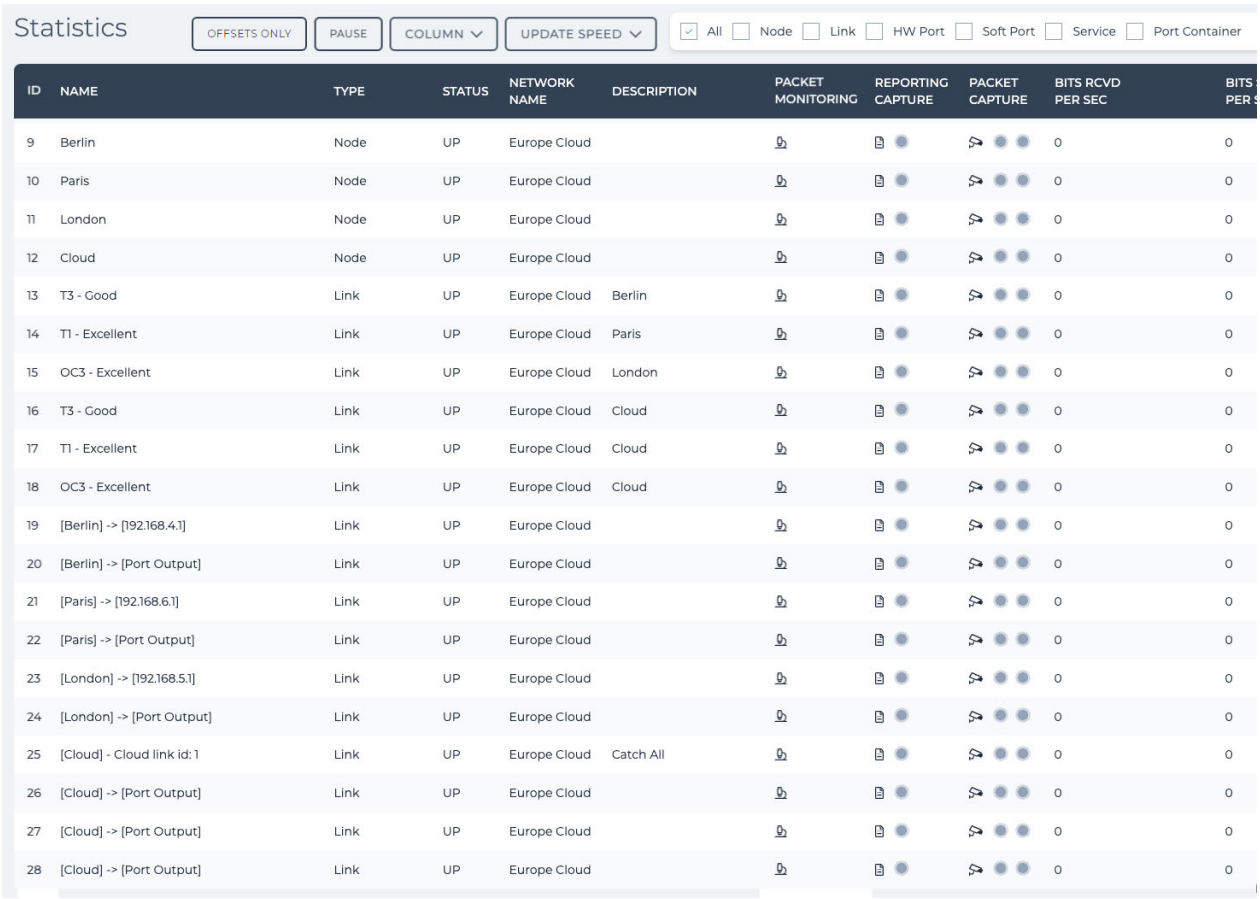
    You are returned to the **Multi-Point Designer** page.

14. Save the finalized Cloud Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

    The Cloud Multi-Point network will appear in the **Multi-Point Designer** page as shown in *Illustration 129* on page 435, and is ready to be run (i.e. played).

    If you click the **PLAY** button in the **Multi-Point Designer** page, the Cloud Multi-Point network starts running and its associated objects appear in the **Statistics** page (see *Illustration 136*).

ILLUSTRATION 136 - EXAMPLE CLOUD NETWORK ASSOCIATED OBJECTS VISIBLE IN THE STATISTICS PAGE



ID	NAME	TYPE	STATUS	NETWORK NAME	DESCRIPTION	PACKET MONITORING	REPORTING CAPTURE	PACKET CAPTURE	BITS RCVD PER SEC	BITS PER S
9	Berlin	Node	UP	Europe Cloud					0	0
10	Paris	Node	UP	Europe Cloud					0	0
11	London	Node	UP	Europe Cloud					0	0
12	Cloud	Node	UP	Europe Cloud					0	0
13	T3 - Good	Link	UP	Europe Cloud	Berlin				0	0
14	T1 - Excellent	Link	UP	Europe Cloud	Paris				0	0
15	OC3 - Excellent	Link	UP	Europe Cloud	London				0	0
16	T3 - Good	Link	UP	Europe Cloud	Cloud				0	0
17	T1 - Excellent	Link	UP	Europe Cloud	Cloud				0	0
18	OC3 - Excellent	Link	UP	Europe Cloud	Cloud				0	0
19	[Berlin] -> [192.168.4.1]	Link	UP	Europe Cloud					0	0
20	[Berlin] -> [Port Output]	Link	UP	Europe Cloud					0	0
21	[Paris] -> [192.168.6.1]	Link	UP	Europe Cloud					0	0
22	[Paris] -> [Port Output]	Link	UP	Europe Cloud					0	0
23	[London] -> [192.168.5.1]	Link	UP	Europe Cloud					0	0
24	[London] -> [Port Output]	Link	UP	Europe Cloud					0	0
25	[Cloud] - Cloud link id: 1	Link	UP	Europe Cloud	Catch All				0	0
26	[Cloud] -> [Port Output]	Link	UP	Europe Cloud					0	0
27	[Cloud] -> [Port Output]	Link	UP	Europe Cloud					0	0
28	[Cloud] -> [Port Output]	Link	UP	Europe Cloud					0	0

4-4. Creating Hub and Spoke Networks

In this example, we need to connect three private (sub) networks e.g. 192.168.4.0/24, 192.168.5.0/24 and 192.168.6.0/24 to each other and also out to the corporate network and thus to the Internet. The structure for connection is a Hub and Spoke network.

These subnets are connected to a VLAN (802.1Q) capable switch which has up to now been routing (it is a layer 3 switch) between these subnets and the main corporate network.

Unfortunately, the switch cannot create WAN conditions between these subnets and in the “real world”. That is, in the non-test environment these subnets will be in geographically dispersed locations (for example, London, Berlin, Paris, and Barcelona).

The requirement is to connect the NE-ONE to the VLAN corporate switch and produce a Hub and Spoke WAN between these subnets with the minimum amount of changes.

We are told that:

- The Berlin test site has Network 192.168.4.0 is on VLAN 601 with gateway 192.168.4.1.
- The Paris test site has Network 192.168.5.0 is on VLAN 602 with gateway 192.168.5.1.
- The London test site has Network 192.168.6.0 is on VLAN 603 with gateway 192.168.6.1.
- The corporate network in Barcelona is 192.168.202.0 on VLAN 604 with gateway 192.168.202.31.
- The IP address for the NE-ONE to have in the corporate network is 192.168.202.121.

In the following example (*Illustration 138* on page 453), the Hub and Spoke network topology template is used to create a Hub and Spoke based Multi-Point network, with the following configuration:

- Berlin (end node):
  - Input port : 192.168.4.1
  - Output port : 192.168.4.1
  - One link : Type : WAN, T3 - Good, with link name T3 - Good
  - Routing table : one route with input port as 192.168.4.1, output port as T3 - Good : this routes all traffic to/from the Berlin end node into the hub, with no packet filtering.
- London (end node):
  - Input port : 192.168.5.1
  - Output port : 192.168.5.1
  - One link : Type : WAN, E3 - Good, with link name E3 - Good
  - Routing table : one route with input port as 192.168.5.1, output port as E3 - Good : this routes all traffic to/from the London end node into the hub, with no packet filtering.
- Paris (end node):
  - Input port : 192.168.6.1
  - Output port : 192.168.6.1
  - One link : Type : WAN, T1 - Excellent, with link name T1 - Excellent
  - Routing table : one route with input port as 192.168.6.1, output port as T1 - Excellent : this routes all traffic from the Paris end node into the hub, with no packet filtering.
- Barcelona (end node):
  - Input port : 192.168.202.121
  - Output port : 192.168.202.121
  - One link : Type : WAN, OC3 - Excellent, with link name OC3 - Excellent
  - Routing table : one route with input port as 192.168.202.121, output port as OC3 - Excellent : this routes all traffic from the Paris end node into the hub, with no packet filtering.

- Hub node, with the following routing table rules (i.e. one for each inbound link):
  - Input port as None, output port as T3 - Good, IP address 192.168.4.1 and netmask 255.255.255.0 : this routes all traffic to/from the Berlin end node into the hub, with no packet filtering.
  - Input port as None, output port as T1 - Excellent, IP address 192.168.6.1 and netmask 255.255.255.0 : this routes all traffic from the Paris end node into the hub, with no packet filtering.
  - Input port as None, output port as E3 - Good, IP address 192.168.6.1 and netmask 255.255.255.0 : this routes all traffic to/from the London end node into the hub, with no packet filtering.
  - Input port as None, output port as OC3 - Excellent, with no IP address or netmask defined: this routes all traffic to/from the Barcelona end node into the hub, with no packet filtering. It is intentional that no IP address and netmask for the Barcelona node. This is because we want to route all traffic that does not go to our private networks there.

Note:

An assumption is made that the total I/O we are handling can be covered in total by one of the NE-ONE's hardware ports, if this is not true then a modified version of this example can be produced by using more than one NE-ONE hardware ports.

ILLUSTRATION 137 - EXAMPLE SIMPLE HUB AND SPOKE NETWORK (MULTI-POINT WORKSPACE)

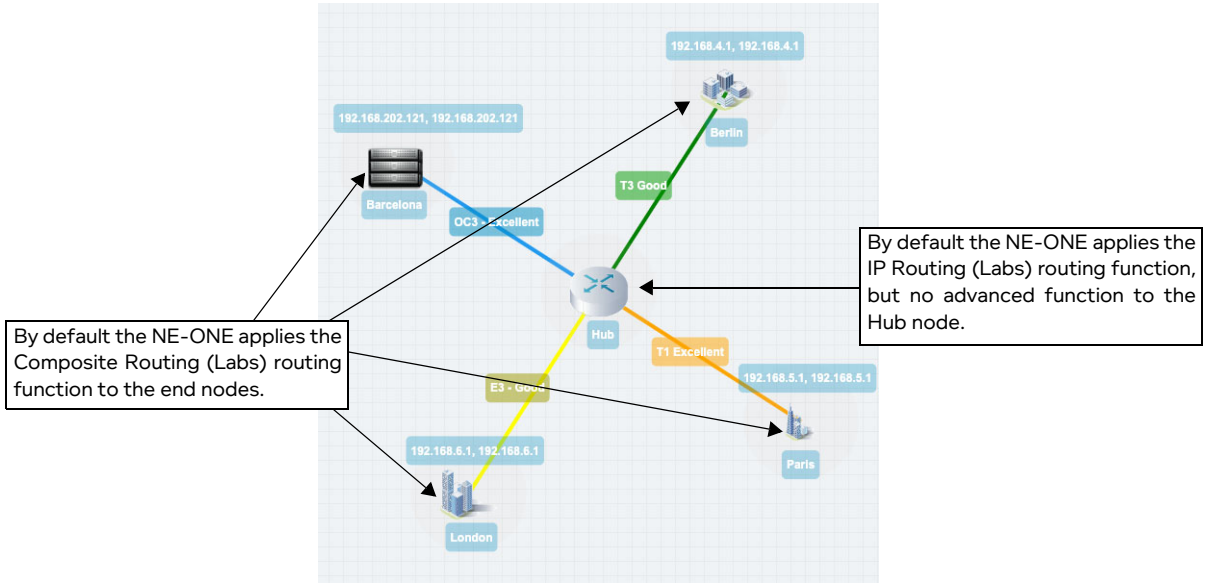
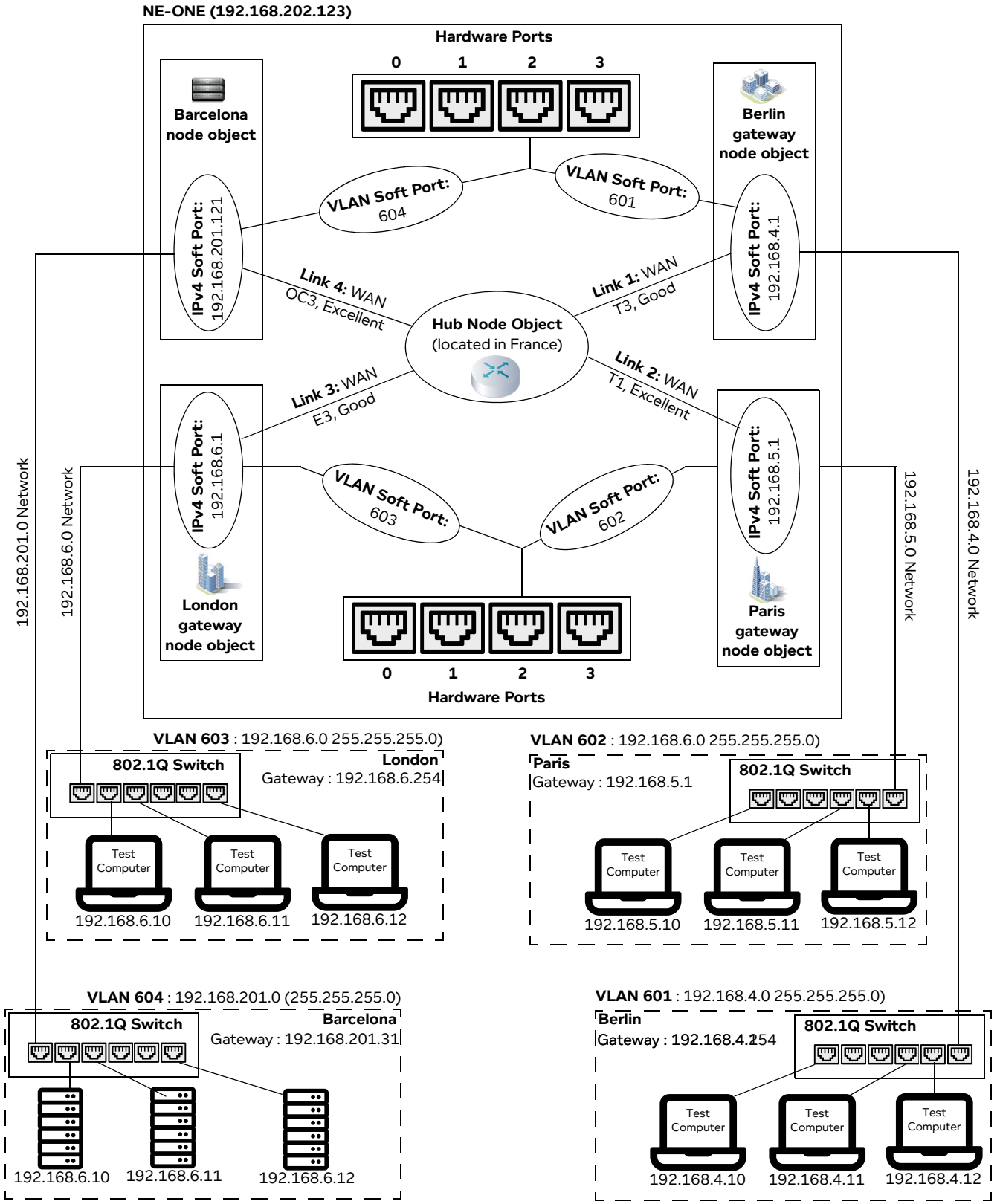


ILLUSTRATION 138 - EXAMPLE HUB AND SPOKE NETWORK (WITH VLAN AND IPV4 SOFT PORTS)

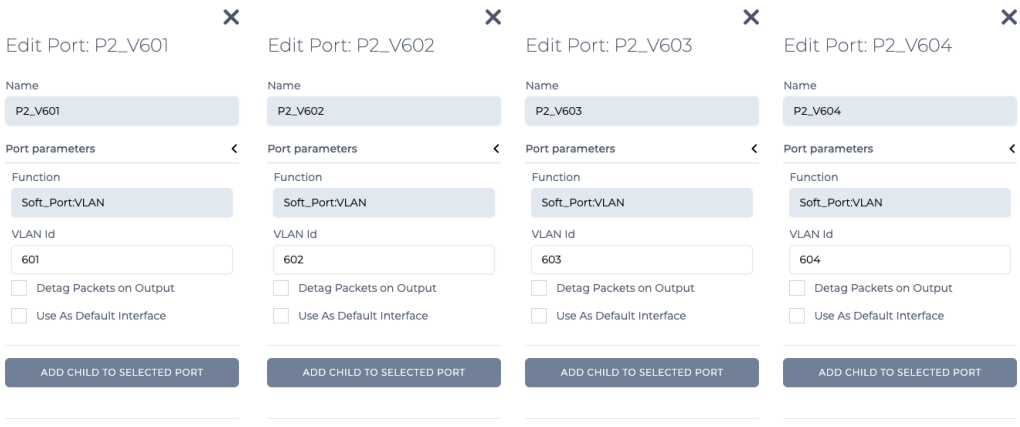


4-4-1. Prerequisite Steps Performed by an Admin User

In order for a non-admin user to create a Hub and Spoke network based on this example, an admin user needs to do the following prerequisite steps:

1. Configure the NE-ONE with a static IP address of 192.168.202.121 according to the steps described in *Configuring the Management Port Settings* on page 60 of *Chapter 4*, *Installation and Configuration*.
2. Request to the corporate network administrator that a VLAN (802.1Q) Trunk port is set up on the switch, trunking at least VLANs 601, 602, 603 and 604.
3. Request to the corporate network administrator that the corporate switch's routing addresses 192.168.4.1, 192.168.5.1, 192.168.6.1 are removed from its routing tables, as the NE-ONE will take over that function.
4. Connect NE-ONE hardware port (in our example, hardware port 2) to that Trunk port with a suitable cable.
5. Create one VLAN soft port for each required VLANs (601, 602, 603 and 604) on the NE-ONE's hardware port (in our example, hardware port 2) according the steps described in *Creating a VLAN Soft Port* on page 107 in *Chapter 5*, *Ports and Services Management*, with each VLAN soft port having **Detag Packets** on **Output and Default Interface** settings disabled (unticked), as shown in *Illustration 107*.

ILLUSTRATION 139 - VLAN SOFT PORT CONFIGURATIONS



VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2

Note: The naming convention of the VLAN soft ports uses the P2 prefix to indicate that these ports are children of hardware port 2, where VNNN denotes a VLAN port with that ID (tag). You can use any soft port names you want, but they should be meaningful.

6. Create and assign IPv4 soft ports to the VLAN soft ports. To do this, within each of the VLAN soft ports, create an IPv4 soft port according the steps described in *Creating an IPv4 Soft Port* on page 114 in *Chapter 5*, *Ports and Services Management*, with the following settings (*Illustration 140* on page 455).
   - VLAN 601 soft port contains IPv4 soft port called 192.168.4.1, with IP address 192.168.4.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway as there are no other routers in the network 192.168.4.0, only the NE-ONE itself which is acting as the gateway.
   - VLAN 602 soft port contains IPv4 soft port called 192.168.5.1, with IP address 192.168.5.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway as there are no other routers in the network 192.168.5.0, only the NE-ONE itself which is acting

as the gateway.

- VLAN 603 soft port contains IPv4 soft port called 192.168.5.1, with IP address 192.168.5.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway as there are no other routers in the network 192.168.6.0, only the NE-ONE itself which is acting as the gateway.
- VLAN 604 soft port contains IPv4 soft port called 192.168.202.121, with IP address 192.168.202.121, netmask 255.255.255.0, and gateway 192.168.202.31.

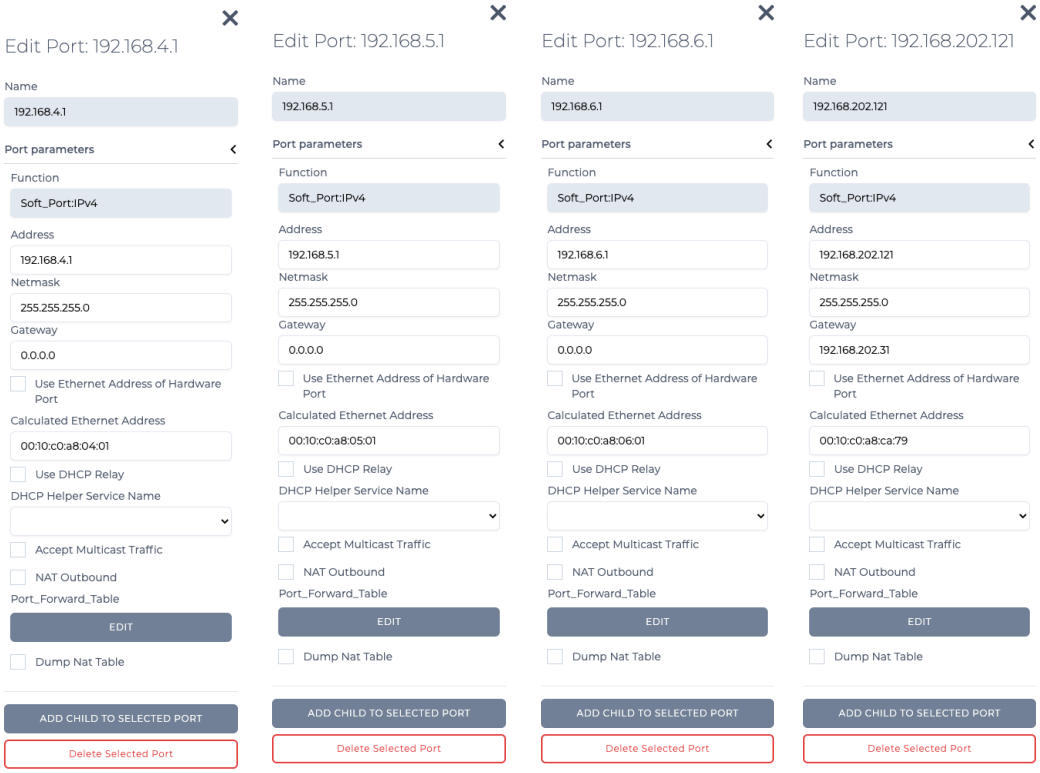
Note: Notice that there is only one IPv4 soft port in each VLAN soft port, as we only require one IP address in each VLAN network. Also, again for clarity, name given to each of the IPv4 soft ports is the same name as its IP address.

The resulting soft port layout for this example is shown in *Illustration 141* on page 456, which give a non-admin user all the soft ports they need to create a Hub and Spoke type Multi-Point network based on our example described above.

Note: Our example is for four end nodes, a hub node, and four links with four VLAN soft ports and four IPv4 soft ports. This is easily extensible to much larger networks with many more end nodes, links, VLAN soft ports and IPv4 soft ports.

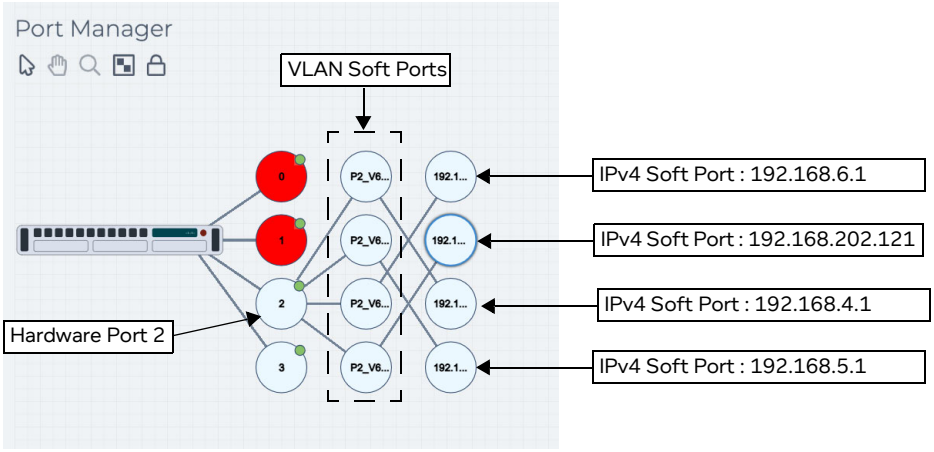
7. Assign the created IPv4 soft ports (192.168.4.1, 192.168.5.1, 192.168.6.1, and 192.168.202.31) to the intended non-admin user who will create the Hub and Spoke Multi-Type network according to the steps described in *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205 in *Chapter 6*, *User Administration*.

ILLUSTRATION 140 - IPV4 SOFT PORT CONFIGURATIONS FOR HUB AND SPOKE EXAMPLE



IPv4 Soft Port assigned to VLAN Soft Port 601 | IPv4 Soft Port assigned to VLAN Soft Port 602 | IPv4 Soft Port assigned to VLAN Soft Port 603 | IPv4 Soft Port assigned to VLAN Soft Port 604

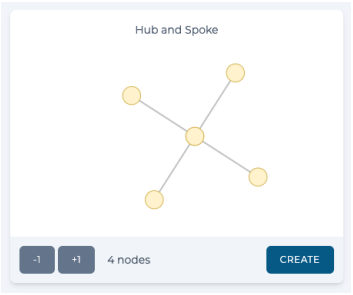
ILLUSTRATION 141 - RESULTING VLAN AND IPV4 SOFT PORT LAYOUT FOR HUB AND SPOKE EXAMPLE



4-4-2. Hub and Spoke Network Creation Steps Performed by a Non Admin User

Once the NE-ONE has been configured by an admin user according to *Section 4-4-1*, a non-admin user (or admin user) can create a Hub and Spoke Multi-Point network for the example described above, using the following steps:

1. Launch the **Multi-Point Designer** page, and choose the Hub and Spoke network topology template, using the following sub-steps:
   a. Select **Networks** from the Menu.
   b. From the **Networks** page (see *Illustration 4* on page 42) that appears, click **New Network**.
   c. From the **Network Wizard** page (see *Illustration 84*) that appears, in the **Hub and Spoke** panel, click the **+1** or **-1** icon to increase or decrease the total number of end nodes used by the Hub and Spoke network topology template, then click **CREATE**.

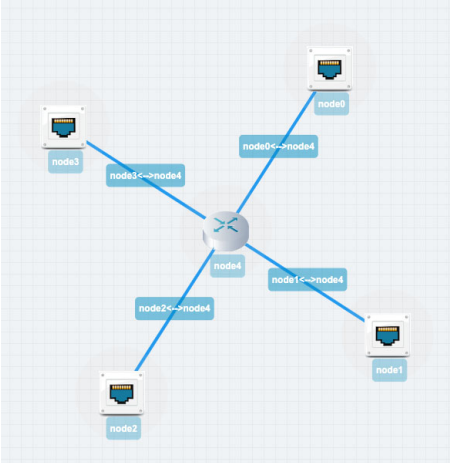


   In our example we want four end nodes, so click the **-1** button once so only three nodes are shown in the **Hub and Spoke** panel, then click **CREATE**.
   d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`European HaS`**), then click **OK**.

A new (i.e. undefined) Multi-Node network appears based on the selected Hub and Spoke network topology template you selected. At this stage, nothing is configured in the Hub and Spoke network. You will need to configure the:

- routing for each of the nodes (i.e. assign input and output ports, and optionally define routing rules),
- links between each of the end nodes and the central hub node
- routing table of the hub node (i.e. at least four routes for each of the end nodes going into the

hub node)



2. From the **Multi-Point Designer** page, optionally tick the **Show node names**, **Show link names**, and **Show node ports** check boxes from the **VIEW** drop-down menu.

   Note: This optional step is useful in letting you identify what still needs configuring in the Multi-Point network. Undefined nodes have the generic names **node0**, **node1**, **node2**, **node3**, **node4**, etc. Undefined links have the format **node0<-->node4**, **node1<-->node4**, **node3<-->node4**, **node2<-->node4**,etc. End nodes with undefined input and output ports show nothing.

3. For each of the end nodes and cloud node in the Workspace, click on the end node/cloud node, and from the **Edit node** panel that appears do the following to define the node's basic properties.

   a. In the **Name** field, type an appropriate node name. The node name can contain alpha-numeric characters and spaces. In our example, do the following:

      For the first end node (which was initially called node0), type **`Berlin`**.

      For the second end node (which was initially called node1), type **`Paris`**

      For the third end node (which was initially called node2), type **`London`**.

      For the fourth end node (which was initially called node3), type **`Barcelona`**.

      For the central hub node (which was initially called node4), type **`Hub`**.

   b. In the **Description** field, optionally type an appropriate description.The node description can contain alpha-numeric characters and spaces.

   c. From the **Country** drop-down field, select an appropriate country to define the country where the node is located. In our example, do the following:

      For the first end node, select **Germany**.

      For the second end node, select **France**.

      For the third end node, select **United Kingdom**.

      For the fourth end node, select **Spain**.

      For the central hub node, select **France**.

      Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.

   d. From the **Choose a location** drop-down field, select and appropriate area for the location. In our example, do the following:

      For the first end node, select a location within **Berlin**.

      For the second end node, select a location within **Paris**.

      For the third end node, select a location within **London**.

For the fourth end node, select a location within **Barcelona**.

For the central hub node, select a location somewhere within **France**.

Note: You can start typing the location in order to select it quickly from the list of locations. The list of locations proposed depend on the string you specified in the **Name** field. In this case for example, locations in an around London are proposed.

e. Click on the icon, and from the dialog box that appears click on the an appropriate icon, and then click **OK**.

In our example, do the following:

For the first end node, select the four low buildings icon from the **Standard** category in the **Node Icons** panel.

For the second end node, select the four buildings point icon from the **Standard** category in the **Node Icons** panel.

For the third end node, select the commercial center icon from the **Standard** category in the **Node Icons** panel.

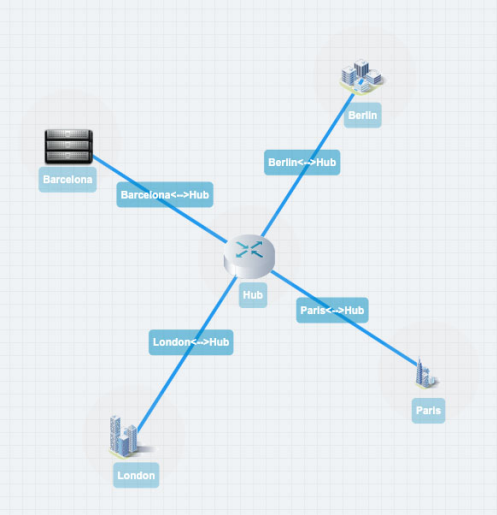
For the fourth end node, select the rack servers icon from the **IT** category in the **Node Icons** panel.

For the central hub node, leave it set to the standard router icon.

f. Click to ✕ close the **Edit node** panel.

At this stage the basic properties of each of the end nodes and hub node are defined. Since the node names were changed, the link names automatically update to include the node names, such that:

- **node0<-->node4** becomes **Berlin<-->Hub**
- **node1<-->node4** becomes **Paris<-->Hub**
- **node2<-->node4** becomes **London<-->Hub**
- **node3<-->node4** becomes **Barcelona<-->Hub**



Next, define the links between the end nodes and the central hub node. In the example below, the automatically assigned link names are changed, however this is purely optional.

4. For each of the links in the Workspace, click on the link, and from the **Edit link** panel that appears, click the **EDIT** button. Then from the **Link** page that appears, do the following to define the link's properties.

a. In the **Name** field, type an appropriate link name. The link name can contain alpha-numeric characters and spaces. In our example, do the following:
   For the link going between the first end node and the central hub node (which is currently called **Berlin<-->Hub**), type **`T3 – Good`**.
   For the link going between the second end node and the central hub node (which is currently called **Paris<-->Hub**), type **`T1 – Excellent`**.
   For the link going between the third end node and the central hub node (which is currently called **London<-->Hub**), type **`E3 – Good`**.
   For the link going between the fourth end node and the central hub node (which is currently called **Barcelona<-->Hub**), type **`OC3 – Excellent`**.
b. In the **Description** field, type a description. The link name can contain alpha-numeric characters and spaces.
c. From the **Type** drop-down field, select an appropriate link type. In our example, do the following:
   For the link going between the first end node and the central hub node (which is now called **T3 - Good**), select **WAN**.
   For the link going between the second end node and the hub cloud node (which is now called **T1 - Excellent**), select **WAN**.
   For the link going between the third end node and the hub cloud node (which is now called **OC3 - Excellent**), select **WAN**.
   For the link going between the fourth end node and the hub cloud node (which is now called **OC3 - Excellent**), select **WAN**.
d. From the **Subtype** drop-down field, an appropriate link type. In our example, do the following:
   For the link going between the first end node and the central hub node (which is now called **T3 - Good**), select **T3/DS3**.
   For the link going between the second end node and the central hub node (which is now called **T1 - Excellent**), select **T1**.
   For the link going between the third end node and the central hub node (which is now called **E3 - Good**), select **E3**.
   For the link going between the fourth end node and the central hub node (which is now called **OC3 - Excellent**), select **OC3**.
e. From the **Link Quality** drop-down field, select an appropriate link quality. In our example, do the following:
   For the link going between the first end node and the central hub node (which is now called **T3 - Good**), select **Good**.
   For the link going between the second end node and the central hub node (which is now called **T1 - Excellent**), select **Excellent**.
   For the link going between the third end node and the central hub node (which is now called **E3 - Good**), select **Excellent**.
   For the link going between the fourth end node and the central hub node (which is now called **OC3 - Excellent**), select **Excellent**.
f. From the **Link Color** drop-down field, select an appropriate link color. In our example, do the following:
   For the link going between the first end node and the central hub node (which is now called **T3 - Good**), select **Green**.
   For the link going between the second end node and the central hub node (which is now called **T1**

- Excellent), select **Orange**.

For the link going between the third end node and the central hub node (which is now called **OC3 - Excellent**), select **Red**.

For the link going between the fourth end node and the central hub node (which is now called **OC3 - Excellent**), leave the color set to **Blue**.

g. Click **OK** to submit the link properties.

At this stage the link names are now defined to something meaningful within your Hub and Spoke Multi-Point network. The link names you defined will appear as selectable output ports within the routing table you define for the central hub node.

5. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click the **SAVE** button.
6. For each of the end nodes in the Workspace, click on the end node, and from the **Edit node** panel that appears, click the **ROUTES** button, then do the following in the **Routing Properties** window that appears to define the end node's routing properties.
   a. In the **Port In** drop-down field, select an appropriate input port for the end node. In our example, do the following:

      For the first end node (i.e. Berlin), select **192.168.4.1**.

      For the second end node (i.e. Paris), select **192.168.5.1**.

      For the third end node (i.e. London), select **192.168.6.1**.

      For the fourth end node (i.e. Barcelona), select **192.168.202.121**.

   b. In the **Port Out** drop-down field, select an appropriate out port for the end node. In our example, do the following:

      For the first end node (i.e. Berlin), select **192.168.4.1**.

      For the second end node (i.e. Paris), select **192.168.5.1**.

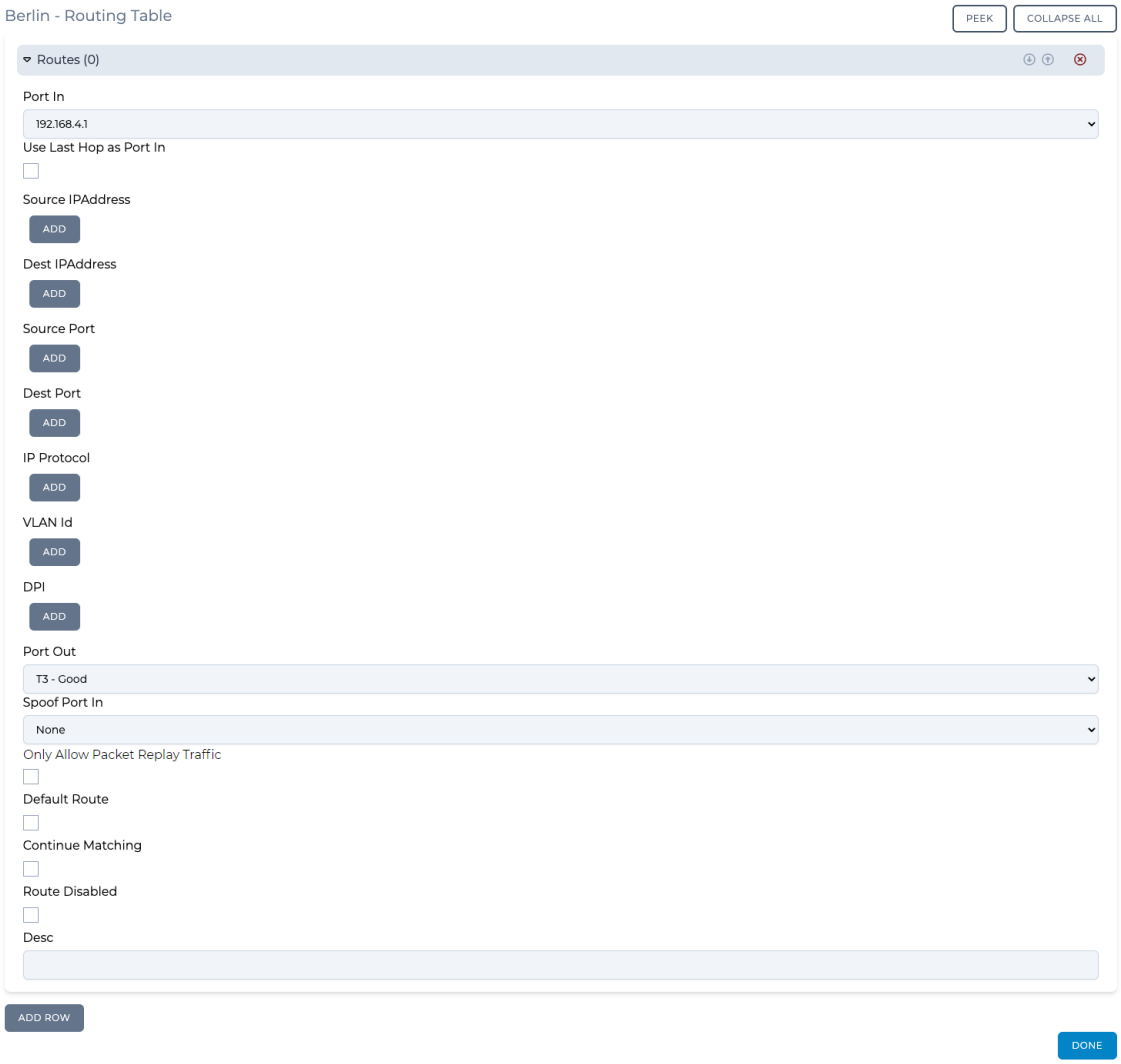
      For the third end node (i.e. London), select **192.168.6.1**.

      For the fourth end node (i.e. Barcelona), select **192.168.202.121**.

      By default, the NE-ONE automatically creates one working (all traffic, no filtering) route in the end node's routing table (see *Illustration 142* on page 461). That is, the NE-ONE automatically selects **Port In** value you specified in the **Routing Properties** window, and automatically selects the connected link for the **Port Out**.

      If necessary, to create additional routing rules within the routing table for the end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes with filtering are set up.

ILLUSTRATION 142 - EXAMPLE OF AN AUTO GENERATED ROUTE RULE



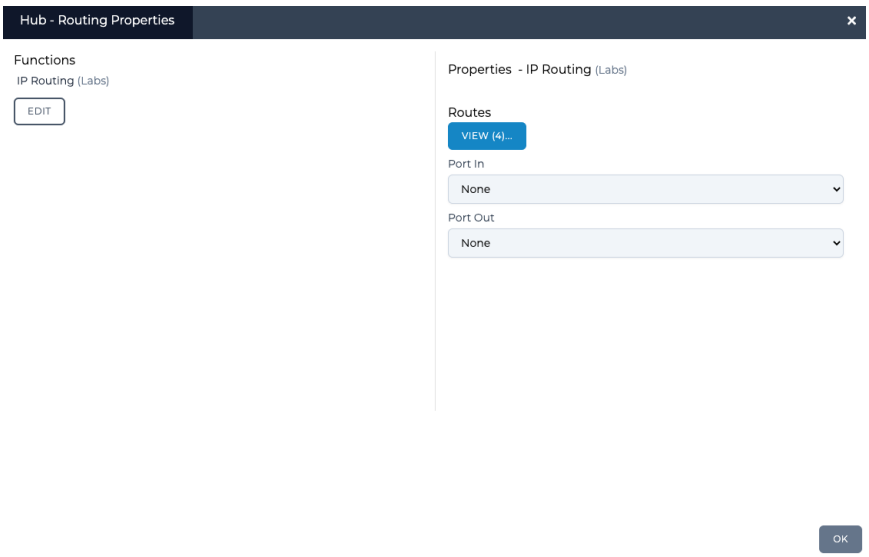
c. In the **Routing Properties** window, click **OK**.

You are returned to the **Multi-Point Designer** page.

At this stage the routing configuration is now complete for each of the end nodes. You are now ready to define the routing table of the central hub node.

7. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click the **SAVE** button.
8. Now define the routing table for the hub node. To do this, click on the hub node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button, then do the following in the **Hub - Routing Properties** window that appears to define the central hub node's routing properties:
   a. Leave the **Port In** drop-down field set to **None** (as traffic is coming in to the hub from all inbound links (in our example, four inbound links).
   b. In the **Port Out** drop-down field, (as traffic is coming in to the hub from all inbound links (in our

example, four inbound links).



By default, the central hub node's routing table inherits an empty (undefined) route rule for each of the inbound links. Each of the empty (undefined) route rule corresponding to each of the inbound links must be defined. In our example, four route rules for the four inbound links going into the central hub node need to be defined.

c. Click the **VIEW** button, and from the **Hub - Routing Properties** window that appears, do the following for each of the route rules:

Leave the **Port In** drop-down field set to **None**.

In the **IPv4 Network Address** field, type the IP address of the end node. In our example, do the following:

For the first end node (i.e. Berlin), type **`192.168.4.1`**

For the second end node (i.e. Paris), type **`192.168.5.1`**

For the third end node (i.e. London), type **`192.168.6.1`**

In the **IPv4 Netmask** field, type the netmask of the end node. In our example, do the following:

For the first end node (i.e. Berlin), type **`255.255.255.0`**

For the second end node (i.e. Paris), type **`255.255.255.0`**

For the third end node (i.e. London), type **`255.255.255.0`**

Leave the **IPv6 Address** drop-down field blank.

In the **Port Out** field, select the link name corresponding to the end node whose IP address and network you define. In our example, do the following:

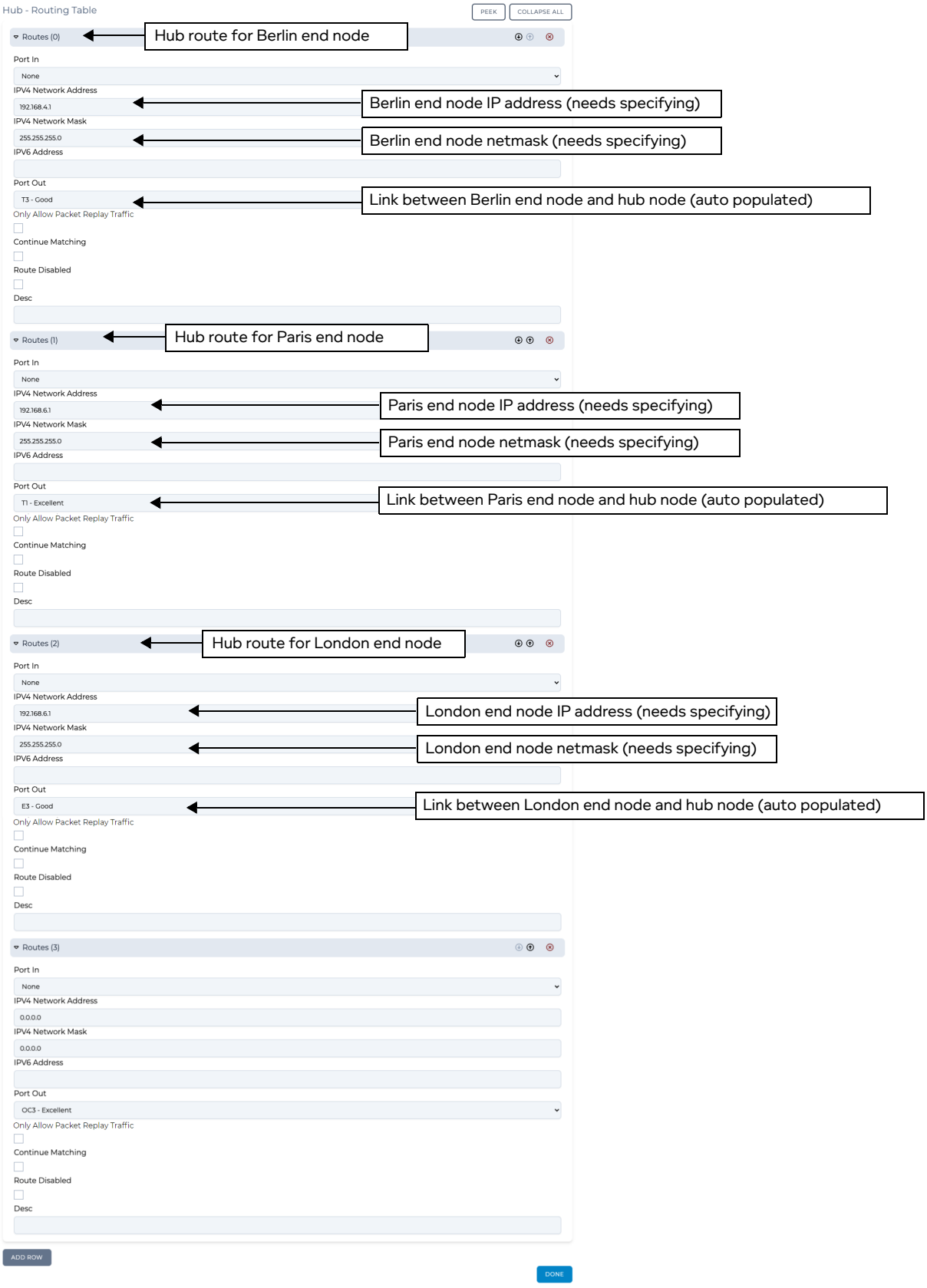
For the first end node (i.e. Berlin), type **T3 - Good** link.

For the second end node (i.e. Paris), select **T1 - Excellent** link.

For the third end node (i.e. London), select **OC3 - Excellent** link.

The **Routes** window shown in *Illustration 143* on page 463 shows three of the for rules defined for our example.

ILLUSTRATION 143 - EXAMPLE ROUTES WINDOW



Notice that in fourth row (i.e. **Routes(3)**) for Barcelona, no IP address or netmask is defined for the Barcelona end node. This is because we want to route all traffic that does not go to our private networks there.

Click **DONE** to return to the **Route Properties** window.

If necessary, to create additional routing rules within the routing table for the central cloud node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table.

d. From the **Route Properties** window, click **OK**.

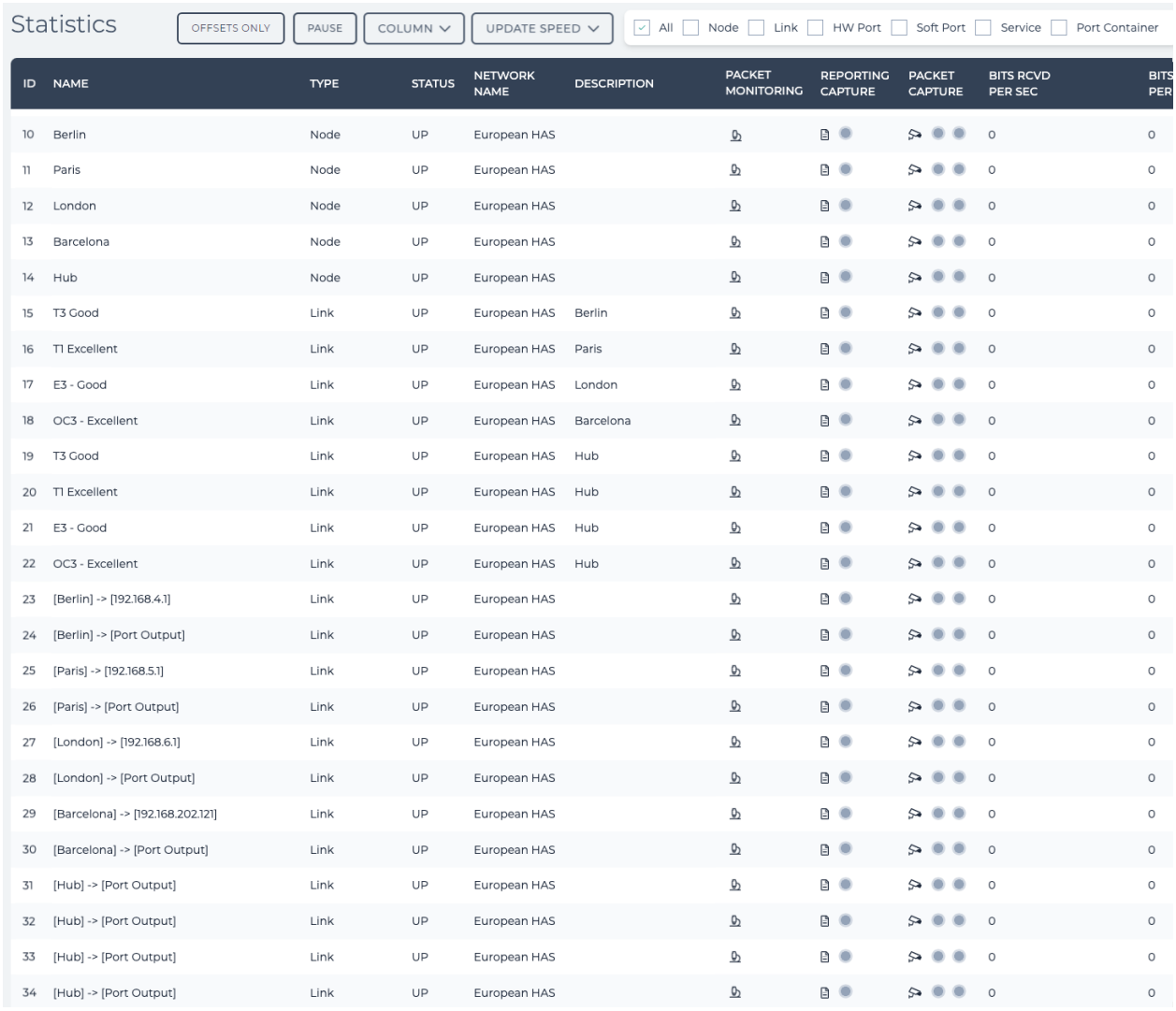
You are returned to the **Multi-Point Designer** page.

9. Save the finalized Hub and Spoke Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

   The Hub and Spoke Multi-Point network will appear in the **Multi-Point Designer** page as shown in *Illustration 137* on page 452, and is ready to be run (i.e. played).

   If you click the **PLAY** button in the **Multi-Point Designer** page, the Hub and Spoke Multi-Point network starts running and its associated objects appear in the **Statistics** page (see *Illustration 144*).

ILLUSTRATION 144 - EXAMPLE SIMPLE HUB AND SPOKE NETWORK ASSOCIATED OBJECTS VISIBLE IN THE STATISTICS PAGE



ID	NAME	TYPE	STATUS	NETWORK NAME	DESCRIPTION	PACKET MONITORING	REPORTING CAPTURE	PACKET CAPTURE	BITS RCVD PER SEC	BITS PER
10	Berlin	Node	UP	European HAS					0	0
11	Paris	Node	UP	European HAS					0	0
12	London	Node	UP	European HAS					0	0
13	Barcelona	Node	UP	European HAS					0	0
14	Hub	Node	UP	European HAS					0	0
15	T3 Good	Link	UP	European HAS	Berlin				0	0
16	T1 Excellent	Link	UP	European HAS	Paris				0	0
17	E3 - Good	Link	UP	European HAS	London				0	0
18	OC3 - Excellent	Link	UP	European HAS	Barcelona				0	0
19	T3 Good	Link	UP	European HAS	Hub				0	0
20	T1 Excellent	Link	UP	European HAS	Hub				0	0
21	E3 - Good	Link	UP	European HAS	Hub				0	0
22	OC3 - Excellent	Link	UP	European HAS	Hub				0	0
23	[Berlin] -> [192.168.4.1]	Link	UP	European HAS					0	0
24	[Berlin] -> [Port Output]	Link	UP	European HAS					0	0
25	[Paris] -> [192.168.5.1]	Link	UP	European HAS					0	0
26	[Paris] -> [Port Output]	Link	UP	European HAS					0	0
27	[London] -> [192.168.6.1]	Link	UP	European HAS					0	0
28	[London] -> [Port Output]	Link	UP	European HAS					0	0
29	[Barcelona] -> [192.168.202.121]	Link	UP	European HAS					0	0
30	[Barcelona] -> [Port Output]	Link	UP	European HAS					0	0
31	[Hub] -> [Port Output]	Link	UP	European HAS					0	0
32	[Hub] -> [Port Output]	Link	UP	European HAS					0	0
33	[Hub] -> [Port Output]	Link	UP	European HAS					0	0
34	[Hub] -> [Port Output]	Link	UP	European HAS					0	0

4-5. Creating TDMA Networks

In this example, we need to connect two private (sub) networks e.g. 192.168.5.0/24 and 192.168.6.0/24 to each other and also out to the corporate network and thus to the Internet.

The structure for connection is a Time Division Multiple Access (TDMA) network (*Illustration 146* on page 469). The three tactical platforms (i.e. Airborne Warning and Control System (AWACS) in Paris, M1 Abrams Tank in London, and F35 combat aircraft in Berlin) can only transmit data into the TDMA Mesh when their allocated slots are available (i.e. when their allocated slots "pass by" during the cycle time). The three tactical platforms can always receive data via the TDMA Mesh (i.e. the reception of the data is not impacted by their allocated slots). When a "source" tactical platform transmits data into the TDMA Mesh (i.e. when its allocated slots are "passing by" during the slot cycle time) the transmitted data passes via the TDMA Mesh onto the "destination" platform, which can always receive data.

A tactical platform can be allocated one or more unique slots (i.e. the same slot number cannot be used for more than one tactical platform). Multiple slots can be allocated in a contiguous manner (i.e. 0, 1, 2, and 3), in which case there is no break in the ability for the tactical platform to transmit into the TDMA Mesh between those contiguous slots. In our example, the three tactical platforms transmit into the TDMA Mesh directly after each other on slots 0,1,2,3, slots 4,5, and slots 6,7,8, respectively.

Note:

You can only create TDMA networks if the NE-ONE is licensed with the Defense Pack.

These subnets are connected to a VLAN (802.1Q) capable switch which has up to now been routing (it is a layer 3 switch) between these subnets and the main corporate network.

Unfortunately, the switch cannot create WAN conditions between these subnets and in the “real world”. That is, in the non-test environment these subnets will be in geographically dispersed locations (for example, London, Berlin, and Paris.

The requirement is to connect the NE-ONE to the VLAN corporate switch and produce a TDMA WAN between these subnets with the minimum amount of changes.

We are told that:

- The corporate network in Berlin has Network 192.168.4.0 is on VLAN 601 with gateway 192.168.4.254.
- The Paris test site has Network 192.168.6.0 is on VLAN 602 with gateway 192.168.6.1.
- The London test site has Network 192.168.5.0 is on VLAN 603 with gateway 192.168.5.1.
- The IP address for the NE-ONE to have in the corporate network is 192.168.4.100.

In the following example (*Illustration 146* on page 469), the Free Form Multi-Point Designer is used to create a TDMA based Multi-Point network, with the following configuration:

- F35 (end node):
  - Located in Berlin (Germany)
  - Input port : 192.168.4.1
  - Output port : 192.168.4.1
  - One link : Type : Custom, 3600 bps, with link name Link16_F35
  - Routing table : one route with input port as 192.168.4.1, output port as Link16_F35 : this routes all traffic to/from the F35 end node into the TDMA Mesh, with no packet filtering.
- M1_Abrams (end node):
  - Located in London (United Kingdom)
  - Input port : 192.168.5.1
  - Output port : 192.168.5.1

- One link : Type : Custom, 3600 bps, with link name Link16_M1_Abrams
- Routing table : one route with input port as 192.168.5.1, output port as Link16_M1_Abrams : this routes all traffic to/from the M1_Abrams end node into the TDMA Mesh, with no packet filtering.

• AWACS (end node):
- Located in Paris (France)
- Input port : 192.168.6.1
- Output port : 192.168.6.1
- One link : Type : Custom, 3600 bps, with link name Link16_AWACS
- Routing table : one route with input port as 192.168.6.1, output port as Link16_AWACS : this routes all traffic from the AWACS end node into the TDMA Mesh, with no packet filtering.

• TDMA_Mesh node (using the automatically system applied TDMA Mesh (Labs) function), with the following mesh link rules (i.e. one for each end node on their allocated slots):
- Link Id 1: this mesh link rule accepts traffic from the F35 end node with no packet filtering
  Slot List: 0,1,2,3 - these are the TDMA Mesh slots assigned to the F35 end node
  Bandwidth: 10000000 bps
  Queue Length: 6400
  Node In: F35
  Use Last Hop as node in enabled : this uses the port that the packet just came from.
- Link Id 2: this mesh link rule accepts traffic from the M1_Abrams end node with no packet filtering
  Slot List: 4,5 - these are the TDMA Mesh slots assigned to the M1_Abrams end node
  Bandwidth: 10000000 bps
  Queue Length: 6400
  Node In: M1_Abrams
  Use Last Hop as node in enabled : this uses the port that the packet just came from.
- Link Id 3: this mesh link rule accepts traffic from the AWACS end node with no packet filtering
  Slot List: 6,7,8 - these are the TDMA Mesh slots assigned to the AWACS end node
  Bandwidth: 10000000 bps
  Queue Length: 6400
  Node In: AWACS
  Use Last Hop as node in enabled : this uses the port that the packet just came from.

With the following routing table rules (i.e. one for each inbound link):
- Input port as None, output port as Link16_F35, IP address 192.168.4.1 and netmask 255.255.255.0 : this routes all traffic to/from the F35 end node into the TDMA Mesh, with no packet filtering.
- Input port as None, output port as Link16_M1_Abrams, IP address 192.168.5.1 and netmask 255.255.255.0 : this routes all traffic to/from the M1_Abrams end node into the TDMA Mesh, with no packet filtering.
- Input port as None, output port as Link16_AWACS, IP address 192.168.6.1 and netmask 255.255.255.0 : this routes all traffic from the AWACS end node into the TDMA Mesh, with no packet filtering.

Note:
An assumption is made that the total I/O we are handling can be covered in total by one of the NE-ONE's hardware ports, if this is not true then a modified version of this example can be produced by using more than one NE-ONE hardware ports.

ILLUSTRATION 145 - EXAMPLE SIMPLE TDMA NETWORK (MULTI-POINT WORKSPACE)

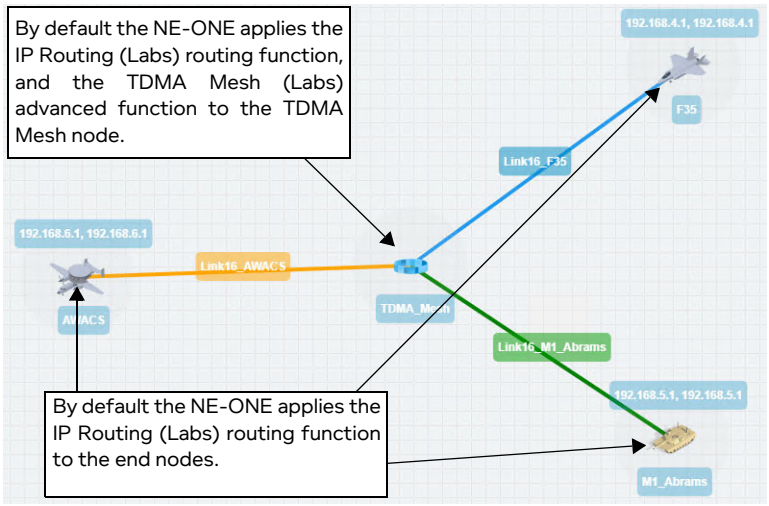
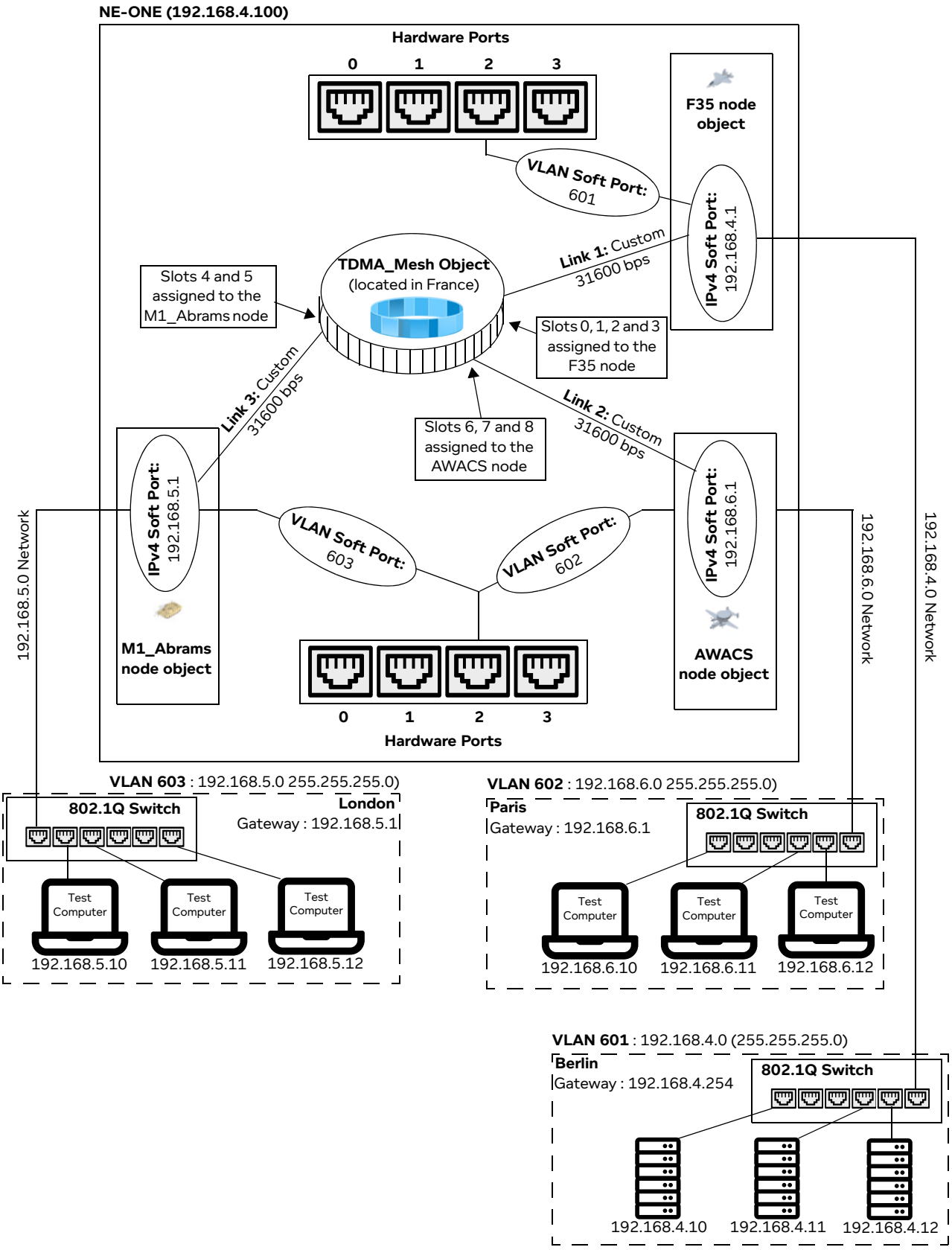


ILLUSTRATION 146 - EXAMPLE TDMA NETWORK (WITH VLAN AND IPV4 SOFT PORTS)

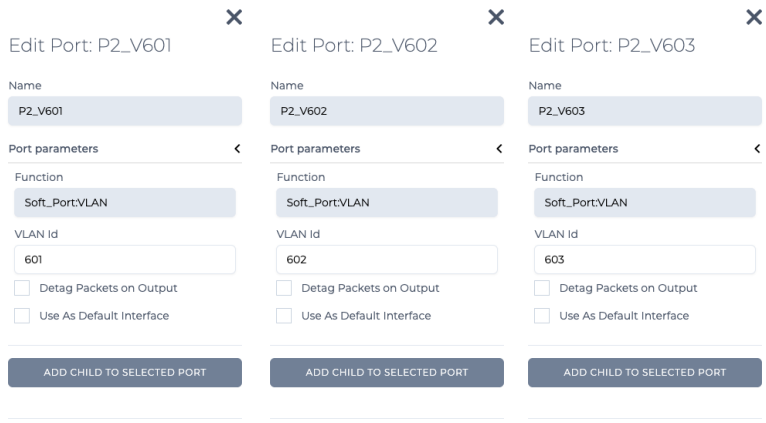


4-5-1. Prerequisite Steps Performed by an Admin User

In order for a non-admin user to create a TDMA network based on this example, an admin user needs to do the following prerequisite steps:

1. Configure the NE-ONE with a static IP address of 192.168.4.50 according to the steps described in *Configuring the Management Port Settings* on page 60 of *Chapter 4*, *Installation and Configuration*.
2. Request to the corporate network administrator that a VLAN (802.1Q) Trunk port is set up on the switch, trunking at least VLANs 601, 602, and 603.
3. Request to the corporate network administrator that the corporate switch's routing addresses 192.168.5.1 and 192.168.6.1 are removed from its routing tables, as the NE-ONE will take over that function.
4. Connect NE-ONE hardware port (in our example, hardware port 2) to that Trunk port with a suitable cable.
5. Create one VLAN soft port for each required VLANs (601, 602, and 603) on the NE-ONE's hardware port (in our example, hardware port 2) according the steps described in *Creating a VLAN Soft Port* on page 107 in *Chapter 5*, *Ports and Services Management*, with each VLAN soft port having **Detag Packets** on **Output and Default Interface** settings disabled (unticked), as shown in *Illustration 107*.

ILLUSTRATION 147 - VLAN SOFT PORT CONFIGURATIONS



VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2 | VLAN Soft Port assigned to hardware port 2

Note: The naming convention of the VLAN soft ports uses the P2 prefix to indicate that these ports are children of hardware port 2, where VNNN denotes a VLAN port with that ID (tag). You can use any soft port names you want, but they should be meaningful.

6. Create and assign IPv4 soft ports to the VLAN soft ports. To do this, within each of the VLAN soft ports, create an IPv4 soft port according the steps described in *Creating an IPv4 Soft Port* on page 114 in *Chapter 5*, *Ports and Services Management*, with the following settings (*Illustration 140* on page 455).
   - VLAN 601 soft port contains IPv4 soft port called 192.168.4.1, with IP address 192.168.4.1, netmask 255.255.255.0, and gateway 192.168.4.254.
   - VLAN 602 soft port contains IPv4 soft port called 192.168.6.1, with IP address 192.168.6.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway as there are no other routers in the network 192.168.6.0, only the NE-ONE itself which is acting as the gateway.
   - VLAN 603 soft port contains IPv4 soft port called 192.168.5.1, with IP address 192.168.5.1, netmask 255.255.255.0, and gateway 0.0.0.0 (i.e it is acting as a gateway). There is no gateway

as there are no other routers in the network 192.168.6.0, only the NE-ONE itself which is acting as the gateway.

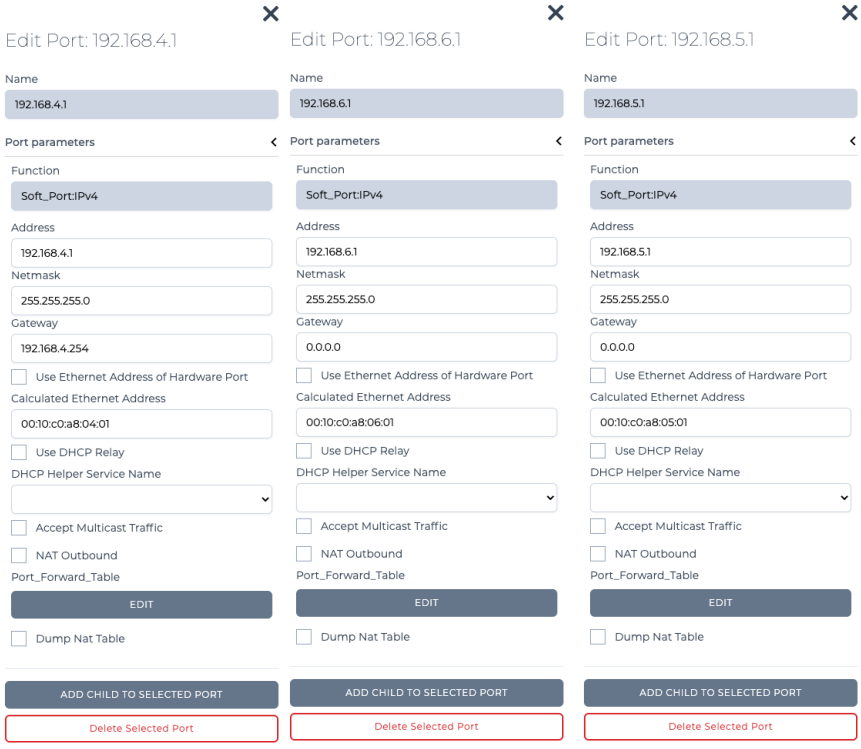
Note: Notice that there is only one IPv4 soft port in each VLAN soft port, as we only require one IP address in each VLAN network. Also, again for clarity, name given to each of the IPv4 soft ports is the same name as its IP address.

The resulting soft port layout for this example is shown in *Illustration 141* on page 456, which give a non-admin user all the soft ports they need to create a Free Form type Multi-Point network based on our example described above.

Note: Our example is for three end nodes, a TDMA Mesh node, and three links with three VLAN soft ports and three IPv4 soft ports. This is easily extensible to much larger networks with many more end nodes, links, VLAN soft ports and IPv4 soft ports.

7. Assign the created IPv4 soft ports (192.168.4.1, 192.168.5.1, and 192.168.6.1) to the intended non-admin user who will create the Free Form Multi-Type network according to the steps described in *Configuring and Editing User Permissions (for Built-in and LDAP authentication)* on page 205 in *Chapter 6*, *User Administration*.

ILLUSTRATION 148 - IPV4 SOFT PORT CONFIGURATIONS FOR CLOUD SPOKE EXAMPLE

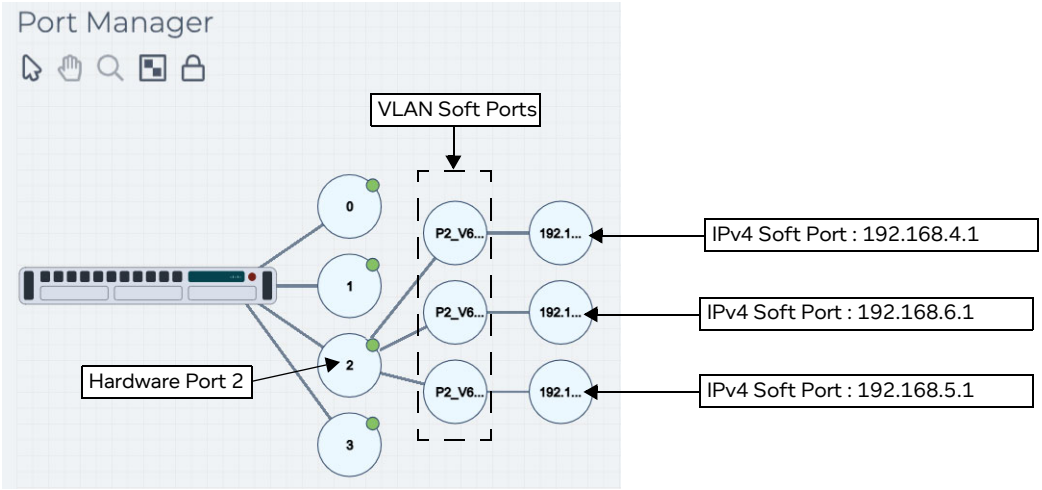


IPv4 Soft Port assigned to VLAN Soft Port 601

IPv4 Soft Port assigned to VLAN Soft Port 602

IPv4 Soft Port assigned to VLAN Soft Port 603

ILLUSTRATION 149 - RESULTING VLAN AND IPV4 SOFT PORT LAYOUT FOR TDMA EXAMPLE



4-5-2. TDMA Network Creation Steps Performed by a Non Admin User

Once the NE-ONE has been configured by an admin user according to *Section 4-3-1*, a non-admin user (or admin user) can create a Free Form Multi-Point network for the example described above, using the following steps:

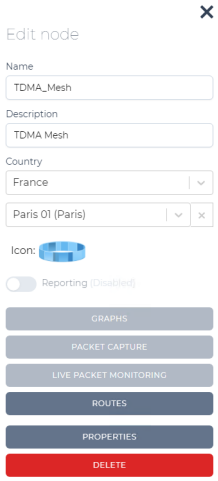
1. Launch the **Multi-Point Designer** page, and choose the Free Form network topology template, using the following sub-steps:
   a. Select **Networks** from the Menu.
   b. From the **Networks** page (see *Illustration 4* on page 42) that appears, click **New Network**.
   c. From the **Network Wizard** page (see *Illustration 84*) that appears, in the **Free Form** panel, click **CREATE**.
   d. From the **Network Name** dialog box that appears, type an appropriate network name (in our example, type **`TDMA Mesh`**), then click **OK**.

   A new (i.e. undefined) Multi-Node network appears based on the selected Free Form network topology template you selected. At this stage, the Workspace is empty, and nothing is configured in the network.
2. From the **Multi-Point Designer** page, optionally tick the **Show node names**, **Show link names**, and **Show node ports** check boxes from the **VIEW** drop-down menu.

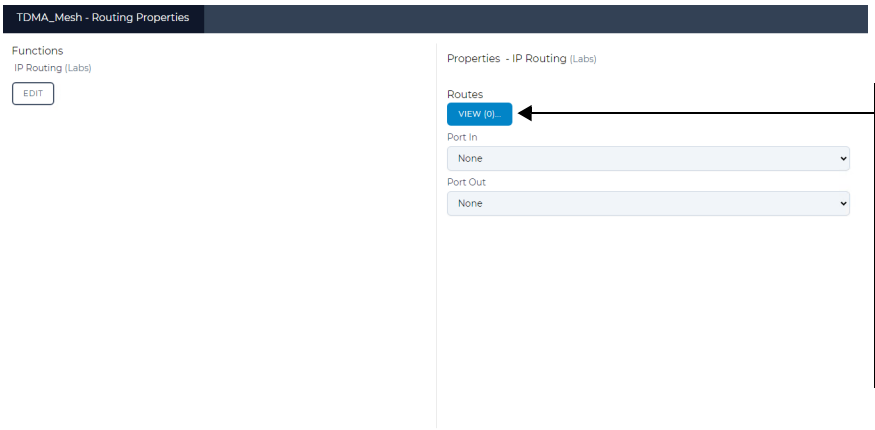
   Note: This optional step is useful in letting you identify what still needs configuring in the Multi-Point network. Undefined nodes have the generic names **node0**, **node1**, etc. Undefined links have the format **node0<-->node1**, etc. End nodes with undefined input and output ports show nothing.
3. Create the TDMA Mesh node on the Workspace. To do this, from the **Node Icons** panel, drag the TDMA Mesh icon from within the **Defense** tab) into the middle of the Workspace. For more information, see *Creating Nodes in the Workspace* on page 318.
4. Define the TDMA node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:
   a. In the **Name** field, type **`TDMA_Mesh`**. By default it gets named TDMA Mesh 0.
   b. In the **Description** field, type **`TDMA Mesh`**.
   c. From the **Country** drop-down field, select **France**.

      Note: You can start typing the word `france` in order to select **France** quickly from the list of countries.

d. From the **Choose a location** drop-down field, select **Paris 01 (Paris)**.
Note: You can start typing the location in order to select it quickly from the list of locations.
The **Edit node** panel now looks as follows.



e. Since the TDMA Mesh node will accept traffic from all end nodes, the **Port In** and **Port Out** are left set to **None**. However, to see this and the status of the other routes, click on the **Routes** button.
A **TDMA_Mesh Routing Properties** window appears.



At this stage no routes exist. As you create the end nodes and links between the end nodes and the TDMA Mesh, the routes are automatically generated by the NE-ONE, and the number in the **View** button updates corresponding to the number of links. Later on in the procedure you need to complete configuring the routes that are automatically generated by the NE-ONE.

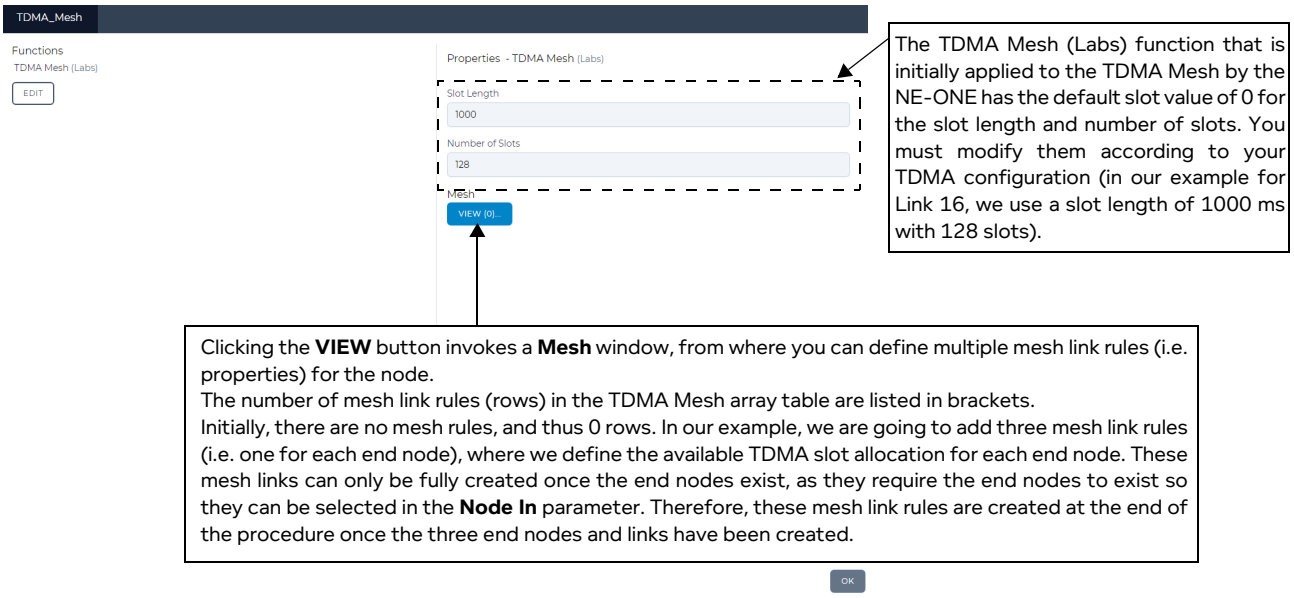
By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down field is set to **None**. These do not need changing. Notice that because at this stage no other end nodes or links have been added, the **Routes View** button indicates 0 routes. As you create the end nodes and links later on, these routes will be automatically created by the NE-ONE. You will need to complete the configuration of these routes later on in this procedure.

f. Click **OK** to return to the **Edit node** panel.

g. At this stage you can define the slot length and number of slots for the TDMA Mesh. When you dragged the TDMA Mesh into the Workspace, the NE-ONE automatically assigns it the TDMA Mesh (Labs) function with 0 slots and 0 ms slot length. In the **Edit Node** panel, click on the **PROPERTIES** button, then from the **Node Properties Window** that appears (see *Illustration 98*

on page 345), click on the **Cloud** button.

A **TDMA_Mesh** window appears with 0 mesh link rules.



h. In the **Slot Length** field enter **1000** (i.e. 1000 ms). This creates a slot length of 1 second.

i. In the **Number of Slots** field, enter **128**.

Note:

Although the three end nodes that you will add will not use up all the slot numbers, is it recommended to set the maximum number of slots to "future proof" the capacity (i.e. cycle time (slot length x number of slots) of your TDMA configuration without the need to change it later on. The NE-ONE will implement the same cycle time and the unused slots are still present in the cycle. This lets you add additional end nodes at a later time on the unused slots, and thus future proofing your TDMA implementation on the NE-ONE.

j. Click to ✕ close the **Edit node** panel.

5. Create the F35 node on the Workspace. To do this, from the **Node Icons** panel, drag the F35 icon from within the **Defense** tab into the top right hand side area of the Workspace. For more information, see *Creating Nodes in the Workspace* on page 318.

6. Define the F35 node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:

   a. In the **Name** field, type **`F35`**.

   b. In the **Description** field, type **`F35 Combat Aircraft`**.

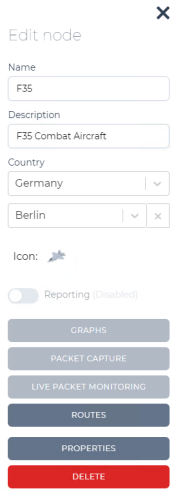
   c. From the **Country** drop-down field, select **Germany**.

   Note: You can start typing the word `germany` in order to select **Germany** quickly from the list of countries.

   d. From the **Choose a location** drop-down field, select **Berlin**.

   Note: You can start typing the location in order to select it quickly from the list of locations.

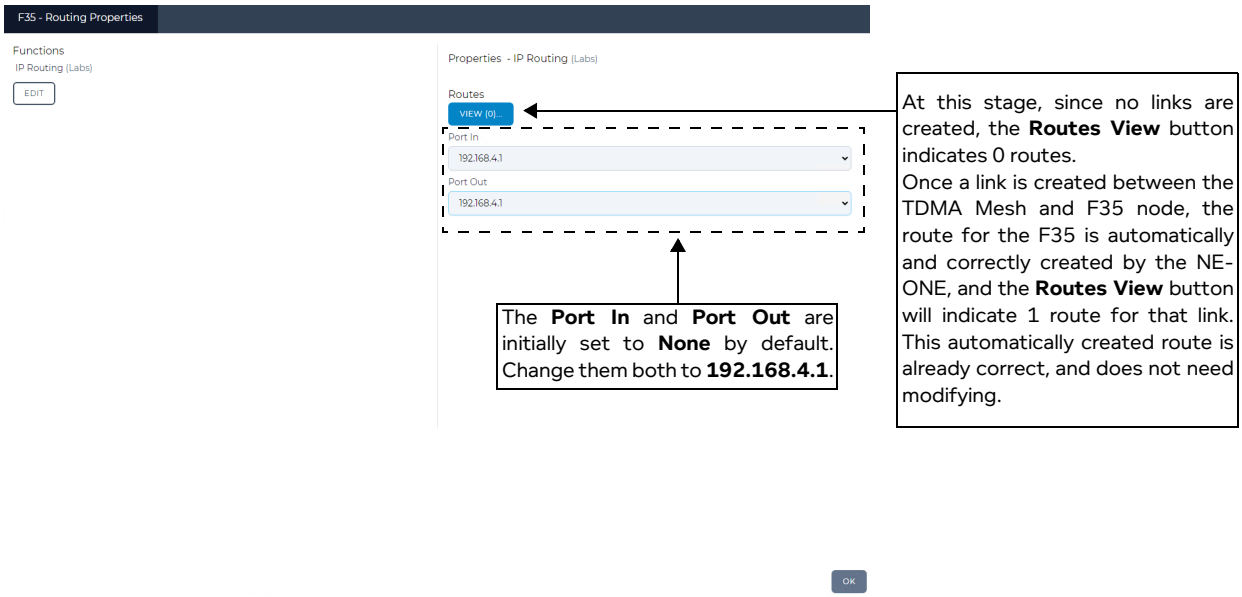
The **Edit node** panel now looks as follows.



At this stage you now need to assign the IPv4 soft port 192.168.4.1 to the F35 node.

e. Click on the **Routes** button.

An **F35 - Routing Properties** window appears, letting you define the F35 node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down field is set to **None**.



f. In **Port In** drop-down field of the **F35 - Routing Properties** window, select an appropriate input port for the F35 node. In our example, select **192.168.4.1**, which represents the IPv4 soft port with IP address 192.168.4.1 that was created within the VLAN soft port 601 of the NE-ONE.

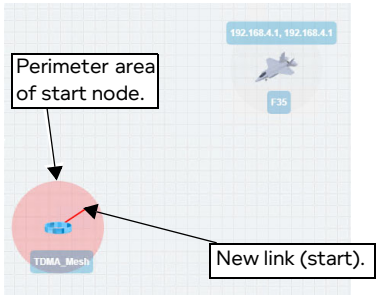
g. In **Port Out** drop-down field of the **F35 - Routing Properties** window, select an appropriate input port for the F35 node. In our example, select **192.168.4.1**, which represents the IPv4 soft port with IP address 192.168.4.1 that was created within the VLAN soft port 601 of the NE-ONE.

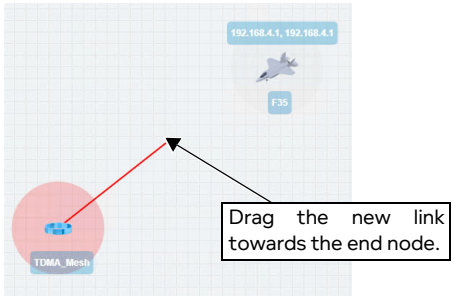
h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

i. Click to ✕ close the **Edit node** panel.

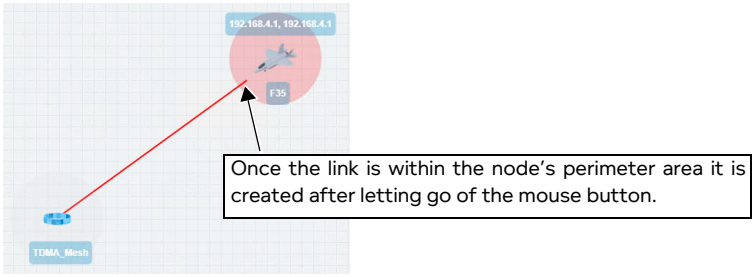
At this stage no link exists between the F35 node and the TDMA Mesh node.

7. Create a link between the TDMA Mesh node and F35 nodes, going from starting from the TDMA Mesh (left side) to F35 (right side). To do this, do the following:
   a. On the TDMA Mesh node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).
      A red line representing the new link appears within the perimeter area of the TDMA Mesh node.





   b. Continue dragging the link into the perimeter area of the F35 node (considered the right node).

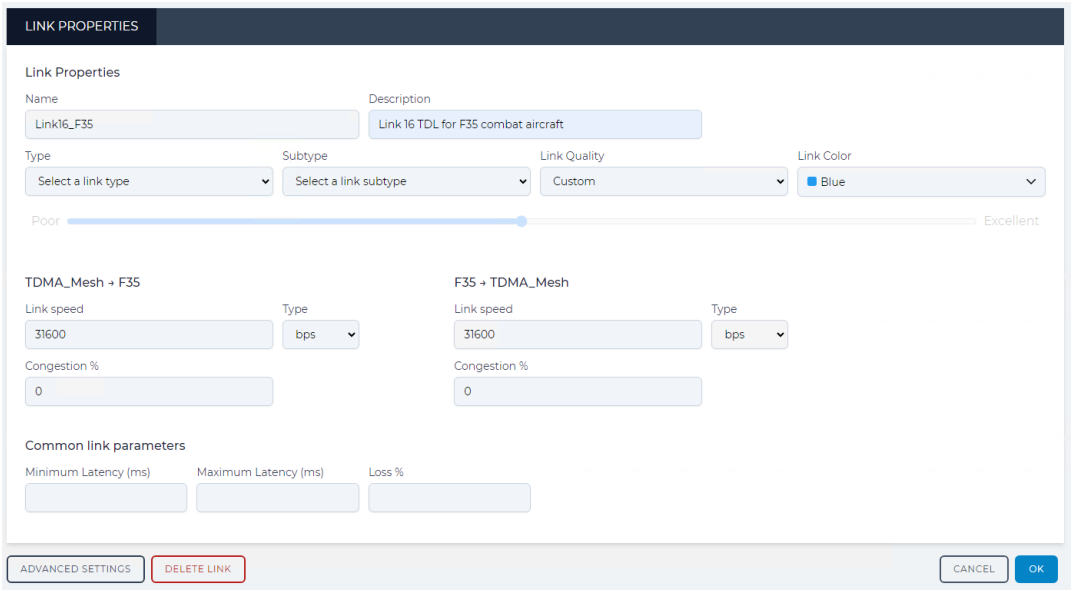


   c. Once the end of the link is in the perimeter area of the F35 node, let go of the mouse button.
      A **Link Name** dialog box appears.
   d. From the **Link Name** dialog box that appears, type **`Link16_F35`**, then click **OK**.

   At this stage the newly created and named **Link16_F35** link appears between the TDMA Mesh and F35 nodes.

   The newly created **Link16_F35** link now needs configuring. In our example it will be configured as a custom link with a data rate of 31600 bps.
8. In the Workspace, click on the **Link16_F35** link, and from the **Edit link** panel that appears click the **EDIT** button.
   A **Link** page appears.
9. From the **Link** page that appears, do the following:
   a. Leave the **Name** field unchanged as it inherits the name you originally specified when you created the link.
   b. In the **Description** field, type **`Link 16 TDL for F35 combat aircraft`**.
   c. Leave the **Type** drop-down field unchanged.

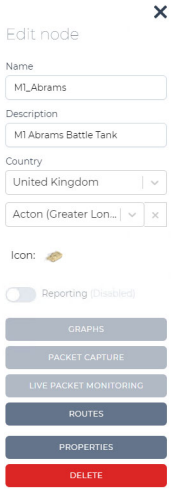
d. Leave the **Subtype** drop-down field unchanged.
e. From the **Link Quality** drop-down field, select **Custom**.
f. In the **Link speed** field for the TDMA_Mesh to F35 direction, type **31600**.
g. In the **Link speed** field for the F35 to TDMA_Mesh direction, type **31600**.
h. Leave the two Congestion% parameters, the **Minimum Latency (ms)** parameter, the **Maximum Latency (ms)** parameter, and the **Loss %** parameter unchanged.
i. From the **Link Color** drop-down field, leave the color set to **Blue**.



j. Click **OK** to submit the link properties.
You are returned to the Workspace in the **Multi-Point Designer** page.

10. Create the M1_Abrams node on the Workspace. To do this, from the **Node Icons** panel, drag the M1 Abrams icon from within the **Defense** tab into the top right hand side area of the Workspace. For more information, see *Creating Nodes in the Workspace* on page 318.
11. Define the M1_Abrams node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:
    a. In the **Name** field, type **`M1_Abrams`**.
    b. In the **Description** field, type **`M1 Abrams Battle Tank`**.
    c. From the **Country** drop-down field, select **United Kingdom**.
    Note: You can start typing the word `united` in order to select **United Kingdom** quickly from the list of countries.
    d. From the **Choose a location** drop-down field, select **Acton (Greater London)**.
    Note: You can start typing the location in order to select it quickly from the list of locations.

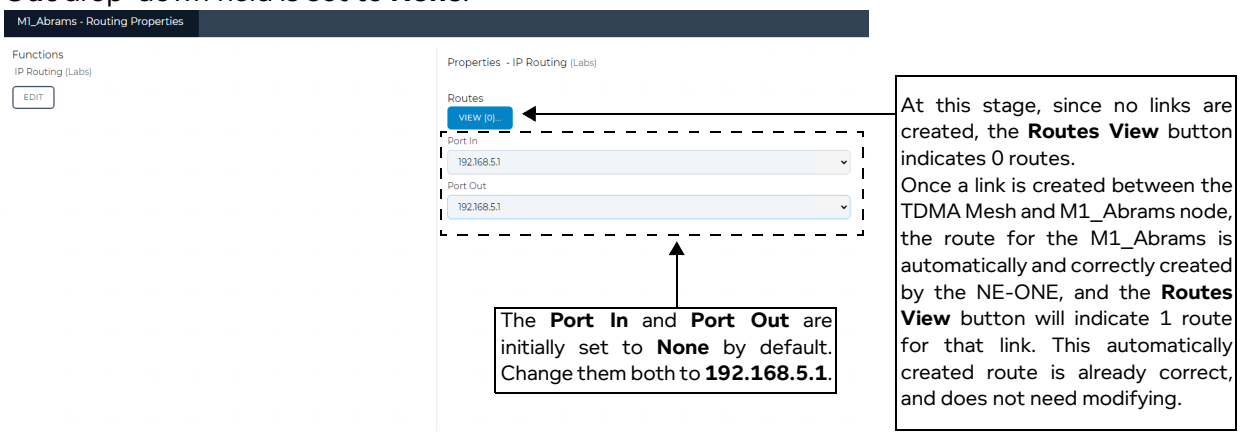
The **Edit node** panel now looks as follows.



At this stage you now need to assign the IPv4 soft port 192.168.5.1 to the M1_Abrams node.

e. Click on the **Routes** button.

An **M1_Abrams - Routing Properties** window appears, letting you define the M1_Abrams node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down field is set to **None**.



f. In **Port In** drop-down field of the **M1_Abrams - Routing Properties** window, select an appropriate input port for the M1_Abrams node. In our example, select **192.168.5.1**, which represents the IPv4 soft port with IP address 192.168.5.1 that was created within the VLAN soft port 603 of the NE-ONE.

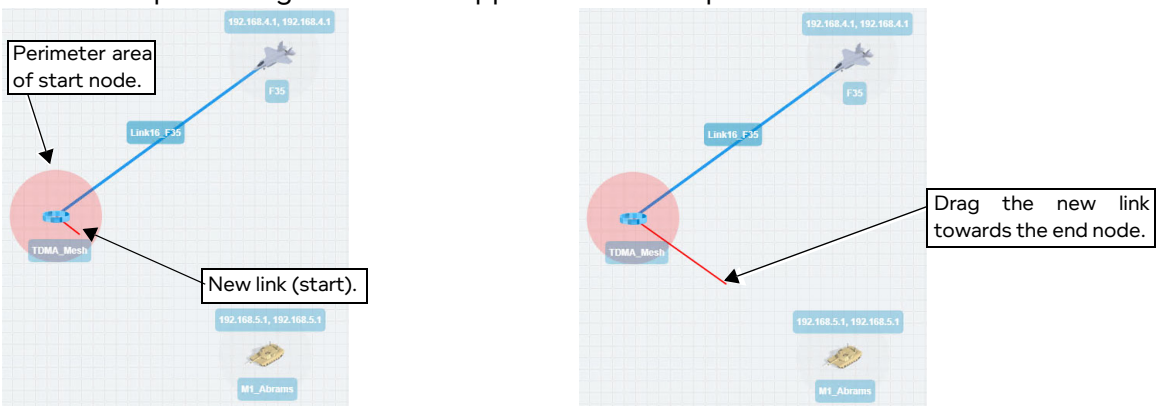
g. In **Port Out** drop-down field of the **M1_Abrams - Routing Properties** window, select an appropriate input port for the M1_Abrams node. In our example, select **192.168.5.1**, which represents the IPv4 soft port with IP address 192.168.5.1 that was created within the VLAN soft port 603 of the NE-ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

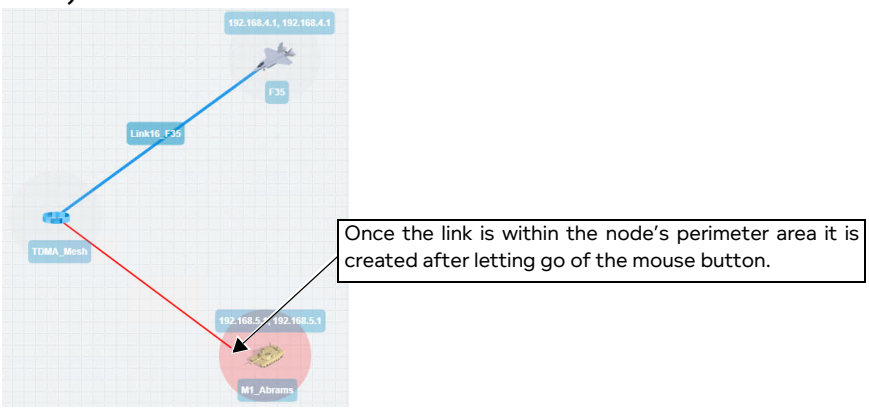
i. Click to ✕ close the **Edit node** panel.

At this stage no link exists between the M1_Abrams node and the TDMA Mesh node.

12. Create a link between the TDMA Mesh node and M1_Abrams nodes, going from starting from the TDMA Mesh (left side) to M1_Abrams (right side). To do this, do the following:
    a. On the TDMA Mesh node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).
    A red line representing the new link appears within the perimeter area of the TDMA Mesh node.

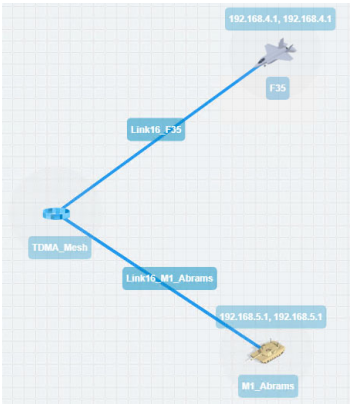


    b. Continue dragging the link into the perimeter area of the M1_Abrams node (considered the right node).



    c. Once the end of the link is in the perimeter area of the M1_Abrams node, let go of the mouse button.
    A **Link Name** dialog box appears.
    d. From the **Link Name** dialog box that appears, type **`Link16_M1_Abrams`**, then click **OK**.

At this stage the newly created and named **Link16_M1_Abrams** link appears between the TDMA Mesh and M1_Abrams nodes.



The newly created **Link16_M1_Abrams** link now needs configuring. In our example it will be configured as a custom link with a data rate of 31600 bps.

13. In the Workspace, click on the **Link16_M1_Abrams** link, and from the **Edit link** panel that appears click the **EDIT** button.

    A **Link** page appears.

14. From the **Link** page that appears, do the following:

    a. Leave the **Name** field unchanged as it inherits the name you originally specified when you created the link.

    b. In the **Description** field, type **`Link 16 TDL for M1 Abrams Battle Tank`**.

    c. Leave the **Type** drop-down field unchanged.

    d. Leave the **Subtype** drop-down field unchanged.

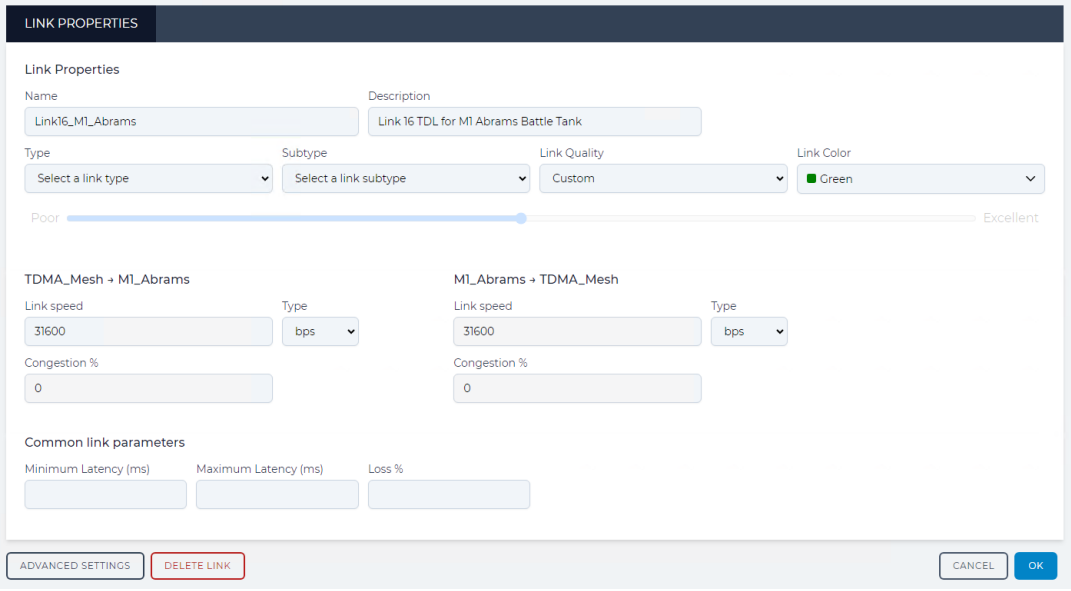
    e. From the **Link Quality** drop-down field, select **Custom**.

    f. In the **Link speed** field for the TDMA_Mesh to M1_Abrams direction, type **`31600`**.

    g. In the **Link speed** field for the M1_Abrams to TDMA_Mesh direction, type **`31600`**.

    h. Leave the two Congestion% parameters, the **Minimum Latency (ms)** parameter, the **Maximum Latency (ms)** parameter, and the **Loss %** parameter unchanged.

    i. From the **Link Color** drop-down field, select **Green**.



    j. Click **OK** to submit the link properties.

    You are returned to the Workspace in the **Multi-Point Designer** page.

15. Create the AWACS node on the Workspace. To do this, from the **Node Icons** panel, drag the AWACS icon  from within the **Defense** tab into the top right hand side area of the Workspace. For more information, see *Creating Nodes in the Workspace* on page 318.

16. Define the AWACS node parameters. In the Workspace, click on the node icon, and from the **Edit node** panel that appears, do the following:

    a. In the **Name** field, type **`AWACS`**.

    b. In the **Description** field, type **`Airborne Warning and Control System`**.

    c. From the **Country** drop-down field, select **France**.

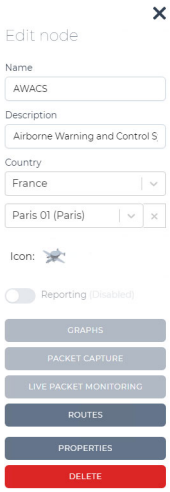
    Note: You can start typing the word `france` in order to select **France** quickly from the list of

countries.

d. From the **Choose a location** drop-down field, select **Paris 01 (Paris)**.

Note: You can start typing the location in order to select it quickly from the list of locations.

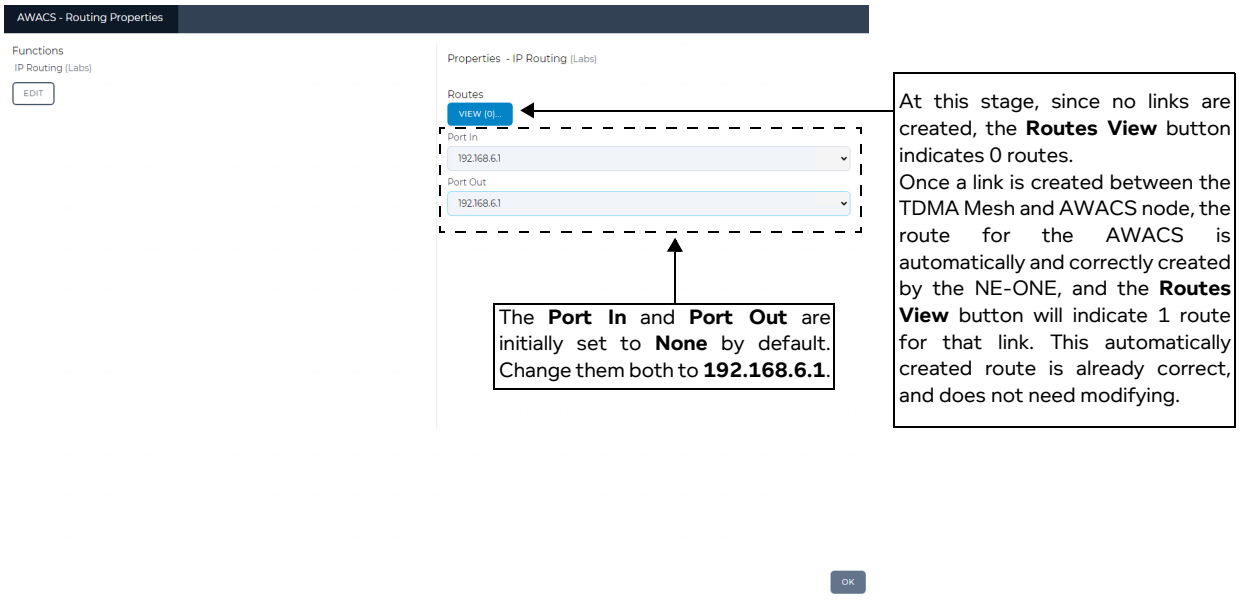
The **Edit node** panel now looks as follows.



At this stage you now need to assign the IPv4 soft port 192.168.6.1 to the AWACS node.

e. Click on the **Routes** button.

An **AWACS - Routing Properties** window appears, letting you define the AWACS node's routing properties. By default, the **Port In** drop-down field is set to **None**, and the **Port Out** drop-down field is set to **None**.



f. In **Port In** drop-down field of the **AWACS - Routing Properties** window, select an appropriate input port for the AWACS node. In our example, select **192.168.6.1**, which represents the IPv4 soft port with IP address 192.168.6.1 that was created within the VLAN soft port 602 of the NE-ONE.

g. In **Port Out** drop-down field of the **AWACS - Routing Properties** window, select an appropriate input port for the AWACS node. In our example, select **192.168.6.1**, which represents the IPv4 soft port with IP address 192.168.6.1 that was created within the VLAN soft port 602 of the NE-

ONE.

h. Click **OK** to commit the routing settings and return to the **Edit node** panel.

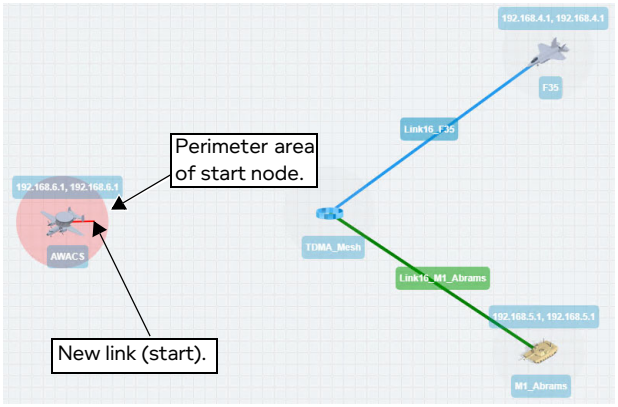
i. Click to ✕ close the **Edit node** panel.

At this stage no link exists between the AWACS node and the TDMA Mesh node.

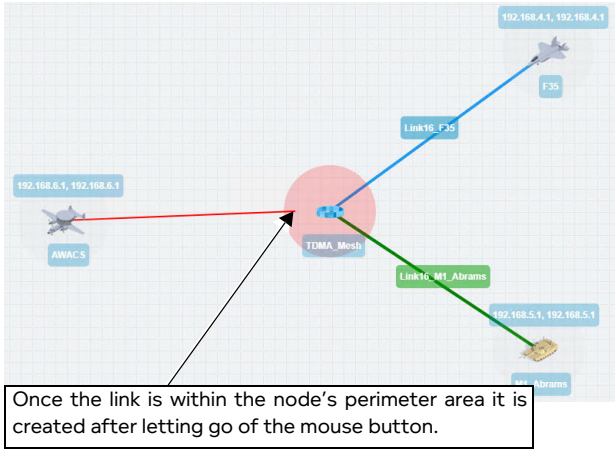
17. Create a link between the TDMA Mesh node and AWACS nodes, going from starting from the TDMA Mesh (left side) to AWACS (right side). To do this, do the following:

a. On the TDMA Mesh node (considered the left node) where you want the link to begin, click within the node perimeter area of the node (but not on the actual node icon).

A red line representing the new link appears within the perimeter area of the TDMA Mesh node.



b. Continue dragging the link into the perimeter area of the AWACS node (considered the right node).



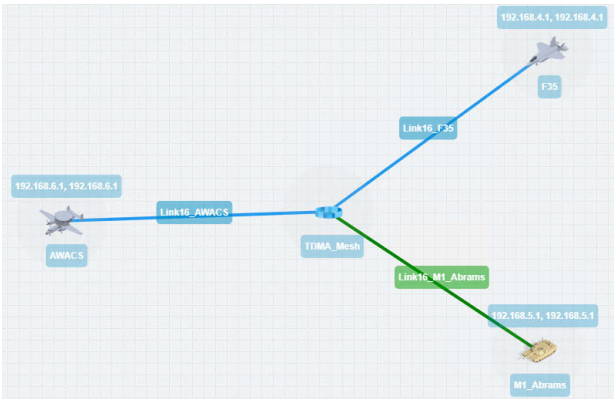
c. Once the end of the link is in the perimeter area of the AWACS node, let go of the mouse button.

A **Link Name** dialog box appears.

d. From the **Link Name** dialog box that appears, type **`Link16_AWACS`**, then click **OK**.

At this stage the newly created and named **Link16_AWACS** link appears between the TDMA Mesh

and AWACS nodes.



The newly created **Link16_AWACS** link now needs configuring. In our example it will be configured as a custom link with a data rate of 31600 bps.

18. In the Workspace, click on the **Link16_AWACS** link, and from the **Edit link** panel that appears click the **EDIT** button.

    A **Link** page appears.

19. From the **Link** page that appears, do the following:

    a. Leave the **Name** field unchanged as it inherits the name you originally specified when you created the link.

    b. In the **Description** field, type **`Link 16 TDL for Airborne Warning and Control System`**.

    c. Leave the **Type** drop-down field unchanged.

    d. Leave the **Subtype** drop-down field unchanged.

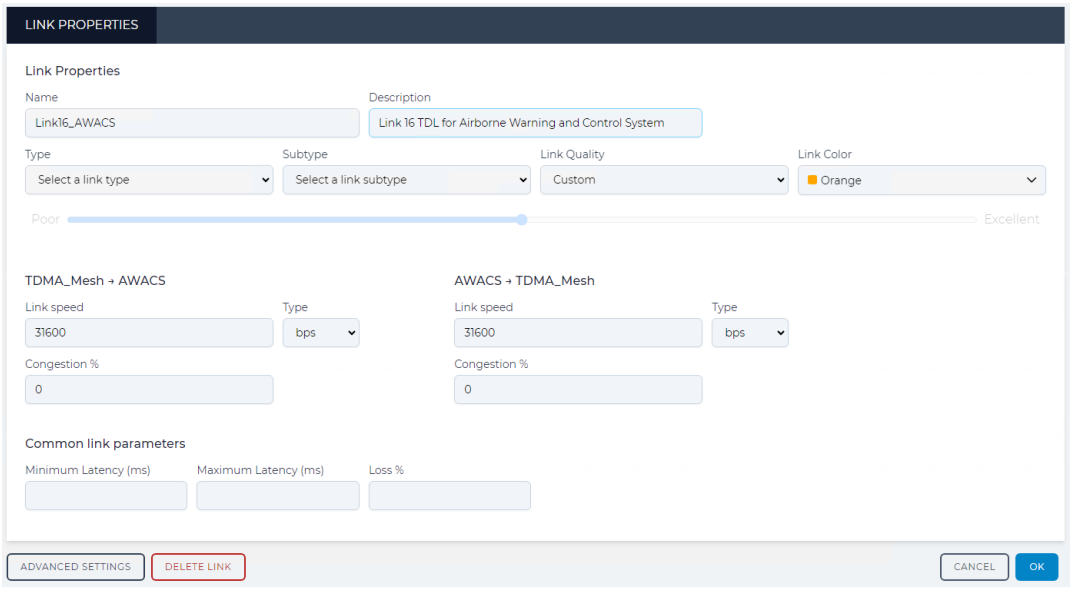
    e. From the **Link Quality** drop-down field, select **Custom**.

    f. In the **Link speed** field for the TDMA_Mesh to AWACS direction, type **31600**.

    g. In the **Link speed** field for the AWACS to TDMA_Mesh direction, type **31600**.

    h. Leave the two Congestion% parameters, the **Minimum Latency (ms)** parameter, the **Maximum Latency (ms)** parameter, and the **Loss %** parameter unchanged.

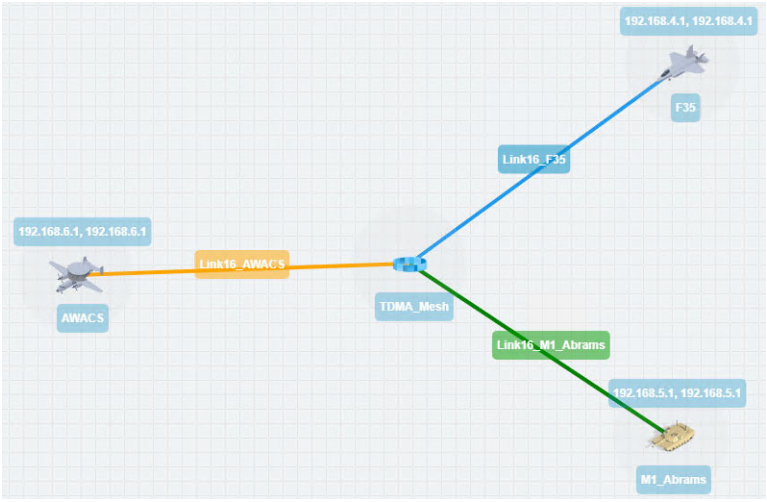
    i. From the **Link Color** drop-down field, select **Orange**.



j. Click **OK** to submit the link properties.

You are returned to the Workspace in the **Multi-Point Designer** page.

At this stage the link names are now defined to something meaningful within your TDMA Mesh Multi-Point network.



