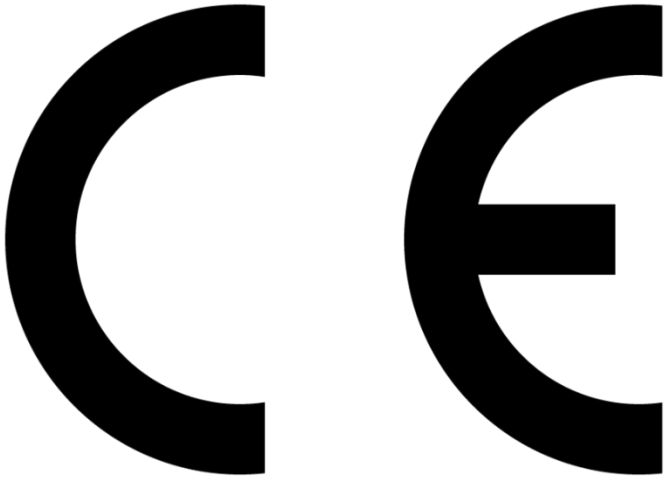
Operating Manual
Spirent Network Emulator

v3.0

Declaration of Conformity

Established following the Directive 2006/95/EC



We, hereby, certify that SNE complies with the dispositions of the European Community Directive for harmonized standards within the Member States related to low voltage (Directive 2006/95/EC).

Contact Information

If you need to contact us regarding the installation or use of the SNE, please do so using the following channels:

Online support: please visit our website https://www.spirent.com/

Telephone Technical Support: +1 800-774-7368

E-mail: support@spirent.com

Office:

Spirent Communications Inc.
2708 Orchard Parkway, Suite 20,
San Jose CA 95134
USA

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 Spirent Communications.

Spirent 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.

Spirent 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: changes/additions/deletions of user information (which is displayed, for example, to users via pop up boxes in the GUI) are not covered by Spirent warranty, and Spirent accepts no responsibility for incorrect or inaccurate translations and any impact that results from this.

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

Trademarks

SNE® is a registered trademark of Spirent Communications. Other trademarks are the property of their respective owners

Table of Contents

1. Safety Notices 7
3. Company Profile 10
4. Unpacking and Installation 10
5. SNE at a glance 11
6. Getting Connected 14
6.1. Pre-installation Notes 14
6.2. Tools and Cables Required 14
6.3. Installation 14
6.4. Hardware: 14
6.5. Installing the GUI Software: 15
6.6 Installing your license key 15
6.7 First time access to SNE 15
7 Positioning SNE Hardware 17
7.1 LAN Configuration Walk Through 18
8 SNE Graphical User Interface: Overview 20
8.1 GUI Overview 22
8.2 Multi-Emulator Usage 23
8.2.1 Launching maps on different emulators 24
8.2.2 Limitations 24
8.3 Map Menu Bar 25
8.3.1 Toggle Tool (on/off) 25
8.3.2 Timeline (Auto-Change) Feature 26
8.3.3 Snapshot Report 29
10 Creating Your First Emulation Run 31
10.1 Introduction 31
10.2 Step 1 – Changing a map name 32
10.3 Step 2 – Adding an impairment 32
10.4 Step 3 – Adjusting an impairment's settings 33
10.5 Step 4 – Running an emulation 34
10.6 Step 5 – Making Live Changes 36
10.6.1 Live Impairment Changes 36
10.7 Step 6 - Stopping an emulation run 36
10.8 Step 7 – Emulating a congested network 36
10.9 Summary 41
11 GUI Walkthrough - Master Menu Bar 42
11.1. Tools Menu 42
11.1.1. GUI Settings 42
11.1.3. Administration 44

11.1.2. About 49
11.1.3. Activate Product 49
12. Routed and Bridged Operations Overview 50
12.1. Introduction 50
12.2. Selecting the required operation 50
12.3. Visualisation of operation 50
13. GUI Walkthrough - Map/Device Navigation Bar 51
13.1. Contents and Settings 51
13.2. Adding, renaming or removing hardware 52
13.3. Maps 52
13.4. Device Settings 56
13.5. Hardware Reset 63
13.6. Captured Traffic Files 63
14. Network Toolbox Overview 64
14.1. Tool and Impairments - General Settings 65
15. Network Toolbox 66
15.1. Overview 66
15.1.1. Bridged vs Routed mode 66
15.1.2. Licensed Tools 66
15.1.3. Network Emulation Tools Available 66
15.2. Network Ports 67
15.3. Packet Delay 71
15.4. Jitter 76
15.5. Bandwidth Throttling 78
15.6. Ethernet Fragmentation 82
15.7. Drop Packets 83
15.8. Packet Sinkhole 86
15.9. Packet Corruption 87
15.10. Bit Error Rate (BER) Corruption 90
15.11. Packet Duplication 91
15.12. Packet Reordering 95
15.13. Merge Point 98
15.14. Null Point (TAP Extender) 100
15.15. MPEG/H.264 Corruptor 101
16. Load Generation 104
16.1. Background Traffic Generation 104
16.2. TCP Server Load Generator 107
17. Filter Tools Overview 111
17.1. Packet Counting Filter 111
17.2. UDP/TCP Filters 114
17.3. Ethernet MAC Address Filter 117
17.4. Ethernet Payload Filter 119

17.5. IP Address Filter 121
17.6. IP Protocol Filter 123
17.7. VLAN Protocol Filter 125
17.8. MPLS Protocol Filter 127
17.9. Output Switching Filter 128
17.10. Input Switching Filter 129
17.11. RTP Filter 129
17.12. MPEG Video Filter 132
17.13. Generic Filter 133
18. Virtual Routers 138
18.1. Feature set 138
18.2. Virtual Routing 139
18.2.1. Introduction 139
18.2.2. Using Virtual Routing 139
18.3. Configuring Your Virtual Routers 140
18.4. General Settings 142
18.5. DHCP Settings 144
18.6. Virtual interface Settings 146
18.7. Real Time Stats 149
18.8. Virtual Routers and Load Generators 152
19. Time Constraints 153
20. Advanced Operations 154
20.1. Introduction 154
20.2. Frame Check Sequence (FCS) 154
20.3. Updating maps on remote clients 156
21. Reporting – TAP Devices 158
21.1. Reports 159
21.2. Statistical Graphs TAP 160
21.3. H.264 Statistical TAP 163
21.4. Root Cause Analysis – Wireshark 164
21.5. Traffic Capture and Replay 166
21.6. Load Generator Analyser 170
22. Reports 171
23.1 Introduction 171
23.2 Adding an Existing Report 172
23.2.1 Report Settings 173
23.2.3 Current Report - Settings 173
23.2.4 Running a report 173
23.2.5 Saving report information 174
23. RESTful Remote Control API 175
23.1. Introduction 175
23.2. Saving XML Network Maps 175

24. Wizards 176
25. Generating maps from PCAP files 177

1. Safety Notices

Caution

TO PREVENT THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE ANY PART OF THE PRODUCT'S CASING. THERE ARE NO USER-SERVICEABLE PARTS INSIDE THIS UNIT.

SERVICING MUST ONLY BE CARRIED OUT BY QUALIFIED SERVICE PERSONNEL.

Safety Specification Table

Safety Specification	SNE Information
Rated Supply Voltage	100-240V
Rated Frequency	50-60Hz
Rated Power Input	350Watts
Rated Power Output	350Watts
Altitude of Operation	3048 meters / 10,000 feet maximum
Operational Temperature	5 - 40°C
Relative Humidity	5 - 85%
Overvoltage Category	Category II
Pollution degree of the intended environment	Pollution Degree 2

Important Safety Notice

To ensure safe operation and to guard against potential shock hazard or risk of fire, the following must be observed:

- Ensure any fuses fitted are the correct rating and type. If unsure, please contact us for support.
- The unit must be earthed by connecting to a correctly wired and earthed power outlet. The power cord supplied with the unit must be wired as follows:
- The **green/yellow** coloured wire must be connected to the supply plug terminal marked with the letter **E** or by the earth symbol (I) and is coloured green or green/yellow.
- The **blue** coloured wire must be connected to the supply plug terminal marked with the letter **N** or coloured black or blue.
- The **brown** coloured wire must be connected to the supply plug terminal marked with the letter **L** or coloured red or brown.

At all times the SNE unit should be positioned and used as such that the access to the mains cord is not restricted.

At any time, the SNE unit should not be exposed to excess moisture, dripping or splashing. No objects filled with liquids, such as coffee cups, should be placed on or near the equipment. The SNE equipment is designed and manufactured for **indoor use only**.

General Precautions

- Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) of 30c.
- Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

DO NOT COVER VENTILATION HOLES OR REDUCE AIR FLOW

Slots, fan vents and openings on the SNE unit are provided for ventilation that is needed to ensure reliable operation.

To avoid overheating and loss of warranty please ensure that the ventilation slots are not blocked, place the SNE unit on a smooth, hard surface that has at least five cm (two inches) of clearance around the unit and adequate air circulation. If the equipment is placed in a closed area, such as a rack or a case, ensure that proper ventilation is provided and that the internal rack operating temperature does not exceed the maximum rated temperature (30c) at the position of the SNE unit.

If Calnex find that the SNE was used in such a manner that the above safety specifications where not taken into consideration and above safety notices were not followed, this will result in a loss of warranty that covers the unit.

2. Introduction

Thank you for purchasing the SNE - an advanced, user friendly and powerful hardware-based Wide Area Network emulation device.

The manual guides you through the simple installation process and explains how to gain the maximum benefit from the rich feature set provided for emulation.

It is recommended that all new users of this product read this manual prior to switching the unit on for the first time.

3. Company Profile

Calnex develop innovative solutions that allow IT and communications industries to evaluate the performance, agility and security of the latest technologies, infrastructure and applications being deployed worldwide. As well as working with customers in the IT and communications industries, we work with other sectors, including aerospace, automotive, consumer electronics, energy, finance, government, and many more. We also provide tools for service technicians and field test engineers to improve network quality and make troubleshooting of live networks efficient and effective.

4. Unpacking and Installation

After carefully unpacking the unit, please:

- Check the unit for any damage that may have occurred during transit. We protect all our products with industry standard packing but damage can still occur.
- Check that the contents supplied match the following list:

    1. One 2U rack-mountable hardware device.
    2. Cabling:
        1. One mains cable (connector subject to destination country)
        2. Ethernet cables for connection to the ports on the front of the hardware unit
    3. One hard copy of the Quick Start Guide
    4. One USB stick containing the Operating Manual and other documentation.
    5. Hardware configuration (if applicable)

If the equipment supplied does not match all the above components, please contact us immediately using the contact details found at the start of this user manual.

5. SNE at a glance

The SNE is a hardware-based Wide Area Network Emulator, designed to accurately replicate conditions that applications and systems could experience when making WAN traversals. SNE is used in the test lab to test applications, protocols and end user experience under real world conditions before and after deployment.

SNE can emulate the following WAN links:

- Satellite
- Microwave
- 3G
- 4G
- GPRS
- E1/T1
- ISDN
- Modems
- And others

The version of SNE that has been shipped to you has come installed with the following impairment tools, filtering tools and reporting:

- **Virtual Router Simulation**
  - Simulate routers for WAN environment simulations
  - Support multiple ports, DHCP and ARP

- **Packet corruption**
  - Bitflips and byte overwrites, bit error rate simulation, etc.

- **Drop packets (packet loss)**
  - Drops a variable number of packets

- **Packet Sinkhole**
  - Drops all packets received

- **Packet Duplication**
  - Single, timed or complex (delay and multiple duplication)

- **Packet Delay**
  - Delays packages by static amount (with variable jitter) or by a dynamic range

- **Bandwidth throttling**
  - Throttles bandwidth to a set amount, various options.

- **Ethernet fragmentation**
  - MTU min/max range

- **Jitter**

- **Reordering of packets**

- **Background traffic Generation**
    - Emulates link usage – fixed or percentage of available link

- **Load Generation**
    - TCP, UDP, etc. load generators

- **Filters**
    - TCP, UDP, IP address, IP, MAC (Ethernet filtering), packet count, Ethernet payload, Generic, etc.

- **Packet Modification**
    - Generic (byte/bit) modification

- **Null Point Object**
    - Allows the creation of more TAP device points for reporting purposes

- **Traffic Capture**
    - Record live traffic to the SNE hard drive, for analysis via Wireshark PCAP files

- **Traffic Replay**
    - Replay previously recorded traffic (either traffic captured on the emulator or remotely)

- **Statistical Graphs**
    - Bandwidth Graph – Showing bandwidth in various units (bits, megabytes, etc.)
    - Packets per second – reports the number of packets
    - Inter-packet gap – shows the time between packets.

- **Wireshark**
    - Provides root cause analysis and packet capture/replay capability
    - Note that Wireshark must be installed on the client PC.

- **Hardware latency measurements**

Please see section "Network Impairment Tools" for more information on each impairment tool and how to use these in your emulation, and the section titled 'Reporting – TAP devices' on how to view the output of your emulation.

The SNE unit provides flexibility with up to 16 ports 1Gbps, up to 12 ports 10Gbps or up to 4 ports 25GbE, and is positioned between any two compatible devices so that it acts as an 'intermediary' between these attached devices. Using the GUI, users can inject common WAN impairments onto this connection and analyse the results, either through viewing the resultant input to the device, or through the GUI's reporting system (if available / licensed).

The SNE is provided as a 2U (3.5 – inch height) standard chassis. The 2U unit has no labelled ports, this is intentional. Please see the graphic below detailing the front panel components on the unit.

Figure 1 – SNE hardware at a glance

Power On/Off button

See figure 2:
Front Panel group

Ethernet RJ45 Control port – used to provide communication between the SNE hardware and the GUI

Ethernet RJ45 or SFP/SFP+ ports – used to connect the SNE onto the LAN via the supplied Ethernet cables.

Figure 2 – Front Panel group

Power LED: Lights when the unit is connected to a power source

Running LED: Lights when the unit is performing an emulation run

Forwarding LED: Lights when the unit is not performing an emulation run (data packets are automatically being forwarded without any impairment; this may be disabled in settings)

Fault LED: Lights when the unit is experiencing a fault during an emulation run – consult GUI for more information

Overload LED: Lights when the unit is experiencing high load; Network packets may be dropped.

Reset IP Address 'pin hole': Inserting and holding in a non-metallic object (when unit is running) will result in the IP address being reset to its default.

6. Getting Connected

6.1. Pre-installation Notes

Please note:

- Avoid cable interconnection length in excess of 1 meter (3.3 feet) in strong RF environments.
- All network interface ports (Ethernet) and mains power connection must be externally protected from lightning strikes – damage from lightning strikes is not covered by the warranty.
- The network interface ports do not support Power over Ethernet; attaching PoE-enabled devices may result in failure of the product. Damage from PoE devices is not covered by the warranty.

6.2. Tools and Cables Required

In addition to the content of the packing list, the following items are necessary to complete the installation (if mounting).

- **Tools**: One flat or Phillips screw driver suitable for M 6 rack mounting bolts. A basic electronics toolkit is useful for individual cabling.
- **Rack mounting hardware:** Four M 6 bolts with plastic protection washers.

6.3. Installation

Installing both the SNE hardware and software is an intentionally simple exercise. To start, please follow the instructions below:

6.4. Hardware:

1. Select the chosen physical location on the LAN most appropriate for the unit to be positioned.
2. Connect the supplied power supply cable to the AC input socket at the rear of the machine and connect to a power source. The unit will power up after short circuit and overload protection mechanisms have verified the power supply.
3. Connect a CAT 5E / CAT6 Ethernet cable or fibre from the device under test (or the switch/router with visibility of the device under test) to port 1 on the SNE unit (Port 1 is the upper left most port by default).
4. Connect a second CAT 5E / CAT6 Ethernet cable or fibre from the chosen destination device (or the switch/router with visibility of the destination device) to port 2 on the SNE unit (Port 2 is directly below port 1 by default).
5. Connect a third supplied CAT 5E Ethernet cable from the control port to a switch or router on the LAN (or direct to the machine running the GUI), ensuring the SNE hardware unit can communicate with the computer on which the GUI will be installed (see section "6.7 First time access to SNE")

6.5. Installing the GUI Software:

The SNE software can be installed on Windows and Linux / Mac (using the WINE - https://www.winehq.org/ compatibility system).

Please follow these steps to install the SNE software:

1. Determine which computer the GUI should reside on. Please note, the GUI can be installed onto multiple machines **without licensing restrictions** and can be loaded onto physically remote computers (and will be able to control and receive information from the SNE hardware as long as the Local Area Network configuration permits visibility).
2. Your chosen distributor will have provided a URL from which you may download the GUI. Please download the zip file, extract the executable and launch it.
3. The SNE GUI setup screen will appear.
4. Follow the on-screen instructions to install the GUI.

Please note: when the SNE hardware unit is turned on, it is common for the hardware to take up to 30 seconds to initialise and provide communication with the software.

Make sure that Windows Firewall allows connections to / from SNE GUI.

6.6 Installing your license key

Once the installation has completed the GUI will prompt you for a license key, this must be entered before the GUI will operate.

You will find your license key on the separate license key sheet supplied with your product. Your license key is in the form of a string similar to the following:

353E-705D-5EE3-DA68-0884-D8FF-7379-422F (please note this is not a valid key)

Please keep your license key safe at all times, please contact if you have lost your license key or wish to activate any additional features.

6.7 First time access to SNE

Your SNE unit has shipped with a default IP address of “192.168.1.100”, unless you have indicated before delivery that you require a different default IP address. Most users will need to modify this IP address so that SNE is given a static IP address visible on their LAN.

This process involves temporarily changing your computer's (the one designated as running the GUI) IP address to match the "192.168.1.x" range to gain access to SNE via the GUI. Once the GUI can see the SNE you can freely assign the correct IP address to the SNE before reverting your computer's IP address back to its original IP address.

For the GUI to communicate with the SNE unit you must change your computer's IP address to be within the same subnet range as the SNE. In this example we will set your computer's IP address to "192.168.1.50". This process should only be attempted by network administrators or knowledgeable users.

This example is for Windows 7; please consult your operating system's guide or network administrator for all other OS's.

1. Ensure the device running the GUI is connected via Ethernet cable to 'Port C' on the front of the SNE unit
2. Open the Windows control panel on the device running the GUI and ensure the view is set to 'category view'
3. Select 'View network Status and tasks' under the 'Network and Internet' section
4. On the left menu, select 'Change adapter settings'
5. Right-click on the adapter that the SNE is connected to - usually this is 'Local Area Connection'. Select the 'properties' option
6. The 'Local Area Connection properties' window should open
7. Select 'Internet Protocol Version 4 (TCP/IPv4)' and click 'properties'
8. The 'Internet Protocol Version 4 (TCP/IPv4)' window will open
9. Select the 'Use the following IP address' field
10. In the following fields enter
    - IP Address = 192.168.1.50
    - Subnet Mask = 255.255.255.0
    - Leave default gateway empty
11. Select OK and exit
12. Your computer will now be assigned a static IP address of 192.168.1.50
13. If Windows reports any problems please contact your system administrator

Verify your computer can see the SNE by opening a DOS console and enter 'ping 192.168.1.50' – If you cannot ping the unit please contact your system administrator. At this point your computer will be on the same IP range as the SNE unit. The GUI will start communicating with SNE unit and you will gain full access to the unit.

Please see the "control port network settings" section on how to change the SNE unit IP address to your desired value. After you have changed the SNE unit IP address you should revert back your computer's IP settings (the device which will run the GUI and control the hardware unit).

Under certain circumstances it may be necessary for you to reset the SNE IP address back to the default "192.168.1.100", please see the section under "Hardware Reset" under "control port network settings"

7 Positioning SNE Hardware

SNE can emulate a wide range of WAN links and conditions, but in order to act as a WAN, the positioning of the SNE hardware on your LAN is an important consideration.

SNE is a 'transparent' entity on the LAN – aside from the Control Port (for the sending and receiving of control information to/from the unit and the GUI), the hardware unit's network ports do not have a MAC or IP address. SNE sits between the devices attached on port 1 and port 2 (or port 3 and 4 for 4 port model) transparently emulating your chosen network.

SNE supports Ethernet automatic crossover detection, thereby allowing a device under test (or the device running the application under test) to be directly connected to port 1 or 2. This negates the need for a network switch or router in two DUT (Device Under Test) operations.

Using Network Interface Devices (e.g. switches or routers)

The Ethernet cables connected to port 1 and 2 cannot physically terminate at the same switch, router or bridge. If the cables connected to port 1 and port 2 end at the same switch, the switch (or router, etc.) will detect that the packets intended for WAN emulation need not be sent to the SNE unit, as the intended destination is simply another port on the same switch.

If using routers/switches, please therefore ensure that the Ethernet cables attached to ports 1 and 2 terminate at different routers or switches.

SNE allows data to be sent bi-directionally with data in each direction made subject to different impairments i.e. data sent in one direction can be subject to different impairments and settings from the data flowing in the opposite direction.

7.1 LAN Configuration Walk Through

For ease of understanding, the following example is used – please note this is focused on the 2-port hardware configuration, the same process can be applied for other quantities of ports.

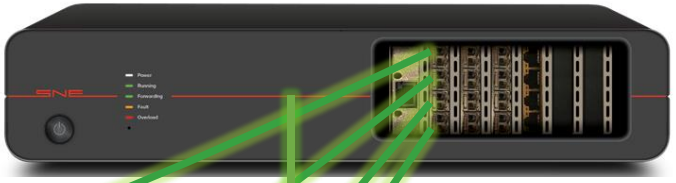
Device A is a desktop PC which is either under test or is running an application under test.
Device B is the destination device that is physically located on the LAN but is being simulated as a remote device on the other side of a WAN.

- Device A can be connected via Ethernet cable directly to port 1 on the SNE front panel.
- Alternatively, device A can be connected to a network interface (such as switch or router), and an Ethernet cable connected from the network interface to port 1.
- Similarly, device B can be either directly connected to port 2 via a single Ethernet cable, or with a network interface acting as an intermediary.

Please note:

- The same device cannot be connected to both port 1 and port 2.
- The same switch/router/hub or any other network interface device cannot be connected to both ports 1 and port 2.
    - A switch or router will 'switch' away traffic before the SNE can introduce impairments.
    - A hub may cause a circular loop resulting in an overload condition.

The following graphic displays how SNE unit can be added to a LAN.



Network Interface e.g. switch or router

OR

Single computer or IP device on LAN

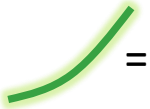
Network Interface e.g. switch or router (must be a different network interface device from the one that is connected to port 1)

OR

Single computer or IP device on LAN

Device running SNE GUI (either directly connected or via a network interface device)

KEY



= Ethernet / Fibre Cable

8 SNE Graphical User Interface: Overview

SNE is designed to be inherently simple to set up, understand and use. Once installation is complete, please navigate to the GUI (in the location defined during software set up).