The link names you defined will appear as selectable output ports within the routing table you define for the central TDMA Mesh node.

20. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click the **SAVE** button.
21. As mentioned in the steps above, the routing for the three end nodes automatically and correctly created by the NE-ONE.

    By default, the NE-ONE automatically creates one working (all traffic, no filtering) route in the end node's routing table. That is, the NE-ONE automatically selects **Port In** value you specified in the **Routing Properties** window, and automatically selects the connected link for the **Port Out**.

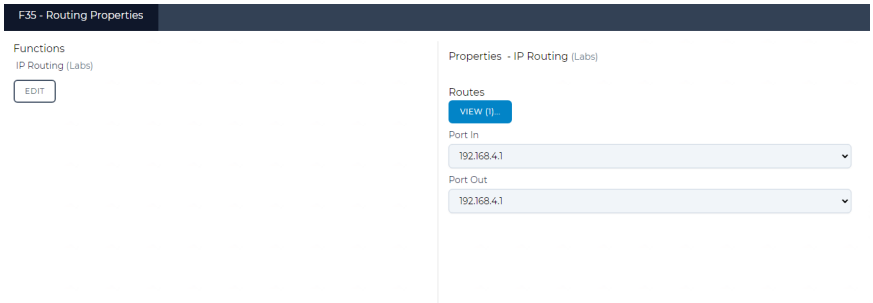
    If necessary, to create additional routing rules within the routing table for the end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes with filtering are set up.

    You can optionally see the routes that were automatically and correctly created by the NE-ONE by following the sub-steps below:

    For the F35 end node, do the following:

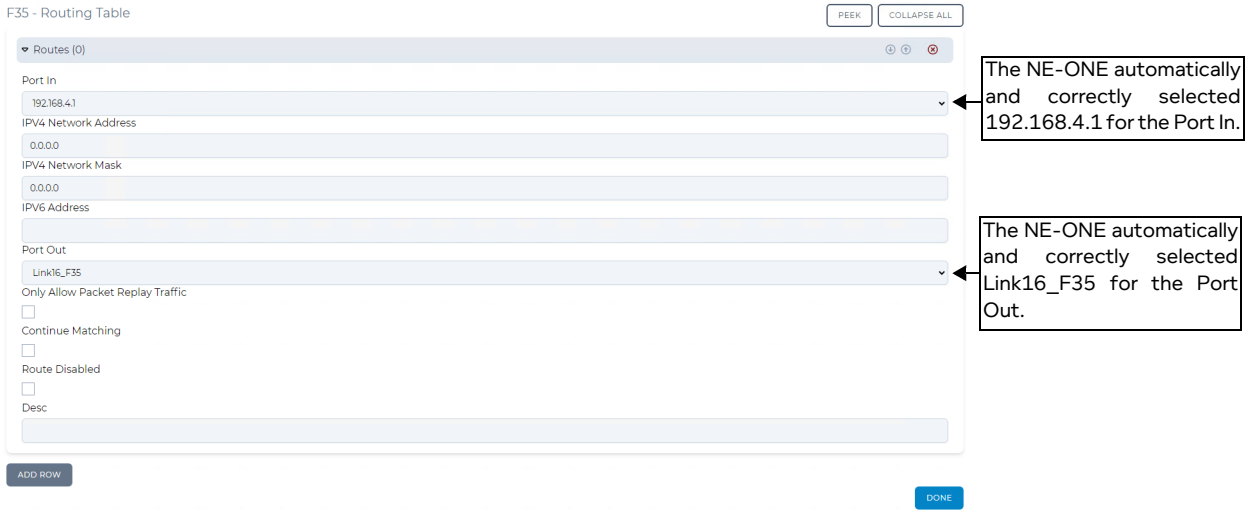
    a. Click on the F35 end node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button.

    The **F35 - Routing Properties** window appears.



    b. From the **F35 - Routing Properties** window that appears, click the **Routes VIEW (1)** button.

The **F35 - Routing Table** window appears.



c. If necessary, to create additional routing rules within the routing table for the F35 end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes with filtering are set up.

d. Click **DONE** to return to the **F35 - Routing Properties** window.

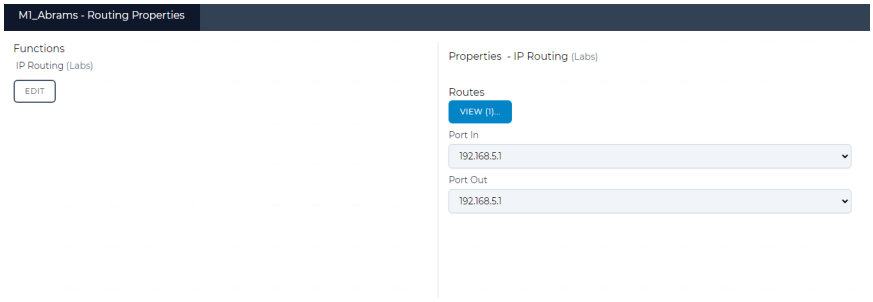
e. In the **F35 - Routing Properties** window, click **OK** to return to the Workspace.

f. In the **Routing Properties** window, click **OK**.

For the M1_Abrams end node, do the following:

a. Click on the M1_Abrams end node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button.

The **M1_Abrams - Routing Properties** window appears.



b. From the **M1_Abrams - Routing Properties** window that appears, click the **Routes VIEW (1)** button.

The **M1_Abrams - Routing Table** window appears.

c. If necessary, to create additional routing rules within the routing table for the M1_Abrams end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes with filtering are set up.

d. Click **DONE** to return to the **M1_Abrams - Routing Properties** window.

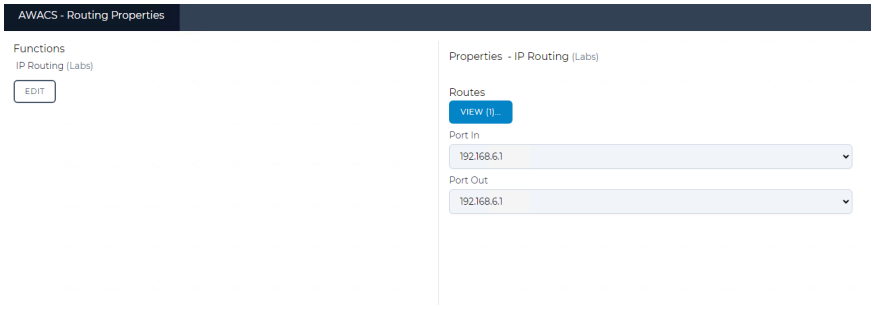
e. In the **M1_Abrams - Routing Properties** window, click **OK** to return to the Workspace.

f. In the **Routing Properties** window, click **OK**.

For the AWACS end node, do the following:

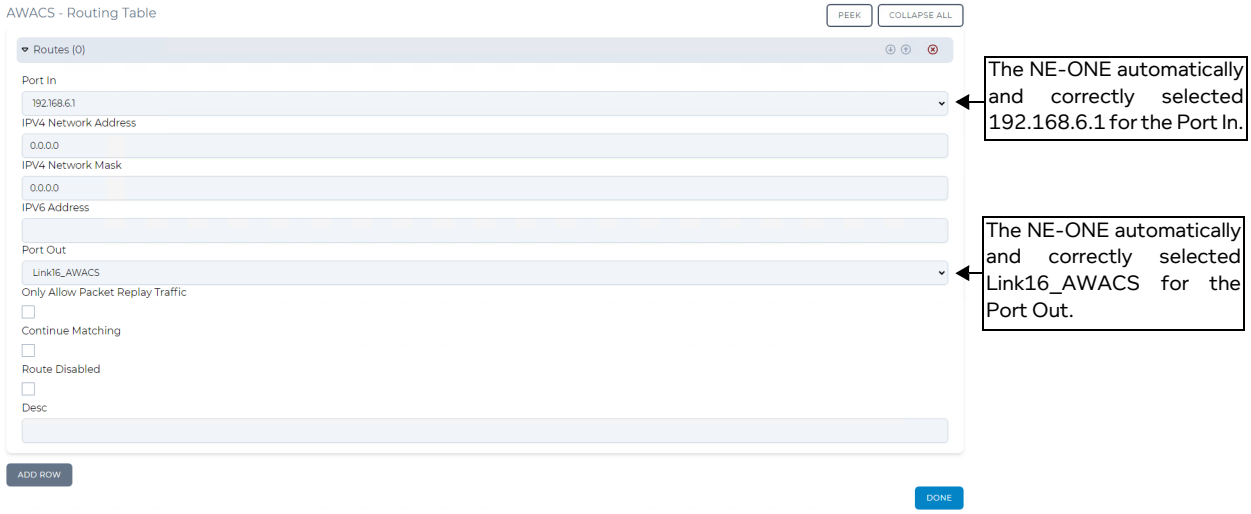
a. Click on the AWACS end node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button.

The **AWACS - Routing Properties** window appears.



b. From the **AWACS - Routing Properties** window that appears, click the **Routes VIEW (1)** button.

The **AWACS - Routing Table** window appears.



c. If necessary, to create additional routing rules within the routing table for the AWACS end node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table. In our example, no additional routes with filtering are set up.

d. Click **DONE** to return to the **AWACS - Routing Properties** window.

e. In the **AWACS - Routing Properties** window, click **OK** to return to the Workspace.

f. In the **Routing Properties** window, click **OK**.

You are returned to the **Multi-Point Designer** page.

At this stage the routing configuration is now complete for each of the end nodes. You are now ready to complete the routing configuration and define the mesh link rule(s) for the central TDMA_Mesh node.

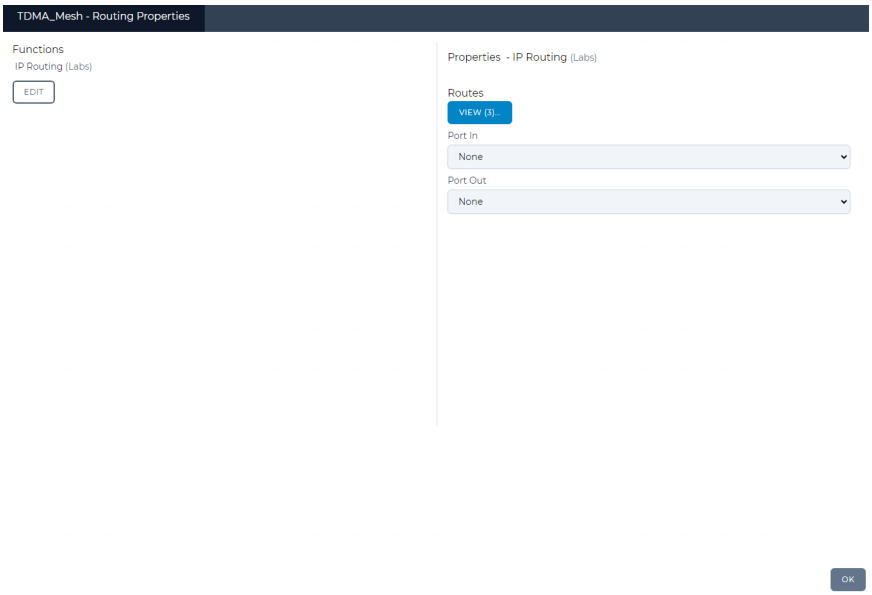
22. At this stage it is prudent to save the progress. To do this, select **FILE > Save** or click the **SAVE** button.

23. Now define the routing table for the TDMA Mesh node. To do this, click on the TDMA_Mesh node in the Workspace, and from the **Edit node** panel that appears, click the **ROUTES** button, then do the following in the **TDMA_Mesh - Routing Properties** window that appears to define the central TDMA Mesh node's routing properties:

a. Leave the **Port In** drop-down field set to **None** (as traffic is coming in to the cloud from all inbound links (in our example, three inbound links)).

b. Leave the **Port Out** drop-down field set to **None** (as traffic is coming out from the cloud to all

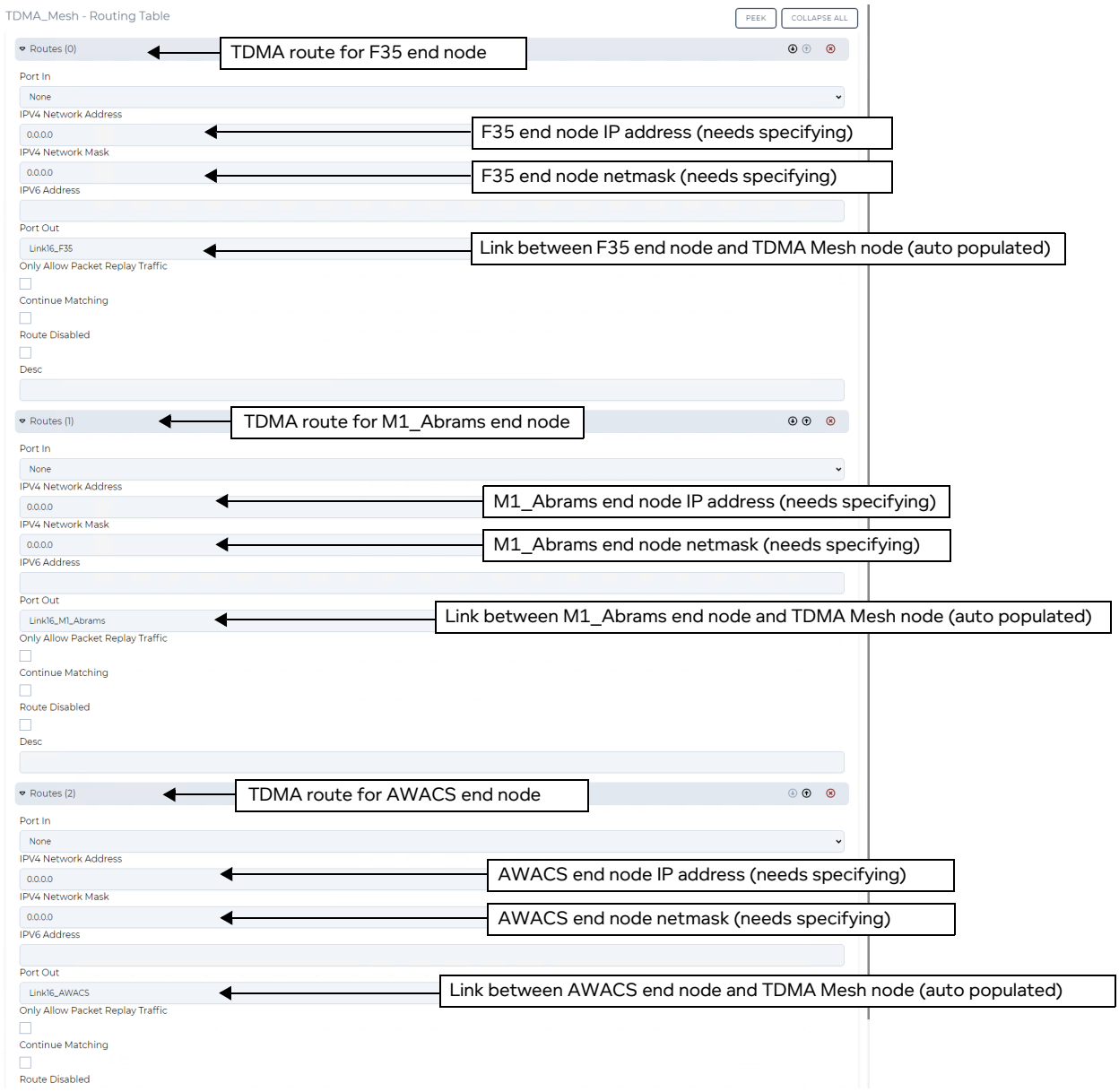
inbound links (in our example, three inbound links)).



By default, the TDMA Mesh node's routing table inherits an empty (undefined) route rule for each of the inbound links. Each of the empty (undefined) route rule corresponding to each of the inbound links must be defined. In our example, three route rules for the three inbound links going into the central TDMA Mesh node need to be defined.

c. From the **TDMA_Mesh - Routing Properties** window that appears, click the **Routes VIEW (1)** button.

The **TDMA_Mesh - Routing Table** window appears with the uncompleted routing configuration.



The **Port Out** field will have already been automatically and correctly configured by the NE-ONE, as follows:

For the F35 end node : **Link16_F16** link.

For the M1_Abrams end : **Link16_M18Abrams** link.

For the AWACS end node : **Link16_AWACS** link.

d. From the **TDMA_Mesh - Routing Table** window that appears, do the following for each of the route rules:

Leave the **Port In** drop-down field set to **None**.

In the **IPv4 Network Address** field, type the IP address of the end node. In our example, do the following:

For the F35 end node (i.e. with the **Port Out** field already automatically set to Link16_F35)), type

192.168.4.1

For the M1_Abrams end node (i.e. with the **Port Out** field already automatically set to Link16_M1_Abrams)), type **192.168.5.1**

For the AWACS node (i.e. with the **Port Out** field already automatically set to Link16_AWACS)), type **192.168.6.1**

In the **IPv4 Netmask** field, type the netmask of the end node. In our example, do the following:

For the F35 end node (i.e. with the **Port Out** field already automatically set to Link16_F35)), type **255.255.255.0**

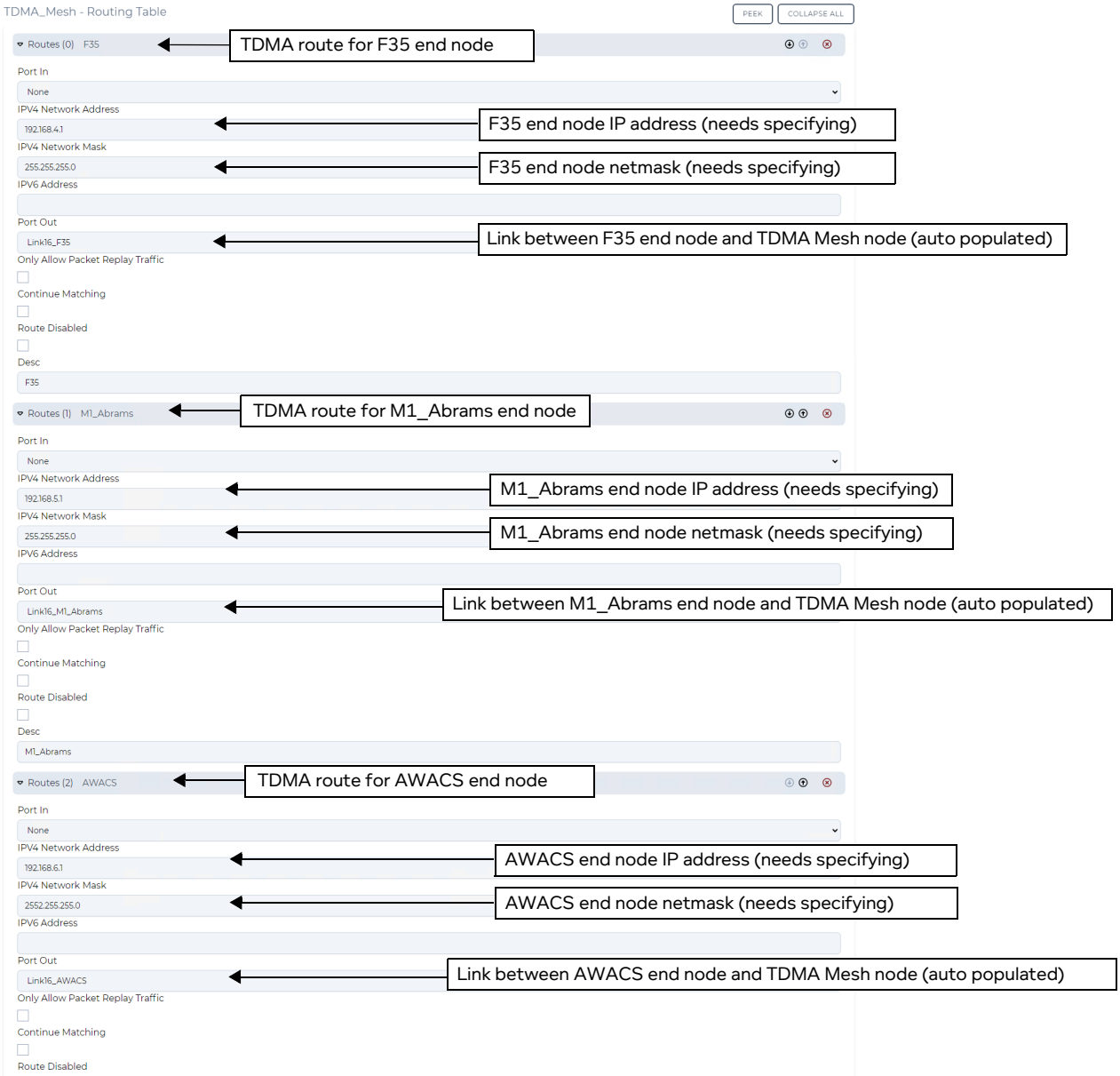
For the M1_Abrams end node (i.e. with the **Port Out** field already automatically set to Link16_M1_Abrams)), type **255.255.255.0**

For the AWACS node (i.e. with the **Port Out** field already automatically set to Link16_AWACS)), type **255.255.255.0**

Leave the **IPv6 Address** drop-down field blank.

The **TDMA_Mesh - Routing Table** window shown in *Illustration 150* on page 491 shows the three rules defined for our example.

ILLUSTRATION 150 - EXAMPLE ROUTES WINDOW (TDMA EXAMPLE)



Click **DONE** to return to the **TDMA_Mesh - Route Properties** window.

If necessary, to create additional routing rules within the routing table for the central TDMA Mesh node, click the **VIEW** button, then **ADD ROW** to define additional routing rules based on the filtering requirements that you want to apply. In our example, no additional route rules are set up in the routing table.

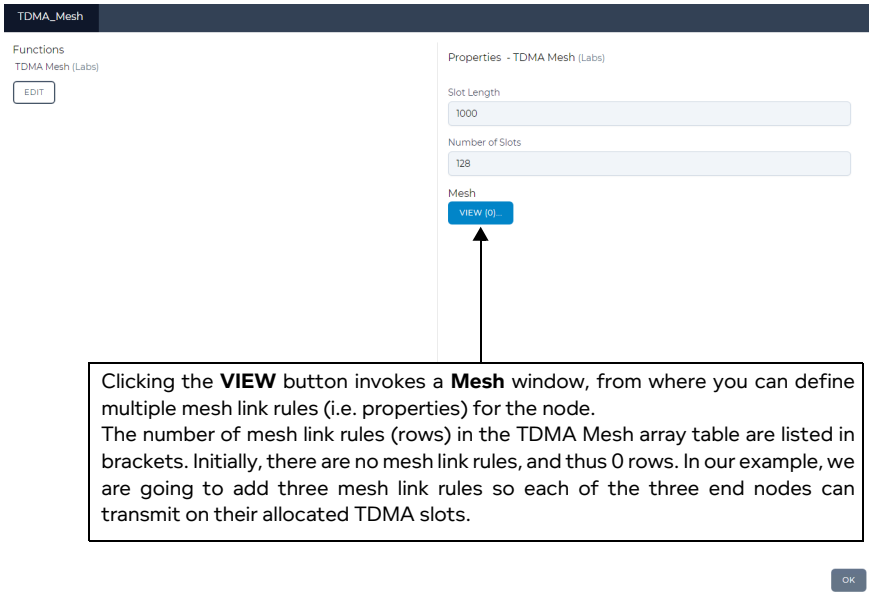
e. From the **TDMA_Mesh - Route Properties** window, click **OK**.

You are returned to the **Multi-Point Designer** page.

24. At this stage the routing configuration is now complete for the central TDMA Mesh node. Now the central TDMA Mesh node's TDMA Mesh (Labs) function needs configuring with three mesh link rules (i.e. one for each end node) so that the transmitted traffic from each of the end nodes can pass through the TDMA Mesh on their allocated slots:
    - Link Id 1: this mesh link rule accepts traffic from the F35 end node with no packet filtering
      Slot List: 0,1,2,3 - these are the TDMA Mesh slots assigned to the F35 end node
      Bandwidth: 10000000 bps
      Queue Length: 6400
      Node In: F35 (this must match the node name that you specified in the **Edit node** panel on the Multi-Point Designer Workspace for the F35 end node).
      Use Last Hop as node in enabled : this uses the port that the packet just came from.
    - Link Id 2: this mesh link rule accepts traffic from the M1_Abrams end node with no packet filtering
      Slot List: 4,5 - these are the TDMA Mesh slots assigned to the M1_Abrams end node
      Bandwidth: 10000000 bps
      Queue Length: 6400
      Node In: M1_Abrams (this must match the node name that you specified in the **Edit node** panel on the Multi-Point Designer Workspace for the M1_Abrams end node).
      Use Last Hop as node in enabled : this uses the port that the packet just came from.
    - Link Id 3: this mesh link rule accepts traffic from the AWACS end node with no packet filtering
      Slot List: 6,7,8 - these are the TDMA Mesh slots assigned to the AWACS end node
      Bandwidth: 10000000 bps
      Queue Length: 6400
      Node In: AWACS (this must match the node name that you specified in the **Edit node** panel on the Multi-Point Designer Workspace for the AWACS end node).
      Use Last Hop as node in enabled : this uses the port that the packet just came from.

    To do this, click on the central TDMA_Mesh node in the Workspace, and from the **Edit node** panel that appears, click the **PROPERTIES** button, then from the **Node Properties Window** that appears (see *Illustration 98* on page 345), click on the **Cloud** button.

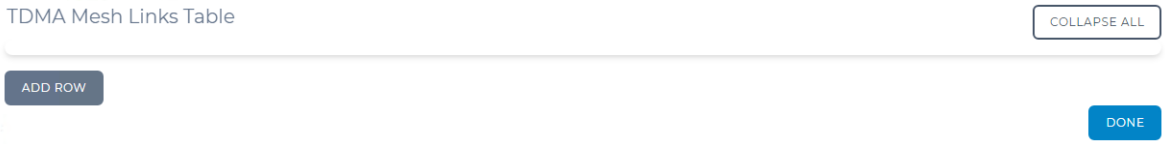
    A **TDMA_Mesh** window appears with no link rules.



Clicking the **VIEW** button invokes a **Mesh** window, from where you can define multiple mesh link rules (i.e. properties) for the node.
The number of mesh link rules (rows) in the TDMA Mesh array table are listed in brackets. Initially, there are no mesh link rules, and thus 0 rows. In our example, we are going to add three mesh link rules so each of the three end nodes can transmit on their allocated TDMA slots.

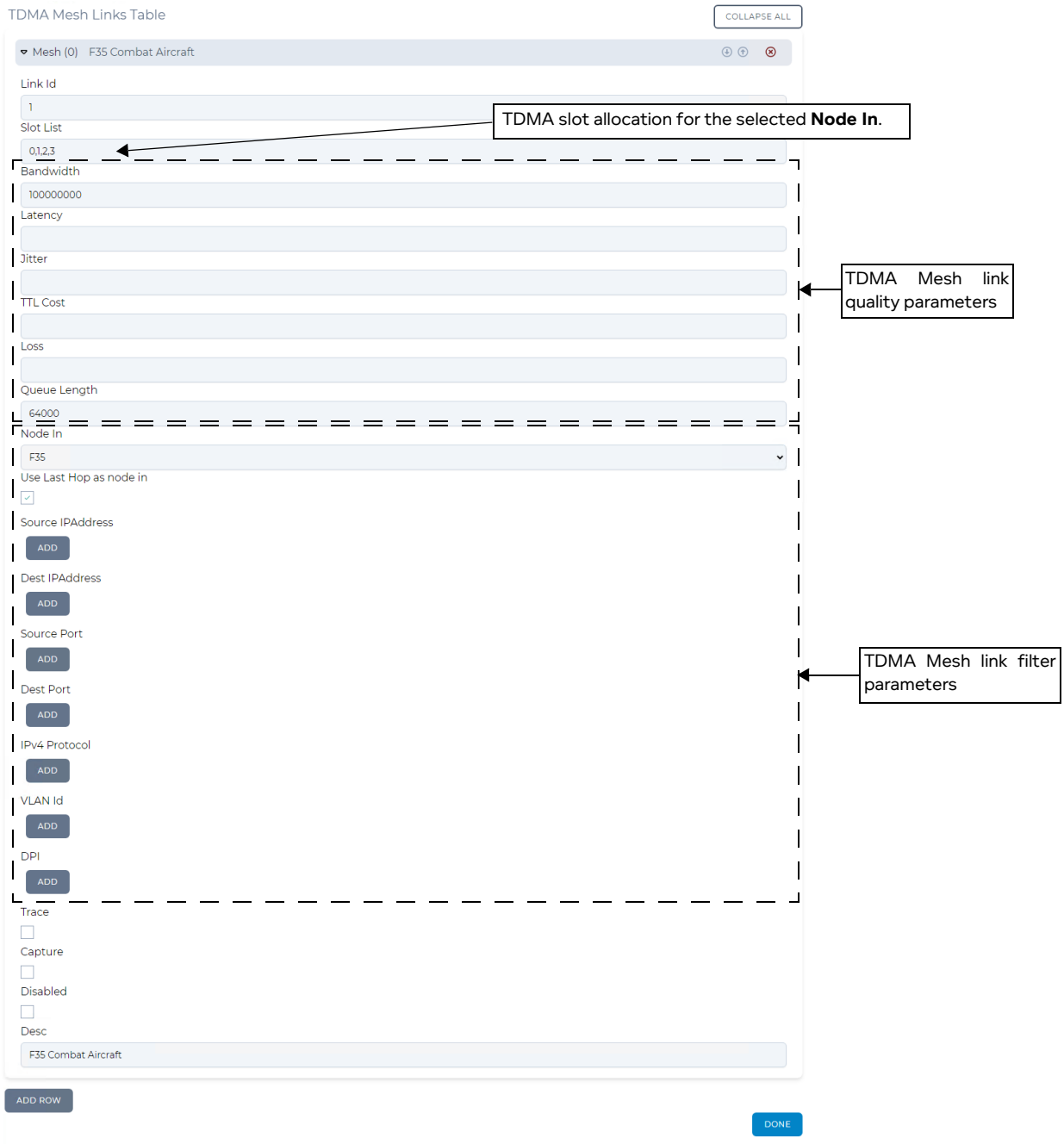
25. Click the **VIEW** button, to open the **TDMA Mesh Links Table** window.

The **TDMA Mesh Links Table** window appears. Initially a node with the TDMA Mesh (Labs) function has no mesh link rules added to it. The **TDMA Mesh Links Table** window lets you add TDMA Mesh link rules. Each TDMA Mesh link rule that you add, appears as a row in the **TDMA Mesh Links Table** window.



26. Click on the **ADD ROW** button.

A new TDMA Mesh link rule row is created, and initially expanded.



Within the TDMA Mesh link rule row, exist all the appropriate elements (i.e. fields, and buttons invoking the definition of ranges - see *Table 60* on page 366), letting you define all aspects of the TDMA Mesh link rule.

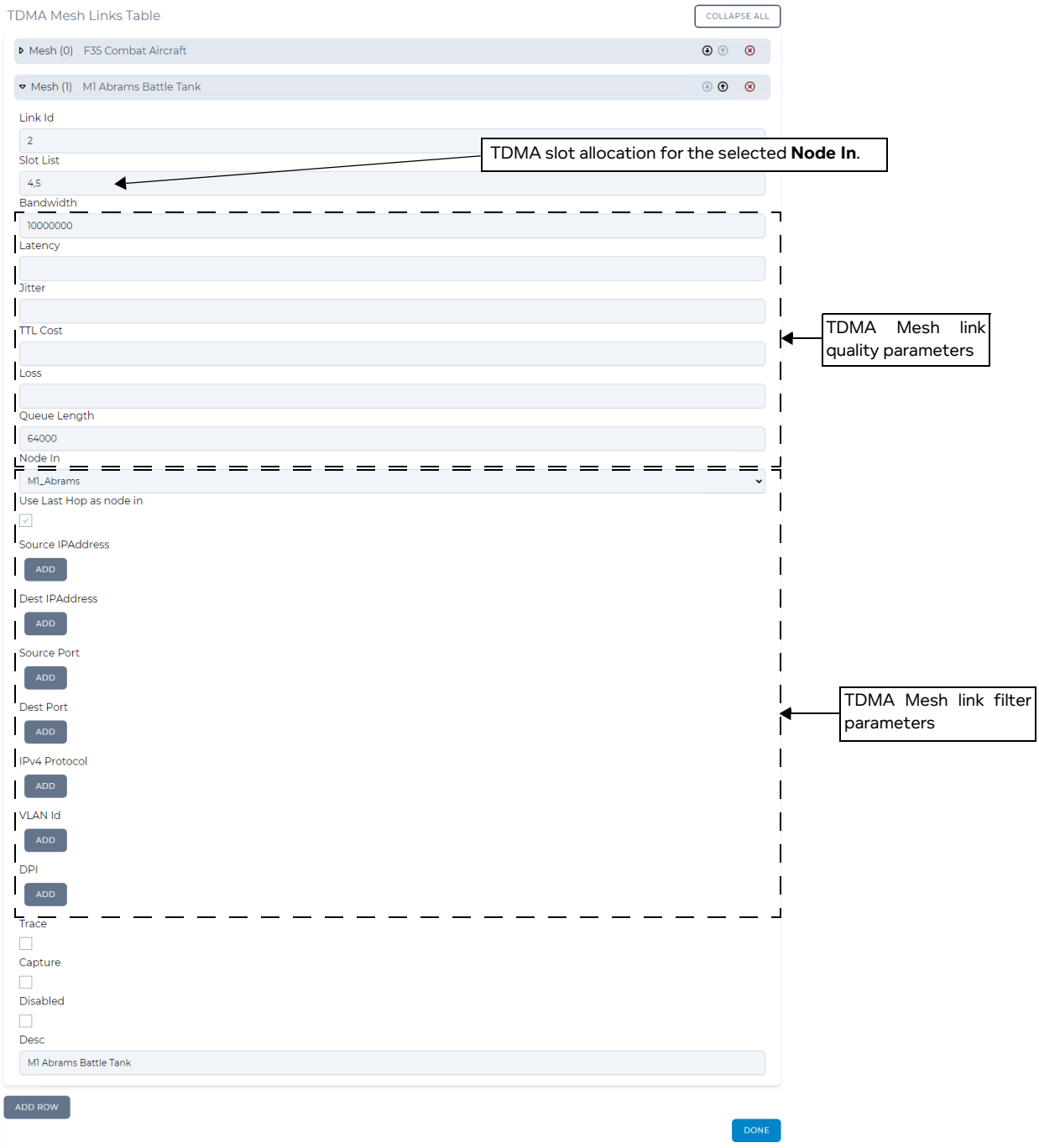
27. Specify the TDMA Mesh link for the F35 end node, as follows:
    - In the **Link Id** field, type **1**.
    - In the **Slot List** field, type **0,1,2,3**. This will assign slots 0, 1, 2 and 3 to the F35 end node. Because a slot length of 1000 ms was created earlier on in step 4, sub-step h for the TDMA Mesh, this effectively creates a transmission window of 4000 ms for the F35 end node.

    Note:
    A slot number can only be used for one end node. The same slot number can not be assigned to another end node. For example, slots 0, 1, 2 and 3 are assigned to the F35 end node, they cannot be assigned to other end nodes.
    - In the **Bandwidth** field, type **10000000**.
    - Leave the **Latency** field blank.
    - Leave the **Jitter** field blank.
    - Leave the **TTL Cost** field blank.
    - Leave the **Loss** field blank.
    - Leave the **Queue Length** field value set to **64000**.
    - From the **Node In** drop-down field, select **F35** (this selects the F35 end node, which will be able to transmit to the TDMA Mesh when the allocated slots 0,1,2 and 3 pass by during the TDMA cycle time).
    - Enable the **Use Last Hop As Port In** check box.
    - Do not define any filters (i.e. leave the **Source IP Address**, **Destination IP Address**, **Source Port**, **Destination Port**, **IPv4 Protocol**, and **VLAN Id** filters to their default (undefined) ranges).
    - Leave the **Trace** check box unticked.
    - Leave the **Capture** check box unticked.
    - Leave the **Disabled** check box unticked.
    - In the **Desc** field, type an appropriate description for the rule (e.g. **F35 Combat Aircraft**).
28. Minimize the newly created **F35 Combat Aircraft** route, click the **ADD ROW** button to add a second mesh link, and expand the newly created (empty) TDMA Mesh link.
29. Specify the TDMA Mesh link for the M1_Abrams end node, as follows:
    - In the **Link Id** field, type **2**.
    - In the **Slot List** field, type **4,5**. This will assign TDMA slots to the M1_Abrams end node. Because a slot length of 1000 ms was created earlier on in step 4, sub-step h for the TDMA Mesh, this effectively creates a transmission window of 2000 ms for the M1_Abrams end node.

    Note:
    A slot number can only be used for one end node. The same slot number can not be assigned to another end node. For example, slots 4 and 5 are assigned to the M1_Abrams end node, they cannot be assigned to other end nodes.
    - In the **Bandwidth** field, type **10000000**.
    - Leave the **Latency** field blank.
    - Leave the **Jitter** field blank.
    - Leave the **TTL Cost** field blank.
    - Leave the **Loss** field blank.

- Leave the **Queue Length** field value set to **64000**.
- From the **Node In** drop-down field, select **M1_Abrams** (this selects the M1_Abrams end node, which will be able to transmit to the TDMA Mesh when the allocated slots 4 and 5 pass by during the TDMA cycle time).
- Enable the **Use Last Hop As Port In** check box.
- Do not define any filters (i.e. leave the **Source IP Address**, **Destination IP Address**, **Source Port**, **Destination Port**, **IPv4 Protocol**, and **VLAN Id** filters to their default (undefined) ranges).
- Leave the **Trace** check box unticked.
- Leave the **Capture** check box unticked.
- Leave the **Disabled** check box unticked.

- In the **Desc** field, type an appropriate description for the rule (e.g. **`M1 Abrams Battle Tank`**).



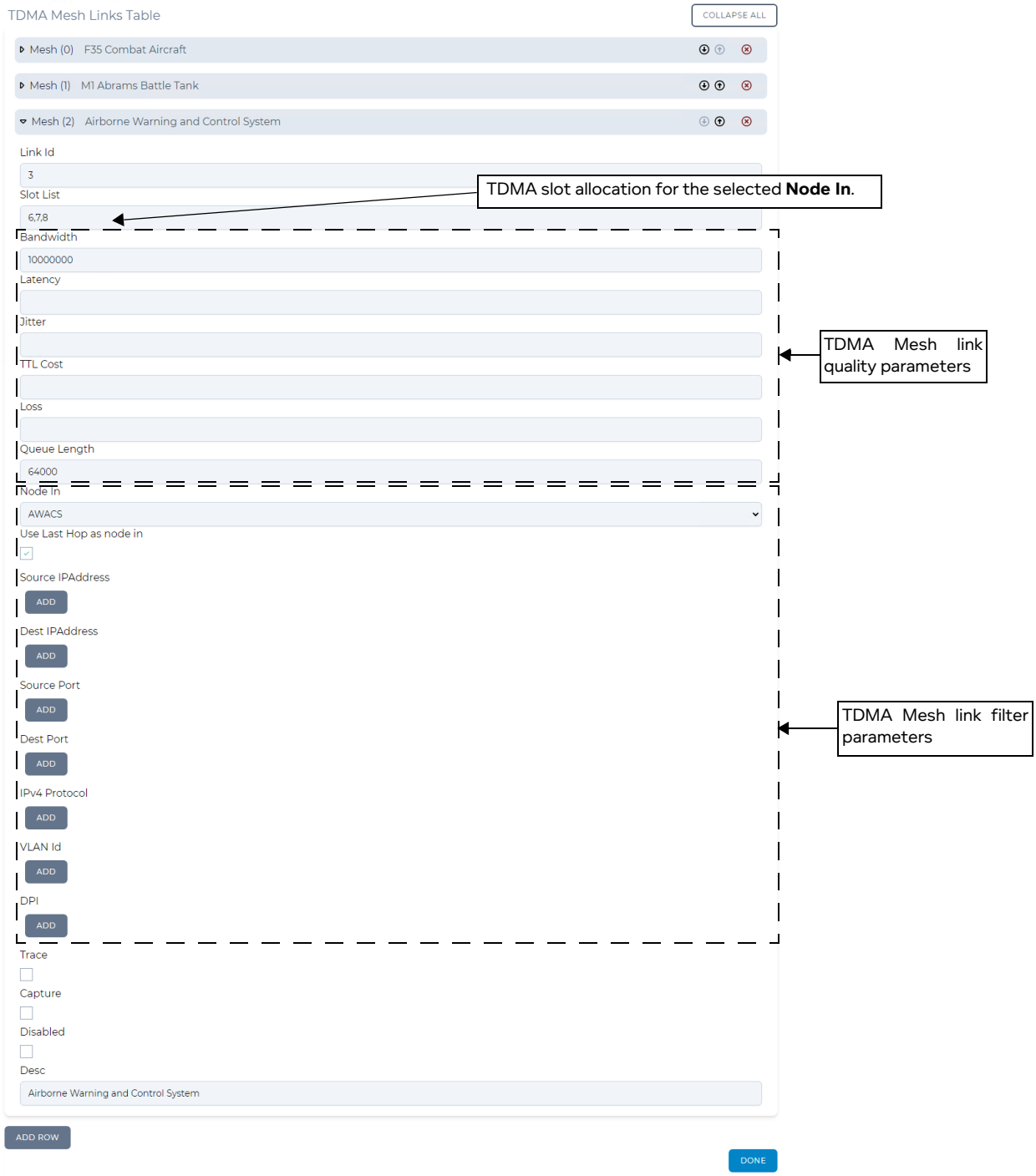
30. Minimize the newly created **M1 Abrams Battle Tank** route, click the **ADD ROW** button to add a third TDMA Mesh link, and expand the newly created (empty) TDMA Mesh link.
31. Specify the TDMA Mesh link for the AWACS end node, as follows:
    - In the **Link Id** field, type **3**.
    - In the **Slot List** field, type **`6,7,8`**. This will assign TDMA slots to the AWACS end node. Because a slot length of 1000 ms was created earlier on in step 4, sub-step h for the TDMA Mesh, this effectively creates a transmission window of 3000 ms for the AWACS end node.

Note:

A slot number can only be used for one end node. The same slot number can not be assigned to another end node. For example, slots 6, 7 and 8 are assigned to the AWACS end node, they cannot be assigned to other end nodes.

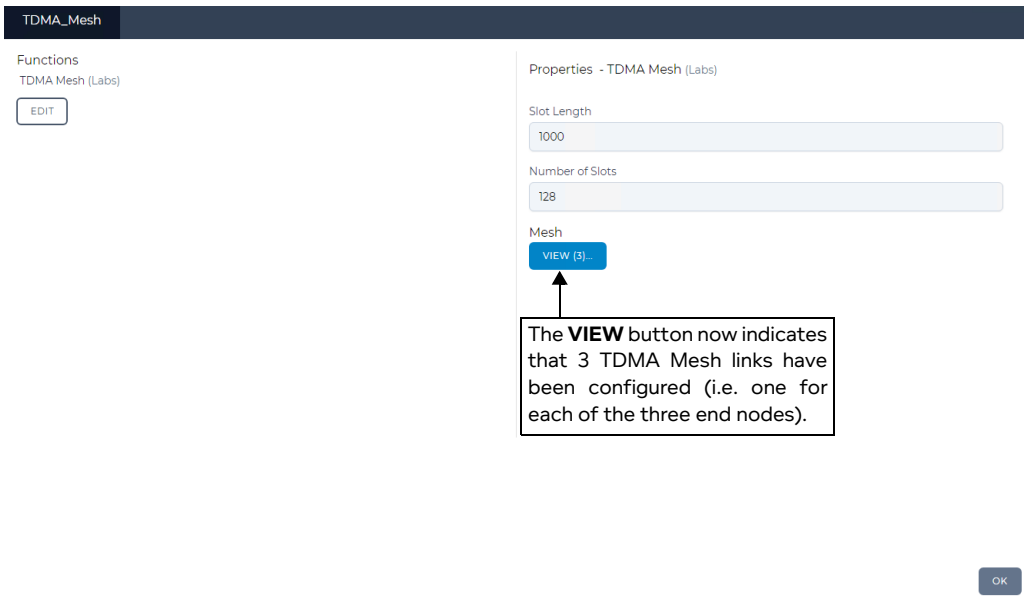
- In the **Bandwidth** field, type **10000000**.
- Leave the **Latency** field blank.
- Leave the **Jitter** field blank.
- Leave the **TTL Cost** field blank.
- Leave the **Loss** field blank.
- Leave the **Queue Length** field value set to **64000**.
- From the **Node In** drop-down field, select **AWACS** (this selects the AWACS end node, which will be able to transmit to the TDMA Mesh when the allocated slots 6, 7 and 8 pass by during the TDMA cycle time).
- Enable the **Use Last Hop As Port In** check box.
- Do not define any filters (i.e. leave the **Source IP Address**, **Destination IP Address**, **Source Port**, **Destination Port**, **IPv4 Protocol**, and **VLAN Id** filters to their default (undefined) ranges).
- Leave the **Trace** check box unticked.
- Leave the **Capture** check box unticked.
- Leave the **Disabled** check box unticked.
- In the **Desc** field, type an appropriate description for the rule (e.g. **Airborne Warning and**

Control System).



32. Click **DONE** to return to the **TDMA_Mesh** window.

The **VIEW** button now shows that 3 TDMA Mesh link rules exist in the **TDMA_Mesh** window.



All the necessary parameters have now been configured for the example TDMA Multi-Point network (*Illustration 145* on page 468).

33. From the **TDMA_Mesh** window, click **OK**.

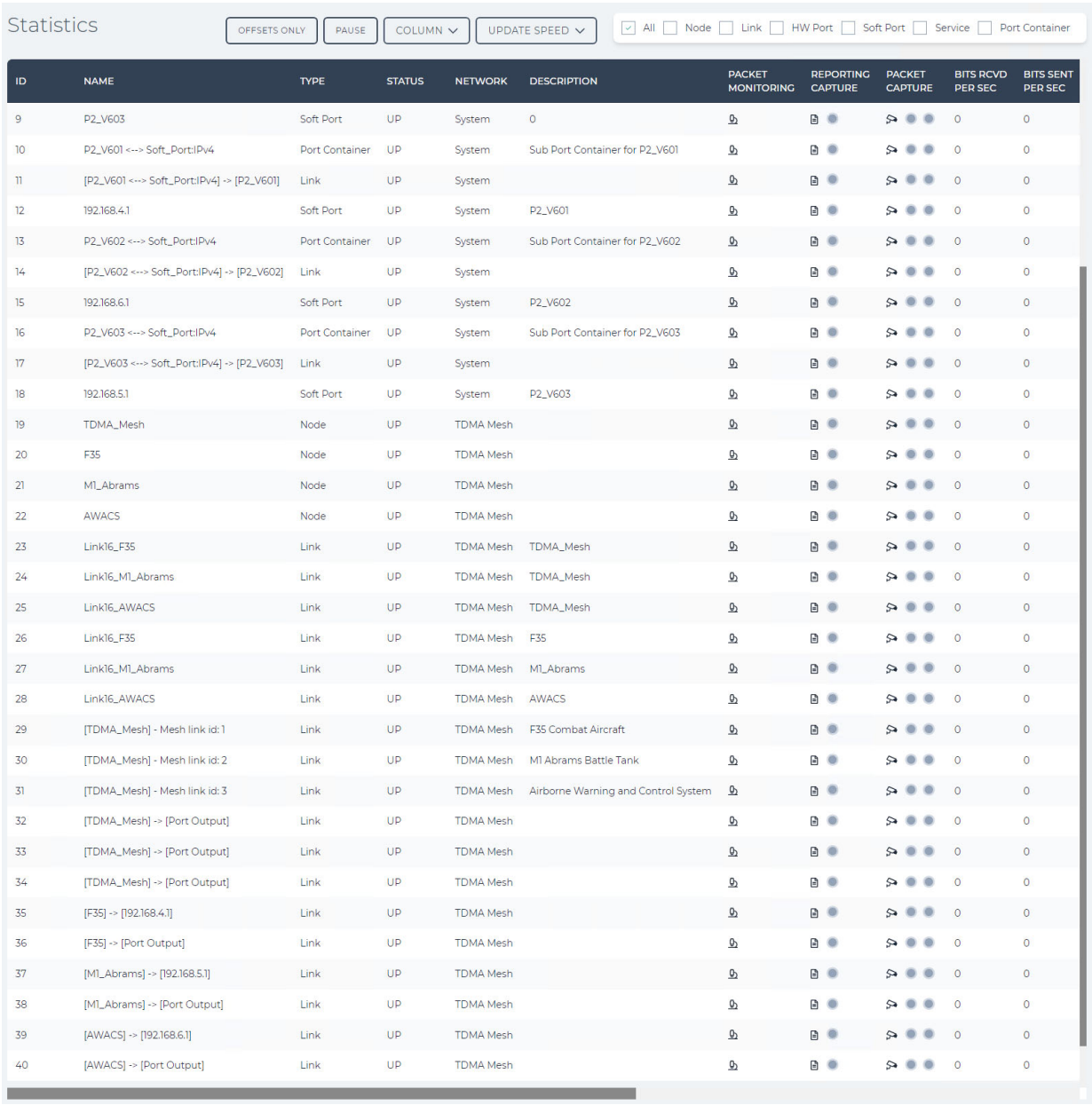
    You are returned to the **Multi-Point Designer** page.

34. Save the finalized TDMA Mesh Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

    The TDMA Mesh Multi-Point network will appear in the **Multi-Point Designer** page as shown in *Illustration 145* on page 468, and is ready to be run (i.e. played).

    If you click the **PLAY** button in the **Multi-Point Designer** page, the TDMA Mesh Multi-Point network starts running and its associated objects appear in the **Statistics** page (see *Illustration 151*).

ILLUSTRATION 151 - EXAMPLE TDMA NETWORK ASSOCIATED OBJECTS VISIBLE IN THE STATISTICS PAGE



ID	NAME	TYPE	STATUS	NETWORK	DESCRIPTION	PACKET MONITORING	REPORTING CAPTURE	PACKET CAPTURE	BITS RCVD PER SEC	BITS SENT PER SEC
9	P2_V603	Soft Port	UP	System	0				0	0
10	P2_V601 <--> Soft_Port:IPv4	Port Container	UP	System	Sub Port Container for P2_V601				0	0
11	[P2_V601 <--> Soft_Port:IPv4] -> [P2_V601]	Link	UP	System					0	0
12	192.168.4.1	Soft Port	UP	System	P2_V601				0	0
13	P2_V602 <--> Soft_Port:IPv4	Port Container	UP	System	Sub Port Container for P2_V602				0	0
14	[P2_V602 <--> Soft_Port:IPv4] -> [P2_V602]	Link	UP	System					0	0
15	192.168.6.1	Soft Port	UP	System	P2_V602				0	0
16	P2_V603 <--> Soft_Port:IPv4	Port Container	UP	System	Sub Port Container for P2_V603				0	0
17	[P2_V603 <--> Soft_Port:IPv4] -> [P2_V603]	Link	UP	System					0	0
18	192.168.5.1	Soft Port	UP	System	P2_V603				0	0
19	TDMA_Mesh	Node	UP	TDMA Mesh					0	0
20	F35	Node	UP	TDMA Mesh					0	0
21	M1_Abrams	Node	UP	TDMA Mesh					0	0
22	AWACS	Node	UP	TDMA Mesh					0	0
23	Link16_F35	Link	UP	TDMA Mesh	TDMA_Mesh				0	0
24	Link16_M1_Abrams	Link	UP	TDMA Mesh	TDMA_Mesh				0	0
25	Link16_AWACS	Link	UP	TDMA Mesh	TDMA_Mesh				0	0
26	Link16_F35	Link	UP	TDMA Mesh	F35				0	0
27	Link16_M1_Abrams	Link	UP	TDMA Mesh	M1_Abrams				0	0
28	Link16_AWACS	Link	UP	TDMA Mesh	AWACS				0	0
29	[TDMA_Mesh] - Mesh link id: 1	Link	UP	TDMA Mesh	F35 Combat Aircraft				0	0
30	[TDMA_Mesh] - Mesh link id: 2	Link	UP	TDMA Mesh	M1 Abrams Battle Tank				0	0
31	[TDMA_Mesh] - Mesh link id: 3	Link	UP	TDMA Mesh	Airborne Warning and Control System				0	0
32	[TDMA_Mesh] -> [Port Output]	Link	UP	TDMA Mesh					0	0
33	[TDMA_Mesh] -> [Port Output]	Link	UP	TDMA Mesh					0	0
34	[TDMA_Mesh] -> [Port Output]	Link	UP	TDMA Mesh					0	0
35	[F35] -> [192.168.4.1]	Link	UP	TDMA Mesh					0	0
36	[F35] -> [Port Output]	Link	UP	TDMA Mesh					0	0
37	[M1_Abrams] -> [192.168.5.1]	Link	UP	TDMA Mesh					0	0
38	[M1_Abrams] -> [Port Output]	Link	UP	TDMA Mesh					0	0
39	[AWACS] -> [192.168.6.1]	Link	UP	TDMA Mesh					0	0
40	[AWACS] -> [Port Output]	Link	UP	TDMA Mesh					0	0

5. OPENING AND PLAYING MULTI-POINT NETWORKS

Multi-Point networks can be opened via two ways. Once opened, a Multi-Point network can be either edited or played.

- Via the Home Page.
- Via the File Browser. For more information, see *Opening a Multi-Point Type Network From the File Browser* on page 590 in *Chapter 13*, *The File Browser*.

Note:
Once a Multi-Point network is playing it is attached to the user who run it, and the ports that it is using cannot be used by any other networks until the currently playing network is stopped. Currently playing networks are listed in the **Active** tab of the **Home** page.

Note:
You can also directly play a Multi-Point network from within the File Browser, without needing to open it. For more information, see *Directly Playing a Multi-Point Type Network From the File Browser* on page 592 in *Chapter 13*, *The File Browser*.

6. DELETING MULTI-POINT NETWORKS

If a Multi-Point network is no longer needed, it can be deleted from the NE-ONE using the File Browser. Multi-Point networks have a file name extension `*.itn`, are located in your

`/Private/networks` directory with the icon, and use the network name that you had specified for the file name. To delete a no longer required Multi-Point network, use the following steps:

1. Click **Management > ••• Platform Settings > File Browser** to launch the File Browser.
2. Navigate to the `/Private/networks` directory, and identify the Multi-Point network you want to delete via its icon and its file name (`*.itn`).
3. Right mouse click on the Multi-Point network file, and select **Delete selected File/Folder** from the File Browser pop-up menu that appears.
4. From the **Confirm delete** dialog box that appears, click **OK**.

This page is intentionally left blank.

CHAPTER 11 CREATING AND RUNNING SCENARIOS

1. INTRODUCTION

This chapter is applicable to non-admin and admin users, and describes:

- the Web Interface's Scenario Builder, which is used for creating, loading and running scenarios
- example procedures for creating scenarios

1-1. Scenario Builder High Level Overview

The Scenario Builder lets you create a network experience over time (either automatically or manually) by graphically combining two or more networks together.

The Scenario Builder works in two different modes; namely automatically or manually. When working automatically, the Scenario Builder is referred to as Automatic Scenario Builder. When working manually, the Scenario Builder is referred to as Manual Scenario Builder. The differences between the Automatic Scenario Builder and Manual Scenario Builder are described below:

- Automatic Scenario Builder

  The Automatic Scenario Builder lets you create a network experience over time by combining two or more networks together, which can be automatically played on a Timeline. To provide a more realistic test scenario, the networks can be optionally joined together using one of three transitions. Transitions define what happens when changing between networks, for example from a 2G to 3G network. This mode is useful when wanting to create more realistic test scenarios (albeit if they take a little more time to create compared to the simpler Manual Scenario Builder).

  The Automatic Scenario Builder page (see *Illustration 156* on page 514) is divided into two horizontal areas:

  - Workspace area, at the top of the page, where you can import networks and view the three transition types for use in your scenario. You then drag the imported networks from the Workspace area to the Timeline area to build the scenario. If necessary, you optionally drag transitions from the Workspace area between the networks in the Timeline area to build a more realistic test scenario.
  - Timeline area, at the bottom of the page, displays the scenario with each segment and the ability to make changes. When played, the timeline vertical bar moves from left-to-right to indicate the current position of the scenario.

- Manual Scenario Builder

  Compared to the more sophisticated Automatic Scenario Builder, the Manual Scenario Builder (see *Illustration 159* on page 516) has a simpler interface with only a Workspace area (i.e. no Timeline area), which lets you quickly create a simple network experience by combining (via importing) two or more networks together, that can then be manually selected and run (played).

Note:

In order for the Automatic Scenario Builder to be active, the NE-ONE must have the Automatic Scenario Builder feature enabled in the license key. If the Automatic Scenario Builder is deactivated and you would like it activated, then please contact your sales representative or Calnex sales to purchase an updated license key.

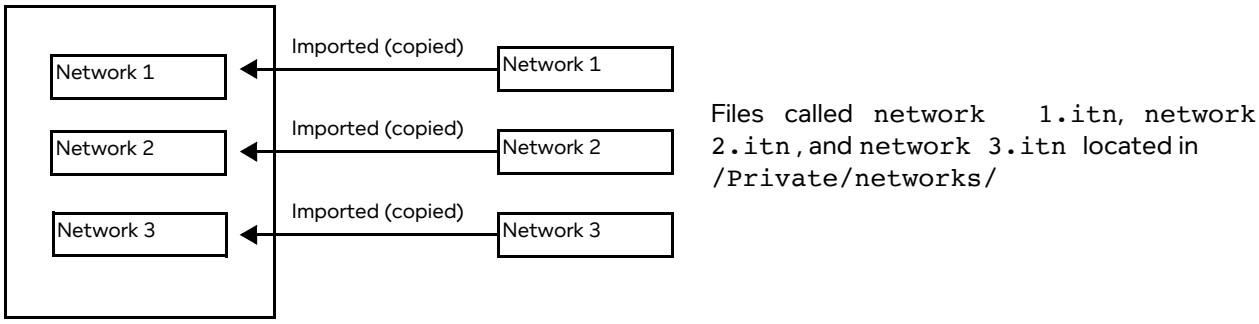
1-2. Scenario Concepts

Before creating a scenario with the either the Automatic Scenario Builder or Manual Scenario Builder, it is useful to discuss the concept of a scenario (summarized in *Illustration 152*).

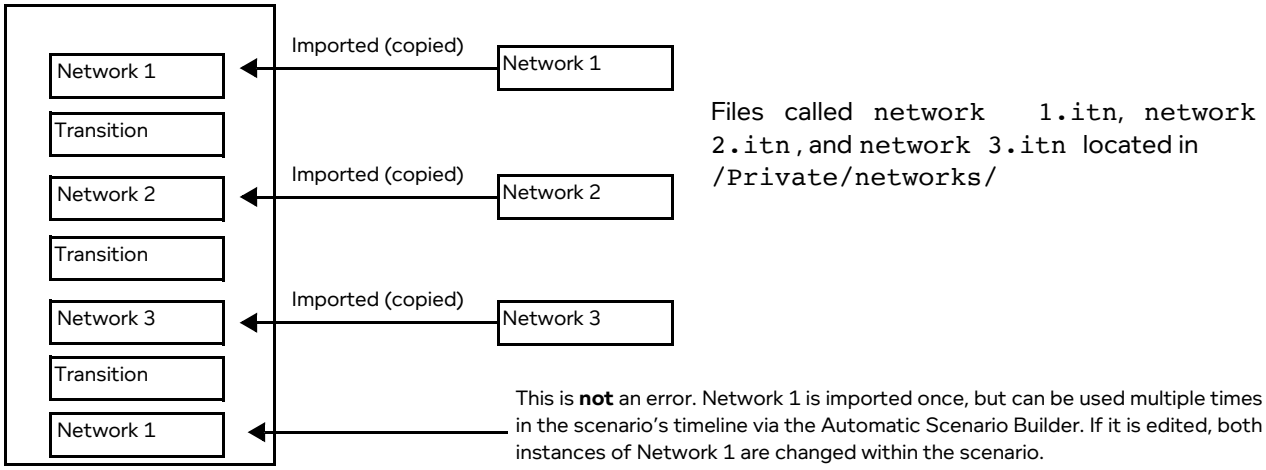
- A scenario itself is actually a network, and thus imposes all usual operational restrictions on the NE-ONE. For example, like networks, if an scenario is running on certain ports (hardware or software) those ports are in use and thus cannot be used by other networks or scenarios until the existing scenario is stopped. From a comparison perspective, you can consider a network as a "single" network, whereas a scenario is a "combination" of multiple networks (of the same type/network topology).
- Although a scenario is a network, to distinguish it from other networks its filename extension is `*.its`.
- A scenario is simply a combination of multiple networks. Each network that is combined into the scenario is done so via an import mechanism (i.e. the contents of the network's file (`*.itn`) is copied into the scenario's file (`*.its`)). Thus, the original network and its associated file (`*.itn`) remain unchanged. The networks imported into the scenario can thus be edited without changing the original network file.
- Additionally, networks imported into the scenario can also be duplicated with an scenario. Duplicating a network is extremely useful when you want to create a variant of the original imported network (e.g. make a variant of the original network with different link properties).
- A network imported into a scenario is visually represented as a network "segment". Initially the label of a network segment is inherited from the original filename of the network. Because the filename of a network imported into a scenario may no have a meaningful name, the Scenario Builder lets you change the label of the network segment to something more meaningful.
- Scenarios can be either simple or complex (see *Illustration 152*).
  - Simple scenarios are created with the Manual Scenario Builder, and simply contain two or more networks.
  - Complex scenarios are created with the Automatic Scenario Builder, and can additionally contain transitions between each of the combined networks within the scenario.

ILLUSTRATION 152 - CONCEPT OF A SCENARIO

Simple Scenario - file called `simple.its` located in `/Private/networks/`



Complex Scenario - file called `complex.its` located in `/Private/networks/`



2. PREREQUISITES

Before creating scenarios on the NE-ONE:

- an admin user must have already done the following:
  - installed and set up the NE-ONE according to the procedures in *Chapter 4, Installation and Configuration*
  - configured all the necessary port pairs, soft ports, and services according to *Chapter 5, Ports and Services Management*

Note:

The Port Manager feature and Service Manager feature are premium features. Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated.

- an admin user or non-admin user must have already created all necessary networks that they want to use within the scenarios they are going to create or modify

3. SCENARIO BUILDER PAGE

This section describes all aspects of the **Scenario Builder** page.

3-1. Launching The Scenario Builder Page

There are two modes in which you can launch the **Scenario Builder** page.

- In Multi-point mode (which supports Multi-Point networks).
  To do this, do the following:
  a. Select **Networks** in the Menu.
  b. From the **Network Wizard** page (see *Illustration 69* on page 240) that appears, click **Scenario Builder**.
  An empty **Scenario Builder** page (see *Illustration 153* on page 508) appears, and operates in a way such that it supports Multi-Point networks. Only Multi-Point type networks can be imported into the **Scenario Builder** page in this mode of operation.
- In point-to-point mode (which supports Point-to-Point network) on a particular port pair, using one of the following methods:
  Method 1 (on an Ad Hoc port pair (not possible if the ports use Port Addressing)):
  a. Select **Networks > ↔ Ad Hoc** in the Menu.
  b. From the **Choose Left Port** dialog box that appears, select the desired port (e.g. **0**) then click **OK**.
  c. From the **Choose Right Port** dialog box that appears, select the desired port (e.g. **1**) then click **OK**.
  The **Network Wizard** page associated to the selected Ad Hoc port pair appears.
  d. From the **Network Wizard** page (see *Illustration 69* on page 240) that appears, click **Scenario Builder**.
  An empty **Scenario Builder** page (see *Illustration 153* on page 508) appears, and operates in a way such that it supports Point-to-Point networks on the Ad Hoc port pair you had selected. Only Point-to-Point type networks can be imported into the **Scenario Builder** page in this mode of operation.
  Method 2 (on a favorited (starred), pre-defined port pair):
  a. Select **Networks > ↔ <Port Pair Name>**, where <Port Pair Name> is the name of the pre-defined port pair (e.g. **P0&P1**) that you want to select.
  The **Port Pair Network Wizard** page associated to the selected pre-defined port pair appears.
  b. From the **Port Pair Network Wizard** page (see *Illustration 70* on page 242) that appears, click **Scenario Builder**.
  An empty **Scenario Builder** page (see *Illustration 153* on page 508) appears, and operates in a way such that it supports Point-to-Point networks on the pre-defined port pair you had selected. Only Point-to-Point type network can be imported into the **Scenario Builder** page in this mode of operation.
  Method 3 (on a non-favorited (non-starred), pre-defined port pair):
  a. Select **Networks > ↔ All Port Pairs**.
  The **Port Pairs** page (see *Example Port Pairs page* on page 157) appears.
  b. From the **Port Pairs** page that appears, click on the **<Port Pair Name>** tile where <Port Pair Name> is the name of the pre-defined port pair (e.g. **P0&P1**) that you want to select.

The **Port Pair Network Wizard** page associated to the selected pre-defined port pair appears.

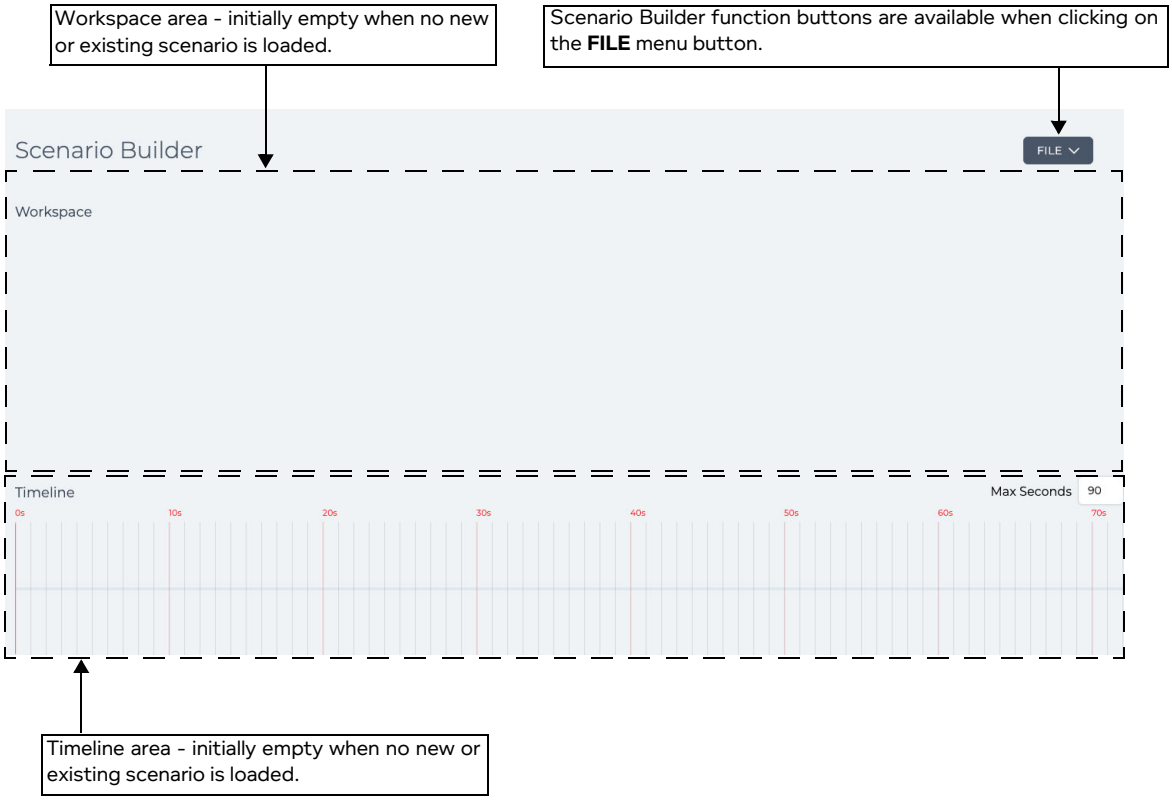
c. From the **Port Pair Network Wizard** page (see *Illustration 70* on page 242) that appears, click **Scenario Builder**.

An empty **Scenario Builder** page (see *Illustration 153* on page 508) appears, and operates in a way such that it supports Point-to-Point networks on the pre-defined port pair you had selected. Only point-to-point type networks can be imported into the **Scenario Builder** page in this mode of operation.

3-2. The Scenario Builder Pages

When the Scenario Builder is initially launched (according to one of the ways described in *Launching The Scenario Builder Page* on page 506), an empty **Scenario Builder** page initially appears.

ILLUSTRATION 153 - EMPTY SCENARIO BUILDER PAGE



The empty **Scenario Builder** page contains only contains the **FILE** menu button. The **FILE** menu button contains the following menu items (described in *Table 62*):

- **New**
- **Load**
- **Save**
- **Save as**
- **Description**
- **Find in file browser**
- **Close**

Once a scenario is loaded (either new via selecting **FILE > New** or **FILE > Load**), the **Scenario Builder** page becomes populated (i.e. no longer empty), and contains additional Scenario Builder function buttons (see *Table 62* for a description), related to creating/editing a scenario.

Additionally, the type of Scenario Builder page (i.e. automatic or manual) that appears, depends on the type of Scenario Builder mode that was loaded (via selecting **FILE > Load**) or chosen (via selecting **FILE > New**).

- Examples of the Automatic Scenario Builder pages are shown and described in *Section 3-2-1*, *Automatic Scenario Builder Pages* on page 512.
- Examples of the Manual Scenario Builder pages are shown and described in *Section 3-2-2*, *Manual Scenario Builder Pages* on page 515.

TABLE 62 - SCENARIO BUILDER PAGE ELEMENTS

Populated Scenario Builder Page Element	Description
New menu item (located in the **FILE** menu button)	Selecting this menu item from the **FILE** menu button launches a series of dialog boxes (i.e. **Scenario Name** and **Scenario Type**) letting you define the name of a new scenario and select the type of Scenario Builder mode (automatic or manual). Once a scenario name and scenario mode are defined, the new (empty) scenario loads into the Workspace area and is ready for having networks imported into it. The Scenario Builder function buttons that are visible change and the additional buttons that are available are associated with creating/editing the loaded scenario. For more information on creating scenarios, see *Creating Scenarios* on page 517. **Note:** If a new scenario is created from an already open scenario that is on a port pair, the new scenario will be assigned to the same port pair for the current Scenario Builder session.
Load menu item (located in the **FILE** menu button)	Selecting this menu item from the **FILE** menu button opens a **Choose a scenario file** dialog box, letting you choose an existing scenario (`*.its`) file to load into the Workspace area. Once an existing scenario is loaded into the workspace area, it is ready for being played or further edited (e.g. having additional networks imported into it and added to its Timeline). The Scenario Builder function buttons that are visible change and the additional buttons that are available are associated with creating/editing the loaded scenario. For more information on creating scenarios, see *Creating Scenarios* on page 517.
Save menu item (located in the **FILE** menu button)	Selecting this menu item from the **FILE** menu button saves the scenario within your `/Private/networks` directory on the NE-ONE. The filename of the scenario is of the format `<scenario name>.its`, where <scenario name> was the scenario name specified in the **Scenario Name** dialog box at the time that the scenario was created.
Save As menu item (located in the **FILE** menu button)	Selecting this menu item from the **FILE** menu button invokes a dialog box allowing to save the scenario within your `/Private/networks` directory on the NE-ONE with a different file name. The filename of the scenario is of the format `<scenario name>.its`, where <scenario name> was the scenario name specified in the dialog box.
FILE > Description menu option	Selecting this option from the **FILE** drop-down menu opens a dialog box with a free field entry letting you write a description of the scenario, and how it is configured and to be used. Since your scenario can be complicated and shared with other users, this dialog box lets you describe important items that need to be remembered and communicate with other users.
Find in File Browser menu item (located in the **FILE** menu button)	This is grayed out until the scenario has been saved. Selecting this option from the **FILE** drop-down menu opens the File Browser with the `.its` file of the scenario selected.
Close menu item (located in the **FILE** menu button)	Selecting this menu item from the **FILE** menu button invokes a confirmation dialog box, which upon clicking **OK** will close the currently open scenario.

Populated Scenario Builder Page Element	Description
▷ **PLAY** button or ☐ **STOP** button (only visible in the Automatic Scenario Builder)	The state of this button varies according to whether or not the scenario is running. When the scenario is not running, a ▷ **PLAY** button is present, and the status icon for the network in the tray is ✎. Clicking on the ▷ **PLAY** button results in: • running the scenario • changing the scenario status icon to the play ⏵ symbol • changing the button state to ☐ **STOP** When the scenario is running, a ☐ **STOP** button is present, and the status icon for the scenario in the tray is ⏵. Clicking on the ☐ **STOP** button results in: • stopping the scenario • changing the scenario status icon to the edit ✎ symbol • changing the button state to ▷ **PLAY**
⏮ button, ⏪ button and ⏩ button (only visible in the Automatic Scenario Builder when the scenario is playing)	The visibility of these buttons vary according to whether or not the scenario is running. If the scenario is running (playing), these buttons are visible. If the scenario is not running, these buttons are not visible. • clicking the ⏮ button returns to playing the scenario from the start of the Timeline (i.e. 0 seconds) • clicking the ⏪ button jumps to playing the scenario from the start of the current segment (network or transition) • clicking the ⏩ button jumps to playing the scenario from the end of the current segment (network or transition)
IMPORT button	Clicking this button opens a dialog box letting you select a network to import into the Workspace area. **Note:** If the Scenario Builder was launched in multi-point mode from the **Network Wizard** page, then only Multi-Point networks can be imported. This is normal as no port pair would have been selected leading up to launching the Scenario Builder. **Note:** If the Scenario Builder was launched in point-to-point mode from either the **Port Pair Network Wizard** page or **Port Pairs** page, then only point-to-point networks can be imported. This is normal as a port pair would have been selected leading up to launching the Scenario Builder.
CLEAR WORKSPACE button or **Clear Workspace** menu item	Automatic Scenarios: Selecting this menu item from the **CLEAR** menu button removes any of the imported networks from the workspace area. Manual Scenarios: Clicking this button removes any of the imported networks from the workspace area.
Clear Timeline menu item	Selecting this menu item from the **CLEAR** menu button removes any of the networks and transitions that were placed into the Timeline area.

Populated Scenario Builder Page Element	Description	
Workspace area	The way in which the Workspace operates depends on the Scenario Builder mode. If the Manual Scenario Builder is being used, this area only contains the imported networks in the order (from left to right) in which they were imported. The order cannot be changed. If the Automatic Scenario Builder is being used, this area contains imported networks and three transition types, that act as "segments" which can be dragged into the Timeline area. The following transition types are available:	
		**Graduating:** This transition changes all network parameters gradually between the values of the segment before and the segment after it. Changes are made every 0.1 seconds. Example: If loss in the segment before is 80% and loss in the next segment is 20%, then during the transition the loss would be gradually reduced from 80% to 20% every 0.1 seconds. If a gradual change cannot be calculated e.g. due to a change of algorithm or a link being enabled, or disabled then the change to that parameter is made at the end of the transition time, not gradually.
		**Variable:** This transition changes all network parameters variably (in a random manner) between the values of the segment before and the segment after it. Changes are made every 0.1 seconds. Example: If loss in the segment before is 80% and loss in the next segment is 20%, then during the transition the loss would take a different random value between 80% to 20% every 0.1 seconds. If a variable change cannot be calculated e.g. due to a change of algorithm or a link being enabled, or disabled then the change to that parameter is made at the end of the transition time, not variably.
		**Outage:** This transition creates an outage as follows: In the first 1/4 of the transition the loss is gradually increased to 100% from the value in the segment before. In the middle 1/2 there is 100% loss. In the last 1/4 the loss is changed gradually from 100% to the value in the next segment. Changes are made every 0.1 seconds. Example: If loss in the segment before is 80% and loss in the next segment is 20% and the transition was 20 seconds long, then during the transition the loss would begin by going from 80% to 100% changing every 0.1 second for the first 5 seconds. Loss would then remain at 100% for 10 seconds. Then loss would change from 100% to 20% in the final 5 seconds in 0.1 second increments. If a variable change cannot be calculated in the first 1/4 or last 1/4 of the transition e.g. due to a change of algorithm or a link being enabled, or disabled then the change to that parameter is made at the end of the transition time, not variably.

Populated Scenario Builder Page Element	Description
Timeline area (only available in the Automatic Scenario Builder)	This area is initially empty for a new scenario. This area is used to organise a Timeline of different networks, optionally separated by transitions. After you have imported all the required networks in to the Workspace area, drag them on to the Timeline in the order you would like to play them. Optionally, you can also drag one of three available transition segments between each of the networks. **Note:** If you try to drag a second transition segment between the same two networks, it will not remain. This is normal as only one transition can existing between each network. Do not worry if you drag the networks and transitions in the wrong order as you can reorder them by simply clicking on them and moving them to the correct order within the Timeline. When you drag an segment (i.e. either network or a transition) into the Timeline, its default duration is 10 seconds. To change the duration of the segment, place the mouse over the right edge of the segment to reveal a cross. Once the cross appears, click on the mouse and drag the right edge of the segment in the appropriate direction to increase or decrease its duration.
Max Seconds field (only available in the Automatic Scenario Builder)	Defines the maximum number of seconds that are displayed on the Timeline.

3-2-1. Automatic Scenario Builder Pages

The following illustrations are associated with the Automatic Scenario Builder:

- *Illustration 154* shows an example of a populated **Scenario Builder** page based on a new scenario (i.e. when no networks have yet been imported into the loaded scenario), and where the Automatic type of Scenario Builder mode was chosen.
- *Illustration 155* shows an example of a populated **Scenario Builder** page based on either a loaded Automatic scenario (i.e. a loaded scenario which contains imported networks) or a new Automatic scenario which has had some networks imported into it.
- *Illustration 156* shows an example of a populated **Scenario Builder** page based on either a loaded Automatic scenario (i.e. a loaded scenario which contains imported networks) or a new Automatic scenario which has had some networks imported into it, and with some segments (i.e. networks and transitions) organized (dragged) in the Timeline area.

ILLUSTRATION 154 - POPULATED AUTOMATIC SCENARIO BUILDER (NO IMPORTED NETWORKS)

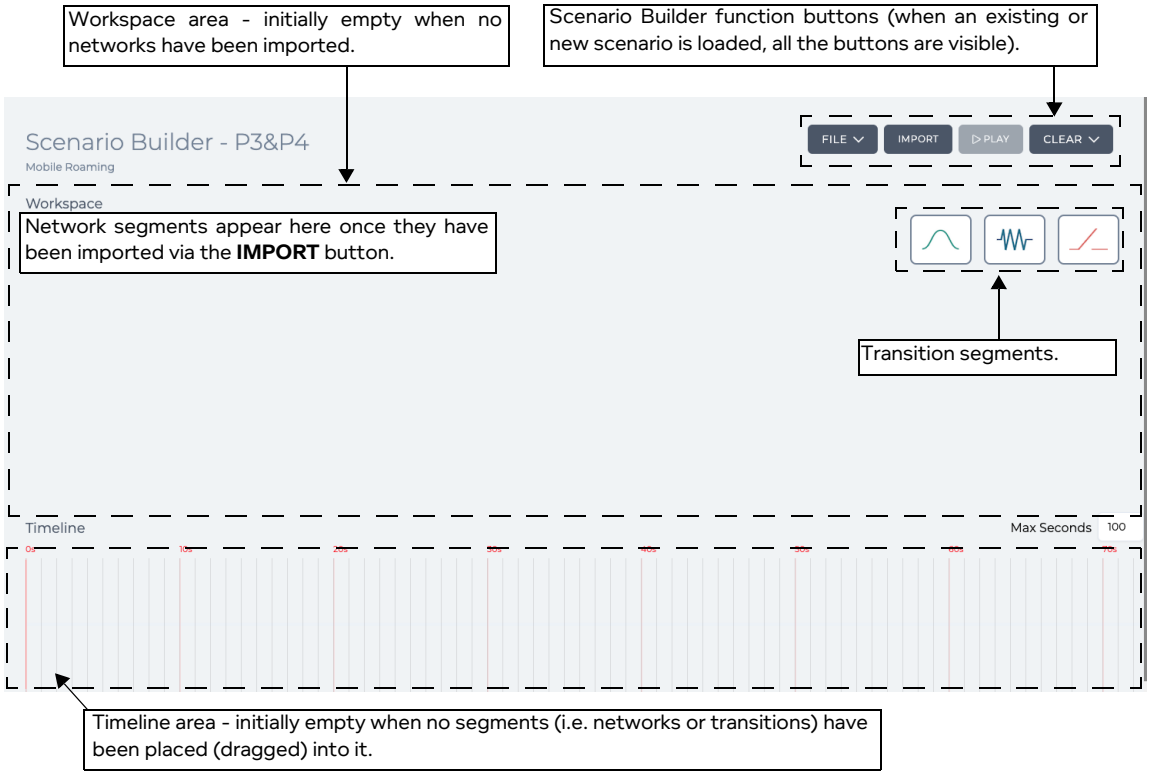


ILLUSTRATION 155 - POPULATED AUTOMATIC SCENARIO BUILDER (WITH IMPORTED NETWORKS)

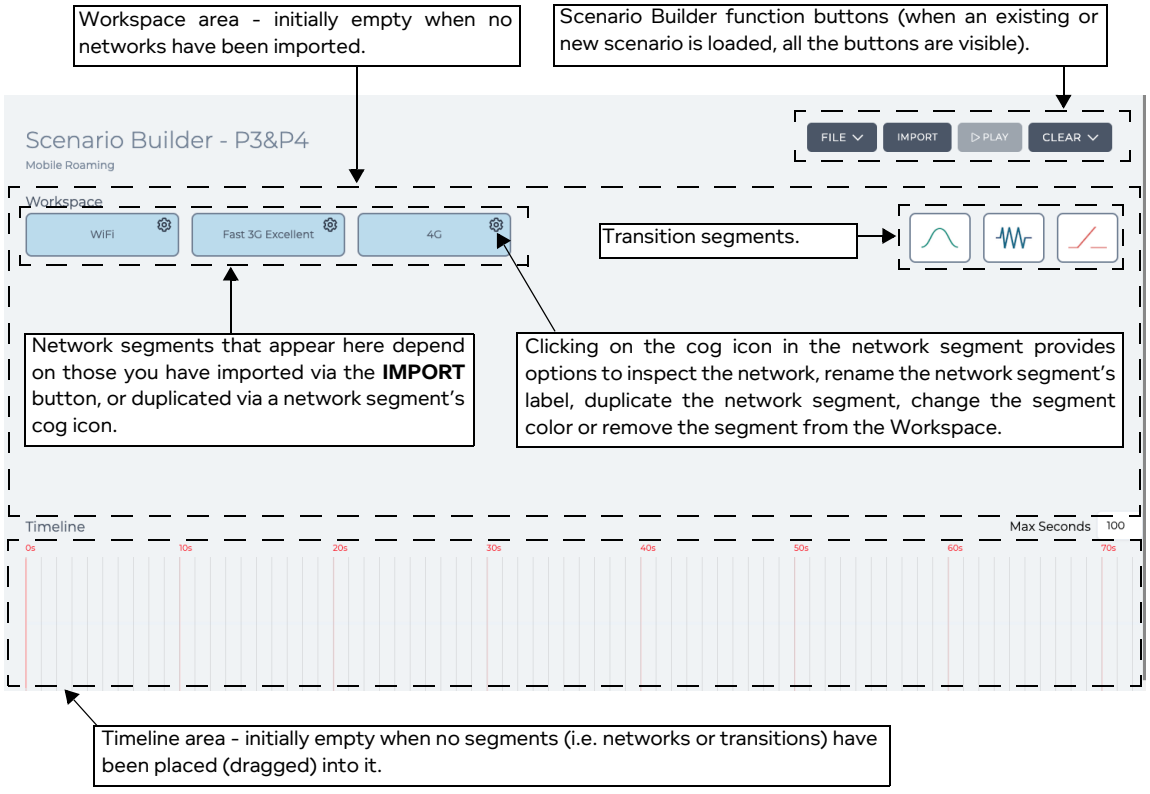
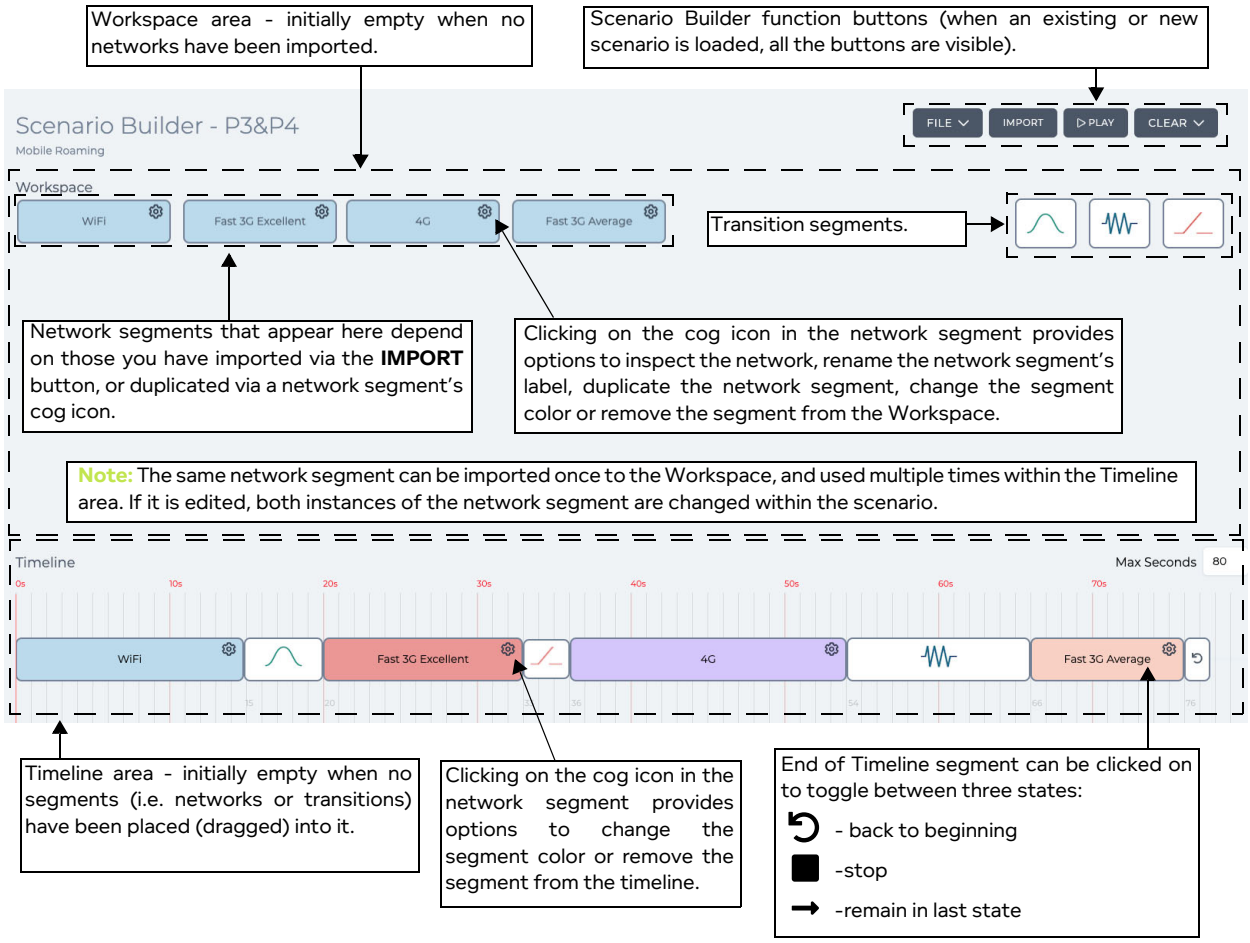


ILLUSTRATION 156 - POPULATED AUTOMATIC SCENARIO BUILDER (WITH A DEFINED TIMELINE)



3-2-1-1. Network Segment Cog Menu (for Automatic Scenarios)

Each network segment contains a cog icon. Clicking on the cog icon opens a menu with a list of menu items. The list of menu items that appear depend on whether the network segment is located in the Workspace area or Timeline area of the automatic scenario.

- If the network segment is located in the Workspace area, the cog icon contains the following menu items, related to the management of network segments within the Workspace area:
  - **Inspect** - selecting this opens the network for inspection. This this opens the network for inspection (i.e. viewing only, and cannot be modified) with an **OK** button. Clicking on the **OK** button of the inspected network returns you to the scenario.
  - **Duplicate** - selecting this makes a copy of the imported network in the Workspace area, letting you create a variant of an existing network segment. Typically you use this when you want to make a small change to an existing network for use within the Scenario Builder. For example, you might have initially imported a 3G network with the link properties "Fast" sub-type and "Excellent" link quality, and create a variant of that 3G network with the link properties "Fast" sub-type and "Average" link quality.
  - **Rename** - Selecting this menu item invokes an **Enter text name** dialog box, which lets you define the label of the network segment in the Timeline area. When you initially import a network into the Scenario Builder's Workspace area, the label given to scenario segment is inherited from the filename of the network that was imported (e.g. `3G.itn`). Typically, you use this function to rename the label of a network segment to a more meaningful name (e.g. `Fast 3G –`

`Excellent`).

- **Change Color** - Selecting this menu item invokes a dialog box with a color palette allowing to choose another color for the network segment in the Workspace area.

- If the network segment is located in the Timeline area, the cog icon contains the following menu items, related to the network segment Timeline related functions:
  - **Remove** - Selecting this removes the network segment from the Timeline area.
  - **Change Color** - Selecting this menu item invokes a dialog box with a color palette allowing to choose another color for the network segment in the Timeline area.

    Note: This color overrides the original color inherited from the network segment located in the Workspace area. The color of the network segment in the Workspace area remains unchanged.

3-2-2. Manual Scenario Builder Pages

The following illustrations are associated with the Manual Scenario Builder:

- *Illustration 157* shows an example of a populated **Scenario Builder** page based on a new scenario (i.e. when no networks have yet been imported into the loaded scenario), and where the Manual type of Scenario Builder mode was chosen.
- *Illustration 158* shows an example of a populated **Scenario Builder** page based on either a loaded Manual scenario (i.e. a loaded scenario which contains imported networks) or a new Manual scenario which has had some networks imported into it, and where the manually chosen network within the Manual scenario is not running (playing).
- *Illustration 159* shows an example of a populated **Scenario Builder** page based on either a loaded Manual scenario (i.e. a loaded scenario which contains imported networks) or a new Manual scenario which has had some networks imported into it, and where the manually chosen network within the Manual scenario is running (playing).

ILLUSTRATION 157 - POPULATED MANUAL SCENARIO BUILDER (NO IMPORTED NETWORKS)

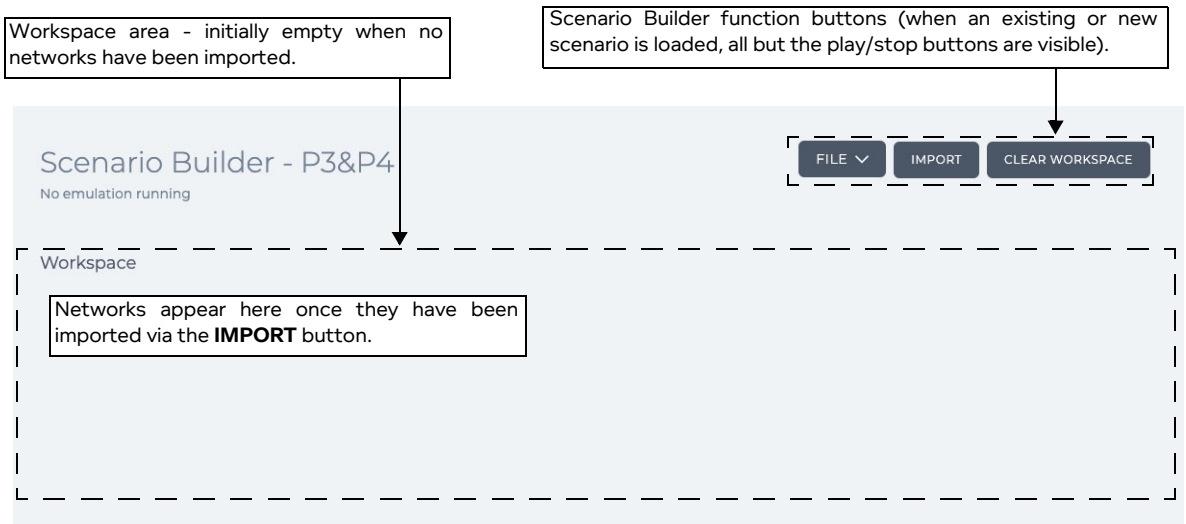


ILLUSTRATION 158 - POPULATED MANUAL SCENARIO BUILDER (WITH IMPORTED NETWORKS, NOT PLAYING)

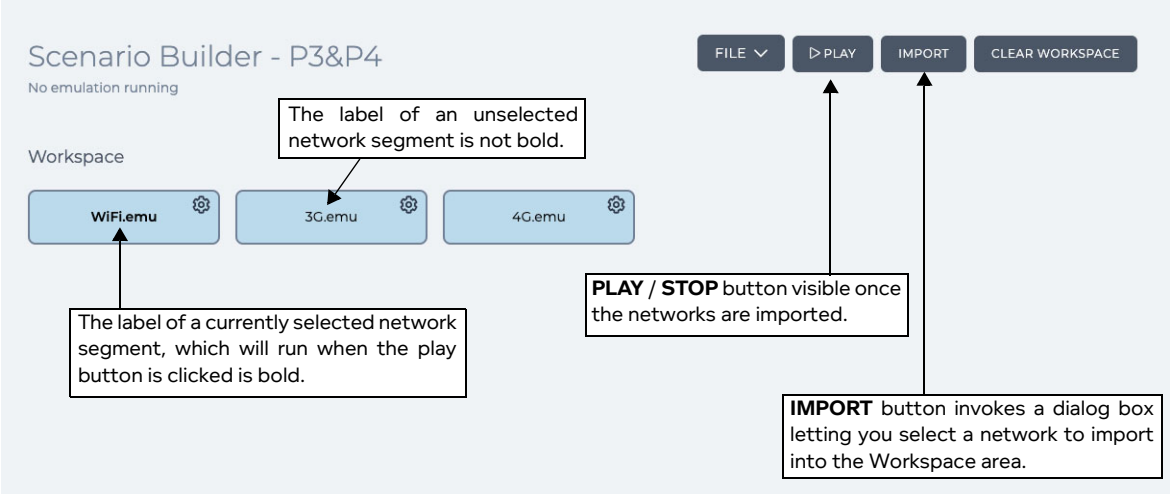
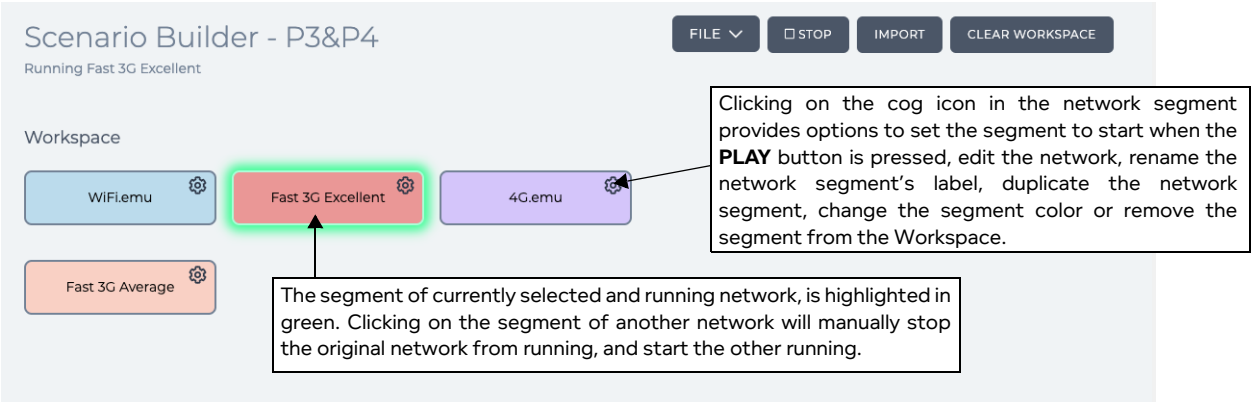


ILLUSTRATION 159 - POPULATED MANUAL SCENARIO BUILDER (WITH IMPORTED NETWORKS, PLAYING)



3-2-2-1. Network Segment Cog Menu (for Manual Scenarios)

Each network segment contains a cog icon. Clicking on the cog icon opens a menu with a list of the following menu items:

- **Set to start** - selecting this opens sets the network segment to start when the **PLAY** button is pressed.
- **Edit** - selecting this opens the network for editing. Any changes you make to the network segment from within the Workspace area are reflected into the network segment located in the Timeline area.
- **Rename** - Selecting this menu item invokes an **Enter text name** dialog box, which lets you define the label of the network segment in the Timeline area. When you initially import a network into the Scenario Builder's Workspace area, the label given to scenario segment is inherited from the filename of the network that was imported (e.g. `3G.itn`). Typically, you use this function to rename the label of a network segment to a more meaningful name (e.g. `Fast 3G – Excellent`).
- **Duplicate** - selecting this makes a copy of the imported network in the Workspace area, letting you create a variant of an existing network segment. Typically you use this when you want to make a small change to an existing network for use within the Scenario Builder. For example, you might have initially imported a 3G network with the link properties "Fast" sub-type and "Excellent" link quality, and create a variant of that 3G network with the link properties "Fast" sub-type and "Average" link

quality.

- **Remove** - Selecting this removes the network segment from the Timeline area.
- **Change Color** - Selecting this menu item invokes a dialog box with a color palette allowing to choose another color for the network segment in the Workspace area.

4. CREATING SCENARIOS

Use one of the following sections to create either an automatic scenario or manual scenario.

Note:

If creating a scenario on an NE-ONE Desktop which has an LCD panel, that scenario can optionally be made accessible from the LCD panel. In order for the scenario to be accessible to the LCD panel you must use the File Browser to copy the scenario from your `/Private/networks` directory to the `/Public/networks` directory. Then you must request an admin type user to copy the scenario from the `/Public/networks` directory to the `/Library/networks/LCD` directory. For more information, see *Making Networks and Scenarios Accessible to the LCD Panel* on page 596 in *Chapter 13*, *The File Browser*.

4-1. Creating Automatic Scenarios

Use the following steps to create an automatic scenario. The example steps below are for a mobile roaming scenario where someone with their mobile device leaves a cafe with WiFi, which then connects to a 3G network (fast, excellent quality link properties), followed by a 4G network, and then a variant (i.e. duplicated) of the 3G network (with medium, good quality link properties) where they remain indefinitely.

1. Ensure that all the networks that you want in the scenario have already been created. In our example, three networks called `WiFi.itn`, `3G.itn`, and `4G.itn` are already created, and will be imported into the Workspace. Then the imported `3G.itn` network will be duplicated, edited and modified.
2. Launch the Scenario Builder (see *Launching The Scenario Builder Page* on page 506).
3. Select **FILE > NEW**.
4. From the **Scenario Name** dialog box that appears, type an appropriate name for the scenario that you want to create, then click **OK**. The scenario name can contain alpha-numeric characters, special characters (except /, \, and *), and can include spaces. In our example, the scenario is called `Mobile Roaming`.

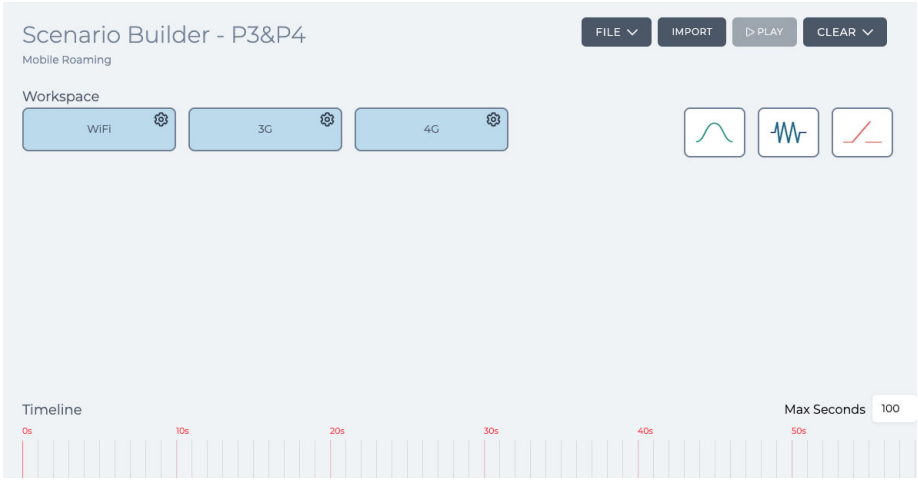
   Note:

   If you want a created scenario on an NE-ONE Desktop to be accessible via the LCD panel, consider the fact that it has two lines of 20 characters. If a scenario name exceeds 18 characters, it will appear truncated in the LCD panel.
5. From the **Scenario Type** dialog box that appears, select **Automatic**, then click **OK**.

   An unpopulated Automatic **Scenario Builder** page appears (*Illustration 154* on page 513).
6. For each of the networks that you want to import into the Workspace area, do the following:
   a. Click **IMPORT**.
   b. From the **Choose a network file** dialog box that appears, click on the network that you want to import, then click **OK**.

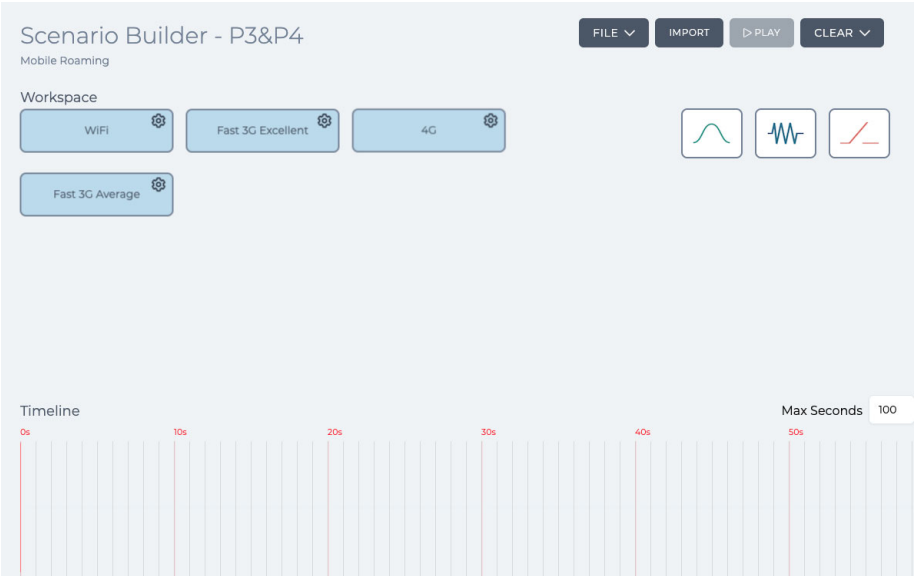
      The imported network appears in the Workspace area of the Automatic Scenario Builder. In our example, three networks called `WiFi.itn`, `3G.itn`, and `4G.itn` are imported. The `*.itn` file extension of the network imported network file is not applied to the label of the network

segment.



7. If necessary, in the Workspace area create duplicates of the imported networks so that you can create variant network segments with different link properties. To do this use the following sub-steps for each of the imported networks that you want to duplicate.
   a. On the network segment that you want to duplicate, click the cog icon, and select **Duplicate**.
      A duplicate network segment is created, and appears in the Workspace area.
   b. On the newly created duplicate network segment click the cog icon, and select **Rename**.
   c. In the **Enter text name** dialog box that appears type a meaningful description for the duplicated network segment label then click **OK**. The network segment label can contain alpha-numeric characters, special characters (except /, \, and *), and can include spaces. Due to the size of the network segments, it is recommended to use a short description not exceeding more than 20 characters (e.g. `Fast 3G Average`).
   d. On the newly created duplicate network segment click the cog icon, and select **Edit**.
      The network of the duplicate network segment appears in either a **Point To Point Designer** page or **Multi-Point Designer** page.
      In our example, you would change the properties of a 3G network so that it is Fast subtype, and Average quality.
   e. In either a **Point To Point Designer** page or **Multi-Point Designer** page, make all appropriate changes you require to create a variant of the original network. When finished, click **DONE**.

You are returned to the **Scenario Builder** page.



8. Each of the networks imported into Workspace area are represented by blue network segments with a the network's filename without the `*.itn` extension as the label. Each of the networks duplicated within Workspace area are represented by network segments with the same color of the original network segment. If necessary, optionally do the following:

   Change the network segment label, using the following sub-steps:

   a. Click the cog icon, and select **Rename**.

   b. In the **Enter text name** dialog box that appears type a meaningful description for the network segment label then click **OK**. The network segment label can contain alpha-numeric characters, special characters (except /, \, and *), and can include spaces. Due to the size of the network segments, it is recommended to use a short description not exceeding more than 20 characters (e.g. `Fast 3G Excellent`).

   Change the network segment color, using the following sub-steps:

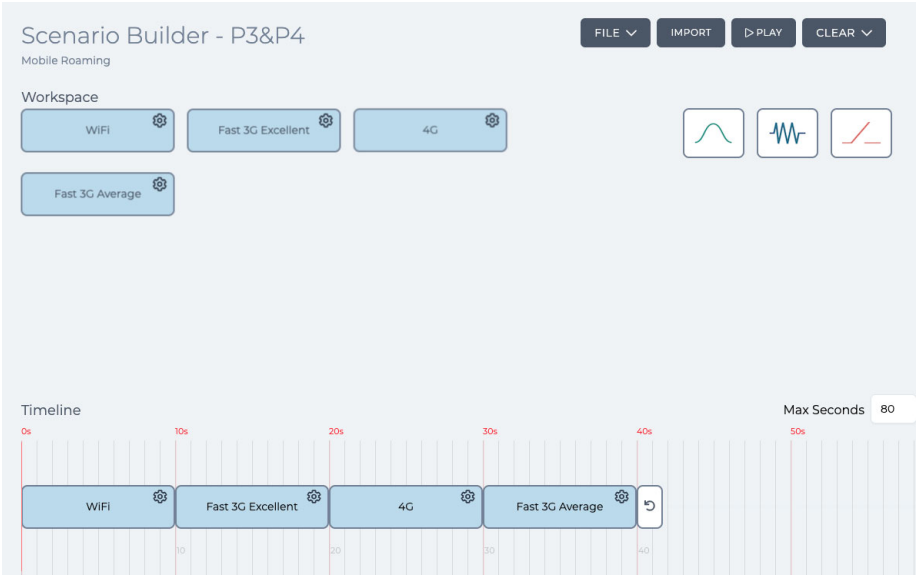
   a. Click the cog icon, and select **Change color**.

   b. In the dialog box with color palette that appears click on an appropriate color.

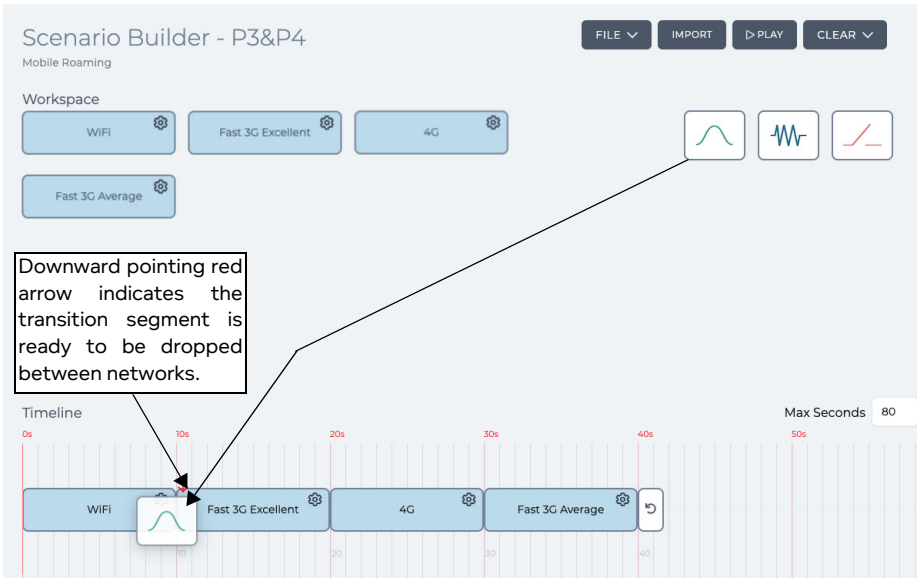
9. Organize the networks and transitions into the Timeline area as follows:

   a. For each network you want in the Timeline, click on the network segment from the Workspace area, and drag it onto the Timeline. In our example, the networks are dragged into the Timeline in

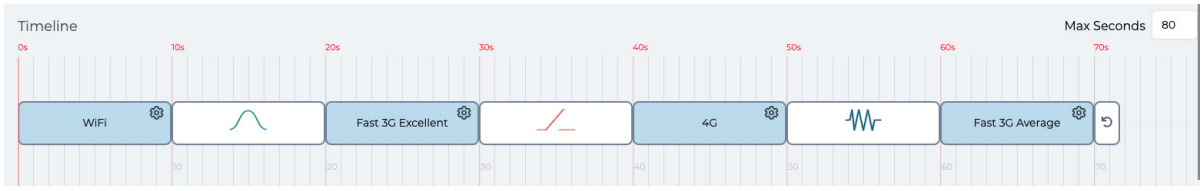
the following order: WIFi, 3G, 4G, and 3G.



b. Between each network for which you want a transition to exist, click on the appropriate transition segment, and drag it from the Workspace area between the two networks. When the transition segment is ready to be dropped between the two networks, a downward pointing red arrow appears.



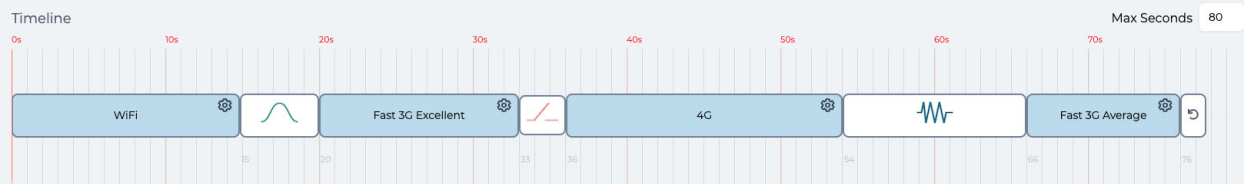
In our example, a graduating transition is placed between the WiFi network segment and the Fast 3G Excellent network segment, an outage is placed between the Fast 3G Excellent network segment and the 4G network segment, and a variable transition is placed between the 4G network and the Fast 3G Average network.



When you drag an segment (i.e. either network or a transition) into the Timeline, its default

duration is 10 seconds.

c. If necessary, change the duration for each segment (i.e. network or transition). To do this, place the mouse over the right edge of the segment to reveal a cross. Once the cross appears, click on the mouse and drag the right edge of the segment in the appropriate direction to increase or decrease its duration.



In our example, the finalized durations on the Timeline are such that the WiFi is 15 seconds, the graduating transition is 5 seconds, the Fast 3G Excellent network is 13 seconds, the outage transition is 3 seconds, the 4G network is 18 seconds, the variable transition is 12 seconds, and the Fast 3G Average network is 10 seconds.

By default, the end of Timeline segment is set to return to the beginning of the Timeline and loop the Timeline sequence.

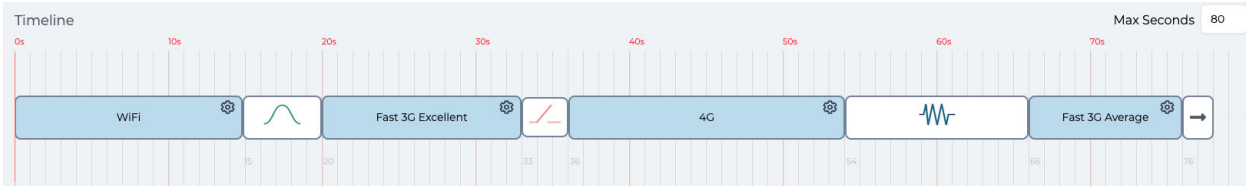
d. If necessary, change what happens once the end of Timeline is reached. To do this, keep clicking on the end of Timeline segment until the appropriate icon appears.

↺ - back to beginning (i.e. loop)

■ -stop

→ -remain in last state

In our example, we want the scenario not to loop, but remain on running the last 3G network indefinitely. In which case, keep clicking the end of Timeline segment until the icon → appears.



10. Select **FILE > SAVE** to save the scenario.

The scenario is saved with the filename `<scenario name>.its` to your `/Private/networks` directory on the NE-ONE, where <scenario name> was the name you gave to the scenario. The scenario is ready to be run (played).

4-2. Creating Manual Scenarios

Use the following steps to create an automatic scenario. The example steps below are for a mobile roaming scenario where someone with their mobile device leaves a cafe with WiFi, which then connects to a 3G network (fast, excellent quality link properties), followed by a 4G network, and then a variant (i.e. duplicated) of the 3G network (with medium, good quality link properties) where they remain indefinitely.

1. Ensure that all the networks that you want in the scenario have already been created. In our example, three networks called `WiFi.itn`, `3G.itn`, and `4G.itn` are already created, and will be imported into the Workspace. Then the imported `3G.itn` network will be duplicated, edited and modified.
2. Launch the Scenario Builder (see *Launching The Scenario Builder Page* on page 506).
3. Select **FILE > NEW**.
4. From the **Scenario Name** dialog box that appears, type an appropriate name for the scenario that

you want to create, then click **OK**. The scenario name can contain alpha-numeric characters, special characters (except /, \, and *), and can include spaces. In our example, the scenario is called `Mobile Roaming`.