The GUI allows users to visually create the network which is to be emulated, by dragging and dropping components/impairments onto the screen. These are then linked together with onscreen connections (so the user can control the 'flow' of data between emulated devices), and simple 'play', 'pause', 'stop' options provide overall control.

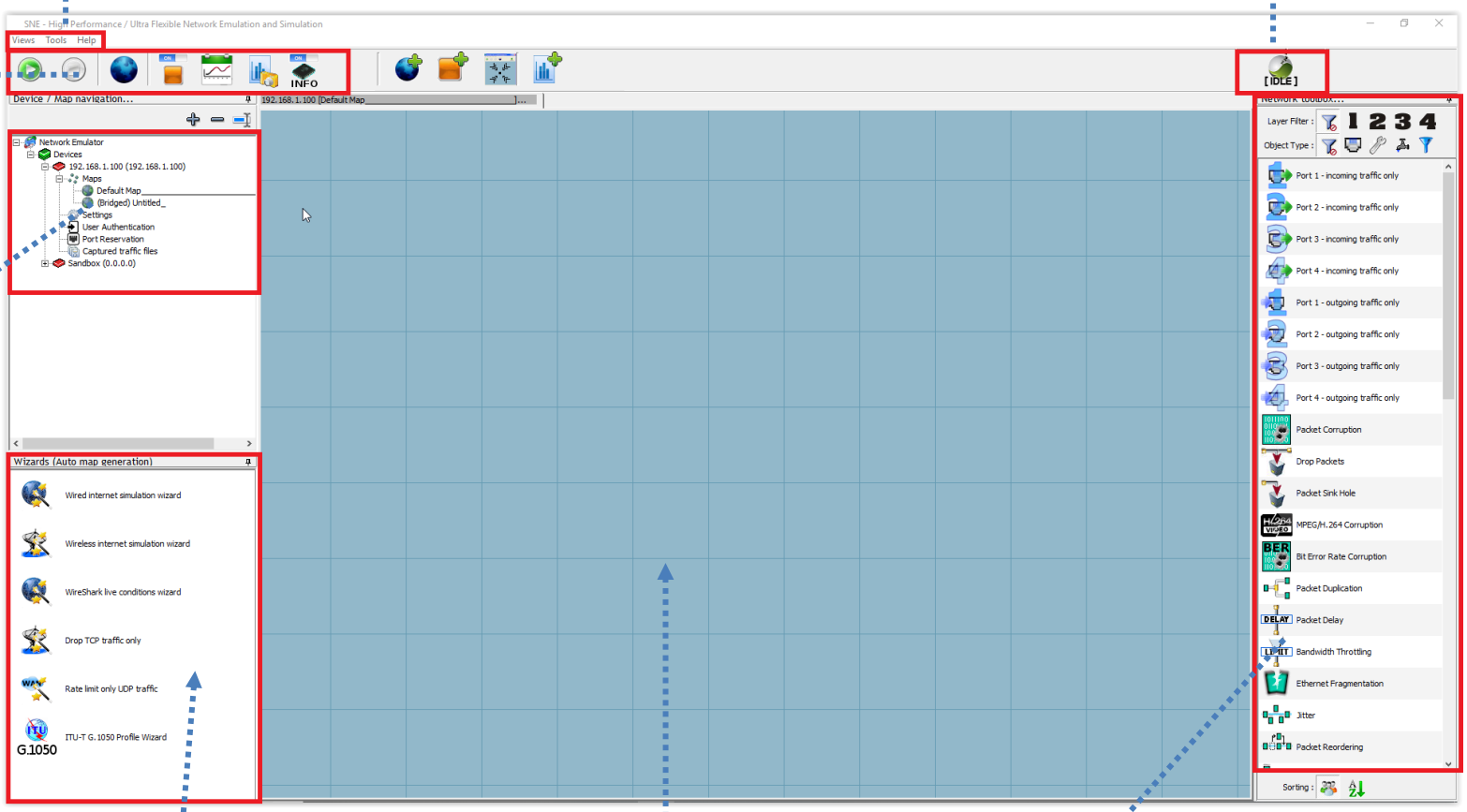
The following screenshot shows how the user interface will appear on first start up:

Figure 4 – SNE GUI Overview

1) Master Menu Bar – provides application wide control

2) Map Menu Bar – enables high level control over an individual network map (such as start emulation, pause, stop and re-centre emulation map)

3) Device / Map Navigation Bar – provides a logical listing of all SNE hardware units installed, and the network emulation maps that have been created for each unit



4) Wizards Bar (dependent on configuration – not available on all versions) provides pre-defined common network maps and impairments, which can then be amended as required.

5) Design pane – provides graphical representation of the WAN under test (populated using Wizards to left or network toolbox to right)

6) Network Toolbox – provides drag and drop facility to create network maps and their conditions for emulation

7) Status Bar – displays CPU load and status of connection with hardware unit (e.g. connected, paused or disconnected)

8.1 GUI Overview

The Design pane (number **5** in the diagram above) is where the emulation map is designed – these maps are graphical representations of the WAN to be simulated, and therefore form the core of the SNE operation.

Each map will contain:

- Input / Output points - Physical port start and end points, network routing start / end points, or the captured traffic replay tool.
- WAN impairment tools between these input / output points
- Any reporting required from TAP points.
- Any traffic capture required

The Network impairments are available to be 'dragged and dropped' from the 'Network Toolbox' (number **6** on the diagram above) onto the Design pane. Reporting is accessed by right-clicking a 'TAP point' – these appear when a link is made between network start/end points and any WAN impairments (please see section 12.10 'Reporting – TAP devices' for more information).

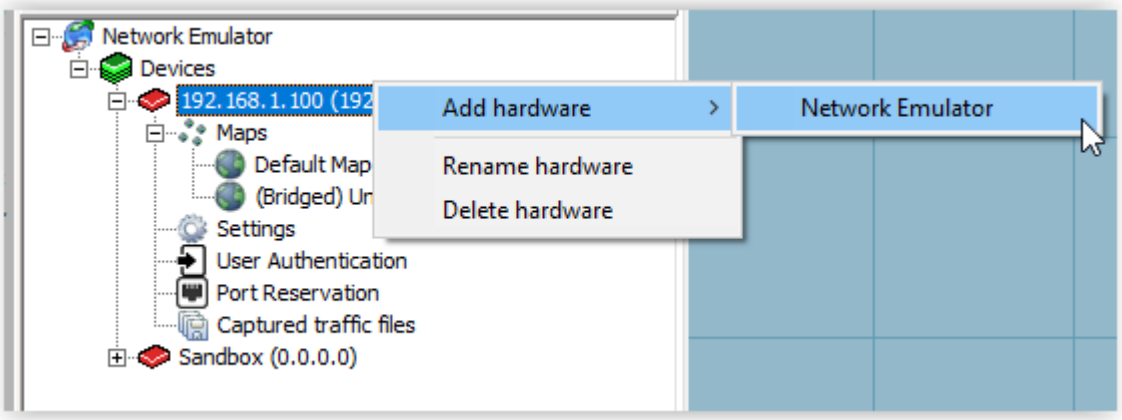
Once an emulation map has been designed, the user simply presses on the 'play' button in the map menu bar to initiate emulation.

It is highly recommended that first time users follow the instructions in the section "Creating your first emulation run", as this will provide quick experience and demonstrates the SNE key features.

8.2 Multi-Emulator Usage

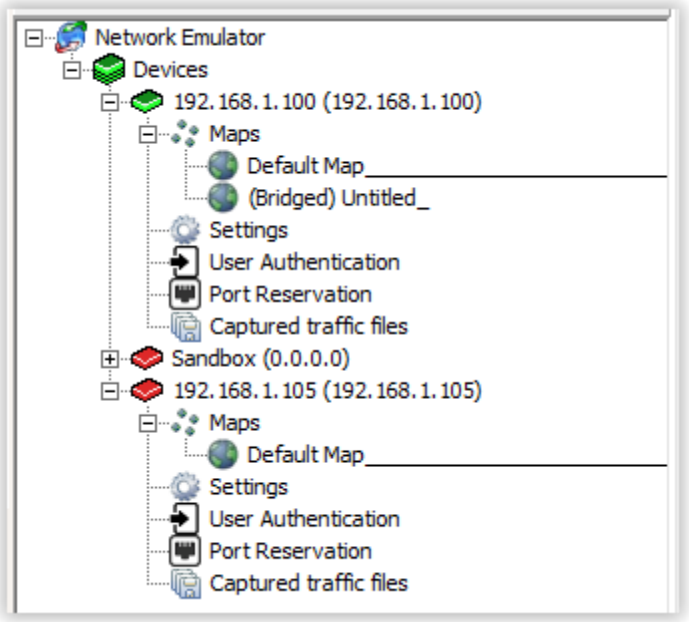
The SNE GUI is fully multi-emulator aware, allowing you to control an unlimited number of hardware emulators from within it. In standard installations you will receive a single hardware device.

You must add in all additional hardware devices by selecting the “Add Hardware” option:



Once you have entered the correct IP Address you will be presented with two hardware devices in your emulation map. The newly created hardware device will have a single “default” network map added to it.

The screenshot below shows two emulators configured as “SNE 1” (192.168.1.101) and “SNE 2” (192.168.1.105). In this instance a number of maps have been copied from the Sandbox and pasted into the emulators.

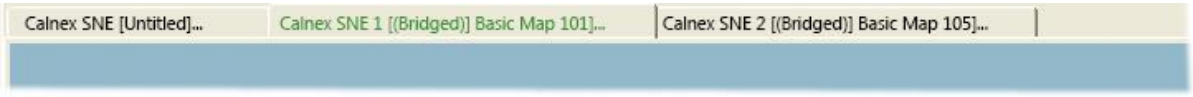


8.2.1 Launching maps on different emulators

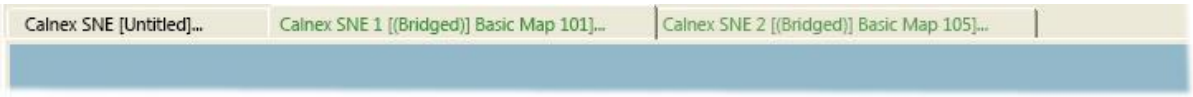
There are no special requirements when launching network maps on different emulators.

The emulator will colour code the tabs at the top of the network maps to show any executing emulation maps. The tab will turn GREEN to indicate the network map is executing.

When a single network map is running (on SNE 1) you will see the following tab bar:



When a network map is running on both emulators, you will see the second map also displayed in green.



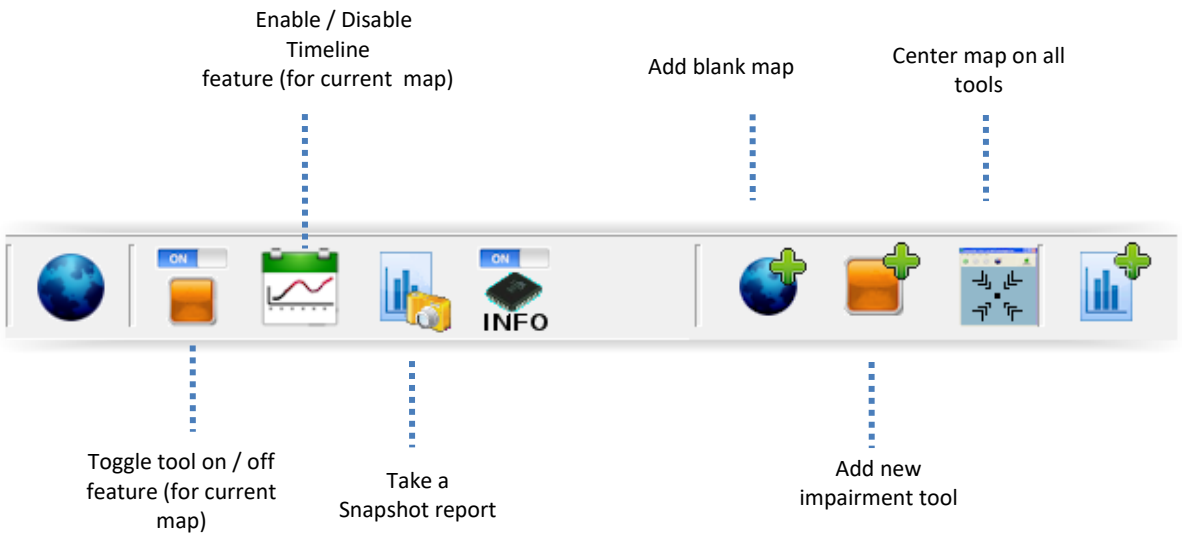
8.2.2 Limitations

The only limitations associated with controlling multiple hardware emulators are around the statistical and analysis aspects of the system. These are:

- The Timeline system will not operate if you switch away from a network map.
- Statistical Graphs information is only available whilst viewing the current live network map.
- Report information is lost if you switch away from the current live network map.

8.3 Map Menu Bar

The map menu bar is shown below:

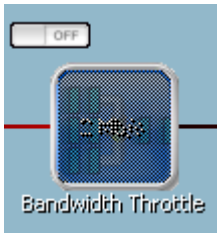


8.3.1 Toggle Tool (on/off)

When selected, the toggle tool allows the user to disable (or re-enable) impairment tools added to an emulation map. Any traffic that encounters a tool that has been disabled will pass it unimpeded.

The following screenshots show how impairment tools are represented when this feature is enabled:

Jitter Tool active ('on')



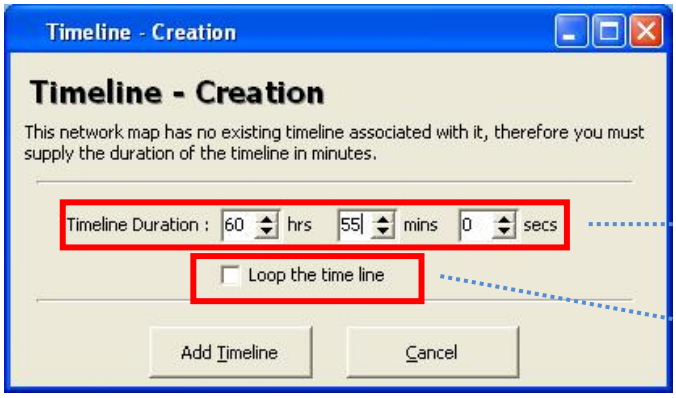
Bandwidth Throttle Tool disabled ('off')

Impairment tools can be toggled on or off while an emulation is being executed i.e. in real time. It should be noted that when an impairment tool that buffers packets (such as delay or jitter) is disabled, it will 'dump' all buffered packets immediately. This can result in a small but inevitable spike in traffic as the packets are released back onto the link.

8.3.2 Timeline (Auto-Change) Feature

This feature allows the user to create an emulation scenario which (once started) changes parameters without any manual input from the user. The following icon in the Master Menu Bar provides this functionality:

Once selected, the timeline feature will first ask the user to set a total duration that the emulation should run for (which can be changed later if required). This can be up to a maximum of 240 hours (10 days). The following screenshot shows this dialog box:

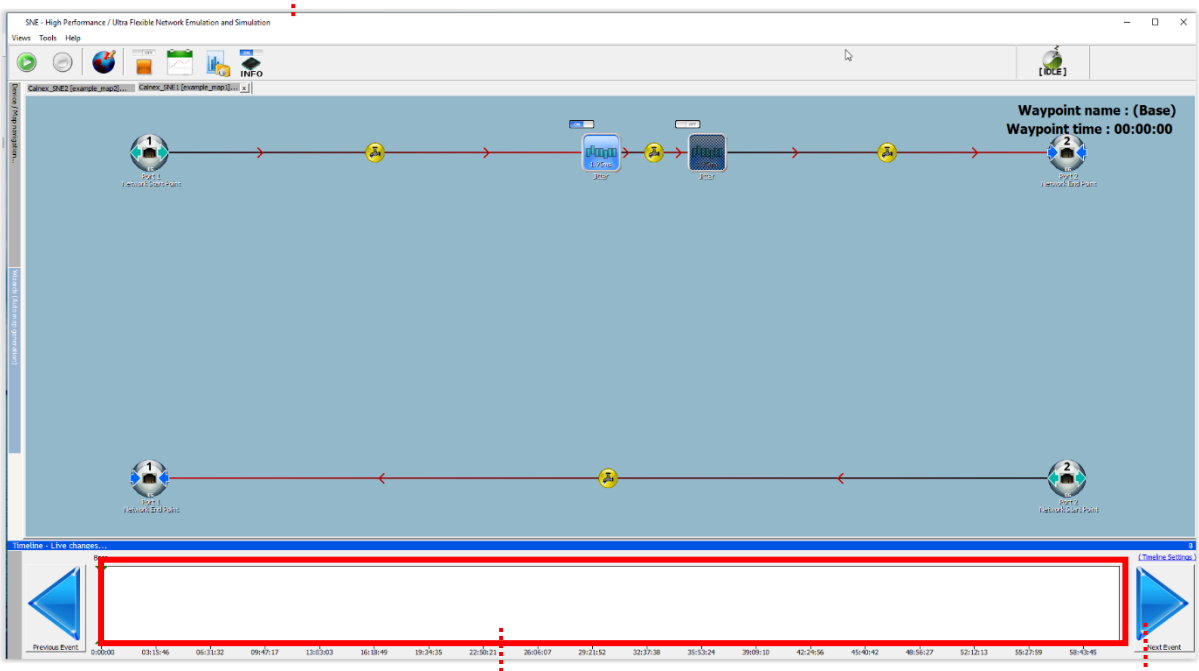


Enter the total duration of the emulation run, then click 'Add Timeline' to present the timeline on screen

If set, the time-line will continuously loop until the emulation map is stopped

Once 'Add Timeline' has been pressed on the screen above, a timeline will be displayed at the bottom of the user interface - please see the diagram below:

Click on the 'Timeline' feature to display the timeline at the bottom of the user interface



The timeline allows the user to set waypoints, each of which allows the user to change any impairment settings and/or turn impairments on and off.

The large blue arrows (see left as well) allow the user to move quickly between any waypoints that have been created on a timeline.

The above screenshot shows an existing emulation map with two impairments (one active, one turned off using the Toggle on/off feature) and an empty timeline. It is normal practice to design an emulation map before enabling the timeline and creating waypoints on it.

Please note:

- Any timeline created is specific to an individual emulation map.
- Turning off the timeline feature (by clicking the Timeline icon again) will not destroy any waypoints created or their settings. They will be available when the timeline is next turned on.

Timeline (Auto-Change) Feature – Creating a waypoint

The following dialog box will appear once the user clicks anywhere on the timeline:

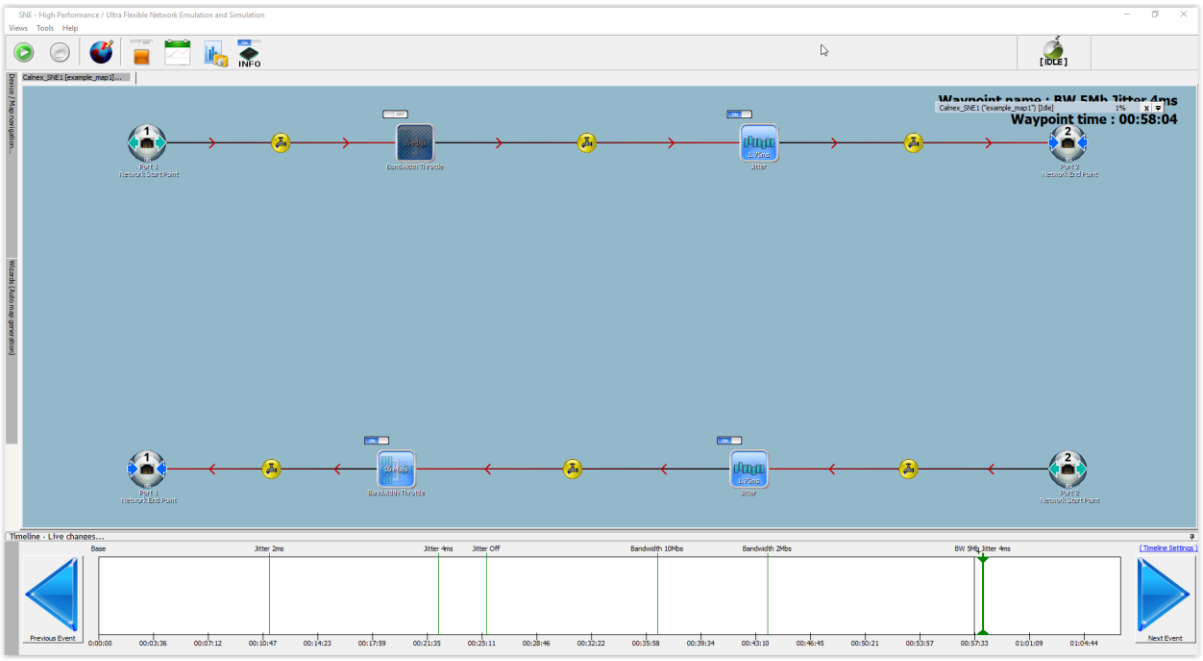
Enter a title to make the waypoint recognisable – this will appear on the timeline immediately above the waypoint for easy identification

The waypoint time (i.e. when the changes will take place) is an offset from the start of the emulation. The user can enter the exact time (to the second) when the changes required will be implemented

Select the 'Create Waypoint' button to create the waypoint.

The user can now edit the settings of any impairment tool on the emulation map as required or turn any on/off (using the toggle on/off feature available from the Map Menu Bar). These changes are automatically stored by the user interface against the waypoint.

The process of creating waypoints can be repeated as many times as is required by the user across the timeline – the screen below shows an emulation map set up with multiple waypoints:



In the above example the map will execute and then, at 11 minutes 15 seconds from the start of the emulation, the jitter will change to 2ms (as per the user defined title of this waypoint). The jitter will remain at 2ms until 22 minutes and 20 seconds into the emulation, when it will automatically change to 4ms, and so on.

Timeline (Auto-Change) Feature – Running an emulation

The user can then press the 'Play' button on the top left of the user interface to start the emulation. At this point the timeline cannot be edited and a red vertical bar will begin scrolling across the timeline showing the time elapsed.

As time passes the red vertical bar will encounter each waypoint created by the user, and the new emulation parameters will instantly and automatically become active.

Timeline (Auto-Change) Feature – Editing the waypoint

A waypoint's settings can be changed by hovering over any waypoint and clicking it (the waypoint will be highlighted with a purple box). The user can then amend any impairment tool's settings for that waypoint as required. Please note that deleting a waypoint will cause all impairment settings for that waypoint to be lost.

8.3.3 Snapshot Report

This feature allows the user to take a visual snapshot of the current network map and save this to a user defined location. To generate a snapshot please click the following icon:

The report consists of a bitmap containing the current network map; a bitmap for each statistical graph and a XML file containing the structure of the current network map. The system will automatically create a date / time folder for each snapshot.

To change the location in which the snapshot is placed please see the options under “GUI Settings” for more information.

9

This section is intentionally left blank.

10 Creating Your First Emulation Run

10.1 Introduction

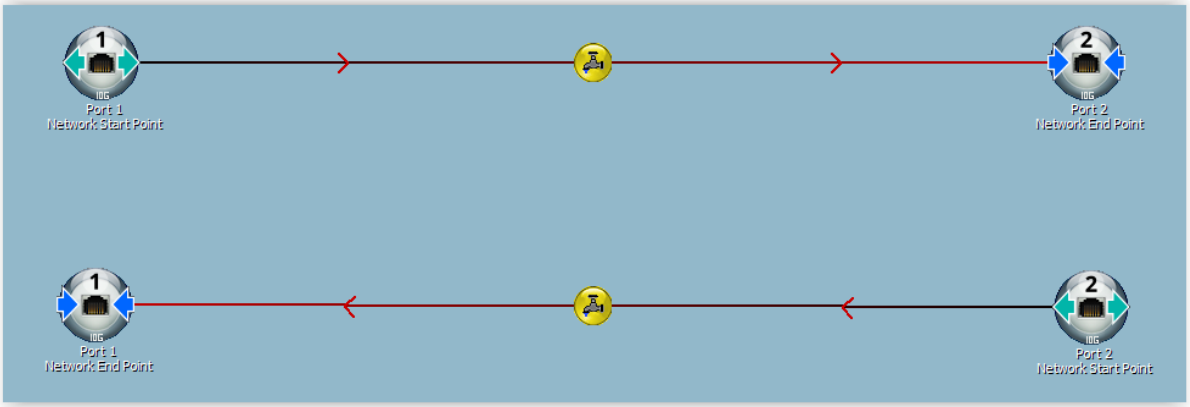
This section will explain the process involved in the creation of an example emulation run, following the installation of both software and hardware. Please note that this chapter provides an overview and is not designed to be a comprehensive walkthrough of the GUI or its features and settings. The objective of this chapter is to serve as a quick start guide to emulation using the SNE product.

Please note: This section describes the "bridged mode" operation of the unit. Bridged mode places the SNE as a "bump in the wire" allowing all packets entering the unit to be impaired. Please see the "Routed and Bridged mode operations" section for more information.

Prior to step 1, please ensure the hardware is connected and positioned as per the guidance in section 7 'Positioning the SNE Hardware'.

For this example, we are going to create a relatively simple wired internet simulation on a 2-port model. When the GUI is launched you will find a default network map named "Vanilla Connections" under the left menu titled 'map/device navigation'. Please double click on this network map to show it.

The arrows between the ports represent the logical direction that data will follow once the emulation is started. Data from Port 1 will flow to Port 2, and vice-versa.



A basic network map

For ease of understanding, the Port 1 objects (on the left of the graphic above) can be thought of as the device connected to port 1 on the front of the SNE hardware. Similarly, the port 2 objects (on the right of the above graphic) can be logically considered as the device connected to port 2 of the SNE hardware.

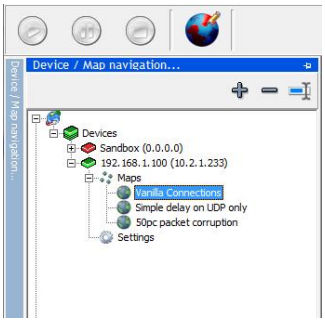
SNE can impair and manipulate traffic in both directions, hence the use of two connections (as shown in the diagram above) for each physical connection that traffic is sent down and received from.

If the 'return' connection between port 1 and port 2 on the Design pane is removed, then **no traffic will be returned**. It is important to remember that, in order to emulate and collect accurate

information regarding an emulation run, all maps should have at least one connection made between ports 1 and 2 and one made between ports 2 and 1.

10.2 Step 1 – Changing a map name

1. Locate the 'Map/Device Navigation' window on the left side of the screen.
2. The current map (called 'Vanilla Connections') and its location within the SNE device navigation hierarchy will be highlighted in blue, as shown below



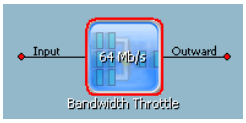
Note: depending on the SNE hardware installed, your view of the Device/Map navigation hierarchy may be different – this screenshot is for general guidance only

3. Locate and right-click on the map titled 'Vanilla Connections" and select 'rename map'.
4. Enter a new name for this emulation map e.g. "Test 1"
5. The title of this map will change, both on the map/device navigation bar and on the tab header which displays this map on the Design pane. As the number of maps created increases, or more SNE hardware units are added, it will become increasingly important to name your maps intuitively.

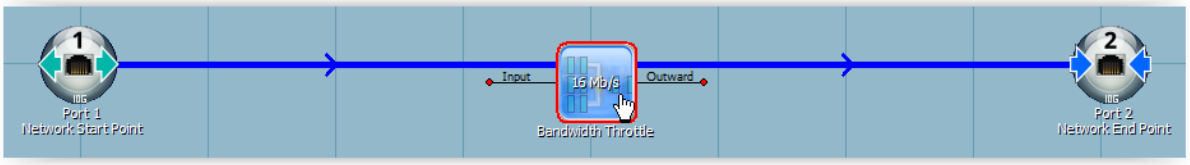
10.3 Step 2 – Adding an impairment

We will start by adding a bandwidth throttle impairment to both the upstream and downstream connections, to emulate a bandwidth limit common on a wired internet connection. For this example, we will limit downstream bandwidth to 1 Mb/s and upstream to 256 kb/s.

1. Locate the network toolbox window on the right side of the screen.
2. Locate the bandwidth throttle icon, which looks like this: 

3. Holding down the left mouse key over this icon, drag the tool unto the main Design pane and release your finger
4. The icon will drop onto the design pane and will now look like this: 

5. Hover the cursor over this icon, press and hold down the left mouse button
6. Drag the icon up to the connection between Ports 1 and 2 - the link will turn blue to indicate the tool can be snapped onto it:



Once the connection link changes to this blue colour, release your finger

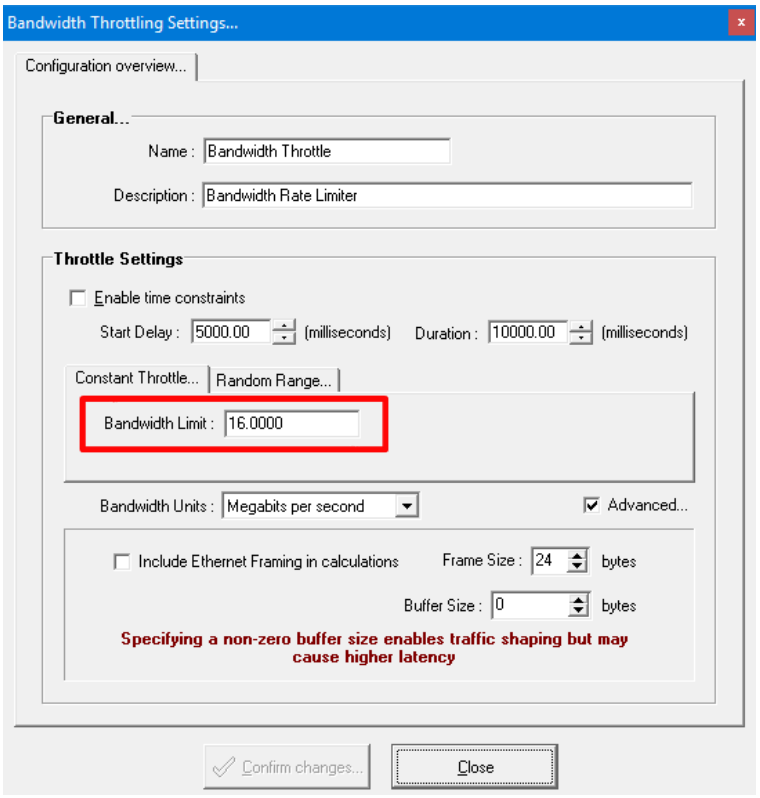
7. The bandwidth throttle tool will snap onto the connection, and will remain on this connection - regardless of where other objects on it are moved to - until it is deleted

10.4 Step 3 – Adjusting an impairment's settings

Viewing the summary information on the bandwidth throttle tool (displayed on the tool), you can see the default setting is 64 Mb/s. This represents the bandwidth limit of traffic moving from the device connected to port 1 on the SNE hardware, to the device connected to port 2.

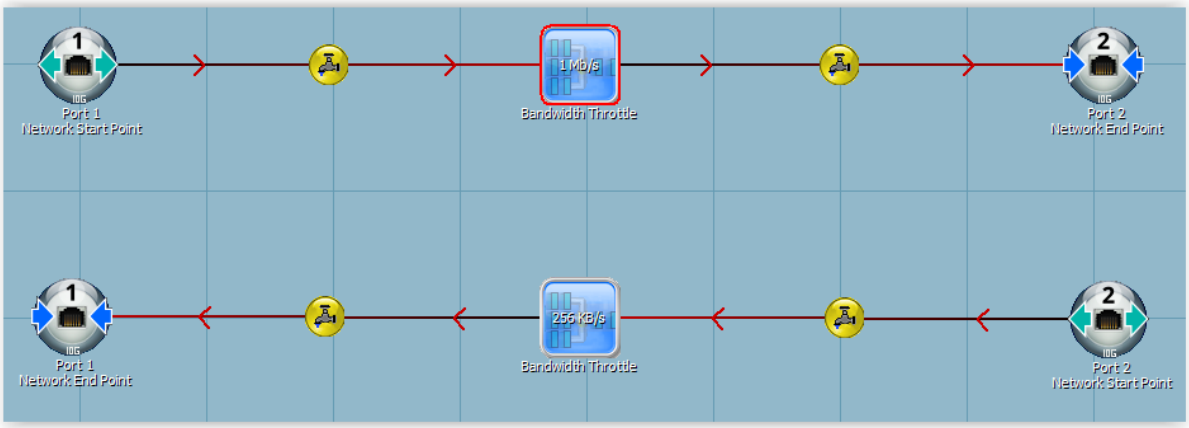
We will now change this to emulate a typical ADSL connection of 1 Mb/s downstream.

1. Right-click the bandwidth throttle icon in the Design pane and select 'settings'
2. The following screen will appear:



3. Change the Bandwidth Limit field (highlighted in red above) from 64.0000 to 25000
4. Once any change is made, the 'Confirm Changes' button will become active – click on this
5. You will be returned to the Design pane, and you can see that you have now set the bandwidth limit to 1 Mb/s on all traffic moving from the device on port 1 to the device on port 2

6. Repeat this exercise for the other connection (upstream from port 2 to 1) – drag and drop the bandwidth throttle icon from the network toolbox, and snap this tool onto the 'port 2 to port 1' connection
7. Right-click and change this second bandwidth throttle to a bandwidth limit of 256 Kb/s (using the drop-down list in the 'Throttle Settings' section to change the measurement to Kilobits per second).
8. Click on 'confirm changes'
9. The Design pane should now appear as follows:



10.5 Step 4 – Running an emulation

You have successfully created the basic conditions of an ADSL connection (although with further network impairments such as packet drop and delay a more accurate emulation is possible).

Any traffic sent to and from the devices connected to port 1 and port 2 will be subject to this bandwidth restriction. We are now going to run this map to demonstrate some of the real time information that is displayed during emulation.

The emulation map that has been created has been designed in **Editor Mode**, which provides the ability to create, design and alter emulation maps. Editor mode is easily recognisable by the blue grid lines on the Design pane. When a map is run (and emulation therefore begins) the GUI switches to **Run Mode,** which prevents any changes to the existing map until emulation is stopped.

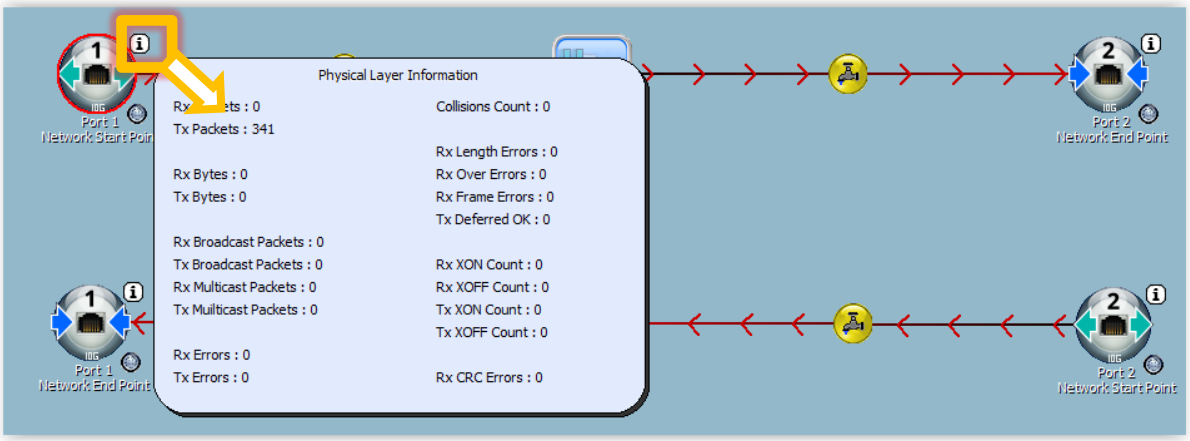
1. To run the map, simple click on the 'play button' in the top left of the GUI:

2. Arrows denoting the flow of network traffic will be shown moving between each port

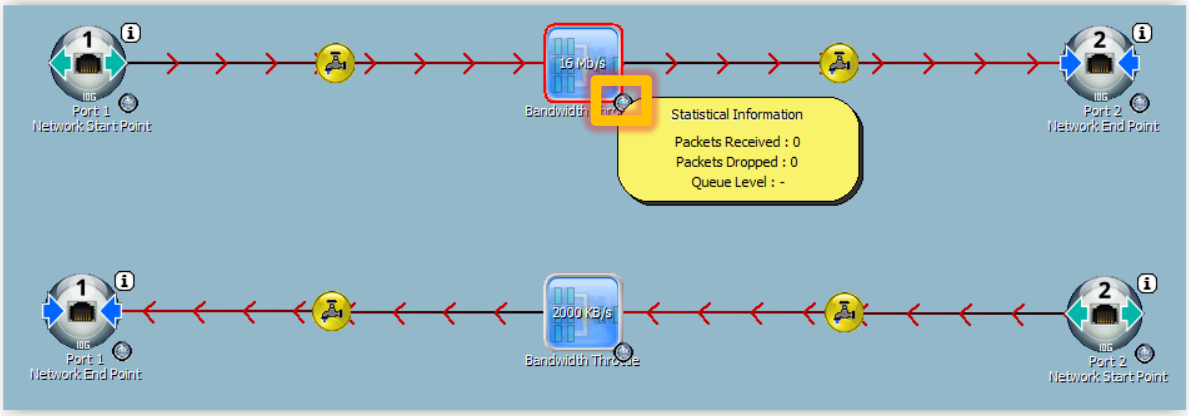
Data Flow Arrows

When an emulation run is started, arrows denoting traffic direction will be shown flowing between ports. In some instances, these arrows may not appear immediately or may be limited to only a portion of the emulation map. This is a simple result of the rendering engine adjusting to your screen's display settings and has no effect whatsoever on the data flowing or results obtained.

3. **Please note**: you cannot edit the settings of any tool or impairment while a map is being executed.
4. We are going to view some of the real-time data displayed when an emulation is being undertaken. To the top right of the Port 1 network start point, you will see a small 'I' icon. Click on this and the following window will appear:



5. The window displayed contains real-time information relating to the physical layer for each Port on an emulation map, and provides the user with details of any collisions, packet errors or control (XON/XOFF) packets received.
6. Real-time packet flow information is also available for any impairment added to an emulation map. These can be accessed by hovering the cursor over the small grey icon at the bottom right of any tool on a map, as shown below:



Moving around an emulation map

Please note that you can navigate around a map, in both Editor and Run Mode, by holding down the space bar and left mouse button, then moving the pointer.

10.6 Step 5 – Making Live Changes

The emulator supports the real-time live changing of both impairment settings and the network map.

10.6.1 Live Impairment Changes

When an emulation map is running, you can change any impairment settings by double clicking on any impairment and enter the new settings. The settings will be reflected immediately and there will be no interruption in emulation.

10.7 Step 6 - Stopping an emulation run

The above example is of a simple, perfect quality bandwidth limited connection. We are now going to add some packet delay onto the connection, to simulate the conditions that may be experienced when sending data over a long distance or at a busy time of day. We will also add in some advanced reporting to demonstrate SNE built in reporting functionality.

1. As the map is executing in Run Mode, we must stop the emulation before we can edit the map in the Design pane. On the top left of the GUI, click on the 'stop' button, as shown below:

2. The emulation will stop and you will be returned to the Editor Mode.

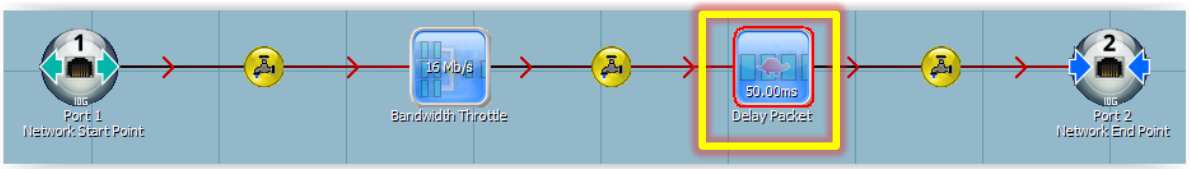
10.8 Step 7 – Emulating a congested network

We are going to add another tool to the emulated network map, to simulate a connection that is suffering from fluctuating high latency.

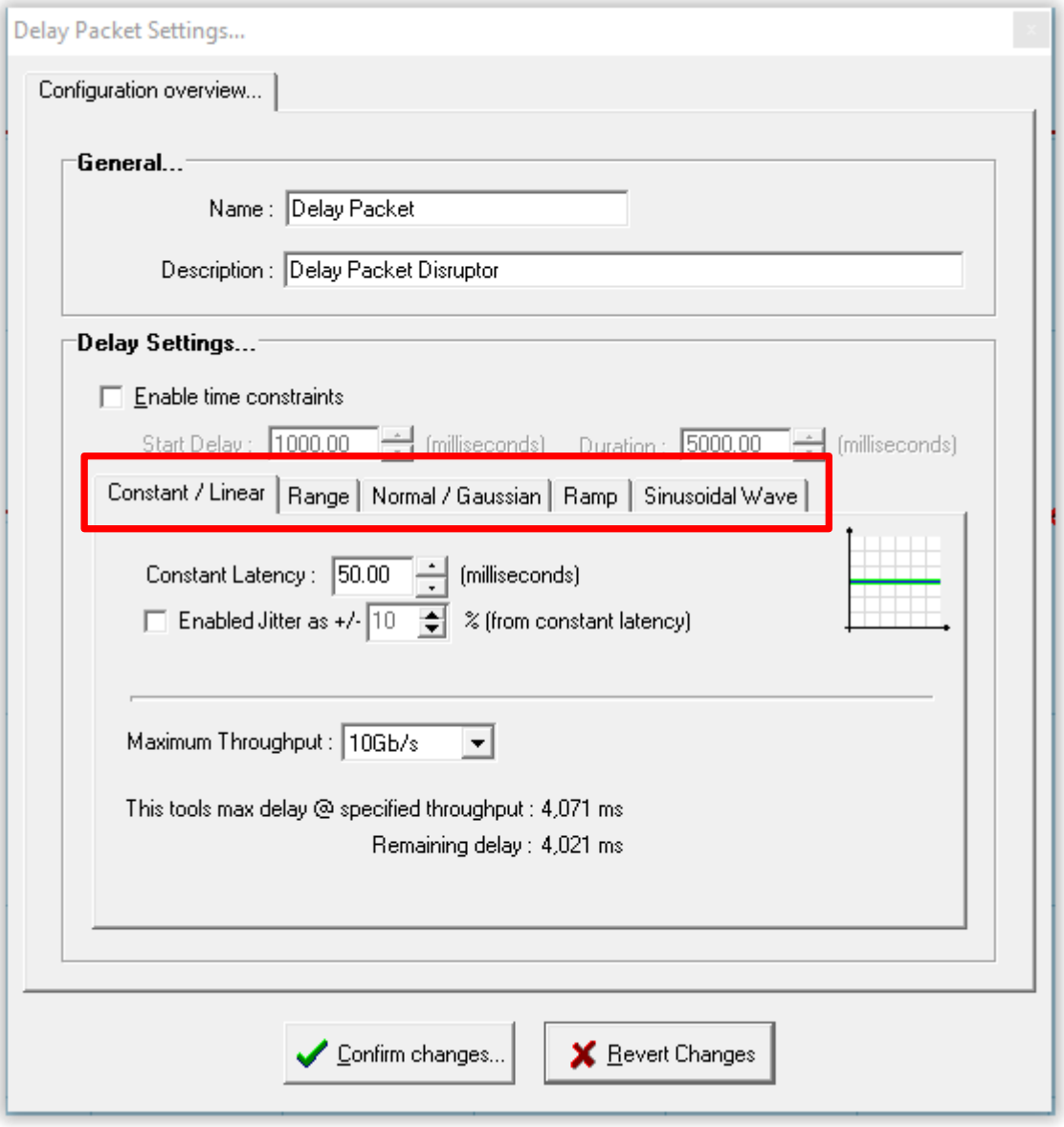
1. As before, pull out the Network Toolbox from the right side of the GUI
2. Click and drag onto the Design Pane the following icon for packet delay:

3. The following icon will appear on the Design Pane:

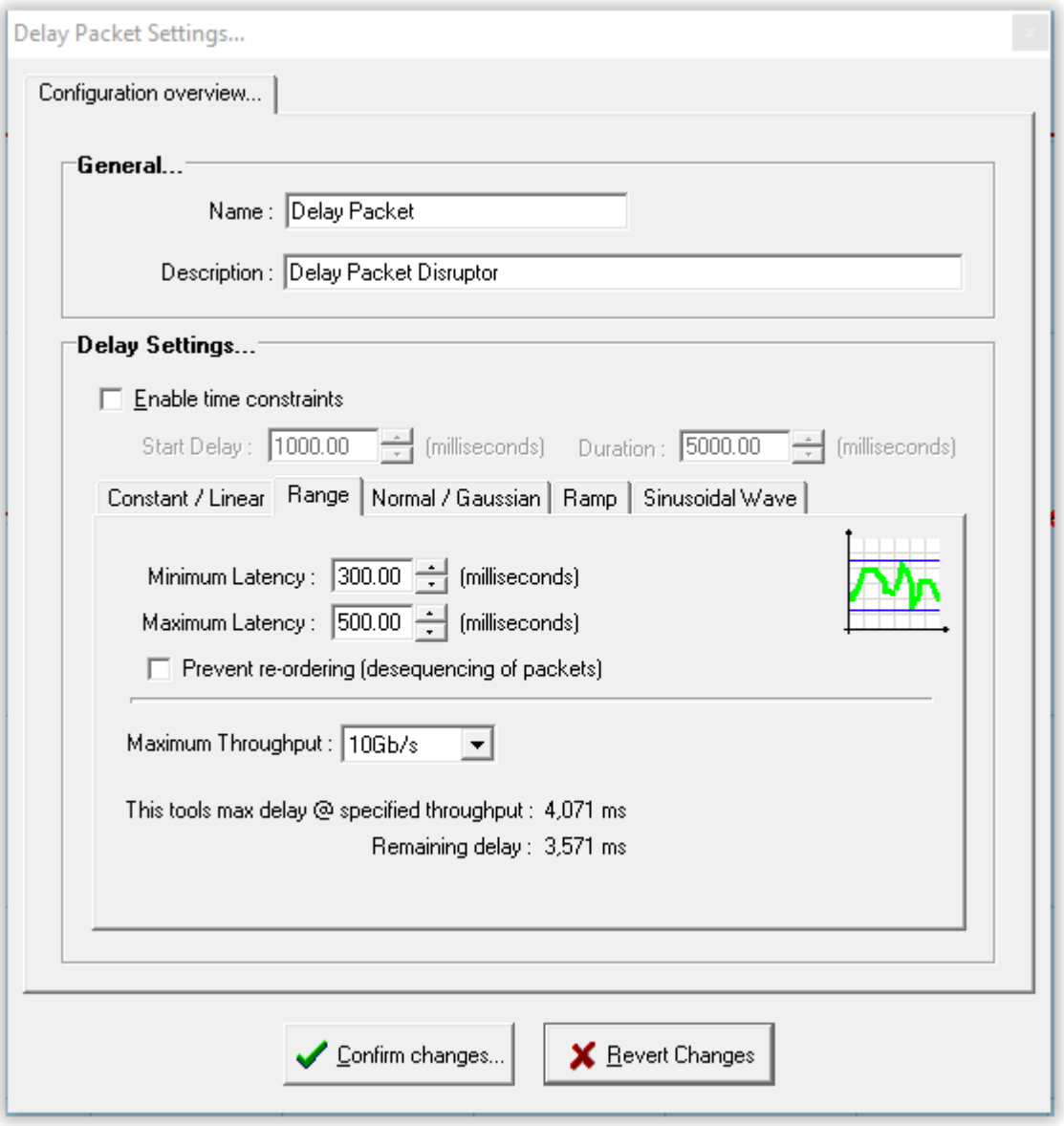
4. As before, drag it onto the connection between Port 1 (network start point) and Port 2 (network end point), as shown below:



5. Right-click the Delay Packet icon and select 'settings'.
6. Click the Range tab.

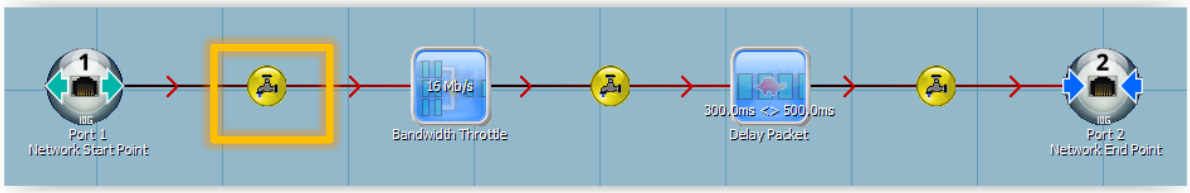


7. Set the minimum latency to 300 milliseconds, and the maximum latency to 500 milliseconds (this is very high latency but we will use it for illustrative purposes in this example):



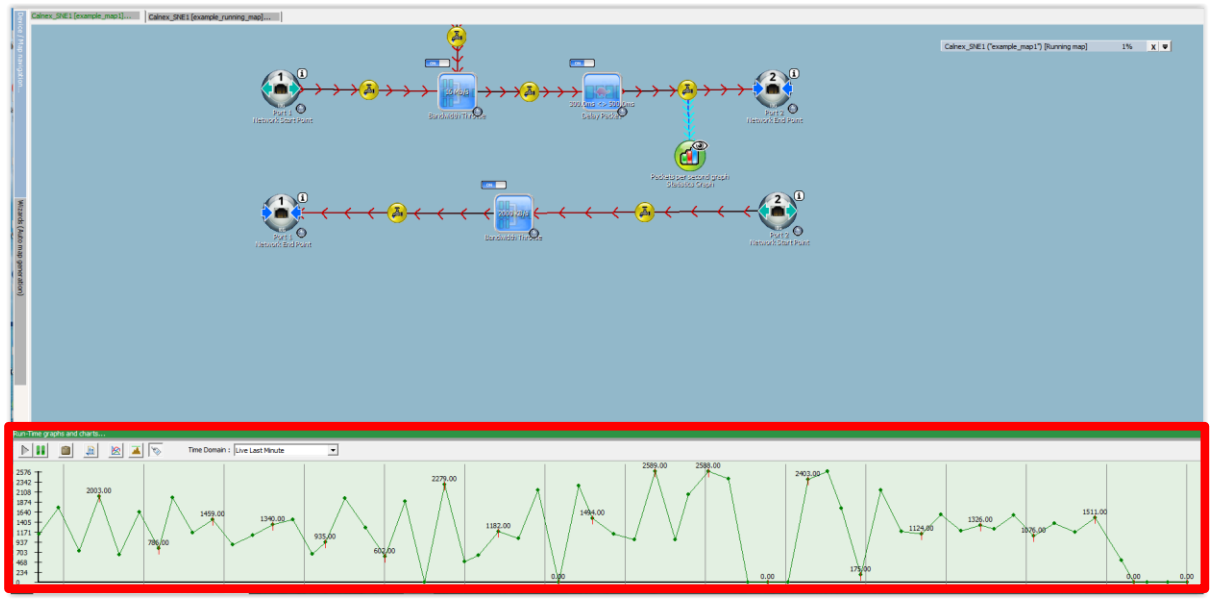
8. Press ‘confirm changes’

The emulation will now act as an ADSL line which is suffering from very significant congestion, ranging from delays to packets of anything from 300 to 500 milliseconds. This would evidently interfere with the delivery and resulting quality of application traffic sent across this link.



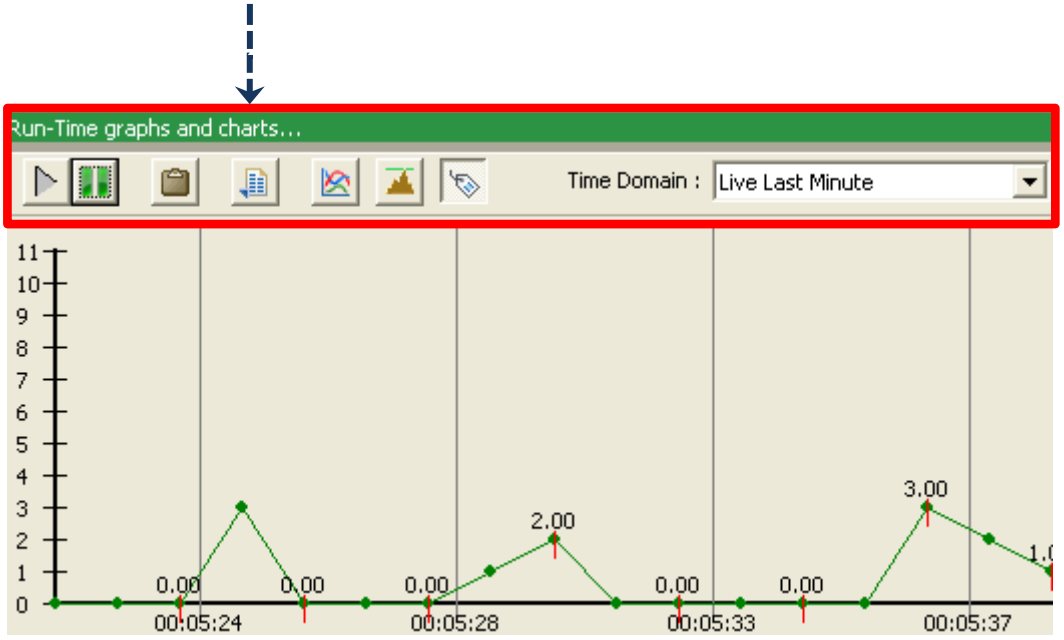
1. Right-click on this icon and select ‘Add Statistics Graph Tap’.
2. The statistics graph should be added as shown below:

3. The default graph attached is the ‘packets per second’ graph, which will show the number of packets passing this TAP point following the bandwidth throttle and the packet delay that were added previously.
4. Click on the ‘Play’ button as described in step 3 above, in order to begin emulation.
5. The emulation map will execute as before, and a new screen at the bottom of the GUI will appear, showing the statistics graph we have now added:



6. The grey section shows a simple line graph of the number of packets being sent past the TAP icon every second.
7. Options on how to change this view, as well as how to export the data, are located on the top left of the stats graph pane, as shown below:

The stats graph allows various operations on the received information.
Play/Pause, Save to Clipboard, Save to CSV File, Show Average, Show Peak, Smart Labelling on/off and the ability to adjust the visible time domain.



10.9 Summary

This completes the walkthrough of the example emulation run. Please note that most of the control and functionality of SNE was not shown here – the sections below provide more information on the SNE rich feature set and reporting options.

SNE Sandbox
SNE inbuilt sandbox (located in the GUI's left navigation bar 'device/map navigation') is an 'offline' area for designing emulation maps. Maps can be built and stored here, then copied over to a 'live device' by right-clicking the map you wish to move.

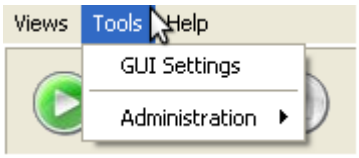
The sandbox can be beneficial to save time when another user is performing an emulation, or it can act as a safe area for new users to practise the creation of emulation maps.

11 GUI Walkthrough - Master Menu Bar

This section will describe SNE GUI in detail, including its features and functionality.

11.1. Tools Menu

Returning to the Master Menu Bar, the next option is 'Tools'. Under this heading are two further options: 'GUI Settings' and 'Administration', as shown below.

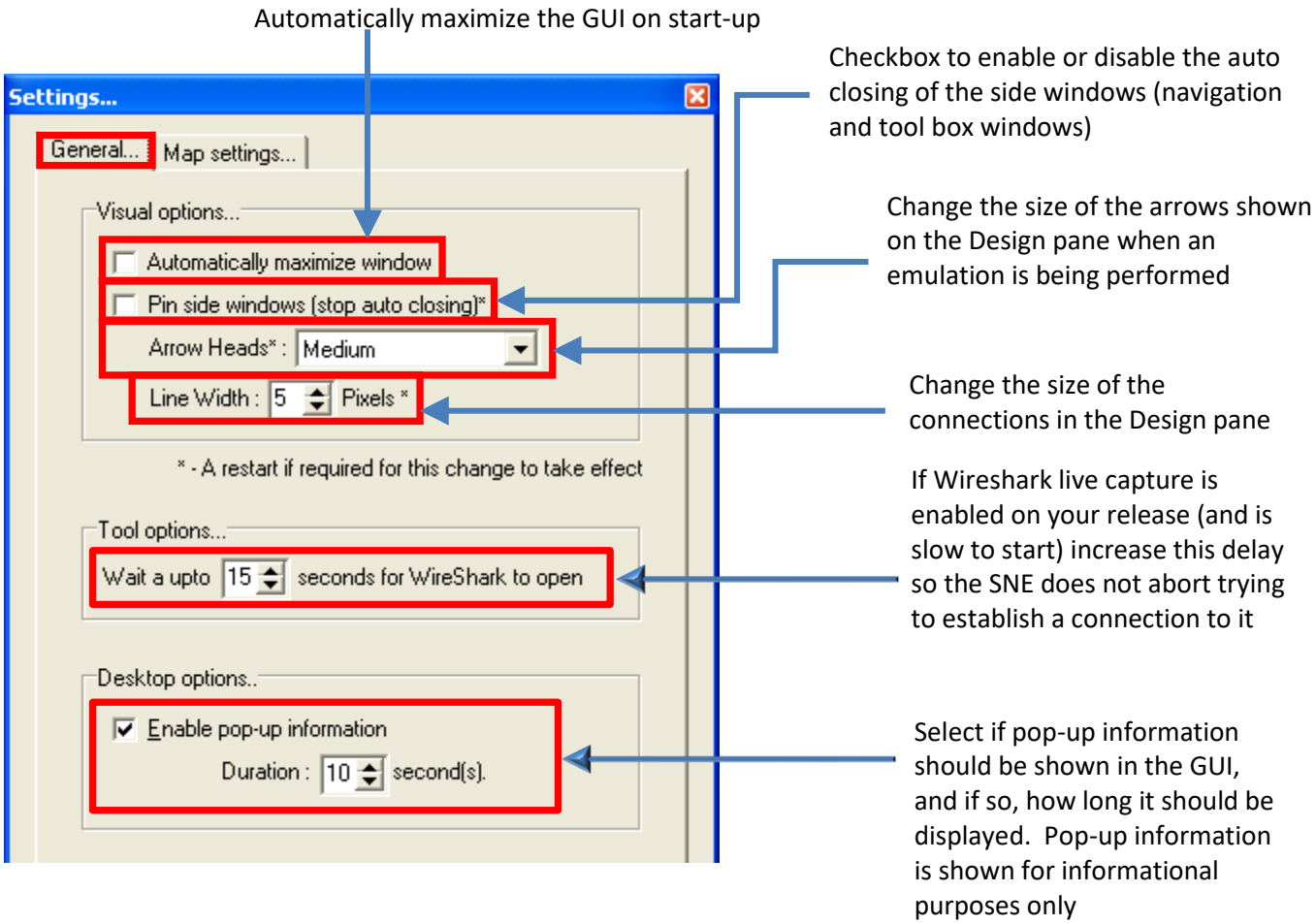


11.1.1. GUI Settings

The GUI Settings menu provides the user with options to change the layout and functionality of the user interface, as follows:

11.1.1.1. General Tab

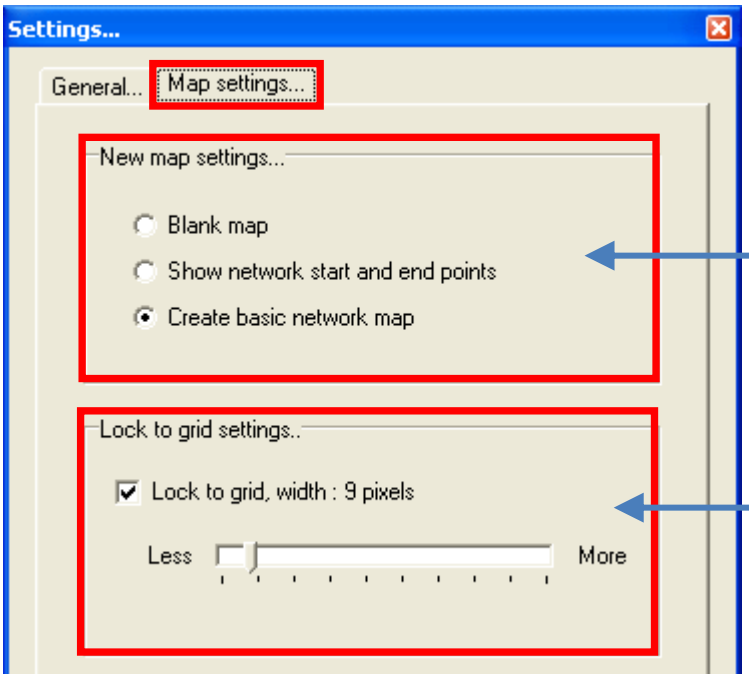
Please see below for a visual description of the GUI Settings 'General' tab:



Please note that for many of the settings above to take effect, a GUI restart is required.

11.1.2. **Map Settings Tab**

Please see below for a visual description of the GUI Settings 'Map Settings' tab:



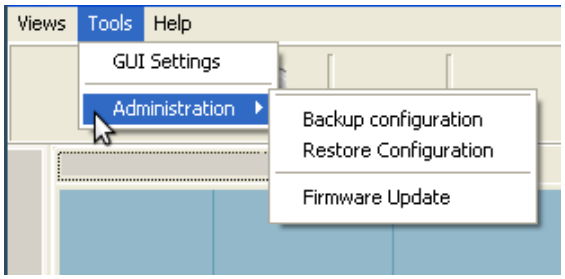
Define what should be created when a new map is created by right-clicking on the 'Map/Device Navigation bar' and selecting 'Create new Map' from the pop-up menu. A blank map can be created by selecting "Create blank map" from the pop-up menu.

Define if, and by how much, objects added to the Design pane should be snapped to an underlying grid. To select complete free form positioning, uncheck the 'lock to grid' checkbox

Please note: The "Multiuser GUI Settings" section is discussed in detail in the advanced operations section.

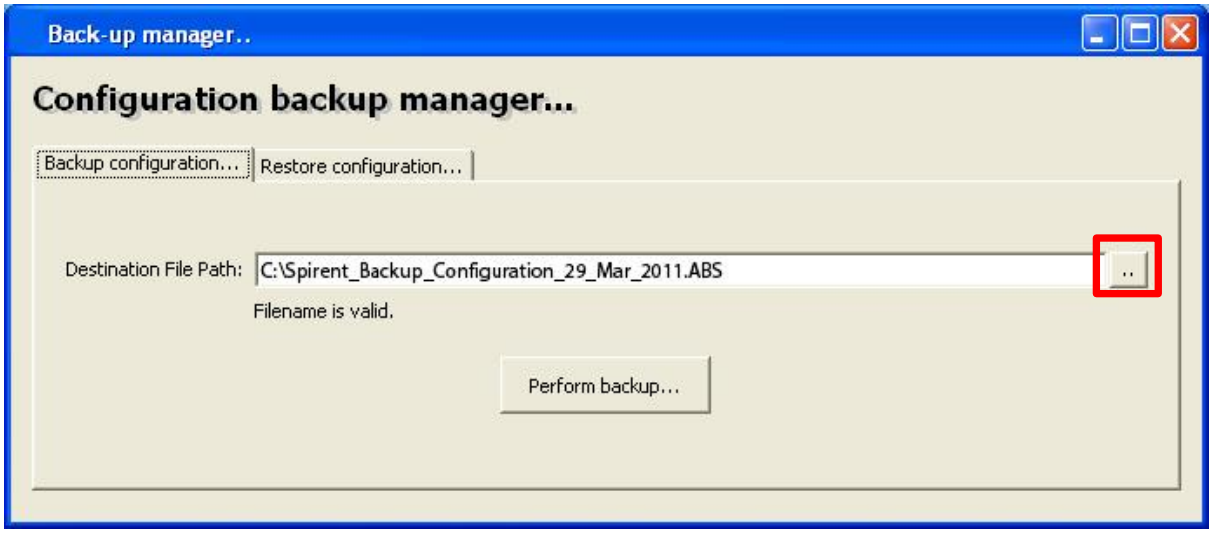
11.1.3. **Administration**

The second option on the Tools menu is 'Administration', which contains three further menus as shown below:



11.1.3.1. **Backup Configuration**

This is an important feature within SNE GUI, which provides the user with the ability to perform a complete back up of all emulation maps that have been designed, their settings and some current GUI settings. It is highly recommended that back-ups are performed on a regular basis to ensure there is no loss of data if the GUI or system it runs upon become unstable.

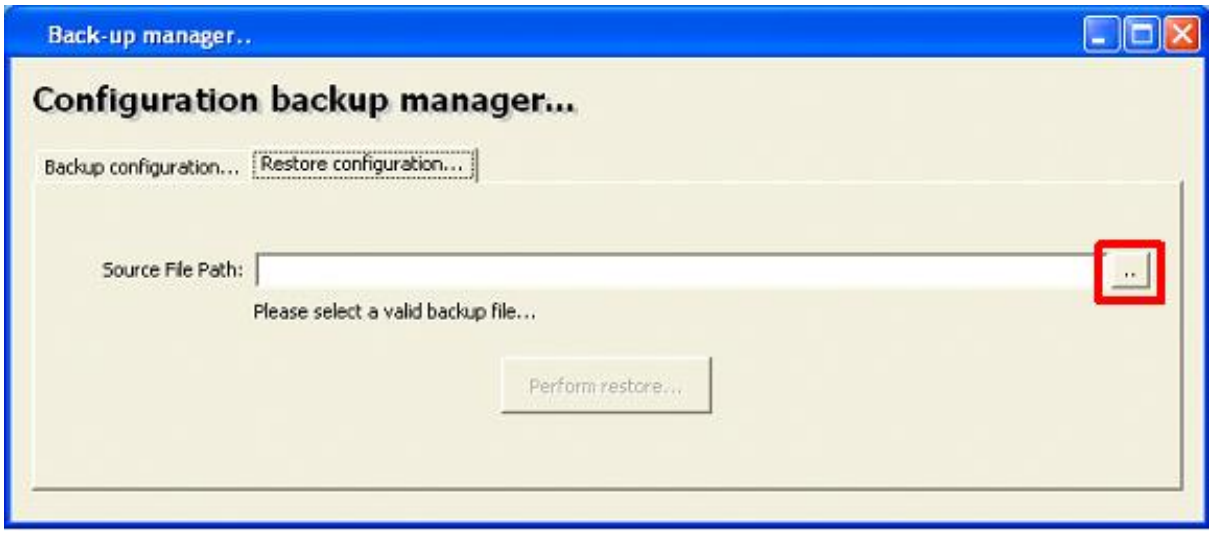


The back-up manager will display a default filename for the file using the current system date settings. You can change the filename and/or path by clicking in the "Destination File Path" field and amending, but the file extension (.ABS) must not be changed otherwise any restoration of this back up may fail. You can change the location where the back-up file is to be saved by clicking on the file navigator icon (highlighted in red above).