Note:

If you want a created scenario on an NE-ONE Desktop to be accessible via the LCD panel, consider the fact that it has two lines of 20 characters. If a scenario name exceeds 20 characters, it will appear truncated in the LCD panel.

5. From the **Scenario Type** dialog box that appears, select **Manual**, then click **OK**.

   An unpopulated Manual **Scenario Builder** page appears (*Illustration 157* on page 515).

6. For each of the networks that you want to import into the Workspace area, do the following:
   a. Click **IMPORT**.
   b. From the **Choose a network file** dialog box that appears, click on the network that you want to import, then click **OK**.

      The imported network appears in the Workspace area of the Automatic Scenario Builder. In our example, three networks called `WiFi.itn`, `3G.itn`, and `4G.itn` are imported. The `*.itn` file extension of the network imported network file is not applied to the label of the network segment.

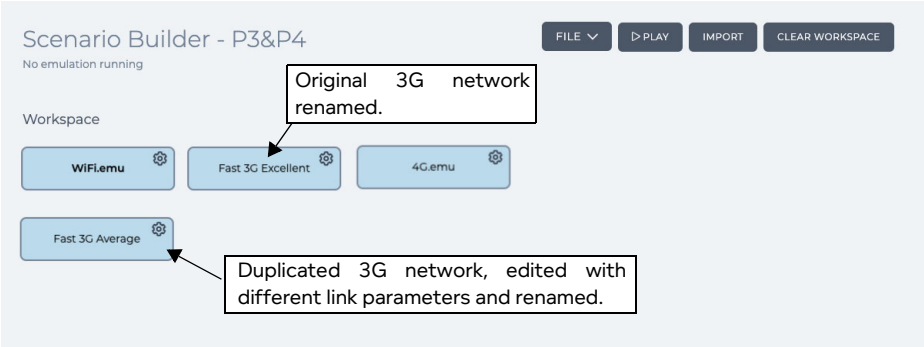
7. If necessary, in the Workspace area create duplicates of the imported networks so that you can create variant network segments with different link properties. To do this use the following sub-steps for each of the imported networks that you want to duplicate.
   a. On the network segment that you want to duplicate, click the cog icon, and select **Duplicate**.

      A duplicate network segment is created, and appears in the Workspace area.
   b. On the newly created duplicate network segment click the cog icon, and select **Rename**.
   c. In the **Enter text name** dialog box that appears type a meaningful description for the duplicated network segment label then click **OK**. The network segment label can contain alpha-numeric characters, special characters (except /, \, and *), and can include spaces. Due to the size of the network segments, it is recommended to use a short description not exceeding more than 20 characters (e.g. `Fast 3G Average`).
   d. On the newly created duplicate network segment click the cog icon, and select **Edit**.

      The network of the duplicate network segment appears in either a **Point To Point Designer** page or **Multi-Point Designer** page.

      In our example, you would change the properties of a 3G network so that it is Fast subtype, and Average quality.
   e. In either a **Point To Point Designer** page or **Multi-Point Designer** page, make all appropriate changes you require to create a variant of the original network. When finished, click **DONE**.

You are returned to the **Scenario Builder** page.



8. Each of the networks imported into Workspace area are represented by blue network segments with a the network's filename without the `*.itn` extension as the label. Each of the networks duplicated within Workspace area are represented by network segments with the same color of the original network segment. If necessary, optionally do the following:

   Change the network segment label, using the following sub-steps:

   a. Click the cog icon, and select **Rename**.

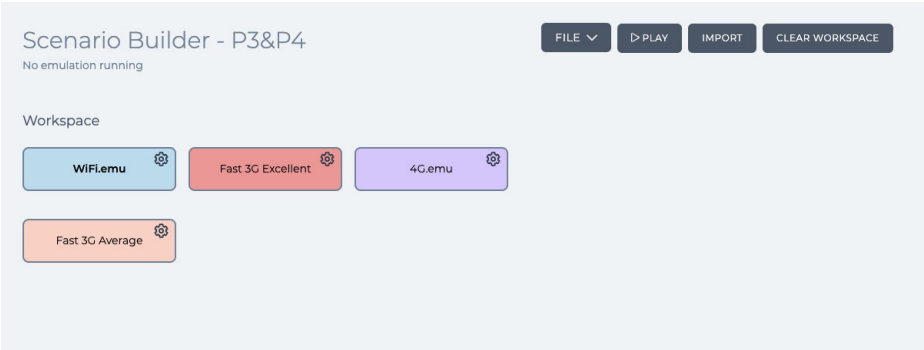
   b. In the **Enter text name** dialog box that appears type a meaningful description for the network segment label then click **OK**. The network segment label can contain alpha-numeric characters, special characters (except /, \, and *), and can include spaces. Due to the size of the network segments, it is recommended to use a short description not exceeding more than 20 characters (e.g. `Fast 3G Excellent`).

   Change the network segment color, using the following sub-steps:

   a. Click the cog icon, and select **Change color**.

   b. In the dialog box with color palette that appears click on an appropriate color.

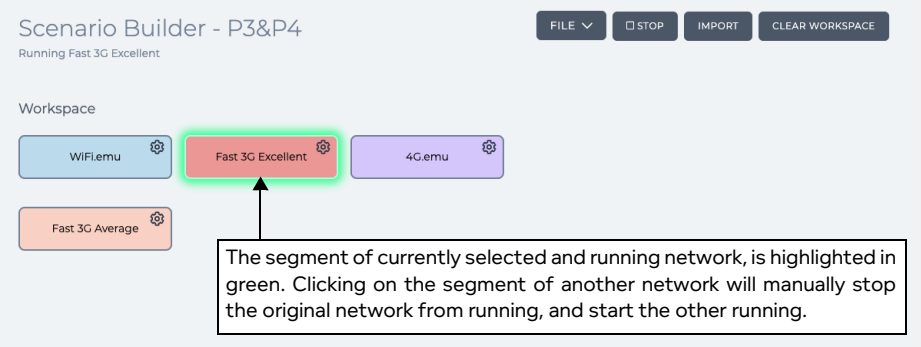
   You are returned to the **Scenario Builder** page.



9. Select **FILE > SAVE** to save the scenario.

   The scenario is saved with the filename `<scenario name>.its` to your `/Private/networks` directory on the NE-ONE, where <scenario name> was the name you gave to the scenario. The

scenario is ready to be manually run (played).



If you want to manually play the scenario, click on the network segment that you want to initially run, click the cog icon and select **Set to start**, then click the ▷ **PLAY** button. When you want to change the network that is running in the scenario, click on the other network segment.

In our example, you would initially click on the **WiFi** network segment's then cog icon and select **Set to start** click the ▷ **PLAY** the button, then after some time click the **Fast 3G Excellent** network segment, and after some more time click on the **4G** network segment, then after more time click again on the **Fast 3G Average** network.

To stop the manual scenario from running, click the ☐ **STOP** button.

5. OPENING AND PLAYING EXISTING SCENARIOS

Scenarios can be opened via two ways. Once opened, an scenario can be either edited or played.

- Via the Home Page.
- Via the File Browser. For more information, see *Opening a Scenario From the File Browser* on page 590 in *Chapter 13*, *The File Browser*.

Note:

Once a scenario is playing it is attached to the user who run it, and the ports that it is using cannot be used by any other networks or scenarios until the currently playing scenario is stopped. Currently playing scenarios are listed in the **Active** tab of the **Home** page.

Note:

You can also directly play a scenario from within the File Browser, without needing to open it. For more information, see *Directly Playing a Scenario From the File Browser* on page 592 in *Chapter 13*, *The File Browser*.

6. DELETING SCENARIOS

If a scenario is no longer needed, it can be deleted from the NE-ONE using the File Browser. Scenarios have a file name extension `*.its`, are located in your `/Private/networks` directory, and use the scenario name that you had specified for the file name. To delete a no longer required scenario, use the following steps:

1. Click **Management > ··· Platform Settings > File Browser** to launch the File Browser.
2. Navigate to the `/Private/networks` directory, and identify the scenario you want to delete by its file name.
3. Right mouse click on the scenario file (`*.its`), and select **Delete selected File/Folder** from the File Browser pop-up menu that appears.
4. From the **Confirm delete** dialog box that appears, click **OK**.

CHAPTER 12 STATISTICS, GRAPHING, REPORTING AND PACKET CAPTURING

1. INTRODUCTION

This chapter is applicable to non-admin and admin users. It describes the Web Interface and procedures related to viewing graphs, capturing packet data, and monitoring live packets for the active Packet Processing Objects (PPOs) that are on running networks.

This chapter contains the following sections:

- *Section 2*, *The Statistics Page* describes the general concepts and usage of the Web Interface's **Statistics** page.
- *Section 3*, *Launching Packet Capture on a PPO* describes from a task oriented perspective, the different ways in which you can launch the packet capture process for a PPO. The packet capture process creates a pcap file that can be used at a later time for analysis.
- *Section 4*, *Launching Live Packet Monitoring on a PPO* describes from a task oriented perspective, the different ways in which you can launch live packet monitoring for a PPO. Live packet monitoring lets you examine in real-time the packet data so that you can quickly debug your network applications.
- *Section 5*, *Launching Live Graphs on a PPO From an Active Network* describes from a task oriented perspective, the different ways in which you can launch graphs on a PPO of interest on an active network from within the **Statistics** page, **Point To Point Designer** page or **Multi-Point Designer** page.
- *Section 6*, *The Reports and Graphs Page* describes the general concepts and usage of the Web Interface's **Reports and Graphs** page, and contains the following sub-sections:
  - *Section 6-1*, *The Graphs Page* describes the general concepts and usage of the Web Interface's **Graphs** page.
  - *Section 6-3*, *The Reporting Page* describes the general concepts and usage of the Web Interface's **Reporting** page.
  - *Section 6-2*, *The Historical Statistics Pages* describes the general concepts and usage of the Web Interface's **Historical Statistics** page.

1-1. Distinction Between Network and System Packet Processing Objects

Before continuing in this chapter, it is useful to understand the concept of PPOs on the NE-ONE. PPOs can be categorized into two types, as follows:

- Network PPOs - these are PPOs that are created (i.e. nodes, and links) (typically by non-admin user) from within either a **Point To Point Designer** page or **Multi-Point Designer** page, and are associated with the created network.
- System PPOs - these are underlying system PPOs that either allow networks to be created or the system to function, and consist of the following:
  - hardware ports
  - Soft ports (defined by an admin user from within the **Port Manager** page)
  - Port containers (automatically created by the NE-ONE when an admin user creates a soft port from within the **Port Manager** page)
  - Services that run in the background (defined by an admin user from with the **Service Manager** page) and enable background tasks such as a DHCP Helper service or Default Transmission of a pre-defined port pair

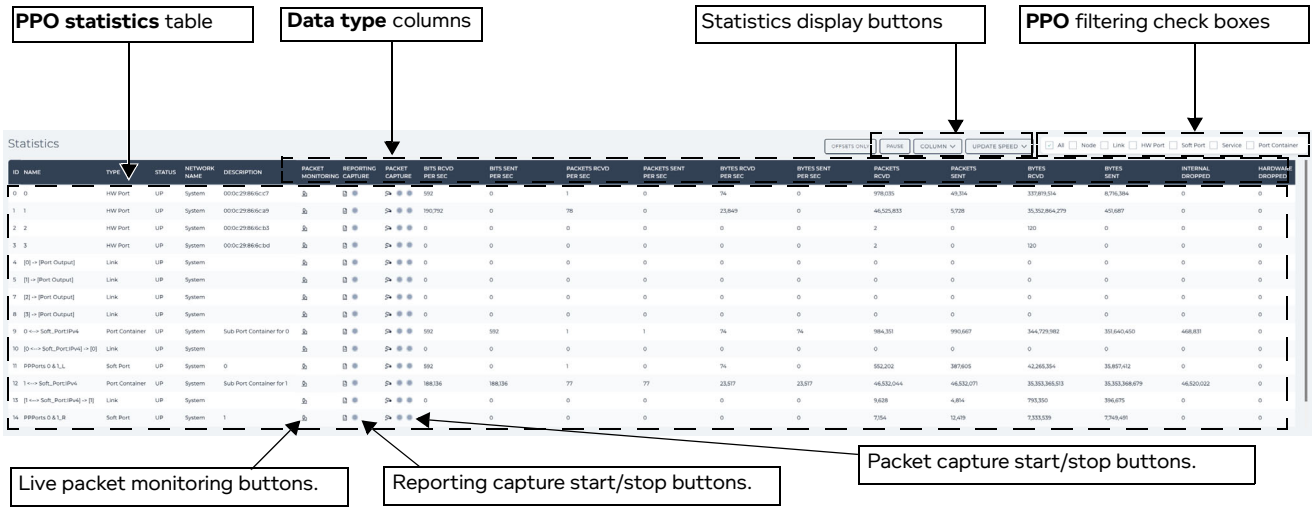
Note:
The Port Manager feature and Service Manager feature are premium features. Depending on your license, the Port Manager feature and Service Manager feature may either be activated or deactivated.

Note:
When a port pair has Port Addressing enabled, the NE-ONE automatically creates a set of IPv4 soft ports, links and port containers for that port pair. Those associated soft ports, links, and port containers associated with the port pair appear in the **Statistics** page. For more information, see *Table 28* on page 168 in *Chapter 5*, *Ports and Services Management*).

2. THE STATISTICS PAGE

The **Statistics** page (see *Illustration 160*) appears after clicking **Statistics** from the Menu.

ILLUSTRATION 160 - STATISTICS PAGE



The **Statistics** page is the central location that lists the statistics of the following PPOs from where you launch packet capture or data graphing for a PPO:

- network PPOs (i.e. links and nodes) associated with any currently active (playing) networks
- system PPOs (i.e. hardware port, soft port, port container, or service)

Note:
Packet capture and data graphing can also be launched for a network PPO directly within a network via either a **Point To Point Designer** page or **Multi-Point Designer** page, either for a specific node when editing a node (in the **Edit node** panel) or for a specific link when opening the **Link** menu for the link. For more information, see *Launching Packet Capture on a PPO* on page 532 and *Launching Live Graphs on a PPO From an Active Network* on page 550.

Note:
Services are not associated with an active network created by an end user. Services are background tasks (i.e. default transmission of data between ports or relaying of DHCP requests) that are put in place by an admin user. If defined and enabled by an admin user, a service will always run in the background and is independent of any user created networks.

Note:
The Port Manager feature is a premium feature. Depending on your license, the Port Manager feature may either be activated or deactivated. If the Port Manager feature is deactivated, the **Soft Port** and **Port Container** PPO filtering check boxes are still available, some soft port and port container PPOs may be listed in the **Statistics** page. This is normal.
For example, when a port pair has Port Addressing enabled (see *Configuring Port Addressing* on page 167 in *Chapter 5, Ports and Services Management*), the NE-ONE creates a soft port and port container for that port pair. The soft ports and port containers associated with the port pair with Port Addressing activated will appear in the **Statistics** page.

Note:
Even if there are no active (playing) networks, the hardware ports (and their associated child soft ports) may still have live packet statistics updating in real time in the **Statistics** page. This is normal, and occurs when the NE-ONE is connected to your local/corporate/virtual network and is associated to the traffic from your local/corporate/virtual network passes through the NE-ONE.

The **Statistics** page contains:

- a set of check boxes letting you filter which PPOs are displayed in the PPO statistics table
- the following statistics display buttons:
  - **OFFSETS ONLY** button - clicking this button resets each of the statistics back to zero so that you can view their offsets (i.e observe the changes in statistics after clicking this button). Each time you click this button, the statistics will reset to zero while you remain on the **Statistics** page.

  Note:
  Clicking this button has no impact on the statistics that have accumulated over the time the network has been running. If you leave the **Statistics** page, then return to the **Statistics** page the total accumulated statistics appear.
  - **PAUSE** button - clicking this button toggles between pausing and un-pausing the statistics updating. When paused, the statistics stop updating until the **PAUSE** button is clicked again.
  - **COLUMN** menu button - clicking this menu button reveals a set of check boxes corresponding to each of the column headings, and let you to show/hide the columns within the **Statistics** page. By default, all the check boxes are ticked. You can enable/disable the different check boxes to show/hide the columns according to your requirements.

  Note:
  You cannot choose to show/hide the **ID** and **Name** columns as they are always visible.
  - **UPDATE SPEED** menu button - clicking this menu button reveals a drop-down menu with different statistics update refresh rates (**Every half second**, **Every second**, **Every 3 seconds**, **Every 5 seconds**) letting you select the refresh rate of the statistics. The default refresh rate when you arrive on the **Statistics** page is every second.
- a PPO statistics table with the following columns that list information for each of the port types that you filtered to be displayed:
  - **ID** : displays the unique identifier of the PPO. This is an incremental integer in the order that any PPOs associated with soft ports and services are created. The hardware ports that already initially exist have the unique identifier 0, 1, 2, 3, 4, etc. PPOs associated with created soft ports and services are incrementally numbered with integers greater than those already given to the hardware ports.
  - **NAME** : displays the name of the PPO. Hardware ports are numbered 0, 1, 2, 3, 4, etc.
  - **TYPE** : displays the PPO type.
  - **STATUS** : displays the PPO status (up or down). Up if the PPO is connected to a valid device, switch, etc. Down if the PPO is not connected.
  - **NETWORK NAME** : displays the that was given to the network or scenario (this is `System` for other PPOs).
  - **DESCRIPTION** : displays different types of descriptive information according to the PPO type (see *Table 63*).

TABLE 63 - DESCRIPTION FORMATS PER PPO TYPE

PPO Type	Description Format
HW Port	MAC Address of the hardware port
LINK	Name of node the link is connected to
Node	Name of the node
Port Container	Inherits the name of the parent port it is assigned to (e.g. if an IPv4 service is created on hardware port 0, `Sub Port Container for 0` is displayed.

PPO Type	Description Format
Soft Port	The name of the parent port that the soft belongs to. For example: • If the parent port is hardware port 0, **0** is displayed. • If the soft port is created at the top level (i.e. does not belong to a parent port, `Top Level` is displayed). • If the soft port belongs to another parent soft port, the name of the parent soft port is displayed.
Service	Displays the service type (e.g. `DHCP Helper` or `Background Service`).

- **LIVE PACKET MONITORING** : This column contains microscope icons for each PPO type. Clicking on a microscope opens a **Live Packets (<PPO Name>)** window (*Illustration 163* **on page 542**) from where you can inspect the packet data in real-time for the associated PPO.
- **REPORTING CAPTURE** : This column contains indicator icons for each PPO type. Clicking on an indicator icon toggles the between the enabling reporting capture and disabling reporting capture. By default reporting capture is not enabled for a PPO (and the indicator icon is gray).
  When you click on an indicator icon to enable reporting capture, it initially flashes amber indicating the request to enable reporting capture has been sent to the system. Once the request is accepted by the system the indicator icon turns to a flashing red, indicating that reporting capture is currently active on the PPO.
  When you click on an indicator icon to disable reporting capture, it initially flashes amber indicating the request to disable reporting capture has been sent to the system. Once the request is accepted by the system the indicator icon turns gray, indicating that reporting capture is currently inactive on the PPO.
- **PACKET CAPTURE** : This column contains two indicator icons for each PPO type. The left hand side indicator icon corresponds to packet capture data before traversing the PPO (i.e. before impairment). The right hand side indicator icon corresponds to packet capture data after traversing the PPO (i.e. after impairment). Clicking on an indicator icon toggles the between the enabling packet capture and disabling packet capture. By default packet capture is not enabled for a PPO (and the indicator icon is gray).
- **BITS RCVD PER SEC** : The rate of bytes received per second from the PPO in bits per second (bps).
- **BITS SENT PER SEC** : The rate of bits sent per second from the PPO in bits per second (bps).
- **PACKETS RCVD PER SEC** : The rate of packets received per second from the PPO in bits per second (bps).
- **PACKETS SENT PER SEC** : The rate of packets sent per second from the PPO in bits per second (bps).
- **BYTES RCVD PER SEC** : The rate of bytes received per second from the PPO in bits per second (bps).
- **BYTES SENT PER SEC** : The rate of bytes sent per second from the PPO in bits per second (bps).
- **PACKETS RCVD** : Total packets received by the port since the statistics counters have been reset, as summarized below.

PPO Type	Packets received data
HW Port	Total packets received by the hardware port.
LINK	Total packets received by the link.
Node	Total packets received by the node.

PPO Type	Packets received data
Port Container	Total packets received by the port container.
Soft Port	Total packets received by the soft port.
Service	Total packets received by the service.

- **PACKETS SENT** : Total packets sent from the PPO since the statistics counters have been reset, as summarized below.

PPO Type	Packets sent data
HW Port	Total packets sent from the hardware port.
LINK	Total packets sent from the link.
Node	Total packets sent from the node.
Port Container	Total packets sent from the port container.
Soft Port	Total packets for from soft port.
Service	Total packets sent from the service.

- **BYTES RCVD** : Total bytes received by the PPO since the statistics counters have been reset, as summarized below.

PPO Type	Bytes received data
HW Port	Total bytes received by the hardware port.
LINK	Total bytes received by the link.
Node	Total bytes received by the node.
Port Container	Total bytes received by the port container.
Soft Port	Total bytes received by the soft port.
Service	Total bytes received by the service.

- **BYTES SENT** : Total bytes sent from the PPO since the statistics counters have been reset, as summarized below.

PPO Type	Bytes sent data
HW Port	Total bytes sent from the hardware port.
LINK	Total bytes sent from the link.
Node	Total bytes sent from the node.
Port Container	Total bytes sent from the port container.
Soft Port	Total bytes sent from the soft port.
Service	Total bytes sent from the service.

- **INTERNAL DROPPED** : Total "internal" packets dropped by the PPO since the statistics counters have been reset.
- **HARDWARE DROPPED** : Total "hardware" packets dropped by the PPO since the statistics counters have been reset.

Note:
Upon arriving to the **Statistics** page only the **All** check box is enabled.

Note:
If a PPO currently has no traffic running through it, the data displayed is zero. This is normal.

Note:

To the right of the data type columns (i.e. **BITS RCVD PER SEC**, **BITS SENT PER SEC**, **PACKETS RCVD PER SEC**, **PACKETS SENT PER SEC**, **BYTES RCVD PER SEC**, **BYTES SENT PER SEC**, **PACKETS RCVD**, **PACKETS SENT**, **BYTES RCVD**, **BYTES SENT**, **INTERNAL DROPPED**, **HARDWARE DROPPED**) is a hidden mouse over graph icon, which upon clicking will open a real-time graph that updates every second.

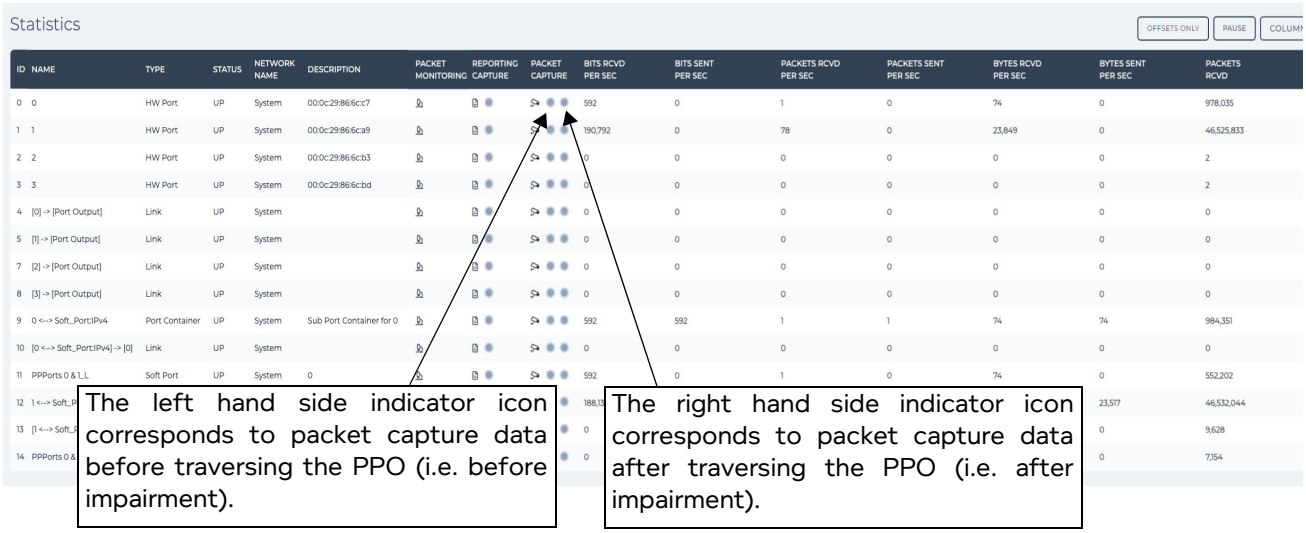
3. LAUNCHING PACKET CAPTURE ON A PPO

The NE-ONE lets you create packet capture (`*.pcap`) files for network PPOs and system PPOs for later use in external tools such as Wireshark or for use with the Packet Replay function on the NE-ONE. If you would like to examine live packet data for in-situ network application testing and debugging, you can use live packet monitoring instead (see *Launching Live Packet Monitoring on a PPO* on page 540).

- Packet capture on a network PPO is disabled by default, and can be enabled when the associated network is running.
- Packet capture on a system PPO is disabled by default, and can be enabled at any time.

The Web Interface offers you various ways to capture packets on a PPO, as follows:

- Via the **Statistics** page (which lists system PPOs and network PPOs of running networks).



  Clicking on an indicator icon toggles the between the enabling packet capture and disabling packet capture. By default packet capture is not enabled for a PPO (and the indicator icon is gray).

  When you click on an indicator icon to enable packet capture, it initially flashes amber indicating the request to enable packet capture has been sent to the system. Once the request is accepted by the system the indicator icon turns to a flashing red, indicating that packet capture is currently active on the PPO.

  When you click on an indicator icon to disable packet capture, it initially flashes amber indicating the request to disable packet capture has been sent to the system. Once the request is accepted by the system the indicator icon turns gray, indicating that packet capture is currently inactive on the PPO.

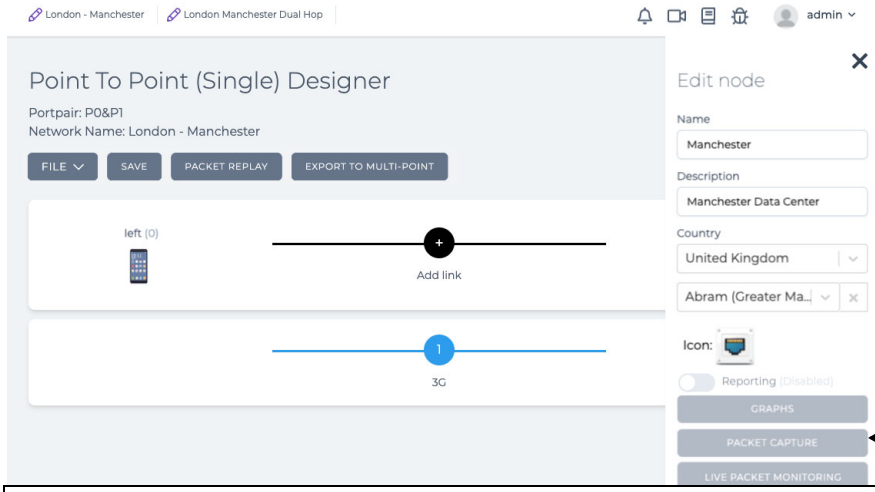
  Note:

  Compared to enabling packet capture via the **Point To Point Designer** page or **Multi-Point Designer** page, which invokes the **Packet Capture** dialog box (*Illustration 161*), enabling packet capture via the **Statistics** page is quick, and avoids the need to define the before impairment and/or after impairment criteria.

  Enabling/disabling packet capture via the **Statistics** page is almost immediate, and has the same effect as enabling/disabling the corresponding **Before impairment** and **After impairment** check boxes of the **Packet Capture** dialog box (*Illustration 161*) that is only invoked via the **Point To Point Designer** page or **Multi-Point Designer** pages.

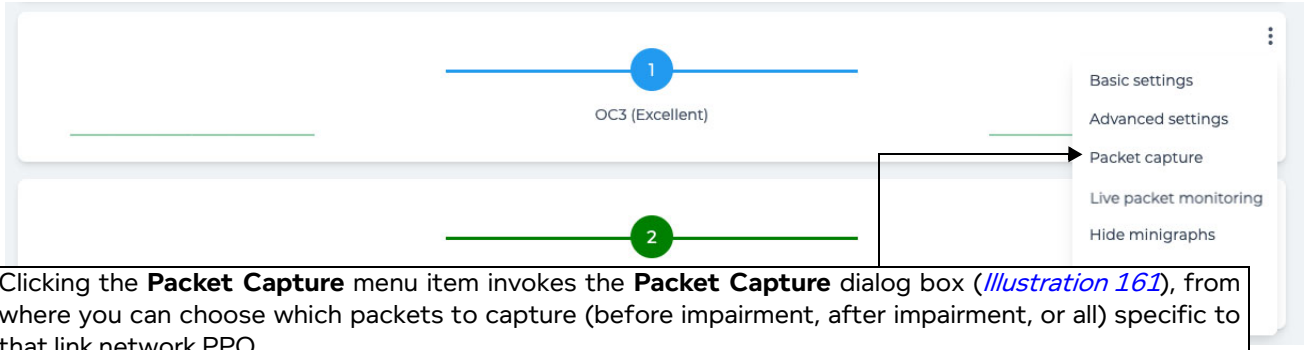
- Via the **Edit Node** panel of either a **Point To Point Designer** page or **Multi-Point Designer** page, from where you can launch a packet capture of the selected node network PPO (and all its associated

links).



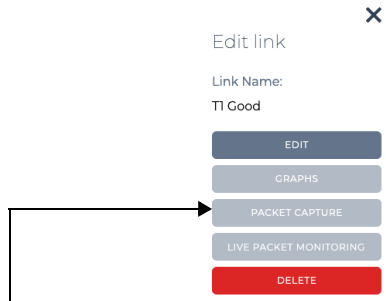
Clicking the **PACKET CAPTURE** button invokes the **Packet Capture** dialog box (*Illustration 161*), from where you can choose which packets to capture (before impairment, after impairment, or all) specific to that node network PPO (and all its associated links).

- Via the link menu of the **Point To Point Designer** page, from where you can launch a packet capture of the selected link network PPO.



Clicking the **Packet Capture** menu item invokes the **Packet Capture** dialog box (*Illustration 161*), from where you can choose which packets to capture (before impairment, after impairment, or all) specific to that link network PPO.

- Via the **Edit link** panel of the **Multi-Point Designer** page, from where you can launch a packet capture of the selected link.



Clicking the **PACKET CAPTURE** button invokes the **Packet Capture** dialog box (*Illustration 161*), from where you can choose which packets to capture (before impairment, after impairment, or all) specific to that link network PPO.

The **Packet Capture** dialog box (*Illustration 161*) contains check boxes that let you choose which packet data (*Table 64*) to capture for the selected PPO. The type of packet data you can choose to capture (and thus available check boxes) vary according to the type of selected PPO (see *Table 64*).

ILLUSTRATION 161 - PACKET CAPTURE DIALOG BOXES

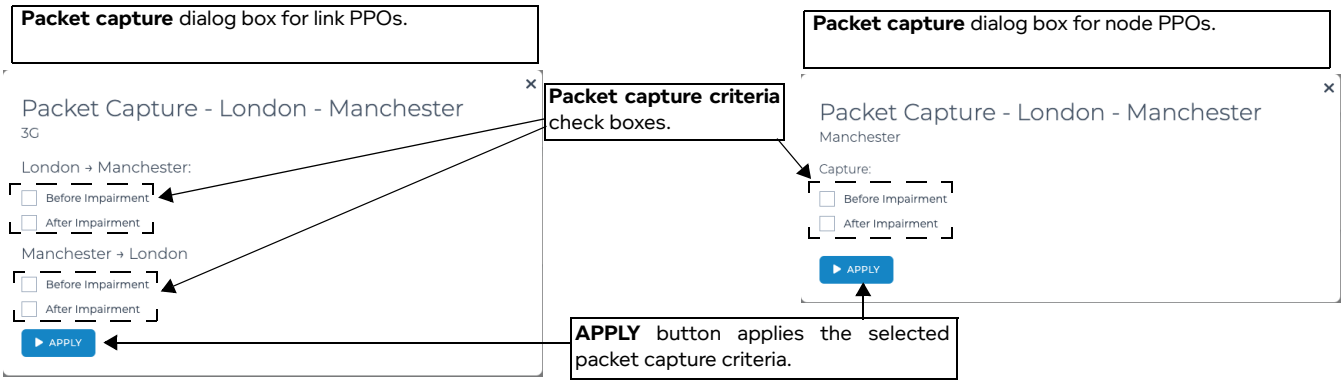


TABLE 64 - PACKET CAPTURE CRITERIA CHECK BOXES

PPO Type	Check Box	Description
Link	Left Port to Right Port direction	
	Before Impairment	Captures packets for the left to right traffic direction before the impairment criteria was applied.
	After Impairment	Captures packets for the left to right traffic direction after the impairment criteria was applied.
	Right Port to Left Port direction	
	Before Impairment	Captures packets for the right to left traffic direction before the impairment criteria was applied.
	After Impairment	Captures packets for the right to left traffic direction after the impairment criteria was applied.
Node	Before Impairment	Captures packets traversing the PPO before the impairment criteria was applied.
	After Impairment	Captures packets traversing the PPO after the impairment criteria was applied.

The **Packet Capture** dialog box also contains an **APPLY** button. Clicking this button applies the currently selected packet capture criteria, which was defined by ticking the appropriate check boxes.

Ticking one or more packet capture criteria check boxes, and clicking the **APPLY** button results in starting the packet capture process for the selected PPO. The packet capture process will continue and write packet capture data to a `*.pcap` file until you decide to stop the packet capture process.

Unticking all the packet capture criteria check boxes, and clicking the **APPLY** button, results in stopping the packet capture process for the selected PPO. Once the packet capture process is stopped, the packet capture data (`*.pcap` files) for each of the selected packet capture types are created.

! Notice:

Packet capture criteria is on a per PPO basis. When changing the packet capture criteria, take special care to note the PPO this applies to. Only the PPO that is displayed in the **Packet Capture** dialog box is loaded in cache, and therefore any changes to the packet capture criteria only apply to the currently selected PPO.

The NE-ONE creates a packet capture file (`*.pcap`) for each type of packet data that you have chosen to capture.

Packet capture files for network PPOs are located within the `/Run Data/<network name>/<network run-time date>` directory of the filing system, where:

- `<network name>` is the name of the network which the network PPO belongs to
- `<network run-time date>` is the date and time when the network was run

As the packet capture process runs on a PPO, the packet capture files for that PPO are appended to every time a packet traverses the PPO.

Packet capture files for system PPOs are located within the `/Run Data/CORE NETWORK/<system run-time date>` directory of the filing system, where `<system run-time date>` directory representing a system runtime session between each system reboot/shutdown event.

As the packet capture process runs on a PPO, the packet capture files for that PPO are appended to every time a packet traverses the PPO.

! Notice:

Packet capture files can grow considerably high in file size (e.g. up-to 1 Gigabyte). Calnex recommends that you regularly clean up packet capture files, otherwise the NE-ONE can run out of disk space and not function at its maximum efficiency. Packet capture files are located within the `/Run Data/<network name>/<network run date>` and `/Run Data/System/<system run-time date>` directories of the filing system.

Table 65 summarizes the packet capture file name conventions used for each of the PPOs used on the NE-ONE.

TABLE 65 - PACKET CAPTURE FILE NAME CONVENTIONS FOR PPOS

PPO Category	PPO Type	Packet Capture Data	Filename
Network PPO	Link	Left to right traffic direction, before impairment (filename does not contain "end")	`<network name> <network run date and time> <originating node name>::<link name> <packet capture start date and time>.pcap`
		Left to right traffic direction, after impairment (filename contains "end")	`<network name> <network run date and time> <originating node name>::<link name> end-<packet capture start date and time>.pcap`
		Right to right traffic direction, before impairment (filename does not contain "end")	`<network name> <network run date and time> <originating node name>::<link name> <packet capture start date and time>.pcap`
		Right to left traffic direction, after impairment (filename contains "end")	`<network name> <network run date and time> <originating node name>::<link name> end-<packet capture start date and time>.pcap`
	Node	Packets traversed before impairment (filename does not contain "end")	`<network name> <network run date and time> <node name> <packet capture start date and time>.pcap`
		Packets traversed after impairment (filename contains "end")	`<network name> <network run date and time> <node name> end-<packet capture start date and time>.pcap`

PPO Category	PPO Type	Packet Capture Data	Filename
Framework PPO	Hardware Port	Packets traversed before impairment	System <system run date and time> <hardware port> <packet capture start date and time>.pcap
		Packets traversed after impairment	System <system run date and time> <hardware port> end-<packet capture start date and time>.pcap
	Soft Port	Packets traversed before impairment	System <system run date and time> <soft port name> <packet capture start date and time>.pcap
		Packets traversed after impairment	System <system run date and time> <soft port name> end-<packet capture start date and time>.pcap
	Port Container	Packets traversed before impairment	System <system run date and time> <port container name> <packet capture start date and time>.pcap
		Packets traversed after impairment	System <system run date and time> <port container name> end-<packet capture start date and time>.pcap
	Service	Packets traversed before impairment	System <system run date and time> <service name> <packet capture start date and time>.pcap
		Packets traversed after impairment	System <system run date and time> <service name> end-<packet capture start date and time>.pcap

Use the procedure from one of the following sub sections to enable and disable a packet capture process on a PPO.

3-1. Enabling Packet Capture for a PPO Within the Statistics Page

Use the following steps to enable a packet capture process on a PPO from within the **Statistics** page:

1. Select **Statistics** from the Menu to open the **Statistics** page (*Illustration 160*).
2. Within the PPO Statistics table, identify the PPO for which you want to enable packet capture. If packet capture is disabled of the PPO, its corresponding packet capture indicator icons will currently be gray.
3. Click on the gray left and/or right packet capture icon(s) to enable the packet capture process for the PPO.
   - To enable packet capture data before traversing the PPO (i.e. before impairment), click on the left hand side indicator icon.

     The left hand side indicator icon will temporarily flash amber while the request is being processed by the system. Once packet capture is enabled and running for the data before traversing the PPO (i.e. before impairment), the left hand side icon will constantly flash red.
   - To enable packet capture data after traversing the PPO (i.e. after impairment), click on the right hand side indicator icon.

     The right hand side indicator icon will temporarily flash amber while the request is being processed by the system. Once packet capture is enabled and running for the data after traversing the PPO (i.e. after impairment), the right hand side icon will constantly flash red.

   The packet capture process will continue running until either it is manually stopped (see *Disabling Packet Capture on a PPO Within the Statistics Page* on page 537), or the associated network is stopped.

3-2. Disabling Packet Capture on a PPO Within the Statistics Page

Use the following steps to disable a packet capture process on a PPO from within the **Statistics** page:

1. Select **Statistics** from the Menu to open the **Statistics** page (*Illustration 160*).
2. Within the PPO Statistics table, identify the PPO for which you want to disable packet capture. If packet capture is enabled on the PPO, its corresponding packet capture indicator icons will currently be flashing red.
3. Click on the gray left and/or right packet capture icon(s) to disable the packet capture process for the PPO.
   - To disable packet capture data before traversing the PPO (i.e. before impairment), click on the left hand side indicator icon.

     The left hand side indicator icon will temporarily flash amber while the request is being processed by the system. Once packet capture is disabled for the data before traversing the PPO (i.e. before impairment), the left hand side icon will be gray.
   - To disable packet capture data after traversing the PPO (i.e. after impairment), click on the right hand side indicator icon.

     The right hand side indicator icon will temporarily flash amber while the request is being processed by the system. Once packet capture is disable for the data after traversing the PPO (i.e. after impairment), the right hand side icon will be gray.

   The packet capture process stops on the selected PPO.

3-3. Enabling Packet Capture for a Node PPO Within the Network Designer

Use the following steps to enable a packet capture process on a node PPO (and its associated ports and links) from within the Network Designer:

1. Open the network that you are interested in via either the **Home** page or **File Browser** page (see *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590).

   Either a **Point To Point Designer** page or **Multi-Point Designer** page appears according to the type of network you opened.
2. In either a **Point To Point Designer** page or **Multi-Point Designer** page of the opened network, click on the node of interest.

   An **Edit node** panel appears on the right hand side of either the **Point To Point Designer** page or **Multi-Point Designer** page.
3. In the **Edit node** panel that appears, click the **PACKET CAPTURE** button.
4. From the **Packet Capture** dialog box (*Illustration 161*) that appears, do the following:
   a. Tick the check boxes according to the type of packets that you want to capture. See *Table 64* for the different packet capture criteria that you can apply.
   b. Click **APPLY** to apply the chosen packet capture criteria.
   c. Click **START** to launch the packet capture on the selected node PPO.

   The packet capture process starts on the selected node PPO, and will continue running until either it is manually stopped (see *Disabling Packet Capture on a Node PPO Within the Network Designer* on page 538), or the associated network is stopped.

3-4. Disabling Packet Capture on a Node PPO Within the Network Designer

Use the following steps to disable a packet capture process on a node PPO (and its associated ports and links) from within the Network Designer:

1. Open the network that you are interested in via either the **Home** page or **File Browser** page (see *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590).

   Either a **Point To Point Designer** page or **Multi-Point Designer** page appears according to the type of network you opened.
2. In either a **Point To Point Designer** page or **Multi-Point Designer** page of the opened network, click on the node of interest.

   An **Edit node** panel appears on the right hand side of either the **Point To Point Designer** page or **Multi-Point Designer** page.
3. In the **Edit node** panel that appears, click the **PACKET CAPTURE** button.
4. From the **Packet Capture** dialog box (*Illustration 161*) that appears, do the following:
   a. Untick all the check boxes.
   b. Click **APPLY** to apply the chosen packet capture criteria.

   The packet capture process stops on the selected node PPO.

3-5. Enabling Packet Capture for a Link PPO Within the Network Designer

Use the following steps to enable a packet capture process on a link network PPO (and its associated ports and nodes) from within the Network Designer:

1. Open the network that you are interested in via either the **Home** page or **File Browser** page (see *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590).

   Either a **Point To Point Designer** page or **Multi-Point Designer** page appears according to the type of network you opened.
2. Launch the **Packet Capture** dialog box, as follows:
   - From within the **Point To Point Designer** page of the opened network, click on the link menu icon ⋮ of the link of interest, and select **Packet Capture**.
   - From withing the **Multi-Point Designer** page, click on the of the link of interest, and from the **Edit link** panel that appears, click the **PACKET CAPTURE** button.
3. From the **Packet Capture** dialog box (*Illustration 161*) that appears, do the following:
   a. Tick the check boxes according to the type of packets that you want to capture. See *Table 64* for the different packet capture criteria that you can apply.
   b. Click **APPLY** to apply the chosen packet capture criteria.

   The packet capture process starts on the selected link PPO, and will continue running until either it is manually stopped (see *Disabling Packet Capture on a Link PPO Within the Network Designer* on page 539), or the associated network is stopped.

3-6. Disabling Packet Capture on a Link PPO Within the Network Designer

Use the following steps to disable a packet capture process on a link network PPO (and its associated ports and nodes) from within the Network Designer:

1. Open the network that you are interested in via either the **Home** page or **File Browser** page (see *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590).

   Either a **Point To Point Designer** page or **Multi-Point Designer** page appears according to the type of network you opened.
2. Launch the **Packet Capture** dialog box, as follows:
   - From within the **Point To Point Designer** page of the opened network, click on the link menu icon ⋮ of the link of interest, and select **Packet Capture**.
   - From withing the **Multi-Point Designer** page, click on the of the link of interest, and from the **Edit link** panel that appears, click the **PACKET CAPTURE** button.
3. From the **Packet Capture** dialog box (*Illustration 161*) that appears, do the following:
   a. Untick all the check boxes.
   b. Click **APPLY** to apply the chosen packet capture criteria.

   The packet capture process stops on the selected link PPO.

4. LAUNCHING LIVE PACKET MONITORING ON A PPO

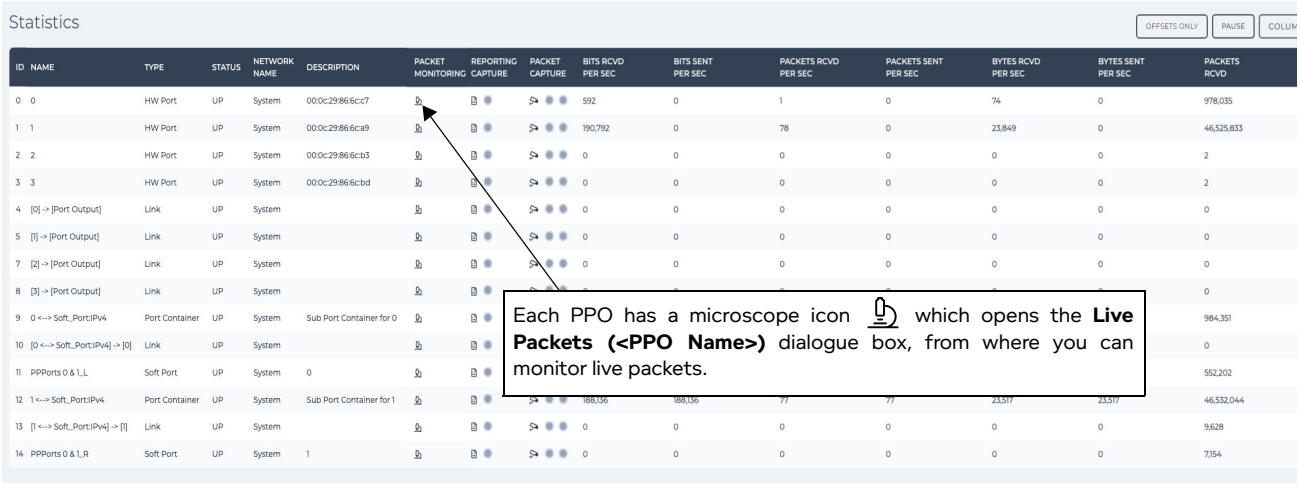
The NE-ONE lets you perform live packet monitoring of network PPOs and system PPOs so that they can be viewed in real time. Compared to packet capture (which creates a create packet capture (`*.pcap`) files for later analysis), live packet monitoring let you examine the packets in real-time so that you can debug your network applications *in-situ*.

- Live packet monitoring on a network PPO is disabled by default, and can be enabled when the associated network is running.
- Live packet monitoring on a system PPO is disabled by default, and can be enabled at any time.

Note:
To perform live packet monitoring on a network PPO (i.e. link or node PPO), its associated network must be running.

The Web Interface offers you various ways to enable live packet monitoring on a PPO, as follows:

- Via the **Statistics** page (which lists system PPOs and network PPOs of running networks).

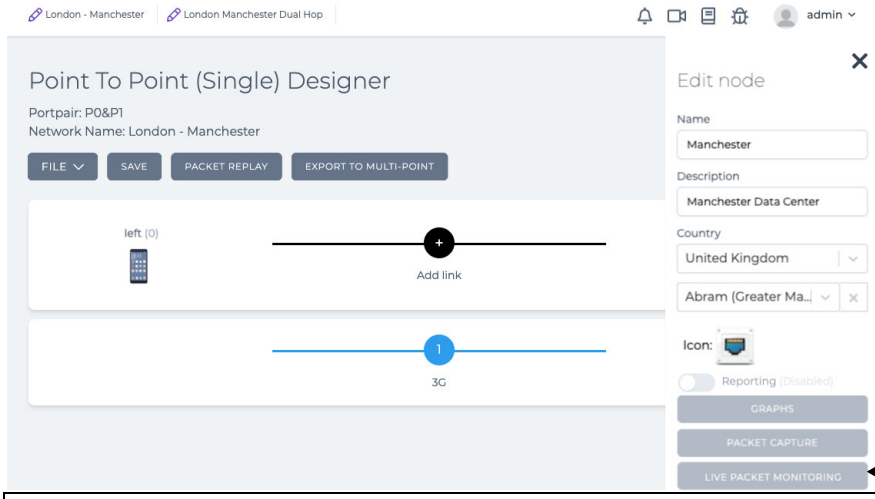


Clicking on the microscope icon invokes the **Live Packets (<PPO Name>)** dialog box (*Illustration 163*), from you can view live packet monitoring of the PPO.

Note:
For link PPOs, compared to enabling live packet monitoring via the **Point To Point Designer** page or **Multi-Point Designer** page, which invokes the intermediate **Live Packet Monitoring** dialog box (*Illustration 162*), enabling live packet monitoring via the **Statistics** page is quicker, taking you immediately to the **Live Packets (<PPO Name>)** dialog box (*Illustration 163*). This is normal, and because the link (like all other PPOs) in the **Statistics page** is a single PPO and for a single link direction, whereas the link represented in the **Multi-Point Designer** and **Point To Point Designer** pages is for two link PPOs (for both traffic directions), and you need to chose which the two link directions you would like to monitor.

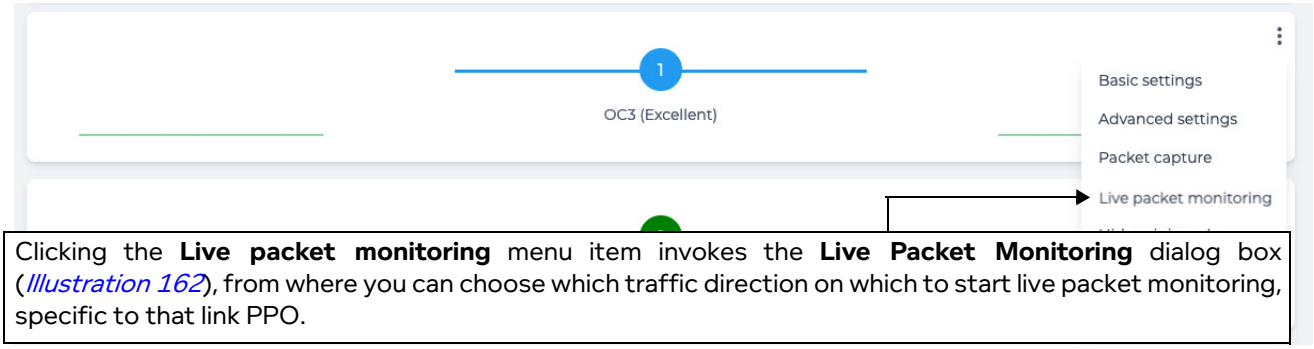
- Via the **Edit Node** panel of either a **Point To Point Designer** page or **Multi-Point Designer** page, from where you can launch live packet monitoring of the selected node PPO (and all its associated

links).



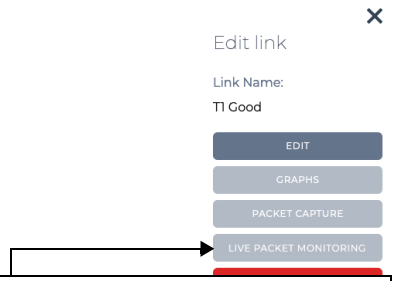
Clicking the **LIVE PACKET MONITORING** button invokes the **Live Packets (<PPO Name>)** dialog box (*Illustration 163*), from where you can immediately view the live packet data for the selected node PPO.

- Via the link menu of the **Point To Point Designer** page, from where you can launch live packet monitoring of the selected link PPO.



Clicking the **Live packet monitoring** menu item invokes the **Live Packet Monitoring** dialog box (*Illustration 162*), from where you can choose which traffic direction on which to start live packet monitoring, specific to that link PPO.

- Via the **Edit link** panel of the **Multi-Point Designer** page, from where you can launch packet decoding of the selected link PPO.



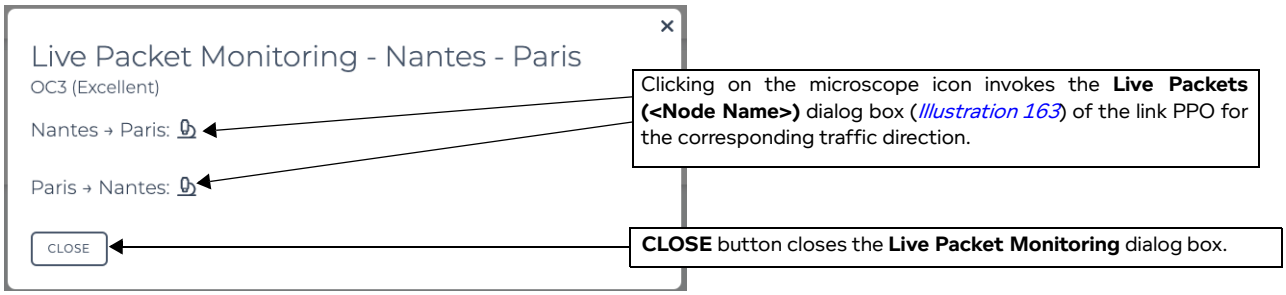
Clicking the **LIVE PACKET MONITORING** button invokes the **Live Packet Monitoring** dialog box (*Illustration 162*), from where you can choose which traffic direction on which to start packet decode process, specific to that link PPO.

4-1. The Live Packet Monitoring Dialog Box

The **Live Packet Monitoring** dialog box (*Illustration 162*) appears if you have launched live packet monitoring on a link within the **Point To Point Designer** or **Multi-Point Designer** pages, and contains a microscope icon for each traffic direction associated with that link PPO.

Clicking the microscope icon invokes the **Live Packets (<PPO Name>)** dialog box (*Illustration 163*) associated with the traffic direction for the link, letting you view the live packet data of the corresponding traffic direction for that link PPO.

ILLUSTRATION 162 - LIVE PACKET MONITORING DIALOG BOX



4-2. The Live Packets Dialog Box and the Live Packet Monitoring Page

When the **Live Packets (<PPO Name>)** dialog box is invoked via the **Statistics** page or the **Point To Point Designer** or **Multi-Point Designer** pages, it appears similar to the example shown in *Illustration 163*.

ILLUSTRATION 163 - LIVE PACKETS DIALOG BOX

The **Live Packets (<PPO Name>)** dialog box contains the elements summarized in *Table 66*, and lets you view the live packet data of the PPO in real time.

TABLE 66 - LIVE PACKETS DIALOG BOX ELEMENTS

Live Packets Dialog Box Element	Description
×	The **Live Packets (<PPO Name>)** dialog box is a temporary dialog box, which needs to be closed in order to continue using the Web Interface. Clicking this icon closes the **Live Packets (<PPO Name>)** dialog box, letting you resume using the Web Interface. **Note:** If you want the live packet data for the PPO to permanently remain being monitored, click the **PIN** button (see below).
Enabled check box	By default live packet monitoring for the PPO is disabled. This check box lets determine whether or not the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box updates with scrolling live packet data. • Tick this check box to enable live packet monitoring, and show the live packet data of the PPO within the packet data area. Upon ticking, the live packet data of the PPO will immediately start scrolling within the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box. • Untick this check box to disable live packet monitoring, and stop showing the live packet data of the PPO within the packet data area. Upon unticking, the live packet data of the PPO will immediately stop scrolling within the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box.
CLEAR button	Clicking on this button results in clearing the existing content within the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box. • If live packet monitoring is enabled, the live packet data of the PPO will continue scrolling within the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box, showing any packet data after the **CLEAR** button was clicked. • If live packet monitoring is disabled, the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box becomes blank, and will only become populated with live packet data once you re-enable live packet monitoring.
PIN button	Clicking on this button results in permanently pinning the **Live Packets (<PPO Name>)** dialog box into a permanent **Live Packet Monitoring** page (*Illustration 164*), and invoking a dialog box asking you whether you stay within the **Live Packets (<PPO Name>)** dialog box or go to the **Live Packet Monitoring** page.
STREAMS button	Clicking on this button opens a dialog box listing all the packet streams (each with a check box) traversing the PPO, and lets you determine which packet streams have their packets visible in the **Packet Data Area**. By default all the check boxes for all the packet streams are disabled (i.e. there is no view filter in effect), and all the packets from all the packet streams are visible in the **Packet Data Area**. Enabling one or more of the check boxes associated with a packet stream brings the view filter into effect, and only the packets from the selected packet streams will be visible in the **Packet Data Area**.
PAUSE / **UNPAUSE** button	Clicking on the **PAUSE** button results in pausing the scrolling live packet data. Clicking on the **UNPAUSE** button results in resuming the scrolling of the live packet data.

Live Packets Dialog Box Element	Description
SAVE TO FILE button	Clicking on this button results in immediately downloading a `download.txt` file to your computer's download directory. The `download.txt` file is a JSON object containing the live packet monitoring data up to the time you clicked this button. You can view the `download.txt` file in any JSON object file viewer. For example, in VS Code (if the JSON Viewer extension is installed) you can open the `download.txt` file, then press **F1** and type **`open in json viewer`**, and select **Open in JSON Viewer** to run the JSON Viewer extension. The `download.txt` file will be opened within the JSON Viewer extension of VS Code.

The **Live Packets (<PPO Name>)** dialog box must be closed using the ✕ icon if you want to continue using the Web Interface. If you want to permanently monitor live packet data for a particular PPO of interest, click the **PIN** button to add it to the **Live Packet Monitoring** page (*Illustration 164*).

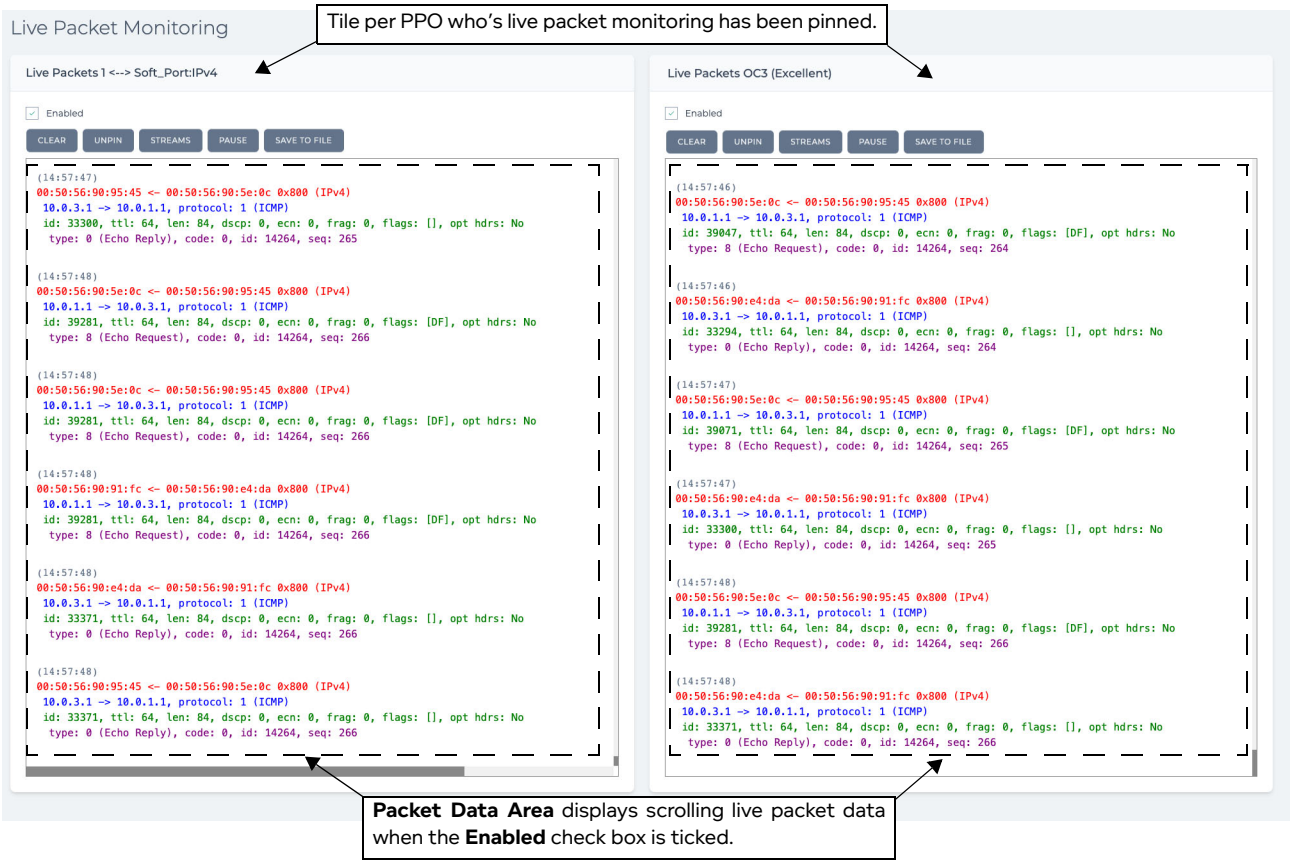
By default, the **Live Packet Monitoring** page initially contains no live packet monitoring data, and is therefore not accessible from within the Web Interface.

Once you have pinned live packet monitoring of one or more PPOs, the Tray area of the Web Interface displays the microscope icon . Clicking the microscope icon from within the Tray area opens the **Live Packet Monitoring** page (*Illustration 164*).

Note:

The live packet monitoring data is not stored on the NE-ONE. The live packet monitoring data is sent to the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box (*Illustration 163*) and the **Live Packet Monitoring** page (*Illustration 164*), and remains present for the particular open web browser session being used to view the NE-ONE Web Interface.

ILLUSTRATION 164 - LIVE PACKET MONITORING PAGE



The **Live Packet Monitoring** page contains a tile for each PPO that you have pinned for live packet monitoring. Each tile has a heading of the format **Live Packets (<PPO Name>)**, and contains the elements summarized in *Table 67*.

TABLE 67 - LIVE PACKETS TILE ELEMENTS

Live Packets Tile Element	Description
Enabled check box	This check box lets determine whether or not the **Packet Data Area** of the **Live Packets (<PPO Name>)** tile updates with scrolling live packet data. • Tick this check box to enable live packet monitoring, and show the live packet data of the PPO within the packet data area. Upon ticking, the live packet data of the PPO will immediately start scrolling within the **Packet Data Area** of the **Live Packets (<PPO Name>)** tile. • Untick this check box to disable live packet monitoring, and stop showing the live packet data of the PPO within the packet data area. Upon unticking, the live packet data of the PPO will immediately stop scrolling within the **Packet Data Area** of the **Live Packets (<PPO Name>)** tile.
CLEAR button	Clicking on this button results in clearing the existing content within the **Packet Data Area** of the **Live Packets (<PPO Name>)** tile. • If live packet monitoring is enabled, the live packet data of the PPO will continue scrolling within the **Packet Data Area** of the **Live Packets (<PPO Name>)** tile, showing any packet data after the **CLEAR** button was clicked. • If live packet monitoring is disabled, the **Packet Data Area** of the **Live Packets (<PPO Name>)** tile becomes blank, and will only become populated with live packet data once you re-enable live packet monitoring.

Live Packets Tile Element	Description
UNPIN button	Clicking on this button results in removing the **Live Packets (<PPO Name>)** tile from the **Live Packet Monitoring** page (*Illustration 164*). **Note:** When you click the **UNPIN** button within the in the **Live Packet Monitoring** page containing only one **Live Packets (<PPO Name>)** tile, the **Live Packet Monitoring** page closes, you are returned to the **Home** page, and the microscope icon in the Task bar disappears.
STREAMS button	Clicking on this button opens a dialog box listing all the packet streams (each with a check box) traversing the PPO, and lets you determine which packet streams have their packets visible in the **Packet Data Area**. By default all the check boxes for all the packet streams are disabled (i.e. there is no view filter in effect), and all the packets from all the packet streams are visible in the **Packet Data Area**. Enabling one or more of the check boxes associated with a packet stream brings the view filter into effect, and only the packets from the selected packet streams will be visible in the **Packet Data Area**.
PAUSE / **UNPAUSE** button	Clicking on the **PAUSE** button results in pausing the scrolling live packet data. Clicking on the **UNPAUSE** button results in resuming the scrolling of the live packet data.
SAVE TO FILE button	Clicking on this button results in immediately downloading a `download.txt` file to your computer's download directory. The `download.txt` file is a JSON object containing the live packet monitoring data up to the time you clicked this button. You can view the `download.txt` file in any JSON object file viewer. For example, in VS Code (if the JSON Viewer extension is installed) you can open the `download.txt` file, then press **F1** and type **`open in json viewer`**, and select **Open in JSON Viewer** to run the JSON Viewer extension. The `download.txt` file will be opened within the JSON Viewer extension of VS Code.

4-3. Enabling and Disabling Live Packet Monitoring of a PPO Within the Statistics Page

Use the following steps to enable and disable a live packet monitoring process on a PPO from within the **Statistics** page:

1. Select **Statistics** from the Menu to open the **Statistics** page (*Illustration 160*).
2. Within the PPO Statistics table, identify the PPO for which you want to enable live packet monitoring.
3. Click on the PPO's microscope icon within the **Live Packet Monitoring** column to launch **Live Packets (<PPO Name>)** dialog box. At this point the live packet monitoring process for the PPO is disabled.
4. From the **Live Packets (<PPO Name>)** dialog box that appears, tick the **Enable** check box.

   The live packet monitoring process will start, and the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box updates with scrolling live packet data for the PPO.

   The **Live Packets (<PPO Name>)** dialog box remains open and you are unable to use the rest of the Web Interface until it is closed.
5. Determine your next step:
   - If you want to disable live packet monitoring, untick the **Enable** check box.
   - If you want to close the **Live Packets (<PPO Name>)** dialog box and continue using the Web Interface, click the ✕ located at the top right of the **Live Packets (<PPO Name>)** dialog box.

- If you want to permanently pin the live packet monitoring information for the PPO into the **Live Packet Monitoring** page, click the **PIN** button.

4-4. Enabling and Disabling Live Packet Monitoring of a Link PPO Within the Network Designer

Use the following steps to enable and disable a live packet monitoring process on a link PPO from within the Network Designer:

1. Open the network that you are interested in via either the **Home** page or **File Browser** page (see *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590).

   Either a **Point To Point Designer** page or **Multi-Point Designer** page appears according to the type of network you opened.
2. In the **Point To Point Designer** page or **Multi-Point Designer** page of the opened network, click on the **PLAY** button to start the network, then do one of the following:
   - From within the **Point To Point Designer** page of the opened network, click on the link menu icon ⋮ of the link of interest, and select **Live packet monitoring**.
   - From within the **Multi-Point Designer** page, click on the of the link of interest, and from the **Edit link** panel that appears, click the **LIVE PACKET MONITORING** button.
3. From the **Live Packet Monitoring** dialog box (*Illustration 162*) that appears, click on the microscope icon corresponding to the traffic direction of the link PPO that you want to monitor.

   A **Live Packets (<PPO Name>)** dialog box (*Illustration 163*) appears corresponding to the traffic direction of the Link PPO that you had selected. At this point the live packet monitoring process is disabled.
4. From the **Live Packets (<PPO Name>)** dialog box that appears, tick the **Enable** check box.

   The live packet monitoring process will start, and the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box updates with scrolling live packet data for the link PPO's selected traffic direction.

   The **Live Packets (<PPO Name>)** dialog box remains open and you are unable to use the rest of the Web Interface until it is closed.
5. Determine your next step:
   - If you want to disable live packet monitoring, untick the **Enable** check box.
   - If you want to close the **Live Packets (<PPO Name>)** dialog box and continue using the Web Interface, click the ✕ located at the top right of the **Live Packets (<PPO Name>)** dialog box.
   - If you want to permanently pin the live packet monitoring information for the link PPO into the **Live Packet Monitoring** page, click the **PIN** button.

4-5. Enabling and Disabling Live Packet Monitoring of a Node PPO Within the Network Designer

Use the following steps to enable and disable a live packet monitoring process on a node PPO from within the Network Designer:

1. Open the network that you are interested in via either the **Home** page or **File Browser** page (see *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590).

   Either a **Point To Point Designer** page or **Multi-Point Designer** page appears according to the type of network you opened.

2. In either the **Point To Point Designer** page or **Multi-Point Designer** page of the opened network, do the following:
   a. Click on the **PLAY** button to start the network.
   b. Click on the node of interest.

   An **Edit node** panel appears on the right hand side of the **Point To Point Designer** page or **Multi-Point Designer** page.
3. In the **Edit node** panel that appears, click the **LIVE PACKET MONITORING** button.

   A **Live Packets (<PPO Name>)** dialog box (*Illustration 163*) appears corresponding to the node PPO that you had selected. At this point the live packet monitoring process is disabled.
4. From the **Live Packets (<PPO Name>)** dialog box that appears, tick the **Enable** check box.

   The live packet monitoring process will start, and the **Packet Data Area** of the **Live Packets (<PPO Name>)** dialog box updates with scrolling live packet data for the node PPO.

   The **Live Packets (<PPO Name>)** dialog box remains open and you are unable to use the rest of the Web Interface until it is closed.
5. Determine your next step:
   - If you want to disable live packet monitoring, untick the **Enable** check box.
   - If you want to close the **Live Packets (<PPO Name>)** dialog box and continue using the Web Interface, click the ✕ located at the top right of the **Live Packets (<PPO Name>)** dialog box.
   - If you want to permanently pin the live packet monitoring information for the node PPO into the **Live Packet Monitoring** page, click the **PIN** button.

4-6. Pinning Live Packets of a PPO to the Live Packet Monitoring Page

Use the following steps to pin the live packets of a PPO to the **Live Packet Monitoring** page:

1. Use one of the following methods to enable live packet monitoring for each PPO of interest:
   - Enable live packet monitoring on a PPO of interest from the **Statistics** page, according to *Enabling and Disabling Live Packet Monitoring of a PPO Within the Statistics Page* on page 546.
   - Enable live packet monitoring on a link PPO of interest from either the **Point To Point Designer** page or **Multi-Point Designer**, according to *Enabling and Disabling Live Packet Monitoring of a Node PPO Within the Network Designer* on page 547.
   - Enable live packet monitoring on a node PPO of interest from either the **Point To Point Designer** page or **Multi-Point Designer**, according to *Enabling and Disabling Live Packet Monitoring of a Node PPO Within the Network Designer* on page 547.
2. Once the **Live Packets (<PPO Name>)** dialog box appears, click the **PIN** button.
3. From the dialog box prompting you to either remain on the **Live Packets (<PPO Name>)** dialog box or go to the **Live Packet Monitoring** page, click the **OK** button.

   The **Live Packets (<PPO Name>)** dialog box closes, and a **Live Packets (<PPO Name>)** tile gets added to the **Live Packet Monitoring** page.
4. If necessary, add pin additional live packets for each PPO of interest to the **Live Packet Monitoring** page.

   The **Live Packets (<PPO Name>)** tiles for each of the PPOs of interest remain in the **Live Packet Monitoring** page until you remove them. If at a later time you want to remove the **Live Packets (<PPO Name>)** tile(s) from the **Live Packet Monitoring** page, follow *Unpinning Live Packets of a PPO from the Live Packet Monitoring Page* on page 549.

4-7. Unpinning Live Packets of a PPO from the Live Packet Monitoring Page

When live packets from a PPO of interest has been pinned to the **Live Packet Monitoring** page, the **Live Packets (<PPO Name>)** tile of the PPO of interest will remain within the **Live Packet Monitoring** page. Once you have finished with your in-situ testing of your network applications, you may want to remove (unpin) the live packets of each PPO on interest from the **Live Packet Monitoring** page. To do this, follow the steps below.

1. From the Task area of the Web Interface, click microscope icon .
2. From the **Live Packet Monitoring** page (*Illustration 164* on page 545) that appears, click on the **UNPIN** button within the **Live Packets (<PPO Name>)** tile that is no longer of interest.
3. Repeat step 2 for each of the **Live Packets (<PPO Name>)** tiles that you want to remove.

Note:

In order for the microscope icon to be present in the Task area of the Web Interface, at least one **Live Packets (<PPO Name>)** tile must exist in the **Live Packet Monitoring** page. If you unpin the last **Live Packets (<PPO Name>)** tile from the **Live Packet Monitoring** page, the **Live Packet Monitoring** page immediately closes, the microscope icon disappears from the Task area, and you are returned to the **Home** page. This is normal behavior. The microscope icon will re-appear in the Task area when you pin at least one **Live Packets (<PPO Name>)** tile to the **Live Packet Monitoring** page. For more information on pinning one or more **Live Packets (<PPO Name>)** tiles to the **Live Packet Monitoring** page, see *Pinning Live Packets of a PPO to the Live Packet Monitoring Page* on page 548.

5. LAUNCHING LIVE GRAPHS ON A PPO FROM AN ACTIVE NETWORK

The Web Interface offers you various ways to launch live graphing on a PPO from an active network (i.e. a network that is being played).

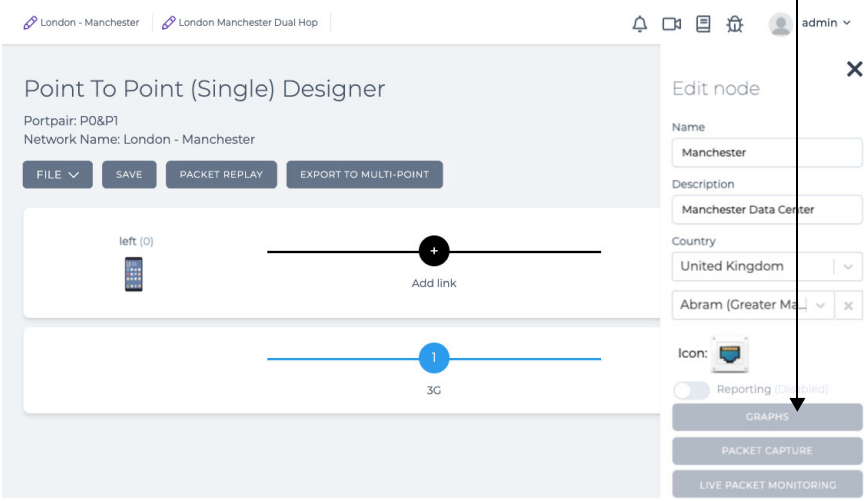
Note:

For a network PPO (i.e. link or node PPO) to be graphed with live data, its associated network must be running (i.e. played). You can also display static graphs with static data from historical networks (i.e. networks that have previously been played / stopped). For more information, see *The Historical Statistics Pages* on page 565.

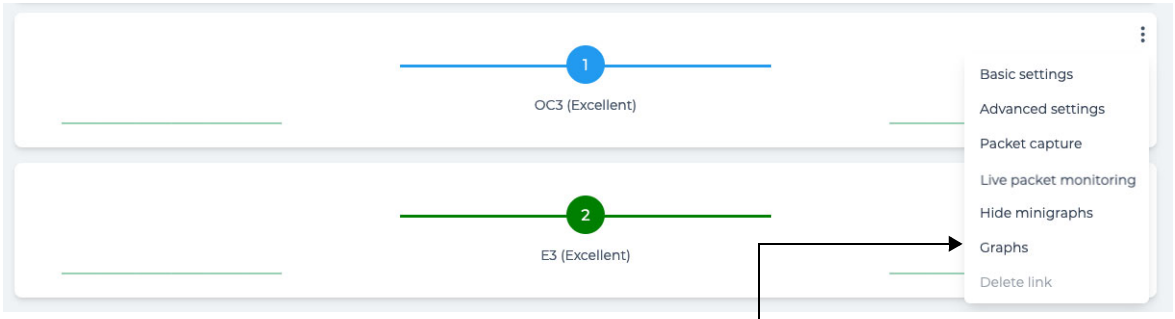
The ways in which you can launch graphing vary according to where you are in the Web Interface, as follows:

- Via the **Edit Node** panel of the **Point To Point Designer** page or **Multi-Point Designer** page, from where you can launch graphing of the selected node PPO.

Clicking the **GRAPHS** button invokes the **Select data to monitor** dialog box (*Illustration 165*), from where you can choose which data to display in a graph specific to that node and the ports it is associated with.
Note: In order for the **GRAPHS** button to be active, the network needs to be running.

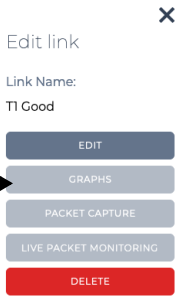


- Via the link menu of the **Point To Point Designer** page, from where you can launch graphing of the selected link PPO.



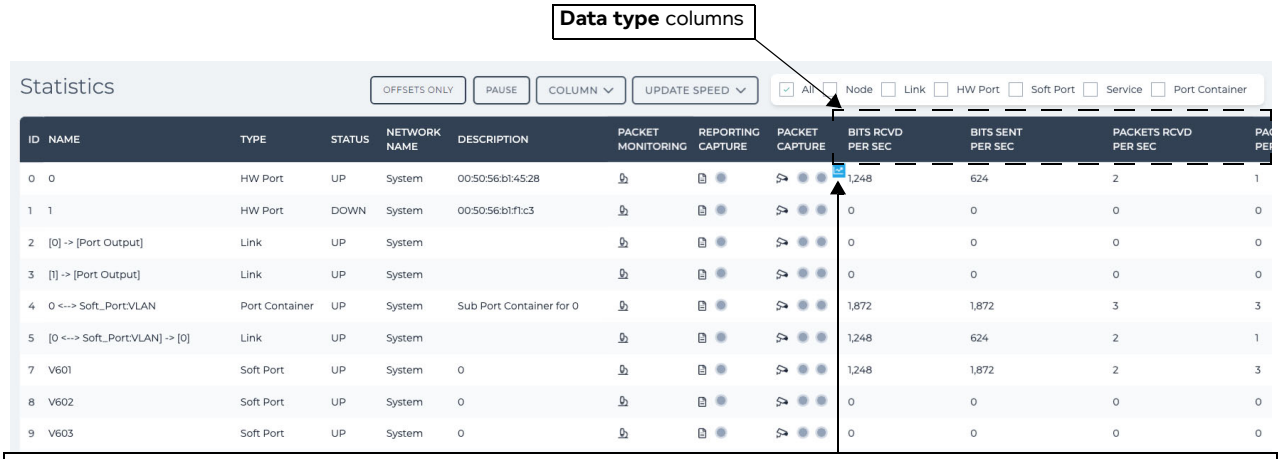
Clicking the **Graphs** menu item invokes the **Select data to monitor** dialog box (*Illustration 165*), from where you can choose which type of data to monitor specific to that link.

- Via the **Edit link** panel of the **Multi-Point Designer** page, from where you can launch graphing of the selected link PPO.



Clicking the **GRAPHS** button invokes the **Select data to monitor** dialog box (*Illustration 165*), from where you can choose which type of data to monitor specific to that link.

- Via the **Statistics** page (which only lists network PPOs for running (playing) networks and system PPOs), from where you can launch graphing data of a PPO from within the list.



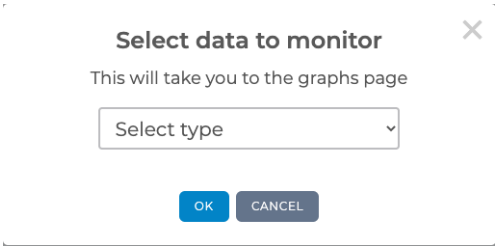
Positioning the mouse pointer at the start of the one of the following data type columns reveals a graph icon , which upon clicking immediately opens the appropriate data type graph in the **Graphs** page (*Illustration 168* on page 556), specific to that network PPO:

- BITS RCVD PER SEC
- BITS SENT PER SEC
- PACKETS RCVD PER SEC
- PACKETS SENT PER SEC
- BYTES RCVD PER SEC
- BYTES SENT PER SEC
- PACKETS RCVD
- PACKETS SENT
- BYTES RCVD
- BYTES SENT
- INTERNAL DROPPED
- HARDWARE DROPPED

- Via the **Graphs** page (see *Illustration 168*) or the **Add New Graph** page (see *Illustration 170*). For more information, see *The Graphs Page* on page 555.

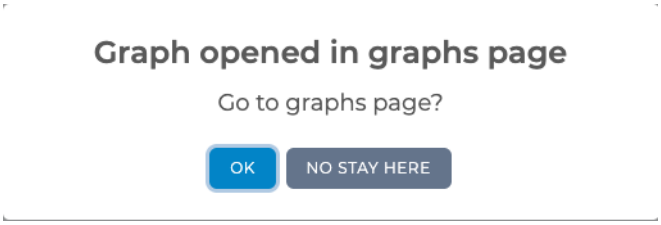
The **Select data to monitor** dialog box (*Illustration 165*) lets you choose which data type you want to monitor on a link or node PPO.

ILLUSTRATION 165 - GRAPH SELECTION DIALOG BOX (INVOKED FROM EDIT NODE PANEL OR LINK MENU)



Upon selecting the data type, then clicking **OK** a graph for the selected data type is opened within the **Graphs** page, and a second **Go to graphs page ?** dialog box (*Illustration 166*) appears prompting you either remain on the existing page (i.e. **NO STAY HERE** button) or go to the **Graphs** page (i.e. **OK** button).

ILLUSTRATION 166 - GO TO GRAPHS PAGE DIALOG BOX (INVOKED FROM EDIT NODE PANEL OR LINK MENU)



Use the procedure from one of the following sub sections to launch a graphing process on a PPO.

5-1. Launching Graphs for a PPO within the Statistics page

Use the following steps to launch a graphing process on a network from within the **Statistics** page:

1. Select **Statistics** from the Menu to launch the **Statistics** page (*Illustration 160*).
2. Within the PPO Statistics table, identify the PPO which you want to monitor via a graphing.
3. For the identified PPO, position the mouse pointer at the start of one of the following **Data type** columns, and click on the graph icon that appear:
   - BITS RCVD PER SEC
   - BITS SENT PER SEC
   - PACKETS RCVD PER SEC
   - PACKETS SENT PER SEC
   - BYTES RCVD PER SEC
   - BYTES SENT PER SEC
   - PACKETS RCVD
   - PACKETS SENT
   - BYTES RCVD
   - BYTES SENT
   - INTERNAL DROPPED
   - HARDWARE DROPPED

   A graph opens in the **Graphs** page, showing data according to the type of data you had selected.

5-2. Launching Graphs for a Node PPO within the Network Designer

Use the following steps to launch a graphing process on a node PPO (and its associated ports and links) from within the Network Designer:

1. Open the network that you are interested in via either the **Home** page or **File Browser** page (see *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590).

   Either a **Point To Point Designer** page or **Multi-Point Designer** page appears according to the type of network you opened.
2. In either the **Point To Point Designer** page or **Multi-Point Designer** page of the opened network, do the following:
   a. Click on the **PLAY** button to start the network.
   b. Click on the node of interest.

   An **Edit node** panel appears on the right hand side of the **Point To Point Designer** page or **Multi-Point Designer** page.
3. In the **Edit node** panel that appears, click the **GRAPHS** button.
4. From the **Select data to monitor** dialog box (*Illustration 165*) that appears, do the following:
   a. Select the data type you want to monitor from the drop-down field.
   b. Click **OK** button apply the chosen data graphing criteria.

   The **Select data to monitor** dialog box closes, and a second **Go to graphs page ?** dialog box appears. The chosen data graphing criteria starts and appears within the **Graphs** page.
5. From the **Go to graphs page ?** dialog box (*Illustration 166*) that appears, do the following:
   - If you want to remain on **Point To Point Designer** page or **Multi-Point Designer** page of the opened network, click the **NO STAY HERE** button.
   - If you want to go to the **Graphs** page, click the **OK** button.

5-3. Launching Graphs for a Link PPO within the Network Designer

Use the following steps to launch a graphing capture process on a Link PPO (and its associated ports and nodes) from within the Network Designer:

1. Open the network that you are interested in via either the **Home** page or **File Browser** page (see *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590).

   Either a **Point To Point Designer** page or **Multi-Point Designer** page appears according to the type of network you opened.
2. In the **Point To Point Designer** page or **Multi-Point Designer** page of the opened network, click on the **PLAY** button to start the network, then do one of the following:
   - From within the **Point To Point Designer** page of the opened network, click on the link menu icon ⋮ of the link of interest, and select **Graphs**.
   - From within the **Multi-Point Designer** page, click on the of the link of interest, and from the **Edit link** panel that appears, click the **GRAPHS** button.
3. From the **Select data to monitor** dialog box (*Illustration 165*) that appears, do the following:
   a. Select the data type you want to monitor from the drop-down field.
   b. Click **OK** button apply the chosen data graphing criteria.

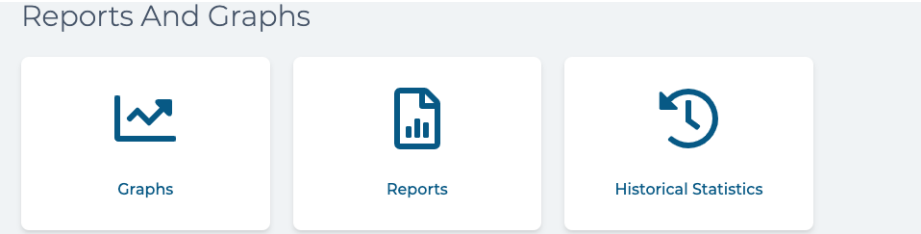
   The **Select data to monitor** dialog box closes, and a second **Go to graphs page ?** dialog box appears. The chosen data graphing criteria starts and appears within the **Graph s** page.

4. From the **Go to graphs page ?** dialog box (*Illustration 166*) that appears, do the following:
   - If you want to remain on **Point To Point Designer** page or **Multi-Point Designer** page of the opened network, click the **NO STAY HERE** button.
   - If you want to go to the **Graphs** page, click the **OK** button.

6. THE REPORTS AND GRAPHS PAGE

The **Reports And Graphs** page (see *Illustration 167*) appears after clicking **Reports & Graphs** from the Menu, and is the central location from where you can perform graphing, generate reports, and view historical statistics.

ILLUSTRATION 167 - GRAPHS AND REPORTS PAGE



The **Reports And Graphs** page contains the following tiles:

- **Graphs** - clicking this tile opens either the **Graphs** page or the **Add New Graph** page. For more information, see *Section 6-1*, *The Graphs Page* on page 555.
- **Reports** - clicking this tile opens the **Reporting** page. For more information, see *Section 6-3*, *The Reporting Page* on page 568.
- **Historical Statistics** - clicking this tile opens a series **Historical Statistics** pages, starting with the **Historical Statistics - Browse Network** page. For more information, see *Section 6-2*, *The Historical Statistics Pages* on page 565.

6-1. The Graphs Page

The **Graphs** page (*Illustration 168* on page 556) is the central location where all graphing data is displayed, and where graphing data can be created. You can create graphs from either active networks (i.e. networks that are currently playing, and not yet stopped) or historical networks (i.e. networks that have been played and stopped).

Note:
Graphing data from active networks can also be created (i.e. launched) via the **Statistics** page, the **Point To Point Designer** page, and the **Multi-Point Designer** page. For more information, see *Section 5*, *Launching Live Graphs on a PPO From an Active Network*.

The **Graphs** page is invoked in one the following cases:

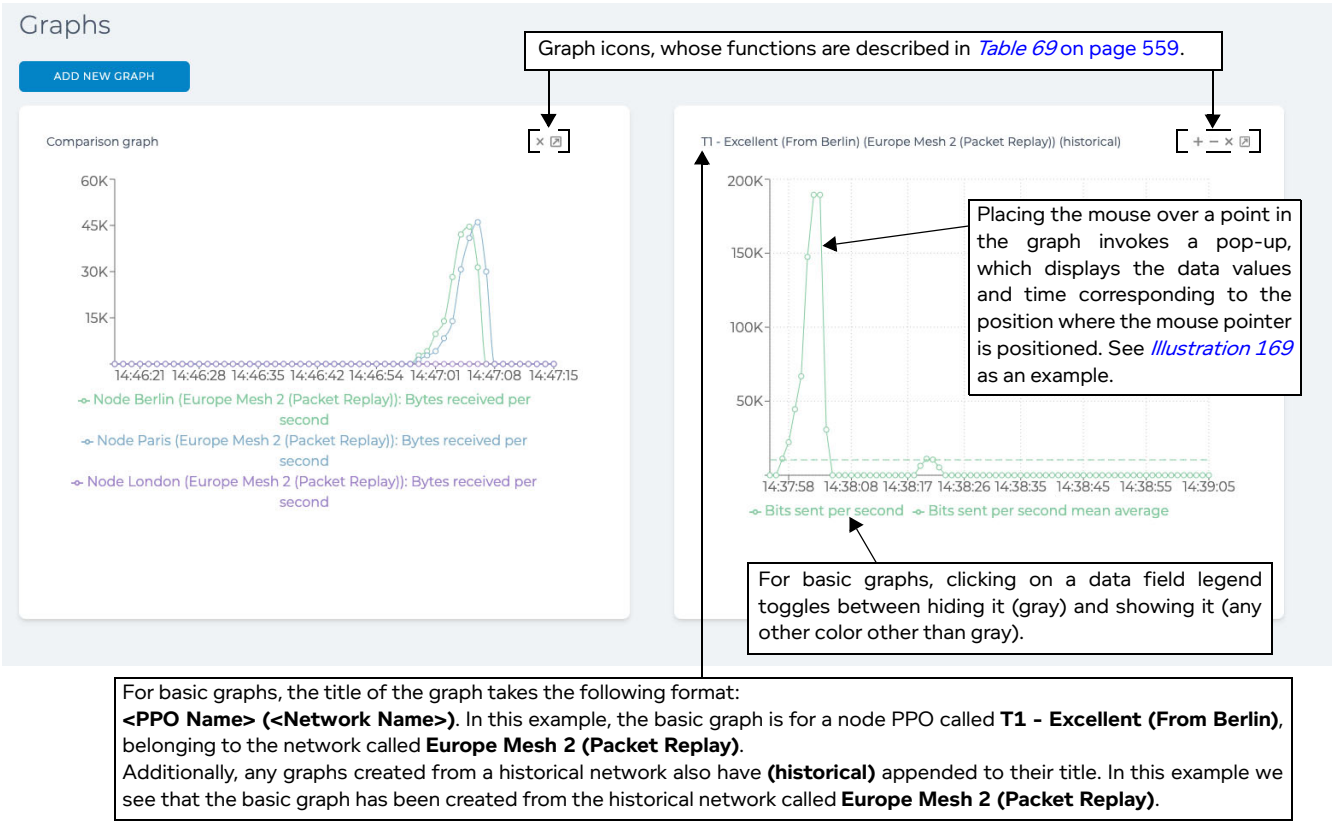
- After clicking **Graphs** from the tile from within the **Reports And Graphs** page (see *Illustration 167* on page 555), and if there is already a graph that has previously been added.

  Note:
  If no graphs are already added on the NE-ONE, you are directly taken to the **Add New Graph - Select Network Type** page (*Illustration 170*).

  Note:
  The **Graphs** page (*Illustration 168*) may appear with no graphs in it with only an **ADD NEW GRAPH** button, but only in the case where you are already on this page containing existing graphs, and delete all the existing graphs. If you do this, the next time you navigate back via the **Reports And Graphs** page, the **Add New Graph - Select Network Type** page re-appears.
- After clicking graph icon on a PPO's data-type column within the **Statistics** page (see *section 5-1*, *Launching Graphs for a PPO within the Statistics page* on page 552).
- After clicking on the **GRAPHS** button of the **Edit node** panel from within either the **Point To Point Designer** page or **Multi-Point Designer** page (see *section 5-2*, *Launching Graphs for a Node PPO within the Network Designer* on page 553).

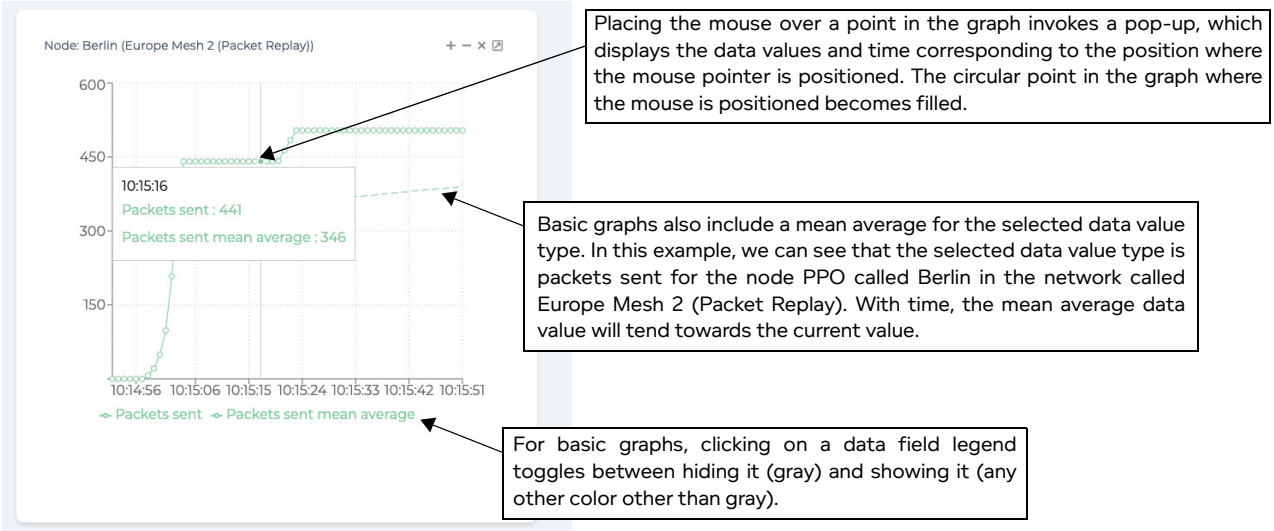
- After selecting the **Graphs** item from the link menu icon ⋮ of a link from within the **Point To Point Designer** (see *section 5-3*, *Launching Graphs for a Link PPO within the Network Designer* on page 553).
- After clicking on the **GRAPHS** button of the **Edit link** panel from within the **Multi-Point Designer** page (see *section 5-3*, *Launching Graphs for a Link PPO within the Network Designer* on page 553).

ILLUSTRATION 168 - AN EXAMPLE GRAPHS PAGE



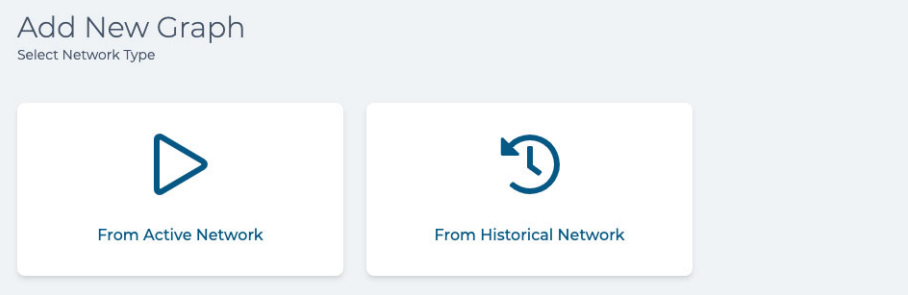
Placing the mouse over a point in the comparison or basic graph invokes a pop-up, which displays the data values and time corresponding to the position where the mouse pointer is positioned.

ILLUSTRATION 169 - EXAMPLE GRAPH DATA POP-UP (BASIC GRAPH EXAMPLE).



The **Graphs** page contains the **ADD NEW GRAPH** button. Clicking this button starts the graph creation wizard, and opens an **Add New Graph - Select Network Type** page (see *Illustration 170* on page 557) from where you can choose to create a graph from either an active network or a historical network.

ILLUSTRATION 170 - ADD NEW GRAPH (SELECT NETWORK TYPE) PAGE



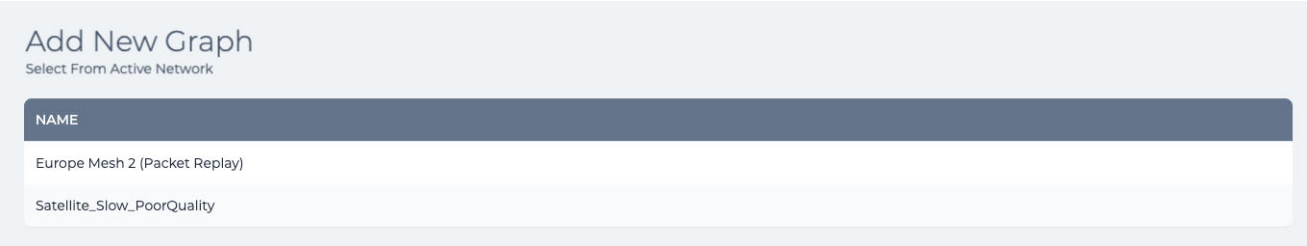
The **Add New Graph - Select Network Type** page contains the following tiles:

- **From Active Network** - clicking on this tile opens the **Add New Graph - Select From Active Network** page, from where you can select an active network, and add one or more graphs from PPOs and data types of interest. For more information, see *Section 6-1-1*, *Creating Basic and Comparison Graphs from Active Networks* on page 557.
- **From Historical Network** - clicking on this tile opens the **Historical Statistics - Browse Networks** page, from where you can select a historical network, and add one or more graphs from PPOs and data types of interest. For more information, see *Section 6-2-1*, *Viewing Historical Statistics and Creating Basic Graphs Based on Historical Statistics* on page 565.

6-1-1. Creating Basic and Comparison Graphs from Active Networks

Upon clicking the **From Active Network** tile from within the **Graphs** page, the **Add New Graph - Select From Active Network** page (*Illustration 171*) appears listing any active networks.

ILLUSTRATION 171 - ADD NEW GRAPH (SELECT FROM ACTIVE NETWORK) PAGE



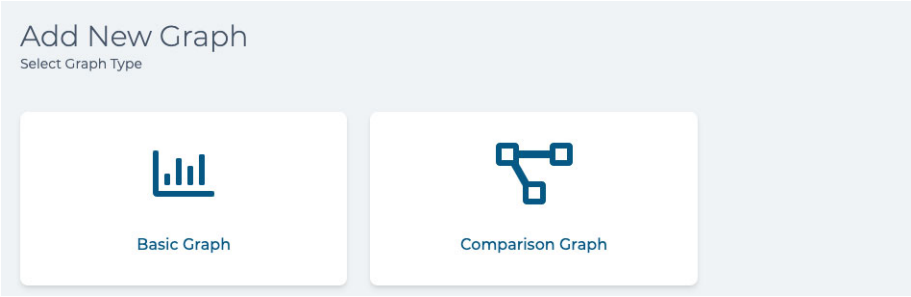
Note:

If no networks are currently active (i.e. being played), the list of active networks is blank.

Clicking on an active network listed within the **Add New Graph - Select From Active Network** page invokes the **Add New Graph - Select Graph Type** page (see *Illustration 172*), from where you can choose between a basic graph or comparison graph.

The **Add New Graph - Select Graph Type** page (see *Illustration 172*) launches the graph creation wizard that lets you create either a basic or combination graph. Once the graph creation wizard is complete, the basic or comparison graph appears in the **Graphs** page.

ILLUSTRATION 172 - ADD NEW GRAPH PAGE (SELECT GRAPH TYPE)



The differences between the basic graph and comparison graph are discussed in *Table 68* on page 558. Once created, the basic or comparison graph gets added to the **Graphs** page. You can add multiple graphs (basic and/or comparison) to the **Graphs** page.

- For more information on creating a basic graph, see *Creating Basic Graphs* on page 559.
- For more information on creating an advanced graph, see *Creating Comparison Graphs* on page 561.

Once basic and/or comparison graphs are created (via either the **Add New Graph** page or via the **Statistics** page, **Point To Point Designer** page or **Multi-Point Designer** page), they appear within the **Graphs** page in the order in which they were created. *Illustration 168* shows an example of a **Graphs** page, containing a basic graph (on the right hand side) and a comparison graph (on the left hand side). In the example of *Illustration 168*, we can see that:

- The comparison graph was created before the basic graph (because the graphs appear from left to right in the order in which they were created).
- The basic graph has the title of the format: **<PPO Name> (<Network Name>)**, with the data field(s) in the legend. In this example, the basic graph was created from a historical network, and additionally has **(historical)** appended to its title.
- The comparison graph has the title **Comparison graph**, with the data field(s) in the legend of the following format: **<PPO Type> <PPO Name> (<Network Name>): <data field>**.

TABLE 68 - DIFFERENCES BETWEEN BASIC GRAPH AND COMPARISON GRAPH

Graph Type	Description	How it is created
Basic	Displays one or more data types for only one PPO. When initially created, the basic graph shows one data type for the PPO. Once created, you can add and remove additional data types using the **+** and **-** icons located in the top right corner of the basic graph.	• Via the **Graphs** page, using the graph creation wizard. For more information, see *Creating Basic Graphs* on page 559. • After clicking on the **GRAPHS** button of the **Edit node** panel from within either the **Point To Point Designer** page or the **Multi-Point Designer** page. • After clicking graph icon on a PPO's data-type column within the **Statistics** page (see Note).

Graph Type	Description	How it is created
Comparison	More advanced that the basic graph, and lets you select multiple data types for multiple PPOs, overlaying all of the data types for all of the PPO types on the same graph.	• Via the **Graphs** page, using the graph creation wizard. For more information, see *Creating Comparison Graphs* on page 561. • After clicking on the **GRAPHS** button of the **Edit link** panel from within the **Multi-Point Designer** page (see Note). • After selecting the **Graphs** item from the link menu icon ⋮ of a link from within the **Point To Point Designer** page (see Note).
Note: Creating a graph for a link PPO from within the **Statistics** page results in creating a basic graph, whereas creating a graph from a link within the **Multi-Point Designer** page or **Point To Point Designer** page results in creating a basic graph. This difference is normal and because the link (like all other PPOs) in the **Statistics** page is a single PPO and for a single link direction, whereas the link represented in the **Multi-Point Designer** and **Point To Point Designer** pages is for two link PPOs (for both traffic directions), and thus the two link directions are displayed in a comparison graph.		

The basic and comparison graphs contain icons whose functions are described in *Table 69*. The icons that exist at the top right of a graph vary according to the graph type as summarized in *Table 69*.

TABLE 69 - GRAPH ICONS

Graph Type	Icon	Icon Function/Description
Basic	+	Adds a new data field to the graph. Clicking on this icon invokes a **Choose field to add** dialog box, which lets you select an additional data field to add to the graph.
	−	Removes an existing data field from the graph. Clicking on this icon invokes a **Choose field to remove** dialog box, which lets you select an existing data field to remove from the graph.
Basic and Comparison	×	Removes the graph from the **Graphs** page. Clicking this icon invokes a confirmation dialog box, which upon clicking **OK** will result in removing the graph from the **Graphs** page.
	⧉	Launches the graph in a separate browser tab. Clicking this icon immediately opens the graph in a separate browser tab. The original graph remains in the **Graphs** page.

6-1-2. Creating Basic Graphs

Use the following steps to create a basic graph on an active (i.e. playing) network:

1. Select **Reports & Graphs** from the Menu to launch the **Reports And Graphs** page.
2. From the **Reports And Graphs** page, click the **Graphs** tile.
3. From the **Graphs** page, click on the **ADD NEW GRAPH** button.

Note:
If no graph currently exists on the NE-ONE you are immediately taken to the **Add New Graph - Select Network Type** page.

4. From the **Add New Graph - Select Network Type** page (see *Illustration 170*) that appears, click the **From Active Network** tile.
5. The **Add New Graph - Select From Active Network** page (*Illustration 171*), click on the network of interest from the list of active networks.

Note:
If no networks are currently active (i.e. being played) the list of active networks is blank. In this case, play the network of interest and re-start this procedure from step 1.

6. From the **Add New Graph - Select Graph Type** page (see *Illustration 172*) that appears, click on the **Basic Graph** tile.

   The **Add New Graph** page updates with different tiles, letting you select one of the following PPO types:

   - **HW Port**
   - **Node**
   - **Link**
   - **Soft Port**
   - **Port Container**

   Note:
   The **Soft Port** and **Port Container** tiles are only visible if a network is running using soft ports, and/or if a network is running with a port pair that has Port Addressing enabled.

7. Click on the appropriate tile (**HW Port**, **Node**, **Link**, **Soft Port** or **Port Container**) corresponding to the PPO type that you want to capture graphing data for.
8. A dialog box appears, requesting you to choose the PPO.
   - If you had selected a **HW Port** PPO type, a **Choose HW Port** dialog box appears with a list of hardware ports to choose from. Select the hardware port that you want to capture graphing data for, then click **OK**.

   Note:
   The hardware ports that are listed can vary depending on the version of the NE-ONE.
   - If you had selected a **Node** PPO type, a **Choose Node** dialog box appears with a list of nodes to choose from. Select the node that you want to capture graphing data for, then click **OK**.

   Note:
   The nodes that are listed correspond to the node names of all the nodes that have been created for each running network.
   - If you had selected a **Link** PPO type, a **Choose Link** dialog box appears with a list of links to choose from. Select the link that you want to capture graphing data for, then click **OK**.

   Note:
   The links that are listed correspond to the link names of all the links that have been created for each running network.
   - If you had selected a **Soft Port** PPO type, a **Choose Soft Port** dialog box appears with a list of soft ports to choose from. Select the soft port that you want to capture graphing data for, then click **OK**.

   Note:
   The soft ports that are listed correspond to the soft port names of all the soft ports that have been created for each running network.
   - If you had selected a **Port Container** PPO type, a **Choose Port Container** dialog box appears with a list of port containers to choose from. Select the port container that you want to capture graphing data for, then click **OK**.

   Note:
   The port containers that are listed correspond to the name of the "accomodating" soft port or hardware port that the port container is associated with, and the soft port type this is

accommodated by the hardware/soft port, and if the port container is in a running network.
For example, if a VLAN soft port called V601 is created on hardware port 0, and an IPv4 soft port called 192.168.1.4 is created within the V601 soft port, and a network is running that uses these VLAN and IPv4 soft ports, then the following two port containers exist from within the list of port containers:
0 <--> Soft_Port:VLAN (System) - which is the port container PPO to support any VLAN soft ports under the hardware port 0
V601 <--> Soft_Port:IP4 (System) - which is the port container PPO to support any IPv4 soft ports under the VLAN soft port V601

A **Choose field** dialog box appears, requesting you to choose the data field to graph for the selected PPO.

9. From the **Choose field** dialog box that appears, select the data field that you want to capture for the selected PPO, then click **OK**.

   The basic graph gets added to the **Graphs** page, and you are returned to the **Graphs** page.

   The basic graph contains with the sole data field that you specified in step 9. If you want to add or remove addition data fields to/from the basic graph see *Adding and Removing Data Fields to Basic Graphs* on page 561.

6-1-2-1. Adding and Removing Data Fields to Basic Graphs

When a basic graph has been created, it will exist in the **Graphs** page with the sole data field that was specified when it was originally created. Once a basic graph exists in the **Graphs** page, you can add or remove additional data fields using the steps below.

1. Select **Reports & Graphs** from the Menu to launch the **Reports And Graphs** page.
2. From the **Reports And Graphs** page, click the **Graphs** tile.
3. From the **Graphs** page, identify the basic graph whose data fields you want to modify.
4. If you want to add addition data fields to the basic graph, use the sub-steps below for each data field that you want to add:
   a. Click the + icon located at the top right of the basic graph.
   b. From the **Choose field to add** dialog box that appears, select an appropriate data field, then click **OK**.

      The **Choose field to add** dialog box closes, and the selected data field is immediately added to the basic graph.
5. If you want to remove existing data fields from the basic graph, use the sub-steps below for each data field that you want to remove:
   a. Click the + icon located at the top right of the basic graph.
   b. From the **Choose field to remove** dialog box that appears, select an appropriate data field, then click **OK**.

      The **Choose field to remove** dialog box closes, and the selected data field is immediately removed from the basic graph.

6-1-3. Creating Comparison Graphs

Use the following steps to create a comparison graph on an active (i.e. playing) network:

1. Select **Reports & Graphs** from the Menu to launch the **Reports And Graphs** page.
2. From the **Reports And Graphs** page, click the **Graphs** tile.
3. From the **Graphs** page, click on the **ADD NEW GRAPH** button.

Note:
If no graph currently exists on the NE-ONE you are immediately taken to the **Add New Graph - Select Network Type** page.

4. From the **Add New Graph - Select Network Type** page (see *Illustration 170*) that appears, click the ▷ **From Active Network** tile.
5. The **Add New Graph - Select From Active Network** page (*Illustration 171*), click on the network of interest from the list of active networks.

Note:
If no networks are currently active (i.e. being played) the list of active networks is blank. In this case, play the network of interest and re-start this procedure from step 1.

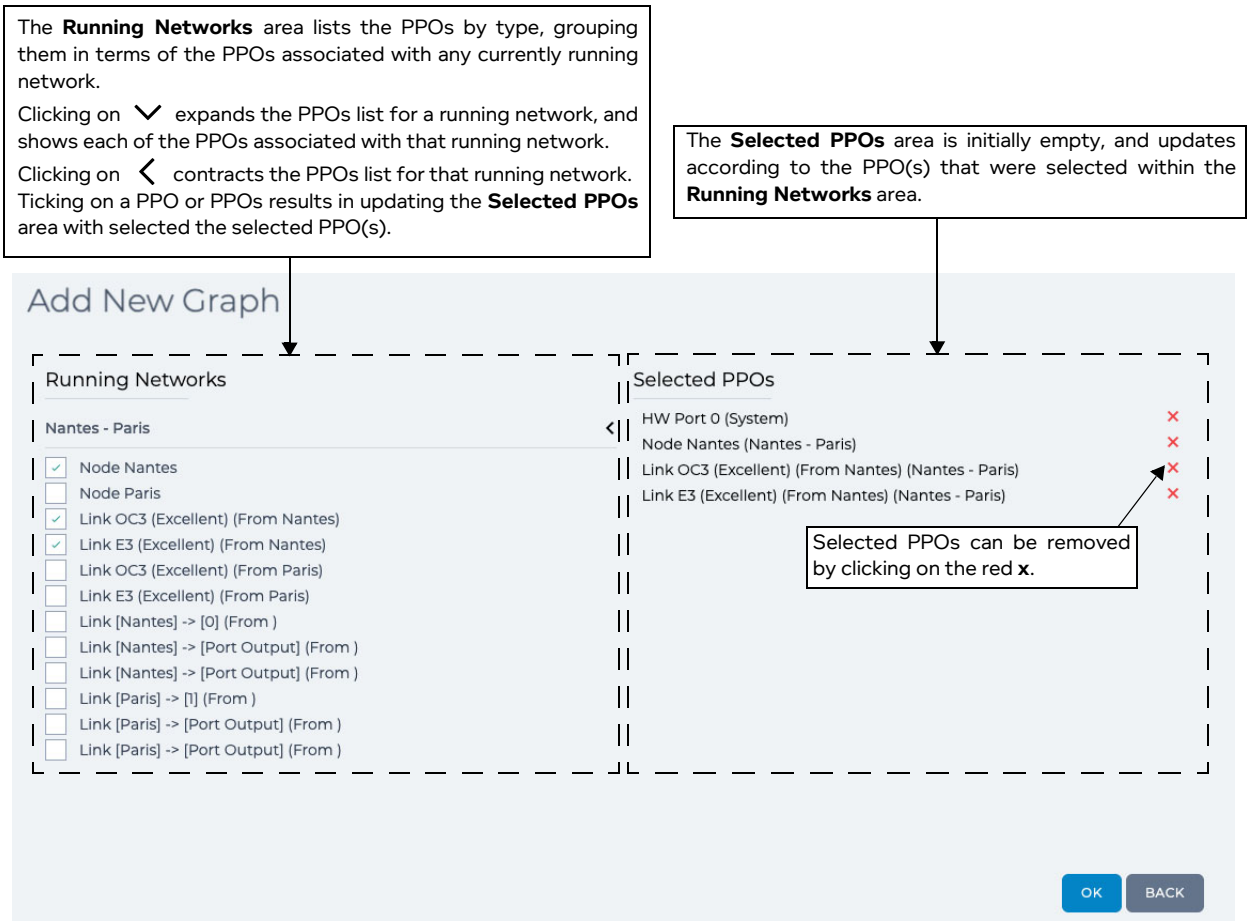
6. From the **Add New Graph - Select Graph Type** page (see *Illustration 172*) that appears, click on the **Comparison Graph** tile.

   The **Add New Graph** page updates similar to *Illustration 173* letting you select one or more of the following PPO types, grouped into any currently running networks:

   - **HW Port**
   - **Node**
   - **Link**
   - **Soft Port**
   - **Port Container**

Note:
The **Soft Port** and **Port Container** check boxes are only visible if a network is running using soft ports, and/or if a network is running with a port pair that has Port Addressing enabled.

ILLUSTRATION 173 - COMPARISON ADD NEW GRAPH PAGE - SELECTING PPOS



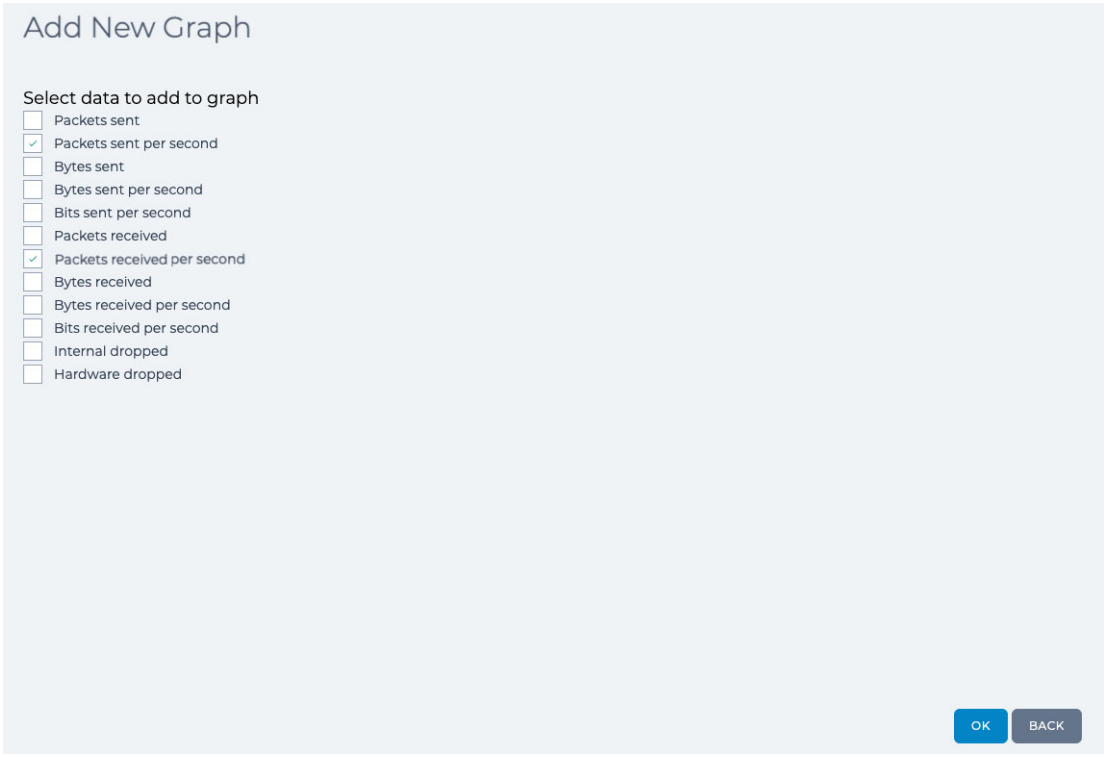
7. From the **Add New Graph** page, do the following:
   a. Click on the ⌄ icon next to the PPO type(s) (i.e. **<Network Name A>**, **<Network Name B>**) to expand the list of available PPOs in the running network of interest.
   b. In the **Running Networks** area, tick the check boxe(s) of the PPO(s) that you want to graph.
      The **Selected PPOs** area updates with a list of PPOs that you selected.
      Note: Selected PPOs can be removed by clicking on the associated red **x** icon.
   c. Once you are happy with the selected PPO(s) for graphing, click **OK**.

The **Graphs** page updates similar to *Illustration 174* letting you select one or more of the following data field types to capture in the graph for the selected PPO(s):

- **Packets sent**
- **Packets sent per second**
- **Bytes sent**
- **Bytes sent per second**
- **Packets received**
- **Packets received per second**
- **Bytes received**
- **Bytes received per second**
- **Bits received per second**

- **Internal dropped**
- **Hardware dropped**

ILLUSTRATION 174 - COMPARISON GRAPHS PAGE - SELECTING DATA TYPES FOR THE SELECTED PPOS



8. From the **Add New Graphs** page, do the following:
   a. In the **Select data to add to graph** area, tick the check boxe(s) of the data field type(s) that you want to graph.
   b. Once you are happy with the selected data field type(s) for graphing, click **OK**.

   A comparison graph with the PPOs and data fields you selected gets added to the **Graphs** page, and you are returned to the **Graphs** page.

6-2. The Historical Statistics Pages

A series of **Historical Statistics** pages appear after clicking the **Historical Statistics** tile from within the **Reports And Graphs** page (see *Illustration 167* on page 555) or from within the **Add New Graph - Select Network Type** page (see *Illustration 170* on page 557).

The series of **Historical Statistics** pages let you view the historical statistics of previously played networks, and create graphs based upon the chosen historical statistics.

Note:

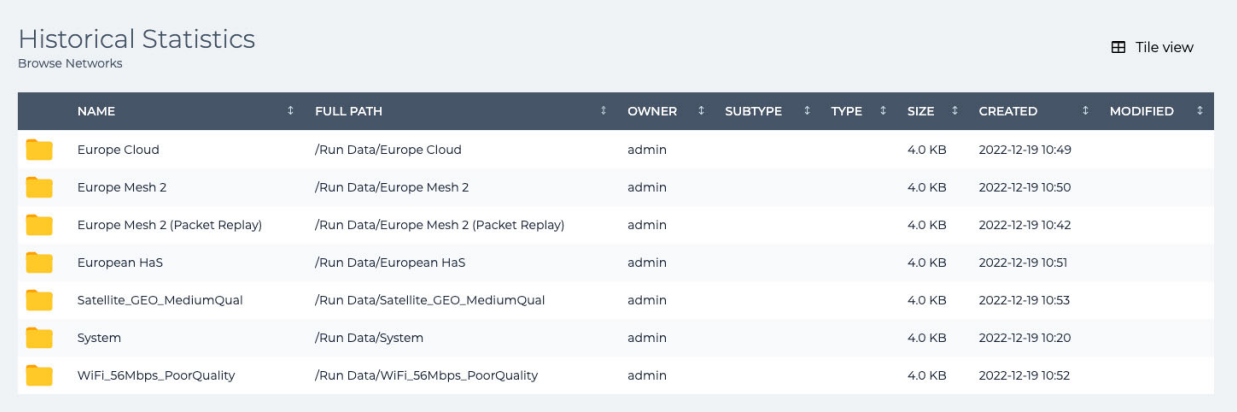
The series of **Historical Statistics** pages also contain any active networks in addition to the networks that were previously played/stopped. Conceptually this is because active networks are also considered historical because although they are active, they have generated data that occurred in the past, and are thus also considered to be historic.

6-2-1. Viewing Historical Statistics and Creating Basic Graphs Based on Historical Statistics

Active networks let you create both comparison graphs and basic graphs. In comparison, the historical statistics from historical networks only let you create basic graphs. Use the following steps to view the historical statistics on a network of interest, and to create basic graphs based on the historical statistics of interest:

1. Select **Reports & Graphs** from the Menu to launch the **Reports And Graphs** page.
2. From the **Reports And Graphs** page that appears, click the **Historical Statistics** tile.

   A **Historical Statistics - Browse Networks** page appears, listing all the networks that have previously been run.



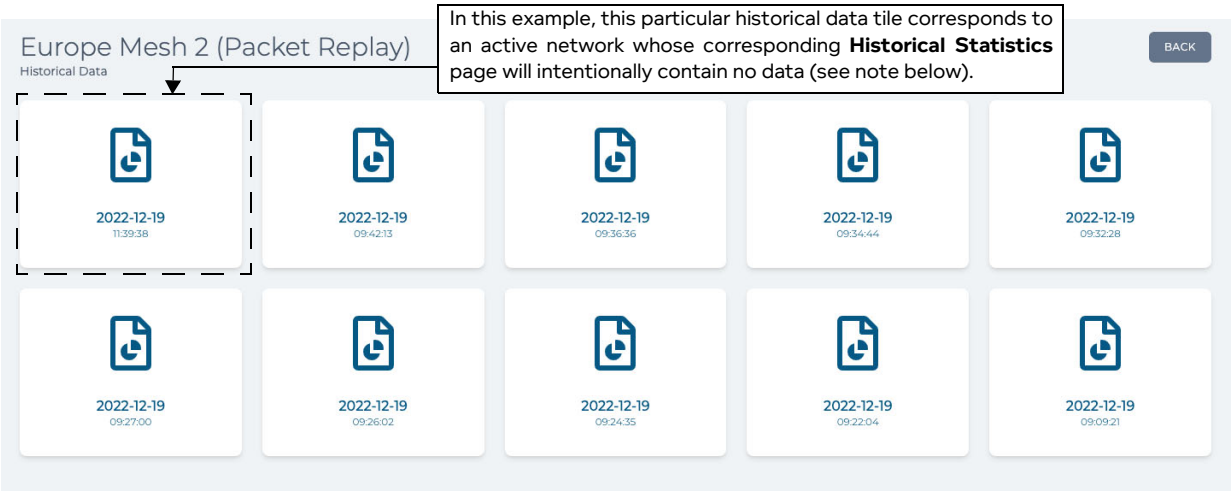
Note:

The **Historical Statistics - Browse Networks** page also contains any active networks in addition to the networks that were previously played/stopped. Conceptually this is because active networks are also considered historical because although they are active, they have generated data that occurred in the past, and are thus also considered to be historic.

3. From the **Historical Statistics - Browse Networks** page, double click on the network of interest.

   A **<Network Name> - Historical Data** page appears, with a list of historical data tiles corresponding to each time the network has previously been played. Each historical data tile contains the "start"

runtime (i.e. the date and time when the network was played (not stopped)).



Note:

If the selected network is currently active, the **<Network Name> - Historical Data** page also contains a historical data tile for the active network in addition to historical data tiles corresponding to when the selected network was previously played/stopped. Conceptually this is because active networks are also considered historical because although they are active, they have generated data that occurred in the past, and are thus also considered to be historic.

4. From the **<Network Name> - Historical Data** page, identify the "start" runtime of interest and click on the corresponding historical data tile.

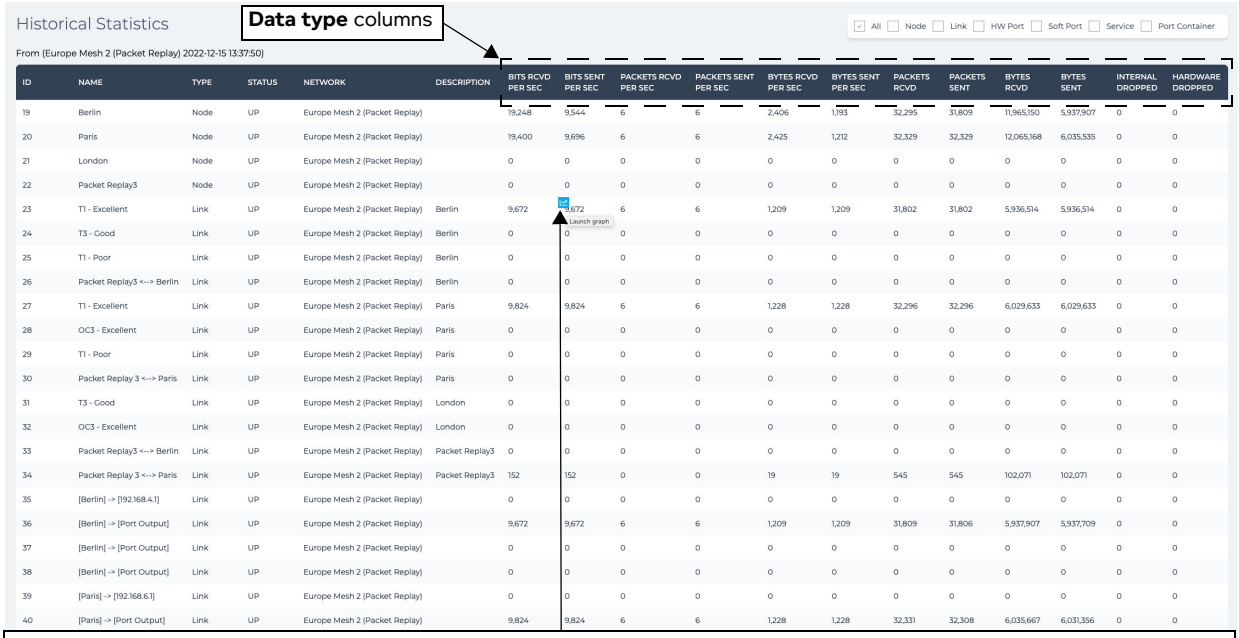
Note:

If you have clicked on a historical data tile corresponding to an active (i.e. currently playing and not yet stopped) network, the **Historical Statistics** page will appear blank as shown below. This is normal as the network is currently active.

If you stop the active network, then re-navigate to and click on the same historical data tile, the **Historical Statistics** page will then contain data.

If you have clicked on a historical data tile corresponding to a historical network, a **Historical Statistics** page appears corresponding to the network and runtime that you selected, and contains

static packet statistics.



ID	NAME	TYPE	STATUS	NETWORK	DESCRIPTION	BITS RCVD PER SEC	BITS SENT PER SEC	PACKETS RCVD PER SEC	PACKETS SENT PER SEC	BYTES RCVD PER SEC	BYTES SENT PER SEC	PACKETS RCVD	PACKETS SENT	BYTES RCVD	BYTES SENT	INTERNAL DROPPED	HARDWARE DROPPED
19	Berlin	Node	UP	Europe Mesh 2 (Packet Replay)		19,248	9,544	6	6	2,406	1,193	32,295	31,809	11,965,150	5,937,907	0	0
20	Paris	Node	UP	Europe Mesh 2 (Packet Replay)		19,400	9,696	6	6	2,425	1,212	32,329	32,329	12,065,168	6,035,535	0	0
21	London	Node	UP	Europe Mesh 2 (Packet Replay)		0	0	0	0	0	0	0	0	0	0	0	0
22	Packet Replay3	Node	UP	Europe Mesh 2 (Packet Replay)		0	0	0	0	0	0	0	0	0	0	0	0
23	T1 - Excellent	Link	UP	Europe Mesh 2 (Packet Replay)	Berlin	9,672	9,672	6	6	1,209	1,209	31,802	31,802	5,936,514	5,936,514	0	0
24	T3 - Good	Link	UP	Europe Mesh 2 (Packet Replay)	Berlin	0	0	0	0	0	0	0	0	0	0	0	0
25	T1 - Poor	Link	UP	Europe Mesh 2 (Packet Replay)	Berlin	0	0	0	0	0	0	0	0	0	0	0	0
26	Packet Replay3 <--> Berlin	Link	UP	Europe Mesh 2 (Packet Replay)	Berlin	0	0	0	0	0	0	0	0	0	0	0	0
27	T1 - Excellent	Link	UP	Europe Mesh 2 (Packet Replay)	Paris	9,824	9,824	6	6	1,228	1,228	32,296	32,296	6,029,633	6,029,633	0	0
28	OC3 - Excellent	Link	UP	Europe Mesh 2 (Packet Replay)	Paris	0	0	0	0	0	0	0	0	0	0	0	0
29	T1 - Poor	Link	UP	Europe Mesh 2 (Packet Replay)	Paris	0	0	0	0	0	0	0	0	0	0	0	0
30	Packet Replay 3 <--> Paris	Link	UP	Europe Mesh 2 (Packet Replay)	Paris	0	0	0	0	0	0	0	0	0	0	0	0
31	T3 - Good	Link	UP	Europe Mesh 2 (Packet Replay)	London	0	0	0	0	0	0	0	0	0	0	0	0
32	OC3 - Excellent	Link	UP	Europe Mesh 2 (Packet Replay)	London	0	0	0	0	0	0	0	0	0	0	0	0
33	Packet Replay3 <--> Berlin	Link	UP	Europe Mesh 2 (Packet Replay)	Packet Replay3	0	0	0	0	0	0	0	0	0	0	0	0
34	Packet Replay 3 <--> Paris	Link	UP	Europe Mesh 2 (Packet Replay)	Packet Replay3	152	152	0	0	19	19	545	545	102,071	102,071	0	0
35	[Berlin] -> [192.168.4.1]	Link	UP	Europe Mesh 2 (Packet Replay)		0	0	0	0	0	0	0	0	0	0	0	0
36	[Berlin] -> [Port Output]	Link	UP	Europe Mesh 2 (Packet Replay)		9,672	9,672	6	6	1,209	1,209	31,809	31,806	5,937,907	5,937,709	0	0
37	[Berlin] -> [Port Output]	Link	UP	Europe Mesh 2 (Packet Replay)		0	0	0	0	0	0	0	0	0	0	0	0
38	[Berlin] -> [Port Output]	Link	UP	Europe Mesh 2 (Packet Replay)		0	0	0	0	0	0	0	0	0	0	0	0
39	[Paris] -> [192.168.6.1]	Link	UP	Europe Mesh 2 (Packet Replay)		0	0	0	0	0	0	0	0	0	0	0	0
40	[Paris] -> [Port Output]	Link	UP	Europe Mesh 2 (Packet Replay)		9,824	9,824	6	6	1,228	1,228	32,331	32,308	6,035,667	6,031,356	0	0

Positioning the mouse pointer at the start of the one of the following data type columns reveals a graph icon , which upon clicking immediately opens the appropriate data type graph in the **Graphs** page, specific to that network PPO:

- BITS RCVD PER SEC
- BITS SENT PER SEC
- PACKETS RCVD PER SEC
- PACKETS SENT PER SEC
- BYTES RCVD PER SEC
- BYTES SENT PER SEC
- PACKETS RCVD
- PACKETS SENT
- BYTES RCVD
- BYTES SENT
- INTERNAL DROPPED
- HARDWARE DROPPED

The **Historical Statistics** page is similar to the **Statistics** page, but does not have live packet statistics or the **PACKET MONIROTING**, **REPORTING CAPTURE**, or **PACKET CAPTURE** columns.

The **Historical Statistics** page contains the accumulated packet statistics that were acquired while the network was run (i.e. played and stopped).

5. You can add one or more basic graphs from the **Historical Statistics** page by clicking on the appropriate graph icon next to the PPO of interest and data type of interest.

   When you click a graph icon, the basic graph for the PPO of interest and data type of interest gets added to the **Graphs** page (see *Illustration 168* on page 556 as an example), and you are taken to the **Graphs** page. Repeat steps 1 to 5 for each basic graph that you want to create based on the historical statistics of interest.

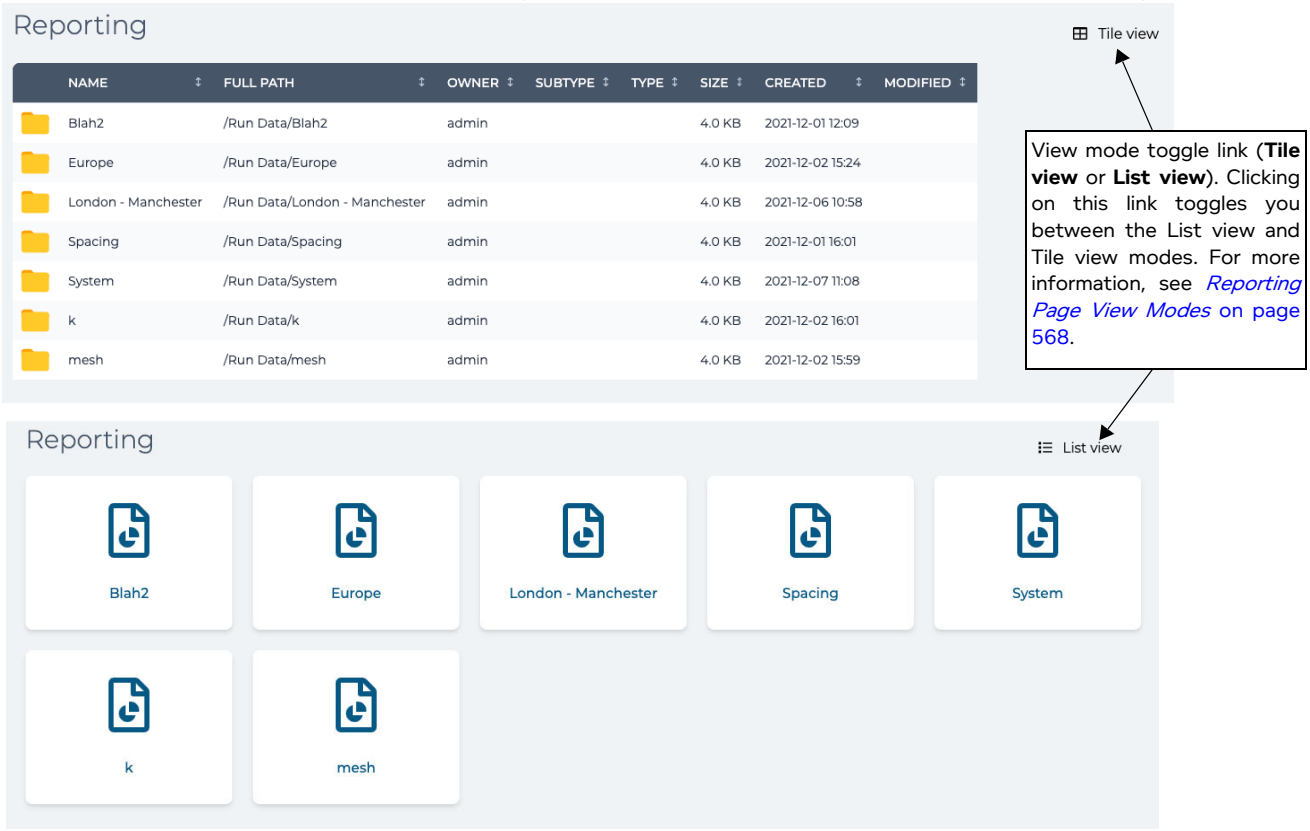
Note:

Compared to active networks, the basic graphs from historical networks are static and do not move with time. This is normal as the basic graphs from historical networks contains the accumulated packet statistics that were acquired while the network was run.

6-3. The Reporting Page

The **Reporting** page (see *Illustration 175*) appears after clicking the **Reports** panel from within the **Reports And Graphs** page (see *Illustration 167* on page 555), and lists all (i.e. active and inactive) the networks and scenarios that have been created on the NE-ONE.

ILLUSTRATION 175 - REPORTING PAGE (DEFAULT LIST VIEW ABOVE, TILE VIEW BELOW)



The **Reporting** page acts as an entry point for each network/scenario, letting you drill down and navigate to one of the report types for a particular network/scenario (see *Illustration 177*).

Note:
The **Reporting** page operates in a similar way to the File Browser in terms of navigation, however, its navigation is limited to within the `/Run Data` directory and lower level directories. This is normal, as all reporting data is found within the `/Run Data` directory.

Note:
Reports are associated to the user that launched the network, and are thus only visible to that user. For example, the reports generated during the runtime of a network launched by the user with user name user1, will only be visible to the user1. If a different user (e.g. user2) logs in to the Web Interface, the reports related to the networks launched by another user (e.g. user1) are not visible.

6-3-1. Reporting Page View Modes

- **List view** : This is the default view mode that appears when the **Reporting** page opens. This view mode shows the directories and files organized in a convenient list, whose order can be sorted (see *Illustration 175* as an example). Clicking on a column header orders the list of files according to the type of column header category. For example, clicking on the **Name** column header sorts by alphabetical order, toggling between starting with A and ending with Z, or starting with Z and ending

with A. Similarly, you can sort by file path, owner, etc. When in this view mode, the **Tile view** toggle link is available letting you switch to the tile view mode.

- **Tile view** : This view mode shows the directories and files organized in tiles, next to each other. When in this view mode, the **List view** toggle link is available letting you switch to the list view mode.

ILLUSTRATION 176 - REPORTING PAGE (TOP LEVEL (RUN DATA) DIRECTORY PATH IN LIST VIEW MODE)

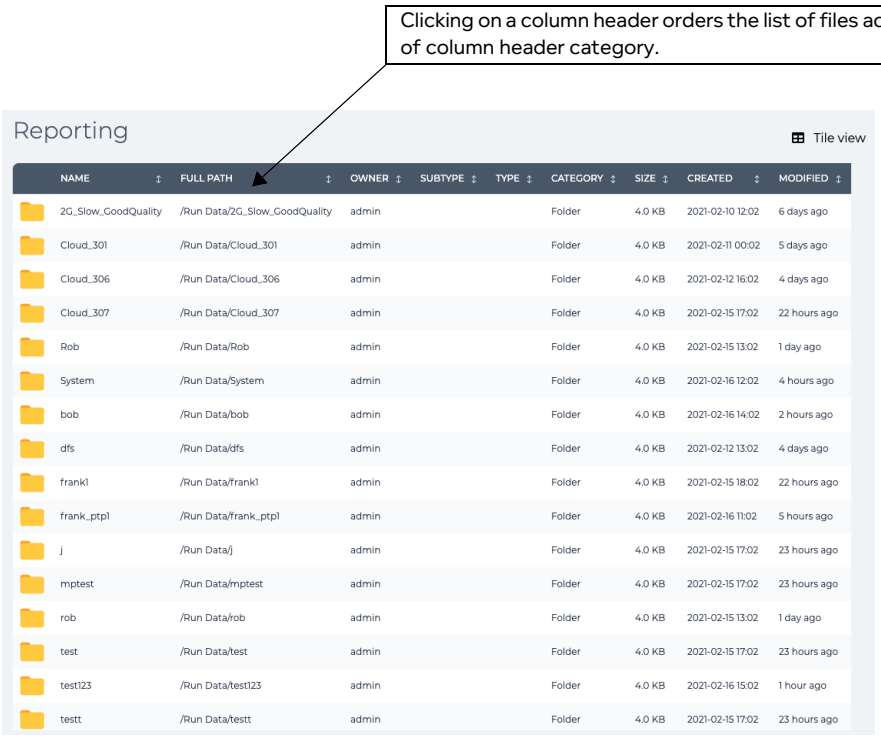
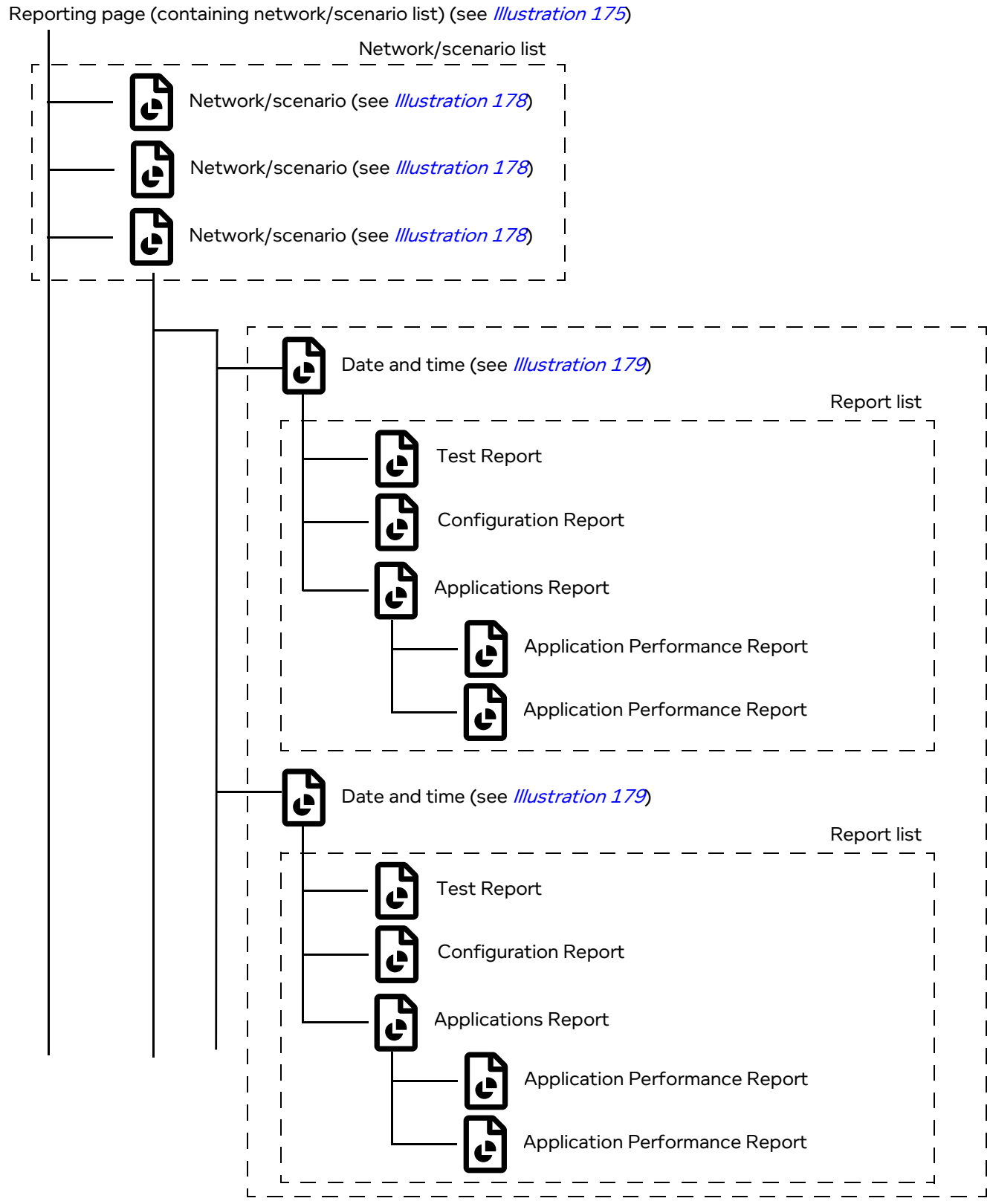


ILLUSTRATION 177 - REPORTING PAGE NAVIGATION PRINCIPLES



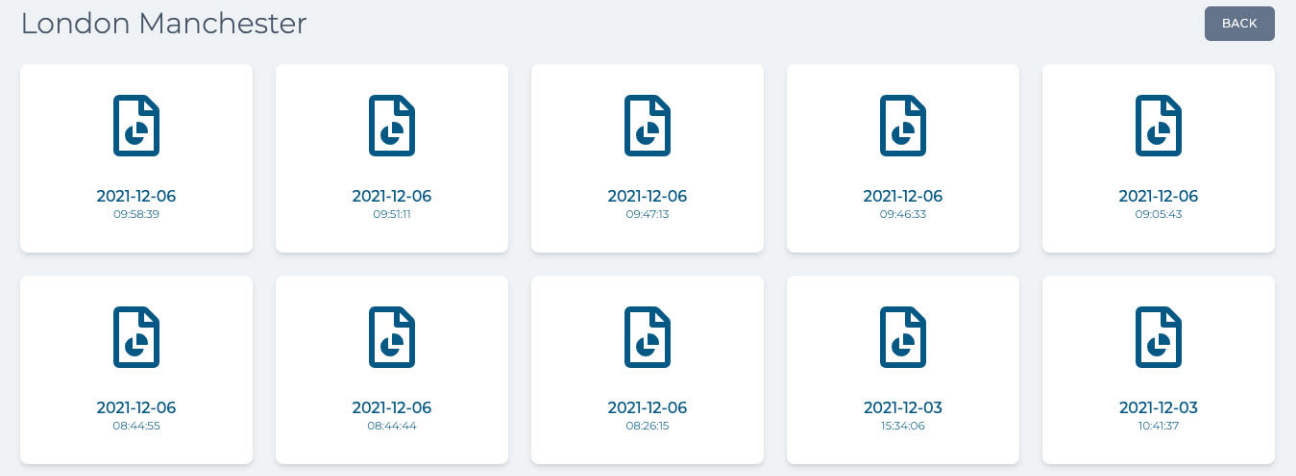
6-3-2. Navigating the Reporting Pages

Clicking on a network/scenario in the **Reporting** page opens a **Report Group** page (see *Illustration 178*) for that network/scenario, which contains a list of report groups organized by date and time. A report group is created and exists for each time a network/scenario is run. Each report group contains different report types for the duration of a network's or scenario's runtime.

Note:

If a network/scenario has not yet run, then the network's/scenario's **Report Group** page is empty. This is normal, and it only contains report groups once the network/scenario is run.

ILLUSTRATION 178 - REPORT GROUP PAGE (POPULATED)



Clicking on the **BACK** button in the **Report Group** page returns you to the **Reporting** page (see *Illustration 175*).

Clicking on a report group in the **Report Group** page opens a **Report Type** page (see *Illustration 179*), which contains a list of the following report types:

- Configuration Report

  This is a standard report available to all NE-ONEs. It provides all relevant configuration information so that you know how the test network was configured during the test run.
- Test Report

  This is a standard report available to all NE-ONEs. It provides all relevant test information so that you know how the test network was used during the test run, including historical bandwidth usage on the tested ports.
- Applications Report (which inside additionally contains an Application Performance Report)

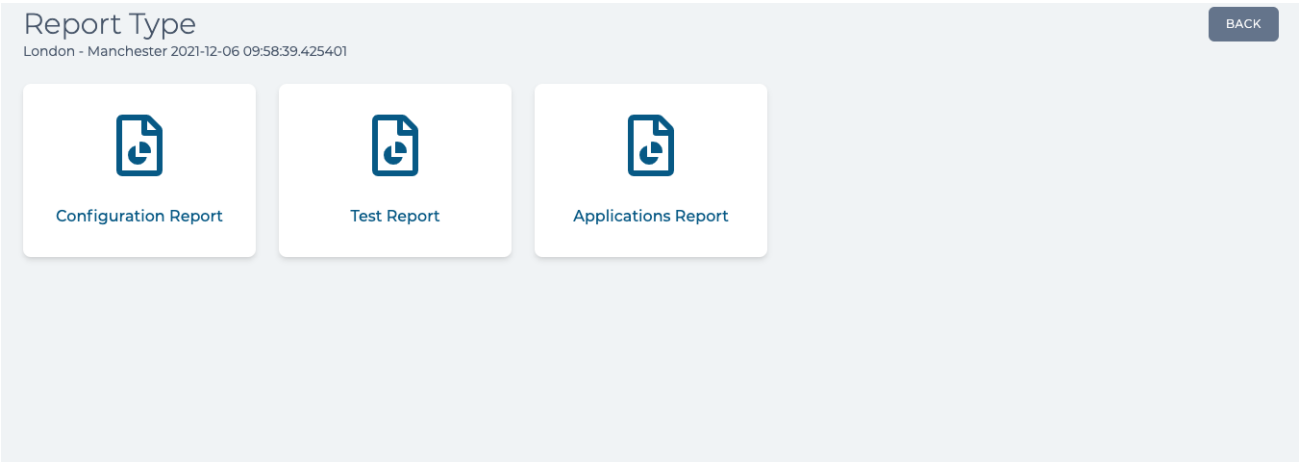
  These reports use built-in expert knowledge to predict how sensitive the applications under test are to bandwidth and latency. These reports include red, orange, amber and green indicators to help you to easily identify which applications need reviewing.

  The Application Performance Report will predict how an application will perform over a range of latencies, and highlight any applications that could experience problems in red or orange.

Note:

All NE-ONEs come with the standard high-level report types Configuration Report and Test Report, which tell you what happened during the test. The and Applications Report and Application Performance Report is a premium reporting feature, which tell you if your applications are network ready. Depending on your license, the Application Performance Report may be either activated or deactivated.

ILLUSTRATION 179 - REPORT TYPE PAGE



6-3-3. Viewing and Downloading Reports

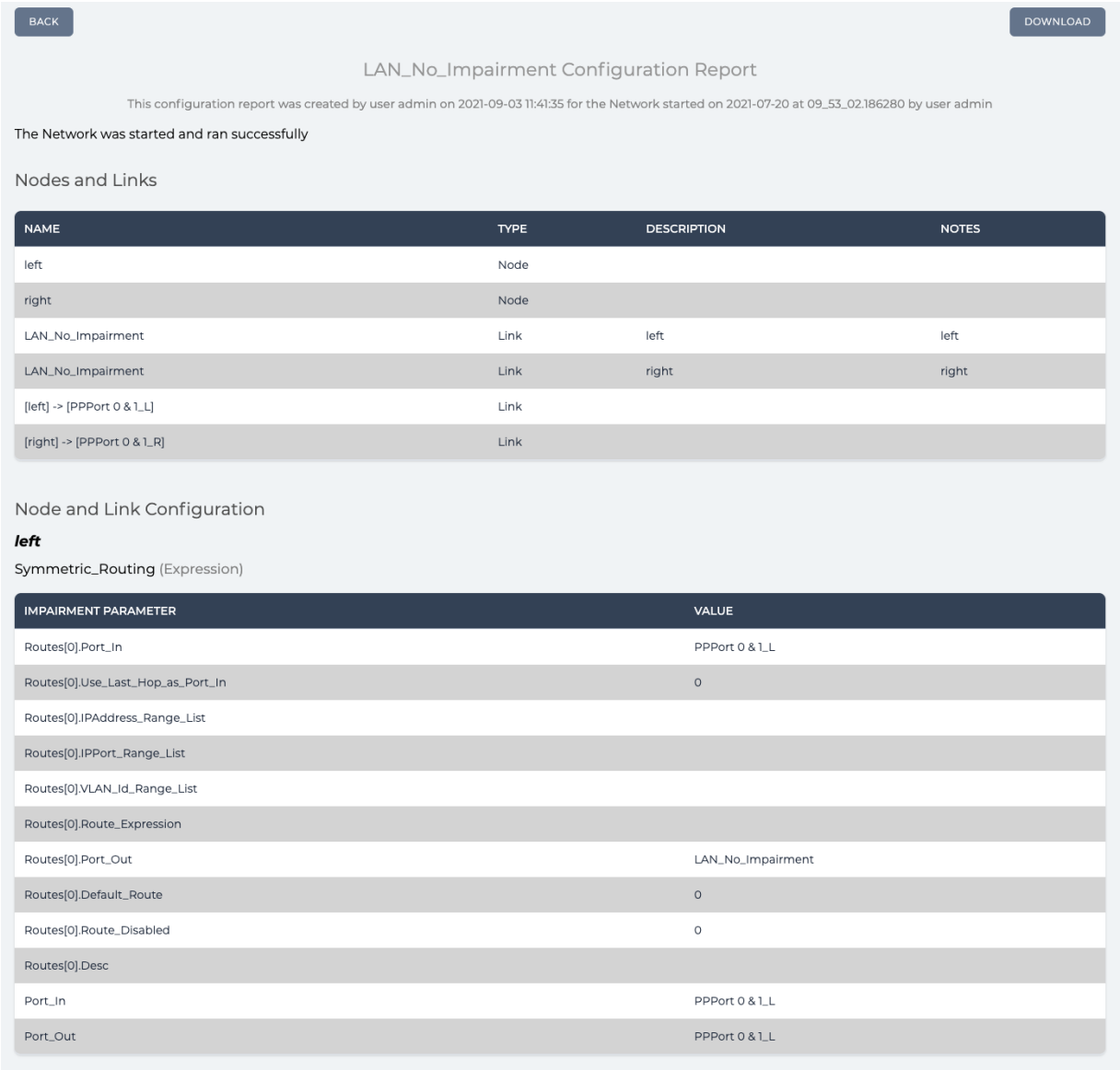
Clicking on the appropriate report tile (**Configuration Report**, **Test Report**, **Applications Report**) in the **Report Type** page (see *Illustration 179*) opens the chosen report.

Clicking on the **BACK** button in the **Report Type** page returns you to the **Report Group** page (see *Illustration 178*).

6-3-3-1. Viewing and Downloading Configuration Reports

Clicking on the **Configuration Report** tile within the **Report Type** page (see *Illustration 179*) opens the **Configuration Report** page (see *Illustration 180*).

ILLUSTRATION 180 - CONFIGURATION REPORT PAGE



The **Configuration Report** page contains the following buttons:

- **BACK** button, upon clicking returns you to the **Report Type** page (see *Illustration 179*).
- **DOWNLOAD** button, upon clicking opens a dialog box, from where you can choose locally on your computer where to download a report in DOCX format.

6-3-3-2. Viewing and Downloading Test Reports

Clicking on the **Test Report** tile within the **Report Type** page (see *Illustration 179*) opens the **Test Report** page (see *Illustration 181*).

ILLUSTRATION 181 - TEST REPORT PAGE

The **Test Report** page contains the following buttons:

- **BACK** button, upon clicking returns you to the **Report Type** page (see *Illustration 179*).
- **DOWNLOAD** button, upon clicking opens a dialog box, from where you can choose locally on your computer where to download a report in DOCX format.

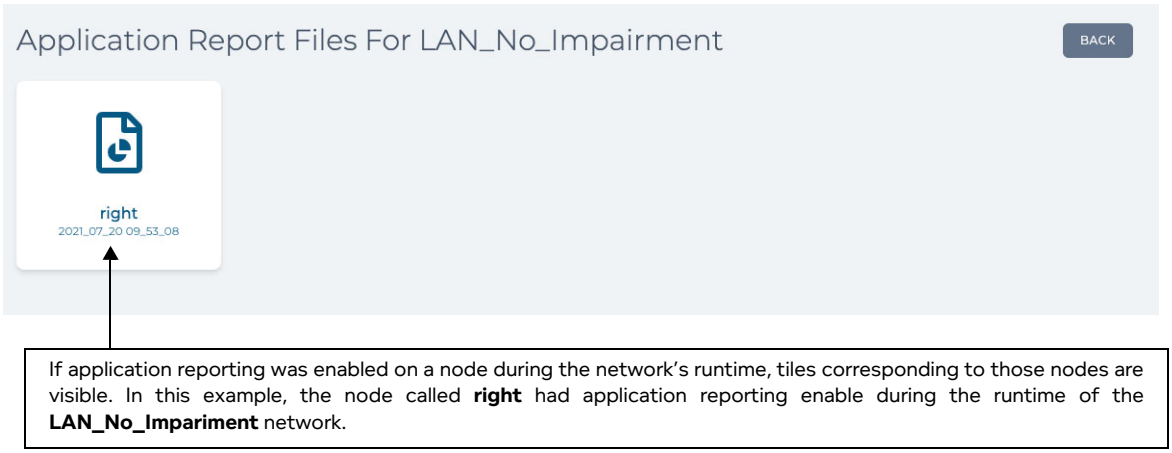
6-3-3-3. Viewing and Downloading Application Reports

Note:

The and Applications Report and its associated Application Performance Report is a premium reporting feature. Depending on your license, the Application Report may be either activated or deactivated.

Clicking on the **Applications Report** tile within the **Report Type** page (see *Illustration 179*) opens the **Application Report Files** page (see *Illustration 182*) relating to the originally selected network/scenario.

ILLUSTRATION 182 - APPLICATION REPORT FILES PAGE



Application report files rapidly grow to a large file size. As a result, by default application reporting is disabled on all nodes, and remains disabled until you have enabled application reporting on each node within your network.

The **Application Report Files** page contain **<node name>** tiles for each of the nodes that have had their **Reporting** switch enabled within their **Edit node** panel (see *Reporting switch* on page 250 for Point-to-Point network nodes, and see *Reporting switch* on page 320 for Multi-Point network nodes).

Note:

It can be normal that **Application Report Files** page contains no **<node name>** tiles for any given network runtime. Standard reports (i.e. Configuration reports and Test reports) always get generated for any given network runtime. If the **Application Report Files** page contains no **<node name>** tiles it simply means that during the runtime of the selected network, none of the associated network nodes had application reporting enabled

Clicking on a **<node name>** tile within the **Application Report Files** page opens the **Application Report** page (see *Illustration 183*) associated with the node.

The **Application Report** page contains the following buttons:

- **BACK** button, upon clicking returns you to the **Report Type** page (see *Illustration 179*).
- **DOWNLOAD** button, upon clicking opens a dialog box, from where you can choose locally on your computer where to download the application report in DOCX format.

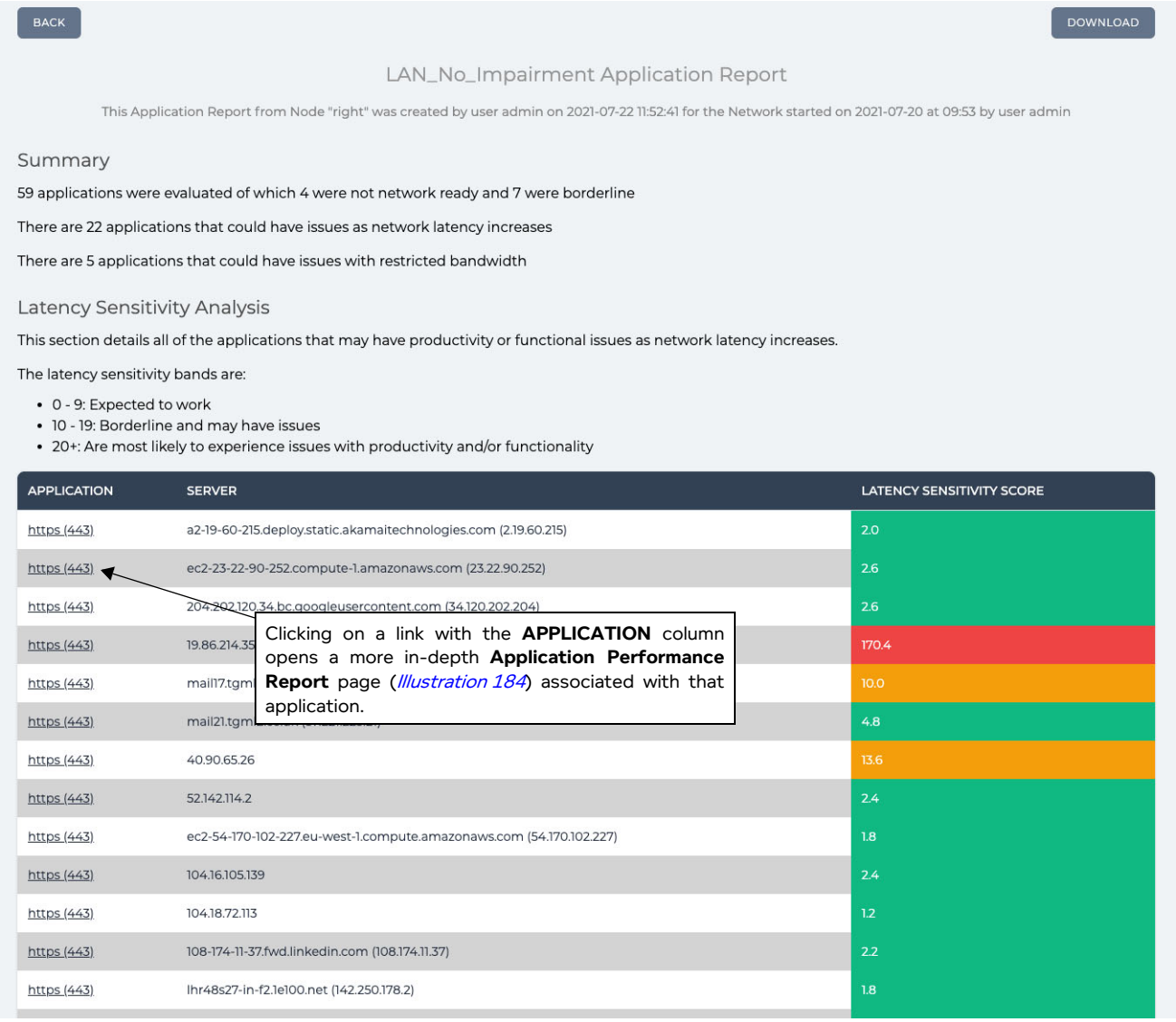
Compared to the standard reports (i.e. Configuration reports and Test reports), the **Application Report** page contains the following sections providing extremely important network metrics information:

- **Summary** section: contains a useful high-level summary such as indicting the number of applications that:
  - are not network ready
  - are borderline to being network ready
  - could have issues as network latency increases

  - could have issues with restricted bandwidth
- **Latency Sensitivity Analysis** section: contains a table with an extremely useful color coded latency sensitivity score for each application (e.g. https (443), sftp (22), etc.) that was tested during network's runtime.
- **Bandwidth Sensitivity Analysis** section: contains a table with an extremely useful color coded bandwidth sensitivity score for each application (e.g. https (443), sftp (22), etc.) that was tested during network's runtime.
- **Network Ready Analysis** section: contains a table with the following extremely useful color coded scores for each application (e.g. https (443), sftp (22), etc.) that was tested during network's runtime:
  - network readiness score
  - latency sensitivity score
  - bandwidth sensitivity score

  The table also includes the following for each application that was tested during network's runtime:
  - data sent by client (bytes)
  - data received by client (bytes)
  - peak bandwidth (bits per second)

ILLUSTRATION 183 - APPLICATION REPORT PAGE



Clicking on an application within the **APPLICATION** column within either the **Bandwidth Sensitivity Analysis**, **Bandwidth Sensitivity Analysis**, or **Network Ready Analysis** section opens a **Application Performance Report** page (see *Illustration 184*), which provides more in-depth application performance reporting information associated with that application.

ILLUSTRATION 184 - APPLICATION PERFORMANCE REPORT PAGE

The **Application Performance Report** page contains the following buttons:

- **BACK** button, upon clicking returns you to the **Application Report** page (see *Illustration 183*).
- **DOWNLOAD** button, upon clicking opens a dialog box, from where you can choose locally on your computer where to download the application performance report in DOCX format.

CHAPTER 13 THE FILE BROWSER

1. INTRODUCTION

This chapter is applicable to all users, and describes the use of the NE-ONE's File Browser.

The File Browser (see *Illustration 185*) lets you navigate within different directories of the NE-ONE's local filing system, and perform a host of useful actions via a pop-up menu (*Illustration 186*) when the right mouse button is clicked. The File Browser page supports two different view modes (see *File Browser View Modes* on page 585).

ILLUSTRATION 185 - FILE BROWSER (INITIAL PRIVATE DIRECTORY PATH IN TILE VIEW)

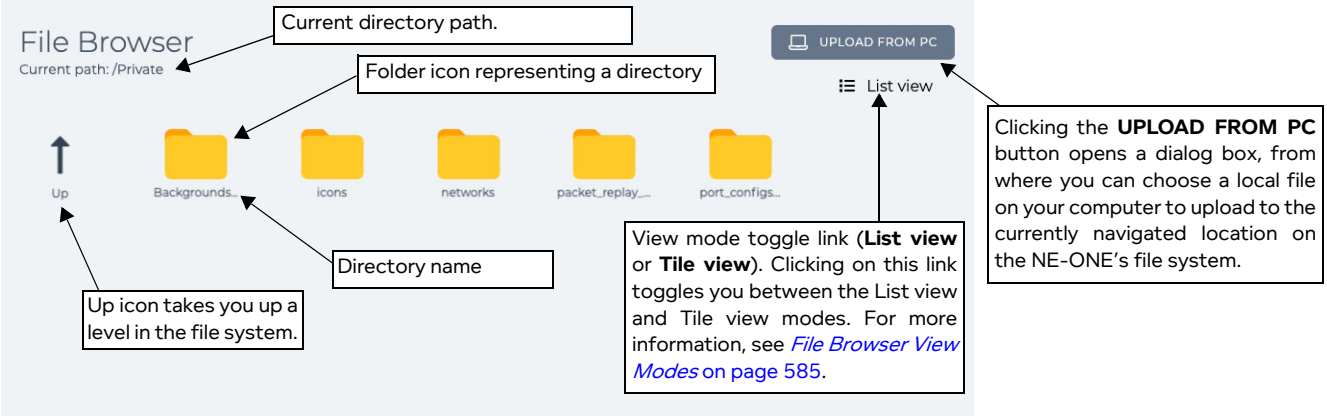
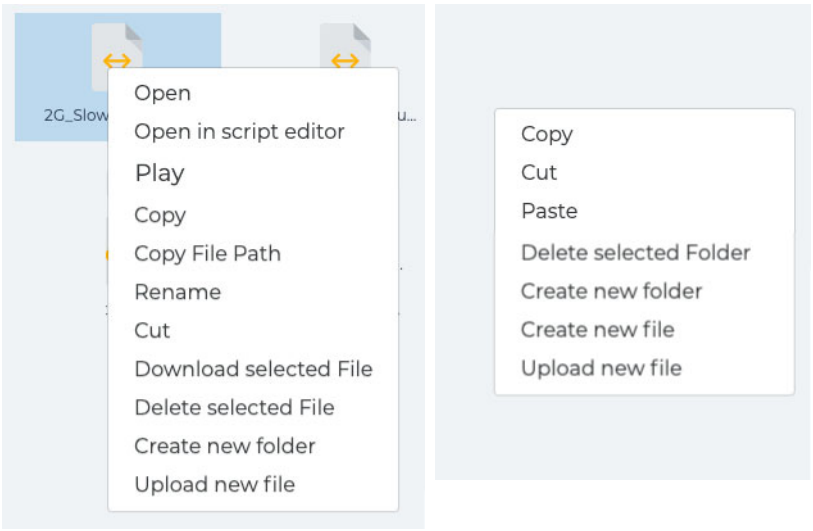


ILLUSTRATION 186 - FILE BROWSER POP-UP MENU (VARIES ACCORDING TO WHERE YOU CLICK)



By default, when the **File Browser** page opens it automatically navigates within, and shows the contents of the `/Private` directory. This is normal, as in most cases you perform the majority of file management actions withing your `/Private` directory.

1-1. Launching the File Browser

To launch the **File Browser** page, click **Management > ··· Platform Settings > File Browser**.

1-2. Navigating Within The File Browser

The File Browser contains folder icons to represent directories, and file icons to represent files. When you have drilled down within a lower level directory (i.e. not at the top level directory), the File Browser also displays an **Up** arrow icon .

- Double clicking on a folder icon takes you down one level into the directory represented by the folder.
- Double clicking the **Up** arrow icon takes you up one directory level.
- Double clicking on a network file results in opening the network (for more information, see *Opening a Point-to-Point Type Network From the File Browser* on page 589, and *Opening a Point-to-Point Type Network From the File Browser* on page 589).
- Double clicking on a scenario file results in opening the scenario (for more information, see *Opening a Scenario From the File Browser* on page 590).

1-3. File Browser Directories

The directories that are visible depend on the user type logged into the Web Interface. *Table 70* summarize each of the top level directories, and indicates which user type they are accessible to.

TABLE 70 - TOP LEVEL FILE SYSTEM DIRECTORIES

Top Level Directory	Description	Access ?	
		Admin	Non Admin
`Backup`	Contains backup files that were wither created by an admin user on the **Backup** page (see *Backing up the System* on page 220) or uploaded by an admin user on the **Restore** page (see *Restoring a System Backup* on page 223).	Read Write	Not Visible
`Library`	Contains system library directories and files relating to the customization of the network elements used by the Network Designer in the Web Interface: • `Backgrounds` : contains `*.png` (and `*.jpg`) image files for each of the backgrounds that can be used in a network. An admin user can add more or delete existing backgrounds (see *Customizing the Web Interface Background and Node Icons* on page 586). • `countries` : files and directories associated with the country data used by the networks. These files must never be changed, moved or deleted. • `customer_countries` : contains `<country code>.tsv` files corresponding to custom locations that can be created and grouped within a particular country. An admin user can create custom locations. For more information, see *Importing Already Created Custom Locations to Other NE-ONEs* on page 87. • `documentation` : contains the Calnex end user agreement which a user will view and accept the first time they login to the NE-ONE, and this User and Administration Guide. It may also contain a custom User Acceptance Document if the admin user has applied an Audit and Compliance Agreement according to *Applying a Compliance and Audit Acceptance Agreement* on page 73. • `networks` : contains an `Examples` directory, which contain `*.itn` files for each of the example networks. These files can be edited by an admin user using the Script Editor. For more information, see *Chapter 14*, *Using The Script Editor* on page 599. • `LCD` : this is only present on NE-ONE Desktop versions which have an LCD panel. This directory is initially empty. When populated with network (`*.itn`) files and scenario (`*.its`) files, those networks and scenarios are accessible via the LCD panel. For more information, see *Making Networks and Scenarios Accessible to the LCD Panel* on page 596. • `icons` : initially contains a contains a `nodes.zip` file, which contains `*.png` image files for each of the icons that are used to represent a node in a network. An admin user can customize existing node icons if required (see *Customizing the Web Interface Background and Node Icons* on page 586).	Read Write	Read

Top Level Directory	Description	Access ?	
		Admin	Non Admin
`Run Data`	Contains directories for each of the networks and scenarios that exist on the NE-ONE and their associated network objects (i.e. links and nodes). Within each directory are other date and time stamped sub-directories which correspond to when the network/scenario was run. Each of these date and time stamped sub-directories contain the following files: • an SQL lite database file, which contains all the statistics of the network which is used for reporting (associated with the link or node network objects of the network/scenario) • if packet capture has been run on one or more network objects belonging to the network/scenario, a packet capture (`*.pcap`) file for each of the chosen packet capture types will exist with the file name format summarized in *Table 65* on page 535. For more information on packet capturing, see *Launching Packet Capture on a PPO* on page 532 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.	Read Write	Read Write
`Run Data/ System`	Contains directories for each of the networks and scenarios that exist on the NE-ONE their associated framework objects (i.e. hardware port, software port, port container and service). Within each directory are other date and time stamped sub-directories which correspond to when the network/scenario was run. Each of these date and time stamped sub-directories contain the following files: • an SQL lite database file, which contains all the statistics of the network which is used for reporting (associated with the hardware or soft ports used by the network/scenario) • if packet capture has been run on one or more framework objects associated with the network/scenario during its run-time, a packet capture (`*.pcap`) file for each of the chosen packet capture types will exist with the file name format summarized in *Table 65* on page 535. For more information on packet capturing, see *Launching Packet Capture on a PPO* on page 532 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*.	Read Write	Not Visible

Top Level Directory	Description	Access ?	
		Admin	Non Admin
`Private`	Directory used for private use, which is only visible to the currently logged in user. This directory contains a `networks` sub-directory, which stores the files of any networks (`*.itn`) or scenarios (`*.its`) that the user has created. If this directory contains an `icons` sub-directory with `*.png` image files, `*.jpg` image files, or a `*.zip` file (who's contents include `*.png` or `*.jpg` image files), those images will appear in the **Private** list of selectable node icons for that user. For more information, see *Illustration 75* on page 251 in the *Editing a Node via the Edit Node Panel (Point-to-Point Networks)* section of *Chapter 9*, *Creating and Running Point-to-Point Networks* and *Illustration 89* on page 322 in the *Editing a Node via the Edit Node Panel (Multi-Point Networks)* section of *Chapter 10*, *Creating and Running Multi-Point Networks*. If this directory contains a `Backgrounds` sub-directory with `*.png` image files or `*.jpg` image files, those images will appear as additional available backgrounds in the Multi-Point Designer for that user. For more information, see the *The Workspace Background Image* section of *Chapter 10*, *Creating and Running Multi-Point Networks*. This directory also contains system diagnostics files that get generated after running a system diagnostics. For more information, see *Running Diagnostics* on page 226 in *Chapter 7*, *System Maintenance*. This directory also contains a `port_configs` directory, which may contain files corresponding to saved port configurations. For more information, see *Saving a Ports Configuration* on page 152 and *Copying Ports Configurations Between Different NE-ONEs* on page 154 of *Chapter 5*, *Ports and Services Management*. This directory also contains a `packet_replay_files` directory, which may contain packet capture (pcap) files that can be used for detailed testing using the packet replay functions. For more information, see *Chapter 15*, *Packet Input Functions*.	Read Write	Read Write
`Public`	Directory used for different users to publicly share with each other different files. For example, one user might create an example network, and choose to share it within this directory. If this directory contains an `icons` sub-directory with `*.png` image files, `*.jpg` image files, or a `*.zip` file who's contents include `*.png` or `*.jpg` image files), those images will appear in the **Public** list of selectable node icons. For more information, see *Illustration 75* on page 251 in the *Editing a Node via the Edit Node Panel (Point-to-Point Networks)* section of *Chapter 9*, *Creating and Running Point-to-Point Networks* and *Illustration 89* on page 322 in the *Editing a Node via the Edit Node Panel (Multi-Point Networks)* section of *Chapter 10*, *Creating and Running Multi-Point Networks*.	Read Write	Read Write
`Support`	Contains system and start-up and log files (`system.log` and `startup.log`). Log files can be viewed locally using the Script Editor. For more information, see *Chapter 14*, *Using The Script Editor* on page 599. Contains software update files if the NE-ONE has been updated according to *Updating the System Software* on page 217.	Read Write	Not Visible

1-4. File Browser Popup Menu

When you right mouse click on a directory or file within the File Browser, a pop-up menu (see *Illustration 186*) appears with a set of commands, described in *Table 71*. The set of menu commands that appear vary according to the file type that was selected.

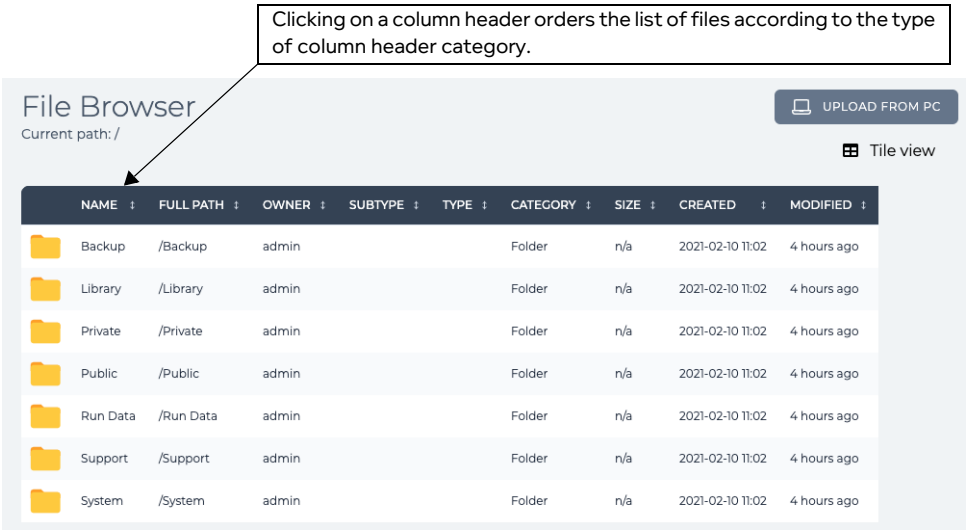
TABLE 71 - FILE BROWSER POPUP MENU COMMANDS

Command	Description
Open	Opens a network file (`*.itn`) or scenario file (`*.its`). **Note:** This menu option only appears when selecting a network file (`*.itn`) or scenario file (`*.its`).
Open in script editor	Opens a network file (`*.itn`) or scenario file (`*.its`) in an embedded Script Editor. For more information, see *Chapter 14*, *Using The Script Editor* on page 599. **Note:** This menu option does not appear when selecting a directory or background (i.e. no file).
Play	Directly plays a network file (`*.itn`) or scenario file (`*.its`). If the network is a type is Point-to-Point, you are also prompted to select the port pairs to use. **Note:** This menu option only appears when selecting a network file (`*.itn`) or scenario file (`*.its`).
Copy	Copies the file (temporarily in memory) so that the file can be pasted elsewhere within the file system via the File Browser.
Copy File Path	Copies the file path of the selected file into the clipboard of your computer. The copied file path can then be pasted from your computer's clipboard. This is useful for example when you want to specify a pcap file to be replayed using the packet replay functions. For more information, see *Chapter 15*, *Packet Input Functions*.
Cut	Copies the file (temporarily in memory), so that the file can be pasted elsewhere within the file system via the File Browser. Once pasted elsewhere within the file system, the file is removed from the original location.
Paste	Pastes a file that was either copied or cut to the currently navigated path of the file system.
Download selected File	Downloads the selected file to your computer's local file system. For more information, see *Downloading Files via the File Browser* on page 595.
Delete selected File/Folder	Opens a **Confirm delete** dialog box. Upon clicking the **OK** button, the selected file or folder is deleted from the NE-ONE's file system. For more information about deleting scenarios, Point-to-Point networks, and Multi-point networks, see *Deleting Scenarios* on page 524, *Deleting Point-to-Point Networks* on page 305, and *Deleting Multi-Point Networks* on page 501, respectively.
Create new folder	Opens a **New Folder** dialog box from where you can specify a directory name.
Create new file	Creates and empty file, which you can edit using the script editor. For more information on using the Script Editor, see *Chapter 14*, *Using The Script Editor* on page 599.
Upload new file	Opens a dialog box with a **SELECT A FILE** button, which lets you upload a file from your computer's local file system to the current File Browser location on the NE-ONE. **Note:** This has the same action as the **UPLOAD FROM PC** button that is located on the top, right of the File Browser.

1-5. File Browser View Modes

- **Tile view** : this is the default view mode that appears when the **File Browser** page opens. This view mode shows the directories and files organized in tiles, next to each other (see *Illustration 185* on page 579 as an example). When in this view mode, the **List view** toggle link is available letting you switch to the list view mode.
- **List view** : This view mode shows the directories and files organized in a convenient list, whose order can be sorted (see *Illustration 187* as an example). Clicking on a column header orders the list of files according to the type of column header category. For example, clicking on the **Name** column header sorts by alphabetical order, toggling between starting with A and ending with Z, or starting with Z and ending with A. Similarly, you can sort by file path, owner, etc. When in this view mode, the **Tile view** toggle link is available letting you switch to the tile view mode.

ILLUSTRATION 187 - FILE BROWSER (TOP LEVEL (/) DIRECTORY PATH IN LIST VIEW MODE)



1-6. File Types

The File Browser represents different file types with different icons. *Table 72* summarizes the File Types supported by the File Browser and the icon that is used to represent each file type.

TABLE 72 - FILE TYPES

File Type	File Extension	Icon	Description
Multi-Point Network	`*.itn`		Multi-Point type networks have the file extension `*.itn`.
Point-to-Point Network	`*.itn`		Point-to-Point type networks have the file extension `*.itn`.
Scenario	`*.its`		Scenarios have the file extension `*.its`. **Note:** Scenarios themselves are also networks. However to distinguish them within the filing system they have a different file extension.
Node icon	`*.png`		Node icons support the PNG and JPG image file type. If necessary, you can locally create customized node icons, upload them and share them with other users. For more information see *Customizing and Sharing Node Icon Files* on page 587.
Background image	`*.png`		Background images support the PNG and JPG image file type. If necessary, you can locally create customized background images, upload them and share them with other users. For more information see *Customizing and Sharing Background Files* on page 587.
ZIP file	`*.zip`		Node icon files can be compressed into a ZIP file. For example, all the PNG image files representing the node icon files delivered with the NE-ONE are located in a `nodes.zip` file within the `/Library/icons` directory.
Packet capture file	`*.pcap`		If packet capture has been run on one or more framework objects associated with the network/scenario during its run-time, a packet capture (`*.pcap`) file for each of the chosen packet capture types will exist in the `/Run Data/System` directory, with the file name format summarized in *Table 65* on page 535. For more information on packet capturing, see *Launching Packet Capture on a PPO* on page 532 in *Chapter 12*, *Statistics, Graphing, Reporting and Packet Capturing*. Packet capture (`*.pcap`) files can be copied to the `/Run Data/System` directory, and used for more detailed testing using the Packet Replay functions. For more information, see *Chapter 15*, *Packet Input Functions*.

2. CUSTOMIZING THE WEB INTERFACE BACKGROUND AND NODE ICONS

You can use the File Browser to customize (i.e. add additional or remove existing) background image files and node icon files that are used by the Network Designer.

2-1. Customizing and Sharing Background Files

Background files must adhere to the following specifications:

- File type : png or jpg
- Image size : no restrictions, but at least 800 pixels wide x 600 pixels high is recommended

Use the following steps to customize and share the background files.

1. Create or obtain an appropriate background file image meeting the background image specifications.
2. Launch the File Browser (click **Management > Platform Settings > File Browser**).
3. Navigate one of the following directories:
   - If you want the background image to only be available to you within the **Private** tab of the **Select Background** dialog box of the Multi-Point **Network Designer** page, navigate into your `/Private/Backgrounds` directory.
   - If you want the background image to available to all users from within the **Public** tab of the **Select Background** dialog box of the Multi-Point **Network Designer** page, navigate into the `/Public/Backgrounds` directory.
   - If you want the background image to available to all users from within the **Library** tab of the **Select Background** dialog box of the Multi-Point **Network Designer** page, navigate to the `/Library/Backgrounds` directory.

   Note:
   The **Select Background** dialog box that is invoked from the Multi-Point **Network Designer** page lists alphabetically all the background images from the `/Library/Backgrounds` directory first, followed by all the background images from the `/Public/Backgrounds` directory, followed by all the background images from the `/Private/Backgrounds` directory.
4. Click on the **UPLOAD FROM PC** button or right mouse click and select **Upload new file** from the pop-up menu that appears.

   A dialog box appears prompting you to select a file to upload.
5. Click the **SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the background file to upload. Then click **OK**.

   The background image file is now available from within either the **Library** tab, **Private** tab, or **Public** tab of the **Select Background** dialog box of the Multi-Point **Network Designer** page.

2-2. Customizing and Sharing Node Icon Files

Node icon files must adhere to the following specifications:

- File type : png or jpg (see note)
- Image size : 100 pixels wide x 80 pixels high

Note:
The JPG format supports palette-based images (of three 8-bit channels of RGB), but with no option of an alpha channel for transparency. The PNG format supports palette-based images (of three 24-bit channels of RGB or four 32-bit channels of RGBA), with the option of an alpha channel for transparency. Therefore, because the PNG format supports transparency, for aesthetic purposes Calnex recommend that you create any custom node icons in the PNG format because they can be created with a transparent background.

Note:
The NE-ONE has the ability to automatically parse and know the contents of a `*.zip` file. Therefore, if you intend share many node icon files, Calnex recommend that you organize all of your node icon files into a directory, then compress it into `*.zip` file. Using the procedure below, you

can then upload the compressed `*.zip` file once, instead of uploading multiple node image files one by one.

Use the following steps to customize and share the node icon files.

1. Create or obtain an appropriate node image file image adhering to the node image specifications above.

   Ensure that the filename of the image has the following format:

   `<node icons panel category>-<desciption>.png` for PNG files

   or

   `<node icons panel category>-<desciption>.jpg` for JPG files

   where:

   - `<node icons panel category>` must match one of the following categories that are available **Node Icons** panel of the Multi-Point Network Designer page (*Illustration 87* on page 318): `Standard`, `Gaming`, `IoT`, `LAN`, `Military`, `Radio`, or `WAN`.
   - `<description>` is something meaningful representing the node type, and only contain alphanumeric characters.
2. Optionally (but highly recommended), organize all of the node image files into a directory, and compress the contents of that directory into a `*.zip` file. The `*.zip` file can be called anything with alpha-numeric characters. For example, `nodes.zip`, `nodeicons.zip`, or `MyNodeIcons.zip`, etc.
3. Launch the File Browser (click **Management > Platform Settings > File Browser**).
4. Navigate one of the following directories:
   - If you want the node icon(s) to only be available to you within the **Private** tab of the **Node Icon** dialog box and **Node Icons** panel, navigate into your `/Private/icons` directory.
   - If you want the node icon(s) to available to all users from within the **Public** tab of the **Node Icon** dialog box and **Node Icons** panel, navigate into the `/Public/icons` directory.
   - If you want the node icon(s) to available to all users from within the **Library** tab of the **Node Icon** dialog box and **Node Icons** panel, navigate to the `/Library/icons` directory.

   Note:

   All users (i.e. admin and non-admin type) can access the `/Public/icons` directory. However, only an admin type user can the `/Library/icons` directory.
5. Click on the **UPLOAD FROM PC** button or right mouse click and select **Upload new file** from the pop-up menu that appears.

   A dialog box appears prompting you to select a file to upload.
6. Click the **SELECT A FILE** button, and from the dialog box that appears, navigate your local filing system and choose the node icon file to upload. Then click **OK**.

   Note:

   If you had optionally used step 2 to organize all of your node icon files into a directory, then compress them into a single `*.zip` file, navigate your local filing system and choose the `*.zip` file to upload.
7. If necessary, repeat step 6 for each node icon file that you want to upload.

   The uploaded node icons are now available from within either the **Library** tab, **Private** tab, or **Public** tab of the **Node Icon** dialog box of the Point-to-Point Network Designer (*Illustration 75* on page 251), the **Node Icon** dialog box of the Multi-Point Network Designer (*Illustration 89* on page 322) and **Node Icons** panel in the Multi-Point Network Designer (*Illustration 87* on page 318).

3. OPENING AND PLAYING NETWORKS AND SCENARIOS VIA THE FILE BROWSER

The following sections describe how to open or directly play networks and scenarios from within the File Browser.

Note:
Closed networks are also available for opening from the **Example** and **Recent** and **Active** tabs of the **Home** page. Active networks are also available for opening from the **Active** tab of the **Home** page and from the Tray. You typically use the File Browser to open networks that are not available from the **Home** page (such as non-recent networks, and newly shared networks).

Note:
When you open a network or scenario from the File Browser it does not automatically play, but is opened in the corresponding network or scenario builder, from which it can be played if desired. If you want to directly play a network or scenario, you can use the **Play** menu option in the File Browser pop-up menu.

3-1. Opening a Point-to-Point Type Network From the File Browser

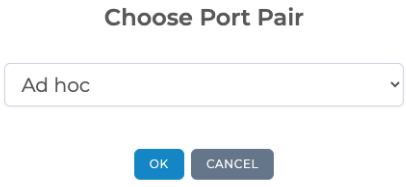
Use the following steps to open a Point-to-Point type network.

1. Launch the File Browser (click **Management > ··· Platform Settings > File Browser**).
2. Navigate one of the following directories:
   - If you want to open one of your own networks, navigate into your `/Private/networks` directory.
   - If you want to open a network shared by another user, navigate into the `/Public/networks` directory.
   - If you want to open an example network, navigate to `/Library/networks/Examples` directory.

   The File Browser updates with a list of all the network files (`*.itn`) and scenario files (`*.its`).
3. Double click on the file ↔ icon representing the Point-to-Point network that you want to open.

Note:
You can also right mouse click, and select **Open** from the pop-up menu that appears.

A **Choose Port Pair** dialog box appears prompting you to select a port pair on which you want to open the network.



4. From the dialog box, select an appropriate port pair, then click **OK**.

Note:
If you select the **Ad Hoc** port pair, two additional **Choose Left Port** and **Choose Right Port** dialog boxes appear, prompting you to select the left and right ports. In this case, select an a appropriate port in each of those dialog boxes, and click **OK**.

The Point-to-Point network opens in the **Network Designer** page, from where you can perform a whole host of network related tasks (i.e. editing, playing, etc.). For more information, see *Point To Point Designer Page for Point-to-Point Topologies* on page 242 in *Chapter 9*, *Creating and Running Point-to-Point Networks*.

Note:
Any of the example networks opened from the `/Library/networks/Examples` directory, will be saved to your `/Private/networks` directory upon saving.

Note:
Any of the publicly shared networks opened from the `/Public/networks` directory, will be saved to your `/Private/networks` directory upon saving.

3-2. Opening a Multi-Point Type Network From the File Browser

Use the following steps to open a Multi-Point type network.

1. Launch the File Browser (click **Management > Platform Settings > File Browser**).
2. Navigate one of the following directories:
   - If you want to open one of your own networks, navigate into your `/Private/networks` directory.
   - If you want to open a network shared by another user, navigate into the `/Public/networks` directory.
   - If you want to open an example network, navigate to the `/Library/networks/Examples` directory.

   The File Browser updates with a list of all the network files (`*.itn`) and scenario files (`*.its`).
3. Double click on the file icon representing the Multi-Point network that you want to open.

Note:
You can also right mouse click, and select **Open** from the pop-up menu that appears.

The Multi-Point network opens in the **Network Designer** page, from where you can perform a whole host of network related tasks (i.e. editing, playing, etc.). For more information, see *Multi-Point Designer Page for Multi-Point Topologies* on page 309 in *Chapter 9*, *Creating and Running Point-to-Point Networks*.

Note:
Any of the example networks opened from the `/Library/networks/Examples` directory, will be saved to your `/Private/networks` directory upon saving.

Note:
Any of the publicly shared networks opened from the `/Public/networks` directory, will be saved to your `/Private/networks` directory upon saving.

3-3. Opening a Scenario From the File Browser

Use the following steps to open a scenario.

1. Launch the File Browser (click **Management > Platform Settings > File Browser**).
2. Navigate one of the following directories:
   - If you want to open one of your own scenarios, navigate into your `/Private/networks` directory.
   - If you want to open a scenario shared by another user, navigate into the `/Public/networks` directory.

   The File Browser updates with a list of all the network files (`*.itn`) and scenario files (`*.its`).
3. Double click on the file icon representing the scenario that you want to open.

Note:
You can also right mouse click, and select **Open** from the pop-up menu that appears.

The scenario opens in the **Scenario Designer** page, from where you can perform a whole host of scenario related tasks (i.e. editing, playing, etc.). For more information, see *Chapter 11*, *Creating and Running Scenarios*.

Note:
Any of the example scenarios opened from the `/Library/networks/Examples` directory, will be saved to your `/Private/networks` directory upon saving.

Note:
Any of the publicly shared scenarios opened from the `/Public/networks` directory, will be saved to your `/Private/networks` directory upon saving.

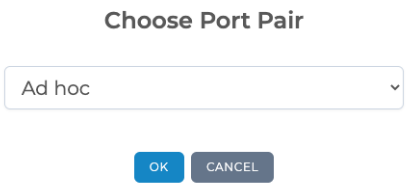
3-4. Directly Playing a Point-to-Point Type Network From the File Browser

Use the following steps to directly play a Point-to-Point type network.

1. Launch the File Browser (click **Management > ••• Platform Settings > File Browser**).
2. Navigate one of the following directories:
   - If you want to directly play one of your own networks, navigate into your `/Private/networks` directory.
   - If you want to directly play a network shared by another user, navigate into the `/Public/networks` directory.
   - If you want to directly play an example network, navigate to `/Library/networks/Examples` directory.

   The File Browser updates with a list of all the network files (`*.itn`) and scenario files (`*.its`).
3. Right mouse click on the file ↔ icon representing the Point-to-Point network that you want to play, and select **Play** from the pop-up menu that appears.

   A **Choose Port Pair** dialog box appears prompting you to select a port pair on which you want to play the network.



4. From the dialog box, select an appropriate port pair, then click **OK**.

Note:
If you select the **Ad Hoc** port pair, two additional **Choose Left Port** and **Choose Right Port** dialog boxes appear, prompting you to select the left and right ports. In this case, select an a appropriate port in each of those dialog boxes, and click **OK**.

The Point-to-Point network directly plays. It is not listed in the tray (as it is not open), but is listed within the **Active** tab of the **Home** page, from where it can be opened (if necessary).

3-5. Directly Playing a Multi-Point Type Network From the File Browser

Use the following steps to directly play a Multi-Point type network.

1. Launch the File Browser (click **Management > Platform Settings > File Browser**).
2. Navigate one of the following directories:
   - If you want to open one of your own networks, navigate into your `/Private/networks` directory.
   - If you want to open a network shared by another user, navigate into the `/Public/networks` directory.
   - If you want to open an example network, navigate to the `/Library/networks/Examples` directory.

   The File Browser updates with a list of all the network files (`*.itn`) and scenario files (`*.its`).
3. Right mouse click on the file icon representing the Multi-Point network that you want to play, and select **Play** from the pop-up menu that appears.

   The Multi-Point network directly plays. It is not listed in the tray (as it is not open), but is listed within the **Active** tab of the **Home** page, from where it can be opened (if necessary).

3-6. Directly Playing a Scenario From the File Browser

Use the following steps to directly play a scenario.

1. Launch the File Browser (click **Management > Platform Settings > File Browser**).
2. Navigate one of the following directories:
   - If you want to open one of your own scenarios, navigate into your `/Private/networks` directory.
   - If you want to open a scenario shared by another user, navigate into the `/Public/networks` directory.

   The File Browser updates with a list of all the network files (`*.itn`) and scenario files (`*.its`).
3. Right mouse click on the file icon representing the scenario that you want to play, and select **Play** from the pop-up menu that appears.

   The scenario directly plays. It is not listed in the tray (as it is not open), but is listed within the **Active** tab of the **Home** page, from where it can be opened (if necessary).

4. SHARING NETWORKS VIA THE FILE BROWSER

Networks can be publicly shared by copying them to either the `/Library/networks/Examples` directory or the `/Public/networks` directory. Only an admin type user has access to the `/Library/networks/Examples` directory. Whereas, all users have access to the `/Public/networks` directory.

Note:

If the `/Public/networks` directory does not exist, you can create it as follows:

1. Navigate to within the `/Public` directory.
2. Right mouse click and select **Create new folder**.
3. From the **Folder Name** dialog box that appears, type **`networks`** in the field, then click **OK**.

Use the following steps to share your network publicly with all users.

1. Launch the File Browser (click **Management > ··· Platform Settings > File Browser**).
2. Navigate into your `/Private/networks` directory.

   The File Browser updates with a list of all the networks (`*.itn`) and scenarios (`*.its`) you have previously created.
3. Right mouse click on the network file (`*.itn`) that you want to share, and select **Copy** from the pop-up menu that appears.
4. Navigate into one of the following directories as follows:
   - If you are an admin user, and want the shared network to be visible within the **Examples** tab within the **Home** page (*Illustration 3* on page 40), navigate to the `/Library/networks/Examples` directory.
   - If you are an anmin or non-admin user, navigate to the `/Public/networks` directory.
5. Right mouse click background within the File Browser, and select **Paste** from the pop-up menu that appears.

   A dialog box appears confirming that the network file was successfully copied.
6. From the confirmation dialog box, click **OK**.

   The dialog box closes.

   If the network file is copied to the `/Public/networks` directory it will be available to all users via the File Browser. All users will then be able to open the network according to *Opening a Point-to-Point Type Network From the File Browser* on page 589 or *Opening a Multi-Point Type Network From the File Browser* on page 590.

   If the network file is copied to the `/Library/networks/Examples` directory, it will be available to all users from within the **Examples** tab within the **Home** page (*Illustration 3* on page 40).

5. SHARING SCENARIOS VIA THE FILE BROWSER

Use the following steps to share your scenario publicly with all users.

1. Launch the File Browser (click **Management > ••• Platform Settings > File Browser**).
2. Navigate into your `/Private/networks` directory.
   The File Browser updates with a list of all the networks (`*.itn`) and scenarios (`*.its`) you have previously created.
3. Right mouse click on the scenario file (`*.its`) that you want to share, and select **Copy** from the pop-up menu that appears.
4. Navigate into the `/Public/networks` directory.
5. Right mouse click background within the File Browser, and select **Paste** from the pop-up menu that appears.
   A dialog box appears confirming that the scenario file was successfully copied.
6. From the confirmation dialog box, click **OK**.
   The dialog box closes.
   The scenario file is copied to the `/Public/networks` directory, and will be available to all users via the File Browser. All users will then be able to open the scenario according to *Opening a Scenario From the File Browser* on page 590.

6. DOWNLOADING FILES VIA THE FILE BROWSER

The File Browser lets you download files locally to your PC. The file download feature is useful in many situations, such as:

- Downloading log files and emailing them to your support representative or Calnex support for support purposes.
- Downloading packet capture files (`*.pcap`) for analysis in Wireshark.
- Downloading Point-to-Point and Multi-Point network files (`*.itn`) for local offline modification in a script editor, backup purposes, or for transferring to another NE-ONE.
- Downloading scenario files (`*.its`) for local offline modification in a script editor, backup purposes, or for transferring to another NE-ONE.

Note:

Although you can download and edit network and scenario files locally to a PC for offline editing in a script editor installed on your PC, Calnex recommends that you the NE-ONE's built-in script editor so that you can edit the network and scenario files directly. For more information on using the built-in script editor, see *Chapter 14*, *Using The Script Editor* on page 599.

Use the steps below download a file from the NE-ONE's filing system to your local PC:

1. Click **Management > Platform Settings > File Browser** to launch the File Browser.
2. Navigate to the appropriate directory and identify the file that you want to download.
   - For example, if you want to download a Multi-Point network file from your `/Private` directory, navigate to `/Private/networks` directory, and identify the Multi-Point network you want to download via its icon and its file name (`*.itn`).
   - For example, if you want to download a Point-to-Point network file from your `/Private` directory, navigate to `/Private/networks` directory, and identify the Point-to-Point network you want to download via its icon ↔ and its file name (`*.itn`).
   - For example, if you want to download a scenario file from your `/Private` directory, navigate to `/Private/networks` directory, and identify the scenario you want to download via its icon and its file name (`*.its`).
3. Right mouse click on the file, and selected **Download selected File** from the File Browser pop-up menu that appears.

7. MAKING NETWORKS AND SCENARIOS ACCESSIBLE TO THE LCD PANEL

This section is only applicable to NE-ONE Desktop version, which has an LCD panel. The NE-ONE Desktop version has an additional and special lcd user, that is needed in order to operate the LCD menu. The lcd user does not have access to the Web Interface, and is not managed via the Web Interface.

When users create networks (`*.itn`) and scenarios (`*.its`) the corresponding files get created in the user's `/Private/networks` directory. Any of the networks (`*.itn`) and scenarios (`*.its`) in the user's `/Private/networks` directory will be accessible via the Web Interface for either further editing, or running.

The LCD panel of the NE-ONE Desktop version can also be used to access any networks (`*.itn`) and scenarios (`*.its`) via the **Networks** main menu item (see *Networks* on page 698 in *Chapter 16*, *The LCD Panel*). This access is limited to querying existing active (i.e. running) networks/scenarios, and launching networks/scenarios so they are running in the background (i.e. active).

Any networks (`*.itn`) and scenarios (`*.its`) that are located in the `/Library/networks/LCD` directory will be accessible via the **Networks** main menu item of the LCD panel. However, by default, no networks or scenarios initially exist within the `/Library/networks/LCD` directory NE-ONE Desktop. Therefore, until a user's network/scenario is copied into the `/Library/networks/LCD` directory, no networks/scenarios will be accessible via the LCD panel.

If a user wants any of their networks and scenarios to also be quickly accessible for launching from the LCD panel, they must do the following:

1. Use the steps in *Sharing Networks via the File Browser* on page 593 to identify which networks (`*.itn`) they want to be accessible via the LCD panel, and copy them to the `/Public/networks` directory.
2. Use the steps in *Sharing Scenarios via the File Browser* on page 594 to identify which scenarios (`*.its`) they want to be accessible via the LCD panel, and copy them to the `/Public/networks` directory.
3. Communicate with an admin type user of the NE-ONE Desktop the filenames of the networks (`*.itn`) and scenarios (`*.its`) they have copied to `/Public/networks` directory.

The admin user will then need to undertake the following steps in order for the user's networks and scenarios to be accessible from the LCD panel:

1. Launch the File Browser (click **Management > ••• Platform Settings > File Browser**).
2. Navigate into the `/Public/networks` directory.

   The File Browser updates with a list of all the network (`*.itn`) and scenario (`*.its`) files that were previously shared by the user.

   Note:

   There may be filenames of networks (`*.itn`) and scenarios (`*.its`) from different users, so be careful to identify the correct filenames that were communicated to you by the user.
3. Perform the sub-steps below for each of the user's networks and scenarios that you want to make accessible to the LCD panel:
   a. Right mouse click on the network file (`*.itn`) or scenario file (`*.its`) that you want to make accessible to the LCD panel, and select **Copy** from the pop-up menu that appears.
   b. Navigate into the `/Library/networks/LCD` directory.

c. Right mouse click background within the File Browser, and select **Paste** from the pop-up menu that appears.

   A dialog box appears confirming that the network or scenario file was successfully copied.

d. From the confirmation dialog box, click **OK**.

   The dialog box closes.

   The network or scenario file is copied to the `/Library/networks/LCD` directory, and will now be accessible via the **Networks** main menu item of the LCD panel. Anyone with access to the LCD panel of the NE-ONE Desktop will now be able to check the current status and launch the copied network/scenarios. For more information, see *Networks* on page 698 in *Chapter 16*, *The LCD Panel*.

This page is intentionally left blank.

CHAPTER 14 USING THE SCRIPT EDITOR

1. INTRODUCTION

This chapter is applicable to non-admin and admin users, and describes the Web Interface and procedures related to using the script editor.

The script editor is an extremely useful built-in text editor, that lets you do a whole host of file viewing/ editing tasks directly on the files within the local filing system of the NE-ONE. The type of tasks you can perform are as follows:

- view log files (`*.log`)
- view and edit network files (`*.itn`)
- view and edit scenario files (`.*its`) - This is useful if you want to make elaborate scenarios that are not possible to make in the Scenario Builder. For example, you could initially create a scenario which loops back to the start network segment in the Automatic Scenario Builder, then modify it further within the Script Editor to put multiple loops to different network segments within the timeline (something that is not possible to construct within the Automatic Scenario Builder).

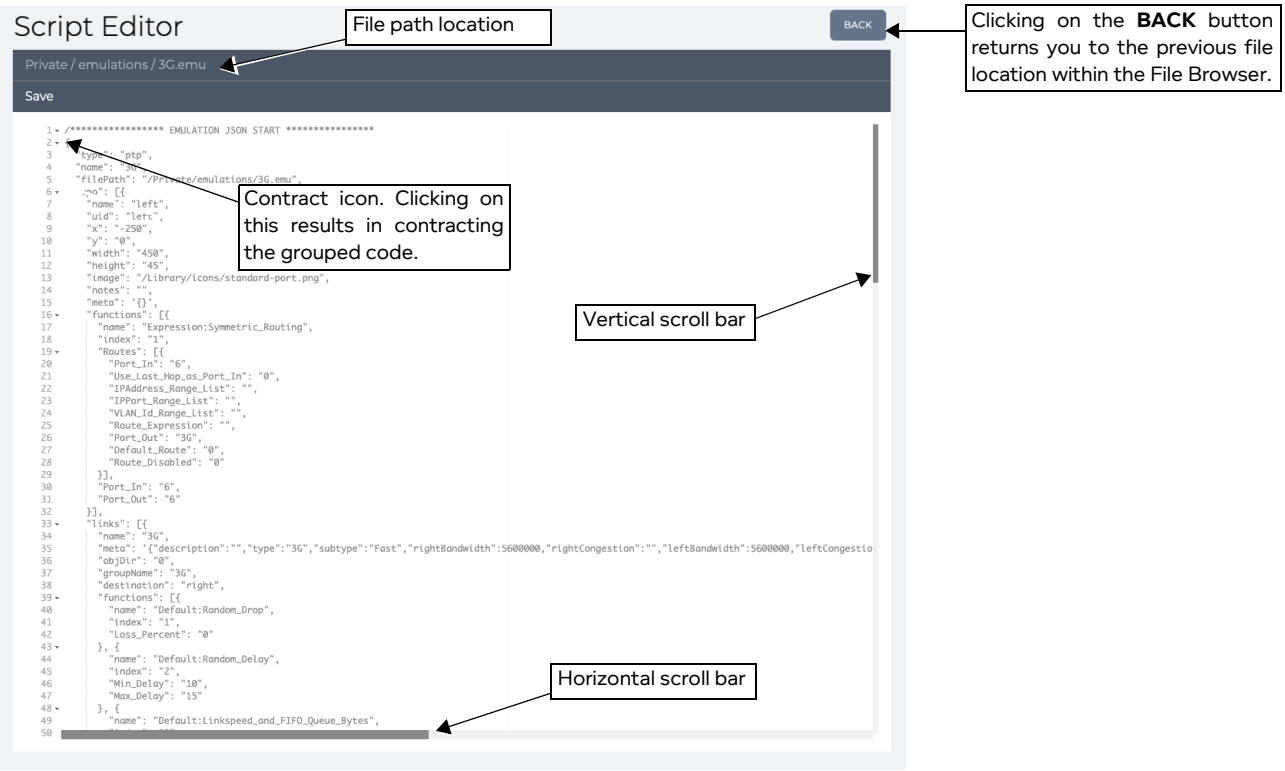
Note:

In order for the Automatic Scenario Builder to be active, the NE-ONE must have the Automatic Scenario Builder feature enabled in the license key.

2. THE SCRIPT EDITOR PAGE

The **Script Editor** page (see *Illustration 188*) appears after navigating within the File Browser, and right mouse clicking on a file, and selecting **Open in script editor** from the pop-up menu that appears.

ILLUSTRATION 188 - SCRIPT EDITOR PAGE



The contents of the **Script Editor** page varies according to the type of file you have selected for

viewing/editing. The **Script Editor** page contains the following:

- File Panel area, which contains the following:
  - File path location of the file that is currently open in the Script Editor.
  - **Save** link. Clicking this link saves the currently open file on the local filing system of the NE-ONE.

Note:
The **Save** link is only visible if you have the rights to write the file to the local file system. For example, the `<country code>.tsv` files located in the `/Library/customer_countries` directory is a read only file, so if you view a `<country code>.tsv` file with the Script Editor, the **Save** link is not visible.

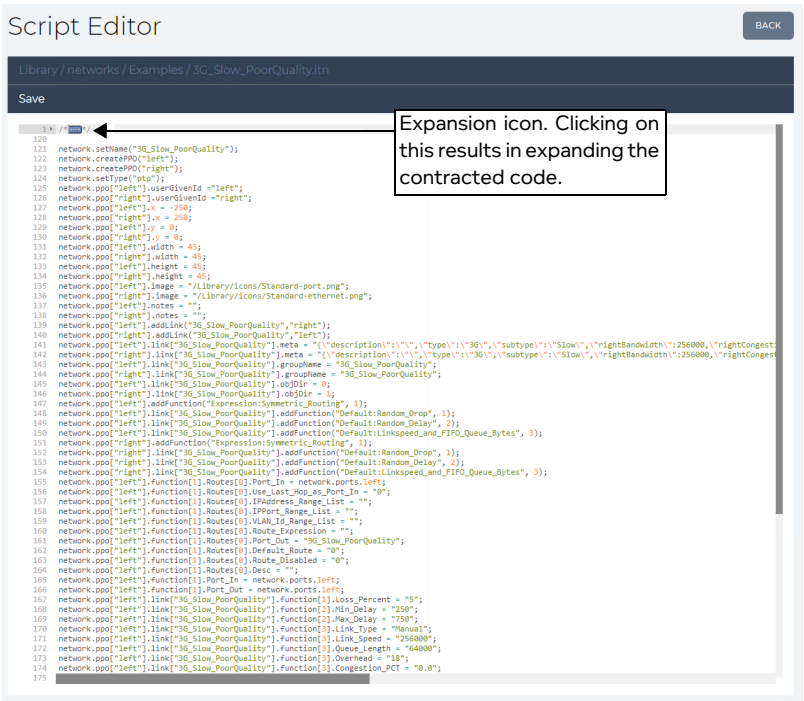
Note:
If the opened file is of JSON format, but all on one line an additional **Format JSON** link appears. Clicking the **Format JSON** link results in formatting the JSON file in a structured output over multiple lines.

- File Edit area, which contains the following:
  - Content of the file (displayed with color coding according to the syntax used inside the `*.itn`, `*.its`, and `*.log` files).
  - Horizontal and vertical scroll bars, letting you display the entire contents of the file.
  - Expand and contact icons letting you expand and contract areas within the file.

    Clicking on the contract icon results in contracting a grouped portion of the code within the Script Editor (see *Illustration 189* as an example).

    Clicking on the expand icon results in expanding a contracted portion of code within the Script Editor.

ILLUSTRATION 189 - SCRIPT EDITOR PAGE (START OF *.ITN FILE CONTRACTED)



Network files (`*.itn`) and scenario files (`*.its`) contain and easy to understand scripting language. It is beyond the scope of this document to describe the rules and syntax of this scripting language. For more information, refer to the *Network and Scenarios Scripting Language* document.

Note:

Before using the Script Editor to make changes on a network file (`*.itn`) or scenario file (`*.its`) on the NE-ONE, make a local backup by downloading the file to your PC. That way, if you make errors when directly editing the file on the NE-ONE, you have a local backup on your PC that you can use for re-uploading to the NE-ONE and for local file contents examination. For more information, see *Downloading Files via the File Browser* on page 595 in *Chapter 13*, *The File Browser* on page 579.

This page is intentionally left blank.

CHAPTER 15 PACKET INPUT FUNCTIONS

1. PASSIVE PACKET REPLAY AND INTELLIGENT PACKET REPLAY

The packet input functions let you to add additional traffic into your SDTNs by replaying selected packet streams from a packet capture (pcap) file, via the use of either the Passive Packet Replay function or Intelligent Packet Replay function, whose parameters are described within *Table 73*.

- The Passive Packet Replay function "passively" replays the selected packet streams, and does not care if the packets with the packet stream that are sent from the initiator endpoint node are received by the responder endpoint node. The original conversation (i.e. packet stream) from the pcap file will carry on playing out even if the packets are lost, slowed down, or arrive in the wrong order. In this case, the order of the packets from the original conversation (i.e. packet stream) from the pcap file are not respected.
- The Intelligent Packet Replay function "intelligently" replays the selected packet streams by monitoring the initiator and responder endpoint nodes. It knows when the responder endpoint node receives a packet from the initiator endpoint node so that the initiator endpoint node can send the next packet in original conversation (i.e. packet stream). In this case, the order of the packets from the original conversation (i.e. packet stream) from the pcap file are respected, and TCP backoff is recreated under the network conditions of the SDTN.

Note:
The Intelligent Packet Replay function is only available if your NE-ONE is licensed with the Advanced Packet Replay feature.

Note:
For brevity, unless specifically required, the Passive Packet Replay function and Intelligent Packet Replay function will be generically referred to as packet replay functions.

TABLE 73 - PASSIVE PACKET REPLAY AND INTELLIGENT PACKET REPLAY PARAMETERS

Parameter	Passive Packet Replay	Intelligent Packet Replay
Path field	The path to the pcap file within the NE-ONE file system that will be replayed.	
Running check box	Determines whether or not the pcap file is currently being replayed while the network is running. This check box lets you turn on and off the packet replay as required and thus determine if you want the additional traffic to be running on the network.	
End action drop-down field	Determines what action to take (either stop or loop) once the pcap file has finished being replayed.	
SELECT STREAMS (Point-to-Point) **STREAM CONFIGURATION** (Multi-Point)	Opens an interactive stream configuration tool (i.e. **Select Streams** dialog box (*Illustration 194* on page 612) and **Configure Stream Directions** dialog box (*Illustration 194* on page 612)), which let you determine which packet streams from the pcap file will be replayed in the generated traffic stream, and if necessary correct their directions. **Note:** On the Multi-Point Designer the use of interactive stream configuration tool invoked by clicking the **STREAM CONFIGURATION** button is optional, but recommended. You can choose not to use these stream configuration dialog boxes, and manually configure the filters and routing from the offset. However, for expediency, Calnex recommend that you use the stream configuration dialog boxes to initially configure the generated traffic stream, and if necessary, make further changes to the Filters and routing configuration.	

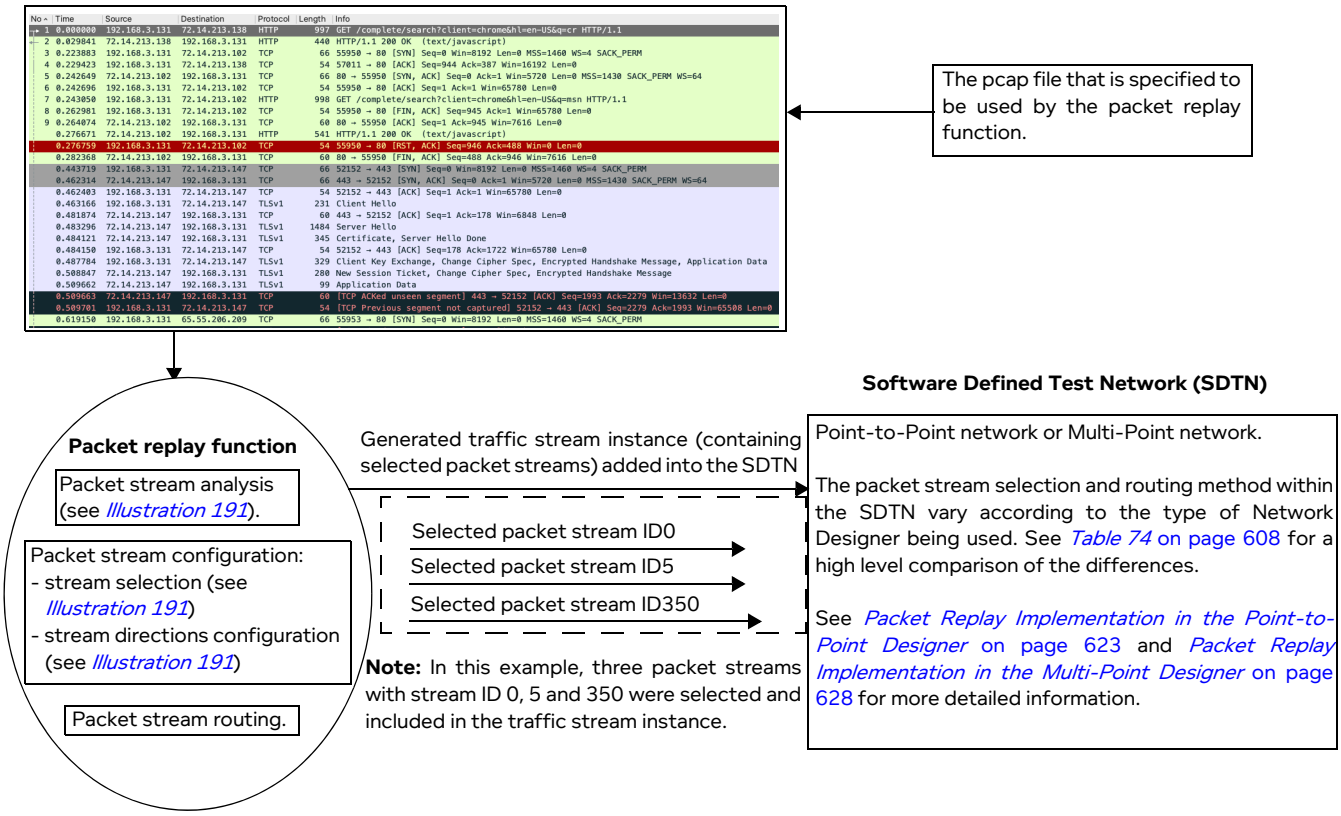
Parameter	Passive Packet Replay	Intelligent Packet Replay
Filters button (see note)	Opens a filters table (see *Illustration 211* on page 643 to *Illustration 214* on page 646), that optionally lets you define a set of filter criteria that is applied to the packet streams within the specified pcap file. The filter criteria that you define, and filter action that you select (i.e. either pass or drop) will determine which packet streams from the specified pcap file are used to generate the traffic stream. You can apply filters on the following criteria on the filtered packet streams: • **Source IP Address** - this must be either an IPv4 address using the dotted decimal format, or an IPv6 address using the hexadecimal segment format. • **Destination IP Address** - this must be an IPv4 address using the dotted decimal format, or an IPv6 address using the hexadecimal segment format. • **Source Port** - this must an integer value, defining the source port. • **Destination Port** - this must an integer value, defining the destination port. • **IP Protocol** - This must use the IP Protocol Number format published by the Internet Assigned Numbers Authority (IANA). For example, ICMP has IP Protocol Number 1, TCP has IP Protocol Number 7, and UDP has IP Protocol Number 17. • VLAN Id • DPI **Note:** Because packet streams are bi-directional conversations between endpoint nodes, you need to create a "pair of packet filters" in order to filter on a packet stream. For more detailed information, see the discussion within the sections *Method 1: Stream Configuration Tool*, and *Method 2: Using Filters* below.	
Filter action drop-down field (see note)	Determines the action to use (either pass or drop) on the filtered packet streams from the pcap file being replayed.	
Loop times field	Defines how many times the pcap file is looped during the packet replay. Setting this to 0 is the equivalent to infinite.	
Speed Multiplier field	This is a multiplier that lets you redefine the delay between sending packets. The default value is 1, which is the normal, correct delay between the packets in the original pcap file. • A decimal value or integer value higher than 1 (e.g. 1.3, 2, etc.) reduces the delay between sending packets by that speed multiplier factor, and thus each packet is sent on a quicker time line than in the original pcap file. This is useful when you want to intensify the original delay between sending the packets compared to the original pcap file. • A decimal value less than 1 (e.g. 0.7, 0.5, etc.) increases the delay between sending packets by that speed multiplier factor, and thus each packet is sent on slower time line than in the original pcap file. This is useful as it lets you easily observe in detail what is happening to the packets on a slower timescale without missing vital information. If you find that the packet data scrolls too quickly in the **Live Packets** dialog box (see *Illustration 163* on page 542) and **Live Packet Monitoring** page (see *Illustration 164* on page 545) you can use this multiplier with a decimal value less than 1 to slow down the rate at which the packet data scrolls.	
Note: The **Filter action** button and **Filter actions** drop-down field only exist on the Multi-Point Designer. This is because there are two methods for selecting which packet streams are to be used in the generated traffic stream. Multi-Point Designer lets you use both the interactive stream configuration tool or the traditional method of manually creating Filters and routes.		

1-1. Functional Overview of the Packet Replay Functions

Illustration 190 shows a high-level functional overview of how the packet replay functions work. The packet replay functions generate a traffic stream based on the packet streams that have been selected from the specified pcap file.

The packet replay functions let you select the type of packet streams that you want to add into your SDTN, and thus define the type of testing that you want to perform. For example, if you are interested in the effects of a certain protocol (such as HTTP) within your SDTN, you can apply filters to the pcap file to filter and select the original HTTP streams within the injected traffic stream.

ILLUSTRATION 190 - HIGH LEVEL FUNCTIONAL OVERVIEW OF THE PACKET REPLAY FUNCTIONS



The packet replay functions also let you define where the selected packet streams in the generated traffic stream are routed within the SDTN.

The way in which packet stream routing is achieved, and how the packet replay functions are accessed vary according to the type of Network Designer you are using, and are described in the following sub-sections:

- *Section 1-7*, *Packet Replay Implementation in the Point-to-Point Designer* on page 623
- *Section 1-8*, *Packet Replay Implementation in the Multi-Point Designer* on page 628

1-2. The Concept of Initiators and Responders for Packet Streams

Before describing the Web Interface implementation of the packet replay functions, it is useful to discuss the concept of initiators and responders for packet streams that you find in a pcap file.

In our example (see *Illustration 191*), we will consider the packets associated with a packet stream (with stream ID 0) for a conversation (i.e. bidirectional communication) between a client PC (with address 192.168.3.131 on port 57011) attempting to access a web server (with address 72.14.213.138 on port 80).

A pcap file contains packets, which have a source address and a destination address. Each packet is unidirectional (i.e. source address/port to destination address/port). If you initially open a pcap file in Wireshark, each packet is represented by a Frame number, with a source address and destination address, and initially ordered in a chronological time-line according to when the packet was captured. It is beyond the scope of this document to describe the use of Wireshark, however, you can colorize the view in Wireshark in order to highlight which packet stream (i.e. conversation) the packet belongs to (see *Illustration 191*).

A pcap file also contains packet streams (each with a unique stream ID), which is set of two or more packets with the same source and destination addresses, and which defines bidirectional communication (i.e. conversation) between two endpoint nodes. You can also see packet streams as conversations within Wireshark by opening the conversation statistics window (see *Illustration 191*). When viewing conversations in Wireshark, the endpoint node considered to have initiated the conversation is called A (with an address A on port A), while the endpoint who responded to the conversation is called B with and address B on port B). The Web Interface on the NE-ONE refers to these endpoint nodes as an initiator (with an initiator address and an initiator port) and a responder (with a responder address and responder port).

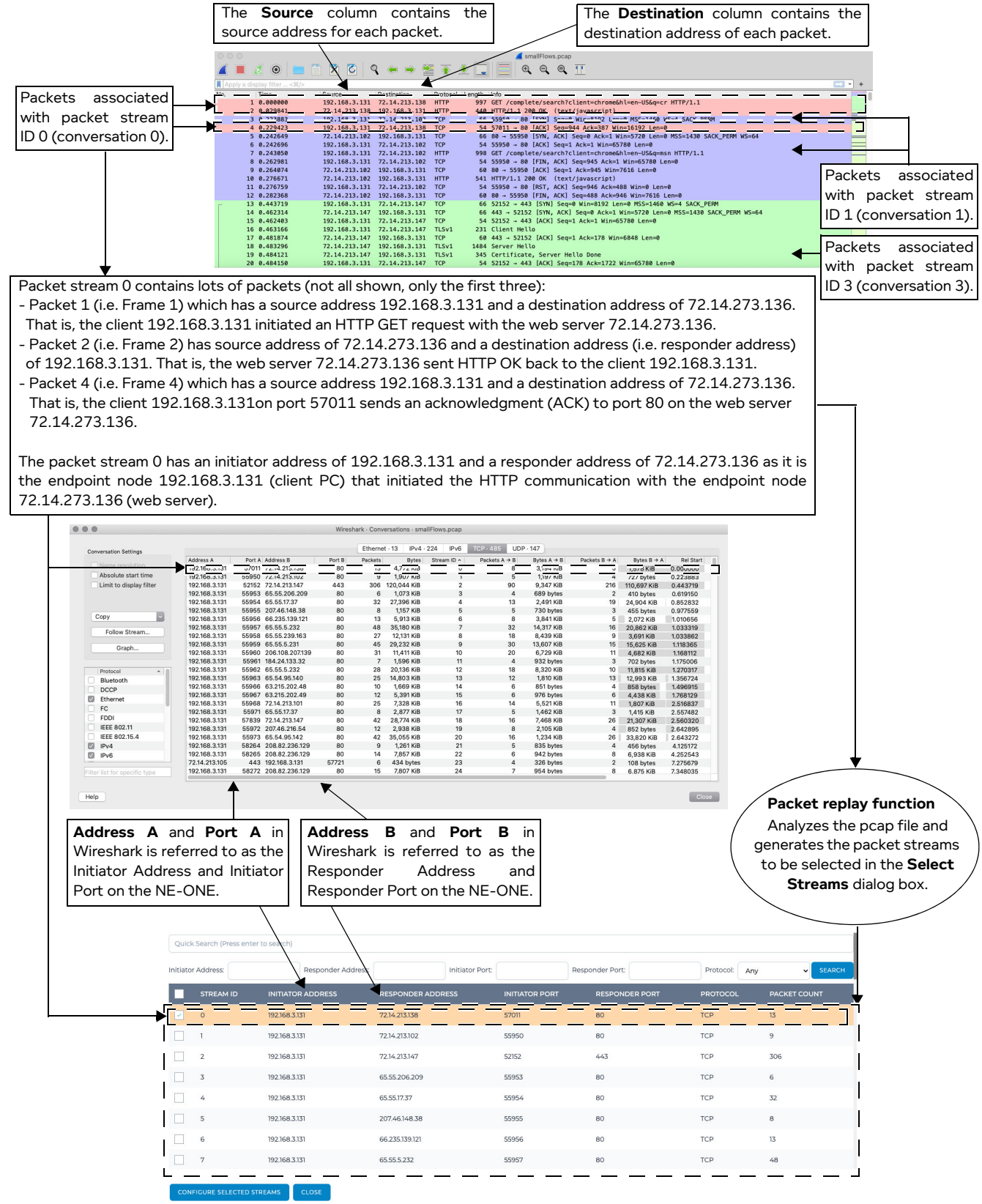
In our example below, packet stream 0 contains lots of packets (not all shown, only the first three):

- Packet 1 (i.e. Frame 1) which has a source address 192.168.3.131 and a destination address of 72.14.273.136. That is, the client 192.168.3.131 initiated an HTTP GET request with the web server 72.14.273.136.
- Packet 2 (i.e. Frame 2) has source address of 72.14.273.136 and a destination address (i.e. responder address) of 192.168.3.131. That is, the web server 72.14.273.136 sent HTTP OK back to the client 192.168.3.131.
- Packet 4 (i.e. Frame 4) which has a source address 192.168.3.131 and a destination address of 72.14.273.136. That is, the client 192.168.3.131on port 57011 sends an acknowledgment (ACK) to port 80 on the web server 72.14.273.136.
- etc., etc. (other packets not shown)

The packet stream 0 has an initiator address of 192.168.3.131 and a responder address of 72.14.273.136, as it is the endpoint node 192.168.3.131 (client PC) that initiated the HTTP communication with the endpoint node 72.14.273.136 (web server).

When the packet replay function processes the specified pcap file, it analyzes each of the individual packets and packet streams, and builds a list of packet streams based on that analysis. The packet streams that you select will therefore have an initiator address (and initiator port) and a responder address (and responder port).

ILLUSTRATION 191 - EXAMPLE PCAP FILE DISPLAYED IN WIRESHARK VS THE SELECT STREAMS DIALOG BOX ON THE NE-ONE



1-3. Comparison of the Packet Replay Implementation Between the Point-to-Point Designer and Multi-Point Designer

Table 74 highlights the differences in how the packet replay functions are implemented between the Point-to-Point Designer and the Multi-Point Designer.