Please Note: Always check your back-up file has been created. This facility may silently fail if you do not have privileges to write to the destination folder - it is recommended you save back-ups to your "My Documents" folder if using Windows.

Restore Configuration

There may be instances when a restoration to a previous version of SNE is required. To access back-ups select the 'Restore Configuration' option under the 'Tools' and 'Administration' menus, and navigate to the folder which contains the previously backed up file. To assist, the user can open the file navigation system by clicking on the icon highlighted in red below.



11.1.3.2. Firmware Update via Web UI

SNE supports the remote updating of its firmware. This process is largely automated but care should be taken when performing this operation:

CAUTION – Possible loss of operation may occur. If the product is power cycled or interrupted during the firmware update it may fail to operate correctly and require shipping to us for reprogramming. This is not covered by the warranty.
All network port cables MUST be disconnected during the firmware update process.

Retrieving your firmware update
We do not actively push firmware updates to our customers, if you wish to receive the latest firmware from us please e-mail Support.

The Firmware Package
The SNE's firmware is released in a 'package' file, with the extension '.pck'. As well as containing the new firmware, this package file contains version and validation information. This information allows you to see what version you are upgrading to and make sure the package has not been corrupted in transmission to you.

Understanding your firmware package
Each firmware package presents new features, bug fixes and improvements. You should carefully read the included release notes (available online) for any impacts these new features may have on your existing network maps - if any. By installing the firmware, you agree to accept and be bound by any new or updated terms and conditions (available online).

GUI implications
Please refer to the release notes about any GUI implications. Normally major firmware updates are associated with major GUI updates. If you have received both a firmware package and GUI update, please install the firmware update from the current installation of the GUI. Once firmware has been successfully upgraded, immediately close the GUI, **uninstall the existing GUI** and launch the new GUI installation.

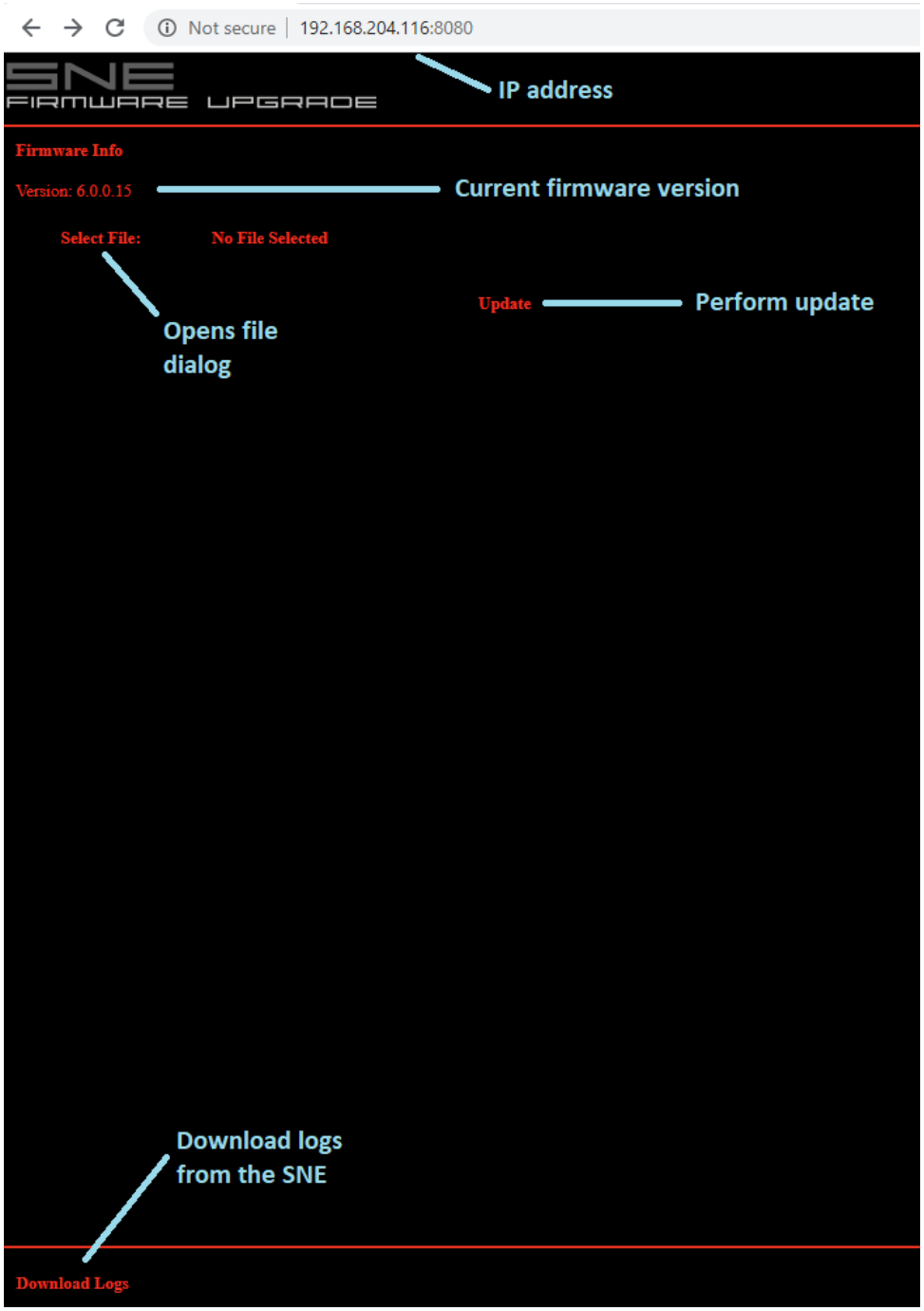
Failure to upgrade your GUI will result in a possible reduction in functionality and incorrect operation.

Firmware Update – Step One – Prerequisites
Please ensure you have the required firmware package file located on your local hard-disk. This is usually named "sne-release-*<version number>*.pck" or something similar.

Ensure that your SNE unit is powered on and connected / visible in the GUI. **You must not have any emulations (maps) running.**

Firmware Update – Step Two – Opening the firmware web updater
Open the firmware update webpage by navigating to the IP Address of the SNE in a web browser (IE, Chrome, Firefox etc...).

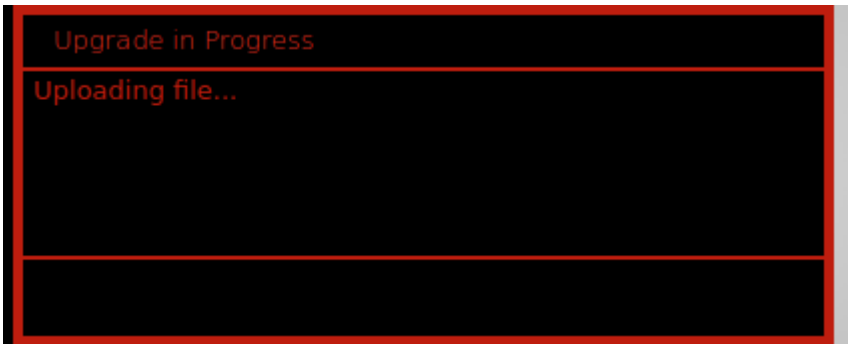
Firmware Update – Step Two – Understanding the firmware window
The firmware window contains many important pieces of information that help assist you with the update process. The window looks as follows:



IP address: This is the IP Address of the SNE you are currently connected to for the purposes of upgrading the firmware.
Version: This shows the current firmware version. This is also available from the 'Settings' window on each SNE unit (in the Map/Device Navigation Bar on the left of the main GUI).
Select File: Click here to browse to the location of the firmware package file.
Update: Once you have selected the firmware .pck file to send to the unit, clicking this button will begin the update.

Firmware Update – Step Three – Selecting your firmware package
Click on Select File to bring up the file dialog. Once you have located your firmware please select it. You will see the file has been selected as the wording "No File Selected" will change to the .pck file you have just selected.

Firmware Update – Step Four – Starting the update
Click on the 'Update' button.
The .pck file will now be uploaded to the SNE and a popup box will be displayed to show you the current process that is taking place.



Firmware Update – Step Five – Finalisation
Once the update has finished the SNE will reboot so that it can bring up the new firmware. After 2 minutes please refresh the webpage and you will now see the current firmware version has now changed to match the latest .pck file.

If the version numbers do not match the .pck file that was uploaded please contact Support.

Firmware Update – Step Six – Optional GUI Update
Major firmware updates are usually accompanied by an updated GUI to allow the user to access new features or functionality.

Please uninstall the GUI, from Control Panel > Programs and Features. Click on the new GUI installation application (normally "setup.exe") and following the on-screen prompts.

11.1.1. Help Menu

Returning to the main Master Menu bar, the last sub menu is 'Help', which contains three options: 'About', 'Activate Product' and 'Dump XML'.

11.1.2. About

Within this option are the terms and conditions relating to the SNE, and its operation, alongside information on the license agreement. **By using Central GUI you are deemed to have accepted the terms and conditions present within the GUI (including any updated terms and conditions)**

11.1.3. Activate Product

Upon installation, the GUI should prompt the user to activate the product using the activation key supplied with the SNE hardware box. If for any reason this screen does not appear, the user can open the Activate Product window from the master menu bar, and follow the onscreen instructions (or those found in section 6.6 of this manual).
If you have licensed additional tools, you will receive a new license key – this should be entered here.

11.1.1. Save Map XML / Show Map XML

The underlying protocol between SNE's and the GUI is XML over TCP. This option allows you to dump the XML from the current map in order to assist with automated testing. Please contact if you would like more information on placing the SNE within your automated test environment.

12. Routed and Bridged Operations Overview

This section details the differences between the routed and bridged mode operations of the unit.

12.1. Introduction

Bridged mode provides a “bump in the wire” network emulation; the SNE unit will sit invisibly between the various systems under test and inject impairments as created by the user.

Routed mode provides Virtual Routers (VRs) that are attached to each physical port, which allows each physical port to act as a router to provide access to a larger network through different subnets.

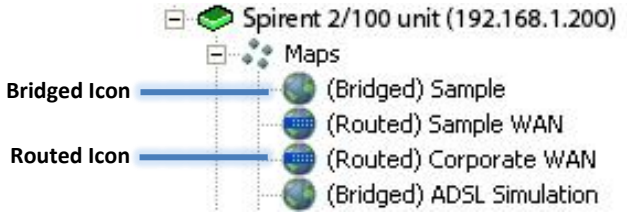
Each Virtual Router has the ability to handle DHCP requests, ICMP messages and provide statistics on DHCP leases, physical and network packets. In Routed mode impairments are placed between each Virtual Router to simulate the required network.

12.2. Selecting the required operation

Locate the “‘Map/Device Navigation” window on the left side of the GUI. Right-click on the hardware you wish to add the map to and select the required operation “New routed mode map” or “New bridged mode map”.

12.3. Visualisation of operation

The “‘Map/Device Navigation” window shows all available network maps; the routed and bridged maps have the words “(Bridged)”and “(Routed)” appear next to their names. The icon used to represent the network map also changes to show the map’s operational mode.

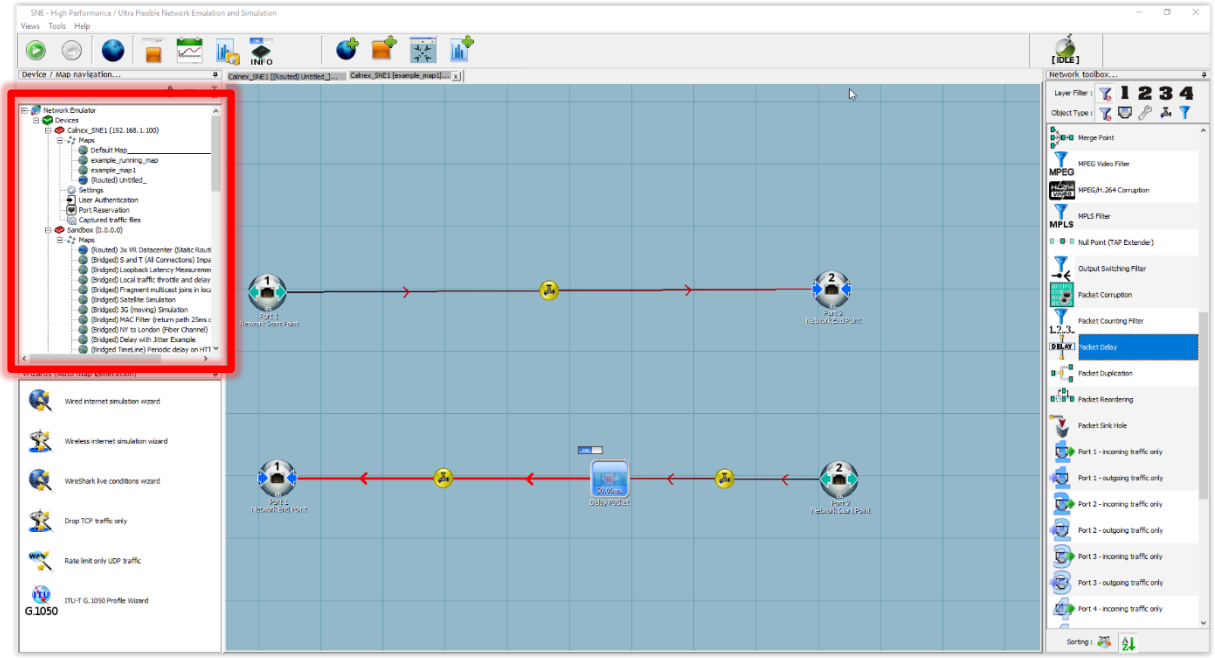


12.3.1. **Tool Differences**

Given the nature of Routed mode and Virtual Routers, the available tools are different. The first major difference is routed mode provides ‘Virtual Routers’ which can be added to the network map. Please note that Routed mode does not currently support filters.

13. GUI Walkthrough - Map/Device Navigation Bar

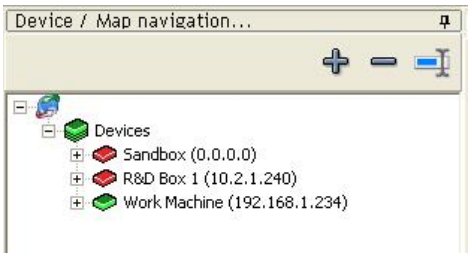
Located on the left of the GUI is the 'Map/Device Navigation' bar, as highlighted in red below:



The map/device navigation bar allows the user to logically group the SNE hardware units (known as 'devices') and maps that have been designed for each device. It also provides access to settings which are specific to each SNE device. If only one SNE hardware unit has been purchased, this view is limited to one device, although please note a 'sandbox' will also appear in the map/device navigation bar. The 'sandbox' is explained in more detail below.

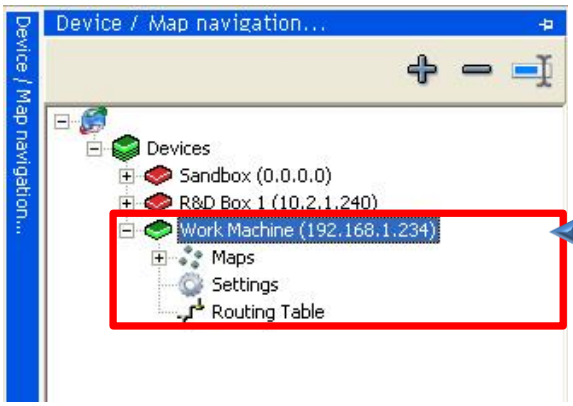
13.1. Contents and Settings

Upon installation, your SNE hardware unit will be visible in the Device/Map navigation bar, titled "SNE". Also present in this pane will be a virtual device titled 'Sandbox'. The sandbox is an offline, 'design-only' area where new maps can be designed if another user is currently running an emulation. Offline devices (e.g. SNE hardware units which are currently not connected or turned on) will be denoted with a red icon, and the device from which emulations can be performed will be denoted by a green icon. In the screenshot below, both the Sandbox and the 'R&D Box 1' devices are offline, while the 'Work Machine' device is online and can perform emulations. Multiple SNE devices can be added to each instance of the SNE GUI.



By default, and to aid recognition the IP address of each device is shown in brackets after the device's name.

Each device holds the network emulation maps that have been created or copied to it, alongside device specific settings. Optionally there is the device's routing table and captured traffic lists (if licensed). By clicking on the '+' expander icon beside each device, the user can view these options, as shown below:

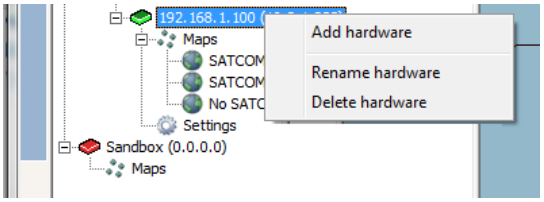


Expanded device titled 'Work Machine', showing 4 further options: 'Maps', 'Settings', 'Routing Table' and "Captured traffic" - Your configuration may differ from this example.

13.2. Adding, renaming or removing hardware

The 'Device/Map Navigation' pane provides the ability to add new hardware (i.e. another SNE hardware device), rename existing hardware devices and delete unwanted devices.

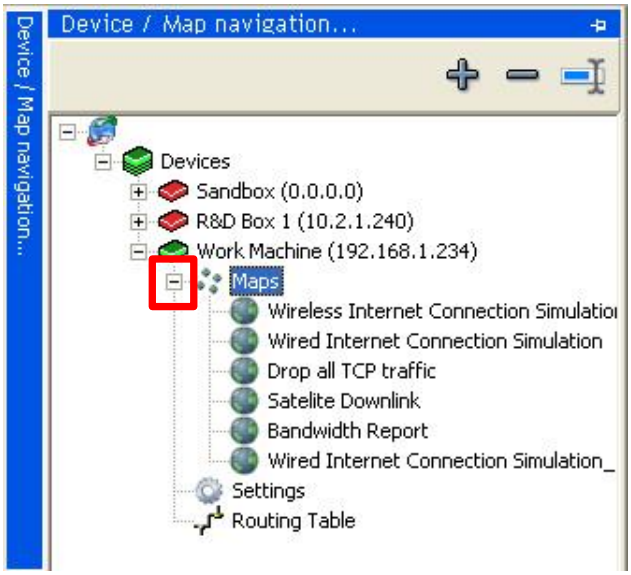
By right-clicking on the title of any hardware device (in the above screenshot, for example, the user would right-click on 'Work Machine (192.168.1.234)', three options are displayed. These are:



- **Add hardware**: Adds a new piece of hardware using its IP address
- **Rename hardware:** Changes the title of the hardware
- **Delete hardware:** selecting this option will remove the device, all its settings and all maps assigned to it from the GUI. It is strongly recommended that a back-up is undertaken prior to deleting a device from the SNE GUI.

13.3. Maps

Maps are at the core of the SNE and its operation. These are the visual representations of the intended WAN and each is stored against a SNE device in the 'Map/Device Navigation' pane. SNE ships with a series of default emulation maps, these are accessed by expanding the '+' icon as highlighted in red below:

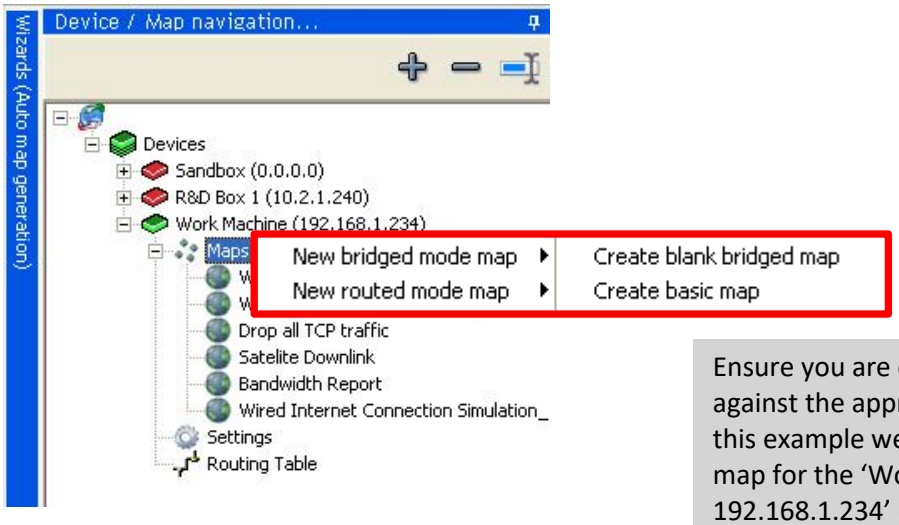


Please note: depending on your software configuration, your view may be different. The graphic to the left is for illustrative purposes only.

By double clicking on any of these maps, they will each appear on a new tab within the main Design pane and are then ready for modification or emulation. **Please note: once a map is modified in any way, the changes are saved automatically** - it is recommended that if a user is unsure if they wish to make any changes, they should make a copy of the map and rename it before proceeding.