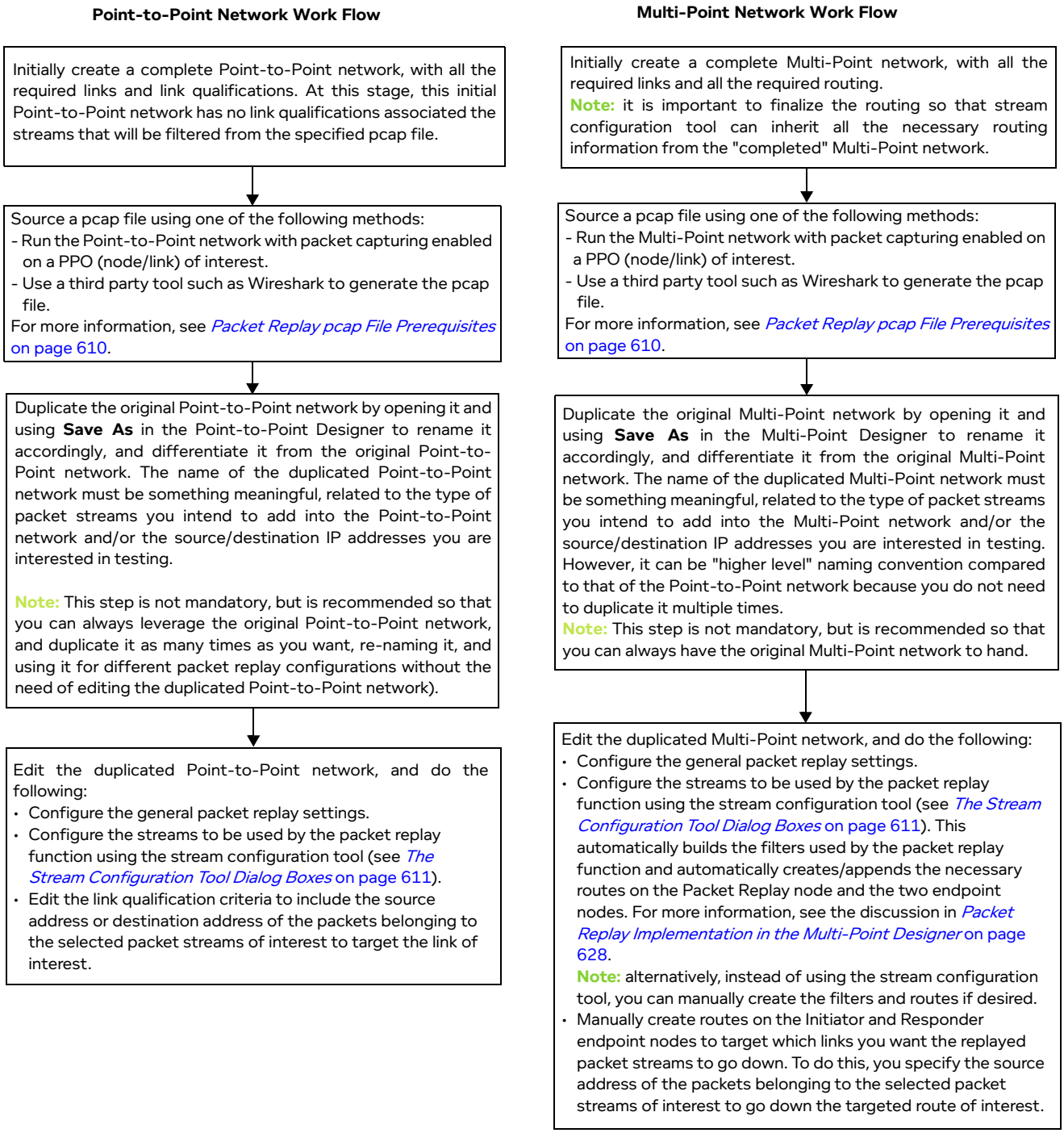
TABLE 74 - HIGH LEVEL COMPARISON OF PACKET REPLAY IMPLEMENTATION BETWEEN POINT-TO-POINT DESIGNER AND MULTI-POINT DESIGNER

Mechanism Used	Point-to-Point	Multi-Point
Number of nodes	1 (per port pair)	Multiple
Node type(s)	Hidden system node (per port pair). Only the parameters of the packet replay functions are visible in the Web Interface	Two types, either: • Existing regular node already part of the SDTN can be used with the packet reply function to add the additional traffic (not recommended). • Dedicated "packet replay" type node can be added into the existing SDTN, and can be used with the packet reply function to add the additional traffic.
Number of packet replay instances per link (a packet replay instance generates a traffic stream instance)	1	Multiple Varies according to the number of nodes in the SDTN that have the packet replay function configured and running. Each node using the packet replay function can use either the same or different pcap file. Each node using the packet replay function can apply the same or different traffic filtering rules. **Note:** useful as it lets you define different packet replay nodes dedicated to replaying different traffic types within the SDTN, which can simply be activated (i.e. running) or dis-activated (i.e. not running) via the **Running** check-box (see *Illustration 202* on page 632).
Mechanism for selecting the packet streams to be used in the generated traffic stream	The packet streams to be used to generate the traffic stream is achieved using an interactive stream configuration tool (see *The Stream Configuration Tool Dialog Boxes* on page 611).	The packet streams to be used to generate the traffic stream is achieved using an interactive stream configuration tool (see *The Stream Configuration Tool Dialog Boxes* on page 611) and/or the Filters dialog box (*Illustration 213* on page 645).
Impacted links selection / routing	Routing not definable, and automatically applied by the NE-ONE. Routing between the endpoint nodes is performed automatically by the invisible node based upon the packet stream directions you configure, and link qualification criteria that you define.	Based on routing, which is definable in the Multi-Point Designer. Routing on the Packet Replay node is configured using the Composite Routing (Labs) function. Routing on the endpoint nodes is configured using the Composite Routing (Labs) function, Symmetric (Expression) Routing function, or IP (Labs) Routing function.

1-4. Typical Work Flow Comparison Using the Packet Replay Functions in Point-to-Point Networks vs Multi-Point Networks

Illustration 192 shows a typical work flow comparison that you apply between using the packet replay functions in a Point-to-Point network vs a Multi-Point network.

ILLUSTRATION 192 - TYPICAL WORK FLOW COMPARISON WHEN THE PACKET REPLAY FUNCTIONS IN POINT-TO-POINT NETWORKS VS MULTI-POINT NETWORKS



The Point-to-Point network work flow varies compared to that in a Multi-Point network, as follows:

- In the Multi-Point network you do not need to duplicate the original network multiple times in order to create different traffic streams. You can use the same duplicated Multi-Point network, and add a dedicated packet replay node into the Multi-Point network for each traffic stream type that you want to create.
- In the Multi-Point network, you can also use the stream configuration tool dialog boxes to select and configure the packet streams that will be used in the generated traffic stream. However, you can also use more elaborate filtering and more elaborate routing by creating/editing the filters and routes according to your needs.

1-5. Packet Replay pcap File Prerequisites

In order to use the packet replay functions, you must have a pcap file located within the file system of the NE-ONE. Calnex recommend that you upload pcap files intended for use with the packet replay function within your `/Private/packet_replay_files` directory on the NE-ONE.

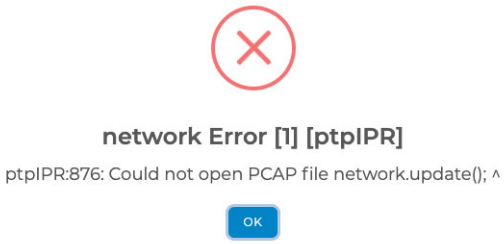
The pcap file must have either:

- Been generated on PPO of interest while running a network on the NE-ONE (see *Launching Packet Capture on a PPO* on page 532), and then copied from the corresponding `/Run Data/<network name>/<network run date>` or `/Run Data/System/<system run-time date>` directory to your `/Private/packet_replay_files` directory using the File Browser. You can create the pcap file for intended use with the packet replay function on both link PPOs and node PPOs. If you prefer to generate a pcap file with more specific traffic, use a link PPO. If you prefer to generate a pcap file with more general traffic, use a node PPO.
- Been sourced from a third party packet analysis utility such as Wireshark, and uploaded to your `/Private/packet_replay_files` directory using the File Browser.

! Notice:

When you apply the packet replay function to a Point-to-Point or Mulit-Point network, the file path of the pcap file is specified in the packet replay function. Each time the Point-to-Point or Mulit-Point network is opened, the packet replay function calls the specified pcap file in order to create the traffic stream based on the packet replay configuration you had previously created. If the pcap file no longer exists when you open and run a Point-to-Point or Mulit-Point network, the error message similar to *Illustration 193* appears. In order to avoid this error message, never delete a pcap file that is currently being used by the packet replay function on a Point-to-Point or Mulit-Point network.

ILLUSTRATION 193 - ERROR MESSAGE IF SPECIFIED PCAP FILE MISSING WHEN RUNNING A NETWORK



Before using a third party sourced pcap file on the NE-ONE, you typically use packet analysis utility such as Wireshark to examine the pcap file, and to determine in advance the packet streams that you are interested in filtering and testing over your Point-to-Point or Mulit-Point network. The NE-ONE, however has an extremely useful and interactive stream configuration tool (see *The Stream Configuration Tool Dialog Boxes* on page 611) for both the Point-to-Point Designer and Mulit-Point

Designer. The dialog boxes associated with the stream configuration tool let quickly apply different search filter criteria so you can quickly select the packet streams of interest, and if necessary correct the traffic direction for the selected packet streams. For more information, see *The Stream Configuration Tool Dialog Boxes* on page 611.

1-6. The Stream Configuration Tool Dialog Boxes

Before reading this section, you are encouraged to read *The Concept of Initiators and Responders for Packet Streams* on page 605 in order to understand the NE-ONE specific terms, initiator and responder.

The stream configuration tool has two dialog boxes, which let you select the packet streams that you want in the generated traffic stream, and (if necessary) correct any of the packet stream directions inherited from the pcap file.

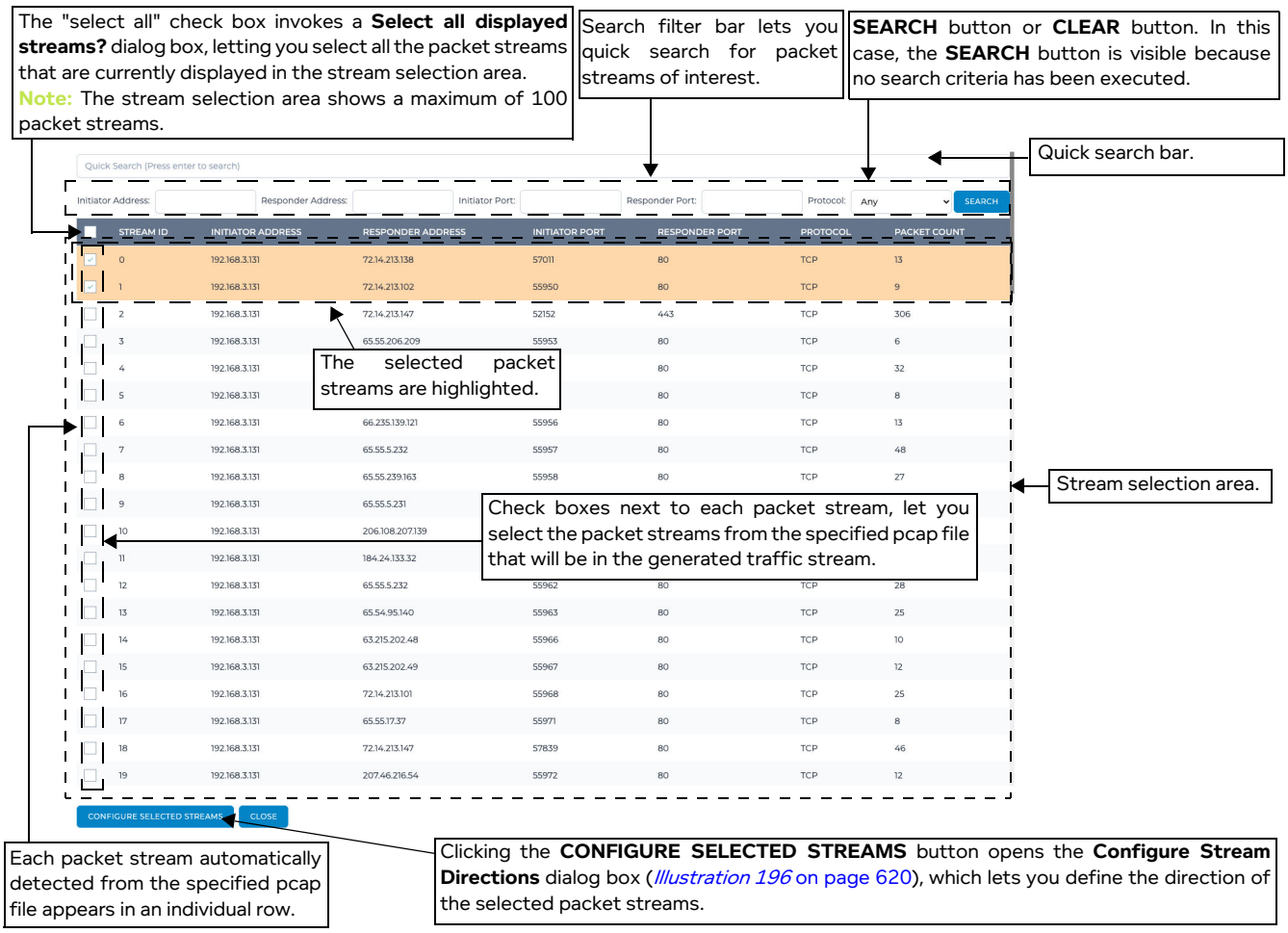
The stream configuration dialog boxes are always used in the Point-to-Point Designer, and are invoked by clicking on the **SELECT STREAMS** button within the **Packet Replay Settings** dialog box (see *Illustration 199*).

The stream configuration dialog boxes are optionally used in the Multi-Point Designer, as you can directly use filter rules and Composite Routing to select and route the packet streams of interest in the generated traffic stream. If you are interested in generating traffic streams of up to 100 packet streams, for expediency, Calnex recommend that you also use stream configuration dialog boxes on the Multi-Point Designer as it is a quicker process than manually defining filter rules and Composite Routing rules. In the Multi-Point Designer, the stream configuration dialog boxes are invoked by clicking on the **STREAM CONFIGURATION** button within the **Advanced Node Properties** window of the Packet Replay node's Intelligent Packet Replay or Passive Packet Replay function (see *Illustration 202*).

1-6-1. Select Streams Dialog Box

Illustration 194 shows an example **Select Streams** dialog box with no filtering criteria applied.

ILLUSTRATION 194 - SELECT STREAMS DIALOG BOX (NO FILTERING APPLIED)



The **Select Streams** dialog box contains the following:

- A stream selection area, containing individual rows for each of the packet streams from the specified pcap file that were automatically detected by the NE-ONE.

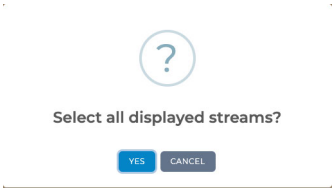
  Note:

  The stream selection area contains a total of up to 100 packet streams in all cases (i.e. when no filter search criteria is applied and when a filter search criteria is applied).
  If the specified pcap contains more than 100 packet streams, you may want to view more than the first 100 packet streams (i.e. packet stream IDs 0 to 99) within the stream selection area. To view more than the 100th packet stream (i.e. packet stream ID 100 and above), you must use the filter search bar area (described below). Upon performing a filter search, the first 100 packet streams matching the filter criteria will appear within the stream selection area.

  Note:

  If the stream selection area contains no results when the **Select Streams** dialog box first appears (i.e. when no search filter is applied) it is because the path that you specified for the pcap file is incorrect or the pcap file was removed. In this case correct the path definition of the pcap file and verify the pcap file exists in the location that you specified.
- Individual check boxes letting you select the packet streams from the pcap file that will be used in the generated traffic stream. You can select one or more packet streams, and up to a total of 100 packet streams.

- A "select all" check box, which lets you select all the packet streams that are currently displayed in the stream selection area. Enabling this check box invokes the **Select all displayed streams?** dialog box.



  The buttons in the **Select all displayed streams?** dialog box act as follows:
  - Clicking the **YES** button results in selecting all the displayed packet streams related to the search filter you applied. Up to 100 packet streams can be displayed and selected (see note above).
  - Clicking the **CANCEL** button returns you to the **Select Streams** dialog box without selecting all the displayed packet streams.
- A quick search bar, with a search field. This lets you quickly and globally search on a string of interest within results of packet stream from the specified pcap file. For example, if you want to quickly identify whether an IP address of interest is in any of the packet streams and currently assigned to the initiator node or responder node, you simply type the IP address of interest and press **Return** key.
- A search bar filter area, with the following fields, letting you filter and search for packet streams of interest:
  - **INITIATOR ADDRESS** - lets you filter by the initiator IP addresses. Leaving this field blank means all initiators appear in the result of filtered packet streams.
  - **RESPONDER ADDRESS** - lets you filter by the responder IP addresses. Leaving this field blank means all responder appear in the result of filtered packet streams.
  - **INITIATOR PORT** - lets you filter by the initiator port. Leaving this field blank means all initiator ports appear in the result of filtered packet streams.
  - **RESPONDER PORT** - lets you filter by the responder port. Leaving this field blank means all responder ports appear in the result of filtered packet streams.
  - **PROTOCOL** - lets you filter by the destination port (i.e. TCP, UDP, or ICMP). Leaving this field blank means all protocols appear in the set of filtered packet streams.

Note:

If however, you have filtered on a particular initiator and/or responder, and the streams related to those initiators and/or responders have only TCP and UDP packet streams (for example), then filtering by ICMP will return an empty set of filtered packet streams. Therefore, as a work flow (in this example, if you were interested in ICMP packets), Calnex recommend that you initially only filter by the ICMP Protocol criteria first, and from the results that appear, you would determine if you want to filter further by initiator and/or responder addresses.

You can apply filtering using one or more of the above fields.

For example, if you are interested in only what happened at a particular responder, you can specify the IP address of the responder in the **RESPONDER ADDRESS** field, then choose the packet streams of interest from the result of the search by using the corresponding check boxes.

Similarly, if you are interested in what happened between a particular initiator and responder, you can specify the IP address of the initiator in the **INITIATOR ADDRESS** field, the IP address of the responder in the **RESPONDER ADDRESS** field, then choose the packet streams of interest from the result of the search by using the corresponding check boxes.

The example in *Illustration 195* shows filtering for all HTTP traffic streams (i.e. TCP 80) from the specified pcap file (i.e. **RESPONDER PORT** set to 80 and **PROTOCOL** field set to TCP) for all initiators and responders (i.e. no initiator or responder IP addressed have been specified). In this

example, all the HTTP packet streams have been selected using the "select all" check box. In this example, the goal of the stream selection is to define a heavy load of HTTP traffic as we have not filtered by initiator or responder addresses, and we have selected all of the resultant packet streams.

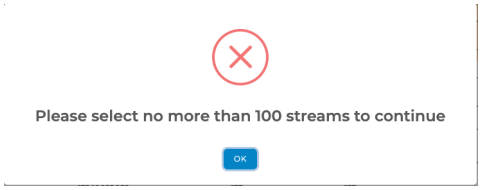
Note:

The search bar filter area contains either a **SEARCH** button or **CLEAR** button. When you specify a search criteria using one or more of the search fields, and click the **SEARCH** button, a set of filtered packet streams appear, and the button changes to **CLEAR**. The set of filtered packet streams will remain, and can then be selected using either the "select all" check box, or by the individual check boxes for each individual filtered packet stream. The set of filtered packet streams will persist and can be removed at any time by clicking the **CLEAR** button. Upon clicking the **CLEAR** button, the filtering criteria is removed, all the traffic streams from the specified pcap file return, and the button changes back to **SEARCH**.

- A **CONFIGURE SELETED STREAMS** button. Clicking this button opens a **Configure Stream Directions** dialog box (see *Illustration 196*), which lets you to choose the direction for each of the selected packet streams.

Note:

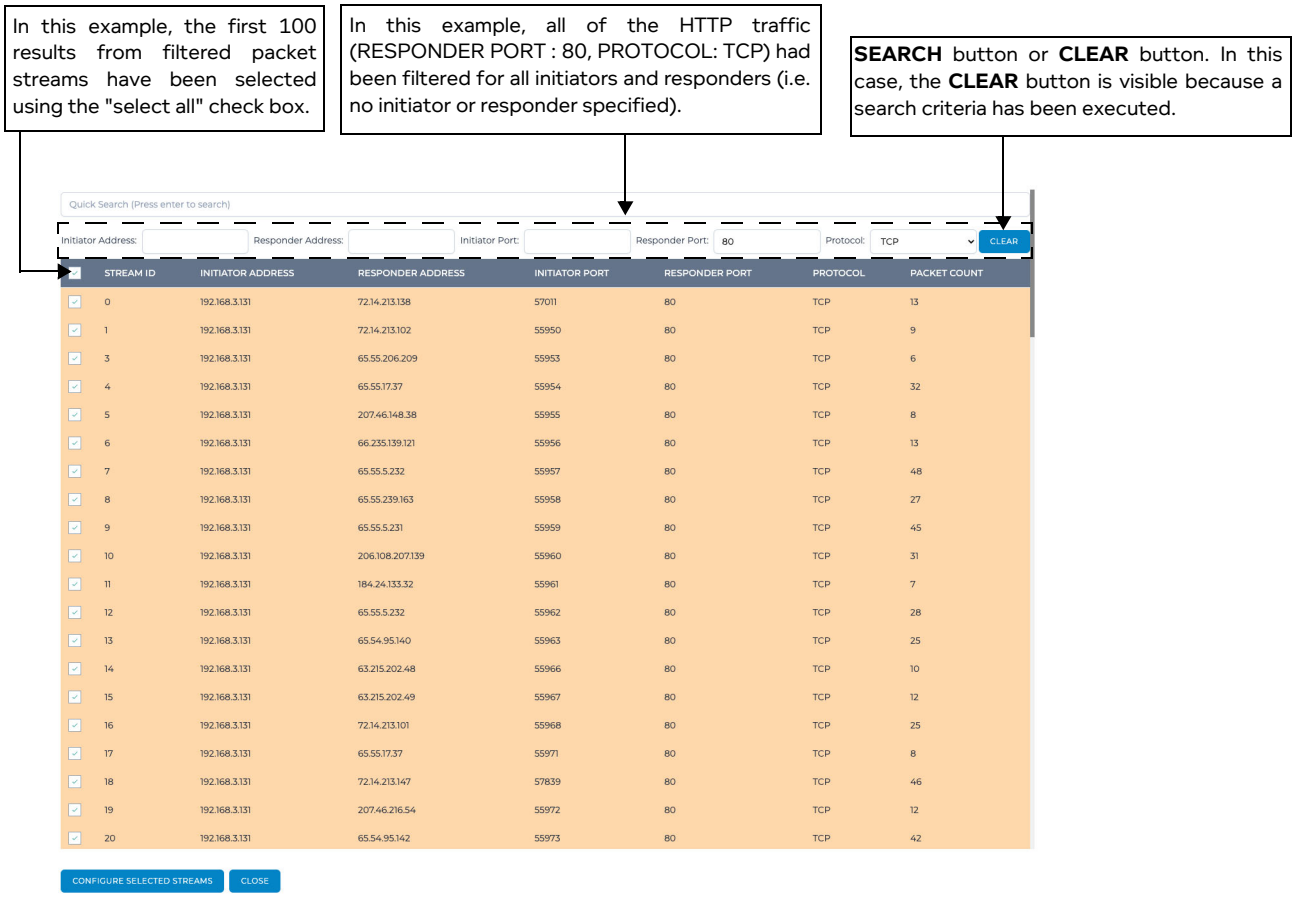
A total of 100 packet steams can be selected from the stream selection area. If you have selected more than 100 packet streams in total, the following dialog box appears prompting you to select up to 100 packet streams before continuing to the **Configure Stream Directions** dialog box.



If this dialog box appears, click the **OK** button to return to the **Select Streams** dialog box, and ensure you have up to a total of 100 streams selected before clicking the **CONFIGURE SELETED STREAMS** button.

- A **CLOSE** button. Clicking this button returns you to the **Packet Replay Settings** dialog box (see *Illustration 199*).

ILLUSTRATION 195 - EXAMPLE SELECT STREAMS DIALOG BOX WITH SEARCH FILTERING APPLIED



Note:

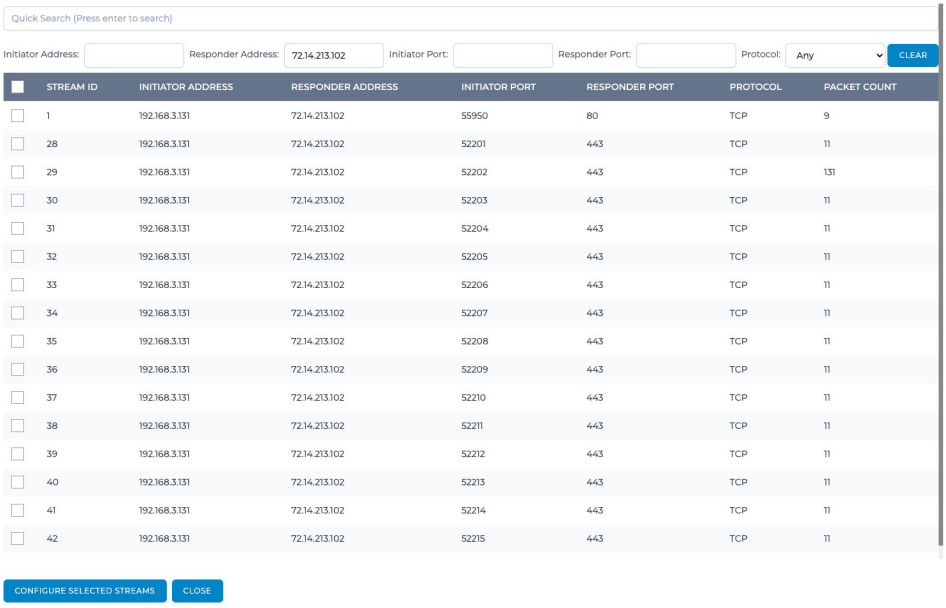
The original stream IDs from the specified pcap file remain the same (which is normal). Therefore, when you apply filters, the stream IDs listed will not be contiguous (i.e. 0, 1, 3, 4 and not 0, 1, 2, 3, 4) because only the filtered streams with their original stream IDs remain in the list of filtered packet streams.

The **Select Streams** dialog box lets you "build up" a set of different packet streams using the work flow where you must specify streams progressively by using different filter searches. As noted above, you can progressively "build up" to a maximum of 100 packet streams in total.

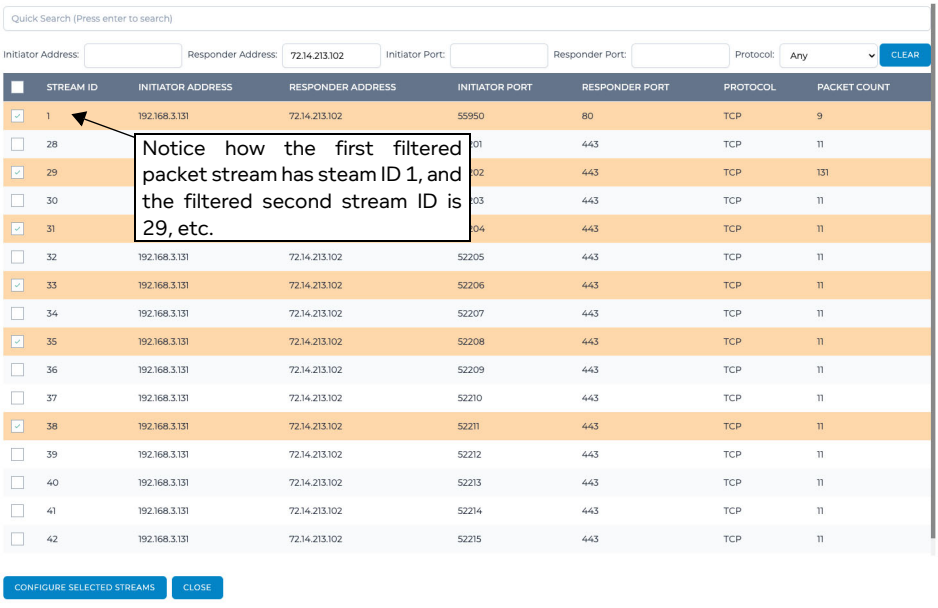
For example, if you were interested in generating traffic for some packet streams related to the Responder Address 72.14.213.102 and some packet streams related to the Responder Address 72.14.213.138, you would do the following:

1. In the **RESPONDER ADDRESS** field, type **72.14.213.102**, then click **SEARCH**.
2. A set of filtered results appear, showing all packet streams relating to responder address 72.14.213.102. The **SEARCH** button changes to **CLEAR**, indicating that the current search criteria is

applied.

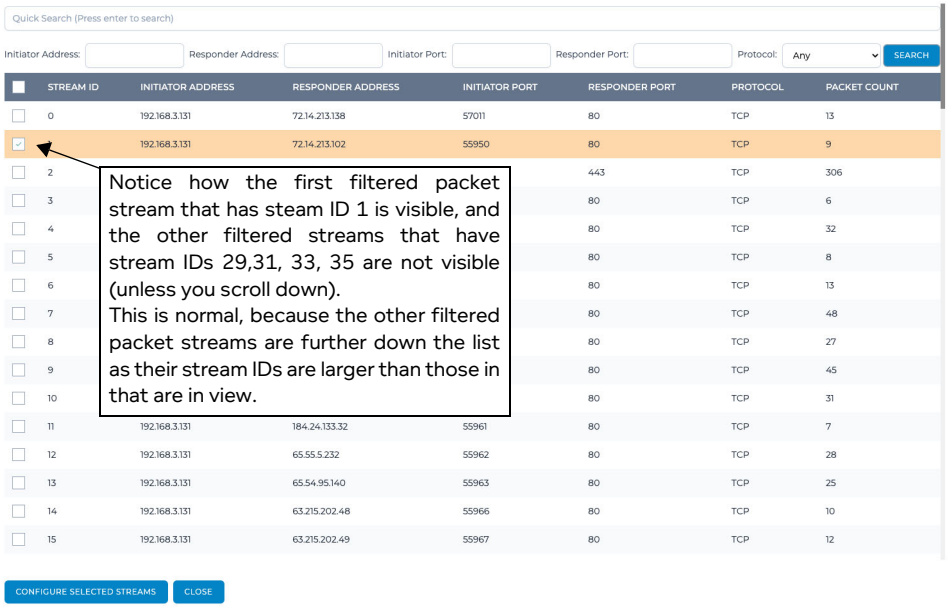


3. In the filtered results that appear, click the check boxes associated with the packet streams that you want to add into the generated traffic stream. In our example, we are interested in packet streams with stream IDs 1, 29, 31, 33, 35 and 38.



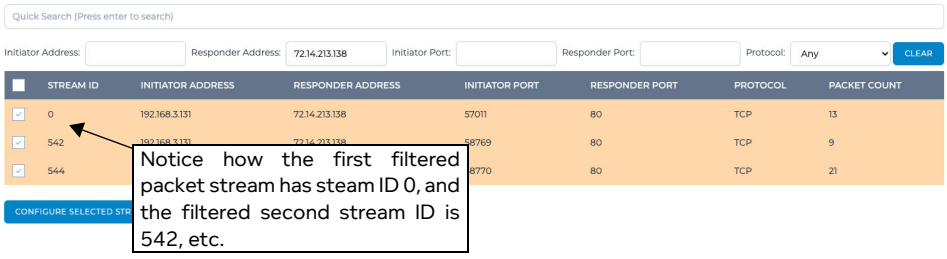
4. Click **CLEAR**.
   The **Select Streams** dialog box updates showing all the streams from the original pcap file, with the

packet streams for responder address 72.14.213.102 enabled and highlighted.

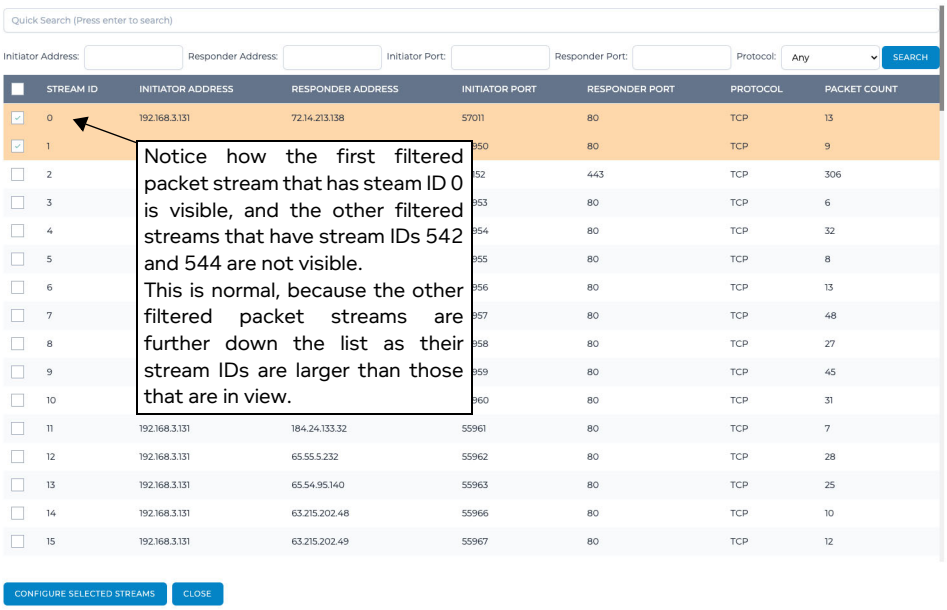


5. In the **RESPONDER ADDRESS** field, type **`72.14.213.138`**, then click **SEARCH**.
6. A set of filtered results appear, showing all packet streams relating to responder address 72.14.213.138. The **SEARCH** button changes to **CLEAR**, indicating that the current search criteria is applied.

7. In the filtered results that appear, click the check boxes associated with the packet streams that you want to add into the generated traffic stream. In our example, we are interested in packet streams with stream IDs 0, 542, and 544.



8. Click **CLEAR**.



The **Select Streams** dialog box updates showing the first 100 streams from the original pcap file, with the packet streams for responder address 72.14.213.102 enabled and highlighted, and also the responder address 72.14.213.136 enabled and highlighted.

Note:

In our example, we stop here "building up" sets of packet streams relating to a particular filter criteria. However, we could continue with additional search filters for selecting specific packet streams as required.

9. Now that the packet stream sets based on different filters (in this example, responder address 72.14.213.102 and responder address 72.14.213.136) have now been "built up", click the **CONFIGURE SELECTED STREAMS** button to continue with the next step (i.e. define the packet stream directions for each of the selected packet streams).

1-6-2. Configure Stream Directions Dialog Box

In terms of communication between the two endpoint nodes (which is bidirectional), any of the two endpoint nodes may have actually initiated the communication (i.e. been the first to send the first packet in the packet stream). But at the instant the pcap file is captured, the node which is seen (and captured) to have initiated the packet stream is considered as the initiator.

In terms of replaying a pcap file, you may want to actually define the other endpoint node (i.e. the endpoint node that was originally captured as the responder) as the initiator, and thus invert the original traffic direction inherited from the pcap file. This is because the recorded pcap file may have not actually captured the first packet from the packet stream. In our example described above in *The Concept of Initiators and Responders for Packet Streams* on page 605, we see that for stream 0:

- Packet 1 (i.e. Frame 1) which has a source address 192.168.3.131 and a destination address of 72.14.273.136. That is, the client 192.168.3.131 initiated an HTTP GET request with the web server 72.14.273.136.
- Packet 2 (i.e. Frame 2) has source address of 72.14.273.136 and a destination address (i.e. responder address) of 192.168.3.131. That is, the web server 72.14.273.136 sent HTTP OK back to the client 192.168.3.131.
- Packet 4 (i.e. Frame 4) which has a source address 192.168.3.131 and a destination address of 72.14.273.136. That is, the client 192.168.3.131on port 57011 sends an acknowledgment (ACK) to

port 80 on the web server 72.14.273.136.

- etc., etc. (other packets not shown)

The packet stream 0 has an initiator address of 192.168.3.131 and a responder address of 72.14.273.136 as it is the endpoint node 192.168.3.131 (client PC) that initiated the HTTP communication with the endpoint node 72.14.273.136 (web server).

However, in the case that the pcap file had not captured Packet 1 mentioned above, and only captured from Packet 2 onwards, the initiator would be captured as the web server instead of the client.

The **Configure Stream Directions** dialog box (*Illustration 196*) lets you resolve this potential inverted packet stream direction issue by assigning the correct endpoint node to appropriate source IP address and port number from packets in the packet stream. The **Configure Stream Directions** dialog box also contains the port numbers that were used for the packets in the packet stream, letting you more easily identify which packet streams may have their direction inverted. You can typically look at the initiator port and responder port in order to determine whether the packet stream directions are inverted or not. With our example above, you would expect to see port 80 for the web server (i.e. the responder endpoint node) as the responder port, and port 57011 for the client PC (i.e. the initiator endpoint node) as the initiator port.

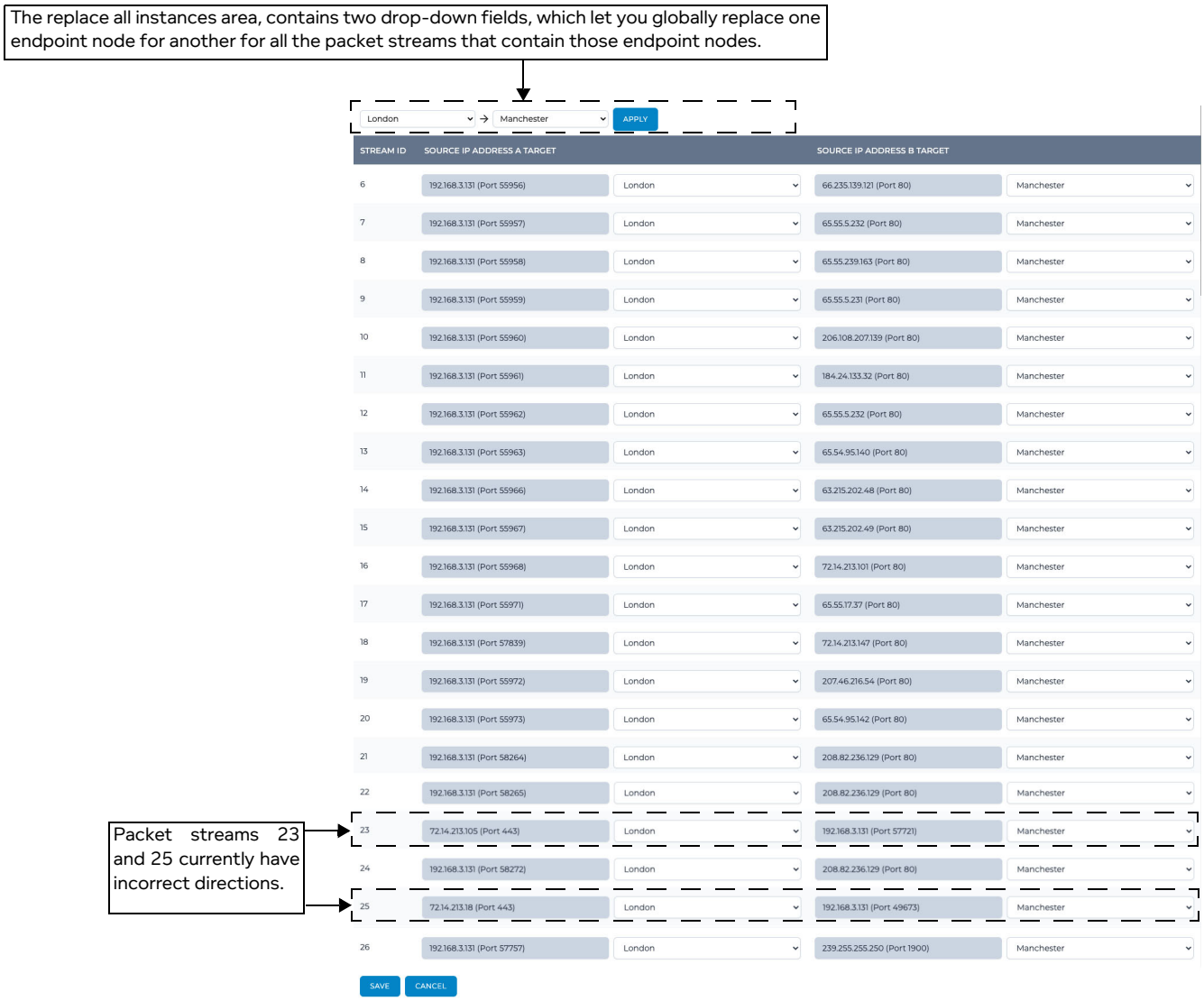
Note:

For simplicity, only 21 packet streams are shown. However, the principles described below are the same for many packet streams.

The **Configure Stream Directions** dialog box contains the following:

- **STREAM ID** column - shows the stream ID for the packet stream. All the packet streams that were selected in the **Select Streams** dialog box appear as separate rows.
- **SOURCE IP ADDRESS A TARGET** column - this is the source IP address and port number of the packet that what was recorded at the initiator endpoint node at the time that the pcap file was created. This cannot be changed (i.e. you assign one of the two endpoint nodes to it, if required).
- Drop-down field to the right of the **SOURCE IP ADDRESS A TARGET** - this is the endpoint node that is currently assigned to the initiator. If this is the wrong endpoint node, you can select the other endpoint node to correct the packet stream direction.
- **SOURCE IP ADDRESS B TARGET** - this is the source IP address and port number of the packet that what was recorded at the responder endpoint node at the time that the pcap file was created. This cannot be changed (i.e. you assign one of the two endpoint nodes to it, if required).
- Drop-down field to the right of the **SOURCE IP ADDRESS B TARGET** - this is the endpoint node that is currently assigned to the initiator. If this is the wrong endpoint node, you can select the other endpoint node to correct the packet stream direction.

ILLUSTRATION 196 - CONFIGURE STREAM DIRECTIONS DIALOG BOX (STREAMS 23 & 25 INCORRECT)



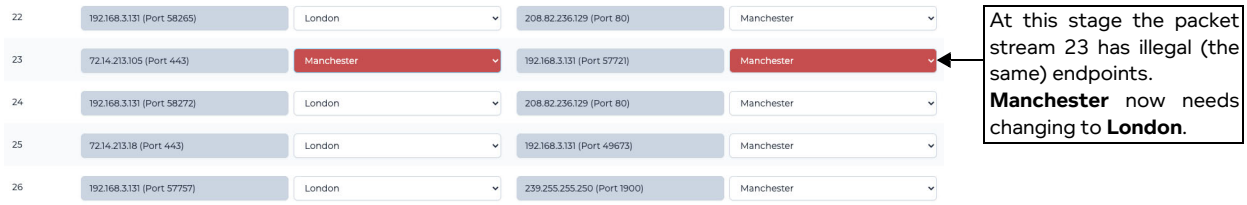
In the example shown in *Illustration 196*, we see that the following two packet streams have incorrect directions:

- Packet stream with stream 23 - The recorded pcap file had originally assigned the Manchester endpoint node as the initiator 192.168.3.131 (Port 57721), and the London endpoint node as the responder 72.14.213.105 (Port 443). This is incorrect as London is a client which initiated the conversation with the web server over SSL (port 443). The London node needs to be the initiator, and assigned to 192.168.3.131 (Port 57721), while the Manchester node needs to be the responder, and assigned to 72.14.213.105 (Port 443).
- Packet stream with stream 25 - The recorded pcap file had originally assigned the Manchester endpoint node as the initiator 192.168.3.131 (Port 49623), and the London endpoint node as the responder 72.14.213.18 (Port 443). This is incorrect as London is a client which initiated the conversation with the web server over SSL (port 443). The London node needs to be the initiator, and assigned to 192.168.3.131 (Port 49623), while the Manchester node needs to be the responder, and assigned to 72.14.213.18 (Port 443).

To make the correct assignments, you would do the following:

1. In the drop-down field to the right of **72.14.213.205 (Port 443)**, select **Manchester**.

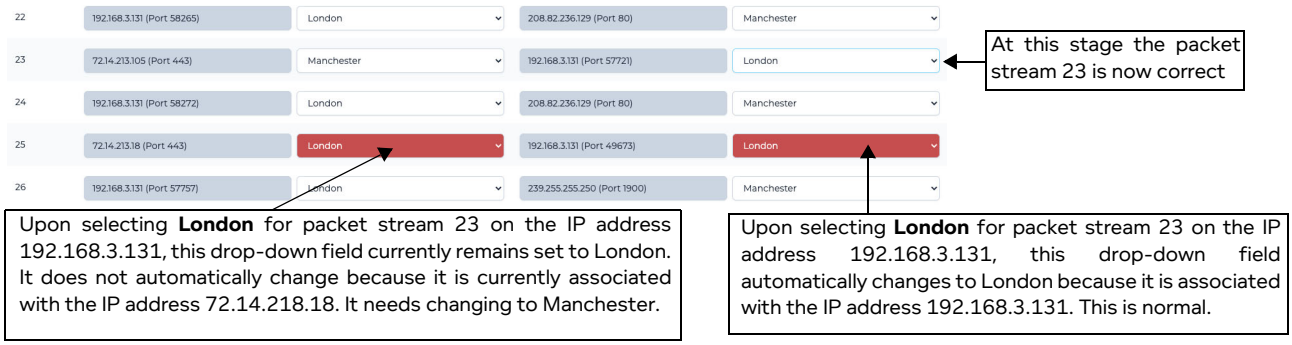
   The row for packet stream 23 updates, highlighting the drop-down fields in red to indicate that the endpoint nodes are the same (which of course is illegal).



2. In the drop-down field to the right of **192.168.3.131 (Port 57721)**, select **London**.

   The row for packet stream 23 updates, and is now correctly defined.

   The drop-down field associated with **192.168.3.131 (Port 49673)** on the row for the packet stream 25 automatically updates to **London** because you had assigned London in packet stream 23 to the IP address 192.168.3.1. This is normal and does not need to be changed. However packet stream 25, is now highlighting the drop-down fields in red to indicate that the endpoint nodes are the same (which of course is illegal), and you must now assign **Manchester** to **72.14.213.18 (Port 443)**.



3. In the drop-down field to the right of **72.14.213.18 (Port 443)**, select **Manchester**.

   The row for packet stream 25 updates, and is now correctly defined, and the **Configure Stream Directions** dialog box now looks like that in *Illustration 197*.

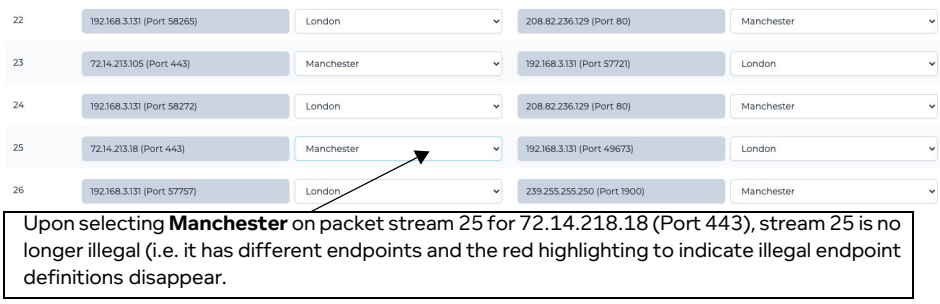
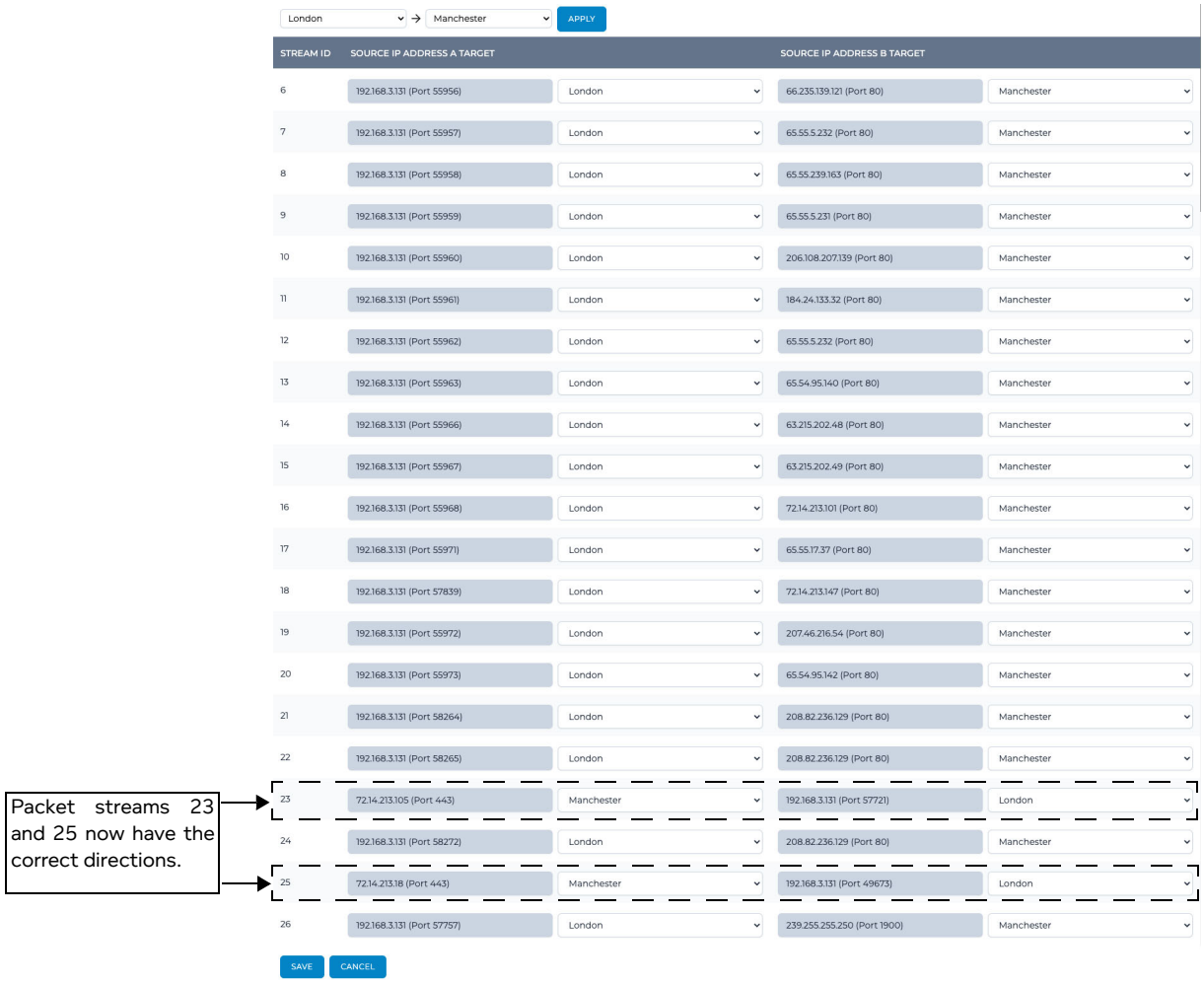


ILLUSTRATION 197 - CONFIGURE STREAM DIRECTIONS DIALOG BOX (STREAMS 23 & 25 CORRECT)



Note:

The **Configure Stream Directions** dialog box may contain many filtered packet streams. Reviewing and configuring each of the filtered packet streams on an individual basis can be a laborious process. The **Configure Stream Directions** dialog box also contains a "replace all instances" area, which lets you globally replace one endpoint node with another for any of the packet streams that contain those endpoint nodes.

The right hand side drop-down field defines the endpoint node name that you want to replace with the endpoint node name selected in the left hand side drop-down field. Clicking the **APPLY** button will globally apply the replacement on any of the packet streams that contain those endpoint nodes.

The bottom of the **Configure Stream Directions** dialog box contains the following elements:

- **SAVE** button - clicking this button saves the current stream configuration, and returns the **Packet Replay Settings** dialog box.

  Note:

  The time it takes to save the stream configuration varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).
- **CANCEL** button - clicking this button cancels the current stream configuration, and returns the **Packet Replay Settings** dialog box.

1-7. Packet Replay Implementation in the Point-to-Point Designer

The sub-sections below describe how the packet replay functions are implemented on the NE-ONE back end and on the NE-ONE Web Interface in the Point-to-Point Designer.

1-7-1. Back End Packet Replay Implementation in the Point-to-Point Designer

In the Point-to-Point Designer, for each port pair, the packet replay functions are implemented on one hidden node (see *Illustration 198* for a functional overview).

Note:

Compared to the Multi-Point Designer (which lets you use multiple packet replay nodes, and Composite routing to create multiple traffic streams per link), the Point-to-Point Designer only lets you define one traffic stream (i.e. one level of traffic) per link between two endpoint nodes in the Point-to-Point network.

This limitation is because each port pair in the Point-to-Point network uses one hidden packet replay node (running one packet replay instance), which generates one traffic stream that is added into the Point-to-Point network.

If you want add multiple levels of traffic per link then you must use the Multi-Point designer. If the Multi-Point Designer feature is licensed on the NE-ONE, you can either initially create a Point-to-Point network and then export it to a Multi-Point network, or directly create a network with two nodes in the Multi-Point Designer.

Compared to the Multi-Point Designer (which lets you use multiple nodes, filters, and Composite routing to create the multiple traffic streams), the packet replay functions in the Point-to-Point Designer use the following three step process:

- Step 1 (packet stream filtering) : Select the packet streams from the specified pcap file that are used in the generated traffic stream (via the **Select Streams** dialog box (*Illustration 194* on page 612)).
- Step 2 (packet stream routing) : Choose the direction of the selected (filtered) packet streams that are used within the generated traffic stream (via the **Configure Stream Directions** dialog box *Illustration 196* on page 620)).

Note:

The packet stream selection parameters defined in the **Select Streams** dialog box (*Illustration 194* on page 612) and the packet stream direction parameters defined in the **Configure Stream Directions** dialog box *Illustration 196* on page 620) are always used within the Point-to-Point designer. They optionally and recommended to also be used in the Multi-Point Designer.

- Step 3 (packet stream routing) : Use link qualifications to target which links receive the routed packet streams.

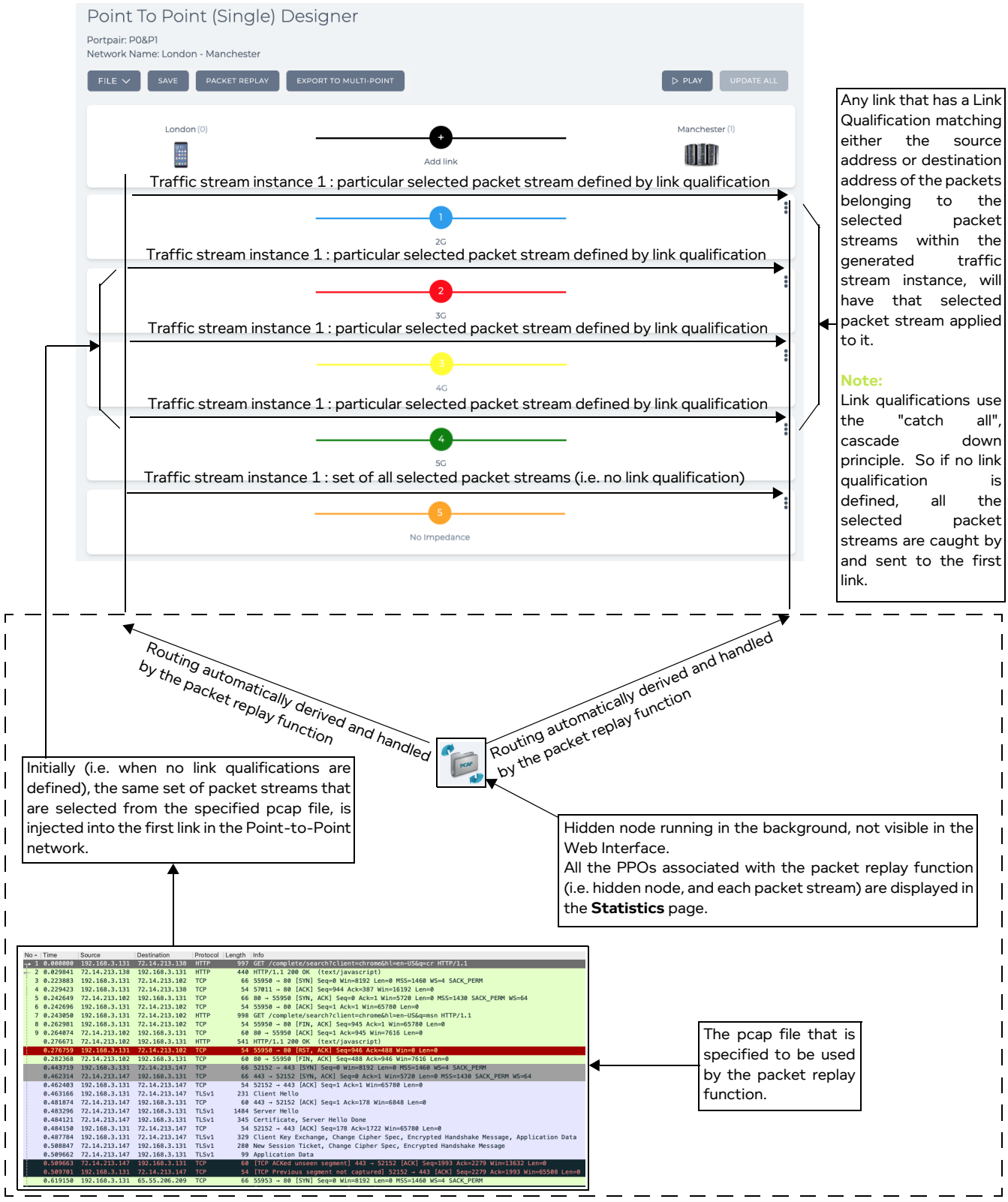
1-7-2. The Principle of Link Qualifications for Targeting Links in Point-to-Point Networks

The generated traffic stream (which contains the selected packet streams) must be used in conjunction with Link Qualifications in order to target which link gets the selected packet streams. Any link that has a Link Qualification matching either the source address or destination address of the packets belonging to the selected packet streams, will have that packet stream applied to it. For more information on how to do this, see the example described in *Packet Replay Example in Point-to-Point Networks* on page 652.

Note:

Link qualifications use the "catch all", cascade down principle. So if no link qualification is defined, all the selected packet streams are caught by the first link, and only sent to the first link in the Point-to-Point network.

ILLUSTRATION 198 - FUNCTION OVERVIEW OF HOW PACKET REPLAY WORKS IN THE POINT-TO-POINT DESIGNER



Note:

Link qualifications work by assessing the source and/or destination address on a per packet level basis (i.e. not at the packet stream level, which contains multiple packets, each of which have a source and destination address).

In *The Concept of Initiators and Responders for Packet Streams* section on page 605 we discussed the concepts of initiator address and responder address. These naming of these addresses apply only to the end nodes of the packet stream, rather than the actual source and destination addresses of the individual packets within the packet stream. The IP addresses of the initiator and responders will obviously be the same as source and destination addresses of the individual packets, since the packet stream contains the all the individual packets with the same source and addresses. At the time that the pcap file was recorded, the initiator will inherit the IP address of the first packet's source address, and the responder will inherit the IP address of the first packet's destination address.

Therefore, when it comes to the concept of using link qualifications to target specific traffic streams down a link, we refer to specifying the source or destination address of the individual packets within the packet stream, rather then the initiator or responder addresses associated with the packet stream. This is normal as link qualifications work by assessing the source and/or destination address on a per packet level basis.

Note:

If required, you can target multiple packet streams from the generated traffic stream to down the same link. To do this, you simply specify the source or destination address associated with packet streams you want to target, separating them with commas.

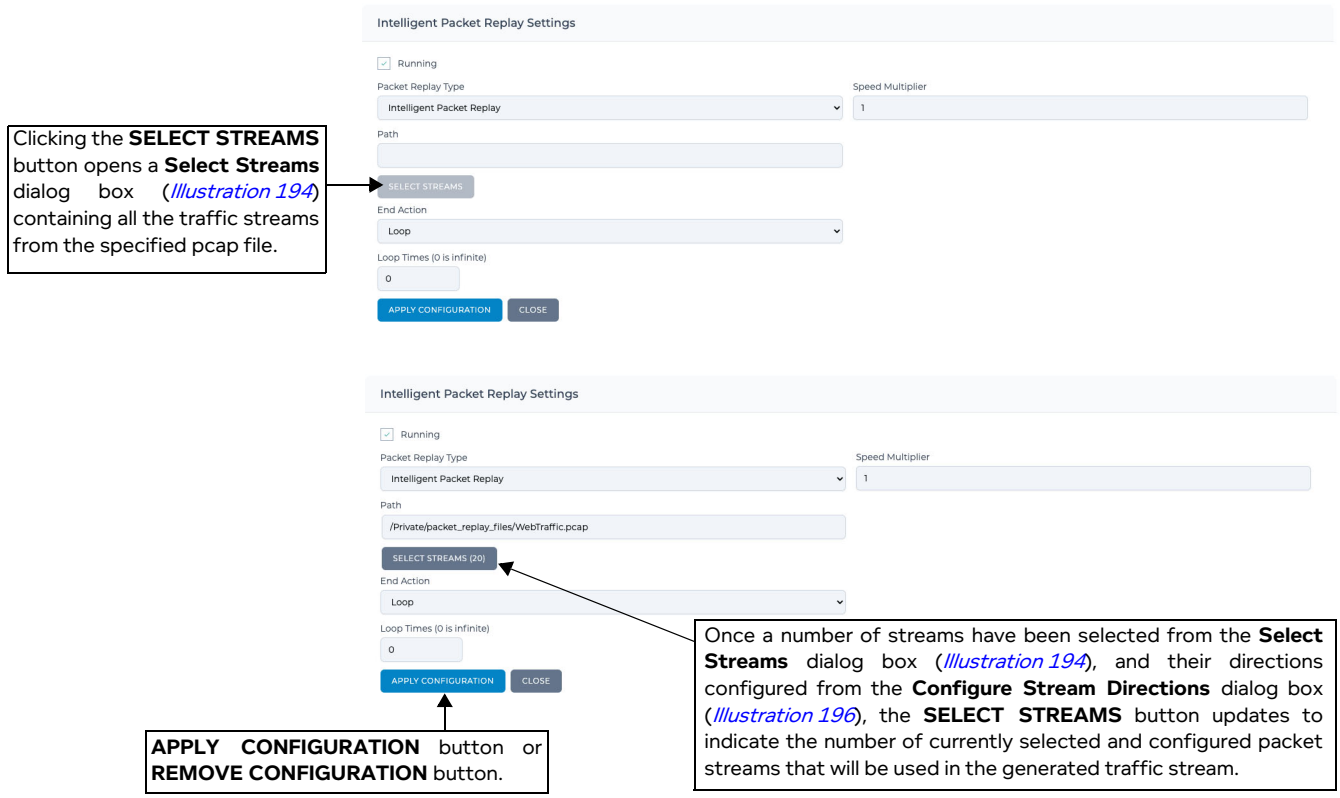
1-7-3. Web Interface Packet Replay Implementation in the Point-to-Point Designer

If you are using the Point-to-Point Designer, the packet replay functions are accessed via a **Packet Replay** button of the **Point To Point Designer** page (see *Illustration 71* on page 243) or **Point To Point (Dual) Designer** page (see *Illustration 72* on page 244).

1-7-3-1. Packet Replay Settings Dialog Box

Clicking on the **Packet Replay** button opens the **Packet Replay Settings** dialog box (see *Illustration 199*), letting you determine which type of packet replay function to use (either Passive Packet Replay or Intelligent Packet Replay), and to define all the associated parameters (i.e. select packet streams of interest from the pcap file, and choose their direction).

ILLUSTRATION 199 - POINT-TO-POINT PACKET REPLAY SETTINGS DIALOG BOX (INTELLIGENT PACKET REPLAY SHOWN)



The **Packet Replay Settings** dialog box contains the elements summarized in *Table 73* on page 603, and additionally contains the following elements:

- **Packet Replay Type** drop-down field - determines which type of packet replay function to use (either Passive Packet Replay or Intelligent Packet Replay).

  Note:

  Once you have selected and configured the packet replay function, the **Packet Replay Type** drop-down field becomes grayed out. If you remove the existing packet replay configuration by clicking the **REMOVE CONFIGURATION** button, the **Packet Replay Type** drop-down field becomes selectable.

- **SELECT STREAMS** button. Clicking on the **SELECT STREAMS** button opens the **Select Streams** dialog box (see *Illustration 194*). This invokes the two step stream configuration process, which is discussed in *The Stream Configuration Tool Dialog Boxes* on page 611.

- **APPLY CONFIGURATION** button or **REMOVE CONFIGURATION** button. The button that appears varies according to whether packet replay has already been configured.
  - Before packet replay has been configured, the **APPLY CONFIGURATION** button exists. Clicking the **APPLY CONFIGURATION** button will commit the existing packet replay configuration to the Point-to-Point network.
  - Once packet replay has been configured and applied by clicking the **APPLY CONFGURATION** button, the **REMOVE CONFIGURATION** button appears, letting you remove the existing packet replay configuration. Clicking the **REMOVE CONFIGURATION** button will remove the existing packet replay configuration from the Point-to-Point network.
- **CLOSE** button. Clicking this button returns you to the **Point To Point Designer** page (see *Illustration 71* on page 243) or **Point To Point (Dual) Designer** page (see *Illustration 72* on page 244).

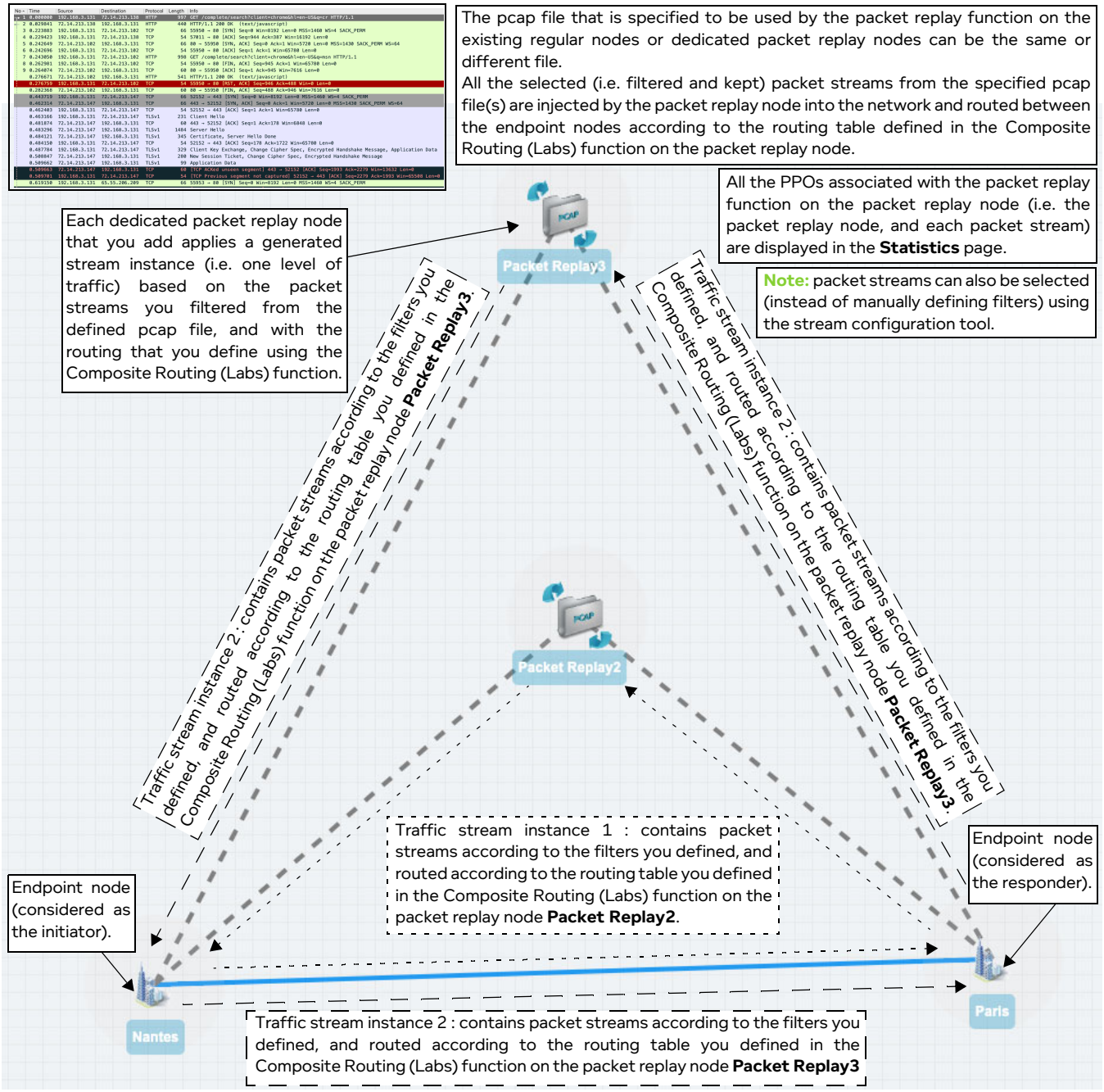
1-8. Packet Replay Implementation in the Multi-Point Designer

The sub-sections below describe how the packet replay functions are implemented on the NE-ONE back end and on the NE-ONE Web Interface in the Multi-Point Designer.

1-8-1. Back End Packet Replay Implementation and Web Interface Implementation in the Multi-Point Designer

Compared to the Point-to-Point Designer (which uses one invisible node to generate one traffic stream instance), the Multi-Point Designer lets you create multiple traffic stream instances on a per node basis (see *Illustration 200*).

ILLUSTRATION 200 - FUNCTION OVERVIEW OF HOW PACKET REPLAY WORKS IN THE MULTI-POINT DESIGNER (EXAMPLE WITH TWO DEDICATED PACKET REPLAY NODES)



In the Multi-Point Designer, each node can be used to inject packet streams into the network via the packet replay functions. Any node that is configured with the packet replay functions will create traffic (in a unique traffic stream instance). The more nodes you have in the Multi-Point network configured with the packet replay function, the more traffic (i.e. traffic stream instances) you create (see *Illustration 200* for a functional overview).

Compared to the Point-to-Point Designer (which automatically configures the routing between the endpoint nodes based on the packet stream directions, and uses link qualifications to target particular links), the Multi-Point Designer lets you (and requires you) to configure the routing of the traffic streams to target particular links. This routing is achieved using the Composite Routing (Labs) function on the Packet Replay node, and routing (either Composite Routing (Labs), Symmetric Routing (Expression) or IP Routing (Labs)) on the endpoint nodes.

You can add the traffic streams generated by the packet replay function into a Multi-Point network by one of the following two methods:

- By using an existing regular node (from the node categories such as **Standard**, **Gaming**, **IoT**, **LAN**, etc.), and applying and configuring the packet replay function to that existing node along with Composite Routing. In this case, the packet stream created by the packet replay function will use the Composite Routing that is you must define on that regular node.
  However, it is highly recommended not to use an existing regular node, because you cannot easily visualize the defined endpoints, and because the routing is not automatically generated. Because of this, we will only discuss the use of the dedicated packet replay node.
- By using a dedicated packet replay node. In addition to the regular node categories (such as **Standard**, **Gaming**, **IoT**, **LAN**, etc.), the Multi-Point Designer also has a special **Packet Replay** category within the **Node Icons** panel (see *Illustration 87* on page 318). The nodes in the **Packet Replay** category are dedicated to packet replay functionality, and already have either the Passive Packet Replay function or Intelligent Packet Replay function applied to them along with the Composite Routing (Labs) function, as follows:
  - the node represented by the  icon already has the Passive Packet Replay function along with the Composite Routing (Labs) function applied to it,
  - the node represented by the  icon already has the Intelligent Packet Replay function along with the Composite Routing (Labs) function applied to it.

Dedicated packet replay nodes let you define specific routing for the replayed packet streams, letting you test traffic on specific routes, without adjusting the existing routing tables of the existing regular nodes in your Multi-Point network.

For each level and type of traffic you want to create, you add a dedicated packet replay node into an existing Multi-Point network by dragging it into the Workspace, and then by doing the following:

- create links between the packet replay node and existing endpoint nodes to define between which endpoint nodes the generated traffic goes,
- define the packet streams that you want to select for the generated traffic stream by using filtering,
- define the routing tables used by the filtered packet streams using the Composite Routing (Labs) function,
- define the general packet replay parameters used by the replayed packet stream.

For more information on how to do this, see the example described in *Packet Replay Example in Multi-Point Networks* on page 667, along with the theoretical discussion below.

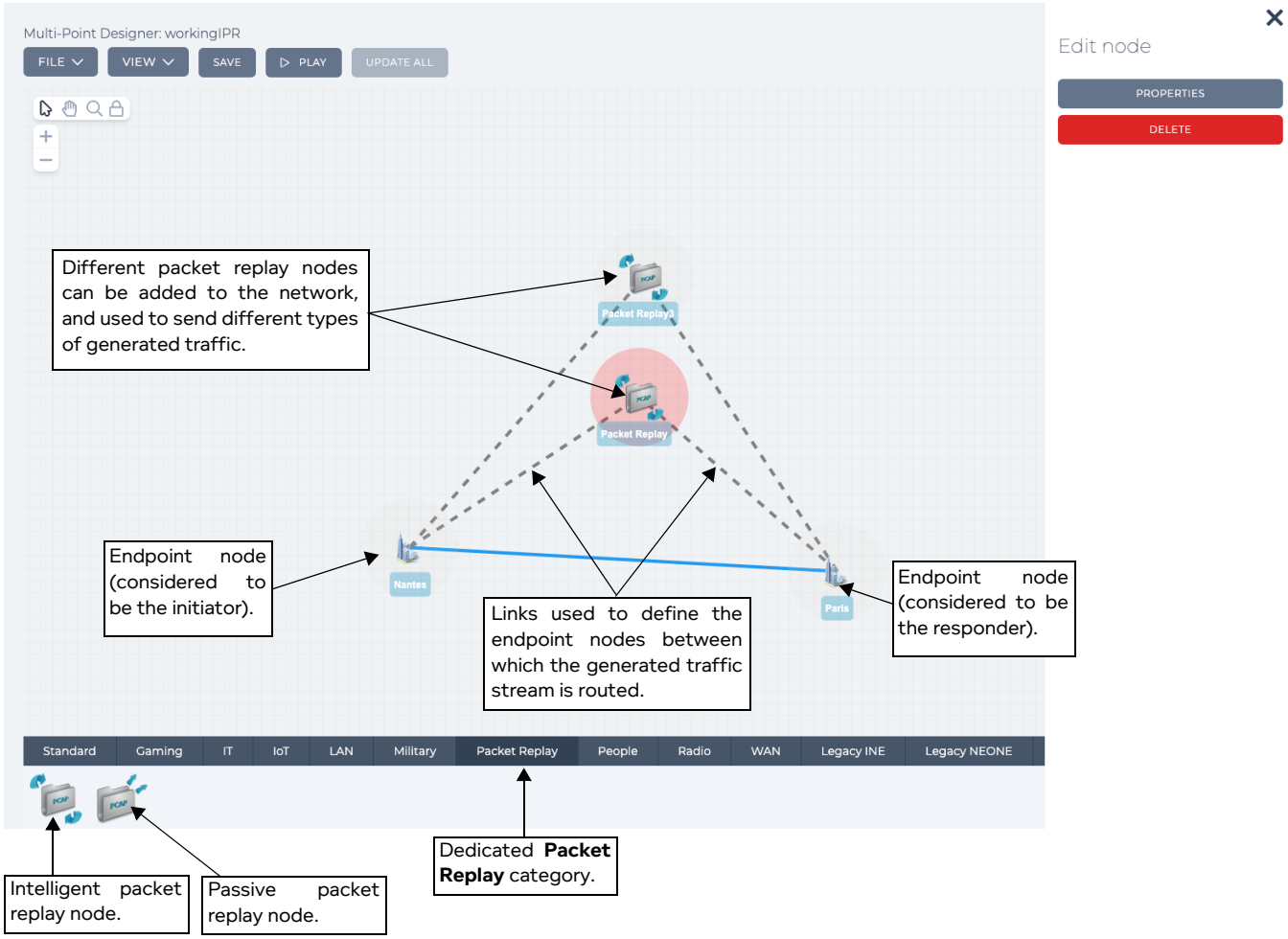
Each packet replay node you add to a Multi-Point network takes the naming format **Packet Replay<N>**,

(e.g. Packet Replay, Packet Replay1, Packet Replay2, Packet Replay3, etc.), where <N> corresponds to the order in which it was added onto the Multi-Point Workspace. For example, if a dedicated packet replay node was added after two regular nodes (which are initially called Node0 and Node1), the dedicated packet replay node will be called Packet Replay2. Similarly, if you built a Multi-Point network from scratch, and the dedicated packet replay node was the first to be added onto the Workspace, it would be called Packet Replay (i.e. without the 0). In *Illustration 201* we see an example where two dedicated packet replay nodes exist in the Multi-Point network, where Packet Replay was added first, and Packet Replay3 was added after the two nodes Nantes and Paris.

In the Multi-Point Designer the packet replay functions are accessed via the node's **Advanced Node Properties** window, which is accessible by clicking on the **PROPERTIES** button within the **Edit node** panel of the node.

The **Edit node** panel (see *Illustration 201*) for dedicated packet replay nodes is intentionally different to that of the regular nodes (see *Illustration 88* on page 319), and only contains the elements listed in *Table 75*.

ILLUSTRATION 201 - THE EDIT NODE PANEL FOR A PACKET REPLAY NODE



The **Edit node** panel for packet replay nodes does not contain the other elements (such as name, location, etc.) of regular nodes. This is normal as the packet replay node is not acting as a regular node within the Multi-Point network, but functioning to replay packet streams into the existing network.

TABLE 75 - EDIT NODE PANEL ELEMENTS FOR PACKET REPLAY NODES ON MULTI-POINT NETWORKS

Edit node element	Description
PROPERTIES button	Clicking this button opens a **Node Properties** window similar to *Illustration 202* on page 632, with the Composite Routing (Labs) function and either the Passive Packet Replay Function or Intelligent Packet Replay function added by default. These functions let you define all the properties (i.e. packet replay parameters, and routing of the replayed packet streams) of the packet replay node.
DELETE button	Clicking this button invokes a **Confirm delete** dialog box, which upon confirming (clicking **OK**) immediately deletes the packet replay node from the network, and returns you to the **Multi-Point Designer** page. **Note:** Clicking outside the **Confirm delete** dialog box cancels the delete operation, and returns you to the **Multi-Point Designer** page.

Clicking the **PROPERTIES** button opens the "initial" **Advanced Node Properties** window (see *Illustration 202*) for the packet replay node. We refer to this as the "initial" **Advanced Node Properties** window, because initially nothing is configured in terms of packet replay.

Note:

In the sentence above we say that nothing is configured "in terms of packet replay". However, this does not imply that nothing is configured in terms of the rest of the Multi-Point network. Before adding and configuring a Packet Replay node to your Multi-Point network, you must have fully configured the Multi-Point network with all nodes, links and routing according to your requirements.

Completely configuring the nodes, links and routing on the Multi-Point network before adding and configuring a Packet Replay node will ensure that all the existing routing of the Multi-Point network is inherited and pushed into the routing tables associated with the packet replay function, and that the Port In routing parameters of the connected endpoint nodes are pushed into the Spoof Port In values in the Composite Routing (Labs) function on the Packet Replay node.

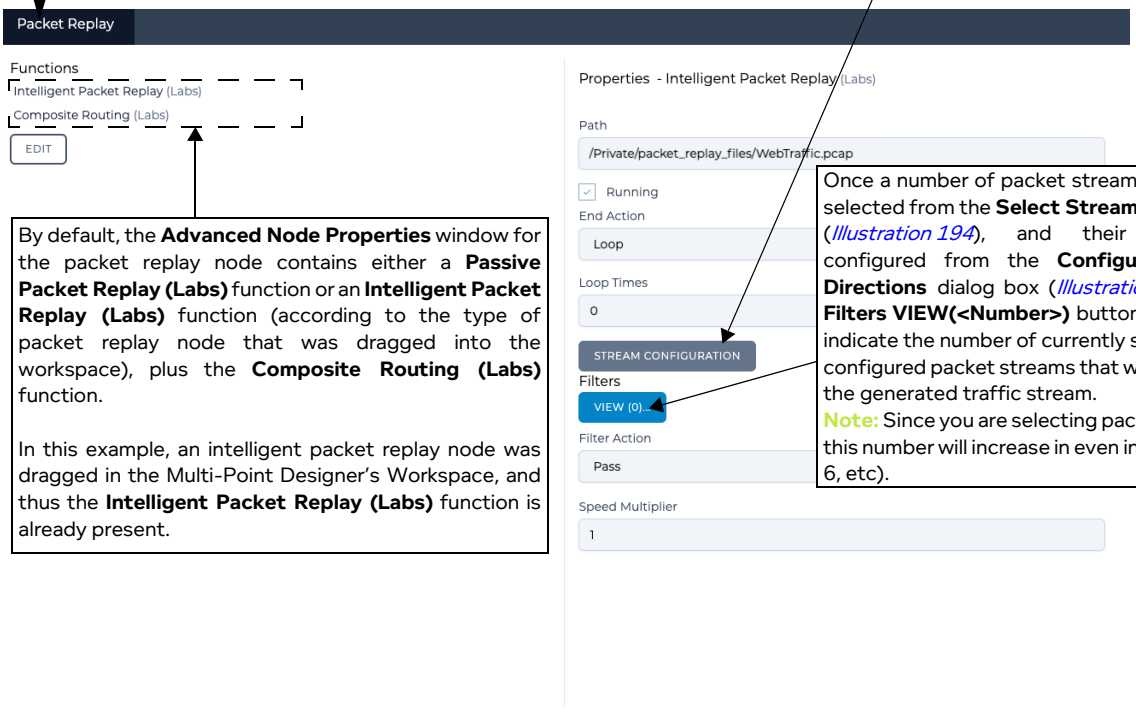
ILLUSTRATION 202 - DEFAULT ADVANCED NODE PROPERTIES WINDOW FOR A PACKET REPLAY NODE (EXAMPLE OF AN INTELLIGENT PACKET REPLAY NODE)

Clicking the **STREAM CONFIGURATION** button opens a **Select Streams** dialog box (*Illustration 194*) containing all the packet streams from the specified pcap file.

Once you have selected the packet streams to be used from the **Select Streams** dialog box (*Illustration 194*), and configured their directions from the **Configure Stream Directions** dialog box (*Illustration 196*), the selected packet streams get automatically applied into the **Filters** configuration, and the directions you configured get automatically applied into the **Composite Routing (Labs)** configuration.

Note: You can choose not to use the stream configuration dialog boxes (which are accessed via clicking the **STREAM CONFIGURATION** button), and manually configure the Filters and Composite Routing from the offset. However, for expediency, Calnex recommend that you use the stream configuration dialog boxes to initially configure the generated traffic stream, and if necessary, make further changes within the Filters and Composite Routing.

Node name of packet replay node that was selected in the Multi-Point Designer's Workspace. In this example, the first packet replay node for an intelligent packet replay node is selected as it is called **Packet Replay**.



By default, the **Advanced Node Properties** window for the packet replay node contains either a **Passive Packet Replay (Labs)** function or an **Intelligent Packet Replay (Labs)** function (according to the type of packet replay node that was dragged into the workspace), plus the **Composite Routing (Labs)** function.

In this example, an intelligent packet replay node was dragged in the Multi-Point Designer's Workspace, and thus the **Intelligent Packet Replay (Labs)** function is already present.

Once a number of packet streams have been selected from the **Select Streams** dialog box (*Illustration 194*), and their directions configured from the **Configure Stream Directions** dialog box (*Illustration 196*), the **Filters VIEW(<Number>)** button updates to indicate the number of currently selected and configured packet streams that will be used in the generated traffic stream.

Note: Since you are selecting packet streams, this number will increase in even integers (2, 4, 6, etc).

OK button (returns you to the **Edit node** panel).

To configure packet replay from the **Advanced Node Properties** window, you do the following:

1. Click on the **Passive Packet Replay (Labs)** or **Intelligent Packet Replay (Labs)** function from the list of Functions.

   The **Properties** area updates corresponding to either the Passive Packet Replay function or Intelligent Packet Replay function.
2. In the **Properties** area, define the general packet replay parameters, as follows:

a. In the **Path** field, specify a valid path to the pcap file.
b. Enable the **Running** check box.
c. Select the appropriate action (**Loop** or **Stop**) from the **End Action** drop-down field.
d. Optionally modify the **Speed Multiplier**.

3. In the **Properties** area, select the packet streams that you want to include in the generated traffic stream.

   There are two methods to select the packet streams.

   Method 1: Stream Configuration Tool

   You can use the stream configuration tool, which automates selecting the packet streams of interest, and if necessary correct their directions. The stream configuration tool is limited to 100 packet streams. If you want to generate a traffic stream containing more than 100 packet streams, you must use filtering. To use the stream configuration tool, click the **STREAM CONFIGURATION** button. A series of dialog boxes will appear (described in *The Stream Configuration Tool Dialog Boxes* on page 611), which allow you to select the packet streams and configure their directions.

   Any of the packet streams that you select and directions you configure get pushed into the Filter table and the Routing table of the Composite Routing (Labs) function on the Packet Replay node, respectively. The packet streams you select get pushed into the Filter table on the Packet Replay node. The routing associated with the packet stream directions you configure get pushed into the Routing table of the Composite Routing (Labs) function of the Packet Replay node.

   Additionally, the routing associated with the packet stream directions you configure also get pushed into the Routing table of the routing function (either Composite Routing (Labs), Symmetric Routing (Expression) or IP Routing (Labs)) on the endpoint nodes that are connected to the Packet Replay node.

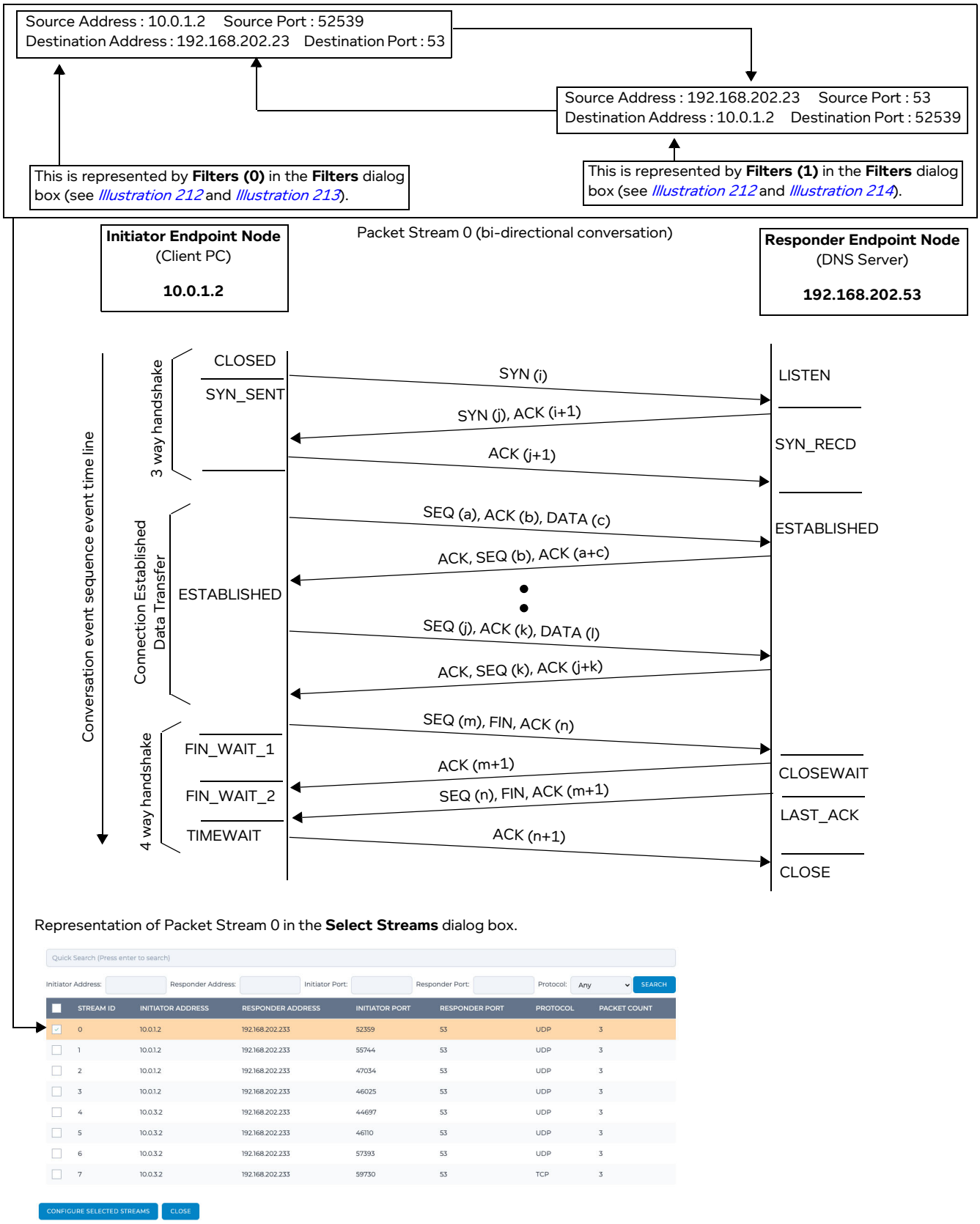
   Each packet stream that you select will generate a pair of **Filter(N)** rows in the Filter table (see *Illustration 212*, *Illustration 213*, and *Illustration 214*). This is normal since a packet stream is a bi-directional conversation between an initiator endpoint node, and a responder endpoint node, both of which whose associated packets will have a source address/port and destination address/port as shown in the example below *Illustration 203*. In effect, the streams selection tool is visually filtering and selecting at the packet stream level and constructs a pair of packet filters, while the Filter table is filtering and selecting at the packet level within the packet stream.

Note:

The stream configuration tool will only create the "fixed" filter rules (i.e. maximum and minimum values are the same) for a fixed source address, fixed destination address, fixed source port, and fixed destination port (see *Illustration 213*, and *Illustration 214* as examples). The stream configuration tool will not create the filter rules based on ranges. This is normal, as when you use the stream configuration tool you are selecting separate streams, and the stream configuration tool creates a separate pair of "fixed" filters (i.e. no ranges) based on each of the selected streams. If you want more sophisticated filtering rules using ranges, then use the tradition method of filtering discussed in the *Method 2: Using Filters* section below, or edit the filtering rules generated by the stream configuration tool.

If you use the traditional method of filtering, you must think to set up a pair of packet-based filters for each packet stream that you want to add into the generated traffic stream. For example, if you were to follow the example described in *Packet Replay Example in Multi-Point Networks* on page 667, but not use the stream configuration tool, you would create 20 filters for the 10 packet streams of interest as summarized in *Table 78* on page 690.

ILLUSTRATION 203 - EXAMPLE OF A PACKET STREAM (CONVERSATION) FOR DNS TRAFFIC



Representation of Packet Stream 0 in the **Select Streams** dialog box.

Each packet stream has a direction that is configured. Based upon the direction that is configured for each packet stream, the stream configuration tool will automatically create/append the following routes to the existing routing tables on the Packet Replay node and on the endpoint nodes:

- Typically create two "packet replay" routes in the Composite Routes (Lab) function on the Packet Replay node. The order in which those routes appear will vary, and correspond to the order in which the links were created in the Multi-Point Designer. Here we have said "typically", because the number of routes that get created depend on the number of streams that are selected, and the number unique pairs of initiator / responder IP addresses that exist in the selected packet streams. See the note below for more information.
- Append one "packet replay" route in the routing function (either Composite Routing (Labs), Symmetric Routing (Expression), or IP Routing (Labs)) on the Initiator endpoint node that is connected to the Packet Replay node via a link. The order in which this route appears will vary, and correspond to the order in which links were created in the Multi-Point Designer.
- Append one "packet replay" route in the routing function (either Composite Routing (Labs), Symmetric Routing (Expression), or IP Routing (Labs)) on the Responder endpoint node that is connected to the Packet Replay node via a link. The order in which this route appears will vary, and correspond to the order in which links were created in the Multi-Point Designer.

Note:

The routing function that exists on the endpoint node varies according to the Multi-Point network type in use. For example, the endpoint nodes on a Cloud or Hub and Spoke type Multi-Point network use the Composite Routing (Labs) function, whereas the endpoint nodes on a Mesh type Multi-Point network use the IP Routing (Labs) function. The endpoint nodes that were created when exporting a Point-to-Point network to a Multi-Point network us the Symmetric Routing (Expression) function.

ILLUSTRATION 204 - EXAMPLE OF A PACKET STREAM (CONVERSATION) DIRECTION CONFIGURATION

For example, imagine the Packet Stream 0 selected above in *Illustration 203* and whose direction is configured as shown in *Illustration 204* for the Multi-Point network shown in *Illustration 205*. The stream configuration tool will automatically create/append the following routes to the existing routing tables on the Packet Replay node and on the Nantes/Paris endpoint nodes:

- Two "packet replay" routes in the Composite Routes (Lab) function on the Packet Replay node, called **Routes (0)** and **Routes (1)** (see *Illustration 206*, *Illustration 207* and *Illustration 208*).

Note:

In this example, one stream is selected. If more than one stream is selected, then multiple "packet replay" routes are automatically added into the Composite Routes (Lab) function on the Packet Replay node. The number of "packet replay" routes that get automatically can vary depending on the unique pairs of initiator / responder IP addresses that exist in the selected packet streams. If we look at *Table 77* on page 688 for the example described in *Packet Replay Example in Multi-Point Networks* on page 667, we see that for two sets of five streams selected for two different initiator IP addresses, there is a split of 6 routes for first initiator IP address versus 4 routes for the second initiator IP address. At first this may initially seem strange. However, upon close

examination of the packet streams selected for the second IP initiator address, we see that there are only three unique initiator / responder address IP pairs opposed to five unique initiator / responder IP address pairs for the first initiator address. The second initiator will have four routes created (i.e. one route for the initiator and three routes for the three unique responders). The first initiator will have six routes created (i.e. one route for the initiator and five routes for the five unique responders).

- One "packet replay" route called **Routes (1)** (see *Illustration 209*) in the routing function (either Composite Routing (Labs), Symmetric Routing (Expression), or IP Routing (Labs)) on the Nantes Initiator endpoint node.
  This "packet replay" route gets created after the "framework" route **Routes (0)** that is initially automatically created when building the link between the Nantes and Paris endpoint nodes.
- One "packet replay" route called **Routes (1)** (see *Illustration 210*) in the routing function (either Composite Routing (Labs), Symmetric Routing (Expression), or IP Routing (Labs)) on the Paris Initiator endpoint node.
  This "packet replay" route gets created after the "framework" routes **Routes (0)** that is initially automatically created when building the link between the Nantes and Paris endpoint nodes.

Note:

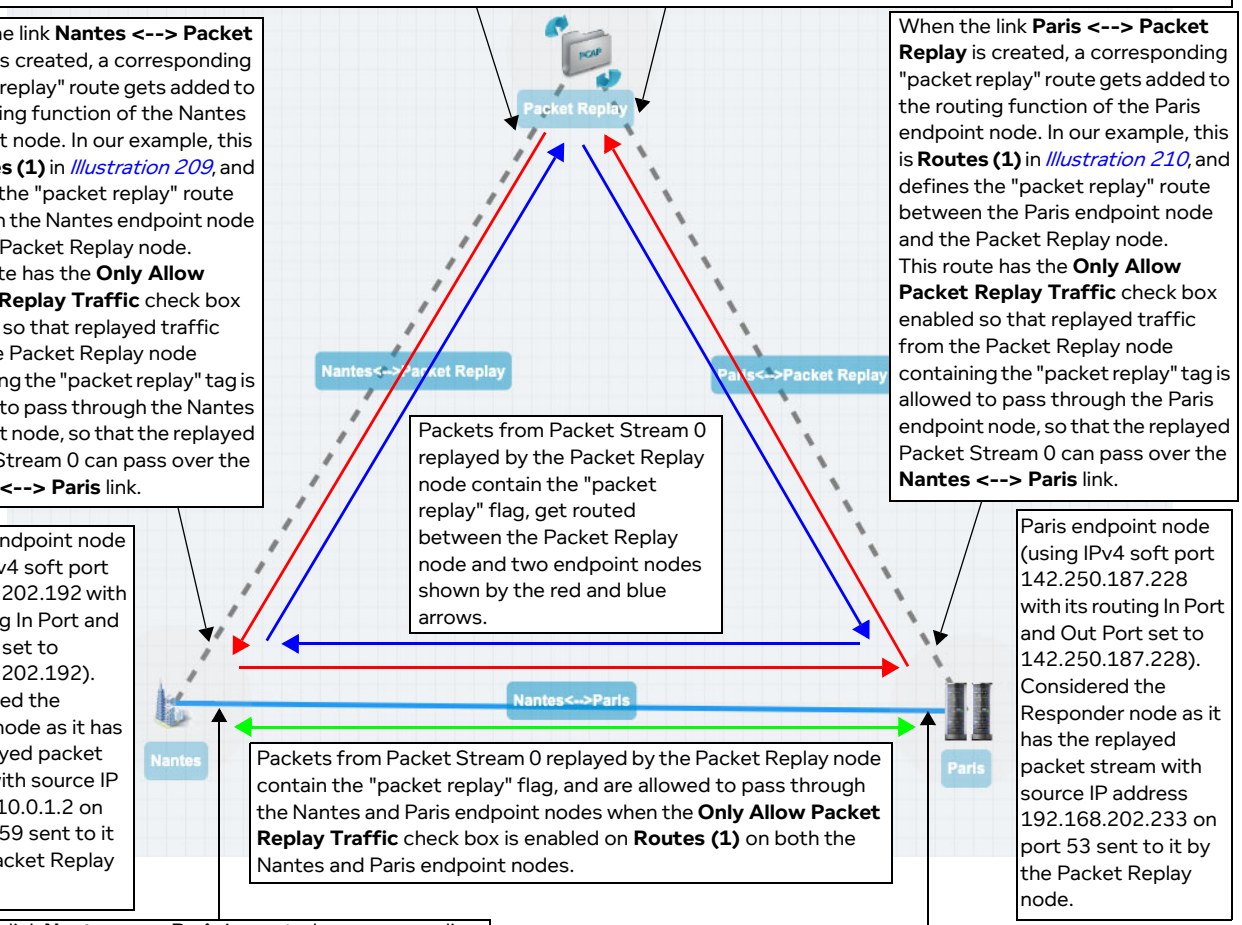
The stream configuration tool only ever automatically creates one "packet replay" route on the endpoint nodes. This "packet replay" route must always be at the bottom of the routing table on the endpoint node. The stream configuration tool never automatically creates the other required routes for targeting the replayed packet streams down certain links. You must always manually create the routes for targeting the replayed packet streams down certain links yourself, and ensure that they are all above the "packet replay" route that gets automatically created by the stream configuration tool. For an example on how to do this, look at the steps 18 and 19 described below in *Packet Replay Example in Multi-Point Networks* on page 667.

ILLUSTRATION 205 - EXAMPLE MULTI-POINT NETWORK TO ILLUSTRATE HOW THE STREAM CONFIGURATION TOOL PUSHES THE STREAM CONFIGURATION INTO THE ROUTING TABLES

The Packet Replay node has one Packet Stream 0 selected and configured as above in *Illustration 203* and *Illustration 204*. Its Composite Routing (Labs) function will have two "packet replay - framework" routes (**Routes(0)** and **Routes(1)**) automatically added to it, as shown in *Illustration 206*, *Illustration 207*, and *Illustration 208*, corresponding to the selected Packet Stream 0 that will be replayed between the Nantes and Paris endpoint nodes.
These "packet replay - framework" routes intentionally do not have the **Only Allow Packet Replay Traffic** check box enabled because they are originating on the Packet Replay node itself, which generates the packet replay packet streams (i.e. packet replay traffic) that contains flags with the "packet replay" tag. Because the Packet Replay node is generating the packet streams containing the "packet replay" flag, by default it is already allowing those replayed packet streams to pass, and thus the **Only Allow Packet Replay Traffic** check box does not need to be enabled.
Conceptually speaking, it is as if these routes are intended for routing the replayed packets from Packet Stream 0 between the Nantes and Paris endpoint nodes (even if they are actually routing between the Packet Replay node and the Nantes / Paris endpoint nodes). In this sense, it is as if the replayed packets from Packet Stream 0 are like any other packet on the network and going between the Nantes and Paris endpoint nodes (even if they are actually originating/returning from the Packet Replay node).

Also, these routes (**Routes(0)** and **Routes(1)**) have an additional **Spoof Port In** parameter, which will inherit the Port In routing configuration of the Nantes and Paris endpoint nodes, respectively. For example, the Nantes endpoint node routing is configured to use IPv4 soft port 192.168.202.192 on the Port In, and so the **Spoof Port In** parameter of **Routes(0)** will be automatically configured to 192.168.202.192. Similarly, the Paris endpoint node routing is configured to use IPv4 soft port 142.250.187.228 on the Port In, and so the **Spoof Port In** parameter of **Routes(1)** will be automatically configured to 142.250.187.228. The **Spoof Port In** parameter is required and used on the Composite Routing (Labs) function on the Packet Replay node so that the replayed Packet Stream 0 from the specified pcap file looks like it is coming from the spoofed Port In of each of the endpoint nodes rather than the original locations specified in the pcap file.

When the link **Nantes <--> Packet Replay** is created, a corresponding "packet replay" route gets added to the routing function of the Nantes endpoint node. In our example, this is **Routes (1)** in *Illustration 209*, and defines the "packet replay" route between the Nantes endpoint node and the Packet Replay node.
This route has the **Only Allow Packet Replay Traffic** check box enabled so that replayed traffic from the Packet Replay node containing the "packet replay" tag is allowed to pass through the Nantes endpoint node, so that the replayed Packet Stream 0 can pass over the **Nantes <--> Paris** link.



When the link **Paris <--> Packet Replay** is created, a corresponding "packet replay" route gets added to the routing function of the Paris endpoint node. In our example, this is **Routes (1)** in *Illustration 210*, and defines the "packet replay" route between the Paris endpoint node and the Packet Replay node.
This route has the **Only Allow Packet Replay Traffic** check box enabled so that replayed traffic from the Packet Replay node containing the "packet replay" tag is allowed to pass through the Paris endpoint node, so that the replayed Packet Stream 0 can pass over the **Nantes <--> Paris** link.

Packets from Packet Stream 0 replayed by the Packet Replay node contain the "packet replay" flag, get routed between the Packet Replay node and two endpoint nodes shown by the red and blue arrows.

Nantes endpoint node (using IPv4 soft port 192.168.202.192 with its routing In Port and Out Port set to 192.168.202.192). Considered the Initiator node as it has the replayed packet stream with source IP address 10.0.1.2 on port 52359 sent to it by the Packet Replay node.

Paris endpoint node (using IPv4 soft port 142.250.187.228 with its routing In Port and Out Port set to 142.250.187.228). Considered the Responder node as it has the replayed packet stream with source IP address 192.168.202.233 on port 53 sent to it by the Packet Replay node.

Packets from Packet Stream 0 replayed by the Packet Replay node contain the "packet replay" flag, and are allowed to pass through the Nantes and Paris endpoint nodes when the **Only Allow Packet Replay Traffic** check box is enabled on **Routes (1)** on both the Nantes and Paris endpoint nodes.

When the link **Nantes <--> Paris** is created, a corresponding "framework" route gets added to the routing function of the Nantes endpoint node. In our example, this is **Routes (0)** in *Illustration 209* and, defines the "framework" route between the Nantes endpoint node and the Paris endpoint node.

When the link **Nantes <--> Paris** is created, a corresponding "framework" route gets added to the routing function of the Paris endpoint node. In our example, this is **Routes (0)** in *Illustration 210* and, defines the "framework" route between the Nantes endpoint node and the Paris endpoint node.

Note:

It is interesting to consider the routes associated with red and blue "traffic loops" shown in *Illustration 205* in terms when they are required. The Intelligent Packet Replay function has to be part of this "traffic loop" as is needs to know the status of the packets on the on the Initiator and Responder endpoint nodes. For example, it needs to know when a packet left the Initiator node, arrived at the Responder node, and know what to do next, and to dispose of the packets. This is why the icon representing the packet replay node with the Intelligent Packet Reply function has two circular, "loop type" arrows. There is a two way conversation between packet replay node with the Packet Replay and the endpoint nodes.

Conversely, the icon representing the packet replay node with the Passive Packet Reply function has two straight arrows, indicating how the replayed packets are passively pushed onto the network. The Passive Replay Function does not need to know the status of the packets on the Initiator and Responder nodes, and thus does not need to be part of these red and blue "traffic loops" shown in *Illustration 205*.

ILLUSTRATION 206 - PACKET REPLAY COMPOSITE ROUTING TABLE (UNEXPANDED) EXAMPLE

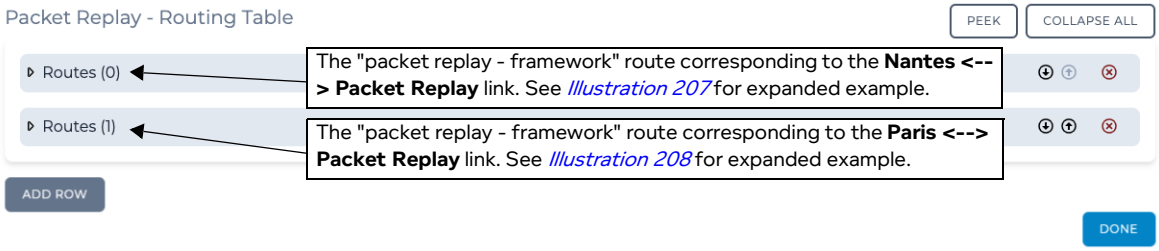


ILLUSTRATION 207 – EXAMPLE "PACKET REPLAY – FRAMEWORK" ROUTE FOR STREAM 0 FOR THE LINK BETWEEN PACKET REPLAY NODE AND NANTES ENDPOINT NODE

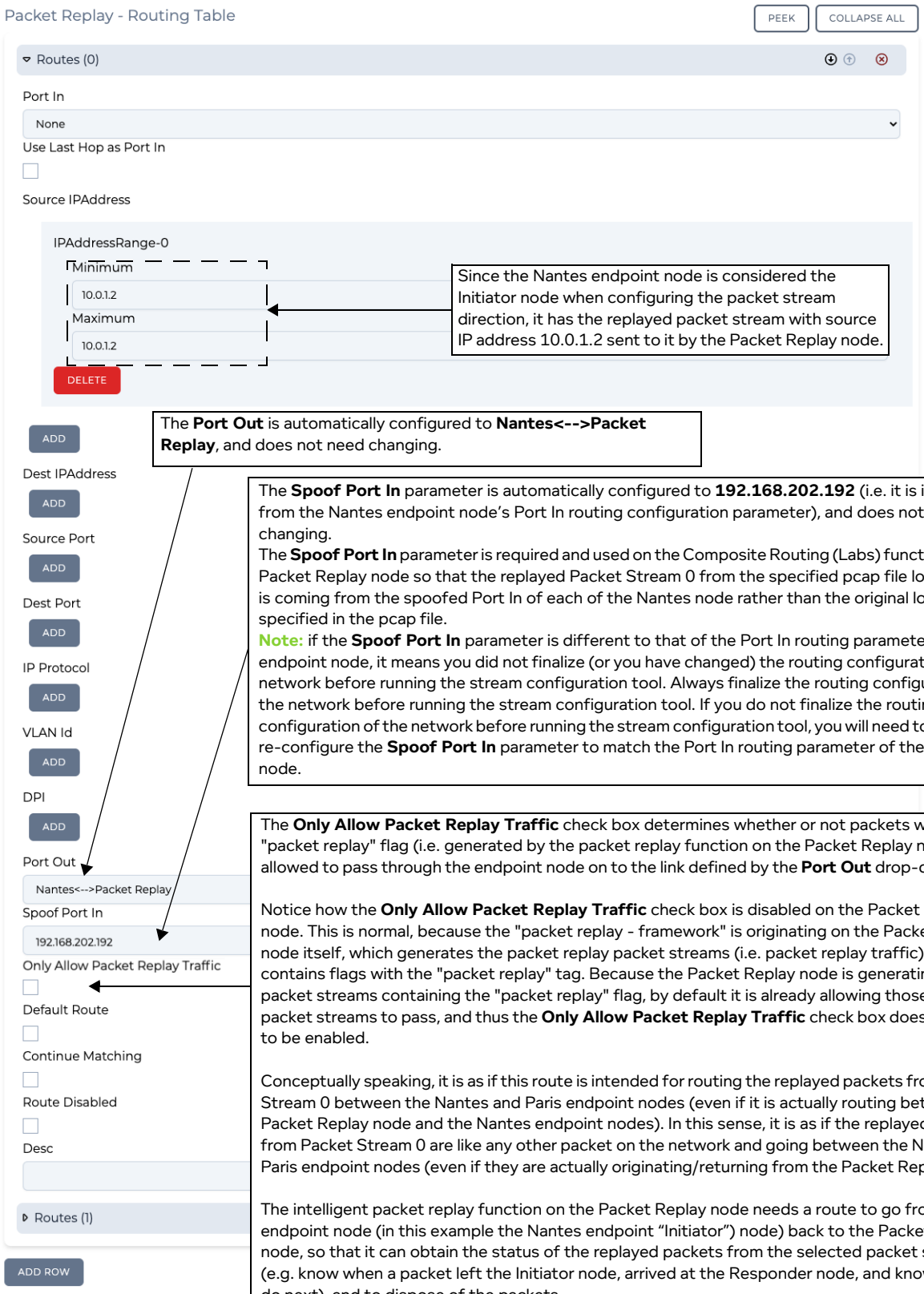


ILLUSTRATION 208 - EXAMPLE "PACKET REPLAY - FRAMEWORK" ROUTE FOR STREAM 0 FOR THE LINK BETWEEN PACKET REPLAY NODE AND PARIS ENDPOINT NODE

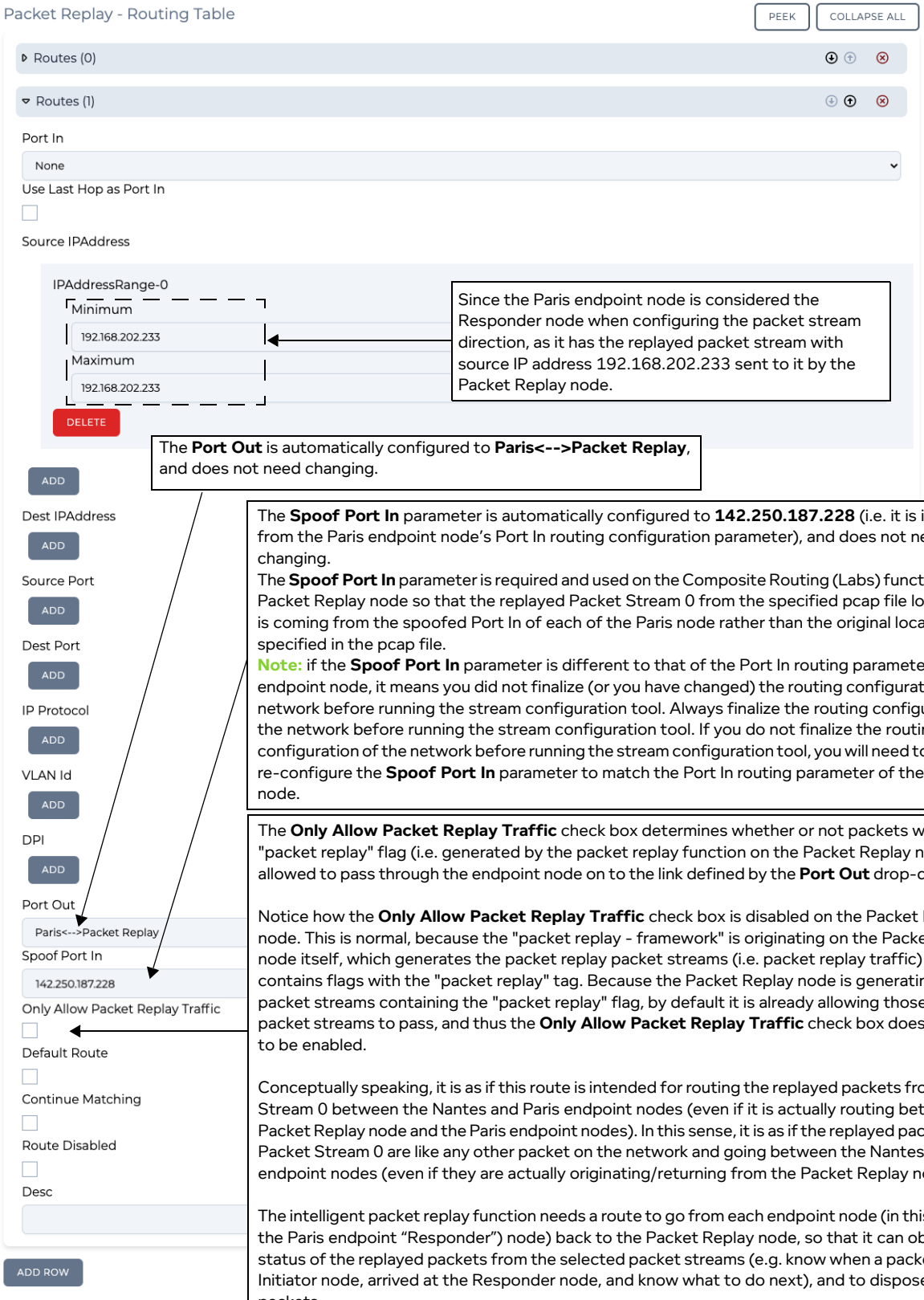
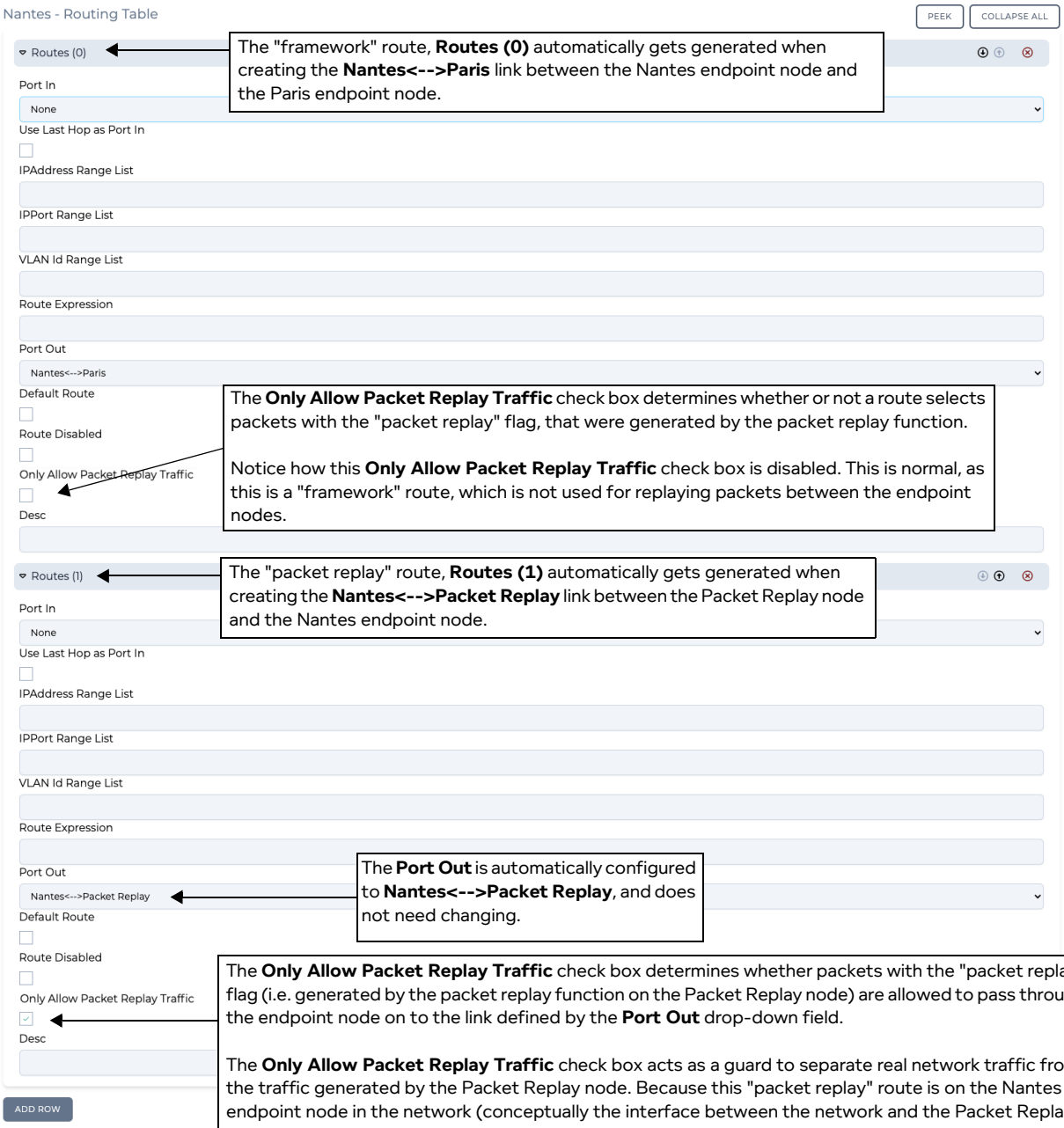


ILLUSTRATION 209 - EXAMPLE ROUTING TABLE FOR NANTES ENDPOINT NODE



The "framework" route, **Routes (0)** automatically gets generated when creating the **Nantes<-->Paris** link between the Nantes endpoint node and the Paris endpoint node.