13.3.1. **Creating a new map for emulation**

Creating new maps is simple: within the map sub-menu, right-click on the 'Maps' title (or any actual map listed) and select which type of map you want to create as your starting canvas:



Ensure you are creating the new map against the appropriate device – in this example we are creating a new map for the 'Work Machine 192.168.1.234' device

- **New Bridged Mode Map - Create blank map:** creates a new bridged mode map, called '(Bridged) untitled' in the Design pane, with no WAN impairments or start/end points. These are then added via the 'Network Toolbox' menu to the right of the GUI
- **New Bridged Mode Map - Create basic map:** creates a new bridged mode map, called '(Bridged) untitled' in the Design pane. The network map is created blank, with just network

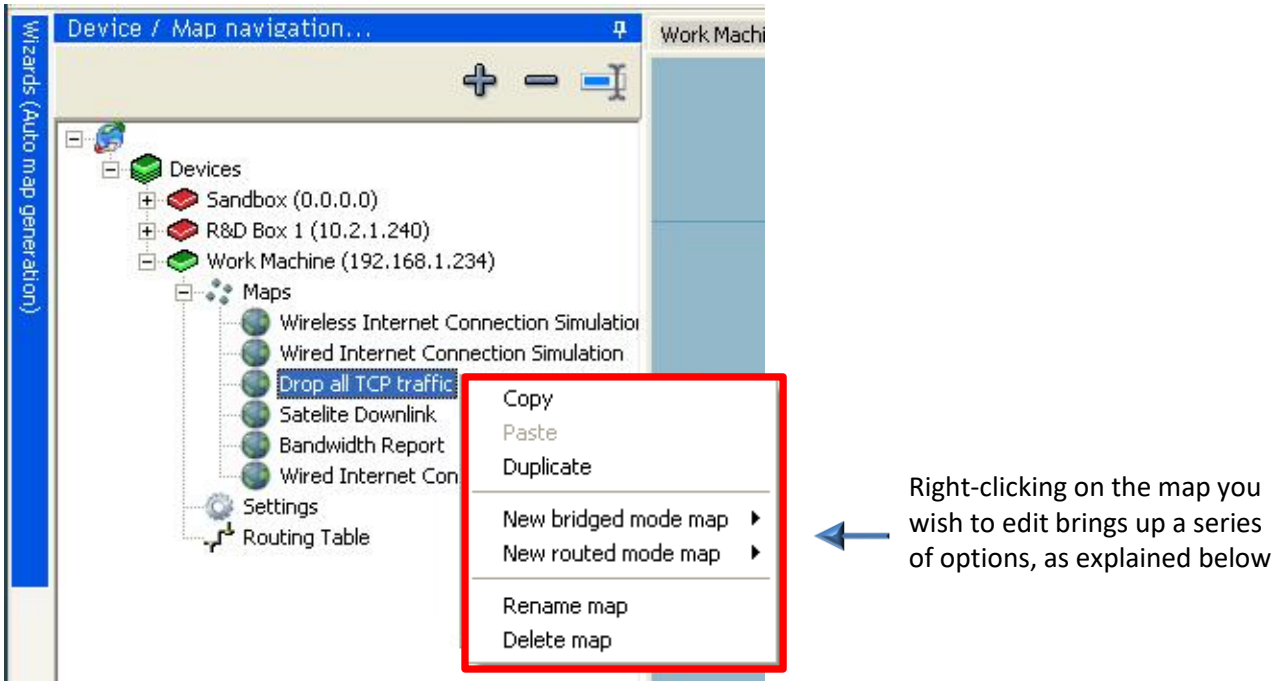
start/end points. The choice of which map is created is decided by the "Map Settings" panel on the 'GUI Settings' window

- **New Routed Mode Map - Create blank routed map:** creates a new routed mode map, called '(Routed) untitled' in the Design pane. The network map is created with no virtual routers, physical ports or impairments.
- **New Routed Mode Map – Routed Mode Wizard:** This option will show the routed mode wizard, allowing you to select IP and DHCP information for each Virtual Router. The network map will then be created to represent the supplied information.

You will note that the map is stored against the device in which it was created. Options for moving maps between devices are explained below.

13.3.2. **Amending Maps**

Maps that are created can be duplicated (within the same SNE hardware device), copied (to a different device), renamed or deleted. This is achieved by right-clicking on the map that is to be amended, which will display the following sub-menu:



- **Copy**: the selected map, its name and all its setting are copied into the clipboard. Use this feature when you wish to copy a map from one device (such as the sandbox) to another (such as a connected SNE hardware device, ready for emulation).
- **Paste**: this option will be greyed out (as shown above) until another map has been copied to the clipboard. Once selected, it will transfer the copied map to the chosen location, including a different SNE hardware device from the one in which it was created.
- **Duplicate**: this copies the selected map, its name and all its settings, and pastes an exact replica within the same device. The duplicate is recognisable by its title, which will be the same as the original except it will be post fixed with an underscore.
- **Create blank map, create new map**: these options create a blank map or a basic map with options chosen from the "Map Settings" panel on the "GUI Settings" window.

- **Rename map**: this option allows the user to rename the map, and can be relevant when copying or duplicating maps
- **Delete map**: this removes the selected map from the device, including all its settings. Please note that this deletion is normally permanent, contact if you accidentally delete an important network map.

Saving and storing

The SNE GUI automatically saves all changes made to any map or SNE hardware device. However, we highly recommend, particularly in a multi-user environment, that regular back-ups are performed and the copying/pasting of maps (as back-ups) into the sandbox is undertaken.

13.4. Device Settings

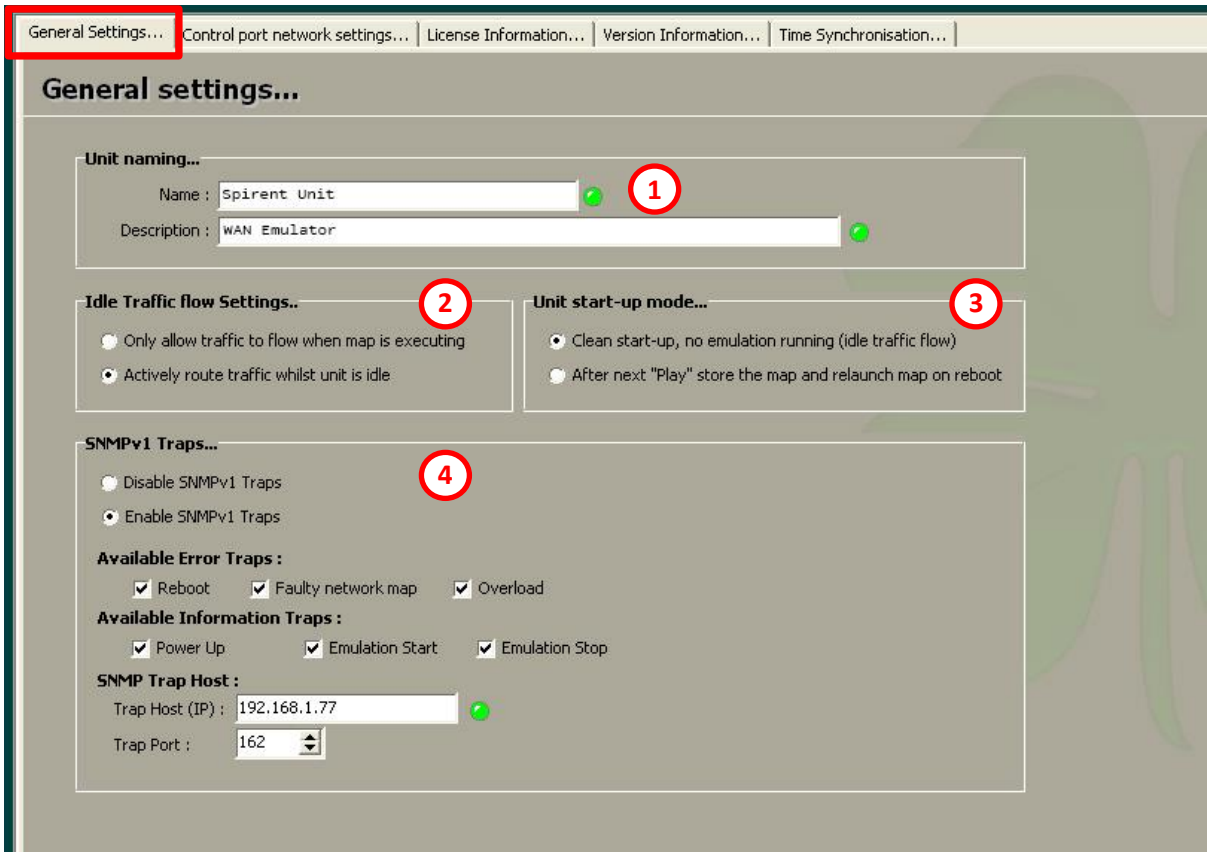
Each device in the 'Device/Map Navigation' pane will have a 'Settings' option, as highlighted in red below:

The settings option for each device allows the user to define and change the SNE hardware device's configuration. By default, it opens on the 'General Settings' tab, as described below:

Please note that most of the settings are only visible when the unit is connected.

13.4.1. **General Settings**

Shown below is the General Settings tab:



1 **Unit Identification**

Name: Change the name of the SNE hardware device if required - use this field to intuitively name each of the SNE device, which becomes increasingly important when more than one SNE device is in operation.

Description: Provide a description of the SNE device, if required, for intuitive identification.

2 **Idle traffic flow settings:**

Only allow traffic to flow when map is executing: No packets will be sent over the physical link between the devices connected to the SNE hardware unless an emulation is being performed. This is useful for Virtual Routing when you do not want packets to “leak” from paired ports when the network map is not running.

Actively route traffic whilst unit is idle [Default Setting]: This option allows data sent from any devices connected to SNE to be routed through the hardware unit while no emulation is being performed.

In this instance the hardware will transmit packets between paired ports, acting as an invisible bridge between each paired port.

Auto-forwarding

By default the SNE hardware will automatically forward packets between paired ports (i.e. Port 1 <> 2, Port 3 <> 4, etc.) This allows for network traffic to flow as normal, with no WAN impairments introduced, when the unit is first powered on or no network map is being executed. When traffic is being forwarded, the LED titled 'Forwarding' on the front of the hardware unit will be lit.

3 Start-Up Mode

This option allows you to control the start-up mode of the emulator.

Under the default option the emulator will reboot into a vanilla mode where it will either forward on packets or disable traffic flow (according to "Idle traffic flow settings").

By selecting the "**After next 'Play' store the map and relaunch map on reboot**" option, the emulator will save the last successfully executed map and attempt to launch it after the next reboot.

4 SNMP v1 Traps

The emulator can generate SNMP v1 traps for error and information conditions. These traps are sent to a destination IPv4 address using the specified IP address and port.

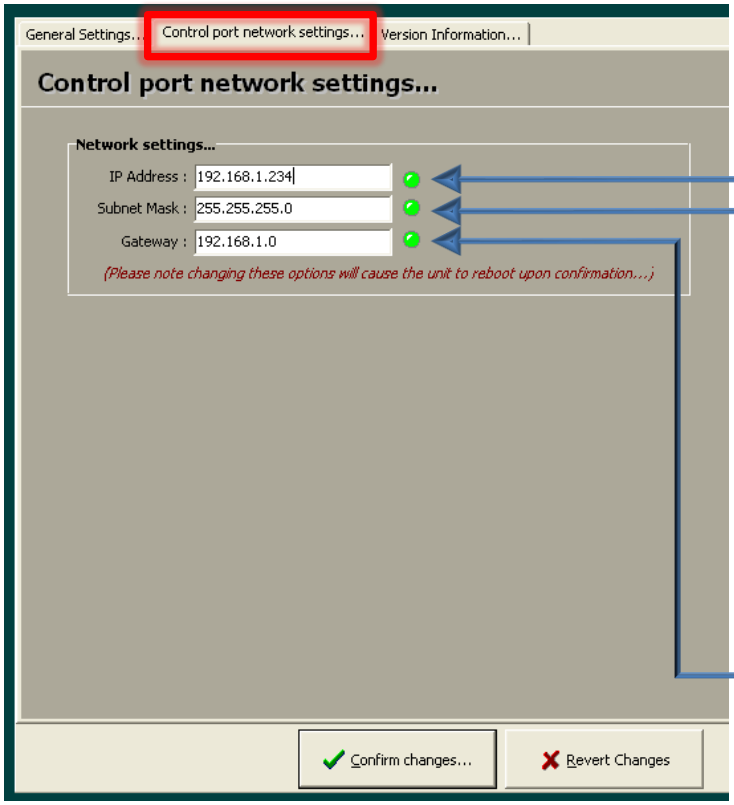
These traps are unsolicited and are not presented in any MIB table. Each trap is sent with an **OID** of "1.3.6.1.4.1.47881", **Trap Type** (TT) of 6 or "Enterprise Specific" and **Specific Trap Type (STT)** equal to the following table:

Trap Meaning	Specific Trap Type Value
Reboot	0
Faulty Network Map	1
Overload	2
Power up	3
Emulation Started	4
Emulation Stopped	5

13.4.2. **Control Port Network Settings**

The control port is located on the front right of the SNE hardware unit (silver) and is connected to a LAN that the computer running the GUI is located on.

Please note: if these settings are changed without the hardware turned on or connected to the GUI then all you will change is the IP address at which the GUI looks for the device. The SNE hardware's IP address will not be changed and the GUI will lose communications with it until the unit's IP address is restored.



IP Address: this uniquely identifies the device running the GUI.

Subnet mask: Provides the subnet mask for the unit, **please ensure the IP address is within this subnet range.**

Gateway: Gateway IP address.

The 'License Information' tab provides the ability to view licensing information and unlock further features should you wish to upgrade your unit in the future.

The 'Version Information' tab provides non-editable versioning data, which may be asked for by Technical Support. The information will be automatically updated if new firmware is sent to the unit following, for example, a new release of features/functionality.

13.4.3. License Information

This panel provides information on the currently installed license.

13.4.4. Version Information

This panel provides information on the current version of firmware.

13.4.5. Time Synchronisation

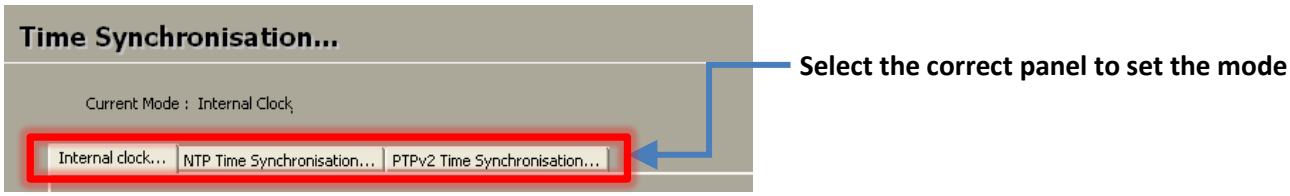
SNE produces time information with various operations, most notably the time stamping of packets within Wireshark captures or live streaming of packets via the Wireshark TAP device.

The hardware ships with internal hardware timers that allows for the high precision time stamping of packets.

For those units shipped with the optional external time synchronisation modules, you can select either Internal, NTP (Network Time Protocol) or PTP (Precision Time Protocol) as an external basis for keeping the hardware timer in sync.

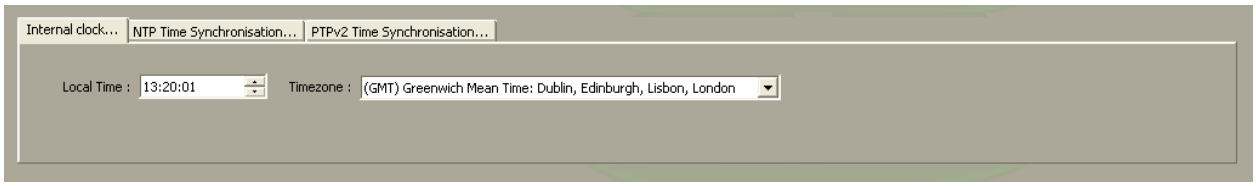
Time Synchronisation Selection

In order to select which mode of operation you wish, you must select the panel which reflects this mode and enter any application settings.



Internal Clock

This option is the “default” option and provides the ability to manually set the internal clock.

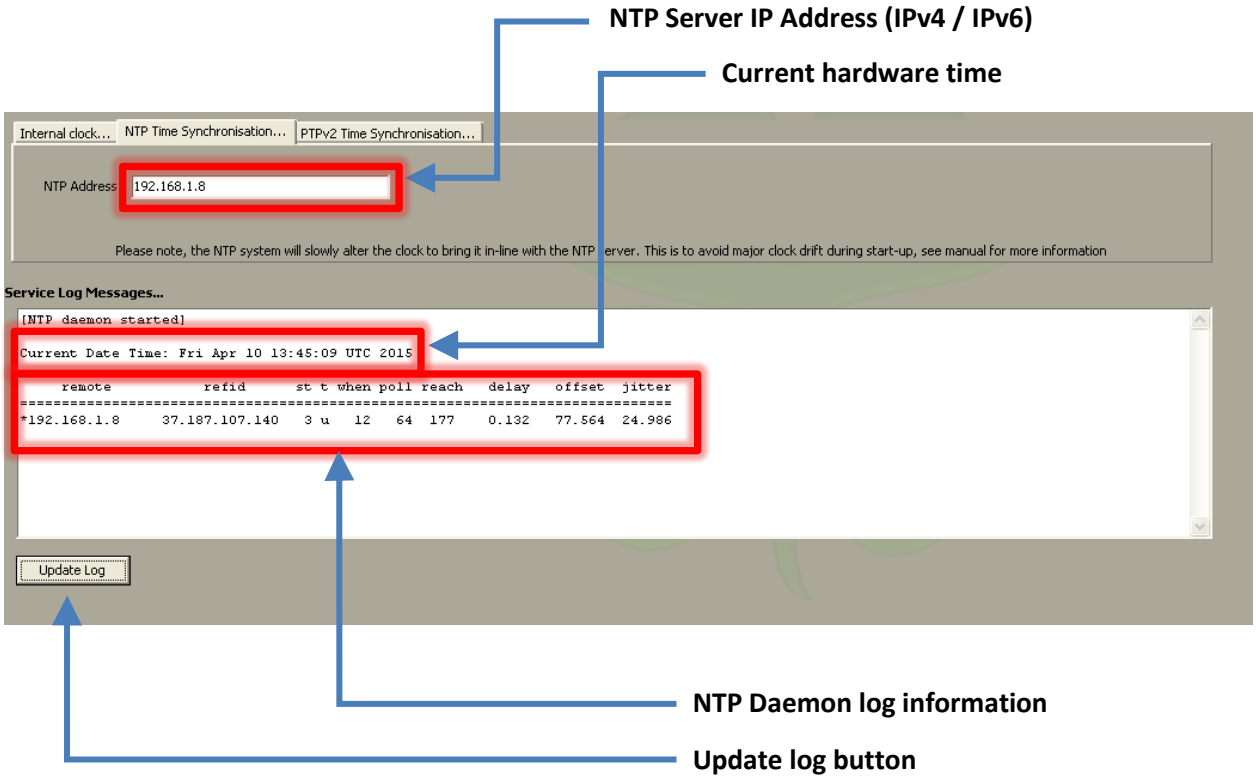


NTP Protocol

The NTP system provides a medium level of synchronisation accuracy by querying an external NTP server for the time. The time taken from the NTP server is used to drive the internal hardware timer to timestamp packets.

SNE requires that the NTP server is on the same local subnet as the emulator's control port. Therefore, if the emulator is configured as 192.168.1.100, a valid IP address for the NTP server is 192.168.1.9

Information on the success or failure of the NTP system can be obtained by clicking the "Update Log" button.

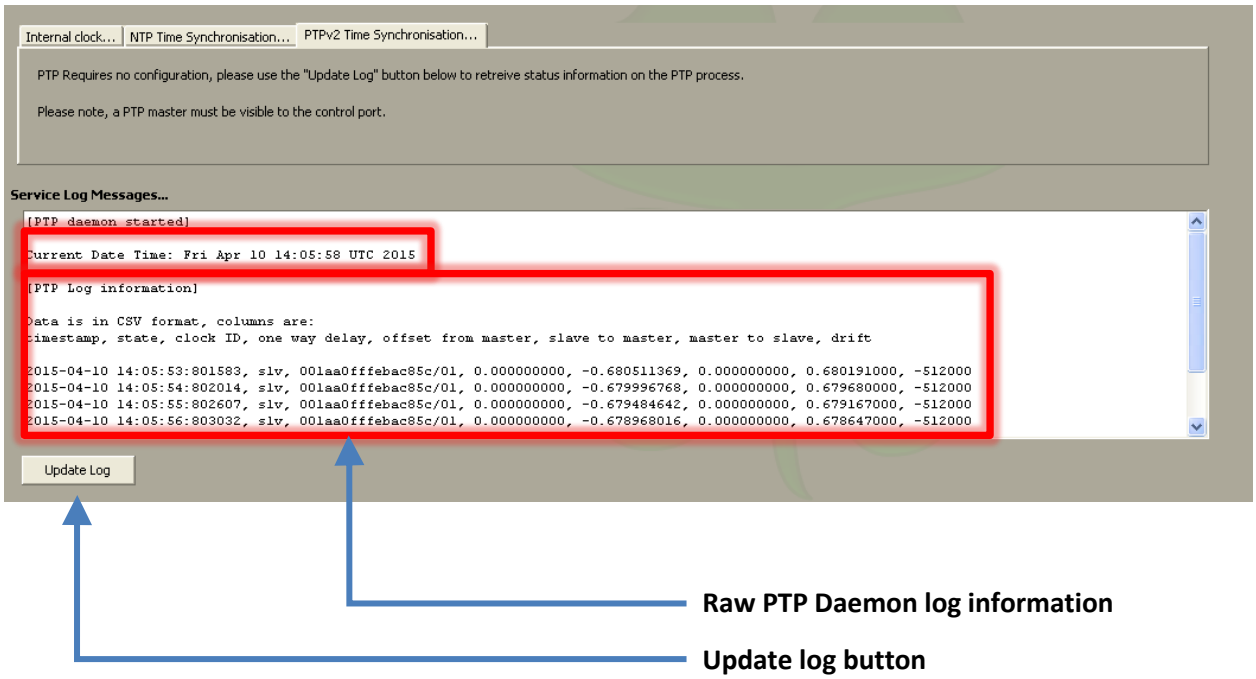


PTP Protocol

The PTP system provides an exceptionally high level of synchronisation accuracy by querying an external PTP server for a microsecond accurate time.

A PTP server must exist on the local Ethernet network connected to the Control Port.

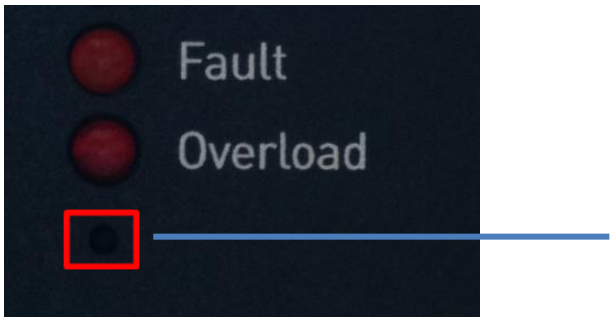
There are no configuration settings for the PTP mode; the PTP daemon will begin to broadcast requests to a PTP master on same network as the control port. Once a PTP master has been found the synchronisation of time is immediate.



The information provided by the daemon is in CSV format, and only the last 32 entries are reported.

13.5. Hardware Reset

Under certain circumstances you may be required to reset the SNE hardware to its default IP address, for example if you are unable to communicate with it due to limitations on your network. To reset the IP address to “192.168.1.100” please insert a small and long non-metallic object into the Reset hole as indicated in the following picture:



Reset IP Address “Pin hole” switch.

When the reset button is depressed the front panel LED’s will flash; continue to hold down the button for 10 seconds. At this point the unit will reset and then become available on “192.168.1.100”.