The **Only Allow Packet Replay Traffic** check box determines whether or not a route selects packets with the "packet replay" flag, that were generated by the packet replay function.

Notice how this **Only Allow Packet Replay Traffic** check box is disabled. This is normal, as this is a "framework" route, which is not used for replaying packets between the endpoint nodes.

The "packet replay" route, **Routes (1)** automatically gets generated when creating the **Nantes<-->Packet Replay** link between the Packet Replay node and the Nantes endpoint node.

The **Port Out** is automatically configured to **Nantes<-->Packet Replay**, and does not need changing.

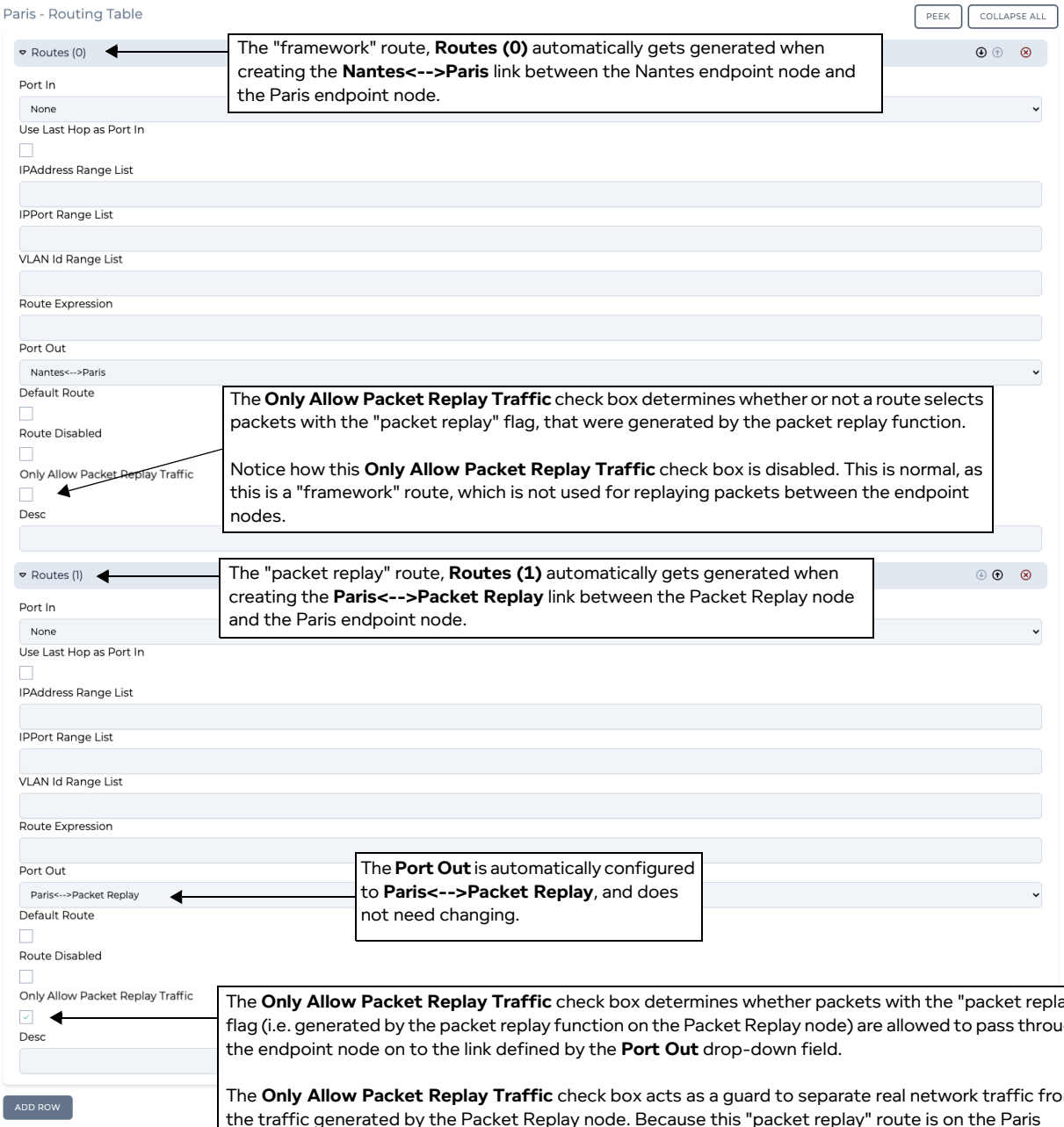
The **Only Allow Packet Replay Traffic** check box determines whether packets with the "packet replay" flag (i.e. generated by the packet replay function on the Packet Replay node) are allowed to pass through the endpoint node on to the link defined by the **Port Out** drop-down field.

The **Only Allow Packet Replay Traffic** check box acts as a guard to separate real network traffic from the traffic generated by the Packet Replay node. Because this "packet replay" route is on the Nantes endpoint node in the network (conceptually the interface between the network and the Packet Replay node), the **Only Allow Packet Replay Traffic** check box must be enabled to allow the packets from the replayed packet stream 0 (with the "packet replay" tag) on to the network. Further more, this route must be the lowest priority on the endpoint node.

Since this route is allowing packets with the "packet replay" flag and to pass through the Nantes endpoint node, the **Only Allow Packet Replay Traffic** check box is automatically enabled when using the stream configuration tool.

Note: If you are not using the stream configuration tool, and manually creating routes yourself, then the **Only Allow Packet Replay Traffic** check box is disabled by default. In this case you must think to enable it for the "packet replay" route going between each endpoint node and the Packet Replay node.

ILLUSTRATION 210 - EXAMPLE ROUTING TABLE FOR PARIS ENDPOINT NODE



Method 2: Using Filters

A more traditional way of selecting the packet streams of interest for the generated traffic stream is to use filtering. Compared to the stream configuration tool (which is effectively a filter with filter action pass), filtering is more powerful than using the stream configuration tool as it lets you select more than 100 packet streams, and lets you apply more sophisticated filtering criteria. Filtering lets you build more sophisticated filters on the packet streams and decide whether or not those filtered packet streams are passed, or dropped.

However, filtering requires that you already know the contents of the specified pcap file, and have viewed it in a tool such as Wireshark so that you can decide on which packet streams to filter, and which filter criteria to define.

The **Properties** area contains a **Filters VIEW<N>** button and a **Filter Action** drop-down field.

The **Filter Action** drop-down field contains the following choices:

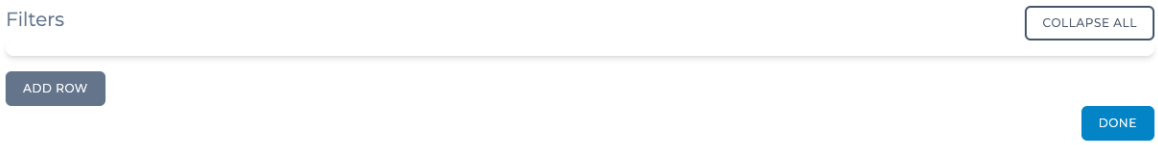
- **Pass** - This is the default choice. Pass will let the filtered packet streams pass into the generated traffic stream. Selecting **Pass** lets the filtered packet streams go into the generated traffic stream. That is any of the filtered packet streams will be in the generated packet stream.
- **Drop** - Drop will drop the filtered packet streams, and let the remaining unfiltered packet streams pass into the generated traffic stream. Selecting **Drop** lets the unfiltered packet streams go into the generated traffic stream. That is any of the unfiltered packet streams will be in the generated packet stream.

Clicking on the **Filters VIEW<N>** button opens an "initial" **Filters** dialog box (see *Illustration 211*). We say "initial" as at this stage there are no defined filters.

Note:

If you have used the stream configuration tool before clicking the **Filters VIEW<N>** button, then the **Filters** dialog box will not be empty, and will already contain a pair of rows for each of the packet streams that were selected in the streams selection tool. The reasons for this are described above within the *Method 1: Stream Configuration Tool* section above.

ILLUSTRATION 211 - INITIAL PACKET REPLAY FILTERS DIALOG BOX

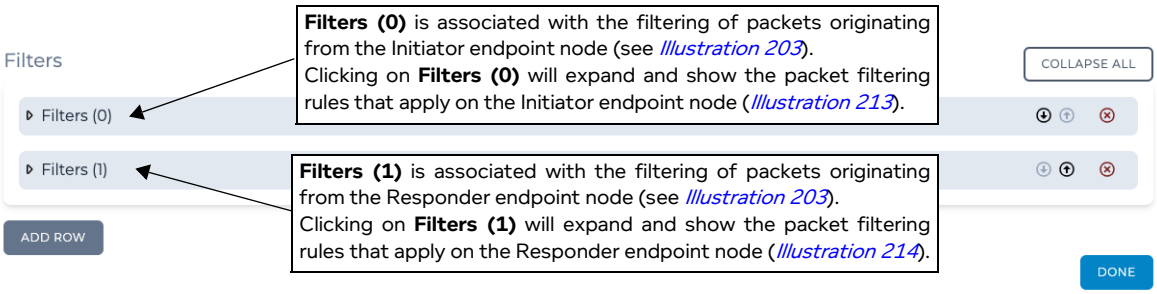


When manually configuring the filters on the Packet Capture node, click the **ADD ROW** button for each filter you want to add.

Note:

Since a packet stream is a bi-directional conversation between two endpoint nodes containing a pair of packets (see *Illustration 203* for the explanation), you must think to set up two filters for each packet stream. One filter for the conversation direction going from the Initiator node to Responder node. And a second filter for the for the conversation direction going from to Responder node to the Initiator Node.

ILLUSTRATION 212 - PACKET REPLAY FILTERS DIALOG BOX (UNEXPANDED) FOR ONE FILTER STREAM



Upon clicking the **ADD ROW** button, a **Filters** page opens similar to those shown in *Illustration 213* and *Illustration 214*.

ILLUSTRATION 213 - PACKET REPLAY FILTERS DIALOG BOX (EXPANDED) FOR ONE FILTER STREAM A

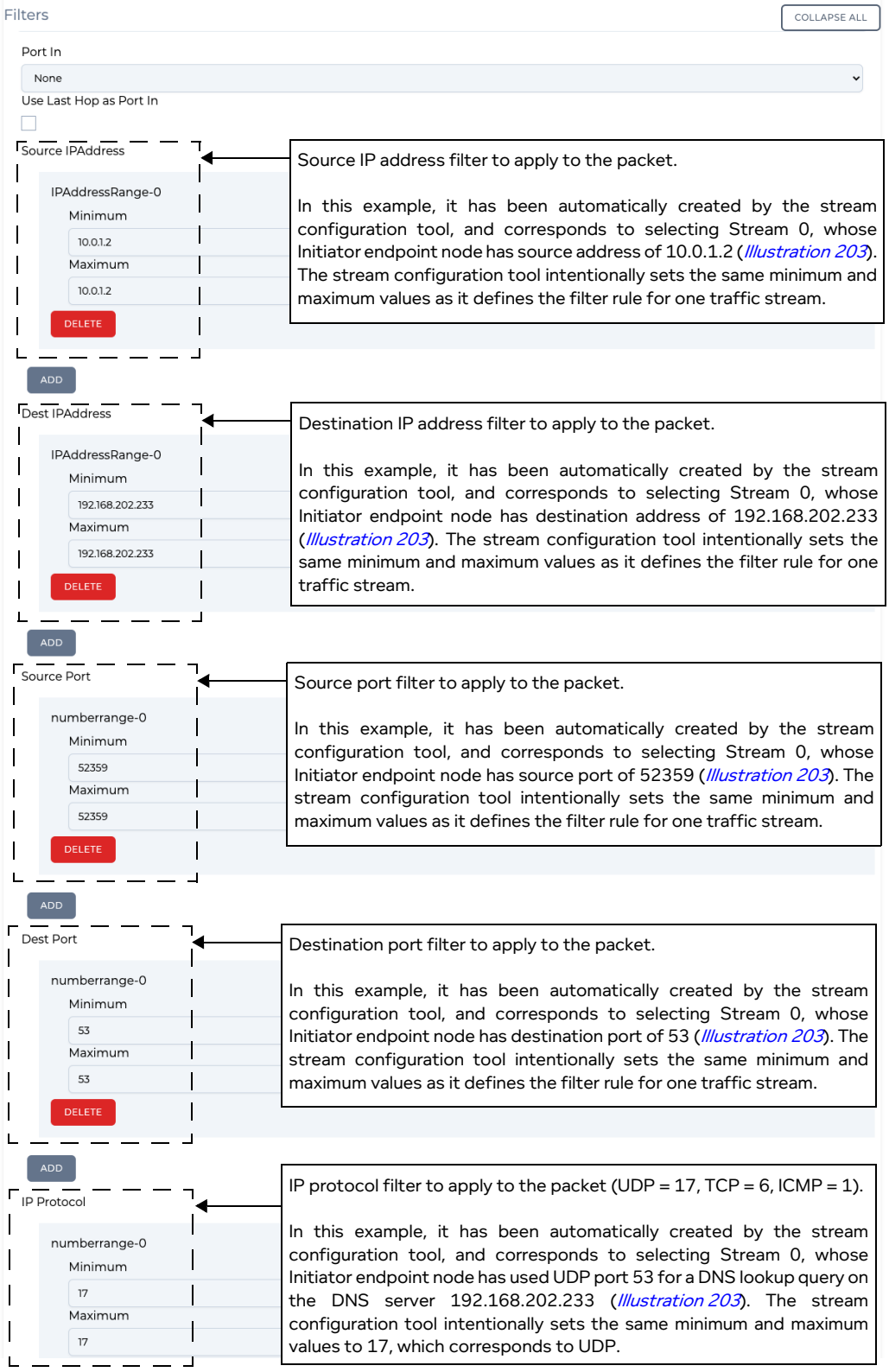
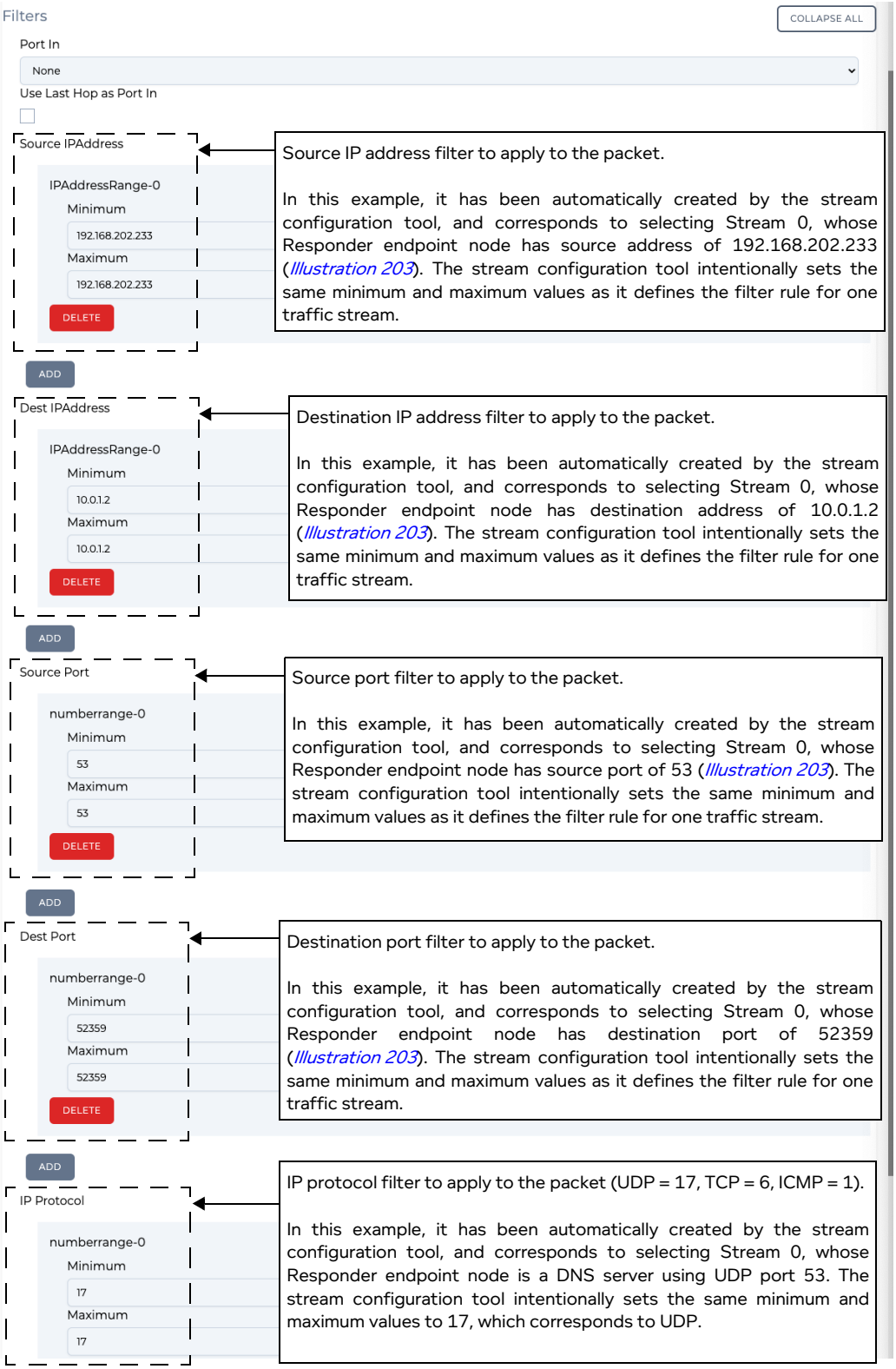


ILLUSTRATION 214 - PACKET REPLAY FILTERS DIALOG BOX (EXPANDED) FOR ONE FILTER STREAM B



For each filter for, you should specify the following:

- A source IP address in the **Source IPAddress** area. This can either be one source IP address (i.e.

the same minimum and maximum value) or a range of source IP addresses (i.e. a different minimum and maximum value).

- A destination IP address in the **Dest IPAddress** area. This can either be one destination IP address (i.e. the same minimum and maximum value) or a range of destination IP addresses (i.e. a different minimum and maximum value).
- A source port in the **Source Port** area. This can either be one source port (i.e. the same minimum and maximum value) or a range of source ports (i.e. a different minimum and maximum value).
- A protocol in the **IP Protocol** area. This must use the IP Protocol Number format published by the Internet Assigned Numbers Authority (IANA). For example, ICMP has IP Protocol Number 1, TCP has IP Protocol Number 7, and UDP has IP Protocol Number 17.

4. Once you have finished defining the filters (via either the *Method 1: Stream Configuration Tool* or *Method 2: Using Filters*), the **Filter VIEW(<N>)** button updates indicating the number of packet streams that were selected/filtered.

   Note:

   Since a packet stream is a bi-directional conversation between two endpoint nodes containing a pair of packets (see *Illustration 203* for the explanation), <N> will be an even integer value (2 for one packet stream, 4 for two packet streams, 6 for three packet streams, etc.). If you have set up filtering manually (instead of using the stream configuration tool), and you see that <N> is an odd number, verify all your filters and ensure you add the missing filter to complete the packet stream that only currently has one packet filter defined.

5. The next thing you need to do is define the routing for the Packet Replay node using the Composite Routing (Labs) function.

   If you used the stream configuration tool (which is recommended), all the routes for all the selected streams will have been automatically created as described above in *Method 1: Stream Configuration Tool*, and no further action is required. In the example above, one stream was selected, which results in automatically creating the two routes shown in *Illustration 207* and *Illustration 208*.

   If however, you have not used the stream configuration tool, then you must manually add the routes for each packet stream. The number of routes that you manually add vary according the number of unique initiator / responder IP address pairs that exist for the selected stream. For more information, look at *Table 77* on page 688 for the example described in *Packet Replay Example in Multi-Point Networks* on page 667 on how you would manually create each route.

6. Once you are happy with the settings in the **Advanced Node Properties** window, click the **OK** button to return to the **Edit node** panel for the Packet Replay node. The configuration is now complete on the Packet Replay node, and you can close the **Edit node** panel.
7. The last thing you need to do is define the routing on each of the endpoint nodes that are connected to the Packet Replay node.

   If you used the stream configuration tool (which is recommended), the following routes are automatically created (these routes must always be at the bottom of the routing table on the endpoint node):

   - One "packet replay" route in the routing function (either Composite Routing (Labs), Symmetric Routing (Expression), or IP Routing (Labs)) on the Initiator endpoint node (see *Illustration 209* as an example).
   - One "packet replay" route in the routing function (either Composite Routing (Labs), Symmetric Routing (Expression), or IP Routing (Labs)) on the Responder endpoint node (see *Illustration 210* as an example).

   If however, you have not used the stream configuration tool, then you must manually add these

routes "packet replay" on the Initiator and Responder endpoint nodes.

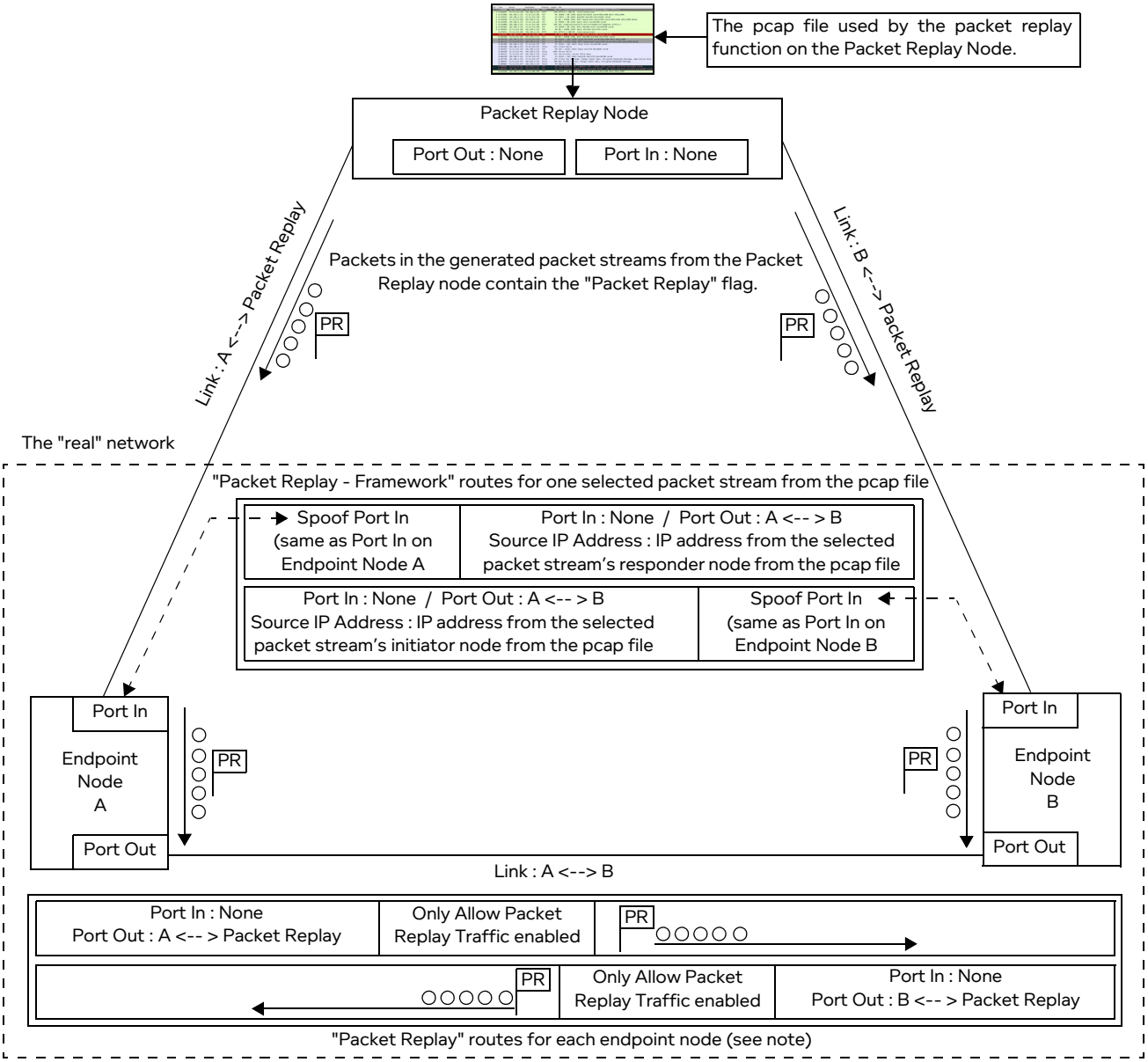
Note:

In all cases (i.e. regardless of whether or not you use the stream configuration tool), you always need to manually create routes on both the Initiator and Responder endpoint nodes to target which links the replayed packet streams will go down. To do this, you add routes based on packets with a particular source IP address from a packet stream of interest to go down the targeted link of interest. Once you have created all the necessary routes, you must move "packet replay" route that gets automatically generated by the stream configuration tool to the bottom of the routing table on the endpoint node. For an example on how to do this, look at the steps 18 and 19 described below in *Packet Replay Example in Multi-Point Networks* on page 667.

1-8-2. Packet Replay Traffic and the Only Allow Packet Replay Traffic and Spoof Port In Parameters

There are two important parameters (i.e. the **Only Allow Packet Replay Traffic** check box, and the **Spoof Port In** drop-down field parameter) to consider, which are easy to overlook when understanding how the Packet Replay node is integrated within the Multi-Point Network. Their implementation within the Web Interface and examples on how and why they used are described in *Section 1-8-1* and *Section 1-8-2*. It is useful to discuss them separately within this section in terms of how the packet replay function works and how replayed packet streams (i.e. traffic) from the Packet Replay node are injected into the Multi-Point network.

ILLUSTRATION 215 - CONCEPTUAL LAYERED OVERVIEW OF PACKET STREAM INJECTION INTO THE MULTI-POINT NETWORK



Note: The two "packet replay" routes that allow the packet replay traffic to pass through the endpoint nodes are actually on links between each endpoint node and the Packet Replay node (i.e. the Port Out is set to the link between endpoint node and Packet Replay node). However, they are logically combined together to create the underlying framework so that replayed packets with containing the "packet replay" flag can go over any of the targeted links between the two endpoint nodes.

Illustration 215 shows a conceptual "layered" overview of how the selected packet streams from the specified pcap file are injected into the network via the packet replay function running on the Packet Replay node.

1-8-2-1. Conceptual Description of the Spoof Port In Parameter

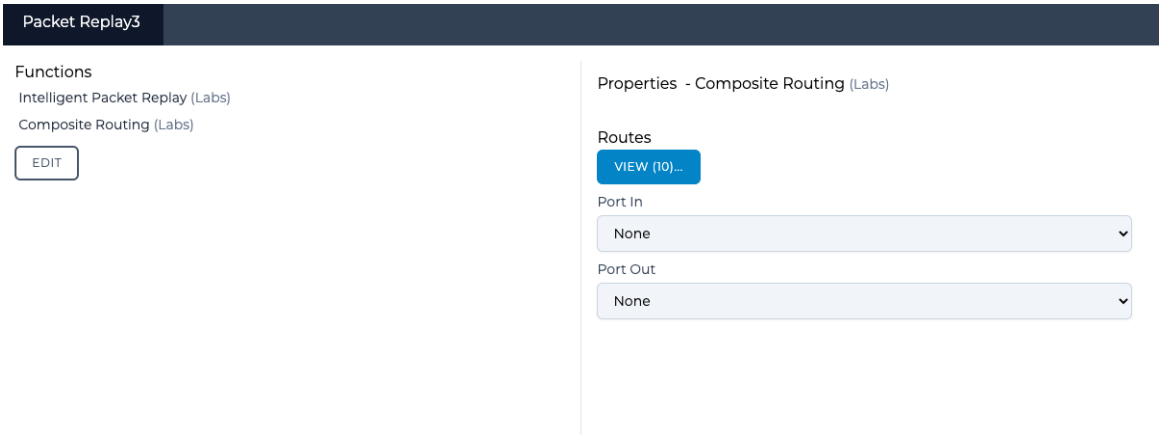
As described in *Section 1-8-1*, the Packet Replay node uses the Composite Routing (Labs) function for the "packet replay - framework" routes, which are associated with the selected packet streams that are injected into the "real" network.

The Packet Replay node's Composite Routing (Labs) function intentionally has both its **Port In** and **Port Out** values set to **None** (*Illustration 215*). At this "top level" routing perspective, the Packet Replay node is not "intgrated" into the network, however this is normal, and not a problem because the "integration" into the network is done via the **Spoof Port In** parameter on each route associated with each of the selected/replayed packet streams.

When examining the routes associated with each of the selected/replayed packet streams, we see that there is **Spoof Port In** parameter for those routes which match the **Port In** value of the associated endpoint node. The **Spoof Port In** parameter is used by the Composite Routing (Labs) function on the Packet Replay node so that the replayed packet streams look like they are coming from the "spoofed" **Port In** of the endpoint node, and thus look like they are coming from the endpoint node within the "real" network. In effect, the **Spoof Port In** parameter makes the replayed packet streams are look like they are within the "real" network, while the packet streams being replayed from the pcap file remain unmodified.

In *Illustration 215* above we can conceptually see (via the dotted bow and dotted arrows) how setting the **Spoof Port In** parameter of the "packet replay - framework" routes for each of the selected/replayed packet streams allow them to be part of the "real" network.

ILLUSTRATION 216 - PACKET REPLAY NODE TOP-LEVEL COMPOSITE ROUTING (LABS) CONFIGURATION



Note:

Before adding and configuring a Packet Replay node to your Multi-Point network, you must have fully configured the Multi-Point network with all nodes, links and routing according to your requirements.

Completely configuring the nodes, links and routing on the Multi-Point network before adding and configuring a Packet Replay node will ensure that all the existing routing of the Multi-Point network is inherited and pushed into the routing tables associated with the packet replay function, and that the Port In routing parameters of the connected endpoint nodes are pushed into the Spoof Port In values in the Composite Routing (Labs) function on the Packet Replay node.

The **Spoof Port In** parameter is only available on the Composite Routing (Labs) function and not other routing functions. This is because the **Spoof Port In** parameter is only ever required on the Packet Replay node in order to perform the required spoofing functionality discussed here.

1-8-2-2. Conceptual Description of the Only Allow Packet Replay Traffic

When the packet replay function on the Packet Replay node processes the selected packet streams from the specified pcap file, it adds a "packet replay" flag to those packets, allowing them to be distinguished from the other packets from real traffic on the network.

The **Only Allow Packet Replay Traffic** check box exists on the Composite Routing (Labs), Symmetric Routing (Expression), and IP Routing (Labs) routing functions, and determines whether packets with the "packet replay" flag are allowed to pass through the endpoint node on to the link defined by the **Port Out** drop-down field. The **Only Allow Packet Replay Traffic** check box acts as a guard to separate real network traffic from the traffic generated by the Packet Replay node.

- If the **Only Allow Packet Replay Traffic** check box is enabled, the traffic from the Packet Replay node can pass through the endpoint node onto the network. All other traffic (without the "packet replay" flag) cannot pass through the endpoint node onto the network.
- If the **Only Allow Packet Replay Traffic** check box is disabled, the traffic from the Packet Replay node cannot pass through the endpoint node onto the network. All other traffic (without the "packet replay" flag) can pass through the endpoint node onto the network.

Each endpoint node connected to the Packet Replay node must contain one "packet replay" route (i.e. **Only Allow Packet Replay Traffic** check box enabled), which must be at the bottom of the endpoint node's routing table (i.e. lowest priority route). It is the lowest priority route because it only lets packet streams (i.e. traffic) containing packets with the "packet replay" flag to pass through the endpoint node on to the "real" network via the endpoint node's defined out port (i.e. **Port Out** drop-down field setting).

Note:

If the "packet replay" route is incorrectly positioned to not be the lowest route on the endpoint node, any real (i.e. non packet replay) traffic (which does not include the "packet replay" flag) will not be able to pass through the endpoint node on to the "real" network. Always make sure that the "packet replay" route is the lowest priority route, and located at the bottom of the endpoint node's routing table.

Note:

If you are not using the stream configuration tool, and manually creating routes yourself, then the **Only Allow Packet Replay Traffic** check box is disabled by default. In this case you must think to enable it for the "packet replay" route that going between each endpoint node and the Packet Replay node.

Table 76 summarizes on which route types (described in *Section 1-8-1*) the **Only Allow Packet Replay Traffic** check box must be enabled or disabled.

TABLE 76 - RECOMMENDED ONLY ALLOW PACKET REPLAY TRAFFIC SETTINGS PER ROUTE TYPE

Route Type	Default Setting Generated by Stream Configuration Tool	Required / Allowed Setting / Notes
Framework route	Disabled	Disabled - must never be enabled, otherwise real traffic from within the network will be blocked.
Packet replay - framework route	Disabled	Can be disabled or enabled. The setting has no real significance in this case as it is the Composite Routing (Labs) function on the Packet Replay node, which by default is generating the packets with the "packet replay" flag, and thus already allowing them to pass through the Packet Replay node.
Packet replay route	Enabled	Enabled - must always be enabled and must always be the last route within the routing table on the endpoint node.

2. PACKET REPLAY EXAMPLES

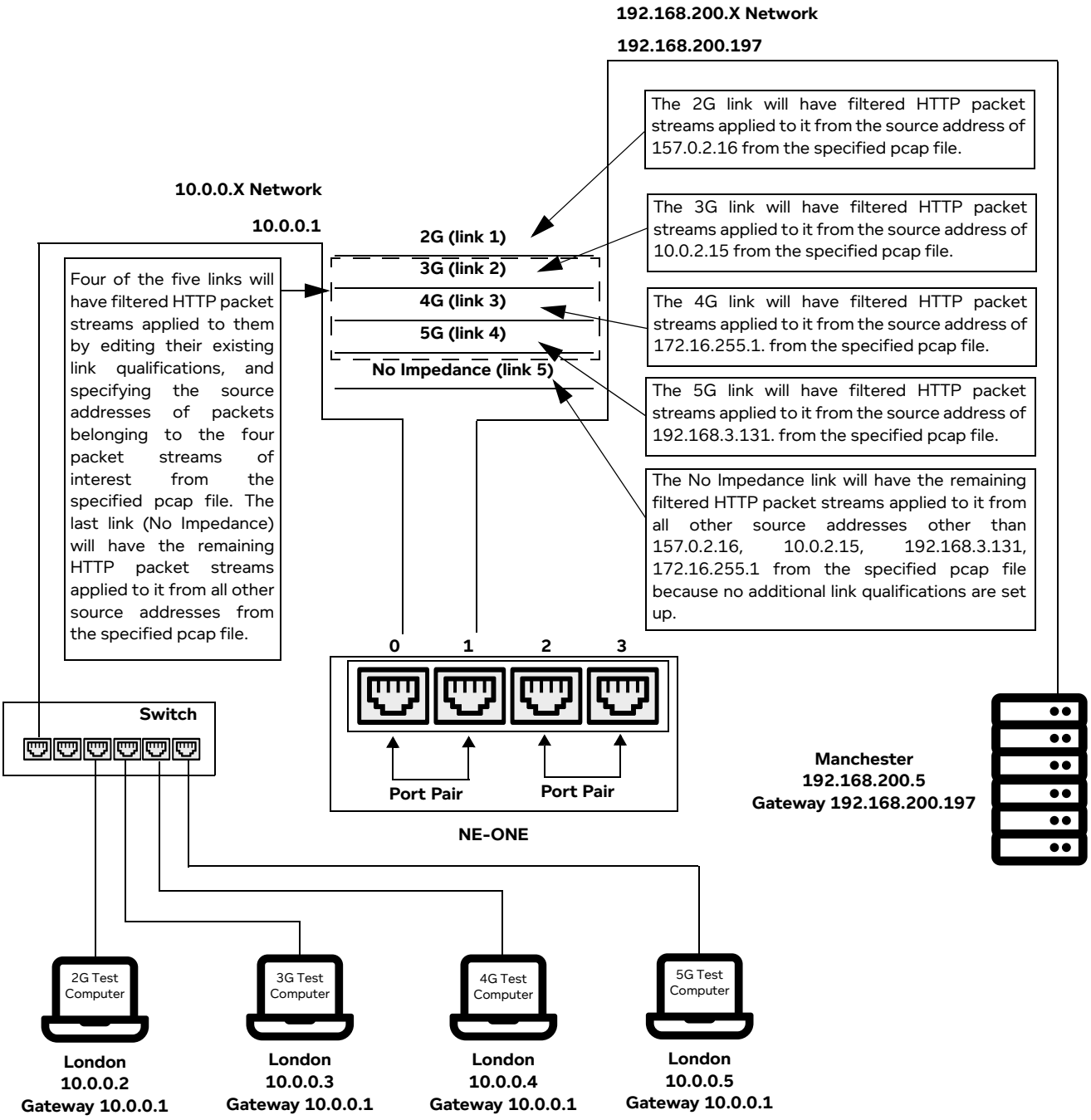
This section describes some examples using the Intelligent Packet Replay function on a Point-to-Point network and Multi-Point network.

Note:
Although the examples below use the Intelligent Packet Replay function the use of the Passive Replay Function from a Web Interface perspective is the same.

2-1. Packet Replay Example in Point-to-Point Networks

In this example, we have already set up a Point-to-Point network with the following configuration (according to the example described in *Creating Point-to-Point Networks (Single)* on page 265):

ILLUSTRATION 217 - POINT-TO-POINT NETWORK (5 LINKS) - TARGET HTTP TRAFFIC TO CERTAIN LINKS



In this example, five links have been configured with different mobile network types, for different client computers, using link qualification criteria on each link:

- Client computer with IP Address 10.0.0.2 (Netmask 255.255.255.0, Gateway 10.0.0.1) uses the 2G link (link1).
- Client computer 10.0.0.3 (Netmask 255.255.255.0, Gateway 10.0.0.1) uses the 3G link (link2).
- Client computer 10.0.0.4 (Netmask 255.255.255.0, Gateway 10.0.0.1) uses the 4G link (link3).
- Client computer 10.0.0.5 (Netmask 255.255.255.0, Gateway 10.0.0.1) uses the 5G link (link4).
- Packets that do not qualify for 2G, 3G, 4G or 5G traverse the 'No impedance' (link 5).

Links 1 to 4 apply different network conditions for the four client computers (i.e. link qualifications have already previously been set up by defining the source address of each client computer on each of the links). Link 5 forwards all other traffic across a link which is not impeded.

In this example, the pcap file that will be used for adding traffic within the Point-to-Point network contains multiple packet streams from different initiators and responders, with different traffic types (e.g. HTTP (TCP 80), FTP (TCP 21), etc.).

We will use the **Select Streams** dialog box (see *Illustration 194*) to select HTTP traffic (TCP 80) from some of the packet streams of the specified pcap file for the following initiator addresses:

- 157.0.2.16
- 10.0.2.15
- 172.16.255.1
- 192.168.3.191

We can optionally also use the **Configure Stream Directions** dialog box (see *Illustration 196*) to modify the original filtered packet stream directions inherited from the pcap file. In this example however, no changes are required as the packet stream directions in inherited from the pcap file are all correct.

Finally, in this example, we must edit the existing link qualification criteria to specify which links the filtered traffic streams (in our example, the HTTP traffic) are sent to. In this example, the link qualifications for the following links are edited to include the source addresses of interest from the specified pcap file, as follows:

- 2G link (link1) : which already includes packets from client computer 10.0.0.2 will have the source address of 157.0.2.16 added to its link criteria.
- 3G link (link2) : which already includes packets from client computer 10.0.0.3 will have the source address of 10.0.2.15 added to its link criteria.
- 4G link (link3) : which already includes packets from client computer 10.0.0.4 will have the source address of 172.16.255.1 added to its link criteria.
- 5G link (link4) : which already includes packets from client computer 10.0.0.5 will have the source address of 192.168.3.191 added to its link criteria.
- No Impedance link (link5) : which does not include packets any client computers will have no additional link criteria defined. The No Impedance link will have the remaining filtered HTTP packet streams applied to it from all other source addresses other than 157.0.2.16, 10.0.2.15, 192.168.3.131, 172.16.255.1 from the specified pcap file because no additional link qualifications are set up.

Note:

Because in this example we have "built up" a set of packet streams from the initiators 157.0.2.16, 10.0.2.15, 192.168.3.131, 172.16.255.1, the generated traffic stream only contains packet streams from those initiators, and thus the No Impedance link (link5) will not have any packet streams from the generated traffic stream.

In this example, do the following:

1. Create the Point-to-Point network according to the example described in *Creating Point-to-Point Networks (Single)* on page 265. This network is called London - Manchester and will have link qualification criteria initially configured only for the client computers described above (i.e. not yet defined for the replayed packet streams from the specified pcap file). The filename of this Point-to-Point network is `London – Manchester.itn` located in your `/Private/networks` directory.
2. Use the following steps to create a copy of the London - Manchester network, which you will rename to London - Manchester (extra HTTP traffic), and use for the additional HTTP traffic that you will add into the Point-to-Point network. To do this, use the following sub-steps:

a. Open the original London - Manchester Point-to-Point network.
b. From the Point-to-Point Designer, select **FILE > Save as**.
c. From the **Network name** dialog box that appears, type **`London – Manchester (extra HTTP Traffic)`**, then click **OK**.

   The a new network file called `London – Manchester (extra HTTP Traffic).itn` in your `/Private/networks` directory is now ready to be used with the Intelligent Packet Replay function.

3. Obtain or create a packet capture file for use within the Point-to-Point network (see *Packet Replay pcap File Prerequisites* on page 610). In our example, the `WebTraffic.pcap` file containing many packet streams (including HTTP (TCP 80)) has been previously generated, and uploaded to within the `/Private/packet_replay_files` directory.

Note:

To potentially save time typing the full path later on in step 6.c., you can use the File Browser's **Copy File Path** pop-up menu function to copy the full path of the pcap file, and then paste it within the **Path** field. To do this, right mouse click on the pcap file (in our example, `WebTraffic.pcap` within the `/Private/packet_replay_files` directory), and select **Copy File Path** from the pop-up menu that appears.

4. Open the copied Point-to-Point network from either the **Home** page or File Browser. In our example, we open the renamed network file called `London – Manchester (extra HTTP traffic).itn`.

   The copied Point-to-Point network appears in the Point-to-Point Designer.

5. Click the **PACKET REPLAY** button.
6. From the **Packet Replay Settings** dialog box that appears, do the following to configure the general settings of the Intelligent Packet Replay function:
   a. Enable the **Running** check box.
   b. Select **Intelligent Packet Replay** from the **Packet Replay Type** drop-down field.
   c. In the **Path** field, type the path to the pcap file within the NE-ONE file system that will be used by the Intelligent Packet Replay function. In our example, the `WebTraffic.pcap` file located within the `/Private/packet_replay_files` directory is used, and you would type **`/Private/packet_replay_files/WebTraffic.pcap`**.

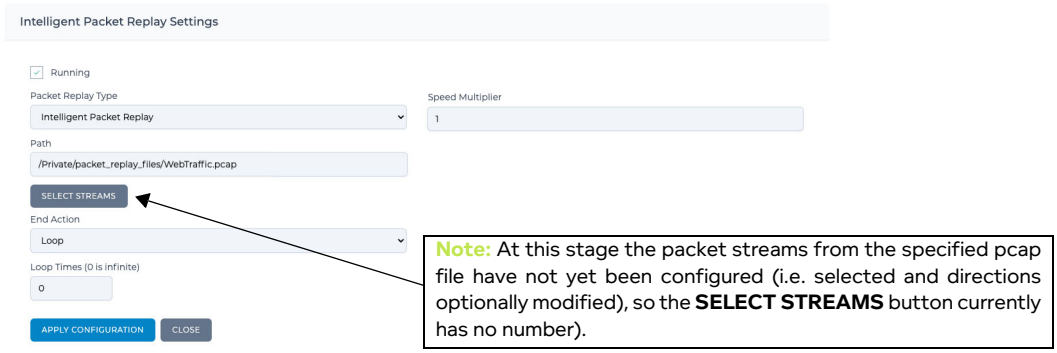
Note: If you previously copied the full path of the pcap file in step 3 above, you can paste it into the **Path** field by right mouse clicking and selecting **Paste**, or by pressing the **CTRL** + **V** keys (on Windows) or by pressing the **CMD** + **V** keys (on MacOS).

d. From the **End Action** drop-down field, select **Loop**.

e. In the **Loop Times** field, leave the default value set to **0**. The default value of 0 is the equivalent to an infinite number of loop times.

f. In the **Slowdown Multiplier** field, leave the default value set to 1.

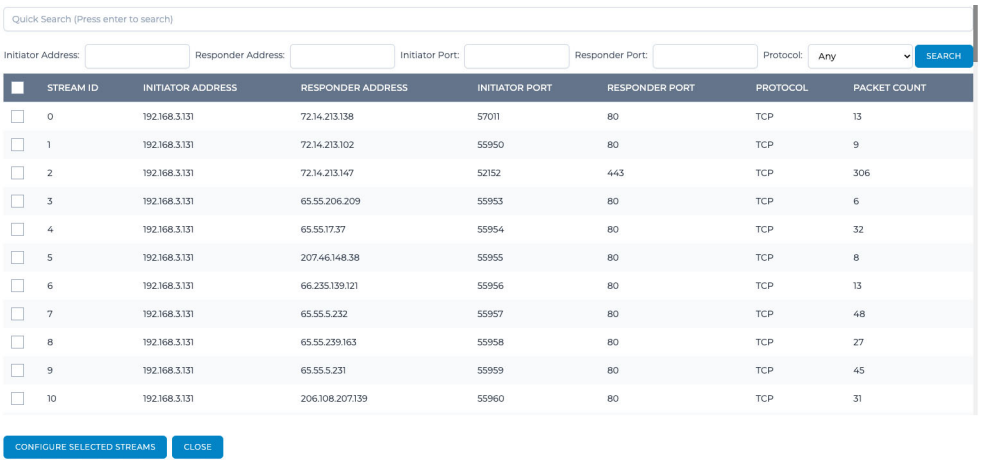
At this stage the general settings of the Intelligent Packet Replay function are now configured.



You must now configure the packet streams.

7. Click the **SELECT STREAMS** button.

The NE-ONE analyzes the specified pcap file. The analysis time varies according to the size of the specified pcap file. Once the NE-ONE finishes analyzing the specified pcap file, an initial **Select Streams** dialog box (with no packet streams selected) similar to the following appears.



You can use the **Select Streams** dialog box to determine which packet streams you want to include in the traffic stream that is generated by the Intelligent Packet Replay function. For more detailed information on using the **Select Streams** dialog box, see *Select Streams Dialog Box* on page 611.

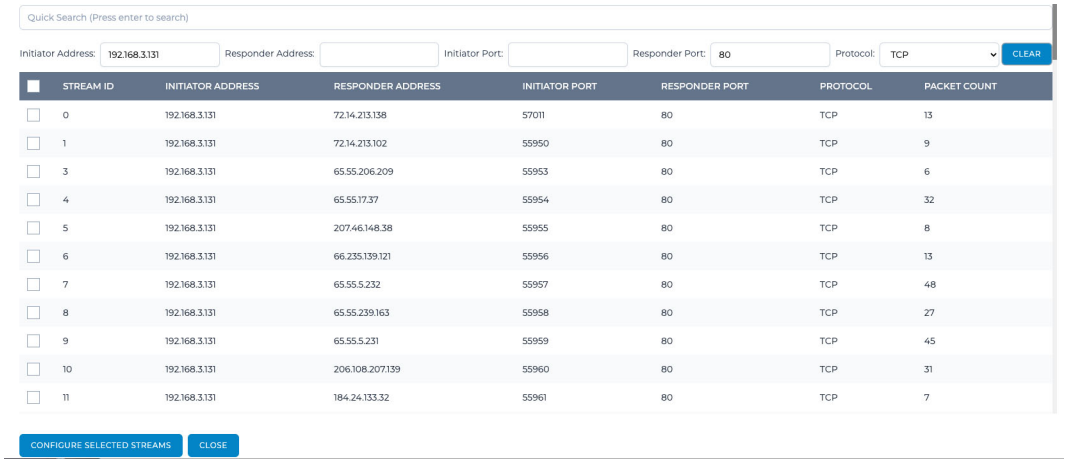
In our example (described in step 8 below) we will select some HTTP traffic (TCP 80) from four initiator nodes, with the following IP addresses 192.168.3.131, 10.0.2.15, 172.16.255.1, and 157.0.2.16.

8. In the **Select Streams** dialog box, do the following to select all HTTP traffic (TCP 80) from for each of the initiator addresses of interest (in our example, 192.168.3.131, 10.0.2.15, 172.16.255.1, and 157.0.2.16).

Select the packet streams of interest for HTTP traffic (TCP 80) on initiator 192.168.3.131:

a. In the **Protocol** field, select **TCP**.
b. In the **Responder Port** field, type **80**.
c. In the **Initiator Address** type **192.168.3.131**.
d. Leave the other **Responder Address** and **Initiator Port** fields empty.
e. Click the **SEARCH** button.

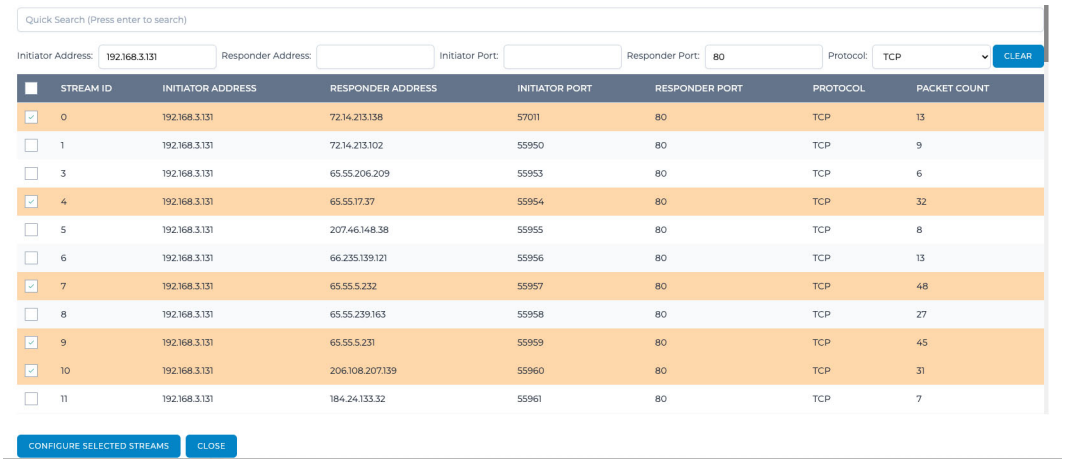
The **Select Streams** dialog box returns a set of unselected packet streams, based upon your specified filter criteria. In our example, all the packet streams corresponding to the filter for HTTP traffic (i.e. Protocol : TCP, Responder Port : 80, and initiator 192.168.3.131) is displayed.



Note: The time it takes to return the set of unselected packet streams varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).

The set of packet streams are initially unselected (i.e. each check box is unselected).

f. Enable the check boxes corresponding to each of the packet streams you want to include in the generated traffic stream. In our example, we enable the check boxes associated with the five packet streams with stream IDs 0, 4, 7, 9, and 10.



Note: At this stage, do not click the **CONFIGURE SELECTED STREAMS** button. You will continue to "build up" and select the HTTP traffic for the rest of the initiators (i.e. 10.0.2.15, 172.16.255.1 and 157.0.2.16).

g. Click the **CLEAR** button.

The search filter bar resets, and the selected HTTP traffic streams for initiator 192.168.3.131

remain selected.

Select the packet streams of interest for HTTP traffic (TCP 80) on initiator 10.0.2.15:

a. In the **Protocol** field, select **TCP**.

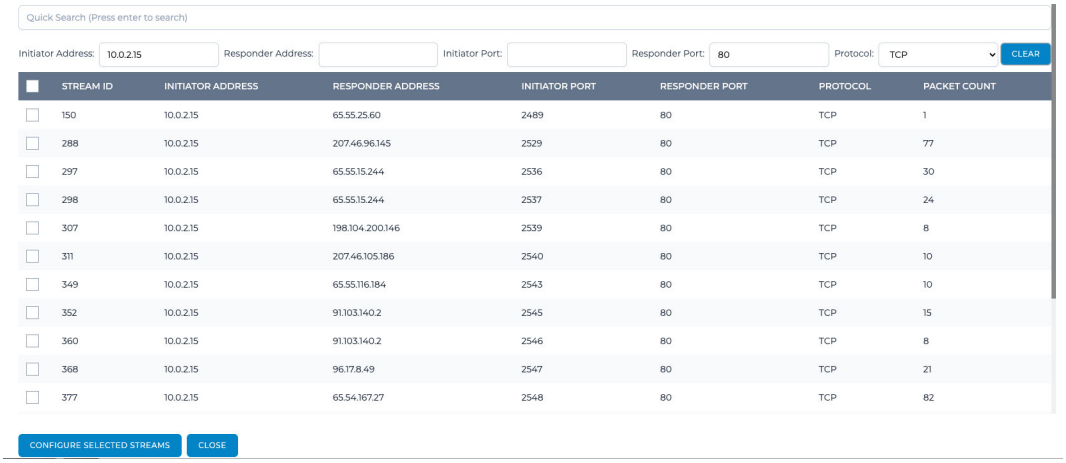
b. In the **Responder Port** field, type **80**.

c. In the **Initiator Address** type **10.0.2.15**.

d. Leave the other **Responder Address** and **Initiator Port** fields empty.

e. Click the **SEARCH** button.

The **Select Streams** dialog box returns a set of unselected packet streams, based upon your specified filter criteria. In our example, all the packet streams corresponding to the filter for HTTP traffic (i.e. Protocol : TCP, Responder Port : 80, and initiator 10.0.2.15) is displayed.



Note: The time it takes to return the set of unselected packet streams varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).

The set of packet streams are initially unselected (i.e. each check box is unselected).

f. Enable the check boxes corresponding to each of the packet streams you want to include in the generated traffic stream. In our example, we enable the check boxes associated with the five packet streams with stream IDs 288, 297, 298, 352, and 368.

Note: At this stage, do not click the **CONFIGURE SELECTED STREAMS** button. You will continue to "build up" and select the HTTP traffic for the rest of the initiators (i.e. 172.16.255.1 and 157.0.2.16).

g. Click the **CLEAR** button.

The search filter bar resets, and the selected HTTP traffic streams for initiator 10.0.2.15 remain selected.

Select the packet streams of interest for HTTP traffic (TCP 80) on initiator 172.16.255.1:

a. In the **Protocol** field, select **TCP**.

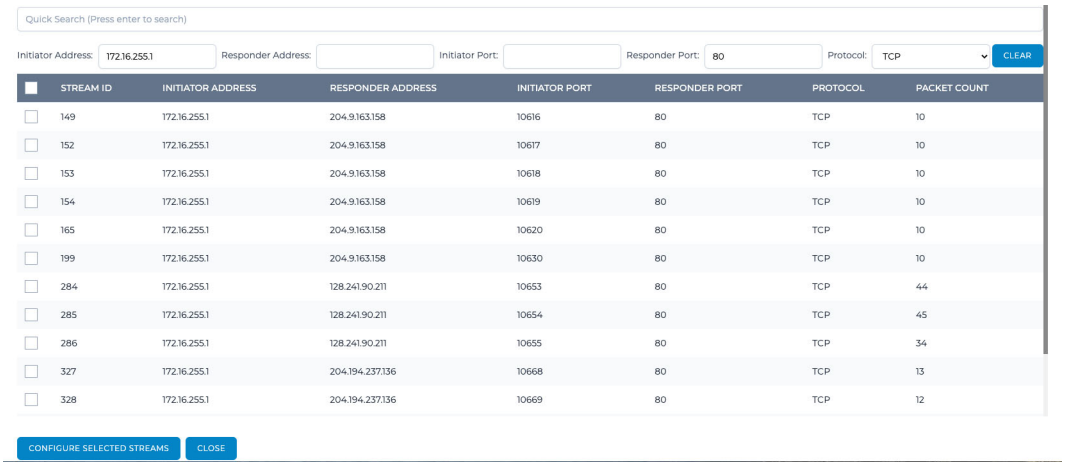
b. In the **Responder Port** field, type **80**.

c. In the **Initiator Address** type **172.16.255.1**.

d. Leave the other **Responder Address** and **Initiator Port** fields empty.

e. Click the **SEARCH** button.

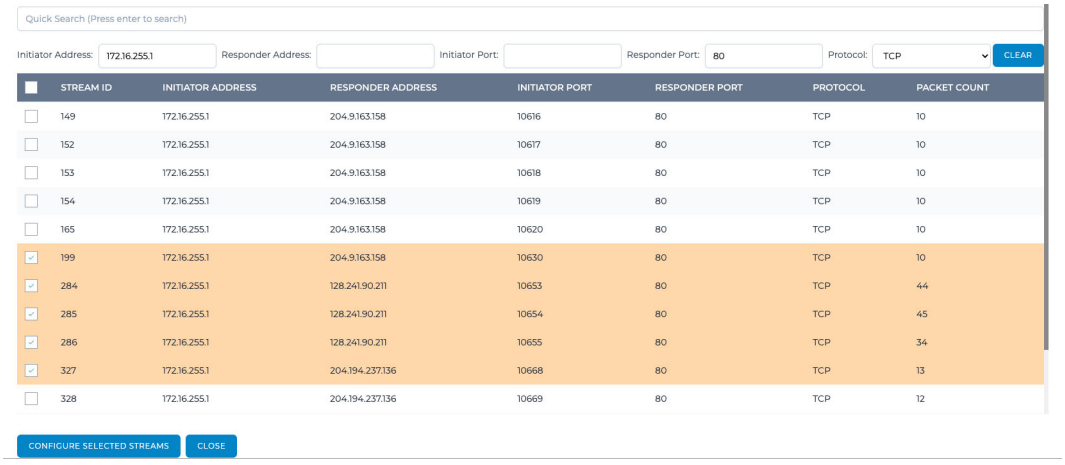
The **Select Streams** dialog box returns a set of unselected packet streams, based upon your specified filter criteria. In our example, all the packet streams corresponding to the filter for HTTP traffic (i.e. Protocol : TCP, Responder Port : 80, and initiator 172.16.255.1) is displayed.



Note: The time it takes to return the set of unselected packet streams varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).

The set of packet streams are initially unselected (i.e. each check box is unselected).

f. Enable the check boxes corresponding to each of the packet streams you want to include in the generated traffic stream. In our example, we enable the check boxes associated with the five packet streams with stream IDs 199, 284, 285, 286, and 327.



Note: At this stage, do not click the **CONFIGURE SELECTED STREAMS** button. You will

continue to "build up" and select the HTTP traffic for the rest of the initiators (i.e. 157.0.2.16).

g. Click the **CLEAR** button.

The search filter bar resets, and the selected HTTP traffic streams for initiator 172.16.255.1 remain selected.

Select the packet streams of interest for HTTP traffic (TCP 80) on initiator 157.0.2.16:

a. In the **Protocol** field, select **TCP**.

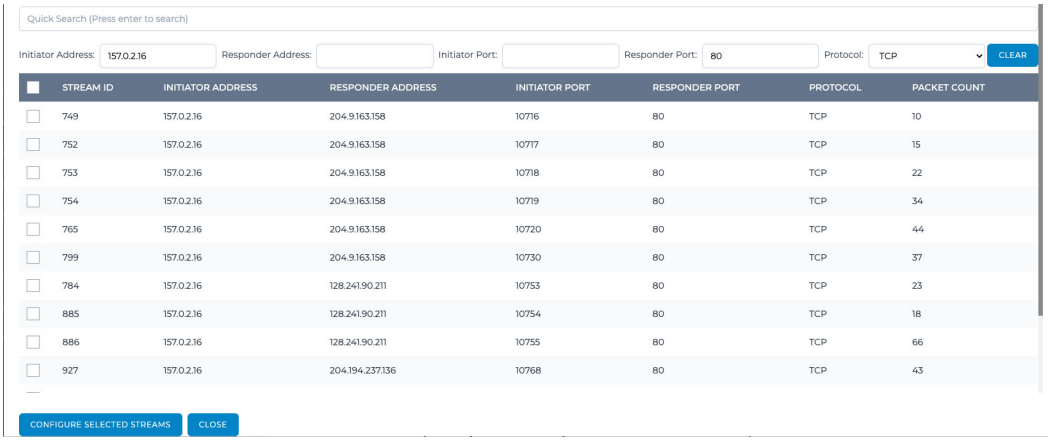
b. In the **Responder Port** field, type **80**.

c. In the **Initiator Address** type **157.0.2.16**.

d. Leave the other **Responder Address** and **Initiator Port** fields empty.

e. Click the **SEARCH** button.

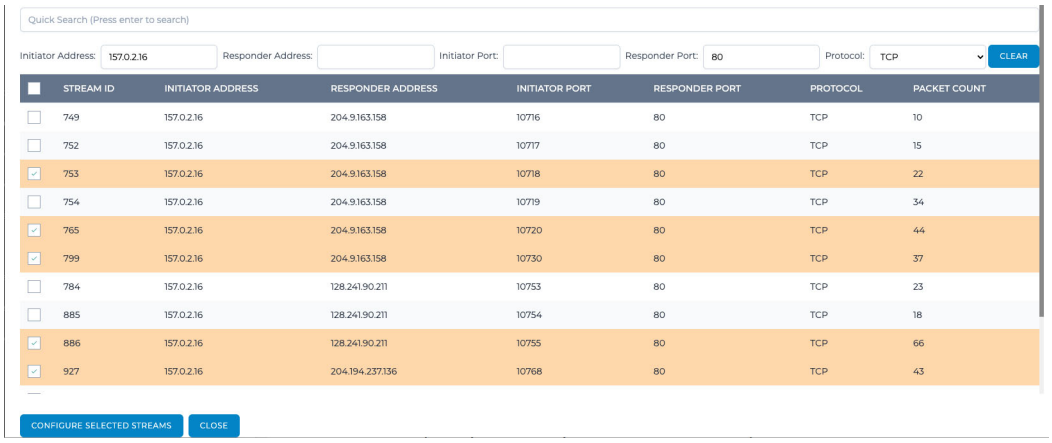
The **Select Streams** dialog box returns a set of unselected packet streams, based upon your specified filter criteria. In our example, all the packet streams corresponding to the filter for HTTP traffic (i.e. Protocol : TCP, Responder Port : 80, and initiator 157.0.2.16) is displayed.



Note: The time it takes to return the set of unselected packet streams varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).

The set of packet streams are initially unselected (i.e. each check box is unselected).

f. Enable the check boxes corresponding to each of the packet streams you want to include in the generated traffic stream. In our example, we enable the check boxes associated with the five packet streams with stream IDs 753, 765, 799, 886, and 927.



Note: At this stage, all the HTTP traffic for all of the initiators have now been built up and

selected. Proceed to step 9.

9. Click the **CONFIGURE SELECTED STREAMS** button.

   A **Configure Stream Directions** dialogue box (similar to *Illustration 196* on page 620) appears.

   You can optionally use the **Configure Stream Directions** dialog box to determine the direction of each packet stream included in the generated traffic stream. For detailed information on using the **Configure Stream Directions** dialog box, see *Configure Stream Directions Dialog Box* on page 618.

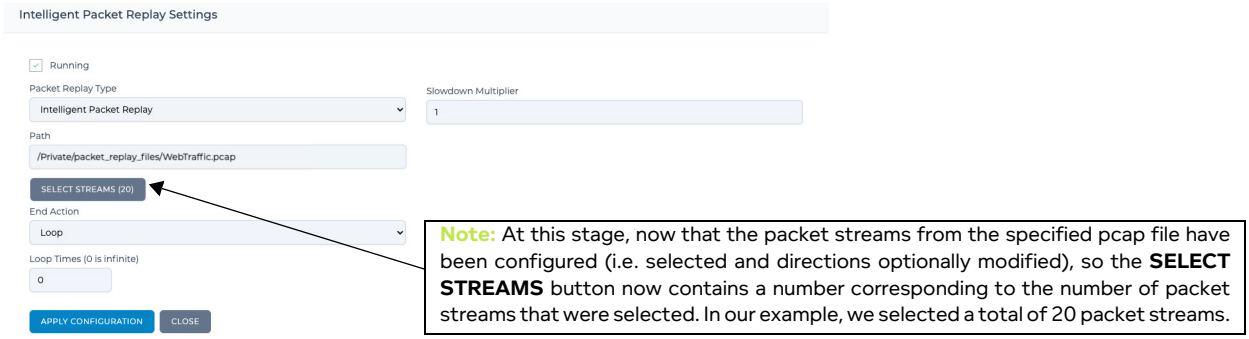
   In our example (described in step 10 below) the packet stream directions inherited by the specified pcap file are already correct, so no changes are required.

10. From the **Configure Stream Directions** dialog box that appears, do the following:
    a. Scroll down and verify the direction of each packet stream, paying attention to which endpoint node (e.g. London and Manchester) is assigned to the IP addresses and port numbers as expected (e.g. a client (the initiator) typically opens a random high port number to communicate with a web server (the responder) who is listening and communicating over port 80).
    b. If required, change the packet stream directions.
    c. When you are happy with the each of the packet stream directions, click **SAVE**.

Note:

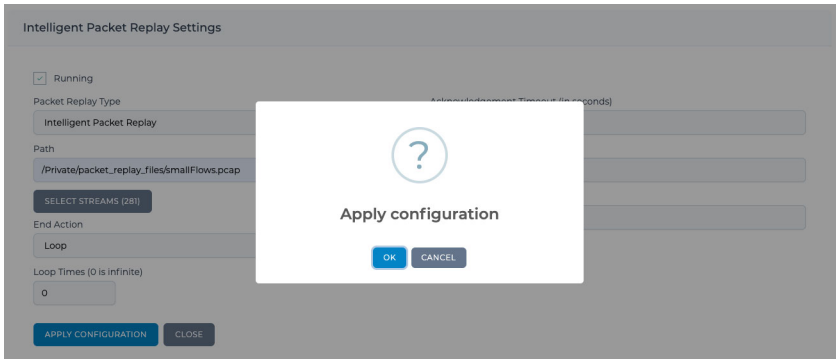
The time it takes to save the stream configuration varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).

Once the stream configuration is saved, you are returned to the **Packet Replay Settings** dialog box. The **SELECT STREAMS** button now also contains a number, indicating the number of packet streams that were selected.



11. In the **Packet Replay Settings** dialog box, click the **APPLY CONIFURATION** button.

    An **Apply configuration ?** dialog box appears.

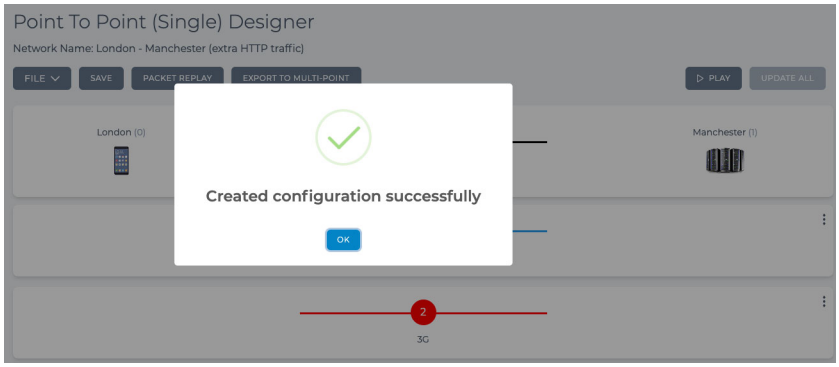


12. From the **Apply configuration ?** dialog box that appears, click **OK**.

Note:

The time it takes to apply the configuration of the Intelligent Packet Replay function to the Point-to-Point network varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute). Once the Intelligent Packet Replay function's configuration has been applied, the **Created configuration successfully** dialog box appears.

13. From the **Created configuration successfully** dialog box that appears, click **OK**.



The **Created configuration successfully** dialog box closes, and you are returned to the Point-to-Point Designer.

Notice:

At the stage, even if the Intelligent Packet Replay function's configuration has been applied to the Point-to-Point network, the Point-to-Point network itself has been modified since it was initially opened, and must be saved in order for the Intelligent Packet Replay function to take effect.

14. Click on **Save** in the Point-to-Point Designer to commit the Intelligent Packet Replay configuration to the Point-to-Point network.

Note:

The time it takes to save the updated Point-to-Point network varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute). During this time, the mouse actions on the menu buttons are intentionally unresponsive until the Point-to-Point network has been saved.

Note:

The Intelligent Packet Replay function uses link qualifications to let you target which links the replayed packet streams are applied. Remember that link qualifications use a "catch all", cascade down approach.

If you run the Point-to-Point network at this stage, all the selected packet streams from the generated traffic stream will only go down the first link (i.e. the 2G link). This is because the existing link qualifications on the Point-to-Point network have not yet been edited to include the source addresses of the streams of interest from the specified pcap file.

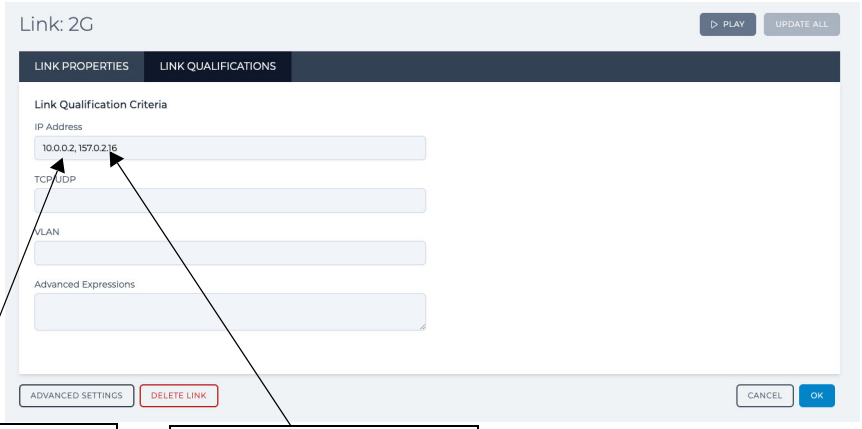
15. Use the following sub-steps to edit the existing link qualification criteria to specify which links the filtered traffic streams are sent to.

    In our example, the link qualifications for the 2G, 3G, 4G, and 5G links are edited to include the source addresses of interest from the specified pcap file.

    Edit the 2G link, as follows:

    a. In the Point-to-Point Designer, click on the **2G** link.

b. From the **Link: 2G** page that appears, click the **LINK QUALIFICATIONS** tab.



Original source address of the client computer (10.0.0.2) from the original Point-to-Point network.

Source address of the packet of interest from the specified pcap file (157.0.2.16).

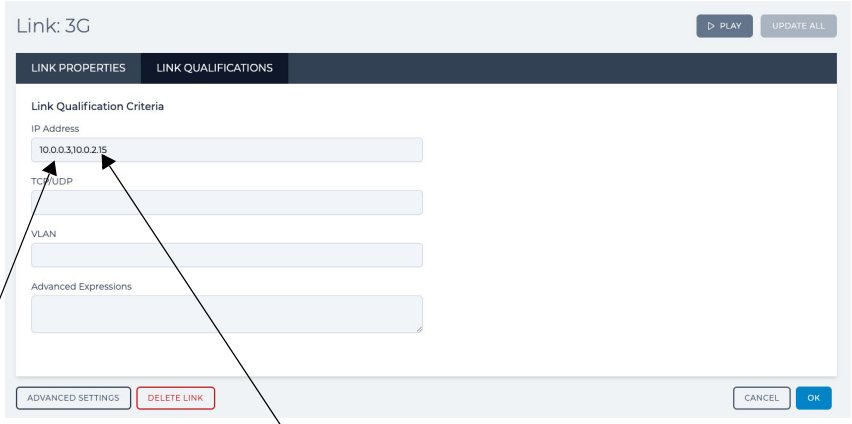
c. The link qualification criteria for the 2G link already includes the source address of the test client computer (i.e. 10.0.0.2). In the **IP Address** field, add the source address of interest from the specified pcap file (in our example, 157.0.2.16), separating it from the original IP address of the test client computer, with a comma.

d. Click **OK**.

Edit the 3G link, as follows:

a. In the Point-to-Point Designer, click on the **3G** link.

b. From the **Link: 3G** page that appears, click the **LINK QUALIFICATIONS** tab.



Original source address of the client computer (10.0.0.3) from the original Point-to-Point network.

Source address of the packet of interest from the specified pcap file (10.0.2.15).

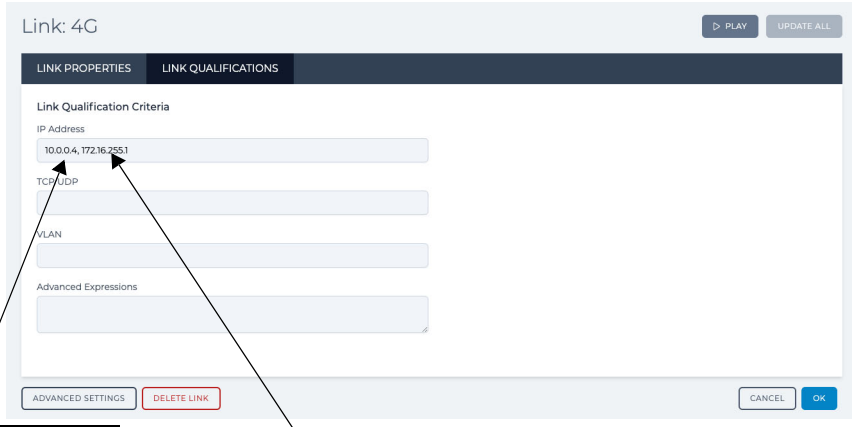
c. The link qualification criteria for the 3G link already includes the source address of the test client computer (i.e. 10.0.0.3). In the **IP Address** field, add the source address of interest from the specified pcap file (in our example, 10.0.2.15), separating it from the original IP address of the test client computer, with a comma.

d. Click **OK**.

Edit the 4G link, as follows:

a. In the Point-to-Point Designer, click on the **4G** link.

b. From the **Link: 4G** page that appears, click the **LINK QUALIFICATIONS** tab.



Original source address of the client computer (10.0.0.4) from the original Point-to-Point network.

Source address of the packet of interest from the specified pcap file (172.16.255.1).

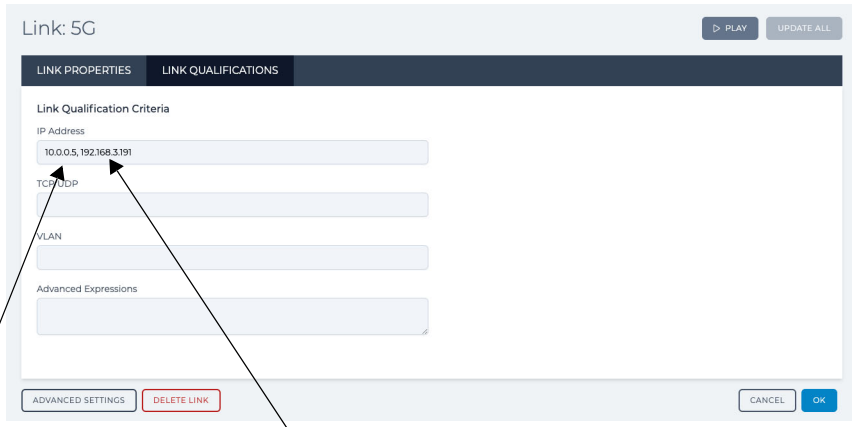
c. The link qualification criteria for the 4G link already includes the source address of the test client computer (i.e. 10.0.0.4). In the **IP Address** field, add the source address of interest from the specified pcap file (in our example, 172.16.255.1), separating it from the original IP address of the test client computer, with a comma.

d. Click **OK**.

Edit the 5G link, as follows:

a. In the Point-to-Point Designer, click on the **5G** link.

b. From the **Link: 5G** page that appears, click the **LINK QUALIFICATIONS** tab.



Original source address of the client computer (10.0.0.5) from the original Point-to-Point network.

Source address of the packet of interest from the specified pcap file (192.168.3.191).

c. The link qualification criteria for the 5G link already includes the source address of the test client computer (i.e. 10.0.0.5). In the **IP Address** field, add the source address of interest from the specified pcap file (in our example, 192.168.3.191), separating it from the original IP address of the test client computer, with a comma.

d. Click **OK**.

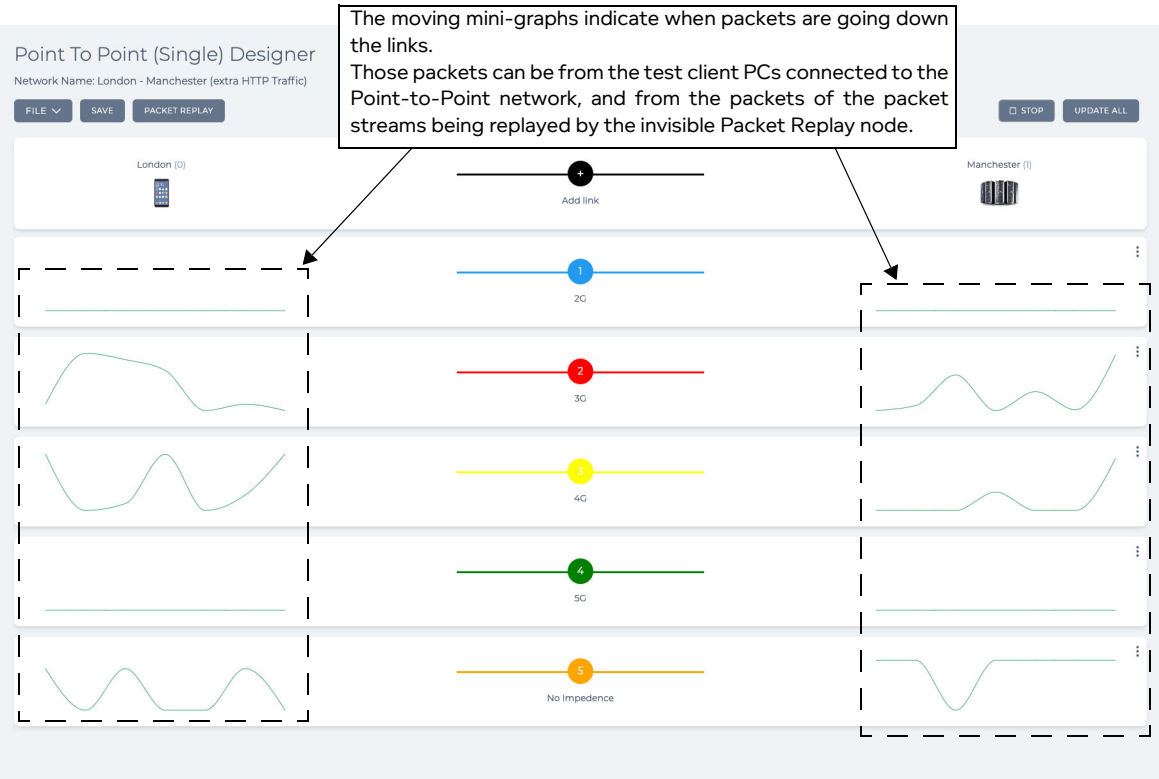
16. The Point-to-Point network is now fully configured. Click on **Save** in the Point-to-Point Designer to commit the Intelligent Packet Replay configuration to the Point-to-Point network.

Note:

The time it takes to save the updated Point-to-Point network varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute). During this time, the mouse actions on the menu buttons are intentionally unresponsive until the Point-to-Point network has been saved.

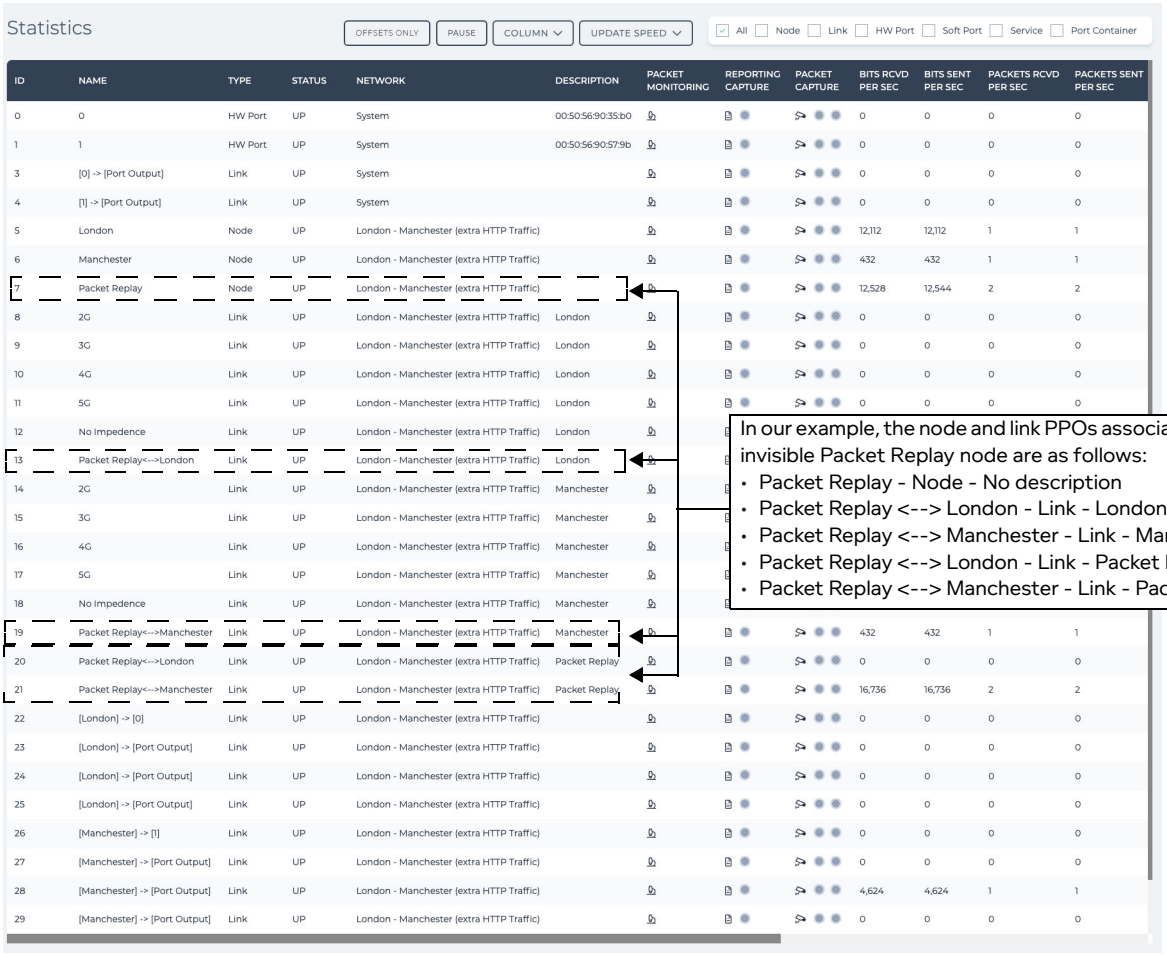
17. Now that the Point-to-Point network is fully configured, it can now be run and the selected HTTP packet streams that you configured in the Intelligent Packet Reply function will be injected into the Point-to-Point network via the invisible Packet Replay node (described in *Back End Packet Replay Implementation in the Point-to-Point Designer* on page 623).

    When you run the Point-to-Point network, any links with packets are going down them will be indicated by the moving mini-graphs. In the example below, packets from the packet streams being replayed by the invisible Packet Replay node are going down the different links between the London and Manchester endpoint nodes.



The node and link PPOs associated with the invisible Packet Replay node can be seen in the **Statistics** page. In example the **Statistics** page, below we see the node PPOs associated with the

invisible Packet Replay node are represented like any other PPO in the Point-to-Point network.

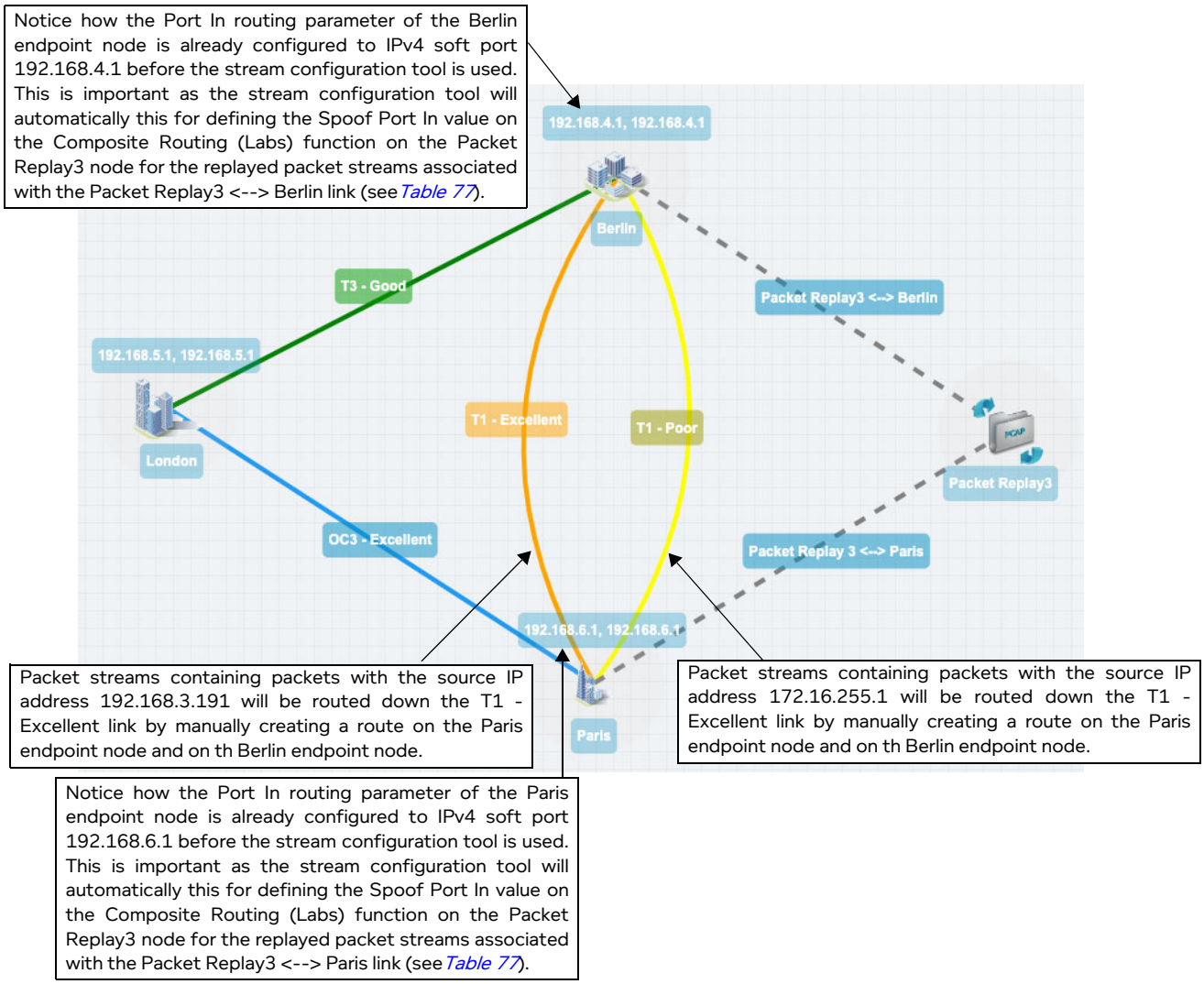


ID	NAME	TYPE	STATUS	NETWORK	DESCRIPTION	PACKET MONITORING	REPORTING CAPTURE	PACKET CAPTURE	BITS RCVD PER SEC	BITS SENT PER SEC	PACKETS RCVD PER SEC	PACKETS SENT PER SEC
0	0	HW Port	UP	System	00:50:56:90:35:b0				0	0	0	0
1	1	HW Port	UP	System	00:50:56:90:57:9b				0	0	0	0
3	[0] -> [Port Output]	Link	UP	System					0	0	0	0
4	[1] -> [Port Output]	Link	UP	System					0	0	0	0
5	London	Node	UP	London - Manchester (extra HTTP Traffic)					12,112	12,112	1	1
6	Manchester	Node	UP	London - Manchester (extra HTTP Traffic)					432	432	1	1
7	Packet Replay	Node	UP	London - Manchester (extra HTTP Traffic)					12,528	12,544	2	2
8	2G	Link	UP	London - Manchester (extra HTTP Traffic)	London				0	0	0	0
9	3G	Link	UP	London - Manchester (extra HTTP Traffic)	London				0	0	0	0
10	4G	Link	UP	London - Manchester (extra HTTP Traffic)	London				0	0	0	0
11	5G	Link	UP	London - Manchester (extra HTTP Traffic)	London				0	0	0	0
12	No Impedence	Link	UP	London - Manchester (extra HTTP Traffic)	London							
13	Packet Replay<-->London	Link	UP	London - Manchester (extra HTTP Traffic)	London							
14	2G	Link	UP	London - Manchester (extra HTTP Traffic)	Manchester							
15	3G	Link	UP	London - Manchester (extra HTTP Traffic)	Manchester							
16	4G	Link	UP	London - Manchester (extra HTTP Traffic)	Manchester							
17	5G	Link	UP	London - Manchester (extra HTTP Traffic)	Manchester							
18	No Impedence	Link	UP	London - Manchester (extra HTTP Traffic)	Manchester							
19	Packet Replay<-->Manchester	Link	UP	London - Manchester (extra HTTP Traffic)	Manchester				432	432	1	1
20	Packet Replay<-->London	Link	UP	London - Manchester (extra HTTP Traffic)	Packet Replay				0	0	0	0
21	Packet Replay<-->Manchester	Link	UP	London - Manchester (extra HTTP Traffic)	Packet Replay				16,736	16,736	2	2
22	[London] -> [0]	Link	UP	London - Manchester (extra HTTP Traffic)					0	0	0	0
23	[London] -> [Port Output]	Link	UP	London - Manchester (extra HTTP Traffic)					0	0	0	0
24	[London] -> [Port Output]	Link	UP	London - Manchester (extra HTTP Traffic)					0	0	0	0
25	[London] -> [Port Output]	Link	UP	London - Manchester (extra HTTP Traffic)					0	0	0	0
26	[Manchester] -> [1]	Link	UP	London - Manchester (extra HTTP Traffic)					0	0	0	0
27	[Manchester] -> [Port Output]	Link	UP	London - Manchester (extra HTTP Traffic)					0	0	0	0
28	[Manchester] -> [Port Output]	Link	UP	London - Manchester (extra HTTP Traffic)					4,624	4,624	1	1
29	[Manchester] -> [Port Output]	Link	UP	London - Manchester (extra HTTP Traffic)					0	0	0	0

2-2. Packet Replay Example in Multi-Point Networks

In this example, we have already set up a Fully Meshed Multi-Point network with the configuration described in *Creating Fully Meshed Networks* on page 416). In addition to the T1 - Excellent link going between the Paris node and Berlin node, an additional T1 - Poor link is created on the Fully Meshed Multi-Point network. This additional T1 - Poor link is created in order to illustrate how we can route packets from the different packet streams in the generated traffic stream to target different links between the endpoint nodes.

ILLUSTRATION 218 - OVERVIEW OF MESH MULTI-POINT EXAMPLE WITH INTELLIGENT PACKET REPLAY



In this example, the pcap file that will be used for adding traffic within the Fully Meshed Multi-Point network contains multiple packet streams from different initiators and responders, with different traffic types (e.g. HTTP (TCP 80), FTP (TCP 21), etc.).

We will use the **Select Streams** dialog box (see *Illustration 194*) to select HTTP traffic (TCP 80) from some of the packet streams of the specified pcap file for the following initiator addresses:

- 192.168.3.191 - Five packet streams are selected (all with unique responder addresses). The packets in the packet streams from this initiator address will be routed down the T1 - Excellent link.
- 172.16.255.1 - Five packet streams are selected (three of which have the same responder address). The packets in the packet streams from this initiator address will be routed down the T1 - Poor link.

We will also use the **Configure Stream Directions** dialog box (see *Illustration 196*) to modify the original filtered packet stream directions inherited from the pcap file. In our example, we need to modify the packet stream directions inherited from the pcap file so that the Berlin endpoint node is assigned to the IP address of packet streams with the port 80.

In this example, do the following:

1. Create the Multi-Point network according to the example described in *Creating Fully Meshed Networks* on page 416. In this Multi-Point network, additionally create a T1 - Poor link between the Berlin and Paris endpoint nodes. This network is called Europe Mesh 2 and must have all the routing already set up before applying the Packet Replay node. The filename of this Multi-Point network is `Europe Mesh 2.itn` located in your `/Private/networks` directory.

   Note:

   You must have fully configured all the routing on the Multi-Point network before proceeding with the steps below.

   When you use the stream configuration tool, it will automatically create the routes in the Composite Routing (Labs) function on the Packet Replay node for each of the selected packet streams with the correct Port Out values (inherited from the links between the Packet Replay node and endpoint nodes) and Spoof Port In values (inherited from the Port In values of the connected endpoint nodes) of the fully configured Multi-Point network, as summarized in *Table 77* on page 688. If you do not fully configure the Multi-Point network before proceeding with the steps below, then you will need to manually create the routes summarized in *Table 77* on page 688 in the Composite Routing (Labs) function on the Packet Replay node.

2. Use the following steps to create a copy of the Europe Mesh network, which you will rename to Europe-Mesh 2 (Packet Replay), and use for the additional HTTP traffic that you will add into the Multi-Point network. To do this, use the following sub-steps:
   a. Open the original Europe Mesh Multi-Point network.
   b. From the Multi-Point Designer, select **FILE > Save as**.
   c. From the **Network name** dialog box that appears, type **`Europe Mesh 2 (Packet Replay)`**, then click **OK**.

      The a new network file called `Europe Mesh 2 (Packet Replay).itn` in your `/Private/networks` directory is now ready to be used with the Intelligent Packet Replay function.

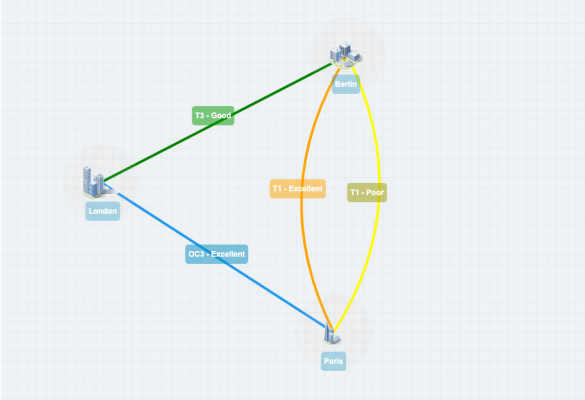
3. Obtain or create a packet capture file for use within the Multi-Point network (see *Packet Replay pcap File Prerequisites* on page 610). In our example, the `WebTraffic.pcap` file containing many packet streams (including HTTP (TCP 80)) has been previously generated, and uploaded to within the `/Private/packet_replay_files` directory.

   Note:

   To potentially save time typing the full path later on in step 9.b., you can use the File Browser's **Copy File Path** pop-up menu function to copy the full path of the pcap file, and then paste it within the **Path** field. To do this, right mouse click on the pcap file (in our example, `WebTraffic.pcap` within the `/Private/packet_replay_files` directory), and select **Copy File Path** from the pop-up menu that appears.

4. Open the copied Multi-Point network from either the **Home** page or File Browser. In our example, we open the renamed network file called `Europe Mesh 2 (Packet Replay).itn`.

The copied Multi-Point network appears in the Multi-Point Designer.



5. Add an Intelligent Packet Replay node into the Multi-Point network and create the appropriate links between the Paris / Berlin endpoint nodes and the Intelligent Packet Replay node, as follows:

   a. Drag the Intelligent Packet Replay node represented by the  icon from the **Packet Replay** node category into the Workspace.

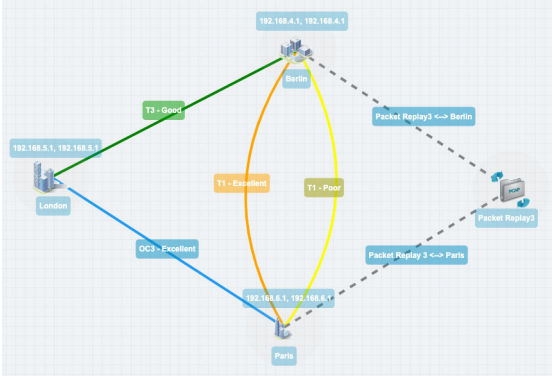
   Note: The Intelligent Packet Replay node gets automatically named **Packet Replay3**. This is normal is it the fourth node to have been created in the Multi-Point network. Berlin (originally called node0) was the first node to have originally be created. Paris (originally called node1) was the second node to have originally been created. London (originally called node2) was the second node to have originally been created.

   b. Create a link starting from the Intelligent Packet Replay node ending at the Berlin endpoint node. In the **Link Name** dialog box that appears, optionally change the default link name. In our example, rename the link name from Packet Replay3 <--> Berlin-1 to **`Packet Replay3 <--> Berlin`**.

   c. Create a link starting from the Intelligent Packet Replay node ending at the Paris endpoint node.

   d. In the **Link Name** dialog box that appears, optionally change the default link name. In our example, rename the link name from Packet Replay3 <--> Paris-1 to **`Packet Replay3 <--> Paris`**.

The Workspace in the Multi-Point Designer now appears as follows.



At this stage the Intelligent Packet Replay function will have created/appended appropriate "framework" routes to the existing IP Routing (Labs) routing functions on the Paris and Berlin endpoint nodes, as described above in *Packet Replay Implementation in the Multi-Point Designer* on page 628.

At this stage the Intelligent Packet Replay function will have also created appropriate "framework" routes to the existing Composite Routing (Labs) routing function on the Packet Replay3 node, as described above in *Packet Replay Implementation in the Multi-Point Designer* on page 628.

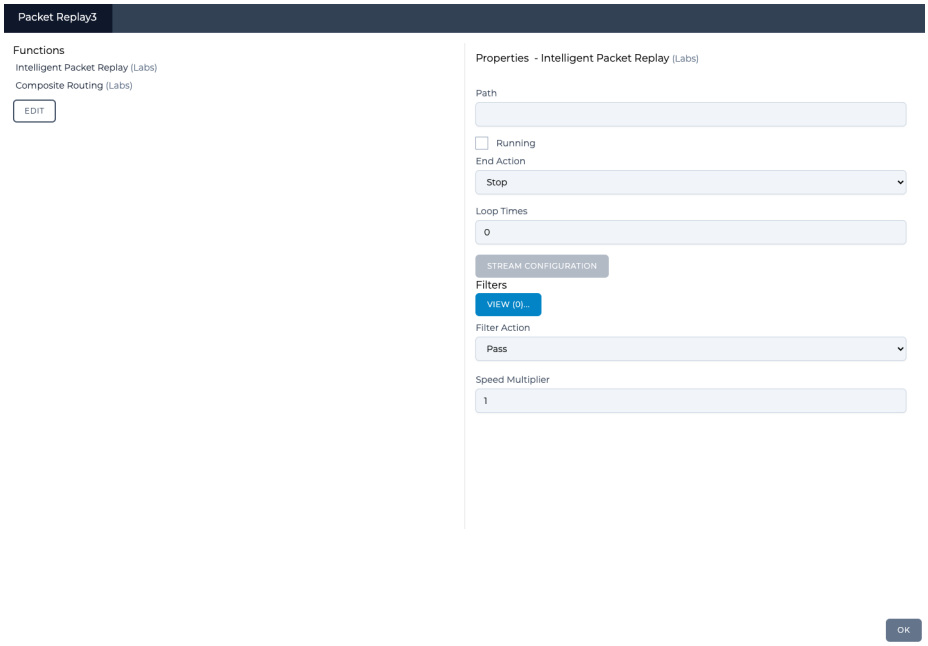
At this stage no "packet replay" routes currently exist because you have not yet selected and configured the packet streams to be used in the generated traffic stream.

6. Optionally save the current "work in progress" Fully Meshed Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

   You must now select and configure the packet streams that you want to include in the traffic stream generated by the Intelligent Packet replay function.

7. Click on the **Packet Replay3** node in the Workspace.
8. From the **Edit node** panel that appears, click the **PROPERTIES** button.

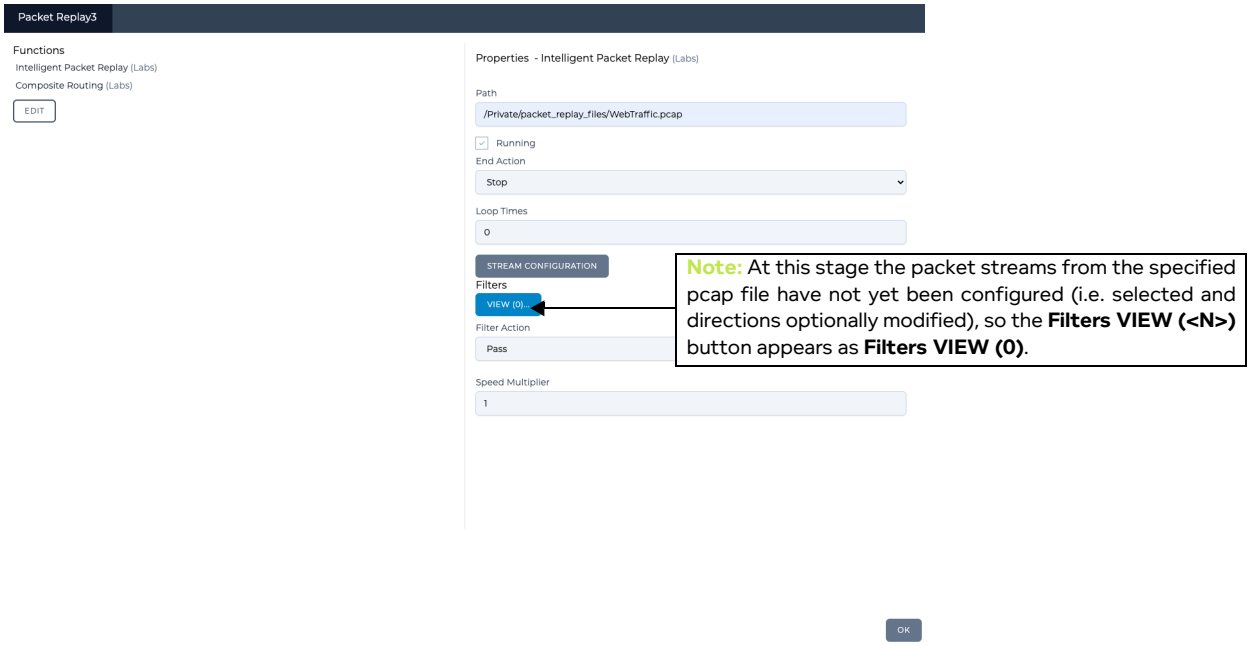
   A **Packet Replay3 - Advanced Node Properties** window appears, with the initial (default) properties of the Intelligent Packet Replay (Labs) function.



9. From the **Properties - Intelligent Packet Relay (Labs)** area of the **Packet Replay3 - Advanced Node Properties** window, do the following to configure the general settings of the Intelligent Packet Replay function:
   a. Enable the **Running** check box.
   b. In the **Path** field, type the path to the pcap file within the NE-ONE file system that will be used by the Intelligent Packet Replay function. In our example, the `WebTraffic.pcap` file located within the `/Private/packet_replay_files` directory is used, and you would type **`/Private/packet_replay_files/WebTraffic.pcap`**.

      Note: If you previously copied the full path of the pcap file in step 3 above, you can paste it into the **Path** field by right mouse clicking and selecting **Paste**, or by pressing the **CTRL** + **V** keys (on Windows) or by pressing the **CMD** + **V** keys (on MacOS).
   c. From the **End Action** drop-down field, select **Loop**.
   d. In the **Loop Times** field, leave the default value set to **0**. The default value of 0 is the equivalent to an infinite number of loop times.
   e. In the **Slowdown Multiplier** field, leave the default value set to 1.

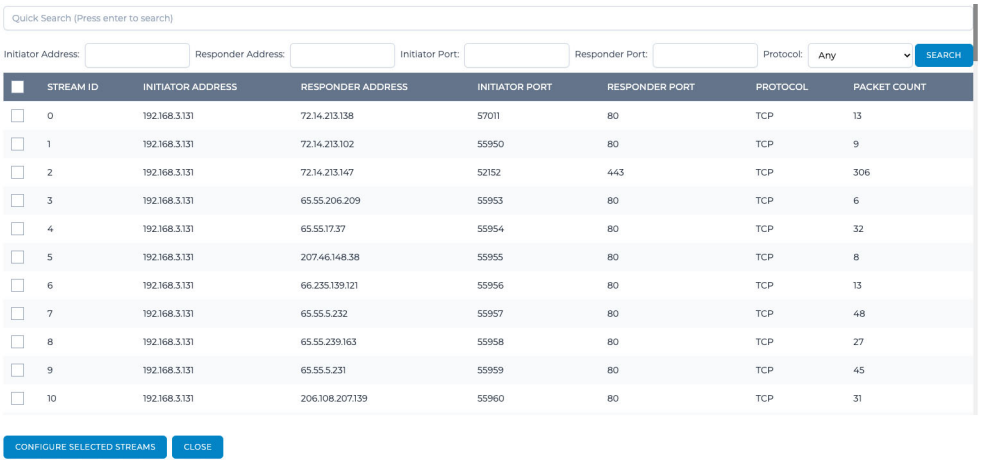
At this stage the general settings of the Intelligent Packet Replay function are now configured.



You must now configure the packet streams.

10. Click the **STREAM CONFIGURATION** button.

    The NE-ONE analyzes the specified pcap file. The analysis time varies according to the size of the specified pcap file. Once the NE-ONE finishes analyzing the specified pcap file, an initial **Select Streams** dialog box (with no packet streams selected) similar to the following appears.



    You can use the **Select Streams** dialog box to determine which packet streams you want to include in the traffic stream that is generated by the Intelligent Packet Replay function. For more detailed information on using the **Select Streams** dialog box, see *Select Streams Dialog Box* on page 611.

    In our example (described in step 11 below) we will select some HTTP traffic (TCP 80) from two initiator nodes, with the following IP addresses 192.168.3.131, and 172.16.255.1.

11. In the **Select Streams** dialog box, do the following to select all HTTP traffic (TCP 80) from for each of the initiator addresses of interest (in our example, 192.168.3.131, and 172.16.255.1).

    Select all of the packet streams for HTTP traffic (TCP 80) on initiator 192.168.3.131:

    a. In the **Protocol** field, select **TCP**.

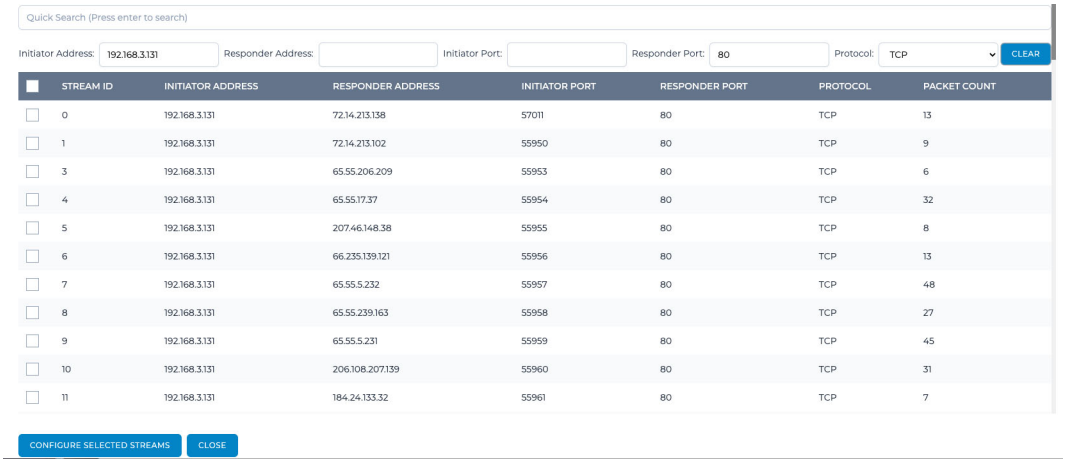
b. In the **Responder Port** field, type **80**.

c. In the **Initiator Address** type **192.168.3.131**.

d. Leave the other **Responder Address** and **Initiator Port** fields empty.

e. Click the **SEARCH** button.

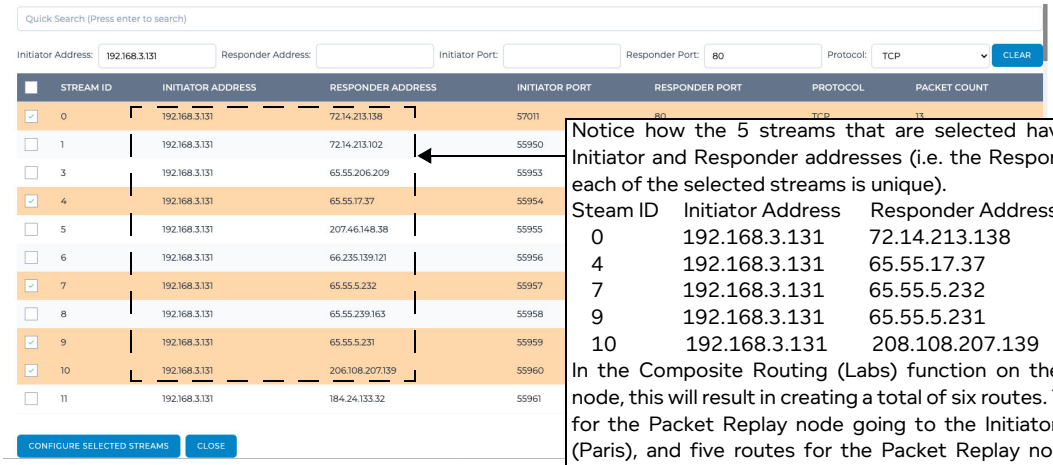
The **Select Streams** dialog box returns a set of unselected packet streams, based upon your specified filter criteria. In our example, all the packet streams corresponding to the filter for HTTP traffic (i.e. Protocol : TCP, Responder Port : 80, and initiator 192.168.3.131) is displayed.



Note: The time it takes to return the set of unselected packet streams varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).

The set of packet streams are initially unselected (i.e. each check box is unselected).

f. Enable the check boxes corresponding to each of the packet streams you want to include in the generated traffic stream. In our example, we enable the check boxes associated with the five packet streams with stream IDs 0, 4, 7, 9, and 10.



Notice how the 5 streams that are selected have the following Initiator and Responder addresses (i.e. the Responder address for each of the selected streams is unique).

Steam ID	Initiator Address	Responder Address
0	192.168.3.131	72.14.213.138
4	192.168.3.131	65.55.17.37
7	192.168.3.131	65.55.5.232
9	192.168.3.131	65.55.5.231
10	192.168.3.131	208.108.207.139

In the Composite Routing (Labs) function on the Packet Replay node, this will result in creating a total of six routes. That is one route for the Packet Replay node going to the Initiator endpoint node (Paris), and five routes for the Packet Replay node going to the Responder endpoint node (Berlin). See step 21 on page 686 along with *Table 77* on page 688for more information.

Note: At this stage, do not click the **CONFIGURE SELECTED STREAMS** button. You will continue to "build up" and select the HTTP traffic for the other initiator (i.e. 172.16.255.1).

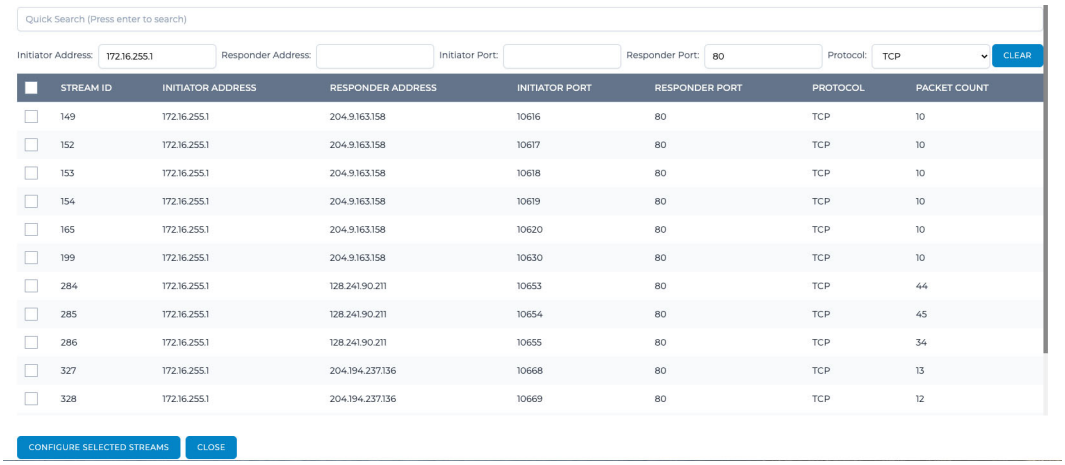
g. Click the **CLEAR** button.