You will have to adjust the settings on the GUI so that it can communicate with the SNE unit now located on “192.168.1.100” – Please see section above 13.4.2 – Control Port Network Settings

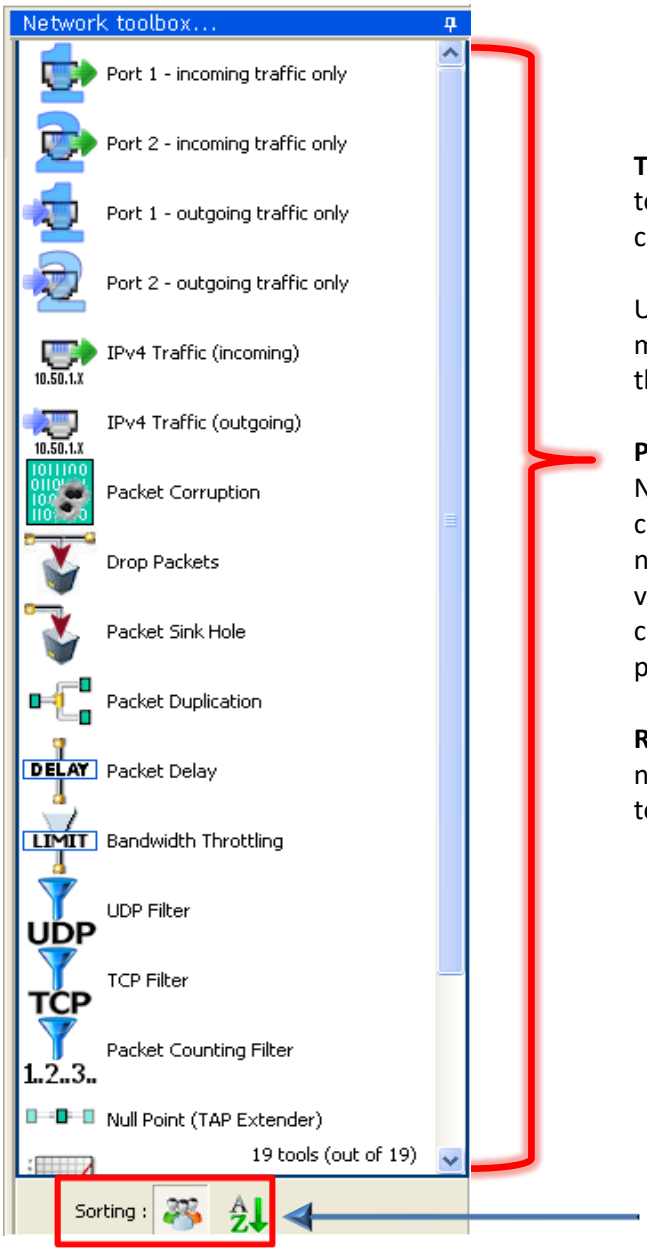
13.6. Captured Traffic Files

On the Map/Device Navigation bar, the user will also see an option titled ‘Captured Traffic Files’ (if available/licensed). This is where traffic that has been recorded is made available for download to a local hard drive or where previously recorded traffic can be uploaded for emulation. Please see section titled ‘stored traffic’ for full information.

14. Network Toolbox Overview

Located on the right of the GUI, the network toolbox contains the objects and impairments required to construct network maps for emulation. Icons in this toolbox can either be 'dragged and dropped' onto the main Design pane or can be double clicked and then dragged into position. The following diagram displays an example of how the network toolbox will appear and provides guidance on its navigation:

As the SNE tools are license based, you may have a sub-set of the tools shown in the screenshots here.



The main Network Toolbox pane provides access to all the tools and impairments required to construct network maps for emulation.

Users can drag and drop required icons onto the main Design pane, or double click to add them to the centre of the Design pane.

Please note: depending on the version of the SNE Network Emulator being used, certain configurations are not permitted (a warning will notify the user). For example, when using a 2-port version of SNE Network Emulator's hardware there can be no more than 2 incoming and 2 outgoing ports added to any single emulation map.

Routed mode vs Bridged mode: If the current network map is a routed mode map, the shown tools will be different than a bridged mode map.

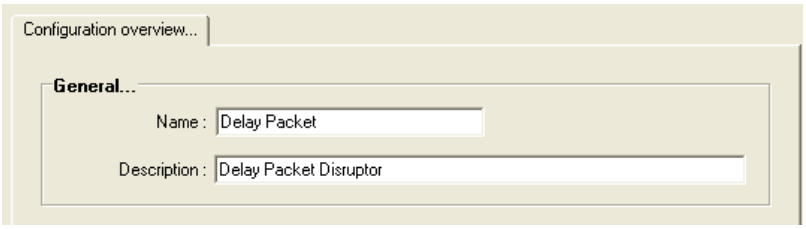
Tools can be sorted as follows:

- By group i.e. grouping all objects relating to ports together, grouping all impairment tools together etc.
- Alphabetically

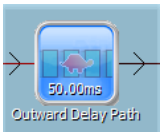
14.1. Tool and Impairments - General Settings

All tools and impairments within SNE have individual settings to allow powerful control over the exact conditions which require emulation - these settings are described in detail below. However, it should be noted that all tools in the Network Toolbox contain user accessible general settings which allow all tools to be re-named and their description changed, if required for ease of use or understanding by third parties.

Once a tool is added to the Design pane, right-clicking will show an option titled 'settings' (only available in Edit mode). When clicked on, the settings menu will appear and the first fields displayed allow the tool's name and/or description to be amended. Below is an example screenshot, showing the general settings section of the 'delay packet' tool:



If the user wishes to name the tool to better suit its specific use on any given network emulation map, they can change the above fields. In this example, the user may wish to change the "Delay Packet" name to reflect the true nature of the object such as "Outward Delay Path". The name is then reflected in the representation on the design pane.



The following section will step through the purpose, functionality and use of each tool available for designing and running emulation maps. Where possible, this has been limited to the tools provided for your configuration.

15. Network Toolbox

15.1. Overview

15.1.1. Bridged vs Routed mode

The available tools will change depending on the type of network map being displayed. For example, on routed mode maps you will find a selection of “Virtual Routers” and “WAN Points” which are missing from the bridged mode. The usage of some tools will also be different in each mode, for example the network start and end points have different purposes in routed mode.

For more information on routed mode and its tools please see the dedicated “Virtual Routers” section.

15.1.2. Licensed Tools

Depending on your model and license requirements you may have some or all of the available emulation tools, if there is a tool you require please contact and we will endeavour to activate the tool on your GUI.

15.1.3. Network Emulation Tools Available

The following sections provide detailed information on all the impairment tools available on the SNE.

15.2. Network Ports

Ports are fundamental in the operation of the SNE, as they represent the source and destination for data that is passed through the SNE and which is therefore subjected to WAN impairment. In effect, the user should consider each port icon within the GUI's Design pane as a network start or end point on the emulated WAN.

15.2.1. **Use in Bridged Mode**

Bridged Mode permits the flow of all packets from physical ports (2, 4 or 8 ports depending on the model) to enter and leave the WAN emulation. All data received from a specific port will be passed to an opposite port (subject to the network port being used in the emulation map) and vice-versa.

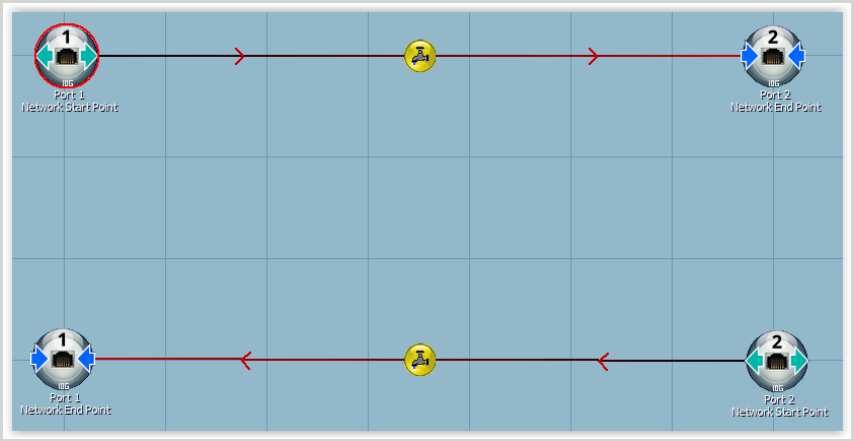
For example the bridged mode is most applicable when there are two (for 2 port unit) devices under test (DUT) physically linked to the SNE network ports 1 and 2 (i.e. no switch or router before the DUT). Using bridged mode also removes some of the complexities associated with virtual routing (for example, they do not need to use DHCP to obtain IP addresses).

Bridged Mode: Bi-directional Impairment

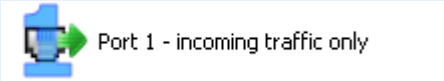
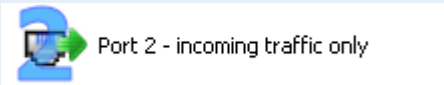
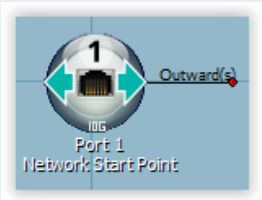
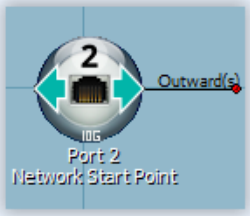
The SNE can perform emulation bi-directionally i.e. data both sent and received by each device connected to the SNE hardware unit can be subjected to WAN impairments. Within the GUI's Design pane, this is represented by 2 network start points (i.e. port 1 and 2) and 2 network end points (again, ports 1 and 2).

Data being sent from the device connected to port 1, to the device connected to port 2

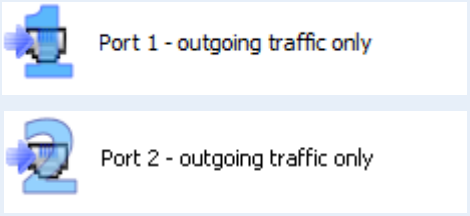
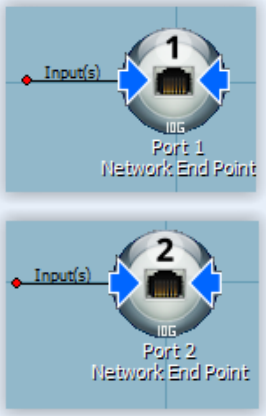
Data being sent from the device connected to port 2, to the device connected to port 1



15.2.2. **Bridged Mode: Port 1 -> Port 8 – incoming traffic only**

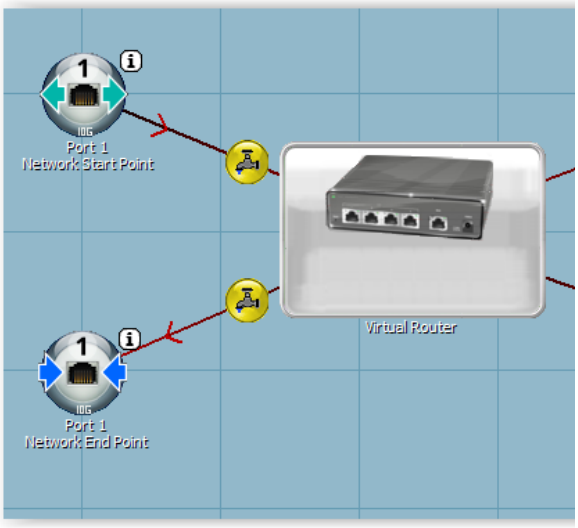
Name:	**Port 1 to Port 8 (depending on model) – incoming traffic only**
Description:	In physical terms these objects represent the incoming source of packets into the WAN emulation. Depending on the model this can present 2, 4 or 8 physical ports.
Network Tool Box Icons:	  These icons represent the incoming traffic into the SNE hardware unit (i.e. the simulated WAN)
Emulation Design Pane Icons:	  These icons (which appear when the above network toolbox objects are dropped onto the Design pane) represent the start points of your data to be emulated.
Available Input(s):	None – these objects represent the start of the network under emulation
Available Output(s)	1 Output – any destination on a connection but for an emulation to work, the connection must terminate at a network end point (see below)

15.2.3. **Bridged Mode: Port 1 -> Port 8 – outgoing traffic only**

Name:	**Port 1 to Port 8 (depending on model) – outgoing traffic only**
Description:	In physical terms these ports represent the network end point for data leaving the SNE hardware unit via ports 1 and 2. Within the GUI, they can be thought of as the end points for data arriving at the 'far end' of the WAN.
Network Tool Box Icons:	
Emulation Design Pane Icons:	 These icons (which appear when the above network toolbox objects are dropped onto the Design pane) represent the end points of your data which has been subject to WAN emulation.
Available Input(s):	1 Input – a connection from any impairment or filter
Available Output(s)	None – this is a network end point.

15.2.4. **Use in Routed Mode**

Routed mode provides virtual routers which are attached to each physical port. In this mode the network start and end points are used to attach a virtual router to a specific port.



Please note that no impairments are allowed between the physical ports and the Virtual Router. You must place all impairments on the WAN link between Virtual Routers. Please see the **Virtual Router** section for further information.

15.2.5. **Routed Mode Rules for Traffic Flow**

Please refer to section 11.4.1 in this user manual to understand how to access overall settings for routed mode operations (including traffic flow rules and forwarding table settings).

15.3. Packet Delay

Impairment Tool Overview:

Name:	Packet Delay
Description:	Introduces fixed and ranged delay to data
Network Tool Box Icon:	
Design Pane Icon:	 Please note that summary information is indicated for this impairment on the Design pane icon – the example above shows a delay setting of 50ms
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	• Linear/Constant delay with Jitter • Range Delay • Normal/Gaussian • Ramp • Sinusoidal

Introduction

The packet delay impairment introduces delays to any packets that enter it.

15.3.1.

Purpose

The 'Packet Delay' impairment will receive data and 'hold' the received packets using the settings defined by the user. This tool replicates latency commonly found on corporate WANs and the Internet.

Mode overview

The Packet Delay tool has a number of different impairment modes:

Constant / Linear

Constant delay is often used on fixed delayed links such as microwave or satellite, and can be useful for simulating the delays experienced by packets as they enter network equipment (routers, switches and other latency-inducing devices). Packets can also be delayed simply because the network interface must undertake other actions first, before it can process and route the packet as required.

Range
Range delay is used to simulate a range of latencies that are experienced by most equipment on the public Internet or over long-hop private circuits.

Normal / Gaussian
This applies a normal or Gaussian distribution to packet delays; if plotted this would resemble the classic bell curve probability distribution which quickly falls off from the mean point.

Ramp
This provides a linear ramp up from a starting latency to a finishing latency. The user can adjust the delays of this tool as well as the speed of ramp-up.

Sinusoidal Wave
A standard sine wave of latency is produced within a given min/max latency and a time period in which to make the sweep.

Mode Reset

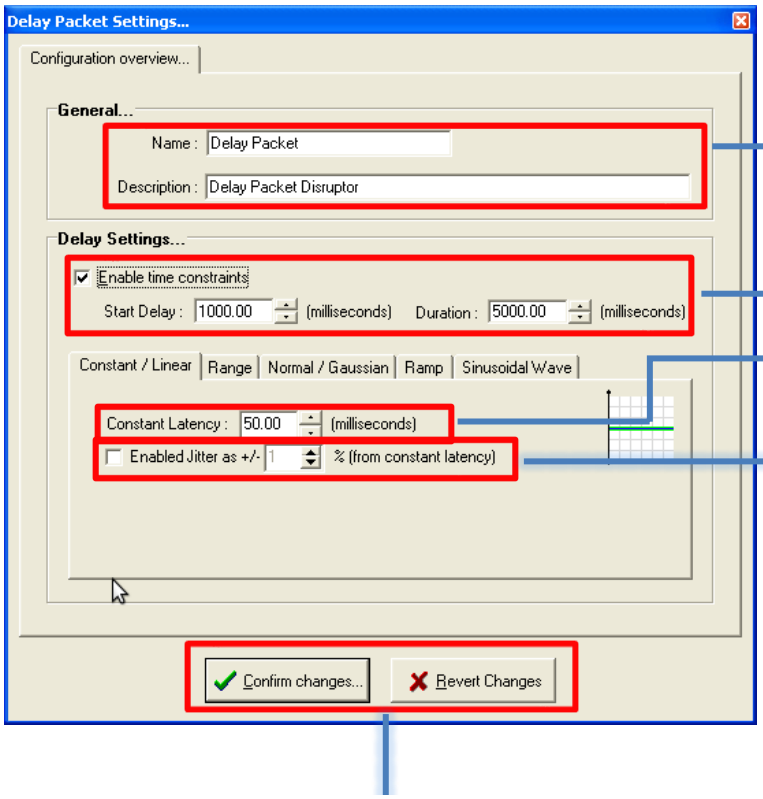
Please Note: If any delay tool is enabled or disabled (either through manual on/off selection, via the time-line or through "time constraints" options) it will reset its operation - i.e. on reset, Ramp mode will reset back to the start latency and will be ramped up in accordance with the user settings.

15.3.2.

Settings

Once the Packet Delay impairment has been added to an emulation map, access its settings by right-clicking on its icon and selecting Settings:

Overview and Constant mode



The default name and description of the Packet Delay tool will be displayed. These can be edited, which will change how the tool appears on screen

The packet delay has "time constraint" control allowing the tool to be enabled after a Start Delay, and disabled after the duration has elapsed.

The 'Constant Latency' field specifies how long each packet will be delayed before being released back onto the connection. This value can range from 0.01 millisecond to 30,000 milliseconds in 0.01ms steps

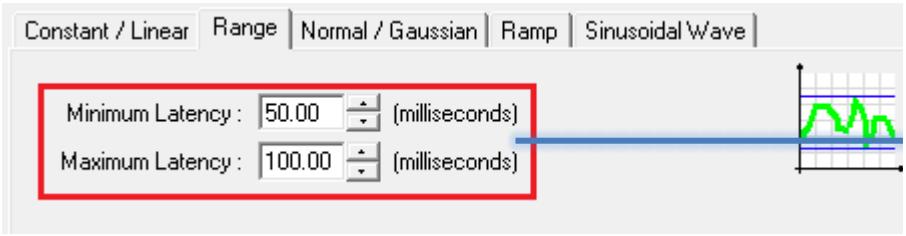
Available within Constant mode is the Jitter option. When enabled, the user can select an amount of jitter to apply as a percentage of variance from the specified Constant latency.

Once any change is made to these settings, they must be confirmed to take effect.

Jitter can be added from within the packet delay impairment. Jitter is a variation in the delay experienced by packets as they traverse a network, with some packets moving unimpeded while others are subject to variations in their delay. Jitter impacts how software handles incoming data and can severely affect time-critical applications (such as those found in the audio and video industry, for example), with packets arriving out of order or dropped from the network.

Range Mode

The Range delay mode allows the user to select a min and max latency to be applied to all received packets. The delay impairment tool will pick a new random delay for each packet that it receives.



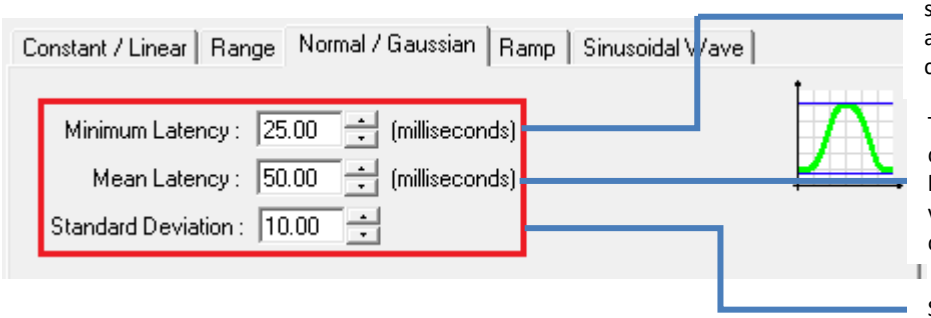
The minimum and maximum latency fields are shown within the Range Mode. These allow the user to specify the smallest and largest delays that data packets traversing the emulated network will experience.

The delay experienced by data packets will vary in a random manner between these two values.

Normal / Gaussian Mode

The Gaussian delay mode allows the user to apply latency using a “bell curve” normal distribution.

The distribution is controlled by the Mean latency and Standard Deviation, with the ability to set a minimum latency that the tool will never drop below.



The minimum latency; if the value selected by the normal distribution algorithm falls below this value it is clamped to this minimum value.

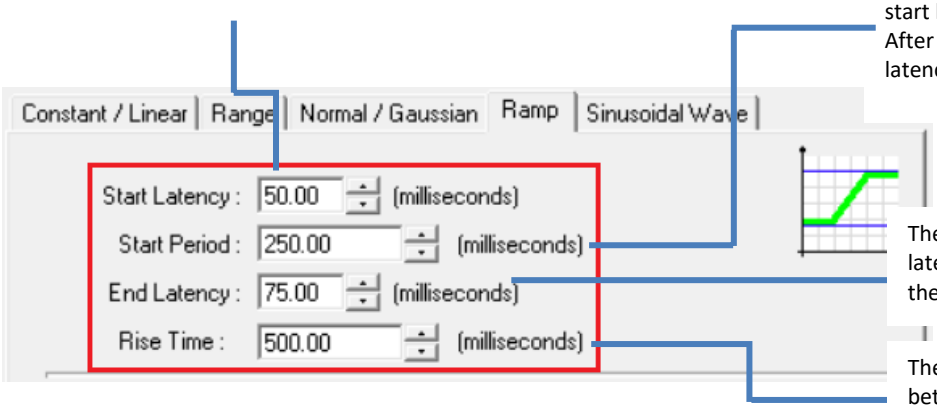
The mean latency to be used by the distribution algorithm. The amount of latency applied will be “around” this value subject to the standard deviation.

Standard Deviation value

Ramp Mode

The ramp delay mode provides the ability to ramp up the latency in a linear manner.

The Start Latency is applied as soon as the delay tool is activated



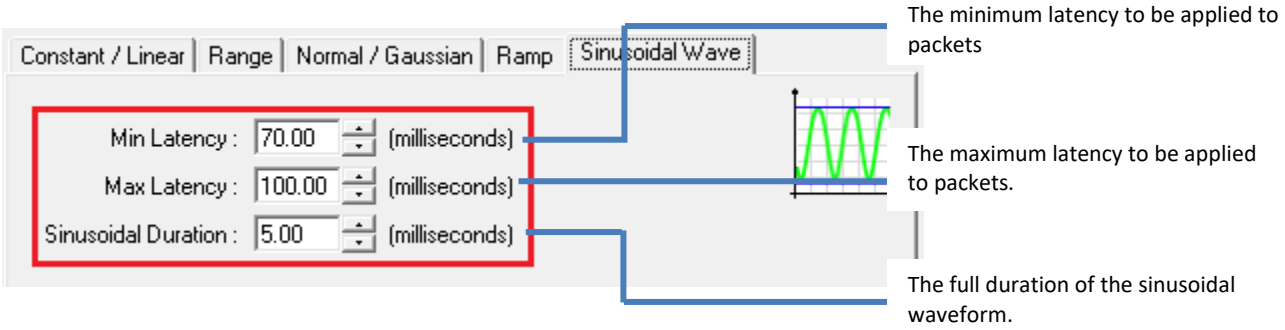
The Start Period defines how long the start latency should be applied for. After this period has elapsed the latency will begin to ramp up.