The search filter bar resets, and the selected HTTP traffic streams for initiator 192.168.3.131 remain selected.

Select all of the packet streams for HTTP traffic (TCP 80) on initiator 172.16.255.1:

a. In the **Protocol** field, select **TCP**.
b. In the **Responder Port** field, type **80**.
c. In the **Initiator Address** type **172.16.255.1**.
d. Leave the other **Responder Address** and **Initiator Port** fields empty.
e. Click the **SEARCH** button.

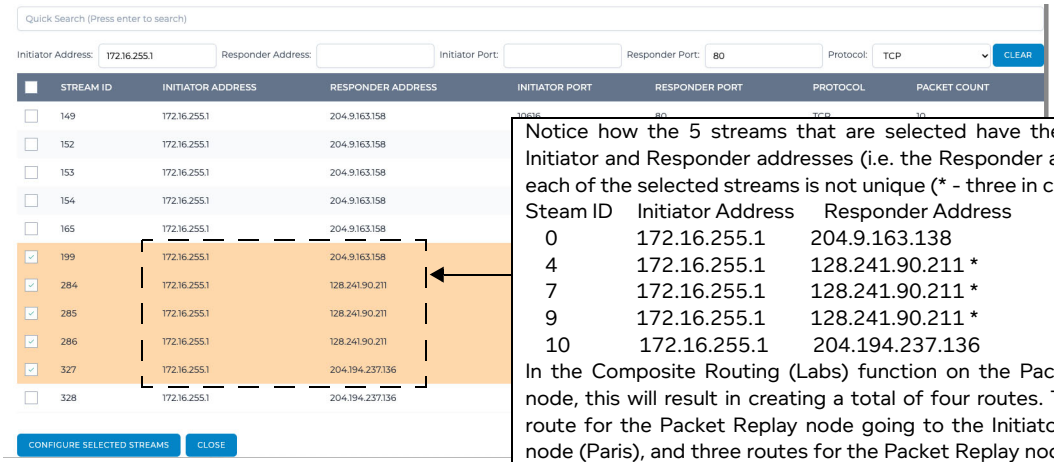
The **Select Streams** dialog box returns a set of unselected packet streams, based upon your specified filter criteria. In our example, all the packet streams corresponding to the filter for HTTP traffic (i.e. Protocol : TCP, Responder Port : 80, and initiator 172.16.255.1) is displayed.



Note: The time it takes to return the set of unselected packet streams varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).

The set of packet streams are initially unselected (i.e. each check box is unselected).

f. Enable the check boxes corresponding to each of the packet streams you want to include in the generated traffic stream. In our example, we enable the check boxes associated with the five packet streams with stream IDs 199, 284, 285, 286, and 327.



Notice how the 5 streams that are selected have the following Initiator and Responder addresses (i.e. the Responder address for each of the selected streams is not unique (* - three in common)).

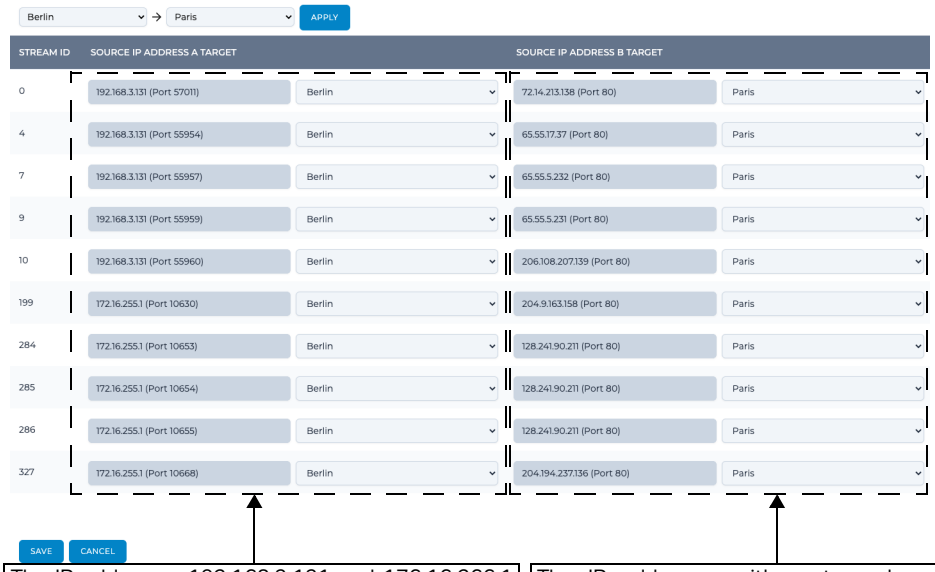
Steam ID	Initiator Address	Responder Address
0	172.16.255.1	204.9.163.138
4	172.16.255.1	128.241.90.211 *
7	172.16.255.1	128.241.90.211 *
9	172.16.255.1	128.241.90.211 *
10	172.16.255.1	204.194.237.136

In the Composite Routing (Labs) function on the Packet Replay node, this will result in creating a total of four routes. That is one route for the Packet Replay node going to the Initiator endpoint node (Paris), and three routes for the Packet Replay node going to the Responder endpoint node (Berlin). See step 21 on page 686 along with *Table 77* on page 688for more information.

Note: At this stage, all the HTTP traffic for all of the initiators have now been built up and selected. Proceed to step 12.

12. Click the **CONFIGURE SELECTED STREAMS** button.

A **Configure Stream Directions** dialogue box appears.

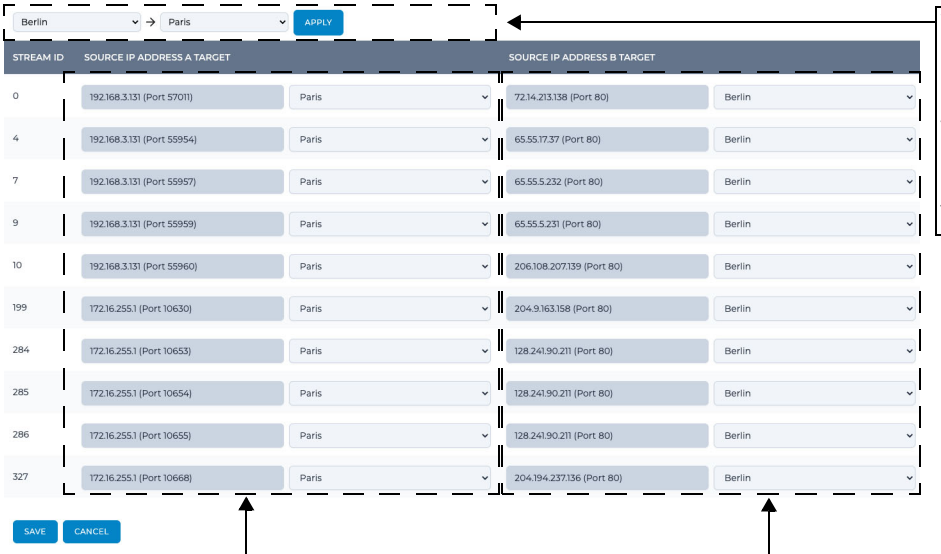


You can optionally use the **Configure Stream Directions** dialog box to determine the direction of each packet stream included in the generated traffic stream. For detailed information on using the **Configure Stream Directions** dialog box, see *Configure Stream Directions Dialog Box* on page 618.

In our example (described in step 13 below) the packet stream directions inherited by the specified pcap file are is initially incorrect. In our Fully Meshed Multi-Point network example, the Berlin endpoint node is the web server (Responder endpoint node) and the Paris endpoint node is the client (Initiator endpoint node). So we want the Berlin endpoint node to be assigned to all the IP addresses with port number 80.

13. From the **Configure Stream Directions** dialog box that appears, do the following:
    a. Scroll down and verify the direction of each packet stream, paying attention to which endpoint node (e.g. Berlin and Paris) is assigned to the IP addresses and port numbers as expected (e.g. a client (the initiator) typically opens a random high port number to communicate with a web server (the responder) who is listening and communicating over port 80).
    b. If required, change the packet stream directions. In our example, we want to assign the Berlin endpoint node to all the IP addresses with port 80, and the Paris endpoint node to the IP addresses 192.168.3.131 and 176.16.266.1 (with varying port numbers of a high value). To save time, instead of changing each stream individually, you can use the replace all instances area to

change all instances of Paris with Berlin (and vice versa).



You can use the replace all instances area, to quick change all instances of Paris with Berlin (and vice versa).
To do this, ensure the left drop-down field has **Berlin** and the right drop-down field has **Paris**, then click **APPLY**.

The IP addresses 192.168.3.131 and 176.16.266.1 (with varying port numbers of a high value) are now assigned to the Paris endpoint node.

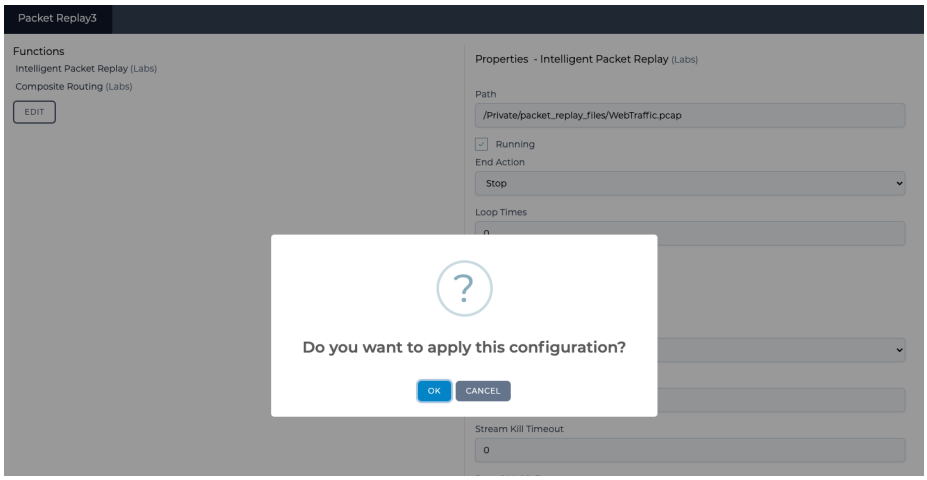
The IP addresses with port number 80 are now assigned to the Berlin endpoint node.

c. When you are happy with the each of the packet stream directions, click **SAVE**.

Note:

The time it takes to save the stream configuration varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute).

Upon clicking **SAVE**, a **Do you want to apply this configuration?** dialog box appears.

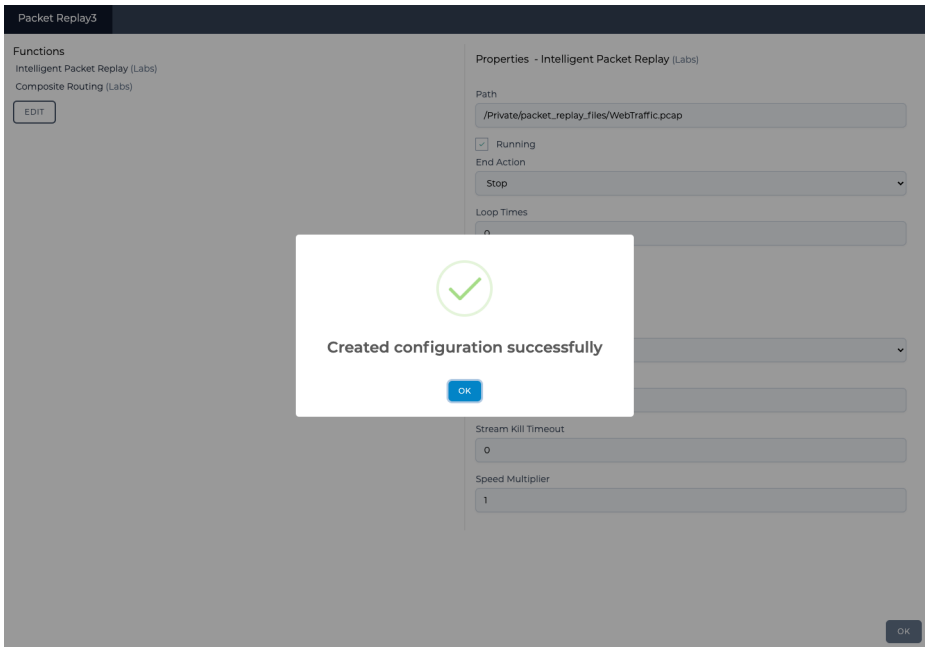


14. From the **Do you want to apply this configuration?** dialog box that appears, click **OK**.

Note:

The time it takes to apply the configuration of the Intelligent Packet Replay function to the Multi-Point network varies according to the size of the specified pcap file. If the pcap file is large, the time to wait may be considerable (i.e. more than a minute). Once the Intelligent Packet Replay function's configuration has been applied, the **Created configuration successfully** dialog box appears.

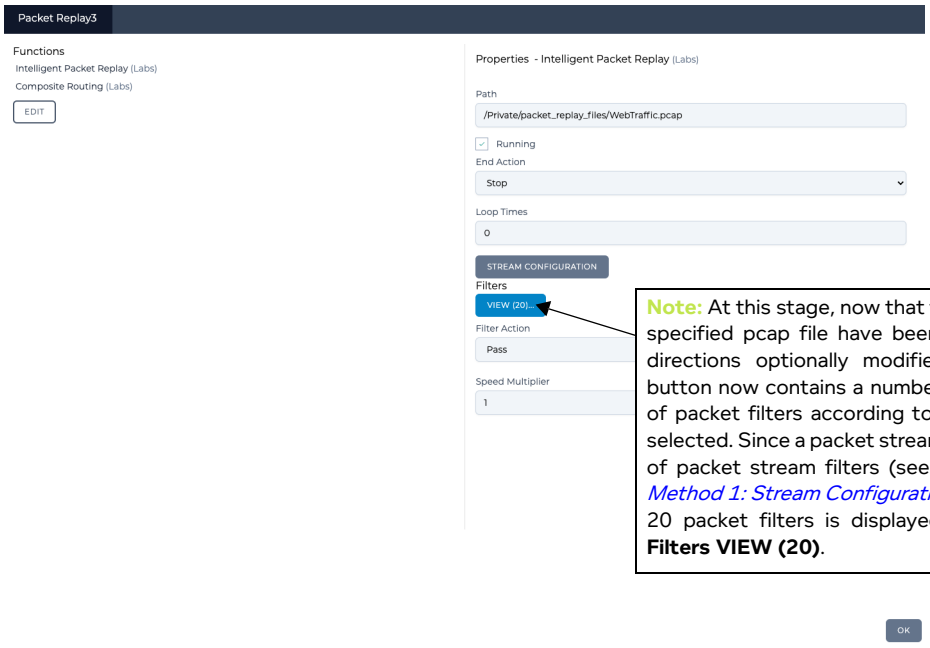
15. From the **Created configuration successfully** dialog box that appears, click **OK**.



The **Created configuration successfully** dialog box closes, and you are returned to the **Packet Replay3 - Advanced Node Properties** window.

Note:

The **Filters VIEW (<N>)** button now also contains a number, indicating the number of packet streams that were selected. In our example, since a total of 10 packet streams were selected and configured, the **Filters VIEW (<N>)** shows 20 (i.e. 2x the number of selected packet streams). This is normal as the filter table is at the packet level (rather than the packet stream level), and a packet stream is a bi-direction conversation between an initiator and responder (and thus corresponds to a pair of packet filters).



Note: At this stage, now that the 10 packet streams from the specified pcap file have been configured (i.e. selected and directions optionally modified), the **Filters VIEW (<N>)** button now contains a number corresponding to the number of packet filters according to the packet streams that were selected. Since a packet stream filter is the equivalent of a pair of packet stream filters (see the description in the section *Method 1: Stream Configuration Tool* on page 633), a total of 20 packet filters is displayed, and the button appears as **Filters VIEW (20)**.

16. Click **OK** to close the **Packet Replay3 - Advanced Node Properties** window.

17. Close the **Edit node** panel.

! Notice:

At the stage, even if the Intelligent Packet Replay function's configuration has been applied to the Multi-Point network, the Multi-Point network itself has been modified since it was initially opened, and must be saved in order for the Intelligent Packet Replay function to take effect.

Note:

If you run the Multi-Point network at this stage, all the selected packet streams from the generated traffic stream will not go down the links between the Paris and Berlin endpoint nodes because their routes are not yet set up.

You must now manually create routes on the Paris and Berlin endpoint nodes, so that:

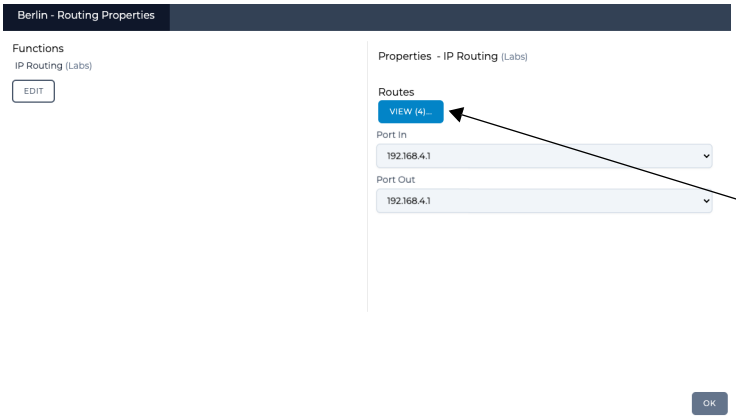
- packet streams containing packets with the source IP address 192.168.3.191 will be routed down the T1 - Excellent link
- packet streams containing packets with the source IP address 172.16.255.1 will be routed down the T1 - Poor link

To manual create these routes, use steps 18 and 19 below.

18. Manually create the two routes on the Berlin node as follows.

a. Click on the **Berlin** endpoint node, and from the **Edit node** panel that appears, click **ROUTES**.

A **Berlin - Routing Properties** window appears.

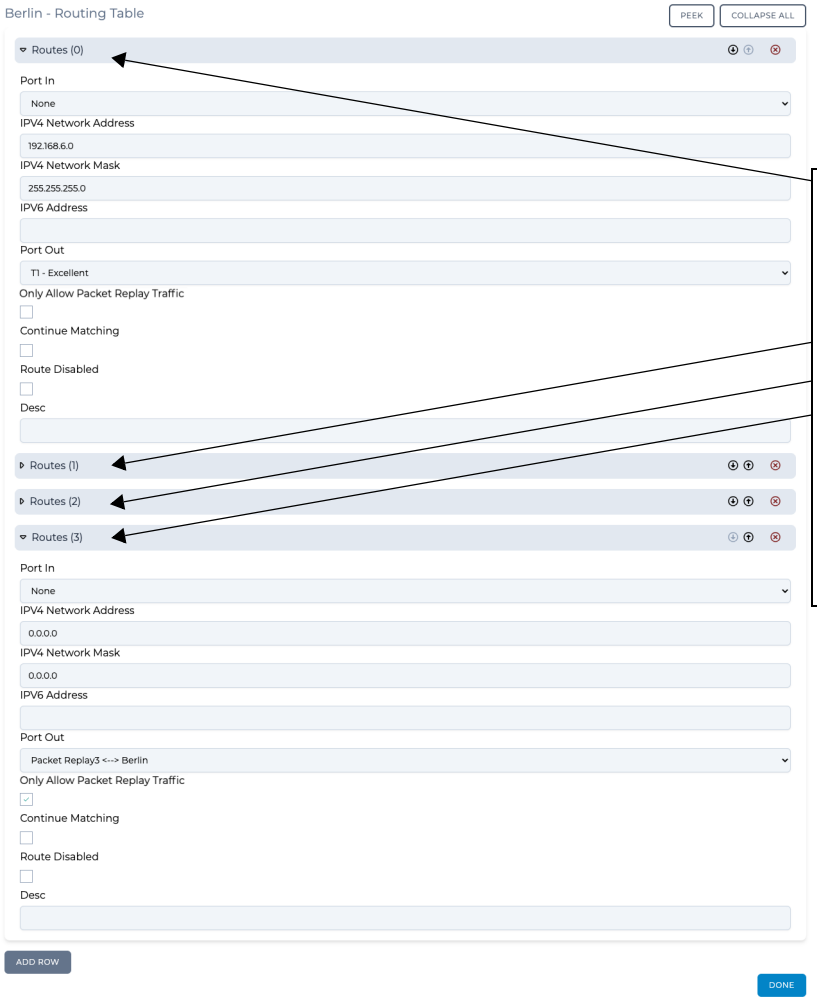


At this stage, the Berlin endpoint node will have four routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Berlin endpoint node
- a fourth "packet replay" route (Routes (4)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Berlin endpoint node. Once the other routes are manually created, this fourth "packet replay" route must be moved to the bottom of the list in the routing table.

b. From the **Berlin - Routing Properties** window that appears, click **Routes VIEW (4)**.

A **Berlin - Routing Table** window appears.



At this stage, the Berlin endpoint node will have four routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Berlin endpoint node
- a fourth "packet replay" route (Routes (3)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Berlin endpoint node. Once the other routes are manually created, this fourth "packet replay" route must be moved to the bottom of the list in the routing table.

c. Click **ADD ROW** twice to create two new routes (i.e. Routes (4) and Routes (5)).
The rows **Routes (4)** and **Routes (5)** get created beneath the **Routes (3)** row.

d. Expand the **Routes (4)** row, type **`192.168.3.191`** in the **IPV4 Network Address** field and select **T1 - Excellent** from the **Port Out** drop-down field.

e. Expand the **Routes (5)** row, type **`172.16.255.1`** in the **IPV4 Network Address** field and select **T1 - Poor** from the **Port Out** drop-down field.

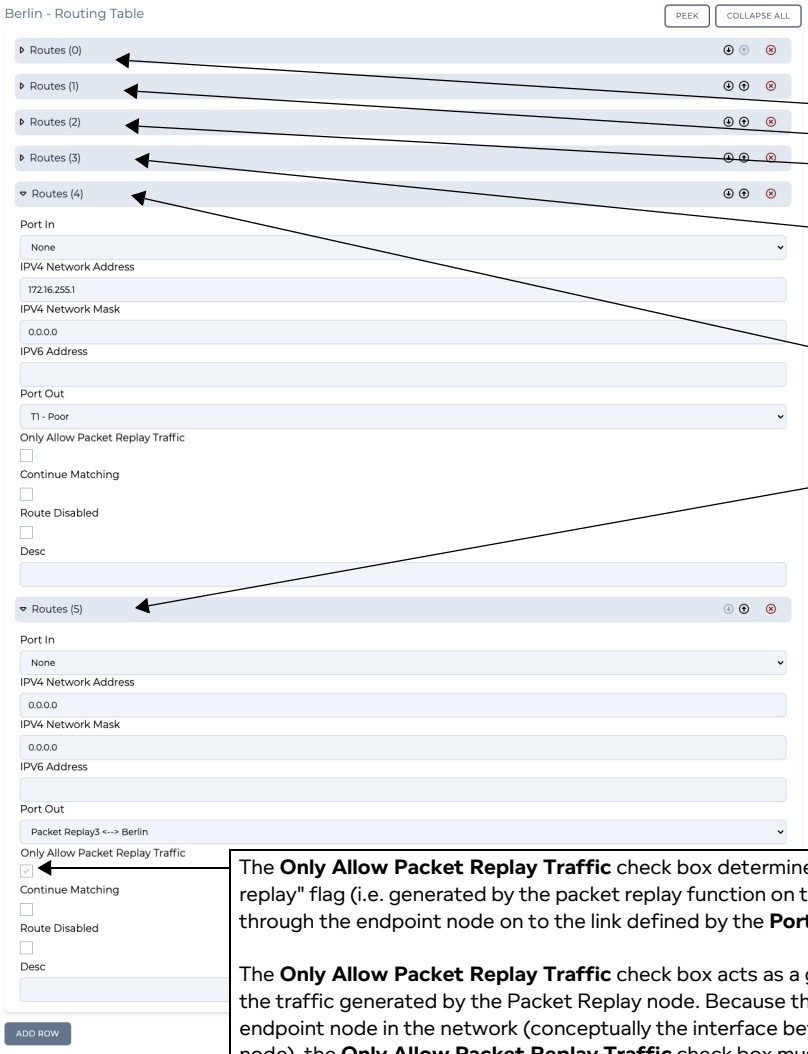
The **Berlin - Routing Table** window now appears as follows.

At this stage, the Berlin endpoint node will have six routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Berlin endpoint node
- a fourth "packet replay" route (Routes (3)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Berlin endpoint node. Now that the other routes are manually created, this fourth "packet replay" route must be moved to the bottom of the list in the routing table.
- a fifth route (Routes (4)) which was manually defined in order to send packet streams containing packets with the source IP address 192.168.3.191 down the T1 - Excellent link
- a sixth route (Routes (5)) which was manually defined in order to send packet streams containing packets with the source IP address 172.16.255.1 down the T1 - Poor link

f. Click on the down arrow for the original "packet replay" route (Routes (3)) until its at the bottom

of the routing table and becomes **Routes (5)** as shown below.



At this stage, the Berlin endpoint node will have six routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Berlin endpoint node
- a fourth route (Routes (3)) which was manually defined in order to send packet streams containing packets with the source IP address 192.168.3.191 down the T1 - Excellent link
- a fifth route (Routes (6)) which was manually defined in order to send packet streams containing packets with the source IP address 172.16.255.1 down the T1 - Poor link
- a sixth "packet replay" route (Routes (5)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Berlin endpoint node, and that you moved to the bottom of the list in the routing table after creating manually creating the two routes.

The **Only Allow Packet Replay Traffic** check box determines whether or not packets with the "packet replay" flag (i.e. generated by the packet replay function on the Packet Replay node) are allowed to pass through the endpoint node on to the link defined by the **Port Out** drop-down field.

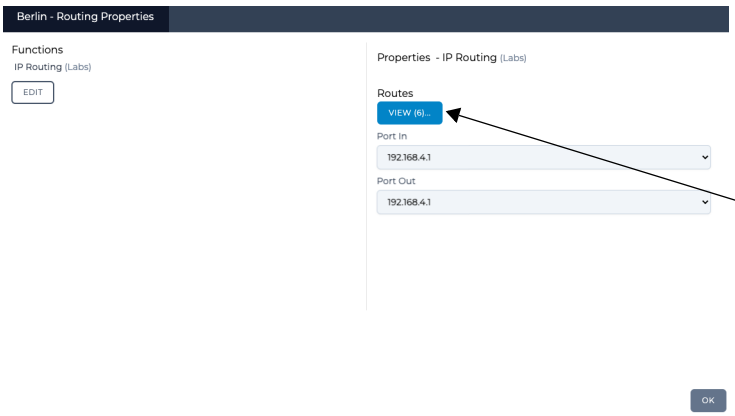
The **Only Allow Packet Replay Traffic** check box acts as a guard to separate real network traffic from the traffic generated by the Packet Replay node. Because this "packet replay" route is on the Berlin endpoint node in the network (conceptually the interface between the network and the Packet Replay node), the **Only Allow Packet Replay Traffic** check box must be enabled to allow the packets from the replayed packet stream(s) (with the "packet replay" tag) on to the network. Further more, this route must be the lowest priority on the endpoint node (i.e. at the bottom of the routing table).

Since this route is allowing packets with the "packet replay" flag and to pass through the Berlin endpoint node, the **Only Allow Packet Replay Traffic** check box is automatically enabled when using the stream configuration tool.

Note: If you are not using the stream configuration tool, and manually creating routes yourself, then the **Only Allow Packet Replay Traffic** check box is disabled by default. In this case you must think to enable it for any routes that going between the endpoint nodes and the Packet Replay node.

g. Click **DONE**.

You are returned to the **Berlin - Routing Properties** window.



At this stage, the Berlin endpoint node will now have six routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Berlin endpoint node
- a fourth route (Routes (3)) which was manually defined in order to send packet streams containing packets with the source IP address 192.168.3.191 down the T1 - Excellent link
- a fifth route (Routes (4)) which was manually defined in order to send packet streams containing packets with the source IP address 172.16.255.1 down the T1 - Poor link
- a sixth "packet replay" route (Routes (5)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Berlin endpoint node, and that you moved to the bottom of the list in the routing table after creating manually creating the two routes.

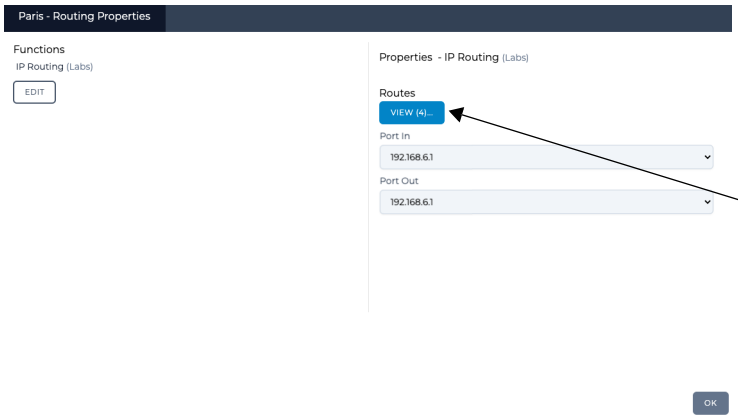
h. Click **OK**.

The **Berlin - Routing Properties** window closes, and you are returned to the Multi-Point Designer.

19. Manually create the two routes on the Paris node as follows.

a. Click on the **Paris** endpoint node, and from the **Edit node** panel that appears, click **ROUTES**.

A **Paris - Routing Properties** window appears.

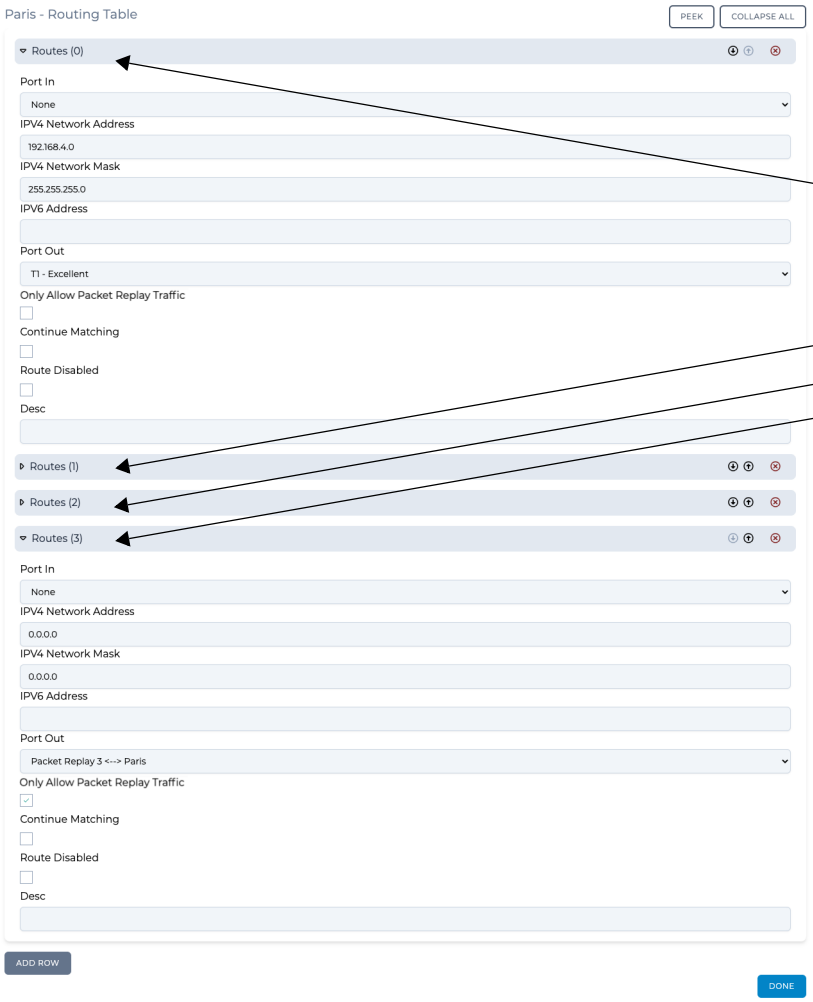


At this stage, the Paris endpoint node will have four routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Paris endpoint node
- a fourth "packet replay" route (Routes (4)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Paris endpoint node. Once the other routes are manually created, this fourth "packet replay" route must be moved to the bottom of the list in the routing table.

b. From the **Paris - Routing Properties** window that appears, click **Routes VIEW (4)**.

A **Paris - Routing Table** window appears.



At this stage, the Paris endpoint node will have four routes in total, consisting of:

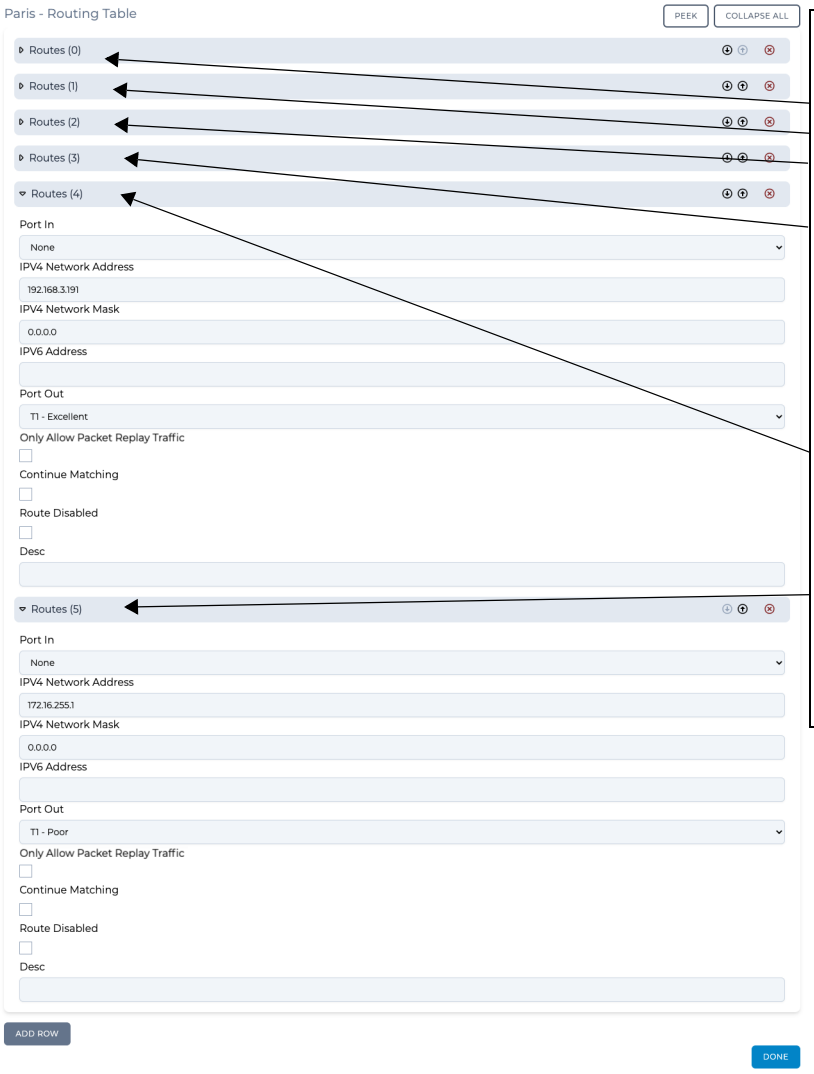
- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Paris endpoint node
- a fourth "packet replay" route (Routes (3)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Paris endpoint node. Once the other routes are manually created, this fourth "packet replay" route must be moved to the bottom of the list in the routing table.

c. Click **ADD ROW** twice to create two new routes (i.e. Routes (4) and Routes (5)).
The rows **Routes (4)** and **Routes (5)** get created beneath the **Routes (3)** row.

d. Expand the **Routes (4)** row, type **`192.168.3.191`** in the **IPV4 Network Address** field and select **T1 - Excellent** from the **Port Out** drop-down field.

e. Expand the **Routes (5)** row, type **`172.16.255.1`** in the **IPV4 Network Address** field and select **T1 - Poor** from the **Port Out** drop-down field.

The **Paris - Routing Table** window now appears as follows.



At this stage, the Paris endpoint node will have six routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Paris endpoint node
- a fourth "packet replay" route (Routes (3)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Paris endpoint node. Now that the other routes are manually created, this fourth "packet replay" route must be moved to the bottom of the list in the routing table.
- a fifth route (Routes (4)) which was manually defined in order to send packet streams containing packets with the source IP address 192.168.3.191 down the T1 - Excellent link
- a sixth route (Routes (5)) which was manually defined in order to send packet streams containing packets with the source IP address 172.16.255.1 down the T1 - Poor link

f. Click on the down arrow for the original "packet replay" route (Routes (3)) until its at the bottom

of the routing table and becomes **Routes (5)** as shown below.

At this stage, the Paris endpoint node will have six routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Paris endpoint node
- a fourth route (Routes (3)) which was manually defined in order to send packet streams containing packets with the source IP address 192.168.3.191 down the T1 - Excellent link
- a fifth route (Routes (6)) which was manually defined in order to send packet streams containing packets with the source IP address 172.16.255.1 down the T1 - Poor link
- a sixth "packet replay" route (Routes (5)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Paris endpoint node, and that you moved to the bottom of the list in the routing table after creating manually creating the two routes.

The **Only Allow Packet Replay Traffic** check box determines whether or not packets with the "packet replay" flag (i.e. generated by the packet replay function on the Packet Replay node) are allowed to pass through the endpoint node on to the link defined by the **Port Out** drop-down field.

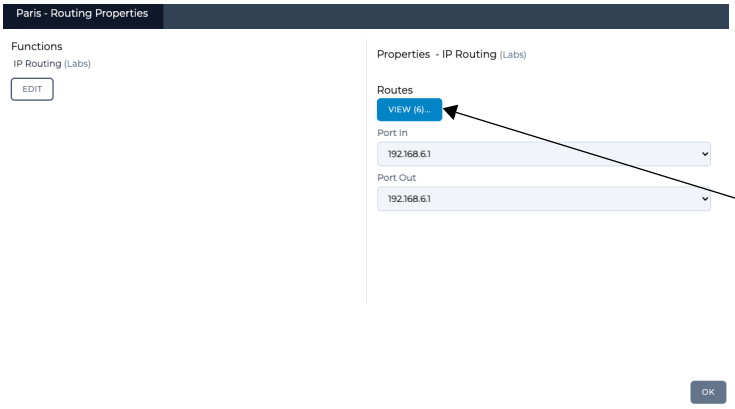
The **Only Allow Packet Replay Traffic** check box acts as a guard to separate real network traffic from the traffic generated by the Packet Replay node. Because this "packet replay" route is on the Paris endpoint node in the network (conceptually the interface between the network and the Packet Replay node), the **Only Allow Packet Replay Traffic** check box must be enabled to allow the packets from the replayed packet stream(s) (with the "packet replay" tag) on to the network. Further more, this route must be the lowest priority on the endpoint node (i.e. at the bottom of the routing table).

Since this route is allowing packets with the "packet replay" flag and to pass through the Paris endpoint node, the **Only Allow Packet Replay Traffic** check box is automatically enabled when using the stream configuration tool.

Note: If you are not using the stream configuration tool, and manually creating routes yourself, then the **Only Allow Packet Replay Traffic** check box is disabled by default. In this case you must think to enable it for any routes that going between the endpoint nodes and the Packet Replay node.

g. Click **DONE**.

You are returned to the **Paris - Routing Properties** window.



At this stage, the Paris endpoint node will now have six routes in total, consisting of:

- the first three routes (Routes (0), Routes (1) and Routes (2) that were created at the time of creating the Multi-Point network and associated with the three links going into the Paris endpoint node
- a fourth route (Routes (3)) which was manually defined in order to send packet streams containing packets with the source IP address 192.168.3.191 down the T1 - Excellent link
- a fifth route (Routes (4)) which was manually defined in order to send packet streams containing packets with the source IP address 172.16.255.1 down the T1 - Poor link
- a sixth "packet replay" route (Routes (5)) that got automatically created when creating the Packet Replay node and creating a link between the Packet Replay node and the Paris endpoint node, and that you moved to the bottom of the list in the routing table after creating manually creating the two routes.

h. Click **OK**.

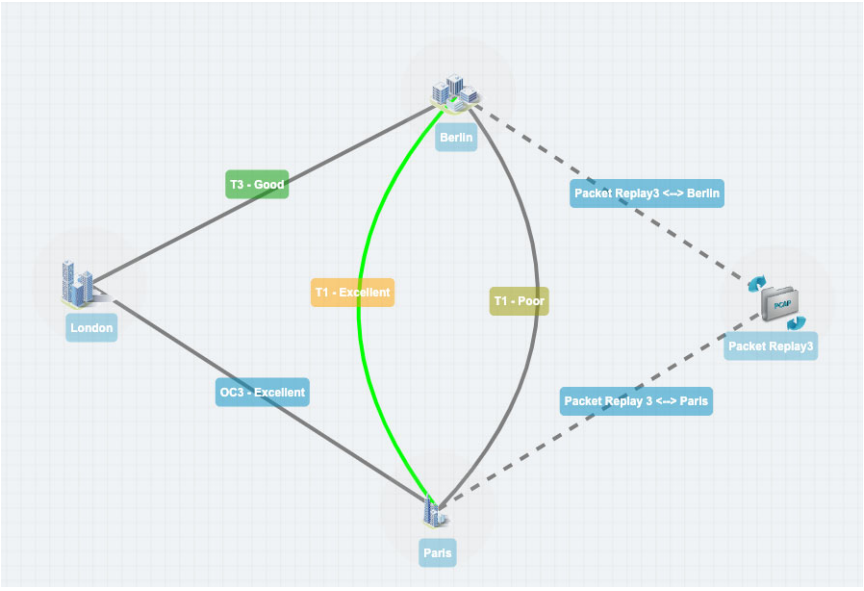
The **Berlin - Routing Properties** window closes, and you are returned to the Multi-Point Designer.

At this stage the Multi-Point network is now fully configured, and finalized.

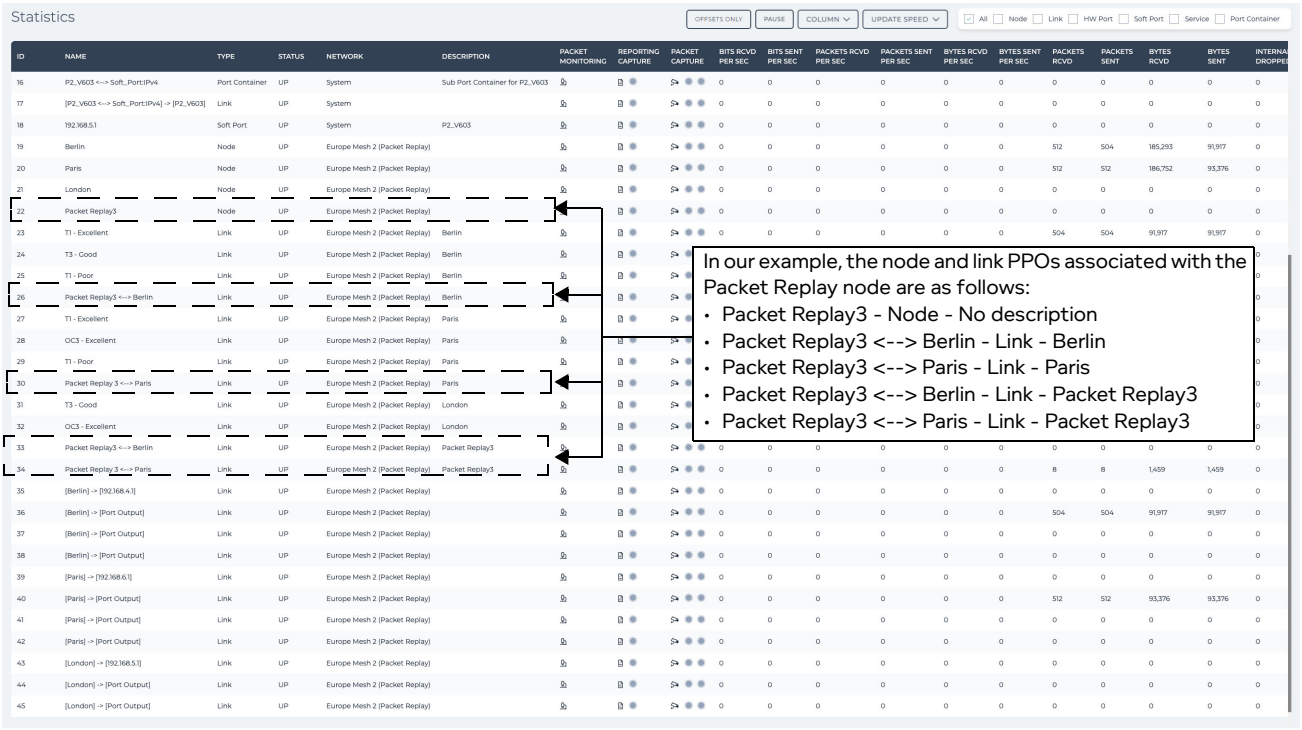
20. Save the finalized Multi-Point network. To do this, select **FILE > Save** or click the **SAVE** button.

Now that the Multi-Point network is fully configured, it can now be run and the selected HTTP packet streams that you configured in the Intelligent Packet Reply function of the Packet Reply node will be injected into the Multi-Point network with the routing criteria you manually specified.

When you run the Multi-Point network, the links will turn gray. Any links with packets are going down them will turn green. In the example below, packets from the packet streams being replayed by the Packet Replay node are going down the T1 - Excellent link between the Berlin and Paris endpoint nodes.

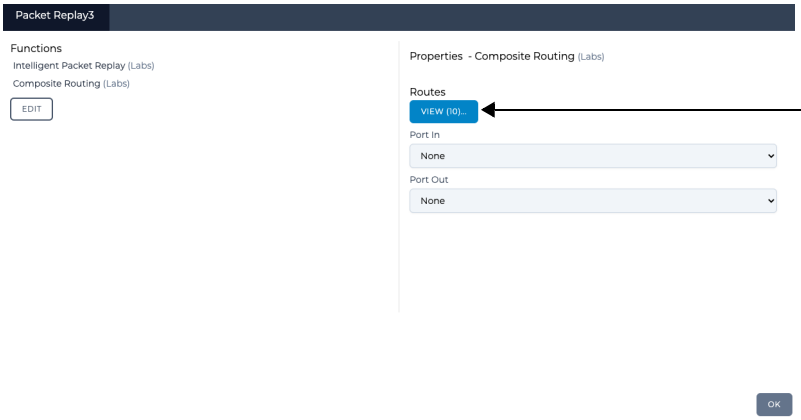


The node and link PPOs associated with the Packet Replay node can be seen in the **Statistics** page. In the example **Statistics** page below, we see the node PPOs associated with the Packet Replay node are represented like any other PPO in the Multi-Point network.



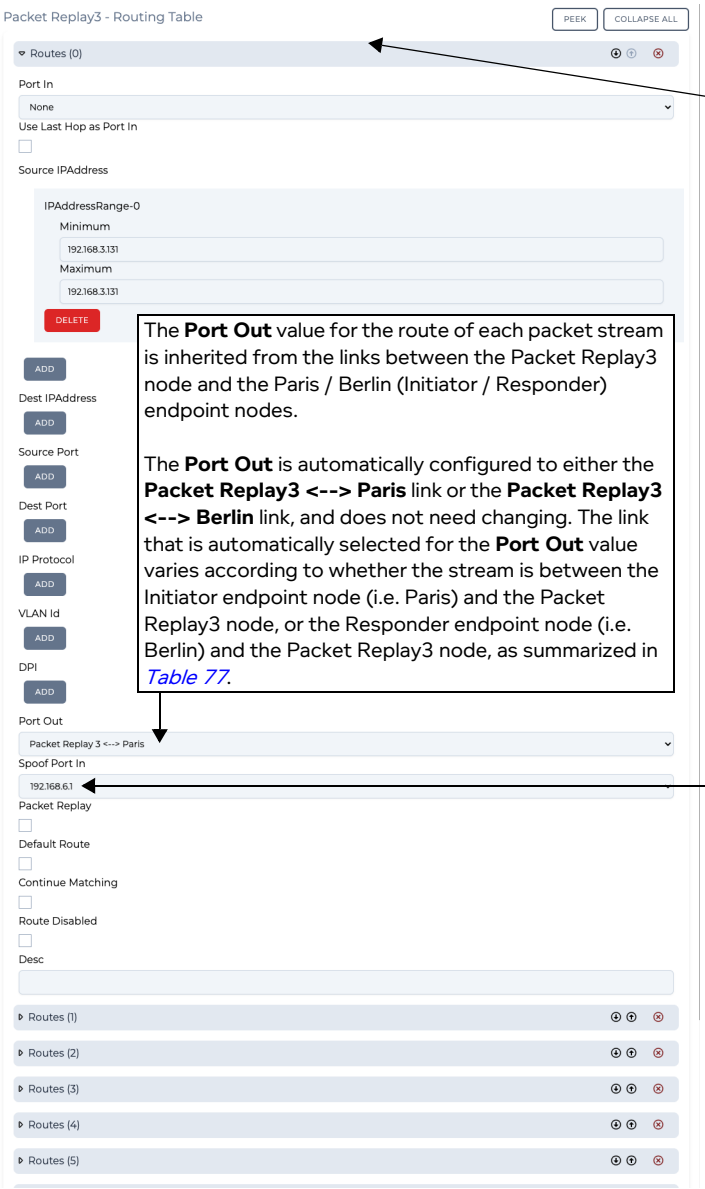
21. Although the configuration of Multi-Point network is finalized, it is interesting to observe the routes that were created by the stream configuration tool in the Composite Routing (Labs) function on the on the Packet Replay node. Observing these routes help you understand how you could manually create these routes (if you choose to do so) instead of using the stream configuration tool. It also highlights the advantages of using the stream configuration tool opposed to manually creating the routes yourself.
    a. Click on the **Packet Replay3** node in the Workspace.
    b. From the **Edit node** panel that appears, click the **PROPERTIES** button.
    c. From the **Packet Replay3 - Advanced Node Properties** window that appears, click the **Composite Routing (Labs)** function.

    The **Packet Replay3 - Advanced Node Properties** window updates with the **Properties - Composite Routing (Labs)** area, as shown below.



In our example, the stream configuration tool automatically created 10 routes in the Composite Routing (Labs) function on the Packet Replay node, these routes are summarized in *Table 77*.

d. Click on the **Routes VIEW (10)** button.
A **Packet Replay3 - Routing Table** window appears.



In our example, the stream configuration tool automatically created 10 routes in the Composite Routing (Labs) function on the Packet Replay node. If you were to expand these routes they would like similar to Route (0) expanded here, with their settings summarized in *Table 77*.

The **Port Out** value for the route of each packet stream is inherited from the links between the Packet Replay3 node and the Paris / Berlin (Initiator / Responder) endpoint nodes.

The **Port Out** is automatically configured to either the **Packet Replay3 <--> Paris** link or the **Packet Replay3 <--> Berlin** link, and does not need changing. The link that is automatically selected for the **Port Out** value varies according to whether the stream is between the Initiator endpoint node (i.e. Paris) and the Packet Replay3 node, or the Responder endpoint node (i.e. Berlin) and the Packet Replay3 node, as summarized in *Table 77*.

The **Spoof Port In** parameter will inherit the Port In routing configuration of the Paris and Berlin endpoint nodes as summarized in *Table 77*. The Paris endpoint node routing is configured to use IPv4 soft port 192.168.6.1 on the Port In, and so the **Spoof Port In** parameter of the routes associated with the **Packet Replay3 <--> Paris** links will be automatically configured to 192.168.6.1. Similarly, the Berlin endpoint node routing is configured to use IPv4 soft port 192.168.4.1 on the Port In, and so the **Spoof Port In** parameter of routes associated with the **Packet Replay3 <--> Berlin** links will be automatically configured to 192.168.4.1. The **Spoof Port In** parameter is required and used on the Composite Routing (Labs) function on the Packet Replay node so that the replayed packet streams from the specified pcap file looks like they are coming from the spoofed Port In of the Paris and Berlin endpoint nodes rather than the original locations specified in the pcap file.

Note: if the **Spoof Port In** parameter is different to that of the Port In routing parameter on the Paris and Berlin endpoint nodes, it means you did not finalize (or you have changed) the routing configuration of the network before running the stream configuration tool. Always finalize the routing configuration of the network before running the stream configuration tool. If you do not finalize the routing configuration of the network before running the stream configuration tool, you will need to manually re-configure the **Spoof Port In** parameter to match the Port In routing parameter of the endpoint node.

If you were to expand and examine each of the routes, they would be as summarized in *Table 77*.

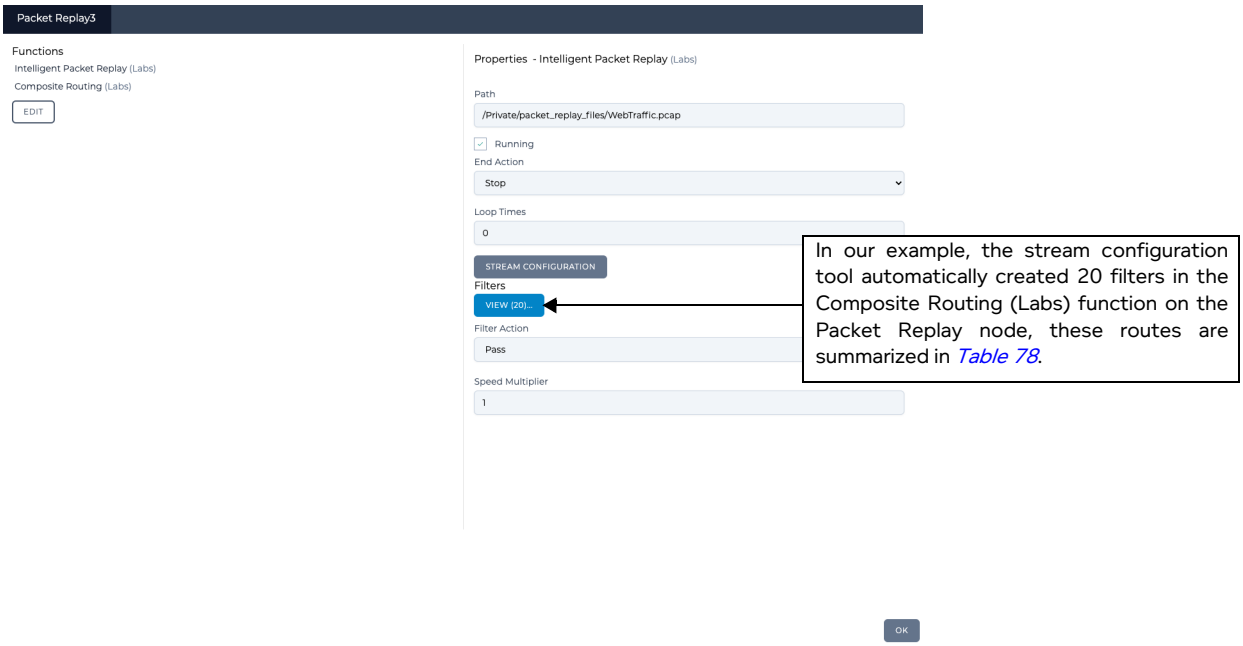
TABLE 77 - ROUTES THAT WERE AUTOMATICALLY GENERATED BY THE STREAM CONFIGURATION TOOL

Route	Source IP Address max and min value	Port Out Value Spoof Port In Value	Corresponding to Stream Number	Initiator or Responder	Initiator filter set
Routes (0)	192.168.3.131	Packet Replay 3 <--> Paris 192.168.6.1	0, 4, 7, 9, 10	Initiator	192.168.3.131
Routes (1)	72.14.213.138	Packet Replay 3 <--> Berlin 192.168.4.1	0	Responder	
Routes (2)	65.55.17.37	Packet Replay 3 <--> Berlin 192.168.4.1	4	Responder	
Routes (3)	65.55.5.232	Packet Replay 3 <--> Berlin 192.168.4.1	7	Responder	
Routes (4)	65.55.5.231	Packet Replay 3 <--> Berlin 192.168.4.1	9	Responder	
Routes (5)	206.108.207.139	Packet Replay 3 <--> Berlin 192.168.4.1	10	Responder	
Routes (6)	172.16.255.1	Packet Replay 3 <--> Paris 192.168.6.1	199, 284, 285, 286, 327	Initiator	172.16.255.1
Routes (7)	204.9.163.158	Packet Replay 3 <--> Berlin 192.168.4.1	199	Responder	
Routes (8)	128.241.90.211	Packet Replay 3 <--> Berlin 192.168.4.1	284, 285, 286	Responder	
Routes (9)	204.194.237.136	Packet Replay 3 <--> Berlin 192.168.4.1	327	Responder	

This illustrates the routes that you could opt to manually configure instead of using the stream configuration tool.

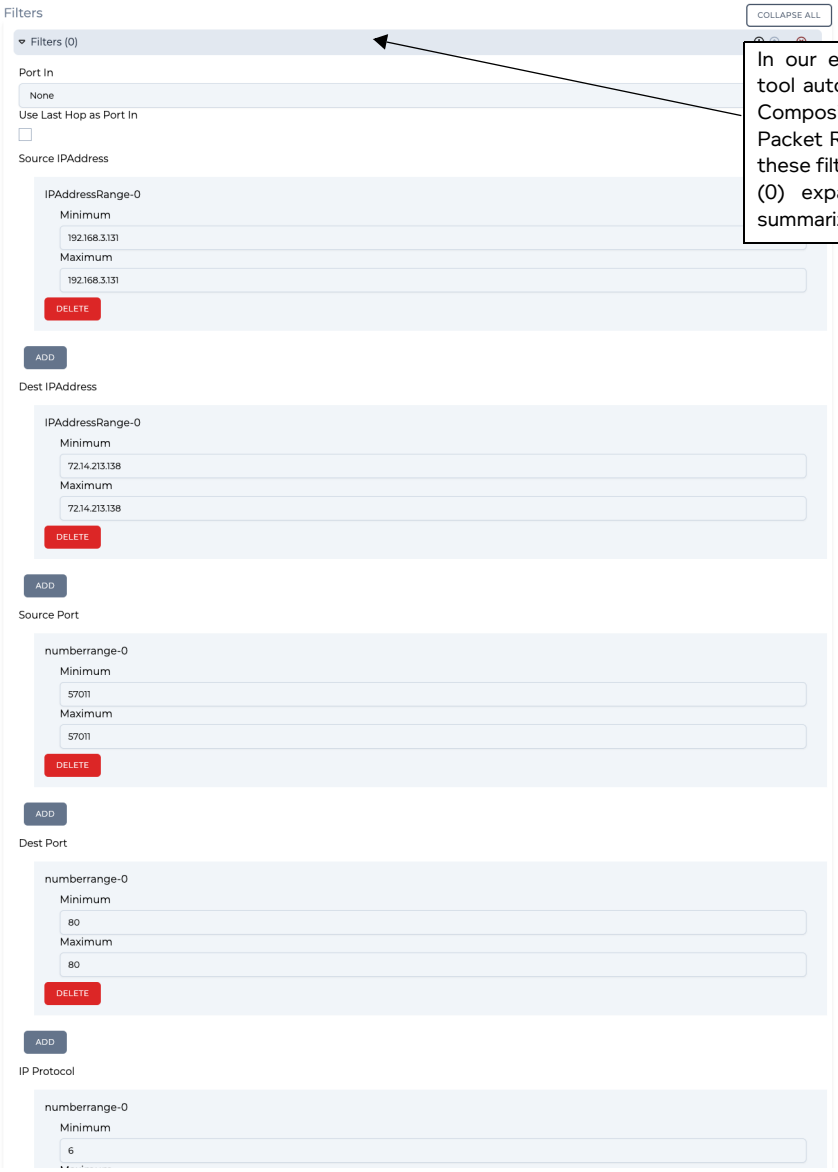
22. Although the configuration of Multi-Point network is finalized, it is interesting to observe the filters that were created by the stream configuration tool in the Composite Routing (Labs) function on the on the Packet Replay node. Observing these filters helps you understand how you could manually create these filters (if you choose to do so) instead of using the stream configuration tool. It also highlights the advantages of using the stream configuration tool opposed to manually creating the filters yourself.
    a. Click on the **Packet Replay3** node in the Workspace.
    b. From the **Edit node** panel that appears, click the **PROPERTIES** button.

c. The **Packet Replay3 - Advanced Node Properties** window appears, as shown below.



d. Click on the **Filters VIEW (20)** button.

A **Filters** window appears.



In our example, the stream configuration tool automatically created 20 filters in the Composite Routing (Labs) function on the Packet Replay node. If you were to expand these filters they would like similar to Filters (0) expanded here, with their settings summarized in *Table 78*.

If you were to expand and examine each of the filters, they would be as summarized in *Table 77*.

TABLE 78 - FILTERS THAT WERE AUTOMATICALLY GENERATED BY THE STREAM CONFIGURATION TOOL

Filter	Source IP Address max and min value	Destination IP Address max and min value	Source Port max and min value	Destination Port max and min value	IP Protocol max and min value	Corresponding to Stream Number
Filters (0)	192.168.3.131	72.14.213.138	57011	80	6	0
Filters (1)	72.14.213.138	192.168.3.131	80	57011	6	
Filters (2)	192.168.3.131	65.55.17.37	55954	80	6	4
Filters (3)	65.55.17.37	192.168.3.131	80	55954	6	
Filters (4)	192.168.3.131	65.55.5.232	55957	80	6	7
Filters (5)	65.55.5.232	192.168.3.131	80	55957	6	

Filter	Source IP Address max and min value	Destination IP Address max and min value	Source Port max and min value	Destination Port max and min value	IP Protocol max and min value	Corresponding to Stream Number
Filters (6)	192.168.3.131	65.55.5.231	55959	80	6	9
Filters (7)	65.55.5.231	192.168.3.131	80	55959	6	
Filters (8)	192.168.3.131	206.108.207.139	55960	80	6	10
Filters (9)	206.108.207.139	192.168.3.131	80	55960	6	
Filters (10)	172.16.255.1	204.9.163.158	10630	80	6	199
Filters (11)	204.9.163.158	172.16.255.1	80	10630	6	
Filters (12)	172.16.255.1	128.241.90.211	10653	80	6	284
Filters (13)	128.241.90.211	172.16.255.1	80	10653	6	
Filters (14)	172.16.255.1	128.241.90.211	10654	80	6	285
Filters (15)	128.241.90.211	172.16.255.1	80	10654	6	
Filters (16)	172.16.255.1	128.241.90.211	10655	80	6	286
Filters (17)	128.241.90.211	172.16.255.1	80	10655	6	
Filters (18)	172.16.255.1	204.194.237.136	10668	80	6	327
Filters (19)	204.194.237.136	172.16.255.1	80	10668	6	

This illustrates the filters that you could opt to manually configure instead of using the stream configuration tool.

This page is intentionally left blank.

CHAPTER 16 THE LCD PANEL

1. INTRODUCTION

In addition to the Web Interface, the NE-ONE Desktop (shown in *Illustration 219* or *Illustration 220*) also has an LCD panel on its front panel, providing quick access to the various operations.

Two versions of the LCD panel exist, as follows:

- V1 LCD Panel (*Illustration 219*) - corresponding to NE-ONE Desktop units manufactured up to the end of 2023
- V2 LCD Panel (*Illustration 220*) - corresponding to NE-ONE Desktop units manufactured from the start of 2024

ILLUSTRATION 219 - NE-ONE DESKTOP VERSION WITH V1 LCD PANEL

ILLUSTRATION 220 - NE-ONE DESKTOP VERSION WITH V2 LCD PANEL

If unlicensed the NE-ONE will boot-up as usual and allow you to access all of the menus. However the **Networks** menu item will not let you run any networks/scenarios until a valid license file is applied via the Web Interface. For more information on applying license files, see *Viewing and Applying License Files* on page 83 in *Chapter 4*, *Installation and Configuration*.

Note:

The LCD panel is only available on the NE-ONE Desktop version. In order to be able to run networks/scenarios from the LCD panel, the NE-ONE Desktop version has a special user called LCD. The LCD user is hidden from the Web Interface as it does not need to be managed like the admin and non-admin users of the Web Interface. The NE-ONE Desktop version has a special directory called `/Library/networks/LCD`, which is the location for copying any networks/scenarios that you want to run/stop via the LCD panel. In order to be able to run networks/scenarios from the LCD panel you must use the File Browser of the Web Interface to copy the appropriate networks/scenarios to the `/Library/networks/LCD` directory. If you are a non-admin user of the Web Interface and want to run/stop your networks/scenarios from the LCD panel you must communicate to an admin user of the Web Interface which networks/scenarios they must copy to the `/Library/networks/LCD` directory.

The operation and behavior of the LCD panel varies according to its version.

- If your NE-ONE Desktop has the V1 LCD panel, read the section *V1 LCD Panel Operation*.
- If your NE-ONE Desktop has the V1 LCD panel, read the section *V2 LCD Panel Operation*.

2. V1 LCD PANEL OPERATION

This section describes the operation of the V1 LCD panel operation. If your NE-ONE Desktop has the V2 LCD panel, see *V2 LCD Panel Operation* on page 710.

The V1 LCD panel on the front panel (shown in *Illustration 219*), provides quick access to the following operations:

- configuration of the Management port (see *Network Settings* on page 703)
- collecting diagnostic data and License/Version information (see *Support* on page 707)
- basic power management functions, such as:
  - Shutdown (see *Shutdown* on page 709)
  - Reboot (see *Reboot* on page 709)
- quick access to network/scenario specific functions such as:
  - starting/stopping networks/scenarios (see *Starting a Network or Scenario* on page 699)
  - querying active networks/scenarios (see *Querying and Stopping Active Networks and Scenarios* on page 702)

2-1. V1 LCD Panel Buttons

The LCD panel (see *Illustration 219*) has a 20 characters by 2 line dot-matrix display, with buttons whose functions are summarized in *Table 79*.

TABLE 79 - NE-ONE DESKTOP V1 LCD BUTTONS

Button Symbol	Button Function
F1	Abandon action and go to the previous menu (except when in the line editor). Go to the start of the line when in the line editor(*).
F2	When in the line editor (*) insert a character.
F3	When in the line editor (*) delete the character to left of the current position within the line.
F4	Abandon when in the line editor (*).
F5	Displays a context sensitive help page corresponding to the currently selected level within the LCD panel's menu hierarchy.
▲	Navigate up through the menus. Increase the character value of the currently selected character within the line editor (**).
▼	Navigate down through the menus. Decrease the character value of the currently selected character within the line editor (**).
OK	Select this menu, or perform (i.e. execute) this operation.
◀	Navigate back to previous level when within the menu hierarchy (normally). Navigate back one character when within the line editor (**). Abandon launch action and go to the top level menu when launching a network/scenario.
▶	Navigate forward one character within the line editor (**).
+	Increase the character value of the currently selected character within the line editor (**).
-	Decrease the character value of the currently selected character within the line editor (**).

Button Symbol	Button Function
⏻	Power on and boot-up or power down.
* - The line editor is active while editing the management port's Static IP Address parameters (i.e. IP address, Netmask, Gateway, Primary DNS server and Secondary DNS server). **- The currently selected character is highlighted with an underline and a solid flashing box.	

Note:
Depending on the current position within the menu structure, the buttons F2, F3, F4 and F5 may be either inactive (not illuminated) or active (illuminated). For example, the buttons F2, F3, and F4 are only active and illuminated when using the line editor for configuring the Management Port.

Note:
For clarity some of the illustrations in this section show more than two lines, although the V1 LCD panel can only show two lines at a time. You must scroll through the menu items using the ▲ and ▼ arrow buttons.

2-2. NE-ONE Initialization Messages on V1 LCD Panel

On powering up or rebooting, the following LCD panel messages appear.

```
System is starting.
Please wait...
```
followed by
```
Welcome to NE-ONE
```

Depending whether the Management port is setup for a static IP address or DHCP the following messages are displayed (in the examples below, the IP address is 192.168.202.57):

- If the Management port is set up with a static IP address, the messages like the following are displayed.

```
Welcome to NE-ONE
IP: 192.168.202.57
```
followed by
```
IP: 192.168.202.57
Type: STATIC
```

- If the Management port is set up with DCHP, and an IP address is successfully obtained from the DHCP server, the messages like the following are displayed (i.e. the obtained IP address is displayed).

```
Welcome to NE-ONE
IP: 192.168.202.57
```
followed by
```
IP: 192.168.202.57
Type: DHCP
```

- If the Management port is set up with DCHP, and an IP address is not successfully obtained from the DHCP server, the messages like the following are displayed.

```
Welcome to NE-ONE
IP:
```
followed by
```
IP: Unknown
Type: Unknown
```

- In the rare event that the NE-ONE failed to obtain any networking information when it attempted to obtain it (e.g. either static or DHCP could be set), the messages like the following are displayed.

```
Welcome to NE-ONE
IP:
```
followed by
```
IP: Unknown
Type: Unknown
```

Once the NE-ONE has booted, the Main Menu Help Page appears as described in *Initial Main Menu Help Page on V1 LCD Panel*.

2-3. Initial Main Menu Help Page on V1 LCD Panel

The Main Menu Help Page (*Illustration 221*) on the LCD panel appears once the NE-ONE has booted, and provides the entry point to the Main Menu. The Main Menu Help Page persists on the LCD panel until you press the **F1** button to display the Main Menu.

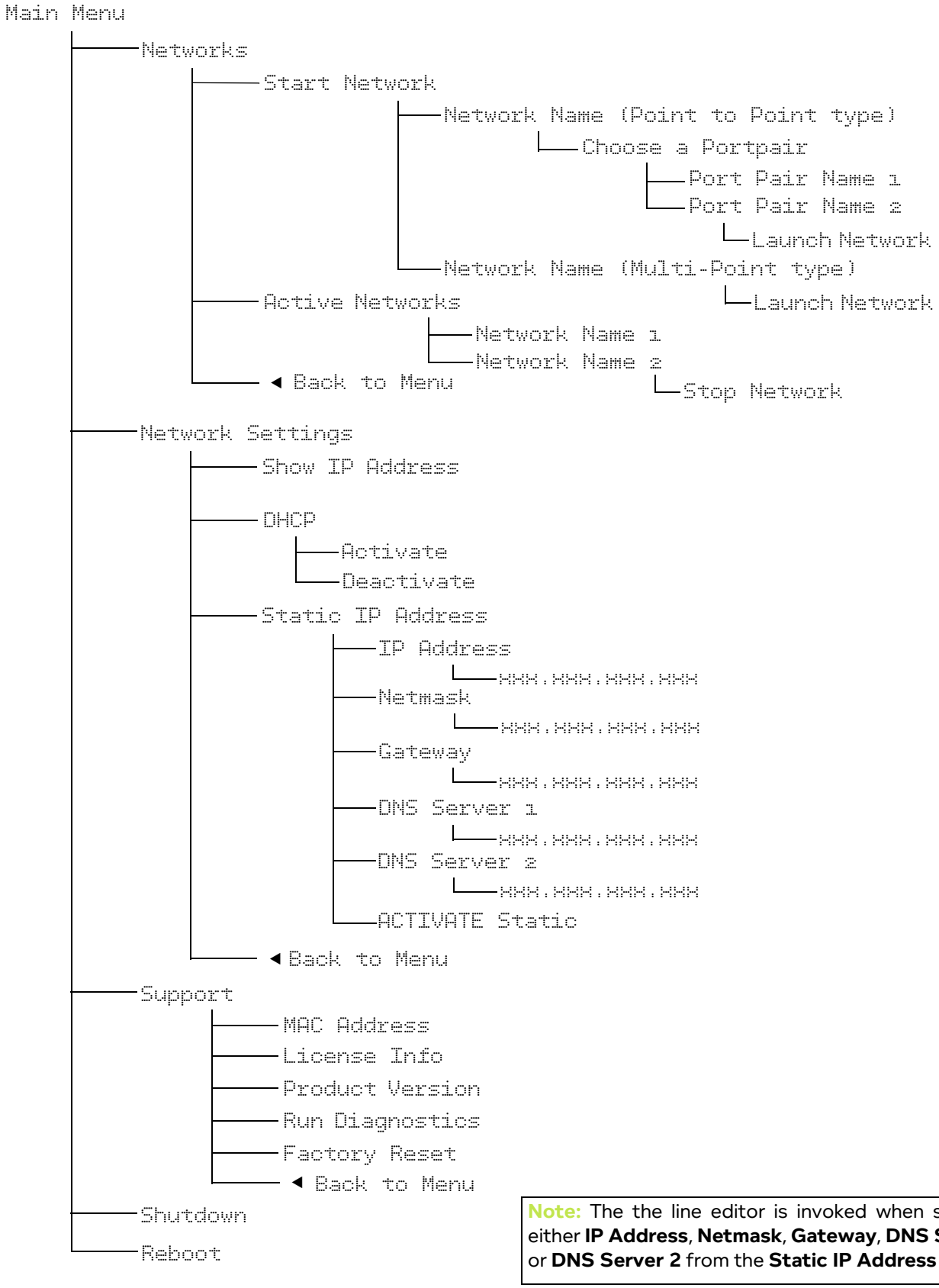
ILLUSTRATION 221 - LCD PANEL MAIN MENU HELP PAGE

Pressing the **F1** button results in displaying the Main Menu (*Illustration 223* on page 698), whose structure hierarchy is summarized in *Illustration 222* on page 697.

2-4. V1 LCD Panel Menu Hierarchy

The hierarchy of the LCD panel's Main Menu items are summarized in *Illustration 222* and described in the sections below.

ILLUSTRATION 222 - NE-ONE DESKTOP V1 LCD PANEL MAIN MENU HIERARCHY

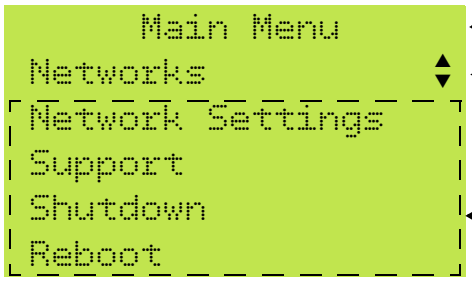


Note: The the line editor is invoked when selecting either **IP Address**, **Netmask**, **Gateway**, **DNS Server 1** or **DNS Server 2** from the **Static IP Address** menu.

2-5. V1 LCD Main Menu Items

All of the NE-ONE's operations are accessible from within the Main Menu (*Illustration 223*). The Main Menu is accessed by pressing the **F1** button at the initial Main Menu Help Page (*Illustration 221*) that appears after the NE-ONE has booted.

ILLUSTRATION 223 - LCD PANEL TOP MAIN MENU ITEMS

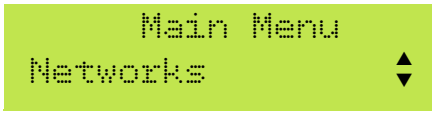


First line acts as the title of the currently selected menu item.
The second line shows the currently selected menu item. The ▲ character indicates that pressing the ▲ or ▼ down buttons will select the previous or next menu item at the current menu level, respectively.
Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

- Selecting **Networks**, and pressing the **OK** button results in displaying the network menu items. For more information, see *Networks* on page 698.
- Selecting **Network Settings**, and pressing the **OK** button results in displaying the network settings menu items. For more information, see *Network Settings* on page 703.
- Selecting **Support**, and pressing the **OK** button results in displaying the support menu items. For more information, see *Support* on page 707.
- Selecting **Shutdown**, and pressing the **OK** button results in immediately shutting down the NE-ONE. For more information, see *Shutdown* on page 709.
- Selecting **Reboot**, and pressing the **OK** button results in immediately rebooting the NE-ONE. For more information, see *Reboot* on page 709.

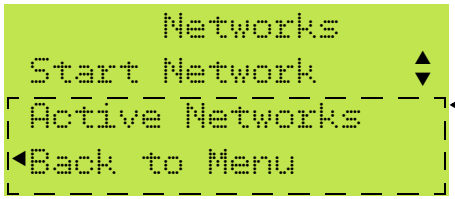
2-5-1. Networks

The **Networks** main menu item provides various options for starting and stopping networks and scenarios, and viewing their current run status.



Selecting the **Networks** main menu item, and pressing the **OK** button results in displaying the **Networks** menu items show in *Illustration 224*.

ILLUSTRATION 224 - NETWORKS MENU ITEMS

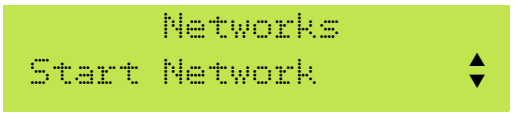


Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

- Selecting **Start Network**, and pressing the **OK** button results in drilling down one level in the menu hierarchy, from where you can select which network or scenario you want to start. For more information, see *Starting a Network or Scenario* on page 699.
- Selecting **Active Networks**, and pressing the **OK** button results in drilling down one level in the menu hierarchy, from where you can view and optionally stop any networks or scenarios. For more information, see *Querying and Stopping Active Networks and Scenarios* on page 702.
- Selecting **Back to Menu**, and pressing the **OK** button results in taking you back up one level to the Main Menu.

2-5-1-1. Starting a Network or Scenario

Selecting the **Start Network** networks menu item, and pressing the **OK** button results in displaying the all of the networks and scenarios that exist in the `/Library/networks/LCD` directory of the NE-ONE.



Note:

If the following message appears, the `/Library/networks/LCD` directory does not currently contain any network or scenario files.

In this case you must use the File Browser to copy the networks/scenarios from your `/Private/networks` directory to the `/Public/networks` directory. Then you must request an admin type user to copy the networks/scenarios from the `/Public/networks` directory to the `/Library/networks/LCD` directory. For more information, see *Making Networks and Scenarios Accessible to the LCD Panel* on page 596 in *Chapter 13*, *The File Browser*.

If networks and scenarios exist in the `/Library/networks/LCD` directory of the NE-ONE, the LCD panel appears like the following, with the selector icon (▶) on the first blank line.

You will need to move the selector icon (▶) down to the second line by pressing the ▼ button.

Then, to start a network/scenario, select the appropriate network/scenario name using the ▲ and ▼ buttons, and press the **OK** button.

Note:

The network/scenario name maybe truncated as the LCD panel can only display 20 characters in total on each of its two lines.

The NE-ONE Desktop version lets you run both Point-to-Point type and Multi-Point type networks/scenarios, and the description on how to start them are described in *Section 2-5-1-1-1* and *Section 2-5-1-1-2*, respectively.

2-5-1-1-1.Starting a Point-to-Point Network or Scenario

Note:

The LCD panel examples below are for a network called 5G_Slow_PoorQuality.

If you selected a Point-to-Point type network/scenario, the LCD panel temporarily shows the filename of the selected network/scenario.

The LCD panel then temporarily shows the following message before letting you choose over which port

pair the network/scenario should be run.

```
Choose a Portpair
```

The LCD panel then updates with a list of available port pairs, with the selector icon (▶) on the first line.

```
▶   Ports 0 & 1
    Ports 2 & 3 ▲▼
```

Select the appropriate port pair using the ▲ and ▼ buttons, and press the **OK** button (in the example below, the port pair called Ports 2 & 3 are selected).

```
    Ports 0 & 1
▶   Ports 2 & 3  ▲▼
```

Note:
The number of port pairs that are listed depend on how many port pairs are licensed NE-ONE Desktop model. All of the port pairs that are licensed are displayed (i.e. unlike a user of the Web Interface (where ports pairs are assigned to users). This is because all of the licensed port pairs are automatically assigned to the LCD user of the NE-ONE.

Note:
By default, on the NE-ONE Desktop model the port pairs are called Ports 0 & 1 and Ports 2 & 3. The name of port pairs that are listed depend what was given to them by an admin user of the Web Interface. If the default names of the port pairs were changed by the admin user, and have more than 18 characters, they will be truncated.

Note:
If the following message appears, it means that no port pairs exist the NE-ONE Desktop model. This may occur if the admin user has used the Port Manager feature to delete the default port pairs called Ports 0 & 1 and Ports 2 & 3. In this case, demand the admin user to re-create the port pairs.

```
Failed to get
Portpairs
```

Note:
If there is already a network/scenario running on one of the port pairs (for a two port pair licensed NE-ONE Desktop model) then the you are only offered the remaining port pair.

After selecting the port pair, the LCD panel displays a message like the following.

```
Launch Network: OK
Abandon: ◄ or F1  ▲▼
sG_Slow_PoorQuality.
On Portpair:
Ports 2 & 3
```

Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

- You can use the ▲ and ▼ buttons to scroll through the additional lines and review the selected Point-to-Point network/scenario filename and the selected port pair.
- To launch the selected Point-to-Point network/scenario on the selected port pair, press the **OK** button. In this case the LCD panel shows the following message temporarily before either showing a

success (Network Started) or error (Failed to start) message.

```
     Launching...
5G_Slow_PoorQuality.
```

- If no errors were encountered when attempting to launch the selected Point-to-Point network/scenario, the LCD panel displays a success message, like the following.

  ```
  Network started:
  id: <network id>
  ```

  Where <network id> is the numerical order in which the network/scenario is launched. For example, if no networks/scenario are currently running, the <network id> we be 1. Whereas, if one network/scenario is currently running, the <network id> we be 2, etc.

  One a network/scenario is running, the LCD panel remains at the **Network Started** page. You can use the ◀, **F1** and **OK** button to return to the **Networks** menu. If required, you can use the ◀ button to navigate back up to within the higher level menu items within the LCD panel's menu hierarchy.
- If errors were encountered when attempting to launch the selected Point-to-Point network/scenario, the LCD panel displays an appropriate error message, like the following.

  ```
  Failed to start:
  Error: <error code>
  ```

- To abandon launching the selected Point-to-Point network/scenario and return to the Main Menu, press either the ◀ or **F1** button. In this case the LCD panel shows the following message temporarily before returning to the Main Menu.

  ```
  Network Launch
  Abandoned
  ```

2-5-1-1-2.Starting a Multi-Point Network or Scenario

Note:
The LCD panel examples below are for a network called European_Mesh.

If you selected a Multi-Point type network/scenario, the LCD panel temporarily shows the filename of the selected network/scenario.

```
File Chosen:
European_Mesh.itn
```

After selecting the network/scenario, the LCD panel displays a message like the following.

```
Launch Network: OK
Abandon:◄  or F1  ▲▼
European_Mesh.itn
Type: Multi
```

Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

- You can use the ▲ and ▼ buttons to scroll through the additional lines and review the selected Multi-Point network/scenario filename.
- To launch the selected Multi-Point network/scenario, press the **OK** button. In this case the LCD panel shows the following message temporarily before either showing a success (Network Started) or error

(Failed to start) message.

```
Launching...
European_Mesh.itn
```

- If no errors were encountered when attempting to launch the selected Multi-Point network/scenario, the LCD panel displays a success message, like the following.

  ```
  Network started:
  id: <network id>
  ```

  Where <network id> is the numerical order in which the network/scenario is launched. For example, if no networks/scenario are currently running, the <network id> we be 1. Whereas, if one network/scenario is currently running, the <network id> we be 2, etc.

  One a network/scenario is running, the LCD panel remains at the **Network Started** page. You can use the ◀, **F1** and **OK** button to return to the **Networks** menu. If required, you can use the ◀ button to navigate back up to within the higher level menu items within the LCD panel's menu hierarchy.
- If errors were encountered when attempting to launch the selected Point-to-Point network/scenario, the LCD panel displays an appropriate error message, like the following.

  ```
  Failed to start:
  Error: <error code>
  ```

- To abandon launching the selected Multi-Point network/scenario and return to the **Network** menu, press either the ◀ or **F1** button. In this case the LCD panel shows the following message temporarily before returning to the **Network** menu.

  ```
  Network Launch
  Abandoned
  ```

2-5-1-2. Querying and Stopping Active Networks and Scenarios

The **Active Networks** networks menu item lets you view and optionally stop any active networks or scenarios that are running on the NE-ONE.

```
      Networks
Active Networks    ▲▼
```

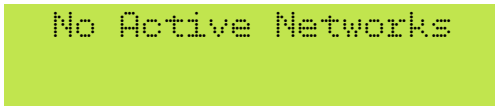
Selecting the **Active Networks** networks menu item, and pressing the **OK** button, results in the LCD panel displaying the following informational message temporarily, followed by a list the filenames of any active networks/scenarios.

```
  Active Networks
Sel using OK to stop
```

The example below shows the networks called WAN_10Mbps_PoorQuality and European_Mesh running, with the European_Mesh network currently selected.

```
  WAN_10Mbps_PoorQual
▸ European_Mesh.itn  ▲▼
```

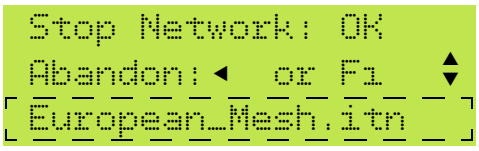
Note:
If no active networks/scenarios are running, the LCD panel displays the following message.



Note:
The network/scenario name maybe truncated as the LCD panel can only display 20 characters in total on each of its two lines.

To stop an active network/scenario, select the appropriate network/scenario name using the ▲ and ▼ buttons, and press the **OK** button.

After selecting the network/scenario, the LCD panel displays a message like the following.

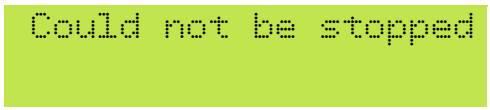


Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown. In this case, the third line which you can cycle to using the ▲ and ▼ buttons displays the filename of the currently selected network/scenario.

- To stop the selected network/scenario, press the **OK** button.
  - If no errors were encountered when attempting to stop the selected network/scenario, the LCD panel displays a success message, like the following.

    Where <network id> is the numerical order in which the network/scenario is launched. For example, if no networks/scenario are currently running, the <network id> we be 1. Whereas, if one network/scenario is currently running, the <network id> we be 2, etc.
  - If errors were encountered when attempting to stop the selected network/scenario, the LCD panel displays an appropriate error message, like the following.

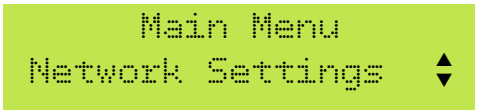
    

- To abandon stopping the selected network/scenario and return to the **Network** menu, press either the ◀ or **F1** button. In this case the LCD panel shows the following message temporarily before returning to the **Network** menu.

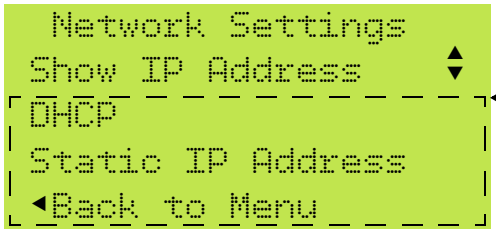
2-5-2. Network Settings

The **Network Settings** main menu item provides management for the NE-ONE's Management port network settings.



Selecting the **Network Settings** main menu item, and pressing the **OK** button results in displaying the network settings menu items show in *Illustration 225*.

ILLUSTRATION 225 - NETWORK SETTINGS MENU ITEMS

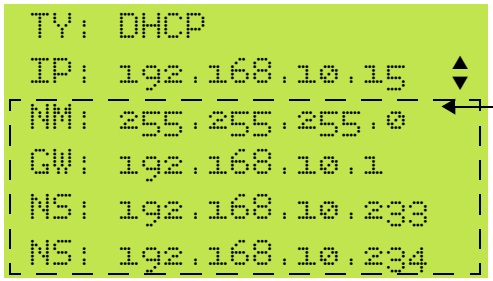


Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

- Selecting **Show IP Address**, and pressing the **OK** button results in drilling down one level in the menu hierarchy, from where you review the existing network settings of the Management Port. For more information, see *Show IP Address* on page 704.
- Selecting **DHCP**, and pressing the **OK** button results in drilling down one level in the menu hierarchy, from where you can configure the Management Port to use either DHCP or have a static IP address. For more information, see *DHCP* on page 705. If you set DCHP to Deactivate, then you must configure the Static IP Address.
- Selecting **Static IP Address**, and pressing the **OK** button results in drilling down one level in the menu hierarchy, from where you can configure the Management Port to use static IP address related settings. For more information, see *Static IP Address* on page 705.
- Selecting **Back to Menu**, and pressing the **OK** button results in taking you back up one level to the Main Menu.

2-5-2-1. Show IP Address

Selecting the **Show IP Address** network settings menu item, and pressing the **OK** button results in displaying the following for the Management port:



Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

Where:

- TY: indicates the way the IP address is obtained (i.e. Static if static is activated or DHCP if DHCP is activated).
- IP: indicates the current IP address.

Note:

If DHCP is activated and the NE-ONE fails to get an IP address from the DHCP server, an Automatic Private Internet Protocol (APIP) IP address of 169.254.15.101 will eventually be given.

- NM: indicates the current Netmask.
- GW: indicates the current Default Gateway.
- NS: indicates the current Primary DNS Server.
- NS: indicates the current Secondary DNS Server.

Note:

You cannot change the Management port IP address from using the **Show IP Address** item. To change the Management port IP address, select either use with the **DHCP** option (for a dynamically assigned IP address) or **Static IP Address** option (for a manually defined static IP address).

2-5-2-2. DHCP

By default, the NE-ONE is configured so that Management port obtains its address dynamically via DHCP, and DHCP is already activated. Use this section if you have configured that Management port to use a static address (i.e. static is activated), and if you want the Management port obtain its address dynamically via DHCP.

Selecting the **DHCP** network settings menu item, and pressing the **OK** button results in displaying the following the following confirmation message.

```
Network Settings
OK to Activate DHCP
```

- To abandon activating using a dynamic address for the Management Port, and return to the **Networks** menu, press either the ◀ or **F1** button.
- To confirm activating using a dynamic address for the Management Port, press the **OK** button.

  The LCD panel will then briefly display the messages like the following (if it successfully obtained an IP address from the DHCP server).

```
Network Settings
DHCP address set!
```

followed by

```
Network Settings
IP: 192.168.202.57
```

  When DHCP is activated, it usually obtains an IP address for the Management Port within 3 seconds. If the NE-ONE fails to get an IP address from the DHCP server it will keep trying, and after multiple failed attempts an Automatic Private Internet Protocol (APIP) IP address of 169.254.15.101 will eventually be given by the NE-ONE's operating system. In this case, resolve your network connectivity issues (i.e. check the NE-ONE Management port connections, DCHP server connections, etc.) then use the **Show IP Address** network settings menu item (see *Show IP Address* on page 704) to show the IP address obtained from the DHCP server.

  The updated setting will then be committed to the NE-ONE's Management Port, and the LCD panel returns to the **Network** menu. The NE-ONE Management port will now use DHCP to dynamically obtain its address.

2-5-2-3. Static IP Address

By default, the NE-ONE is configured so that Management port obtains its address setting vi DHCP. Use this section if you want the NE-ONE Management port to use a static address instead a dynamic address.

Selecting the **Static IP Address** item from the network settings menu results in displaying the following **Static Address** menu items, which allow you to configure each of the static IP Address related parameters for the Management port.

```
Static Address
IP Address
Netmask
Gateway
DNS Server 1
DNS Server 2
ACTIVATE Static
```

Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

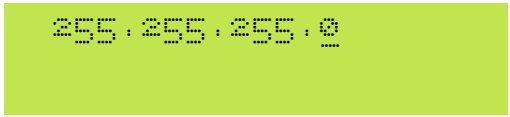
Note:

If the NE-ONE was previously configured to use DHCP and connected to the network with a DHCP server, the previously obtained management port values obtained via the DHCP server will be inherited into the static address settings. You can leverage this functionality to pre-populate the static address settings via DHCP, then edit the static address settings according to your requirements.

To configure the Management port's static address, you must select each of the following parameters using the ▲ and ▼ buttons and press the **OK** button in order to configure that parameter:

- **IP Address** - configures the static IP address of the Management port. If you want the Management port to use a static address you must configure this parameter.
- **Netmask** - configures the Netmask of the Management port. If you want the Management port to use a static address you must configure this parameter.
- **Gateway** - configures the address of the Gateway used by the Management port. This parameter is optional. If you want the Management port to have Internet access, you must configure this parameter.
- **DNS Server 1** - configures the address of the Primary DNS Server used by the Management port. This parameter is optional. If you want the Management port to have Internet access, you must configure this parameter.
- **DNS Server 2** - configures the address of the Secondary DNS Server used by the Management port. This parameter is optional.

Upon pressing the **OK** button for the selected parameter, results in the line editor appearing with the existing value of the selected parameter. In the example below, the line editor is being used to specify the Netmask 255.255.255.0.



Note:

When in the line editor, the currently selected character is highlighted with an underline, and a solid flashing box. In the example above, the 0 from the Netmask 255.255.255.0 is the currently selected character.

When you are in the line editor for the selected parameter, use the buttons on the front panel of the NE-ONE accordingly in order to configure that parameter:

- Press the ▶ button to move one character right within the line.
- Press the ◀ button to move one character left within the line.
- Press the **F1** button to return to the start of the line.
- Press the **F2** to insert a character at the current position within the line.
- Press the **F3** to delete the character to left of the current position within the line.
  Press the **F4** button to abandon the current line editor.
- F5 display help.
- Press the **+** button or ▲ button to change the value of the currently selected character to the next value (i.e. increase the numeric value from 1 to 2).
- Press the **-** button or ▼ button to change the value of the currently selected character to the previous value (i.e. decrease the numeric value from 2 to 1).
- Press the **OK** button to commit the existing parameter, and return to the Static IP Address menu items.

Note:

Once finalizing a parameter and committing, the NE-ONE will perform a validation check. If you made an error with the format, you will be prompted to correct the parameter.

Once you have defined each of the parameters select the **ACTIVATE Static** item and press the **OK** button. The LCD panel will then display the following confirmation message.

```
Static Address
OK to activate.
```

- To confirm activating using a static address for the parameters you defined, and return to the **Static Address** menu, press either the ◀ or **F1** button.
- To confirm activating using a static address for the parameters you defined, press the **OK** button.

  The LCD panel will then briefly display the following messages.

```
Static Address
Activating...
```

followed by

```
Static Address
Static address set!
```

The updated parameters will then be committed to the NE-ONE's Management Port, and the LCD panel returns to the **Static Address** menu. The NE-ONE Management port will now use a static address with the parameters that you defined.

Note:

The changes you make are only committed if you remain within the session of the **Static IP Address** item. For example, if you have made changes to any of the parameters, but have not selected the **ACTIVATE Static** item, the changes will not be committed to the NE-ONE's Management Port. Before navigating out of the **Static IP Address** item, ensure you select the **ACTIVATE Static** item and press the **OK** if you want the parameters to be committed.

2-5-3. Support

The **Support** main menu item provides some management and licensing actions on the NE-ONE.

```
Main Menu
Support                    ▲▼
```

Selecting the **Support** main menu item, and pressing the **OK** button results in displaying the support menu items show in *Illustration 226*.

ILLUSTRATION 226 - SUPPORT MENU ITEMS

```
Support
MAC Address                ▲▼
License Info
Product Version
Run Diagnostics
Factory Reset
```

Note: Only two lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

These support menu items are described in the sub-sections 2-5-3-1 to 2-5-3-5 below.

2-5-3-1. MAC Address

Selecting the **MAC Address** support menu item, and pressing the **OK** button results in displaying the

MAC address of the NE-ONE's Management port.

```
MM:MM:MM:MM:MM:MM
```

The license file used to license the NE-ONE is associated with this MAC address. When requesting a license file for your NE-ONE you must provide Calnex with this MAC address.

2-5-3-2. License Info

The **License Info** support menu item lets you view the license information of the NE-ONE.

```
    Support
License Info      ▲▼
```

Selecting the **License Info** support menu item, and pressing the **OK** button results in displaying the expiry date of the license file used to license the NE-ONE.

```
Prd: <product code>
Exp: YYYY-MM-DD
```

- If the license file has an expiry date (i.e. non-perpetual license) then the expiry date will be displayed in YYYY-MM-DD format.
- If the license file does not have an expiry date (i.e. perpetual license) then the expiry date will be displayed as follows.

```
Prd: <product code>
Exp: Permanent
```

2-5-3-3. Product Version

The **Product Version** support menu item lets you view the product version of the NE-ONE.

```
    Support
Product Version   ▲▼
```

Selecting the **Product Version** support menu item, and pressing the **OK** button results in displaying the NE-ONE's application code version and the application model/type.

```
Ver: <version>
Bld: <build>
```

2-5-3-4. Run Diagnostics

The **Run Diagnostics** support menu item provides you with high level instructions on how to perform a factory reset the NE-ONE.

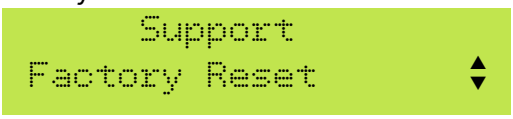
```
    Support
Run Diagnostics   ▲▼
```

Selecting the **Run Diagnostics** support menu item, and pressing the **OK** button results in displaying the following informational message (where the term GUI is referring to the Web Interface procedure (see

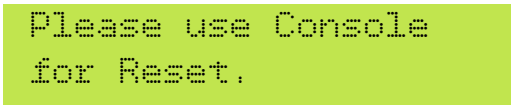
Running Diagnostics on page 226)).

2-5-3-5. Factory Reset

The **Factory Reset** support menu item provides you with high level instructions on how to perform a factory reset the NE-ONE.



Selecting the **Factory Reset** support menu item, and pressing the **OK** button results in displaying the following informational message.

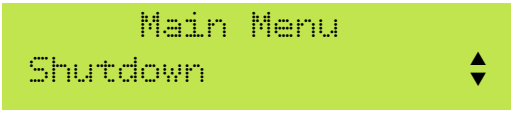


Note:

You will need to use the NE-ONE command line in order to perform a factory reset. For more information, contact your Calnex support representative or Calnex support.

2-5-4. Shutdown

The **Shutdown** main menu item lets you shut down the NE-ONE.



Selecting the **Shutdown** main menu item, and pressing the **OK** button results in immediately shutting down the NE-ONE.

! Notice:

No confirmation message appears. The NE-ONE will immediately start the graceful shutdown sequence after pressing the **OK** button. Shutting down an active NE-ONE will terminate all running networks/scenarios and all unsaved networks/scenarios will be lost.

2-5-5. Reboot

The **Reboot** main menu item lets you reboot the NE-ONE.

Selecting the **Reboot** main menu item, and pressing the **OK** button results in immediately rebooting the NE-ONE.

! Notice:

No confirmation message appears. The NE-ONE will immediately start the reboot sequence after pressing the **OK** button. Rebooting an active NE-ONE will terminate all running networks/scenarios and all unsaved networks/scenarios will be lost.

3. V2 LCD PANEL OPERATION

This section describes the operation of the V2 LCD panel operation. If your NE-ONE Desktop has the V1 LCD panel, see *V1 LCD Panel Operation* on page 694. The V2 LCD panel on the front panel (shown in *Illustration 220* on page 693), provides quick access to the following operations:

- configuration of the Management port (see *Network Settings* on page 719)
- viewing product license/version information, and more (see *Product Info* on page 725)
- basic power management functions, such as:
  - Shutdown (see *Shutdown* on page 728)
  - Reboot (see *Reboot* on page 729)
- quick access to network/scenario specific functions such as:
  - starting/stopping networks/scenarios (see *Starting a Network or Scenario* on page 714)
  - querying active networks/scenarios (see *Querying and Stopping Active Networks and Scenarios* on page 718)

3-1. V2 LCD Panel Buttons

The V2 LCD panel (see *Illustration 220* on page 693) has a 20 characters by 4 line dot-matrix display, with buttons whose functions are summarized in *Table 80*.

TABLE 80 - NE-ONE DESKTOP V2 LCD BUTTONS

Button Symbol	Button Function
Top Left 	Displays a context sensitive help page corresponding to the currently selected level within the LCD panel's menu hierarchy. When within the line editor (*), enables ALT mode.
Bottom Left 	Abandon action and go to the previous menu. When within the ALT mode of the line editor (*), exits ALT mode, and returns you back to the line editor.
▲	Navigate up through the menus. Increase the character value of the currently selected character within the line editor (**). When in ALT mode of the line editor, inserts a character at the currently selected character.
▼	Navigate down through the menus. Decrease the character value of the currently selected character within the line editor (**). When in ALT mode of the line editor (*), deletes the currently selected character.
OK 	Select this menu item, or perform (i.e. confirm) this operation.
◀	Navigate back one character when within the line editor (**).
▶	Navigate forward one character within the line editor (**). **Note:** if you advance the character position further than the last character, a new character is added with the default value of 0.
⏻	Power on and boot-up or power down.
* - The line editor is active while editing the management port's Static IP Address parameters (i.e. IP address, Netmask, Gateway, Primary DNS server and Secondary DNS server). **- The currently selected character is highlighted with a ^ symbol.	

Note:

For clarity some of the illustrations in this section show more than four lines, although the V2 LCD panel can only show four lines at a time. You must scroll through the menu items using the ▲ and ▼ arrow buttons.

3-2. V2 LCD Panel Indicator LEDs

To the left of the LCD panel (see *Illustration 220* on page 693) are three indicator LEDs. All three indicator LEDs act in the same way, with the following states:

- Green : Ready, waiting for input.
- Yellow : Processing (e.g. starting a network, updating settings, etc.)
- Red : When there is an error message.

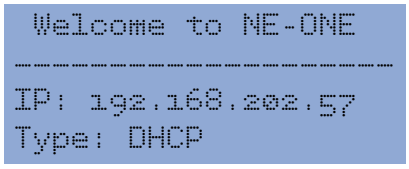
3-3. NE-ONE Initialization Messages on V2 LCD Panel

On powering up or rebooting, the following LCD panel messages appear.

Depending whether the Management port is setup for a static IP address or DHCP the following messages are displayed (in the examples below, the IP address is 192.168.202.57):

- If the Management port is set up with a static IP address, a welcome message like the following appears.

- If the Management port is set up with DCHP, and an IP address is successfully obtained from the DHCP server, a welcome message like the following appears (with the obtained IP address).



- If the Management port is set up with DCHP, and an IP address is not successfully obtained from the DHCP server, a welcome message like the following appears.

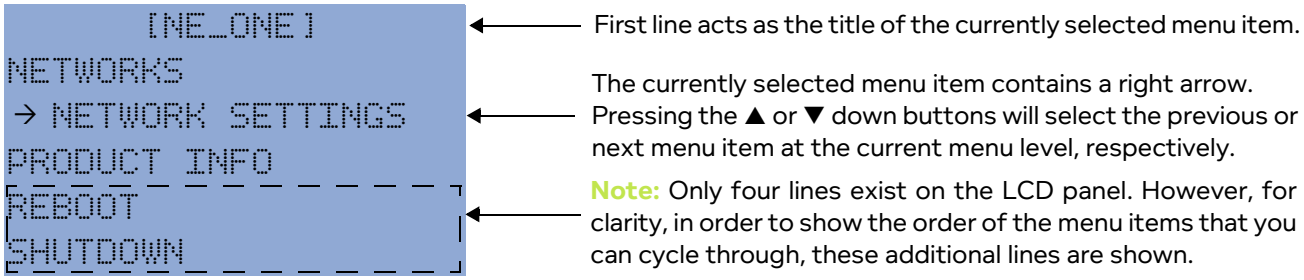
- In the rare event that the NE-ONE failed to obtain any networking information when it attempted to obtain it (e.g. either static or DHCP could be set), a welcome message like the following appears.

The welcome page remains present for 4.5 seconds, then once the NE-ONE has fully booted, the Main Menu Page appears as described in *Main Menu Page on V2 LCD Panel*.

3-4. Main Menu Page on V2 LCD Panel

The Main Menu page (*Illustration 227*) on the LCD panel appears once the NE-ONE has fully booted, and provides the entry point to all of the NE-ONE's operations. The Main Menu page has the menu structure hierarchy as summarized in *Illustration 228* on page 713.

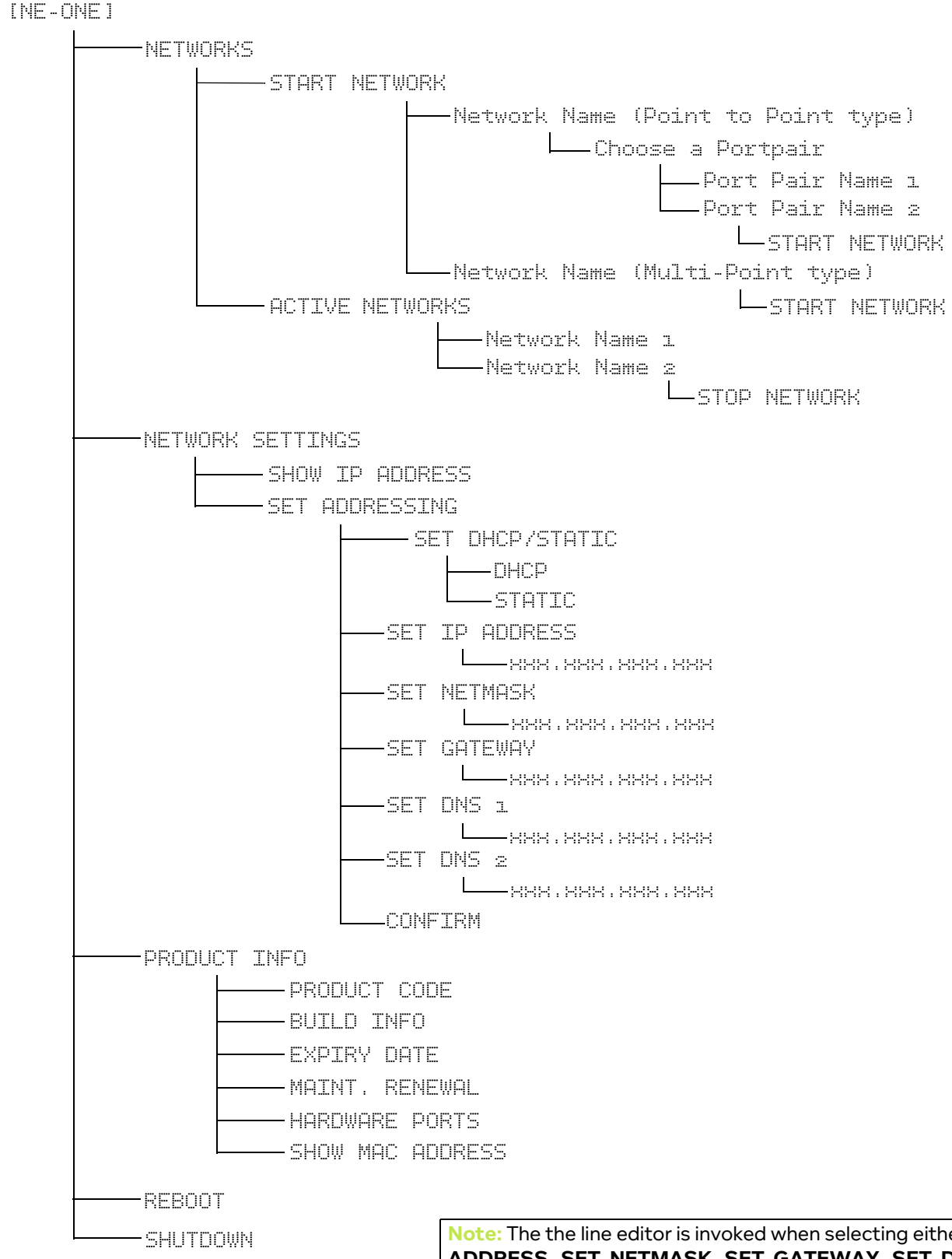
ILLUSTRATION 227 - V2 LCD PANEL MAIN MENU ITEMS



3-5. V2 LCD Panel Menu Hierarchy

The hierarchy of the LCD panel's Main Menu items are summarized in *Illustration 228* and described in the sections below.

ILLUSTRATION 228 - NE-ONE DESKTOP V2 LCD PANEL MAIN MENU HIERARCHY



Note: The the line editor is invoked when selecting either **SET IP ADDRESS**, **SET NETMASK**, **SET GATEWAY**, **SET DNS 1** or **SET DNS 2** from the **SET IP ADDRESS** menu.

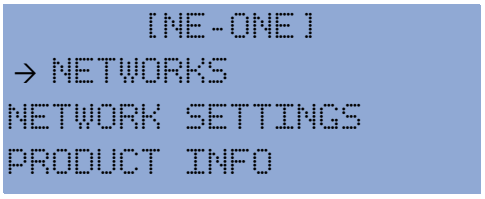
3-6. V2 LCD Main Menu Items

All of the NE-ONE's operations are accessible from within the Main Menu (*Illustration 227* on page 712).

- Selecting **NETWORKS**, and pressing the **OK** button results in displaying the network menu items. For more information, see *Networks* on page 714.
- Selecting **NETWORK SETTINGS**, and pressing the **OK** button results in displaying the network settings menu items. For more information, see *Network Settings* on page 719.
- Selecting **PRODUCT INFO**, and pressing the **OK** button results in displaying the product information menu items. For more information, see *Product Info* on page 725.
- Selecting **SHUTDOWN**, and pressing the **OK** button results in shutting down the NE-ONE. For more information, see *Shutdown* on page 728.
- Selecting **REBOOT**, and pressing the **OK** button results in rebooting the NE-ONE. For more information, see *Reboot* on page 729.

3-6-1. Networks

The **NETWORKS** main menu item provides various options for starting and stopping networks and scenarios, and viewing their current run status.



Selecting the **NETWORKS** main menu item, and pressing the **OK** button results in displaying the **NETWORKS** menu items show in *Illustration 229*.

ILLUSTRATION 229 - NETWORKS MENU ITEMS

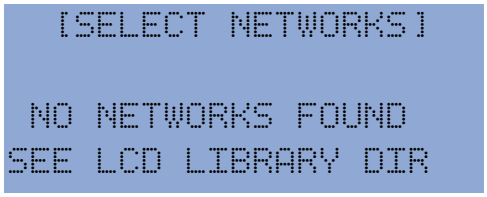
- Selecting **START NETWORK**, and pressing the **OK** button results in drilling down one level in the menu hierarchy, from where you can select which network or scenario you want to start. For more information, see *Starting a Network or Scenario* on page 714.
- Selecting **ACTIVE NETWORKS**, and pressing the **OK** button results in drilling down one level in the menu hierarchy, from where you can view and optionally stop any networks or scenarios. For more information, see *Querying and Stopping Active Networks and Scenarios* on page 718.

3-6-1-1. Starting a Network or Scenario

Selecting the **START NETWORK** networks menu item, and pressing the **OK** button results in displaying the all of the networks and scenarios that exist in the `/Library/networks/LCD` directory of the NE-ONE.

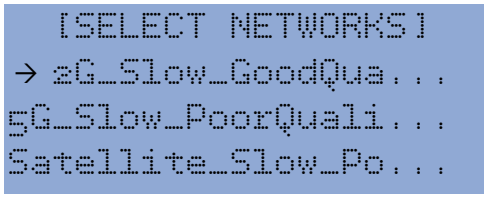
Note:

If the following message appears, the `/Library/networks/LCD` directory does not currently contain any network or scenario files.



In this case you must use the File Browser to copy the networks/scenarios from your `/Private/networks` directory to the `/Public/networks` directory. Then you must request an admin type user to copy the networks/scenarios from the `/Public/networks` directory to the `/Library/networks/LCD` directory. For more information, see *Making Networks and Scenarios Accessible to the LCD Panel* on page 596 in *Chapter 13*, *The File Browser*.

If networks and scenarios exist in the `/Library/networks/LCD` directory of the NE-ONE, the LCD panel appears like the following, with the selector arrow (→) on the first of the listed networks/scenarios.



Then, to start a network/scenario, select the appropriate network/scenario name using the ▲ and ▼ buttons, and press the **OK** button.

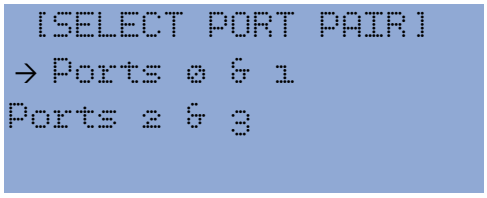
Note:

The network/scenario name maybe truncated as the LCD panel can only display 20 characters in total on each of its two lines.

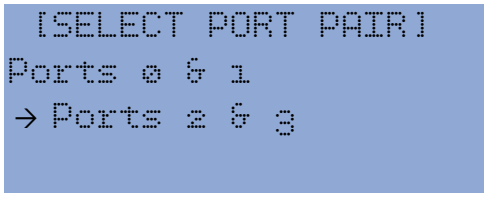
The NE-ONE Desktop version lets you run both Point-to-Point type and Multi-Point type networks/scenarios, and the description on how to start them are described in *Section 3-6-1-1-1* and *Section 3-6-1-1-2*, respectively.

3-6-1-1-1.Starting a Point-to-Point Network or Scenario

If you selected a Point-to-Point type network/scenario, the LCD panel shows the **SELECT PORT PAIR** menu for the selected network/scenario.



Select the appropriate port pair using the ▲ and ▼ buttons, and press the **OK** button (in the example below, the port pair called Ports 2 & 3 are selected).



Note:
The number of port pairs that are listed depend on how many port pairs are licensed NE-ONE Desktop model. All of the port pairs that are licensed are displayed (i.e. unlike a user of the Web Interface (where ports pairs are assigned to users). This is because all of the licensed port pairs are automatically assigned to the LCD user of the NE-ONE.

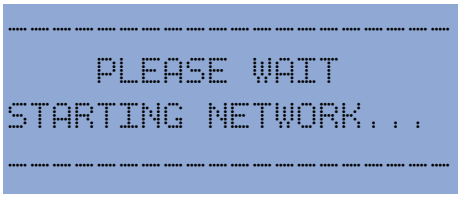
Note:
By default, on the NE-ONE Desktop model the port pairs are called Ports 0 & 1 and Ports 2 & 3. The name of port pairs that are listed depend what was given to them by an admin user of the Web Interface. If the default names of the port pairs were changed by the admin user, and have more than 18 characters, they will be truncated.

Note:
If the following message appears, it means that no port pairs exist the NE-ONE Desktop model. This may occur if the admin user has used the Port Manager feature to delete the default port pairs called Ports 0 & 1 and Ports 2 & 3. In this case, demand the admin user to re-create the port pairs.

Note:
If there is already a network/scenario running on one of the port pairs (for a two port pair licensed NE-ONE Desktop model) then the you are only offered the remaining port pair.

After selecting the port pair, the LCD panel displays the following confirmation message.

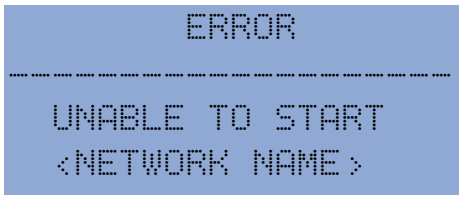
- You can use the ▲ and ▼ buttons to scroll between **YES** and **NO** to confirm or cancel starting the network/scenario, respectively.
- To start the selected Point-to-Point network/scenario on the selected port pair, select **YES** and press the **OK** button. In this case the LCD panel shows the following message temporarily before either showing a success (Network Started) or error (Failed to start) message.



  - If no errors were encountered when attempting to start the selected Point-to-Point network/scenario, the LCD panel displays the following success message.

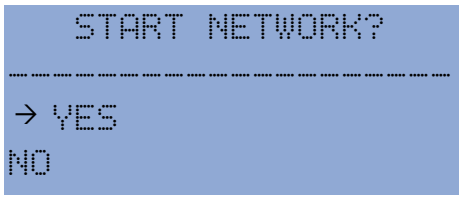
One a network/scenario is running, the LCD panel returns to the **NETWORKS** page (*Illustration 229* on page 714).

- If errors were encountered when attempting to start the selected Point-to-Point network/scenario, the LCD panel displays an error message, like the following (where **<NETWORK NAME>** is the name of the network/scenario that you attempted to start).



3-6-1-1-2.Starting a Multi-Point Network or Scenario

If you selected a Multi-Point type network/scenario, the LCD directly displays the following confirmation message.



- You can use the ▲ and ▼ buttons to scroll between **YES** and **NO** to confirm or cancel starting the network/scenario, respectively.
- To start the selected Multi-Point network/scenario, select **YES** and press the **OK** button. In this case the LCD panel shows the following message temporarily before either showing a success (Network Started) or error (Failed to start) message.

- If no errors were encountered when attempting to start the selected Multi-Point network/scenario, the LCD panel display the following success message.

One a network/scenario is started, the LCD panel returns to the **NETWORKS** page (*Illustration 229* on page 714).

- If errors were encountered when attempting to start the selected Multi-Point network/scenario, the LCD panel displays an error message, like the following (where **<NETWORK NAME>** is the

name of the network/scenario that you attempted to start).

```
        ERROR
--------------------
UNABLE TO START
<NETWORK NAME>
```

- To abandon starting the selected network/scenario and return to the **NETWORKS** page (*Illustration 229* on page 714), either press the **Back** button or select **NO** and press the **OK** button.

3-6-1-2. Querying and Stopping Active Networks and Scenarios

The **ACTIVE NETWORKS** networks menu item lets you view and optionally stop any active networks or scenarios that are running on the NE-ONE.

```
     [NETWORKS]
  START NETWORK
→ ACTIVE NETWORKS
```

Selecting the **ACTIVE NETWORKS** networks menu item, and pressing the **OK** button, results in the LCD panel displaying the **ACTIVE NETWORKS** page. If any networks/scenarios are active they are listed.

```
 [ACTIVE NETWORKS]
→ 2G_Slow_GoodQua...
5G_Slow_PoorQuali...
```

The example above shows the networks called 2G_Slow_GoodQuality and 5G_Slow_PoorQuality running, with the 2G_Slow_GoodQuality network currently selected.

Note:

If no active networks/scenarios are active, the LCD panel displays the following message.

```
  [ACTIVE NETWORKS]

 NO ACTIVE NETWORKS
```

Note:

The network/scenario name maybe truncated as the LCD panel can only display 20 characters in total on each of its two lines.

To stop an active network/scenario, select the appropriate network/scenario name using the ▲ and ▼ buttons, and press the **OK** button.

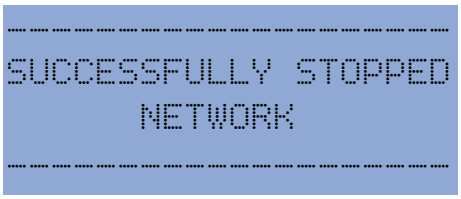
After selecting the network/scenario, the LCD panel displays the following confirmation message.

```
   STOP NETWORK?
--------------------
→ YES
NO
```

- To stop the selected network/scenario select **YES**, then press the **OK** button. In this case the LCD

panel shows the following message temporarily before either showing a success (Network Stopped) or error (Failed to stop) message.

- If no errors were encountered when attempting to stop the selected network/scenario, the LCD panel displays the following success message.



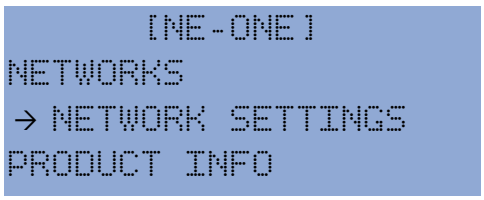
One a network/scenario is stopped, the LCD panel returns to the **NETWORKS** page (*Illustration 229* on page 714).

- If errors were encountered when attempting to stop the selected network/scenario, the LCD panel displays an error message, like the following (where **<NETWORK NAME>** is the name of the network/scenario that you attempted to stop).

- To abandon stopping the selected network/scenario and return to the **NETWORKS** page (*Illustration 229* on page 714), either press the **Back** button or select **NO** and press the **OK** button.

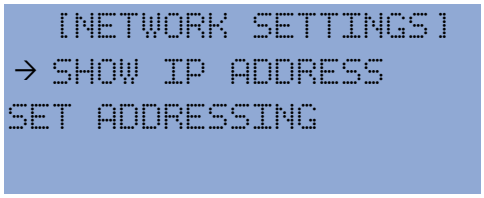
3-6-2. Network Settings

The **NETWORK SETTINGS** main menu item provides management for the NE-ONE's Management port network settings.



Selecting the **NETWORK SETTINGS** main menu item, and pressing the **OK** button results in displaying the network settings menu items show in *Illustration 230*.

ILLUSTRATION 230 - NETWORK SETTINGS MENU ITEMS



- Selecting **SHOW IP ADDRESS**, and pressing the **OK** button results in drilling down one level in the menu hierarchy to the **IP ADDRESS** page, from where you review the existing network settings of the

Management Port. For more information, see *Show IP Address* on page 704.

- Selecting **SET ADDRESSING**, and pressing the **OK** button results in drilling down one level in the menu hierarchy to the **SET ADDRESSING** page, from where you can configure the Management port to use on of the following:
  - dynamically assigned IP address (see *Configuring a dynamic IP Address via DHCP* on page 720)
  - statically configured IP address (*Configuring a Static IP Address* on page 722)

3-6-2-1. Show IP Address

Selecting the **SHOW IP ADDRESS** network settings menu item, and pressing the **OK** button results in displaying the IP address Management port, and whether it is dynamically assigned via DHCP or statically defined.

or

Note:
If DHCP is activated and the NE-ONE fails to get an IP address from the DHCP server, an Automatic Private Internet Protocol (APIP) IP address of 169.254.15.101 will eventually be given.

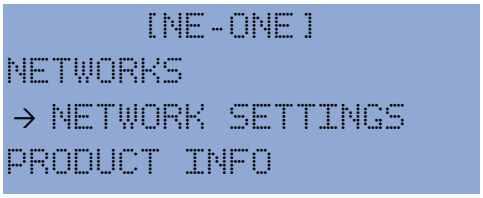
Note:
You cannot change the Management port IP address from using the **SHOW IP ADDRESS** menu item. To change the Management port IP address, use with the **SET ADDRESSING** menu item, and to configure either the **DHCP** option (for a dynamically assigned IP address) or **Static IP Address** option (for a manually defined static IP address). For more information, see *Configuring a dynamic IP Address via DHCP* on page 720 and *Configuring a Static IP Address* on page 722.

3-6-2-2. Configuring a dynamic IP Address via DHCP

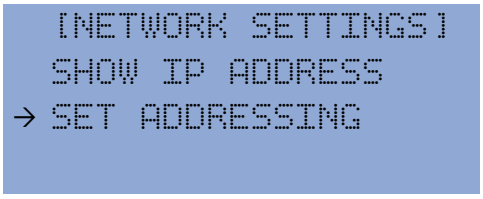
By default, the NE-ONE is configured so that Management port obtains its address dynamically via DHCP, and DHCP is already activated. Use this section if you have configured that Management port to use a static address (i.e. static is activated), and if you want the Management port obtain its address dynamically via DHCP.

To configure the Management port to obtain its IP Address dynamically, do the following:

1. Select **NETWORK SETTINGS** main menu item, and press the **OK** button.

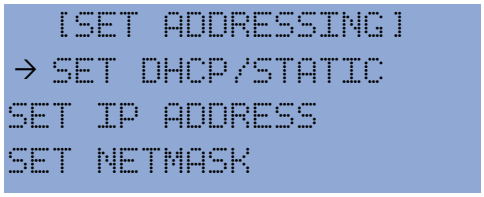


2. From the **NETWORK SETTINGS** page, select the **SET ADDRESSING** network settings menu item, and press the **OK** button.



3. From the **SET ADDRESSING** page, select the **SET DHCP/STATIC** network settings menu item, and

press the **OK** button.

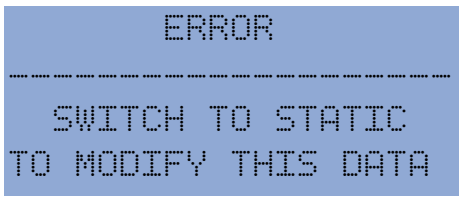


4. From the **DHCP/STATIC** page that appears, select **DHCP** and press the **OK** button.

DHCP mode is set, and you are returned up one level to the **SET ADDRESSING** page.

Note:

Once DHCP is set, if you attempt to select **SET IP ADDRESS**, **SET NETMASK**, **SET GATEWAY**, **SET DNS 1**, or **SET DNS 2**, an error message appears informing you that this setting is not possible in DHCP mode. This is normal as these settings can only be changed when in static mode.



5. Use the ▼ button to scroll down and select **CONFIRM** and the press the **OK** button.

You are returned up one level to the **NETWORK SETTINGS** page, and updated setting is committed to the NE-ONE's Management Port. The NE-ONE Management port will now use DHCP to dynamically obtain its address.

Note:

The changes you make are only committed if you remain within the session of the **SET ADDRESSING** page. For example, if you have made changes to any of the parameters, but have not selected the **CONFIRM** menu item, the changes will not be committed to the NE-ONE's Management Port. Before navigating out of the **SET ADDRESSING** page, ensure you select the **CONFIRM** menu item and press the **OK** if you want the parameters to be committed.

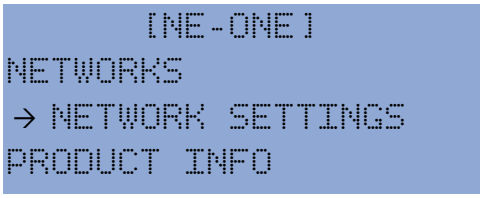
When DHCP is activated, the NE-ONE usually obtains an IP address for the Management Port within 3 seconds. If the NE-ONE fails to get an IP address from the DHCP server it will keep trying, and after multiple failed attempts an Automatic Private Internet Protocol (APIP) IP address of 169.254.15.101 will eventually be given by the NE-ONE's operating system. In this case, resolve your network connectivity issues (i.e. check the NE-ONE Management port connections, DCHP server connections, etc.) then use the **SHOW IP ADDRESS** network settings menu item (see *Show IP Address* on page 720) to show the IP address obtained from the DHCP server.

3-6-2-3. Configuring a Static IP Address

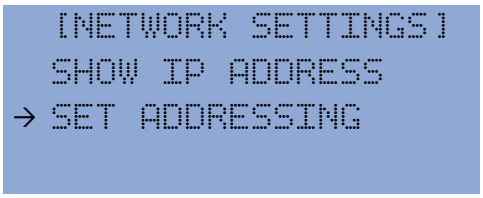
By default, the NE-ONE is configured so that Management port obtains its address setting via DHCP. Use this section if you want the NE-ONE Management port to use a static address instead a dynamic address.

To configure the Management port with a static IP Address, do the following:

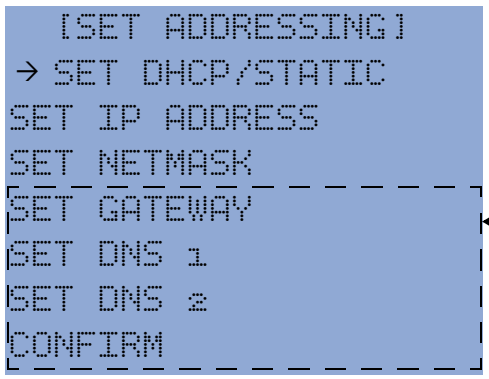
1. Select **NETWORK SETTINGS** main menu item, and press the **OK** button.



2. From the **NETWORK SETTINGS** page, select the **SET ADDRESSING** network settings menu item, and press the **OK** button.



3. From the **SET ADDRESSING** page, select the **SET DHCP/STATIC** network settings menu item, and press the **OK** button.



Note: Only four lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

4. From the **DHCP/STATIC** page that appears, select **STATIC** and press the **OK** button.

Static mode is set, and you are returned up one level to the **SET ADDRESSING** page.

Note:

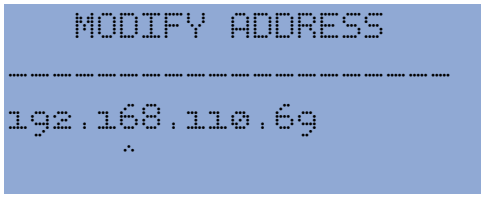
If the NE-ONE was previously configured to use DHCP and connected to the network with a DHCP server, the previously obtained management port values obtained via the DHCP server will be inherited into the static address settings. You can leverage this functionality to pre-populate the static address settings via DHCP, then edit the static address settings according to your requirements.

5. To configure the Management port's static address, you must select each of the following

parameters using the ▲ and ▼ buttons and press the **OK** button in order to configure that parameter:

- **SET IP ADDRESS** - configures the static IP address of the Management port. This is a mandatory parameter. If you want the Management port to use a static address you must configure this parameter.
- **SET NETMASK** - configures the Netmask of the Management port. This is a mandatory parameter. If you want the Management port to use a static address you must configure this parameter.
- **SET GATEWAY** - configures the address of the Gateway used by the Management port. This parameter is optional. If you want the Management port to have Internet access, you must configure this parameter.
- **SET DNS 1** - configures the address of the Primary DNS Server used by the Management port. This parameter is optional. If you want the Management port to have Internet access, you must configure this parameter.
- **SET DNS 2** - configures the address of the Secondary DNS Server used by the Management port. This parameter is optional.

Upon pressing the **OK** button for the selected parameter, results in the line editor appearing with the existing value of the selected parameter. In the example below, the line editor is being used to specify the IP address of 192.168.110.69.



Note:

When in the line editor, the currently selected character is highlighted from below with the hat (^) symbol. In the example above, the 6 from the IP Address 192.168.110.69 is the currently selected character.

When you are in the line editor for the selected parameter, use the buttons on the front panel of the NE-ONE accordingly in order to configure that parameter:

- Press the ▶ button to move one character right within the line.
- Press the ◀ button to move one character left within the line.
- Press the ▲ button to change the value of the currently selected character to the next value (i.e. increase the numeric value from 1 to 2).
- Press the ▼ button to change the value of the currently selected character to the previous value (i.e. decrease the numeric value from 2 to 1).
- Press the **OK** button to commit the existing parameter, and return to the **SET ADDRESSING** page.
- Press the **Bottom Left** button to abandon the current line editor session. Any changes that were made during the line editor session are lost, and the original address is retained.
- Press the **Top Left** button to invoke ALT Mode (see note below).
- If the character selector goes further than length of the address, a new character is added with a default value of 0. This value of the new character can be modified using the ▲ and ▼ buttons.

Note:

ALT Mode lets you either insert a character or delete a character within the line. To enter ALT mode, press the **Top Left** button.

When in ALT mode you can select the position of the current character as usual by using the ◀ and ▶ buttons.

When in ALT mode, you can insert a new character by pressing the ▲ button. The new character is inserted at the current position, and the existing characters are moved to the right.

When in ALT mode, you can delete an existing character by pressing the ▼ button. The currently selected character is deleted, and the existing characters will move to the left.

When in ALT mode, you can view its help page by pressing the **Top Left** button.

To exit ALT mode, press the **Bottom Left** button. Upon exiting ALT mode you are returned to the line editor where you can modify the values of any newly inserted characters by using the ▲ and ▼ buttons.

Note:

Once finalizing a parameter and committing, the NE-ONE will perform a validation check. If you made an error with the format, you will be prompted to correct the parameter.

Note:

When modifying an existing character, the available characters are 0 through 9, dot (.), and space. The space is not used in defining an address, and is ignored if at the end of an address. This is useful if you have added too many characters at the end of the address because you can use a space (instead of going into the ALT mode) to remove the added character(s). This only works at the end of an address. If you have a space in the middle of an address the NE-ONE will raise an error on attempting to commit that address.

6. Once you have defined each of the parameters, use the ▼ button to scroll down and select **CONFIRM** in the **SET ADDRESSING** page, and the press the **OK** button.

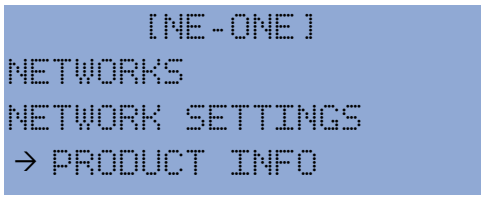
You are returned up one level to the **NETWORK SETTINGS** page, and updated setting is committed to the NE-ONE's Management Port. The NE-ONE Management port will now use a static addressing scheme.

Note:

The changes you make are only committed if you remain within the session of the **SET ADDRESSING** page. For example, if you have made changes to any of the parameters, but have not selected the **CONFIRM** menu item, the changes will not be committed to the NE-ONE's Management Port. Before navigating out of the **SET ADDRESSING** page, ensure you select the **CONFIRM** menu item and press the **OK** if you want the parameters to be committed.

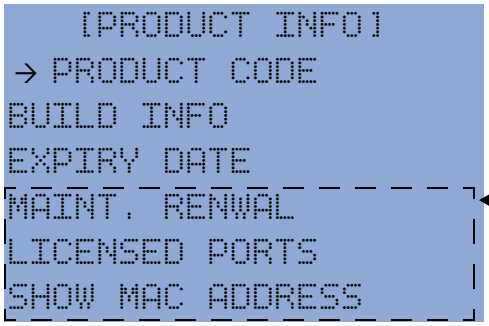
3-6-3. Product Info

The **PRODUCT INFO** main menu item provides various options for viewing various production information related to the NE-ONE.



Selecting the **PRODUCT INFO** main menu item, and pressing the **OK** button results in displaying the **PRODUCT INFO** menu items show in *Illustration 231*.

ILLUSTRATION 231 - PRODUCT INFO MENU ITEMS

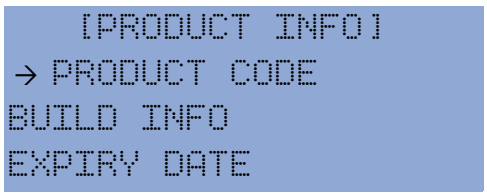


Note: Only four lines exist on the LCD panel. However, for clarity, in order to show the order of the menu items that you can cycle through, these additional lines are shown.

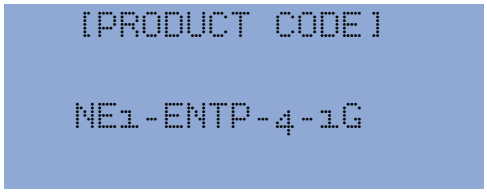
These **PRODUCT INFO** items are described in the sub-sections 3-6-3-1 to 3-6-3-6 below.

3-6-3-1. Product Code

The **PRODUCT CODE** product info menu item lets you view the product information of the NE-ONE.



Selecting the **PRODUCT CODE** product info menu item, and pressing the **OK** button results in displaying the product code of the NE-ONE.



The displayed product code has the following format:

NE1-<Edition>-<Licensed Hardware Ports>-<Maximum Bandwidth>

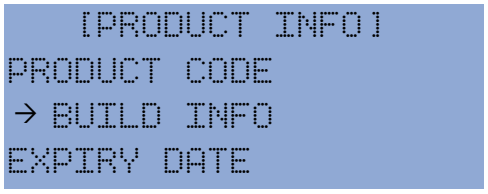
where:

- <Edition> is the NE-ONE edition type (this will vary according to the feature set that was sold to you by your sales representative).
- <Licensed Hardware Ports> is the number of licensed Hardware ports available for use.
- <Maximum Bandwidth> is the maximum bandwidth permitted on the fastest port of the group of licensed Hardware ports. For example, if an NE-ONE has two 1 Gigabit/s Hardware ports and two 10 Gigabit/s Hardware ports, the maximum permitted bandwidth displayed is 10G.

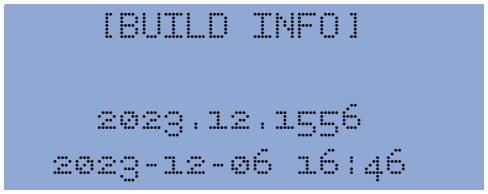
In the example above, the NE-ONE is an Enterprise edition, with four licensed hardware ports whose maximum permitted bandwidth is 1 Gigabit/s.

3-6-3-2. Build Information

The **BUILD INFO** product info menu item lets you view the build information of the NE-ONE.



Selecting the **BUILD INFO** product info menu item, and pressing the **OK** button results in displaying the build information of the NE-ONE.



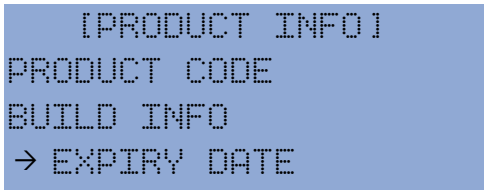
The displayed build information contains the following on two separate lines:

Build version, of the format : **<Year>.<Month>.<Incremental Build Number>**.

Build date, of the format : **<Year>.<Month>.<Day> <Hour>:<Minute>**.

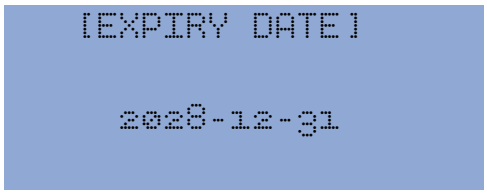
3-6-3-3. Expiry Date

The **EXPIRY DATE** product info menu item lets you view the expiry date of the NE-ONE's license.



Selecting the **EXPIRY DATE** product info menu item, and pressing the **OK** button results in displaying the expiry date of the NE-ONE's license.

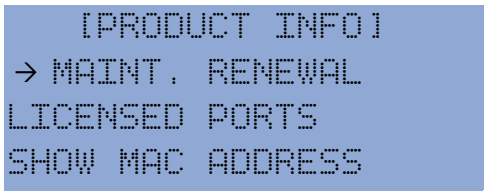
or



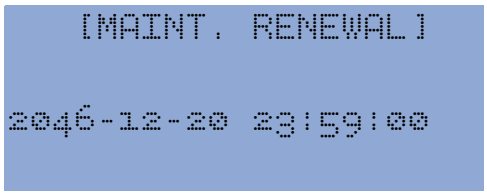
- If the license file has an expiry date (i.e. non-perpetual license) then the expiry date will be displayed in **<Year>-<Month>-<Day>** format.
- If the license file does not have an expiry date (i.e. perpetual license) then the expiry date will be displayed as **PERMANENT**.

3-6-3-4. Maintenance Renewal

The **MAINT. RENEWAL** product info menu item lets you view the maintenance renewal date of the NE-ONE.



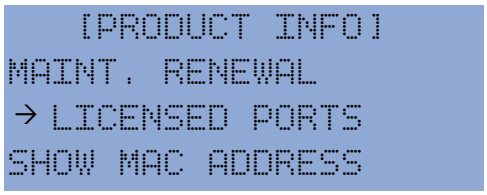
Selecting the **MAINT. RENEWAL** product info menu item, and pressing the **OK** button results in displaying the maintenance renewal date of the NE-ONE's license.



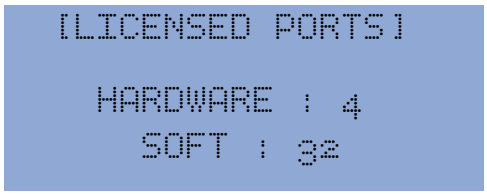
The displayed maintenance renewal date has the following format: **<Year>.<Month>.<Day> <Hour>:<Minute>:<Second>** .

3-6-3-5. Licensed Ports

The **LICENSED PORTS** product info menu item lets you view the number of licensed hardware ports and soft ports on the NE-ONE.



Selecting the **LICENSED PORTS** product info menu item, and pressing the **OK** button results in displaying the number of licensed hardware ports and soft ports on the NE-ONE.

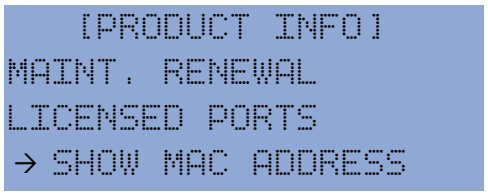


Note:

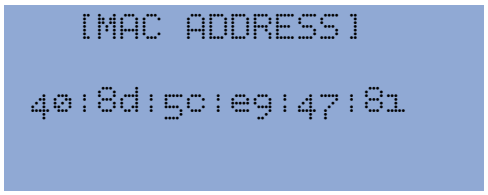
The number of licensed hardware ports on the NE-ONE Desktop unit may be less than four. In the case that the licensed hardware ports is less than four, the remaining ports on the NE-ONE Desktop are unlicensed. The hardware ports are licensed in order of 0, 1, 2, and 3. For example, if you have less than two hardware ports licensed, hardware ports 0 and 1 will be licensed, while hardware ports 2 and 3 will be unlicensed.

3-6-3-6. MAC Address

The **SHOW MAC ADDRESS** product info menu item lets you view the MAC address the NE-ONE's Management port. The license file used to license the NE-ONE is associated with this MAC address. When requesting a license file for your NE-ONE you must provide Calnex with this MAC address.

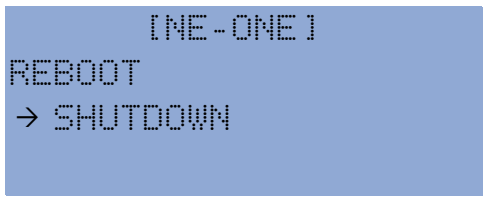


Selecting the **SHOW MAC ADDRESS** product info menu item, and pressing the **OK** button results in displaying the MAC address of the NE-ONE's Management port.



3-6-4. Shutdown

The **SHUTDOWN** main menu item lets you shut down the NE-ONE.

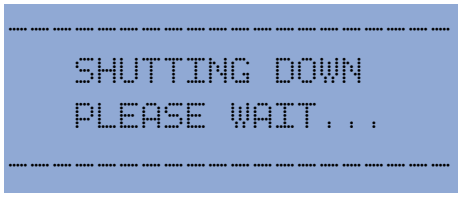


! Notice:

Shutting down an active NE-ONE will terminate all running networks/scenarios and all unsaved networks/scenarios will be lost.

To shut down the NE-ONE, select the **SHUTDOWN** main menu item, then press the **OK** button. The LCD panel displays the following confirmation message.

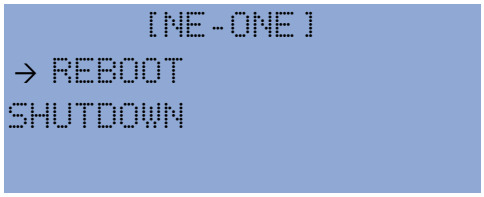
- To shut down the NE-ONE, select **YES** then press the **OK** button. In this case the LCD panel shows the following message temporarily before shutting down the NE-ONE.



- To abandon shutting down the NE-ONE and return to the main menu, either press the **Back** button or select **NO** and press the **OK** button.

3-6-5. Reboot

The **REBOOT** main menu item lets you reboot the NE-ONE.

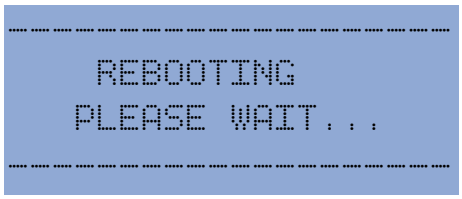


! Notice:

Rebooting an active NE-ONE will terminate all running networks/scenarios and all unsaved networks/scenarios will be lost.

To reboot the NE-ONE, select the **REBOOT** main menu item, then press the **OK** button. The LCD panel displays the following confirmation message.

- To reboot the NE-ONE, select **YES** then press the **OK** button. In this case the LCD panel shows the following message temporarily before rebooting the NE-ONE.



- To abandon rebooting the NE-ONE and return to the main menu, either press the **Back** button or select **NO** and press the **OK** button.

This page is intentionally left blank.

APPENDIX 1 SPECIFYING EXPRESSIONS

This appendix provides examples of expressions that are used in different parts of the Web Interface when defining the following:

- Link Qualifications for port pairs.
- A Background Routed Expression service (see *Creating a Background Expression Routed service* on page 178).
- A Filter soft port (see *Creating a Filter Soft Port* on page 124).
- An Expression Filter soft port (see *Creating an Expression Filter Soft Port* on page 132).

Note:
The ability to create a Background Routed Expression service is only possible the NE-ONE if the Service Manager feature activated. Depending on your license, the Service Manager feature may be activated or deactivated.

Note:
The ability to create soft ports is only possible the NE-ONE if the Port Manager feature activated. Depending on your license, the Port Manager feature may be activated or deactivated.

1. LINK QUALIFICATION EXPRESSIONS

Expressions use a powerful packet classification (packet selection) engine. With Expressions packet classification (packet selection) is performed by creating a Wireshark like expression.

For example, to select all those packets in VLAN 601 which have a destination IPv4 address of 192.168.4.1 to be selected in link classification is performed by the expression:

```
Vlan.id = 601 and ipv4.dst = 192.168.4.1
```

Very sophisticated selections can be put together using:

- Boolean (logical) operators: **and**, **or**
- Comparison operators: **=**, **<>**, **>**, **<**, **>=**, **<=** (note: **<>** for not equal)
- Bit operators **&**, **|**, **<<**, **>>** (bit and, bit or, left shift, right shift)
- Arithmetic operators: **+**, **-**, *****, **/**, **%** (mod)
- Brackets **( )**

A more sophisticated expression, demonstrating some of these operators might be as follows:

```
((192.168.10.10 = ipv4.src) OR (192.168.10.10 = ipv4.dst) OR (192.168.10.10 =
arp.Sender_Protocol_Address) OR (192.168.10.10 = arp.Target_Protocol_Address)) AND
ipv4.dst=192.168.10.20
```

Firstly, that is all one expression which broadly says that the packet matches if:

(its source IP address is 192.168.10.10 or its destination IP address is 192.168.10.10 or its ARP sender address is 192.168.10.10 or its ARP target address is 192.168.10.10)

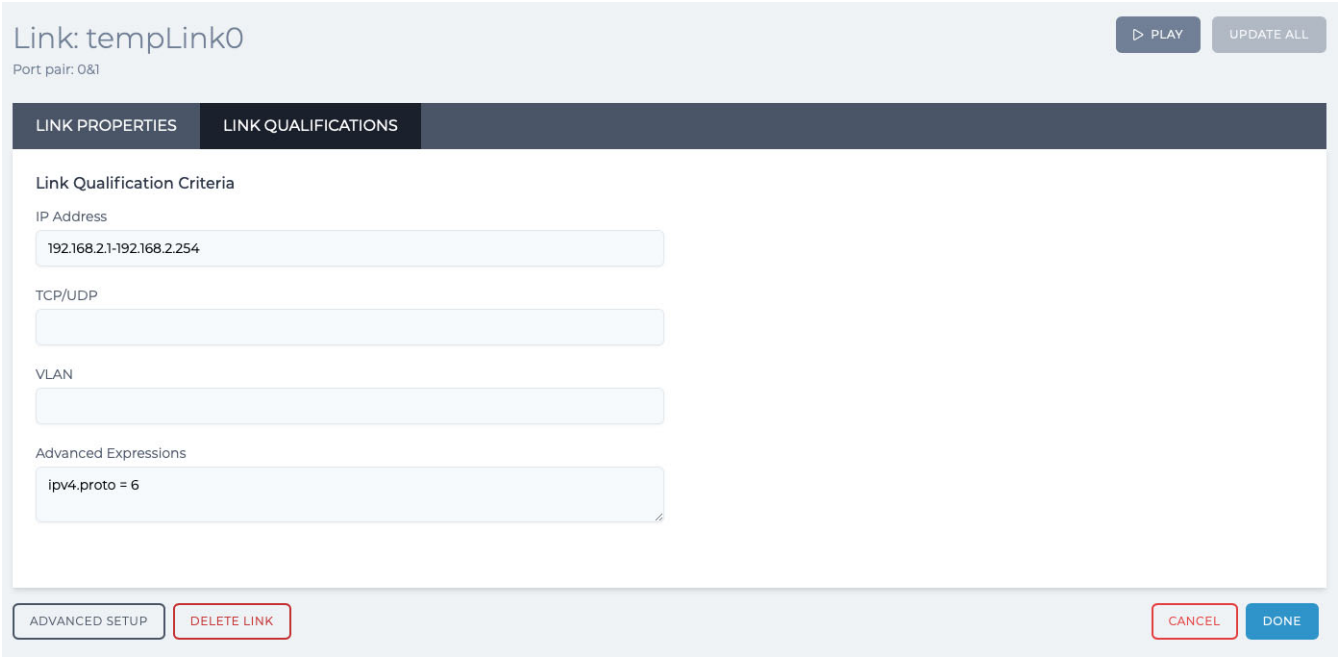
A lot going on there. You might use this statement in a bridged network to send both IPv4 and ARP down the same link provided it has the address 192.168.10.10 somewhere in the addressing (source, dest, arp).

You can see the use of **bracketing** and logical operators, **and** and **or**, also the comparison operator **=**.

1-1. Combining Expressions With Other Link Qualification Fields

As an example, assume you have completed the **IP Address** and **Advanced Expressions** fields in the **LINK QUALIFICATIONS** area of the **Link** page as shown in *Illustration 232* for a particular link.

ILLUSTRATION 232 - LINK QUALIFICATION COMBINED EXPRESSION EXAMPLE 1



The link qualification criteria needs to make sure your IP addresses are in the correct range and the expression is true to qualify. To do this behind the scenes the Packet Classification Engine creates the following expression (it is actually a little more sophisticated even than this) for you:

```
((ipv4.dst >= 192.168.2.1 and ipv4.dst <= 192.168.2.254) or (ipv4.src >=
192.168.2.1 and ipv4.src <= 192.168.2.254)) and (ipv4.proto = 6)
```

You do not see this process, as it happens in the background.

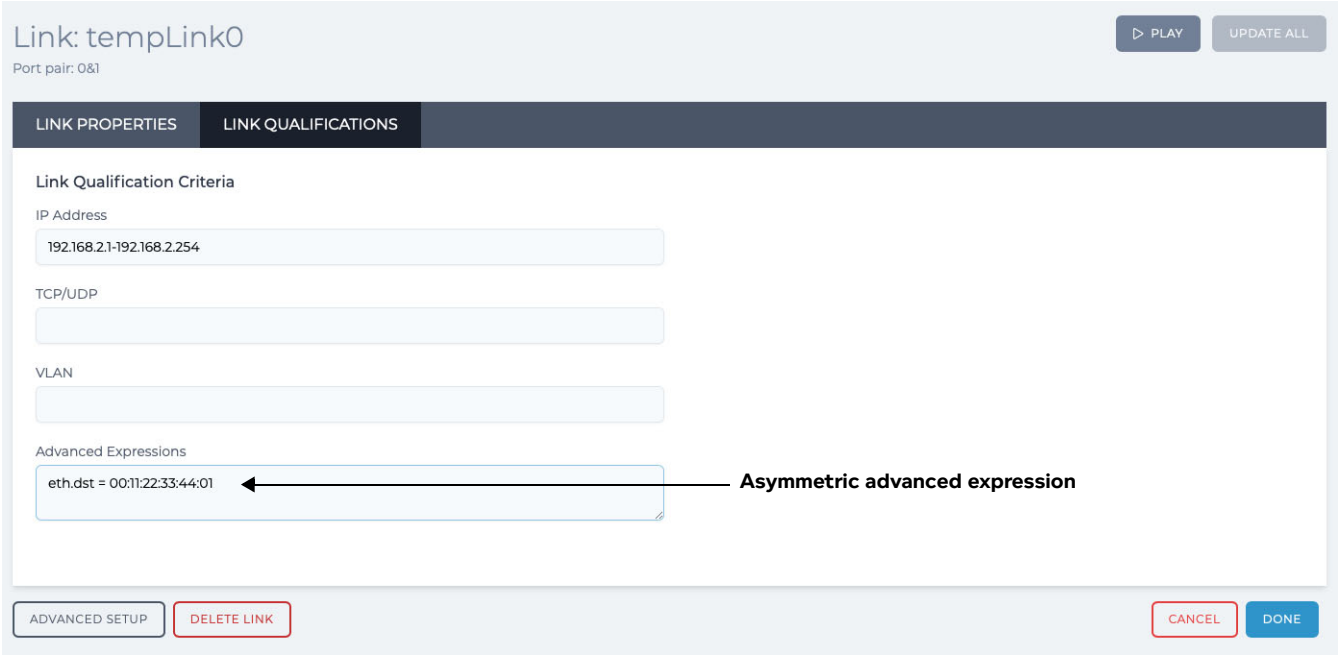
From the resulting expression (part generated and part input by you) it is evaluated whether the packet matches your link (i.e. when the expression is TRUE).

The **IP Address**, **TCP/UDP**, and **VLAN** fields always generate a symmetric link qualification (i.e. traffic comes back down the same link it went out on). However, depending on the type of advanced expression you specify, the **Advanced Expressions** field will create either a symmetric or asymmetric link qualification. For more information, see *Symmetry vs Asymmetry* on page 733.

1-2. Symmetry vs Asymmetry

Suppose that in the example of *Illustration 232* instead of having specified `ipv4.proto = 6` in the **Advanced Expression** field, you had specified `eth.dst = 00:11:22:33:44:01` as shown in *Illustration 233*.

ILLUSTRATION 233 - LINK QUALIFICATION COMBINED EXPRESSION EXAMPLE 2 - ASYMMETRIC



Then the resulting auto generated combined expression would be:

```
((ipv4.dst >= 192.168.2.1 and ipv4.dst <= 192.168.2.254) or (ipv4.src >=
192.168.2.1 and ipv4.src <= 192.168.2.254)) and (eth.dst = 00:11:22:33:44:01)
```

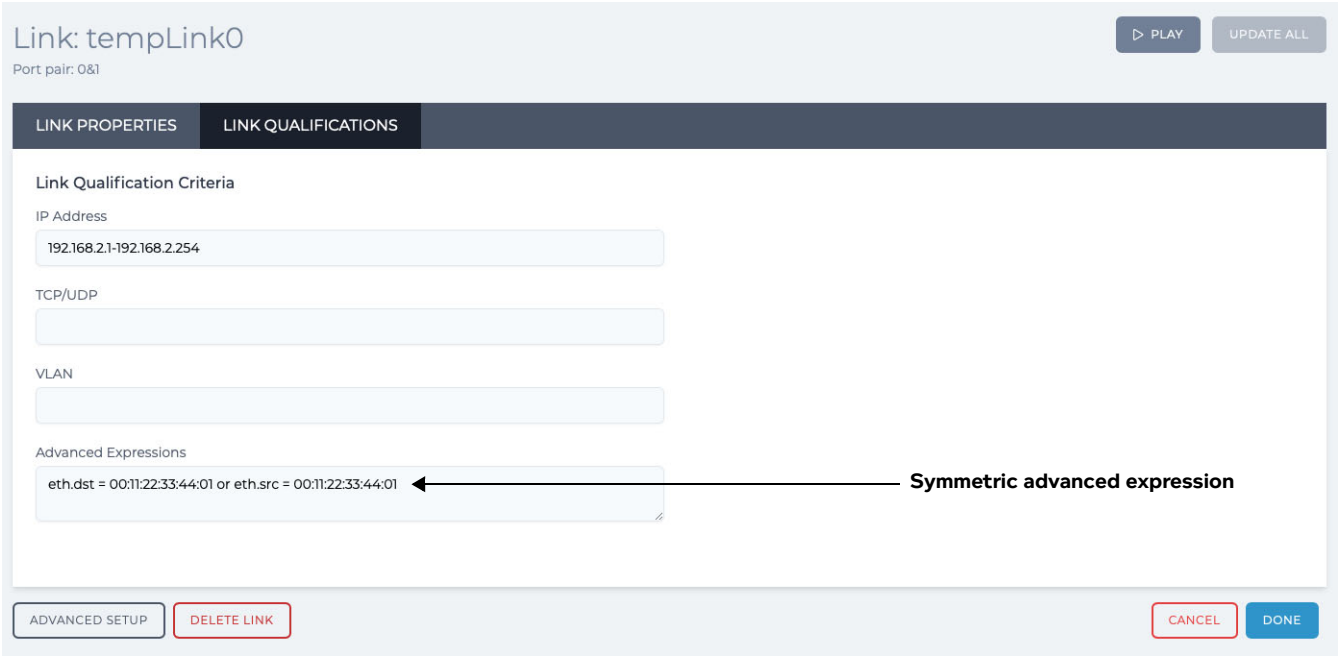
which is of course is no longer symmetric because `eth.dst = 00:11:22:33:44:01` is itself not symmetric in the MAC address.

If you want to keep it symmetric (you do not have to), you need to make sure that your advanced expressions are symmetric. For example, if in the **Advanced Expression** field you specify `eth.dst = 00:11:22:33:44:01 or eth.src = 00:11:22:33:44:01` as shown in *Illustration 234* then the resulting auto generated expression is:

```
((ipv4.dst >= 192.168.2.1 and ipv4.dst <= 192.168.2.254) or (ipv4.src >=
192.168.2.1 and ipv4.src <= 192.168.2.254)) and (eth.dst =
00:11:22:33:44:01 or eth.src = 00:11:22:33:44:01)
```

This is quite an expression, but the hard work is automatically done for you and it is also compiled to machine code by the just in time (JIT) compiler and so evaluated quickly.

ILLUSTRATION 234 - LINK QUALIFICATION COMBINED EXPRESSION EXAMPLE 3 - SYMMETRIC



2. EXPRESSION LIBRARY FUNCTIONS

The expression functions are listed in the appropriate sections e.g. debug in the Debug section, Filter in the Filter section etc, so why are we dealing with them separately here?

This is because they all have a common theme: They use a powerful packet classification (packet selection) engine.

Fundamentally, using these functions there is no more setting tables of ranges of source and/or destination IP addresses or ports, or IP protocols or VLAN Ids. Instead packet classification (packet selection) is performed by creating a Wireshark like expression.

For example, to select all those packets in VLAN 601 which have a destination IPv4 address of 192.168.4.1 to be "routed" can now be performed by the *Expression Routing (Expression)* function where the routing selection is:

```
Vlan.id = 601 and ipv4.dst = 192.168.4.1
```

Very sophisticated selections can be put together using:

- Boolean (logical) operators: **and**, **or**
- Comparison operators: **=**, **<>**, **>**, **<**, **>=**, **<=** (note: **<>** for not equal)
- Bit operators **&**, **|**, **<<**, **>>** (bit and, bit or, left shift, right shift)
- Arithmetic operators: **+**, **-**, *****, **/**, **%** (mod)
- Brackets **( )**

So, the *Expression Routing (Expression)* function could replace the *IPv4 Routing* function by simply describing routes like this:

- `ipv4.dst & 255.255.255.0 = 192.168.1.0`
- `ipv4.dst & 255.255.255.0 = 192.168.2.0`
- `ipv4.dst & 255.255.255.0 = 192.168.3.0`

But it would be equally at home with "source" IP routing like this (note the src field):

```
ipv4.src & 255.255.255.0 = 192.168.1.0
```

```
ipv4.src & 255.255.255.0 = 192.168.2.0
ipv4.src & 255.255.255.0 = 192.168.3.0
```

Those are pretty simple expressions though, in this example we see more of the power:

```
@packet.ingress_port = 2 AND ((192.168.10.10 = ipv4.src) OR (192.168.10.10 = ipv4.dst) OR (192.168.10.10 = arp.Sender_Protocol_Address) OR (192.168.10.10 = arp.Target_Protocol_Address)) AND ipv4.dst=192.168.10.20
```

Firstly, that is all one expression which broadly says that the packet matches if:

- It entered the NE-ONE on port 2 and (its source IP address is 192.168.10.10 or its destination IP address is 192.168.10.10 or its ARP sender address is 192.168.10.10 or its ARP target address is 192.168.10.10)

A lot going on there. You might use this statement in a bridged network to send both IPv4 and ARP down the same path in the NE-ONE provided it has the address 192.168.10.10 somewhere in the addressing (source, dest, arp) and it arrived in the NE-ONE on port 2.

You can see the use of bracketing and logical operators, **and** and **or**, also the comparison operator **=**. You can also see the use of a special packet property that is not actually packet data i.e. @packet.ingress_port = 2

The leading @ here signifying this special data.

Expressions are not just limited to routing though. The following functions allow you to use the expression functionality. This table is a quick reference with the functions being fully described in their own sections:

Function	Category / Area	Description
Debug	Initial	This is a much more advanced version of the Default (and Labs) Debug function which uses the expression Protocol files (see *Supplied and User Defined Protocols and Fields* on page 736) to interpret the packet structure (if desired) as well as selecting only certain packets to dump or print based on an Expression (as described above e.g. `Vlan.id = 601` `ipv4.dst = 192.168.5.1`) For more information on this function *Debug (Expression)* on page 749.
Expression Filter with NAT (Expression)	Filter	This is the expression version of *Composite Filter with NAT (Labs)* – equivalent to that function but using expression classification For full information on this function, see *Expression Filter with NAT (Expression)* on page 751.
Expression Routing (Expression)	Routing	This is the expression version of *Composite Routing (Labs)* – equivalent to that function but using expression classification
Symmetric Routing (Expression)	Routing	This is an enhanced version of *Symmetric Routing*, it uses the same syntax as symmetric routing for IP address ranges, IP Port ranges and VLANs, but adds an expression field so you can enter additional selections e.g. Ethernet addresses etc.

2-1. Supplied and User Defined Protocols and Fields

It is possible to define your own protocol definition files, so that you can use Expressions on your own protocols and fields, though the details of this are beyond the scope of this guide.

Nevertheless to see what it entails let's use the IPv4 protocol as an example. This is the supplied IPv4 protocol definition file:

```
Protocol IPv4 Layer 3 MSB Description "IPv4"
Number
Number HEADER LENGTH ActualValue (hdr_len << 2)
Number Number Number
DefaultDisplay X Number
Number Number Number
Number Number Number
version:4 hdr_len:4
tos:8 length:16 id:16
resv:1
df:1
mf:1 frag_off:13
Description "Version" Description "Header Length"
Description "TOS" Description "Length" Description "Packet Id"
Description "Reserved" Description "Don't Fragment" Description "More Fragments"
Description "Fragment Offset"
Description "TTL" Description "Protocol" Description "Checksum"
Description "Source Address" Description "Destination Address"
src or dst
DefaultDisplay X IPv4Address IPv4Address
FilterField
ActualValue (frag_off << 3) ttl:8
proto:8 csum:16
src dst
ip_addr
ProtocolLink
ProtocolLink
ProtocolLink (proto = 1) ICMP
ProtocolLink (proto = 47) gre EndProtocol
```

Without laboring the syntax here, you can see:

- how the IPv4 header structure is expressed
- how n-bit fields are specified e.g. df:1 means df is a one bit field
- how certain fields are computed from the stored values (Fragment_Offset is multiplied by 8 [left shift 3])
- How the next layer of protocols is chained using a link field e.g. if proto = 6 then the next layered protocol is tcp

For more information on Protocols, including how to create your own protocol please contact the Calnex support or your support representative.

3. FIELDS AVAILABLE FOR USE IN EXPRESSIONS

This section describes the fields are available for use in expressions, listed below by Protocol.

The full field names are constructed by prefixing the field name with the protocol name or its alias, separated by a dot (period) character – see the examples below.

Note:
Protocol and Field names are NOT case sensitive.

This is not the full list, in the interests of keeping this user guide to reasonable proportions. If you need other fields please contact Calnex support or your support representative.

Before starting with "proper protocols" we look at an important pseudo protocol containing Packet metadata.

3-1. @Packet – pseudo protocol

We may need to refer to parts of the packet which are not actually in the packet contents but instead are extra fields or descriptive fields. These are available as a pseudo protocol called **@packet**. Following the same format as used for real protocols below:

Protocol Name	@Packet
Network Layer	N/A
Alias	-
Fields	
Field	**Description**
`length`	The size of the packet minus the CRC.
`channel`	The direction of the packet in a full duplex object. This field is NOT supported at this time.
`last_hop`	The id of the object (node or link) where the packet just came from.
`inress_port`	The id of the port (or final soft port, if layered) where the packet entered the NE-ONE.
`egress_port`	The id of the egress port field in the packet structure (if the packet has been routed), determining to which object or port the packet will be sent to after this object has finished processing it.
`user_label`	A user settable numeric value.
`loc[byte offset within packet]`	Test the individual byte offset within the packet, with a base of 0.

Lastly we have two scalar (non protocol values)
True - always 1
False - always 0

Examples:

1. To test the packet is >=200 bytes: **`@packet.length >= 200`**
2. To test the packet is an ARP packet and came in on port id 0 specify: **`@packet.ingress_port = 0 and eth.proto = 0x806`**
   (see below for eth/802.3x protocol)

Note: The value of @packet.ingress_port (and similarly egress_port/last_hop) is the id, not the name of the ingress port, even though for hardware ports this appears to be the same in fact the name is a string and the id is the Ported numeric value which can be obtained from the –`getallports` command line command).

3-2. Ethernet (802.3x) Protocol

Protocol Name	802_3x
Network Layer	2
Alias	eth
Fields	
Field	**Description**
`dst`	Destination Address – MAC address
`src`	Source Address – MAC Address
`proto`	Protocol Number
Examples:	
1. To test the packet is an ARP packet specify: **`eth.proto = 0x806`** 2. To test destination MAC 00:11:22:33:44:01, specify: **`eth.dst = 00:11:22:33:44:01`** 3. To test IPv4 or IPv6, specify: **`802_3x.proto = x800 or 802_3x.proto = x86DD`**	

3-3. VLAN (802.1q) Protocol

Protocol Name	802_1q
Network Layer	2
Alias	vlan
Fields	
Field	**Description**
`pcp`	Priority Code Point
`dei`	Drop Eligible Indicator
`id`	VLAN Id
`proto`	Protocol
Examples:	
1. VLAN between 601 and 700, specify: **`vlan.id >= 601 and vlan.id <=700`** 2. VLAN Id is not 5, specify: **`802_1q.id <> 5`**	

3-4. IPv4 Protocol

Protocol Name	IPv4
Network Layer	3
Alias	-
Fields	
Field	**Description**
`version`	Version (should be 4)
`hdr_len`	Header Length – Calnex provide Actual Value = (hdr_len << 2)
`Length`	Length
`Id`	Packet Id
`resv`	Reserved

`df`	Don't Fragment
`mf`	More Fragments
`frag_off`	Fragment Offset – Calnex provide Actual Value = (frag_off << 3)
`ttl`	TTL – Time to Live (max hops)
`proto`	Protocol
`csum`	Checksum
`src`	Source Address
`dst`	Destination Address
Examples:	
1. TCP packet, specify: **`ipv4.proto = 6`** 2. The ipv4 destination address lies in the interval 192.168.1.1-192.168.1.254, specify: **`192.168.1.1 <= ipv4.dst and ipv4.dst <= 192.168.1.254`**	

3-5. IPv6 Protocol

Protocol Name	IPv6
Network Layer	3
Alias	-
Fields	
Field	**Description**
`version`	Version (should be 6)
`Traffic_Class`	Traffic Class
`Flow_Label`	Flow Label
`Payload_Length`	Payload Length
`Next_Header`	Next Header
`Hop_Limit`	Hop Limit
`Source_Address`	Source Address
`Destination_Address`	Destination Address
Examples:	
1. TCP packet in IPv6, specify: **`ipv6.Next_Header = 6`** 2. Standard IP v6 notation - :: means repeating 0 bytes – true if source and destination ipv6 addresses match the ones specified : **`IPv6.Destination_Address = fe80::612d:7669:d879:1302 and ipv6.Source_Address = fe80::6ced:ec22:1e80:bf1`**	

3-6. ARP Protocol

Protocol Name	ARP
Network Layer	3
Alias	-
Fields	
Field	**Description**
`Hardware_Type`	Hardware Type
`Protocol_Type`	Protocol Type
`Hardware_Address_Length`	Hardware Address Length
`Protocol_Address_Length`	Protocol Address Length
`Operation`	Operation
`Sender_Hardware_Address`	Sender Hardware Address
`Sender_Protocol_Address`	Sender Protocol Address
`Target_Hardware_Address`	Target Hardware Address
`Target_Protocol_Address`	Target Protocol Address
Examples:	
1. Testing a “who is” 192.168.5.100 ARP request, specify: **`arp.Target_Protocol_Address = 192.168.5.100`** 2. Test if 00:11:22:33:44:01 sent out the ARP request, specify: **`arp.Target_Hardware_Address = 00:11:22:33:44:01`**	

3-7. TCP Protocol

Protocol Name	TCP
Network Layer	4
Alias	-
Fields	
Field	**Description**
`Source_Port`	Source Port
`Destination_Port`	Destination Port
`Sequence_Number`	Sequence Number
`Acknowledgment_Number`	Acknowledgment Number
`Data_Offset`	Data Offset
`Reserved`	Reserved
`NS`	ECN-nonce concealment protection
`CWR`	Congestion Window Reduced
`ECE`	ECN Echo
`URG`	Urgent
`ACK`	Acknowledgment
`PSH`	Push
`RST`	Reset
`SYN`	Synchronize Sequence Numbers
`FIN`	Finish
`Window_Size`	Window Size
`Checksum`	Checksum
`Urgent_Pointer`	Urgent Pointer
Examples:	
1. Is it port 80 – http or port 443 – https, specify: **`tcp.Destination_Port = 80 or tcp.Destination_Port = 443`** 2. To drop every 10th packet of a TCP stream, specify: **`tcp.Sequence_Number % 10 = 0`**	

3-8. UDP Protocol

Protocol Name	UDP
Network Layer	4
Alias	-
Fields	
Field	**Description**
`Source_Port`	Source Port
`Destination_Port`	Destination Port
`Length`	Length
`Checksum`	Checksum
Examples:	
1. Is it port 53 and udp i.e. normally dns, specify: **`udp.Destination_Port = 53`**	

APPENDIX 2 AVAILABLE FUNCTIONS

This appendix provides a summary of the current list of functions that are delivered with the NE-ONE. These functions can be used when creating more sophisticated networks with link/node impairments or advanced node testing. Three types of function category exist, as follows:

- Impairment functions - used for creating impairments on links and/or nodes. For more information, see *Available Impairment Functions*.
- Node functions - used for creating cloud nodes. For more information, see *Available Node Functions* on page 759.
- Packet input functions - used for adding additional traffic into your network, so that you can test your network applications in more detail with specific types of traffic. For more information, see *Available Packet Input Functions* on page 762.

The NE-ONE's comprehensive library of functions lets you easily mimic what happens in real-world networks. Each function is controlled by one or more parameters letting you customize its behavior for your specific testing needs. The NE-ONE's functions are frequently updated based on evolving networks and customer needs.

Note:

As network technologies evolve, Calnex keep NE-ONE functions up-to-date via software updates. For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date. An active maintenance contract lets you update the NE-ONE functions when new network technologies and new testing methodologies become available.

1. AVAILABLE IMPAIRMENT FUNCTIONS

The impairment functions that are available vary according whether or not you have the Advanced Functions feature activated. *Table 81* summarizes the impairment functions that are available to both links and nodes.

TABLE 81 - IMPAIRMENT FUNCTIONS AVAILABLE TO LINKS AND NODES

	All NE-ONEs	NE-ONEs with Advanced Functions Feature
Bandwidth Functions		
Linkspeed and FIFO Queue Bytes	✓	✓
Cisco QoS Class Bandwidth (Labs)		✓
Linkspeed with Variable Congestion (Labs)		✓
Cisco QoS Class Bandwidth (Expression)		✓
Bit Error Functions		
Random Packet Error	✓	✓
Poisson Error	✓	✓
Error with Burst	✓	✓
Random Packet Corrupt	✓	✓
Debug Functions		
Debug	✓	✓

	All NE-ONEs	NE-ONEs with Advanced Functions Feature
Debug (Expression)		✓
Debug (Labs)		✓
Duplicate Functions		
Packet Move and Duplicate	✓	✓
Filter Functions		
Generic Filter	✓	✓
Expression Filter with NAT (Expression)		✓
Composite Filter with NAT (Labs)		✓
Composite Filter (Labs)		✓
Fragment Functions		
Fragment MTU	✓	✓
Latency Functions		
Random Delay	✓	✓
Random Delay Nanoseconds	✓	✓
Step Delay Packet Nanoseconds	✓	✓
Fixed Delay	✓	✓
Fixed Delay Nanoseconds	✓	✓
Fixed Delay Milliseconds	✓	✓
City to City Latency	✓	✓
Step Delay Periodic	✓	✓
Gaussian Delay	✓	✓
Delay Sequence (Labs)		✓
Delay Scenarios (Labs)		✓
Fixed Delay with Jitter (Labs)		✓
Loss Functions		
Random Drop	✓	✓
1 in X	✓	✓
Total Drop	✓	✓
No Drop	✓	✓
Burst Loss	✓	✓
Packet Error 1 in X bits	✓	✓
Poisson Drop	✓	✓
Random Drop with Burst	✓	✓
Out Of Order Functions		
Random Packet Move Offset		✓
Random Packet Time Reorder (Labs)	✓	✓
Packet Reorder in X	✓	✓

	All NE-ONEs	NE-ONEs with Advanced Functions Feature
Pause Functions		
Pause Transmission (Labs)		✓
Pause Transmission Repeat (Labs)		✓

The sections below summarize each of the impairment functions, organized by their category.

1-1. Bandwidth Functions

These functions control bandwidth and the related topic of what happens when there is insufficient bandwidth: **queuing**

Some of the functions in this section are in fact **composite**: In addition to controlling bandwidth they may also control other things like Latency, Loss, TTL Cost, QoS and Prioritization. They are placed in this section because bandwidth control functions are the final ones before a packet is transmitted to the next network object (link or node) or port (hardware or soft).

1-1-1. Linkspeed and FIFO Queue Bytes

This function lets you set the **Link Speed** to a pre-defined **Link Type** or choose a Link Type of **Manual** and then set the link speed manually. Setting the Link Speed also implicitly sets a delay called the **Latency of Serialization** to the link (this is only very apparent when bit rates are low and/or packet sizes large) as would happen in real world links.

The **Queue Length** determines the queue size to be used (in bytes) should packets need to be queued because there is insufficient bandwidth available in the link to send them immediately.

The **Overhead** specifies how many bytes should be added to the size of an IP packet to represent the layer 2 overhead when computing packet sizes in bits. The default is 18 bytes (Ethernet header 14 bytes plus Ethernet CRC 4 bytes). Change this if you are emulating a different layer 2 medium.

The **Congestion Pct** emulates the link being congested e.g. 80% congestion will make the link behave as though only 20% is available. This is the correct way to emulate a busy link rather than reducing the Link Speed.

The value in the **TTL Cost** field is subtracted from the packet's TTL value (IP packets only, as other's don't have a cost) and the IP header checksum is recalculated to be correct. If the packet's TTL was to reach 0 (or less) as a result of the TTL cost the packet will be dropped and 1 added to the drop counter.

1-1-2. Linkspeed with Variable Congestion (Labs)

This function has all the options specified above in *Linkspeed and FIFO Queue Bytes* on page 745 but adds an optional **Congestion Duration Limits Table**.

This table has rows which contain values for:

- **Min Congestion Pct & Max Congestion Pct** – an actual congestion percentage is chosen at random between these two values (inclusive). If you want a particular value set the Min and Max to the same value.
- **Min Duration & Max Duration** – a duration for the congestion is chosen at random between Min and Max Duration. At the end of this time the next row in the table is read and a new congestion and duration chosen. This goes on until all the rows in the table have been processed at which point the process starts again with the first row in the table

So, using this feature you can make a link change congestion cyclically without any scripting, holding each congestion value for as long as you like. Congestion emulates busy network links so that traffic can only use what is left of the link, as happens in the real world.

If the congestion limits table has no rows then the static **Congestion Pct** value is used. If the static value is 0 then there is no congestion applied to the link and traffic can use the entire defined Link based on the **Link Speed** parameter.

1-1-3. Cisco QoS Class Bandwidth (Labs)

This is a composite impairment function.

It is similar to Labs:QoS Class Bandwidth having an identical packet classification system to that function, but its Class definitions are algorithms model the Cisco CIR (Committed Information Rate), Bc, Be, Tc, queue size in packets and a choice of Traffic Shaping algorithms.

There are two levels of Bandwidth and traffic shaping control:

- per link
- per class

The next sections describe both the LinkParameters, QoS Class Definitions (Filters) and QoS Classes parameters.

1-1-3-1. Link Parameters

This section documents all the Link level parameters.

TABLE 82 - CISCO QOS CLASS BANDWIDTH (LABS) LINK PARAMETERS

Parameter	Description
Link Speed	This is the speed of the Link itself in bps i.e. the transmission rate of the link. It is used to determine how long it will take to send 1 bit of data out of this link. A 0 value implies an infinitely fast link (as is the convention for all of the bandwidth regulation functions). Do not confuse this with the CIR. Link speed is simulating a physical property.
Shaping Type	The drop-down menu here offers Peak or Average. This behaves in the same way as for Cisco Routers, shapers etc with Peak effectively allowing Bc + Be bits to be sent per time quantum (Tc) and Average allowing Bc bits per time quantum (Tc).
CIR	This is Cisco's CIR (Committed Information Rate) for this Link (Pipe) in bps. It can peak higher during a single time quantum (Tc) - per Cisco's algorithms.
Bc	Cisco's Bc parameter - This is the Committed Bucket Size in bits. Tc (the time quantum) is computed from this and CIR, using this formula: Tc = Bc/CIR.
Be	Cisco's Be parameter - This is the Excess (extra) Bucket size in bits used when Bc is exhausted, if using Peak shaping. Thus with peak shaping we actually get to send more than Bc bits in one time quantum. For example if Be was the same as Bc then the actual rate could be up to 2xCIR.
Tc (computed, not entered)	Cisco's Tc, Time Quantum for measuring used in transmission in seconds, you cannot set it separately - it is computed from CIR and Bc as above using this formula: Tc = Bc/CIR. So if Bc was 100Kbits and CIR 10Kbps then Tc would be computed as 10 (seconds) [while we will emulate this, Cisco's algorithms may not actually permit these values as 10s is huge]. In this example, a 10 second Tc would mean that we could send, depending on linkspeed, all of our 100Kbits in the first second - we could then not transmit any more information until Tc expires (9 seconds later) and our bucket is refreshed. Thus temporarily in the first second we will have exceeded CIR (but not Linkspeed).
Queue Length Packets	The maximum queue size for the Link in packets. So when Bc (Shape Average) or Bc + Be (Shape Peak) is exhausted packets will queue until this queue is exhausted. NOTE that this lead to large latencies if the queue is large compared to CIR
QoS Class Filters	This is a table (array) of definitions of what traffic (by IP address, Port, Protocol, VLAN...) maps a QoS Class Filter to a class i.e. the traffic classification process. This is described in *QoS Class Filters* on page 747.

Parameter	Description
QoS Classes	This is a table (array) of classes - specifying CIR, Bc, Be etc for each class. This is described in *QoS Class Parameters* on page 747.

1-1-3-2. QoS Class Filters

The **QoS Class Filters** table allows definition of the classes by lists, ranges or list of ranges of:

- **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE.
- **Use Last Hop as Port In** – modifies **Port In** to be the name of the immediately previous network object (node or link) or port (hardware or soft) the packet just came from.
- **Source IP Address** – the IP (v4 or v6) address where the packet has come from e.g. for TCP/IP 192.168.1.1-192.168.1.255
- **Dest IP Address** - the IP (v4 or v6) address where the packet is going to e.g. 192.168.2.10
- **Source Port** – which port the packet has come from e.g. for TCP/IP 6000, 6001
- **Dest Port** – which port the packet is going to e.g. 80 (HTTP), 443 (HTTPS), 25 (smtp), 21 (ftp), 110 (pop3), 445 (Microsoft-ds – Network File Access)
- **IPv4 Protocol** – the IP (v4 or v6) protocol of the packet e.g. 0 (Not IP) 1 (ICMP), 6 (TCP), 17 (UDP), 47 (GRE) etc.
- **VLAN Id** – 802.1Q VLAN label (tag), if the packet is VLAN tagged.
- **DPI** – (Deep Packet Inspection) select a packet for this cloud row based on one or more bytes or bits in the header or data part of the packet.
- **QoS Class Id** – The number of the QoS Class (1,2,3,...) being defined by this filter
- **Default QoS Class** – set to True if this is the default class to use.
- **QoS Class Disabled** - If ticked (checked) then this QoS Class is disabled i.e. not in use, as though it's deleted.
- **Desc** – a brief (optional description of the filter's purpose).

Note:

As the QoS Class Filters array can contain overlapping definitions the order in which they're processed is important. To change the order of the filter rows, rows in the table can be re-ordered by using the Up and Down arrows on the right-hand side of the table:

So the key is to define a **QoS Class Id** for a range of traffic. We'll use that QoS Class Id in the **QoS Classes** table. In Cisco QoS Class Bandwidth this table has the following fields (which are quite different to those of Labs:QoS Class Bandwidth):

1-1-3-3. QoS Class Parameters

These classes determine the traffic handling parameters for each class e.g. Shaping Type, CIR, Bc, Be, Tc, Queue.

The fields are very similar to the Link fields but this time there are separate values per class:

TABLE 83 - CISCO QOS CLASS PARAMETERS

Parameter	Description
QoS Class Id	This is a unique number for the QoS Class. The QoS Class Filters match this number to their own in order to figure out which class to deliver traffic to.
Shaping Type	The drop-down menu here offers Peak or Average. This behaves in the same way as for Cisco Routers, shapers etc with Peak effectively allowing Bc + Be bits to be sent per time quantum (Tc) and Average allowing Bc bits per time quantum (Tc).
CIR	This is Cisco's CIR (Committed Information Rate) for this Link (Pipe) in bps. It can peak higher during a single time quantum (Tc) - per Cisco's algorithms.

Parameter	Description
Bc	Cisco's Bc parameter - This is the Committed Bucket Size in bits. - Tc (the time quantum) is computed from this and CIR, using this formula: Tc = Bc/CIR.
Be	Cisco Be parameter - This is the Excess (extra) Bucket size in bits used when Bc is exhausted, if using Peak shaping. Thus, with peak shaping we actually get to send more than Bc bits in one-time quantum. For example, if Be was the same as Bc then the actual rate could be up to 2xCIR.
Tc (computed, not entered)	Cisco's Tc, Time Quantum for measuring used in transmission in seconds, you cannot set it separately - it is computed from CIR and Bc as above using this formula: Tc = Bc/CIR. So if Bc was 100Kbits and CIR 10Kbps then Tc would be computed as 10 (seconds) [while we will emulate this, Cisco's algorithms may not actually permit these values as 10s is huge]. In this example, a 10 second Tc would mean that we could send, depending on linkspeed, all of our 100 Kbits in the first second - we could then not transmit any more information until Tc expires (9 seconds later) and our bucket is refreshed. Thus temporarily in the first second we will have exceeded CIR (but not Linkspeed)
Queue Length Packets	The maximum queue size for the Class in packets. So when Bc (Shape Average) or Bc + Be (Shape Peak) is exhausted packets will queue until this queue is exhausted. NOTE that this lead to large latencies if the queue is large compared to CIR
Use Spare Third Party Bandwidth	If this is checked then after the class has used up its bandwidth it can use the spare bandwidth of other classes. The priority order is in class row order i.e. if class 2 is defined before class 1 in the QoS Class table it will get first call on spare bandwidth if this is checked. If unchecked the class can only use bandwidth (CIR) specifically allocated to it even if the link is underutilized.
Desc	This is a textual description where you can (optionally) document the purpose of that class e.g. Voice Traffic.

Be careful that if all the QoS Classes **CIR**s add up to more than the Link **CIR** then the classes cannot all get the promised bandwidth, instead Class Packets will be queued in the Link buffer.

1-1-4. Cisco QoS Class Bandwidth (Expression)

This function is the expression version of *Cisco QoS Class Bandwidth (Labs)* – equivalent to that function but using Wireshark like expressions for classification instead the properties of the original QoS Class Filters table.

Thus, the Expression version of the **QoS Class Filters** table only has these fields:

- **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE.
- **Use Last Hop as Port In** – modifies Port In to be the name of the immediately previous Object (VI) or Port the packet just came from
- **Class Expression** – A valid "Wireshark like" expression (see *Expression Library Functions* on page 734 in *Appendix 1*, *Specifying Expressions* for details).
- **QoS Class Id** – The number of the QoS Class (1,2,3,...) being defined by this filter.
- **QoS Class Disabled** - If ticked (checked) then this QoS Class is disabled i.e. not in use, as though it's deleted.

The class fields and general behavior are identical to *Cisco QoS Class Bandwidth (Labs)* class described above.

1-2. Bit Error Functions

The functions in the following sub-sections create bit errors in a packet

1-2-1. Error with Burst

Here you can specify the bit error rate (BER) to apply as 1 in X. Error rates can be as small as 1 in 10^{16}.

You can optionally set a deviation so that errors will not occur exactly at the BER specified but rather within a deviation Window specified.

You can also optionally set a Burst Error Rate (BER). This is a higher (or possibly lower) BER which will occur at the specified intervals (Interval Between Bursts) and optionally make these intervals have a random deviation interval. Lastly you can set the burst duration which needs to be non-zero to makes bursts meaningful.

Mimics a steady bit error rate and then a random burst on top providing realistic packet corruption when noise hits a network. Particularly good for wireless and satellite circuit testing.

1-2-2. Poisson Error

Here you can tell it to create a Bit Error in a Poisson process manner – you supply the mean (average) number of bit errors, the time interval which that mean value applies to and a time window in which a bit must arrive after the Poisson timer expires to be errored.

In the real world, when not bursty, bit errors occur according to the Poisson distribution as opposed to normal or uniform distribution.

1-2-3. Random Packet Error

Thus function creates bit errors on a packet basis. Supply a percentage of the packets that you want to have an error (at random). A bit error will then be randomly generated for that packet.

Ensures a certain proportion of packets are corrupted and is as likely to corrupt a small packet as a big one. Good for stress testing in packet error situations to determine if the protocol or application can cope.

1-2-4. Random Packet Corrupt

This function corrupts packets on a random basis specified by a Percentage value. There is a table of corruptions to apply which include **add**ing, **sub**tracting, **and**ing, **or**ing, **xo**ring or overwriting any specified bytes in the packet.

1-3. Debug Functions

The functions in the following sub-sections are used for debugging.

1-3-1. Debug

This function can be very useful in tracing packets within the network. The options are to:

- Turn Dump Packet On and Off
- If Dump Packet is on decide how many bytes of each packet you want to dump

Debug information is written to the file `/Run Data/<network name>/<network name>.log`, from where it can be viewed or downloaded via the Fie Browser.

1-3-2. Debug (Labs)

There is also a more advanced form of the Debug function in the Labs module which has the same parameters as above but provides more detail than the Debug function in the Default module. It especially has information about fragmentation flags in the IPv4 header.

It also writes debug information to the file `/Run Data/<network name>/<network name>.log`, from where it can be viewed or downloaded via the Fie Browser.

1-3-3. Debug (Expression)

This is the most advanced form of Debug

As with the other forms of debug, this function can be very useful in tracing packets within the network.

The options are to:

- Turn Dump Packet On and Off
- If Dump Packet is on decide how many bytes of each packet you want to dump in hex format. This will slow packet processing down so should only be used when needed
- Turn Interpret_Packet On and Off. Turn this on to Interpret Packet Structure, using Protocol definitions.
  Note: this will slow the NE-ONE down and so should not be used when high speed traffic is flowing.
- Filter_Expression - Set up a Wireshark like filter expression e.g. `ipv4.src & 255.255.255.0 = 192.168.1.0` would dump only packets matching this criterion (packet source in ipv4 subnet 192.168.0.1). An empty filter dumps all packets (provided one of Dump_Packet and/or Interpret_Packet are checked. More information on expressions is described in *Expression Library Functions* on page 734 of *Appendix 1*, *Specifying Expressions*.

1-4. Duplicate Functions

Functions in this section are generally about duplicating packets, but they may do more than that.

1-4-1. Packet Move and Duplicate

This function moves a random percentage of packets between a Minimum and Maximum distance from their current position. If duplicate is set to True then it duplicates the randomly chosen packet and moves the duplicate, leaving the original packet where it was in the stream.

This is useful for creating duplicates that are not necessarily next to the packet they are cloned from. It can be used as a simple duplicate function by setting the minimum and maximum move distance to 0.

Allows more realistic testing than simple duplication because the duplicated packet can be held and inserted randomly in the traffic flow and not behind the original. Good for certain cyber/crypto testing.

1-5. Filter Functions

Here you can set an array (list) of filters on the traffic. Filters allow you to decide how to handle traffic. The choices are:

- Impede – affect the packet using the latency, loss, error, bandwidth etc. functions in this VI (note all traffic obeys the routing functions, unless dropped)
- Drop – drop the traffic that matches this filter
- Pass – Route the traffic on to the next VI using the routing function without applying any impairment like latency, loss, error, bandwidth etc.

The filter functions are described in the following sub-sections.

1-5-1. Generic Filter

This is a very comprehensive function. You can use this to Filter by any or all of:

- Source and/or Destination IP (v4 or V6) Address – lists and ranges Source and/or Destination TCP/UDP Port – lists and ranges VLAN Id (802.1Q VLAN tag) – lists and ranges
- Received hardware or soft port
- Or Last hop port or network object (link or node)

For each Filter you can Drop, Pass or Impair traffic as defined earlier. The default behavior is to Impair all traffic.

1-5-2. Composite Filter (Labs)

This function extends Generic Filter having all the options of Generic Filter plus:

- IP Protocol – lists and ranges
- DPI – Deep packet inspection – you can match one or more bytes or bits anywhere (header and data)

in the packet with DPI rules

For each Filter you can Drop, Pass or Impair traffic as defined earlier. The default behavior is to Impair all traffic.

1-5-3. Composite Filter with NAT (Labs)

This function extends Composite Filter allow you to optionally change the Source or Destination IP address of a packet or their Source or Destination TCP/UDP ports.

Checksums are recomputed so that if an address or port is changed the packet will be valid. Use this for redirecting traffic to a different host or different port.

You will need a NAT filter on the way back to restore the IP address and or Port so the client/server believes that the original one fulfilled the request.

Note:

Certain protocols like FTP embed addresses (essentially as text) in some of their commands. These will not work with this function, as the NAT implementation does not fix up addresses and ports held in the data part of a packet, or act as a proxy.

This function has been tested to work with ICMP, HTTP and HTTPS (in the case of the latter two address and ports were changed successfully.

1-5-4. Expression Filter with NAT (Expression)

This function is the expression library counterpart of *Composite Filter with NAT (Labs)* described above.

In this function filter rules are defined by Wireshark like expressions, rather than by tables or lists (as in Generic Filter, Composite Filter or Composite Filter with NAT). See the*Expression Library Functions* on page 734 of *Appendix 1*, *Specifying Expressions* for more on the syntax.

Once defined, as for all other filter functions, for each defined Filter you can Drop, Pass or Impair traffic as defined in *Filter Functions* on page 750). The default behavior is to Impair all traffic.

You can also optionally change (NAT) the Source or Destination IP address of a packet or (PAT) their Source or Destination TCP/UDP ports.

Checksums are recomputed so that if an address or port is changed the packet will be valid. Use this for redirecting traffic to a different host or different port.

You will need a NAT filter on the way back to restore the IP address and or Port so the client/server believes that the original one fulfilled the request.

Note:

Certain protocols like FTP embed addresses (essentially as text) in some of their commands. These will not work with this function, as the NAT implementation does not fix up addresses and ports held in the data part of a packet, or act as a proxy.

This function has been tested to work with ICMP, HTTP and HTTPS (in the case of the latter 2 address and ports were changed successfully.

1-6. Fragment Functions

1-6-1. Fragment MTU

This function deals with IPv4 fragmentation where packets are too large for the MTU.

You specify the parameter **MTU_Limit** (the default value is 0, meaning that the MTU will not be checked) and any IPv4 packets over this size limit will be fragmented to smaller packets which are no bigger than this value. How this behaves is dependent on a second parameter: Do not Fragment Flag Option (sic) which deals with special cases where the Packet's don't fragment flag is set.

Emulates what happens in the real-world and allows applications' and protocols' ability to efficiently reassemble the fragmented packet to be tested.

1-7. Latency Functions

These functions control **latency (delay)** applied to packets, this delay can be varied by the various functions available to produce **Jitter**.

Note:

Because network objects (nodes and links) are unidirectional, if you want to create a delay of 70 ms RTT (Round Trip Time), for example, you must divide this into 35 ms in one direction (on one object) and 35 ms in the other (on the object handling the return flow). If you know the 70 ms RTT is asymmetric then you can use the known asymmetric values instead of halving the RTT.

1-7-1. Gaussian Delay

This function uses the Gaussian distribution (also called the Normal Distribution) for delay. It is one of the most realistic delay functions.

As you would expect you can specify the **Mean** (average) for the delay, as well as the **Standard Deviation** (how much the delay will vary i.e. **Jitter** around the mean).

You can also set the **Minimum Delay** which is the minimum delay that will be applied to a packet, no matter what the normal distribution would calculate. This is very important as all real network circuits have a **base delay** which is the smallest delay you'll ever see in those networks. This base delay usually comes from the route that the circuit takes as well as fixed (non-queuing) delays equipment imposes. To find the base delay of a circuit we are looking for the minimum RTT ever seen for that circuit

A **Maximum Delay** can also be specified which is the maximum delay that will be applied to a packet, no matter what the normal distribution would calculate. This is mostly to stop outrageously large values because in the Gaussian distribution such values are possible (though improbable).

This is probably the most real-world delay impairment but the minimum and maximum delay parameters ensure a base network latency (which is realistic) and rejects low probability but ridiculously high latencies. Creates Gaussian Jitter.

1-7-2. Step Delay Periodic

This varies the delay on packets between a minimum and a maximum in specified Step increments where each step has specified time duration.

When the maximum is reached the steps come down by the Step increment until they get to minimum when the upward trend begins again.

Allows efficient stress testing of applications from a latency point of view to establish limits.

1-7-3. Step Delay Packet Nanoseconds

Description: Increments the delay between a minimum and maximum value specified in nanoseconds applying the step (in nanoseconds) for each packet. Applies a step latency beginning at Min Delay and going up to Max Delay in nanoseconds changing steps every packet. When Max is reached the steps come down to Min Delay and the process repeated.

Parameters: Min Delay; Max Delay; Step Delay.

Summary: Exposes any vulnerabilities to high latency and allows efficient stress testing to establish limits.

1-7-4. Random Delay Nanoseconds

Applies a random delay, between Maximum and Minimum (specified in nanoseconds), to each packet. To get a fixed delay set the minimum and maximum to the same value.

1-7-5. Fixed Delay

This function applies a fixed delay (i.e. no Jitter) to packets in the order of nanoseconds. This function would be used to create circuit delays which are distance or routing dependent and where variation does not occur. Lets you be exact about your delay (+/- 10 nanoseconds in practice) which is useful when

precision is required.

Note:

This impairment function exists for legacy purposes, and is planned to be deprecated (removed) in a future release. This impairment function is the same as the *Fixed Delay Nanoseconds* impairment function. Calnex recommend that you use the *Fixed Delay Nanoseconds* impairment function instead.

1-7-6. Fixed Delay Nanoseconds

This function applies a fixed delay (i.e. no Jitter) to packets in the order of nanoseconds. This function would be used to create circuit delays which are distance or routing dependent and where variation does not occur. Lets you be exact about your delay (+/- 10 nanoseconds in practice) which is useful when precision is required.

Note:

This impairment function is the same as the *Fixed Delay* impairment function, which will be deprecated (removed) in a future release. Calnex recommend that you use the *Fixed Delay Nanoseconds* impairment function rather than the *Fixed Delay* impairment function.

1-7-7. Fixed Delay Milliseconds

This function applies a fixed delay (i.e. no Jitter) to packets in the order of milliseconds. This function would be used to create circuit delays which are distance or routing dependent and where variation does not occur.

Compared to the *Fixed Delay Nanoseconds* impairment function who's value granularity is of the order of nanoseconds, this function gives you a higher precision of value granularity in the order of milliseconds.

Lets you be exact about your delay (+/- 10 milliseconds in practice) which is useful when precision is required.

1-7-8. Fixed Delay with Jitter (Labs)

Description: Applies a fixed base delay (latency) and random jitter (PDV).

Parameters: Base Latency; Max Jitter.

Summary: Lets you separately control base delay and maximum jitter.

1-7-9. Random Delay

Identical to Random Delay Nanoseconds with timing expressed in milliseconds (and decimal milliseconds). This is one of the most widely used delay function.

Lets you easily and quickly set random latency causing Jitter.

1-7-10.Delay Sequence (Labs)

This is a labs function which has a sequence (table) of triplet values:

- Base delay
- Jitter
- Duration

They are all specified in milliseconds.

You can specify the sequence and it will move through each Base Delay (minimum delay) with the jitter you specify holding those values for the duration and then moving on to the next Base Delay, Jitter and duration.

It will do this until it reaches the end of the sequence at which point it can go back to the beginning or stay at the last values, depending on whether repeat is set to true or false

This feature is intended to allow a variety of "burst delay scenarios".

1-7-11.Delay Scenarios (Labs)

Delay Scenarios allow you to pick from a range of pre-defined scenarios e.g.:

- LAN in Building
- LAN in Campus
- WAN Nearby Cities
- WAN Continental
- WAN Distant Cities
- WAN Cross Global Satellite
- etc.

Each of these has a predetermined real-world latency value (which is displayed) and you can add variation as **jitter** by specifying the **jitter interval**.

Finally you can also choose Manual to set your own latency value – jitter will apply in this case too.

Note:

Even though, that latencies are unidirectional – as is normal and correct. You need to set the corresponding latency in the return direction network object (node or link) to create the full RTT of a circuit.

1-7-12.City to City Latency

This is an internal function used and applied by the NE-ONE when you specify location (i.e. country and city) data on a pair of connected nodes in the **Edit node** panel of the Point-to-Point Designer (*Illustration 74* on page 249) or the **Edit node** panel of the Multi-Point Designer (*Illustration 88* on page 319).

This function automatically calculates a fixed delay (i.e. no Jitter) to packets in the order of milliseconds, based upon the locations that were defined for each of the connected nodes.

Note:

Calnex recommend that you do not edit the auto-calculated City to City latency within the Advanced Settings of a link. If you do not want the City to City latency to be automatically used and applied on links between a pair of connected nodes, do not specify the a location (i.e. country and city).

1-8. Loss Functions

The functions described in the following sub-sections control packet loss.

1-8-1. Packet Error 1 in X bits

This will drop a packet based on a specified bit error rate - BER (X) specified. As soon as an error bit hits a packet the packet will be dropped, as it is deemed that it would fail an intermediate CRC or Checksum verification, and so be dropped in transit. Be careful not to use small values of “loss X” as, for example 500 would drop a packet every 500 bits, which is 64 bytes, which will affect every packet.

This is common for networks that create bit errors. The drop simulates other equipment dropping the broken packet due to a checksum mismatch and is very realistic for mimicking satellite and certain wireless transmissions.

1-8-2. 1 in X

This drops 1 in every X packets exactly (i.e. keep X-1 packets then drop one etc.).

Provides a steady drop of 1 in x packets which is good for early testing of protocols and whether they can recover from certain amounts of loss.

1-8-3. Random Drop

This applies a random drop expressed as a percentage of packets, so 1% will drop approximately 1 in a

100 packets (randomly chosen).

The most commonly used drop function to simulate real world drops due to failure to queue etc. Provides a realistic symptoms of what happens when network links are busy and queues are full.

1-8-4. Poisson Drop

Here you can tell it to drop packets in a Poisson process manner – you supply the mean (average) number of packets dropped, the time interval which that mean value applies to and a time window in which a packet must arrive after the Poisson timer expires to be dropped.

Drops packets according to the Poisson distribution to mimic patterns often seen in the real world.

1-8-5. Burst Loss

This function has two loss levels:

- Normal
- Burst

Both are expressed as a percentage of packets (randomly chosen) to drop. Normal is usually a low value (or 0%) and Burst is normally a Higher value such as you would get in a burst of wireless noise. But you can use the parameters in any manner you wish.

You also set the burst's frequency (how often the bursts occur), and duration (how long the bursts last).

Developed for customers that need a random burst rather than period burst for testing dropped packets randomly followed by dropping several in a row - a random burst. Provides a very realistic test network for random bursts of noise, for example in wireless networks.

1-8-6. Random Drop with Burst

This function drops a packet on a random percentage basis that you specify as Loss Percent but once a packet has been selected the function can drop a whole sequence of packets in a row between minimum Packets to Drop (default 1) and Maximum Packets to drop (default 1). This sequence is the burst.

A simple way (without programming) to create networks that suffer periodic noise or high losses to determine the impact on application performance.

1-8-7. No Drop

Setting this stops all dropping. No drop parameters are checked so it operates very quickly on packets. This is a useful function when scripting.

1-8-8. Total Drop

Choosing this function sets 100% loss but as with No drop does not apply any parameters so it operates very quickly on packets. This is a useful function when scripting.

1-9. Out Of Order Functions

These functions primarily concern themselves with putting packets out of order, though it can be seen in *Packet Move and Duplicate* on page 750, that this can place duplicated packet specifically out of order.

1-9-1. Random Packet Time Reorder (Labs)

Description: Takes a packet out of the current stream on a random % basis (uniform distribution) - and holds it between a Minimum and Maximum time in milliseconds.

Parameters: Move Percent; Minimum Time; Maximum Time.

Summary: Used to test protocol resilience and exposes application inadequacies e.g. Jitter buffer ability to efficiently put packets back into order. It is likely that you would have to wait a long time to see this in the real world.

1-9-2. Random Packet Move Offset

Description: Takes a packet out of the current stream on a random % basis (uniform distribution), and

moves it backwards randomly between the defined Minimum and Maximum packet position (in packet terms).

Parameters: Move Percent; Minimum Move; Maximum Move.

Summary: Used to test protocol resilience and exposes application inadequacies e.g. Jitter buffer ability to efficiently put packets back into order. It is likely that you would have to wait a long time to see this in the real world.

1-9-3. Packet Reorder in X

Description: Takes the Xth packet out of the current stream, and moves it backwards randomly between the defined Minimum and Maximum packet position (in packet terms). The other X-1 packets move normally (i.e. unhindered).

Parameters: Xth packet; Minimum Move; Maximum Move.

Summary: Used to test protocol resilience and exposes application inadequacies e.g. Jitter buffer ability to efficiently put packets back into order. It is likely that you would have to wait a long time to see this in the real world.

1-10. Pause Functions

1-10-1.Pause Transmission (Labs)

This function is designed to pause the transmission of packets being sent out from this object (either to another object, or to a hardware or soft port) for an amount of time (the Pause Time).

Packets will continue to be queued for transmission when the object transmission is paused, so that if, for example, the bandwidth function Linkspeed and Fifo Queue Bytes is used, then packets will fill its queue until the queue is full; after this packets will be dropped by that function.

This function has one parameter:

- **Pause Time** - specified in milliseconds (ms)

  After Pause Time milliseconds has passed the Object will continue to transmit again as normal.

  If the function is updated while already in a paused state then the old Pause Time is overridden by the new value supplied. If the new value supplied is 0 then any existing Pause is turned off.

Note:

For legacy purpose this the Pause Transmission (Labs) function is retained on the NE-ONE. You may want to still use it with the API, however, Calnex recommend that you use the Pause Transmission Repeat (Labs) function described below.

1-10-2.Pause Transmission Repeat (Labs)

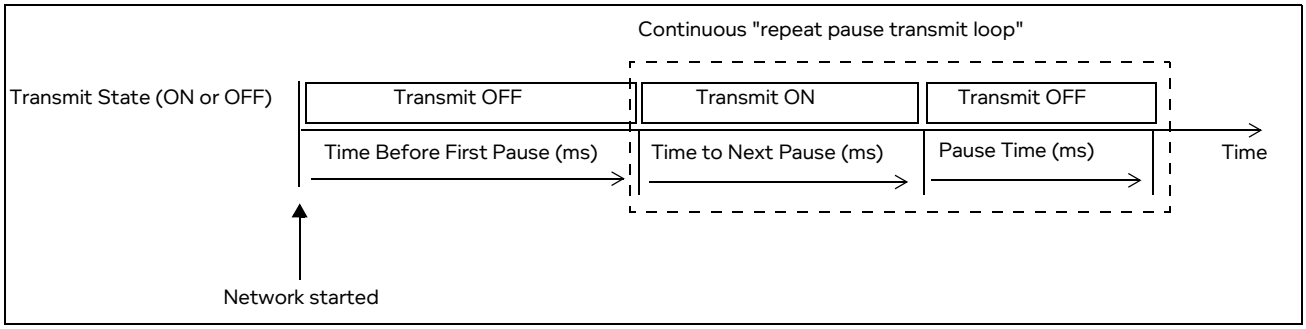
This function (see *Illustration 235*) is designed to pause the transmission of packets being sent out from this object (either to another object, or to a hardware or soft port) initially for an amount of time (the Time Before First Pause), then do one of the following:

- continue to transmit again as normal (if the **Repeat** check box is un-ticked) - in this case it is acting like the legacy Pause Transmission (Labs) function
  or
- repeatedly transmit and pause in a loop for the defined Time to Next Pause with pause a of the defined Pause Time and Time to Next Pause (if the **Repeat** check box is ticked)

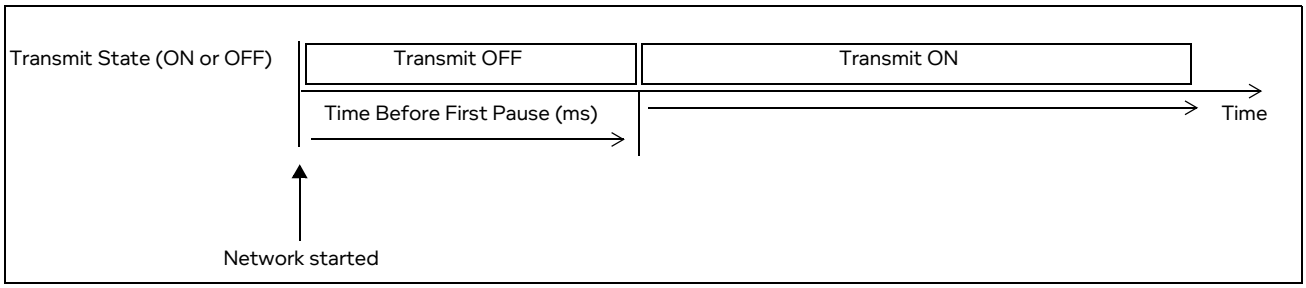
Packets will continue to be queued for transmission when the object transmission is paused, so that if, for example, the bandwidth function Linkspeed and Fifo Queue Bytes is used, then packets will fill its queue until the queue is full; after this packets will be dropped by that function.

ILLUSTRATION 235 - REPRESENTATION OF THE PAUSE TRANSMISSION REPEAT FUNCTION

When Repeat is ON (**Repeat** check box ticked) - the repeat pause transmit loop is in continuous effect



When Repeat is OFF (**Repeat** check box un-ticked) - the repeat pause transmit loop is inactive and the function transmits continuously after the Time Before First Pause



This function has the following parameters:

- **Time Before First Pause** - specified in milliseconds (ms)

  After the Time Before First Pause milliseconds has passed the Object will then do one of the following:

  - continue to transmit again as normal (if the **Repeat** check box is un-ticked)
    or
  - repeatedly transmit in a loop for the defined Time to Next Pause with pause a of the defined Pause Time and Time to Next Pause (if the **Repeat** check box is ticked)

- **Pause Time** - specified in milliseconds (ms)

  This parameter defines the repeat pause transmit loop of the function, and is in effect if **Repeat** check box is ticked.

  After the Pause Time milliseconds has passed the Object will continue to transmit again as normal until the defined Time to Next Pause milliseconds is reached.

- **Time to Next Pause** - specified in milliseconds (ms)

  This parameter defines the repeat pause transmit loop of the function, and is in effect if **Repeat** check box is ticked.

  After the Time to Next Paused milliseconds has passed the Object will stop transmitting until the defined Pause Time milliseconds is reached.

- **Repeat** check box - ticked (ON) or un-ticked (OFF)

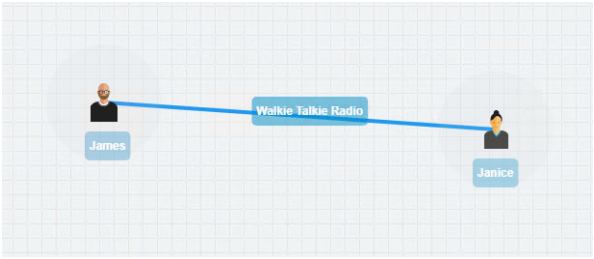
  This parameter determines whether the repeat pause loop of the function is active (ON) or inactive (OFF). If the **Repeat** check box is ticked, the repeat pause transmit loop is active and in effect according to defined the Pause Time and Time to Next Pause parameters. If the **Repeat** check box is un-ticked, the repeat pause transmit loop is inactive and the function continues to transmit normally after the defined Time Before First Pause.

Note:

If the function is updated while already in a paused state then the old Pause Time and Time to Next Pause parameters are overridden by the new values supplied.

The Pause Transmission Repeat (Labs) function is useful for simulating half-duplex communication. For example, if you wanted to simulate half-duplex walkie-talkie communication between two users (James and Janice), you could configure them in a synchronized half-duplex communication schema using the Pause Transmission Repeat (Labs) function as shown in *Illustration 236*. In both examples, the conversation between James and Janice starts after 10 seconds (10000 ms).

ILLUSTRATION 236 - PAUSE TRANSMISSION REPEAT WALKIE-TALKIE EXAMPLES



Example 1 : James talks more than Janice during the conversation

Configuration on James node:		Configuration on Janice node:
Properties - Pause Transmission Repeat (Labs)		Properties - Pause Transmission Repeat (Labs)
Time Before First Pause: 10000.0	Conversation starts after 10s	Time Before First Pause: 10000.0
Pause Time: 1000.0	James listens for 1s / Janice listens for 2.5s	Pause Time: 2500.0
Time to Next Pause: 2500.0	James talks for 2.5s / Janice talks for 1s	Time to Next Pause: 1000.0
Repeat		Repeat

Example 2 : James and Janice talk for an equal amount of time during the conversation

Properties - Pause Transmission Repeat (Labs)		Properties - Pause Transmission Repeat (Labs)
Time Before First Pause: 10000.0	Conversation starts after 10s	Time Before First Pause: 10000.0
Pause Time: 1500.0	James listens for 1.5s / Janice listens for 1.5s	Pause Time: 1500.0
Time to Next Pause: 1500.0	James talks for 1.5s / Janice talks for 1.5s	Time to Next Pause: 1500.0
Repeat		Repeat

In the first example, we see that the Pause Transmission Repeat (Labs) function is configured in such a way that during the conversation, James talks more than Janice (i.e. 2.5 seconds (2500 ms) opposed to 1 second (1000 ms).

In the second example, we see that the Pause Transmission Repeat (Labs) function is configured in such a way that during the conversation, James and Janice talk equally for the same amount of time (i.e. 1.5 seconds (1500 ms)).

2. AVAILABLE NODE FUNCTIONS

The sections below summarize each of the node functions, organized by their category.

Node functions are only available in the Multi-Point Network Designer (i.e. not the Point-to-Point Network Designer), and can be used to create more sophisticated networks.

The node functions available include all of the same impairment functions described in *Available Impairment Functions* on page 743. However, in addition to those impairment functions, the node function also include those described in the section below.

2-1. Cloud

2-1-1. Cloud Object (Labs)

This is a composite impairment function.

This function effectively implements multiple (though simplified) sub-VIs (paths) within a single object. It therefore can represent a complete network of paths as in the Internet or an MPLS network with either a Full or Partial Mesh. Parameters are entered into a single table called Cloud.

Fields in the cloud table are divided into two parts:

- Impairment Fields
- Selection Fields

The Cloud object works by comparing the current packet's selection fields with the Cloud table row, and if they match applying the impairment fields in the same row. If the row does not match on the selection fields the next row is tried, and so on until the end of the table.

If the packet does not match any rows field in the table it is dropped.

To create a "catchall" row simply set up the last row in the table without any selection fields (which means it will match anything); just set the impairment fields you want.

The next two sub-sections document the Impairment and Selection fields in each cloud row.

2-1-1-1. Cloud Impairment Fields

Link Id – This is not strictly an impairment field but does occur first, before bandwidth in the GUI and so is listed here. This needs to be set to a unique value per cloud row to enable the NE-ONE to locate rows that have been updated, deleted and reordered, preserving currently queued packets, where appropriate. Link Ids do not need to be consecutive but must be greater than 0 and less than 1,000,000.

Bandwidth – The maximum bandwidth (in bps) that this traffic can have (0 means unregulated – effectively infinity, not no bandwidth – if no bandwidth is required please use 100% Loss instead).

Latency – This is the base delay in (decimal) milliseconds to apply to the packet.

Jitter – This is a random additional delay (in milliseconds) to be added to the Latency. For each packet a value between 0 and Jitter is randomly added to Latency and the packet is delayed by the combined delay value.

TTL Cost – This value is subtracted from the Packet's IP Time-to-Live (TTL) value and the packet's IP checksum is recomputed to be valid. If the packet's checksum is <= 0 after the subtraction the packet is dropped.

Loss – This is a (decimal) percentage loss (between 0 and 100) which is applied to each packet at random. It represents a loss probability e.g. if it was 10 then 10 in every 100 (10%) of packets would be lost at random.

Queue Length – This sets the queue size for bandwidth purposes for this cloud row. If a packet cannot be immediately transmitted it is queued in this queue. Eventually if there is no space in the queue the packet is dropped. The default queue size is 64000 bytes.

2-1-1-2. Cloud Selection Fields

This function allows selection by lists, ranges or list of ranges of:

- **Port In** – The hardware (0, 1, 2...) or soft port on which the packet originally entered the NE-ONE.
- **Use Last Hop as Port In** – modifies **Port In** to be the name of the immediately previous network object (link or node) or port (hardware or soft) the packet just came from.
- **Source IP Address** – the IPv4 or IPv6 address or range where the packet has come from e.g. for TCP/IP 192.168.1.1-192.168.1.255
- **Dest IP Address** - the IPv4 or IPv6 address or range where the packet is going to e.g. 192.168.2.10
- **Source Port** – which port the packet has come from e.g. for TCP/IP 6000, 6001
- **Dest Port** – which port the packet is going to e.g. 80 (HTTP), 443 (HTTPS), 25 (smtp), 21 (ftp), 110 (pop3), 445 (Microsoft-ds – Network File Access)
- **IPv4 Protocol** – the IP (v4 or v6) protocol of the packet e.g. 0 (Not IP) 1 (ICMP), 6 (TCP), 17 (UDP), 47 (GRE) etc.
- **VLAN Id** – 802.1Q VLAN label (tag), if the packet is VLAN tagged.
- **DPI** – (Deep Packet Inspection) select a packet for this cloud row based on one or more bytes or bits in the header or data part of the packet.
- **Trace** - checking this box will write packet trace information to the emulation log file for this cloud row.
  Note: This should not be left on when not required as tracing greatly slows packet flow.
- **Capture** - check this box will capture packets in pcap format for this cloud row to the with the following file format:
  pcap_<Object name>_LinkId_<cloud link id>_desc_<cloud link description>
  (for example `pcap_Cloud2_LinkId_100_desc_dst 5.1.pcap`) in the `/Run Data/<network name>` directory from where it can be downloaded using the File Browser).
  Note: Packet capturing cloud rows slows down packet processing.
- **Disabled** - If ticked (checked) then this Cloud Row is disabled (i.e. not in use).

2-1-2. TDMA Mesh (Labs)

This is a composite impairment function.

This function effectively implements a TDMA Mesh used in Time Division Multiple Access (TDMA) networks. The implementation of the TDMA Mesh is described in more detail in *Editing the TDMA Mesh Properties of a Node via the Mesh Properties Window (Multi-Point Networks)* on page 360.

This function effectively implements multiple TDMA mesh links within a single TDMA Mesh object.

The following two TDMA Mesh constants are defined in the **TDMA Mesh Node Properties** window (*Illustration 109* on page 362):

- **Slot Length** - defines the slot length (in ms) for the TDMA Mesh.
- **Number of Slots** - defines the number of slots for the TDMA Mesh. The cycle time of the TDMA Mesh = number of slots x slot length.

Note:

It is recommended to set a maximum number of slots to "future proof" the capacity (i.e. cycle time (slot length x number of slots) of your TDMA configuration without the need to change it later on. The NE-ONE will implement the same cycle time and the unused slots are still present in the cycle. This lets you add additional end nodes at a later time on the unused slots, and thus future proof your TDMA implementation on the NE-ONE.

End nodes connected to the TDMA Mesh can always receive data during the entire cycle time of the TDMA Mesh. However, end nodes connected to the TDMA Mesh can only transmit data into the TDMA

Mesh when their allocated slot(s) passes by during the cycle time.

Parameters are entered into a single table called TDMA Mesh.

Fields in the TDMA Mesh table are divided into two parts:

- Impairment Fields
- Selection Fields

The TDMA Mesh works by comparing the current packet's selection fields with the TDMA Mesh table row, and if they match applying the impairment fields in the same row. If the row does not match on the selection fields the next row is tried, and so on until the end of the table.

If the packet does not match any rows field in the table it is dropped.

The next two sub-sections document the Impairment and Selection fields in each TDMA Mesh row.

2-1-2-1. TDMA Mesh Impairment Fields

Link Id – This is not strictly an impairment field but does occur first, before bandwidth in the GUI and so is listed here. This needs to be set to a unique value per TDMA Mesh row to enable the NE-ONE to locate rows that have been updated, deleted and reordered, preserving currently queued packets, where appropriate. Link Ids do not need to be consecutive but must be greater than 0 and less than 1,000,000.

Slot List – This is not strictly an impairment field but does occur second, before bandwidth in the GUI and so is listed here. This is a mandatory parameter, and defines the slots allocated to the selected end node (**Node In**). Each end node uses a unique slot list (i.e. you cannot use the same slot number for a different end node). You must use valid slot numbers. For example if the **Number of Slots** field in the **TDMA Mesh Node Properties** window (*Illustration 109* on page 362) is 128, then the valid slot numbers are 0 - 127. The more slots you list for the selected end node (Node In), the larger their "transmission window" into the TDMA Mesh is. For example, if you assign four slots 0,1,2,3 to an end node, its transmission window will be 4 x the slot length (in ms), where the slot length is defined by the Slot Length field in the TDMA Mesh Node Properties window (*Illustration 109* on page 362).

Bandwidth – The maximum bandwidth (in bps) that this traffic can have (0 means unregulated – effectively infinity, not no bandwidth – if no bandwidth is required please use 100% Loss instead).

Latency – This is the base delay in (decimal) milliseconds to apply to the packet.

Jitter – This is a random additional delay (in milliseconds) to be added to the Latency. For each packet a value between 0 and Jitter is randomly added to Latency and the packet is delayed by the combined delay value.

TTL Cost – This value is subtracted from the Packet's IP Time-to-Live (TTL) value and the packet's IP checksum is recomputed to be valid. If the packet's checksum is <= 0 after the subtraction the packet is dropped.

Loss – This is a (decimal) percentage loss (between 0 and 100) which is applied to each packet at random. It represents a loss probability e.g. if it was 10 then 10 in every 100 (10%) of packets would be lost at random.

Queue Length – This sets the queue size for bandwidth purposes for this TDMA Mesh row. If a packet cannot be immediately transmitted it is queued in this queue. Eventually if there is no space in the queue the packet is dropped. The default queue size is 64000 bytes.

2-1-2-2. TDMA Mesh Selection Fields

This function allows selection by lists, ranges or list of ranges of:

- **Node In** – The end node on which the packet originally entered the TDMA Mesh. This is a mandatory parameter and selects the end node for which you want the defined **Slot List** apply. This defines the end node coming into the TDMA Mesh to filter on. For each end node connected to the TDMA Mesh, you must create a TDMA Mesh link, and select that end node from the **Node In** drop-down field.

- **Use Last Hop as node in** – modifies **Node In** to be the name of the immediately previous end node the packet just came from.
- **Source IP Address** – the IPv4 or IPv6 address or range where the packet has come from e.g. for TCP/IP 192.168.1.1-192.168.1.255
- **Dest IP Address** - the IPv4 or IPv6 address or range where the packet is going to e.g. 192.168.2.10
- **Source Port** – which port the packet has come from e.g. for TCP/IP 6000, 6001
- **Dest Port** – which port the packet is going to e.g. 80 (HTTP), 443 (HTTPS), 25 (smtp), 21 (ftp), 110 (pop3), 445 (Microsoft-ds – Network File Access)
- **IPv4 Protocol** – the IP (v4 or v6) protocol of the packet e.g. 0 (Not IP) 1 (ICMP), 6 (TCP), 17 (UDP), 47 (GRE) etc.
- **VLAN Id** – 802.1Q VLAN label (tag), if the packet is VLAN tagged.
- **DPI** – (Deep Packet Inspection) select a packet for this cloud row based on one or more bytes or bits in the header or data part of the packet.
- **Trace** - checking this box will write packet trace information to the emulation log file for this TDMA Mesh row.
  Note: This should not be left on when not required as tracing greatly slows packet flow.
- **Capture** - check this box will capture packets in pcap format for this TDMA Mesh row to the with the following file format:
  pcap_<Object name>_LinkId_<tdma mesh link id>_desc_<tdma mesh link description>
  (for example `pcap_TDMA_LinkId_100_desc_dst 5.1.pcap`) in the `/Run Data/<network name>` directory from where it can be downloaded using the File Browser).
  Note: Packet capturing TDMA Mesh rows slows down packet processing.
- **Disabled** - If ticked (checked) then this TDMA Mesh Row is disabled (i.e. not in use).

3. AVAILABLE PACKET INPUT FUNCTIONS

The packet input functions let you to add additional traffic into your SDTNs by replaying selected packet streams from a packet capture (pcap) file, via the use of the following packet input functions:

- *Passive Packet Replay (Labs)*
- *Intelligent Packet Replay (Labs)*

3-1. Passive Packet Replay (Labs)

The Passive Packet Replay function "passively" replays the selected packet streams, and does not care if the packets with the packet stream that are sent from the initiator endpoint node are received by the responder endpoint node. The original conversation (i.e. packet stream) from the pcap file will carry on playing out even if the packets are lost, slowed down, or arrive in the wrong order. In this case, the order of the packets from the original conversation (i.e. packet stream) from the pcap file are not respected. This function can be applied on nodes, and contains the following parameters:

- **Path** - the path to the pcap file within the NE-ONE file system that will be replayed.
- **Running** (ON or OFF) - determines whether or not the pcap file is currently being replayed while the network is running.
- **End Action** (Stop or Loop) - determines what action to take once the pcap file has finished being replayed.
- **Loop Times** - defines how many times the pcap file is looped during the packet replay. Setting this to 0 is the equivalent to infinite.

- **Filters** - optionally lets you define a list of filters (e.g. source and destination IP addresses), that are applied on the packets within the pcap file being replayed.
- **Filter Action** (Pass or Drop) - determines the action to use on the filtered packets from the pcap file being replayed.
- **Speed Multiplier** (default 1) - This is a multiplier that lets you redefine the delay between sending packets. The default value is 1, which is the normal, correct delay between the packets in the original pcap file.
  - A decimal value or integer value higher than 1 (e.g. 1.3, 2, etc.) reduces the delay between sending packets by that speed multiplier factor, and thus each packet is sent on a quicker time line than in the original pcap file. This is useful when you want to intensify the original delay between sending the packets compared to the original pcap file.
  - A decimal value less than 1 (e.g. 0.7, 0.5, etc.) increases the delay between sending packets by that speed multiplier factor, and thus each packet is sent on slower time line than in the original pcap file. This is useful as it lets you easily observe in detail what is happening to the packets on a slower timescale without missing vital information. If you find that the packet data scrolls too quickly in the **Live Packets** dialog box (see *Illustration 163* on page 542) and **Live Packet Monitoring** page (see *Illustration 164* on page 545) you can use this multiplier with a decimal value less than 1 to slow down the rate at which the packet data scrolls.

The parameter descriptions above are high-level. For examples on how to use them in more detail, see *Packet Replay Examples* on page 652 within *Chapter 15*, *Packet Input Functions*.

3-2. Intelligent Packet Replay (Labs)

The Intelligent Packet Replay function "intelligently" replays the selected packet streams by monitoring the initiator and responder endpoint nodes. It knows when the responder endpoint node receives a packet from the initiator endpoint node so that the initiator endpoint node can send the next packet in original conversation (i.e. packet stream). In this case, the order of the packets from the original conversation (i.e. packet stream) from the pcap file are respected, and TCP backoff is recreated under the network conditions of the SDTN.

This function can be applied on nodes, and contains the same parameters as the *Passive Packet Replay (Labs)* function described above.

The parameter descriptions above are high-level. For examples on how to use them in more detail, see *Packet Replay Examples* on page 652 within *Chapter 15*, *Packet Input Functions*.

This page is intentionally left blank.

APPENDIX 3 AVAILABLE LINK TYPES AND LINK SUB-TYPES

This appendix provides a summary of the current list of link types and link sub-types that are delivered with the NE-ONE, and that can be used when creating links for Point-to-Point and Multi-Point networks. *Table 84* lists the link types and subtypes supported by the NE-ONE at the time of publication.

Note:

As network technologies evolve, Calnex keep NE-ONE link types and subtypes up-to-date via software updates. For unparalleled product support (i.e. updates and on-line support), Calnex recommends that you keep your maintenance contract up-to-date. An active maintenance contract lets you update the NE-ONE link types and subtypes when new network technologies become available.

TABLE 84 - AVAILABLE LINK TYPES, LINK SUB TYPES, AND LINK QUALITIES

Type	Subtype	Link Quality
LAN	10 Gb/s	Ideal, Excellent, Good, Average, Poor
	1 Gb/s	
	200 Mb/s	
	100 Mb/s	
	50 Mb/s	
	Custom	
WAN	OC3	Excellent, Good, Average, Poor
	155Mb/s	
	T3/DS3	
	E3	
	10 Mb/s	
	E1	
	T1	
WI-FI	AC - 1300Mb/s	Excellent, Good, Average, Poor
	N - 600Mb/s	
	N - 300Mb/s	
	N - 150Mb/s	
	56Mb/s	
	11Mb/s	
ADSL	Fast	Excellent, Good, Average, Poor
	Medium	
	Slow	
SDSL	Fast	Excellent, Good, Average, Poor
	Medium	
	Slow	
2G	GPRS	Excellent, Good, Average, Poor

Type	Subtype	Link Quality
3G	Fast	Excellent, Good, Average, Poor
	Medium	
	Slow	
4G	Fast	Excellent, Good, Average, Poor
	Medium	
	Slow	
5G	Fast - standards level	Ideal, Excellent, Typical, Busy
	Medium - in practice	Excellent, Typical, Busy
	Slow - highly loaded	Typical, Busy
Satellite	GEO - 1Mb/s	Excellent, Good, Average, Poor
	GEO - 512Kb/s	
	GEO - 64Kb/s	
	MEO - 1Mb/s	
	LEO - 1Mb/s	

Revision History

Date	Reference	Reason for change
19/02/2021	Revision 1	Initial 2021 Release.
04/01/2022	Revision 2	Updates for Beta release.
01/03/2022	Revision 3	Updates for March 2022 release.
28/06/2022	Revision 4	Updates for Calnex re-branding and feature updates.
20/02/2023	Revision 5	Updates for packet replay functions, plus other minor updates.
31/03/2023	Revision 6	Updates for packet replay functions (IPR).
20/11/2023	Revision 7	Feature updates and defense pack update.
26/01/2024	Revision 8	V2 LCD panel updates.

User Feedback

To help us continually improve the quality of this Technical Publication, we appreciate your input. Please answer the following questions, and fax or mail the completed questionnaire back to the address noted in *Contact Information* on page 14.

1. Is this Technical Publication easy to use?

2. Is the information presented in a clear and logical way?

3. Is the information accurate?

4. Would you like to see instructions for any additional procedures? Please list them in the space below.

5. Is there something you do not like about this Technical Publication ?

www.calnexsol.com