The final latency required; this is the latency that the tool will reach after the rise time has elapsed

The ‘Rise Time’ defines the time between the ‘start latency’ and the ‘end latency.’

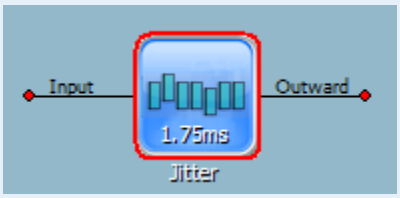
Sinusoidal Mode

The sinusoidal delay mode creates a constantly varying delay between a min and max value using a sinusoidal waveform. The duration of the full sine wave is supplied as the “Sinusoidal Duration”, after which the cycle will repeat.



15.4. Jitter

Impairment Tool overview:

Name:	Jitter
Description:	Imposes jitter on traffic received
Network Tool Box Icon:	
Design Pane Icon:	 Please note the jitter setting is indicated on the Design Pane icon - in range mode this display will be limited to one decimal place (for display purposes only)
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	○ Constant jitter between 0.1ms and 100ms, in increments of 0.01ms

Introduction

The Jitter tool is related to the Packet Delay tool but presents the ability to inject jitter on a link differently.

Purpose

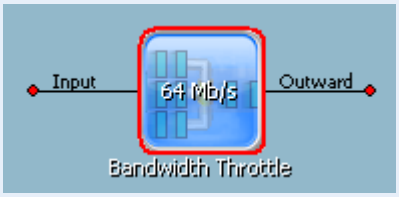
Jitter is a variation in the delay experienced by packets as they traverse a network, with some packets moving at an average delay rate while others are subject to variations in their delay. Jitter impacts how software handles incoming data and can severely affect time critical applications (such as those found in the audio and video industry), with packets arriving out of order or dropped from the network.

Settings

- Maximum Jitter – injects jitter ranging from 0ms to a maximum jitter value defined by the user, adjustable from 0.1ms to 100ms in increments of 0.01ms.

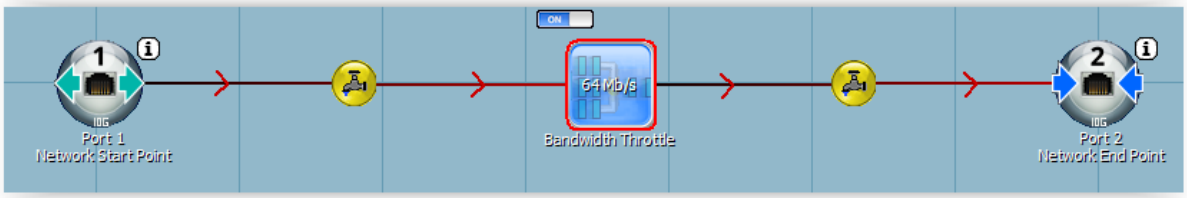
15.5. Bandwidth Throttling

Impairment Tool overview:

Name:	Bandwidth Throttling
Description:	Imposes limits to available bandwidth on a connection between the input and output – the user defined setting will be the maximum average sent on from this impairment.
Network Tool Box Icon:	
Design Pane Icon:	 Please note bandwidth setting is indicated on Design pane icon - the example above showing 64 Mb/s
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	Constant Bandwidth Range Bandwidth

Introduction

The Bandwidth Throttling impairment emulates user defined restrictions on available bandwidth on an emulated connection. The diagram below shows the Bandwidth Throttle tool connected between two physical ports, with a maximum bandwidth of 64 Mb/s.



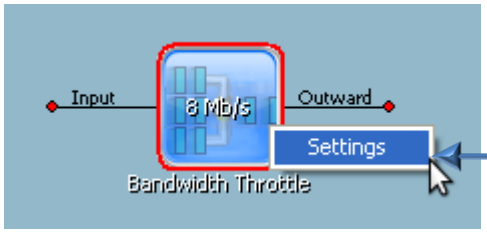
15.5.1.

Purpose

The Bandwidth Throttling impairment tool effectively reduces the bandwidth available, thereby emulating the real-world limitations on data transfer speeds. On a WAN, the data transfer rates can vary greatly over the course of a data packet's lifetime, depending on factors such as network infrastructure and software used.

Settings

Once the Bandwidth Throttling impairment has been added to your emulation, access its settings by right-clicking on its icon and select settings:



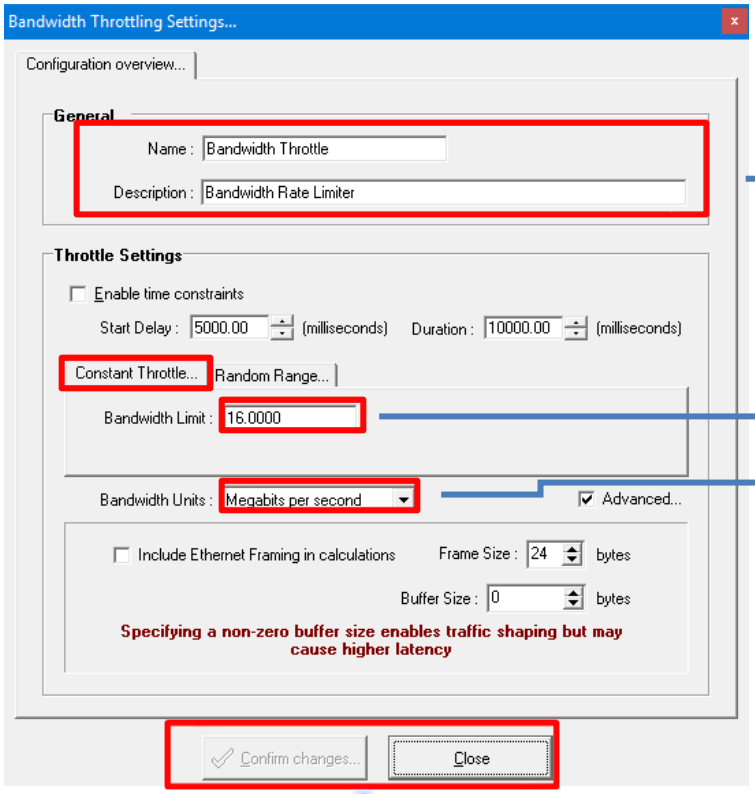
Right-click the Bandwidth Throttle icon to access settings

Bandwidth Throttle Modes

Constant Bandwidth

If the bandwidth throttle is set into constant bandwidth mode it will throttle the bandwidth to a constant / linear value as supplied by the user.

To place the bandwidth throttle in constant throttle please select the “constant throttle” tab sheet as shown below:



As with all other impairment tools the general settings can be changed if required

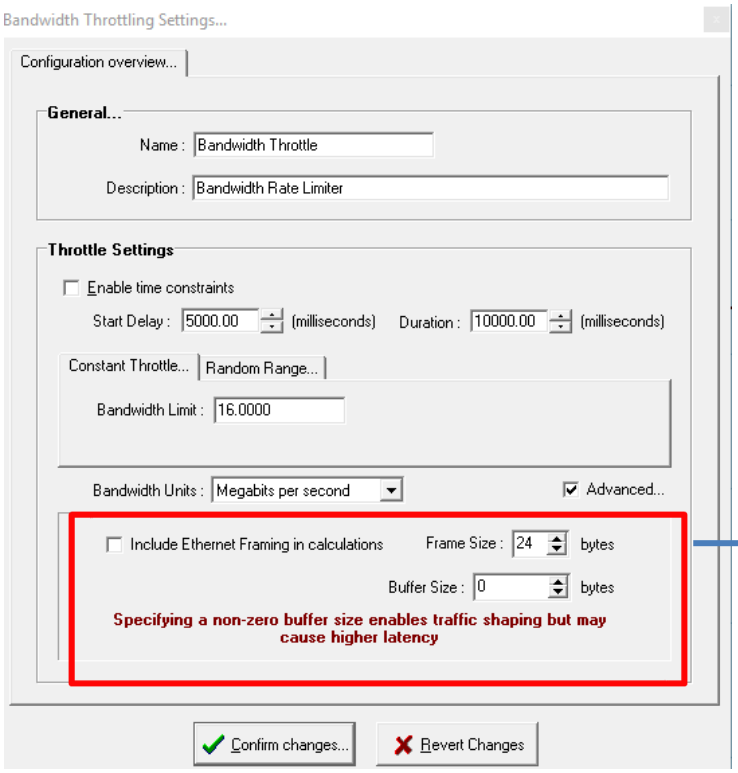
To set a bandwidth limit, enter numeric values into the Bandwidth Limit field and select the data size required from the drop-down list.

The bandwidth units, this can be changed to gain finer control over the bandwidth throttle.

Once any change is made to these settings, they must be confirmed to take effect.

Advanced Mode

When the advanced checkbox is selected, the constant mode settings window will be extended to include further options, as shown in the diagram below:



The advanced options provide finer control over the bandwidth throttle, allowing for simulation of certain bespoke networks and switches / routers.

Include Ethernet Framing in calculations

By default, when packets flow through the Bandwidth throttle on the SNE, the data is throttled by looking at the Layer 2 Ethernet Frame minus the 4 bytes for the FCS. The reason the FCS is left out of the calculation is due to the SNE recalculating the FCS checksum when being transmitted back out onto the network device.

To ensure your bandwidth throttle matches a Layer 2 or Layer 1 calculation, please see the settings below:

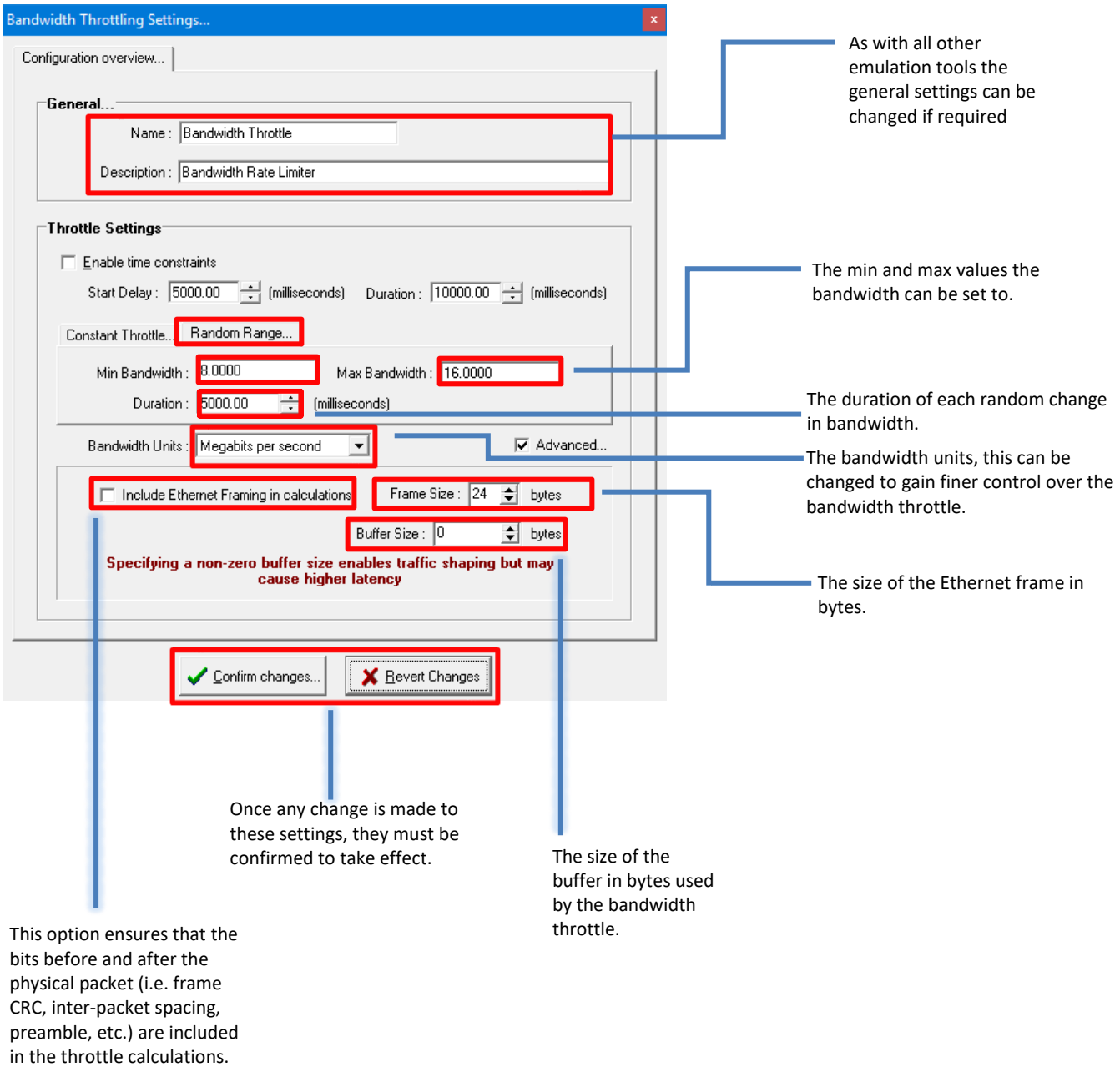
- **Layer 2 Ethernet Frame–** Please enable the "Include Ethernet Framing in calculations" by ticking the checkbox and set the value inside the Frame Size to 4 bytes.
- **Layer 1 Ethernet Frame** – Please enable the "Include Ethernet Framing in calculations" by ticking the checkbox and set the value inside the Frame Size to 24 bytes.

Note:

Layer 2 Ethernet Frame = SNE Calculation + 4 bytes for FCS checksum
Layer 1 Ethernet Frame = SNE Calculation + 4 bytes for FCS checksum + 8 bytes Preamble + 12 bytes Interpacket Gap

Ranged Bandwidth

To place the bandwidth throttle in range mode please select the “range throttle” tab sheet as shown below:

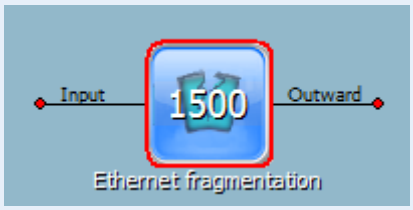


The range throttle will randomly select a new bandwidth throttle value between the user supplied minimum and maximum values. This bandwidth throttle value will be applied until the duration has expired, at which point a new bandwidth throttle will be randomly selected.

This mode has no advanced functionality.

15.6. Ethernet Fragmentation

Impairment Tool overview:

Name:	Ethernet Fragmentation
Description:	Sets the maximum MTU value (in bytes), above which the packet will be fragmented
Network Tool Box Icon:	
Design Pane Icon:	 Please note Ethernet fragmentation setting is indicated on the Design pane icon - the example above shows a MTU setting of 1500 bytes (its default)
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	• MTU value between 128 and 9000 bytes

Introduction

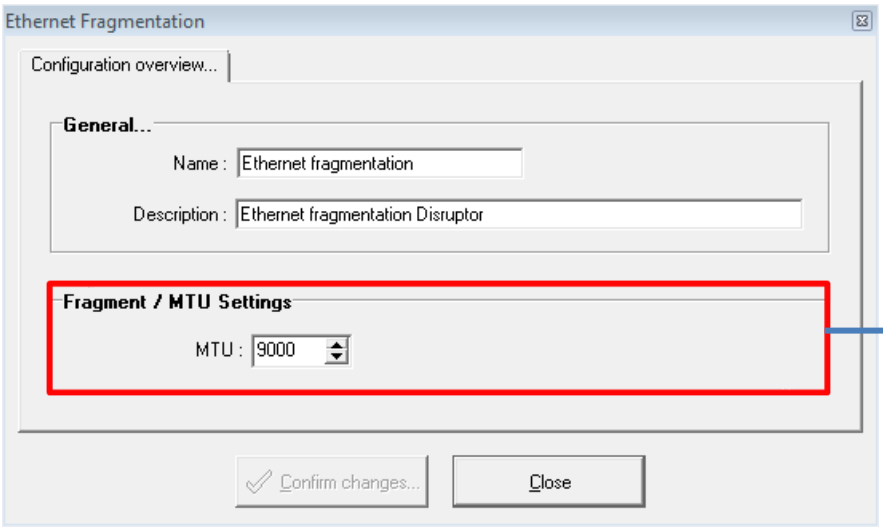
The Ethernet fragmentation tool is used to set the maximum transmission unit parameter across an emulated link.

Purpose

In IPv4, different physical networks vary in the size and structure of their framing methods, represented by the MTU value. As packets traverse different networks and the MTU varies on interfaces, Ethernet packets are fragmented to adapt to the changing MTU values.

Settings

Once the Ethernet fragmentation impairment has been added to your emulation, access its settings by right-clicking on its icon and selecting settings. The following screen will be displayed:



The MTU value is changed by either entering the desired value, or using the up/down arrows to select

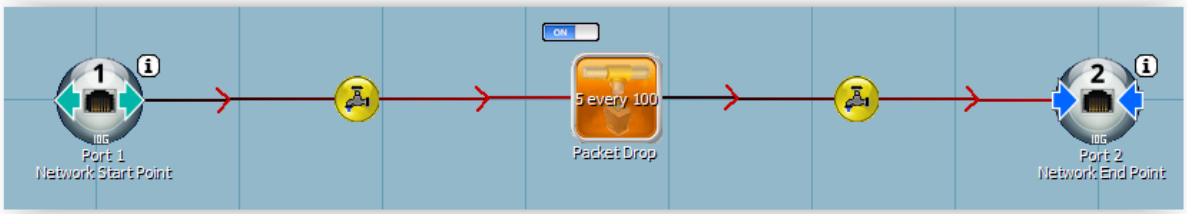
15.7. Drop Packets

Impairment Tool overview:

Name:	**Drop Packets**
Description:	Discards a user determined number of packets received
Network Tool Box Icon:	
Design Pane Icon:	 Please note packet drop setting is indicated on the Design pane icon - the example above showing 5 packets dropped out of every 100 received
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	• Standard (drop a specified number in every user defined total e.g. drop 2 packets for every 10 received) • Drop a percentage of packets received • Drop packets evenly • Drop packets in groups

Introduction

The Drop Packet impairment emulates the loss of packets experienced during communications over a WAN. This tool allows the user to define a set rate of dropped packets, or a percentage of the total number received. The diagram below shows the Drop Packet impairment on the Design pane, with 5 of every 100 packets dropped from the connection.



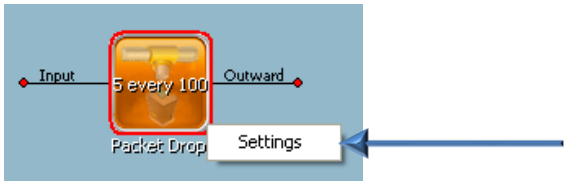
15.7.1.

Purpose

The packet drop impairment simulates the loss of a proportion of the data that is sent over a WAN, a situation which can be caused for a wide variety of reasons. Insufficient buffering, firewalls, collisions on shared connections, damaged hardware, routing instability and so on can act independently or in combination to result in packet loss.

Settings

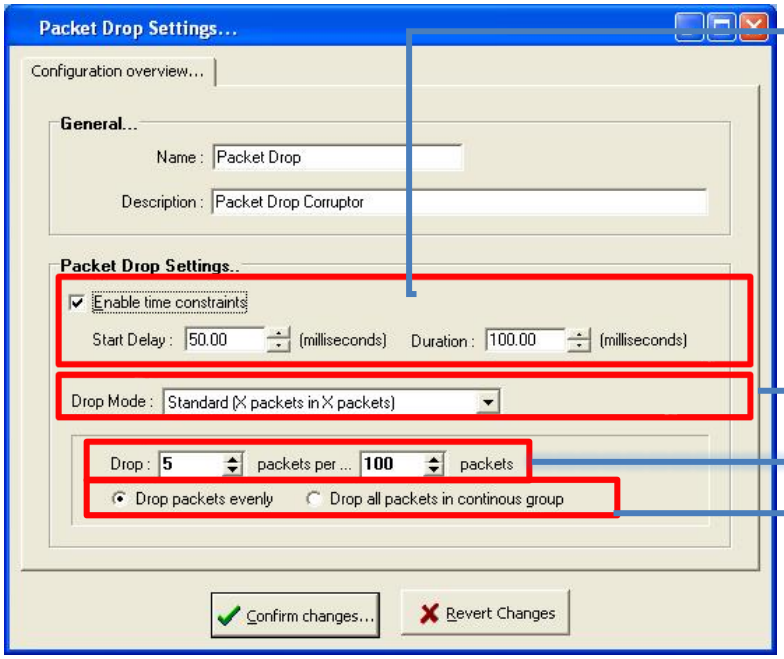
Once the Packet Drop impairment has been added to your emulation, access its settings by right-clicking on its icon and selecting settings:



Right-click the Packet Drop icon to access settings

Standard Packet Drop Mode

The Packet Drop settings window will default to standard mode, as shown below:



If enabled it delays the starting of the tool and controls the duration the tool will be running

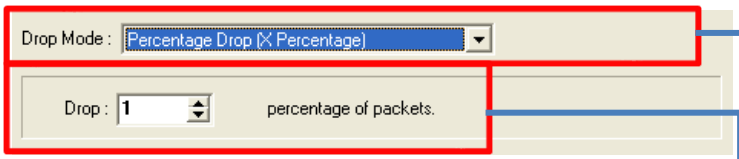
Standard mode drops a specified number of packets received, from a specified total. The dropping of packets will continue until the emulation is paused or stopped.

Enter a numeric value for the number of packets to be dropped, and the total from which that value should be applied. Alternatively, use the up/down scaling arrows to set these values.

"Drop packets evenly" means that the system will space out the dropping of packets. In the above example 5 in 100, would mean 1 packet every 20 packets. If the option for "drop all" was selected 5 packets (in a row) would be dropped every 100 packets.

Percentage Packet Drop Mode

Using the drop-down menu provided for the 'Mode' field, the user can select the Percentage Drop option, as shown below.



Percentage mode drops a specified percentage of all packets received. The dropping of packets will continue until the emulation run is paused or stopped.

The percentage of all packets received which are to be dropped from the emulation is set using this field

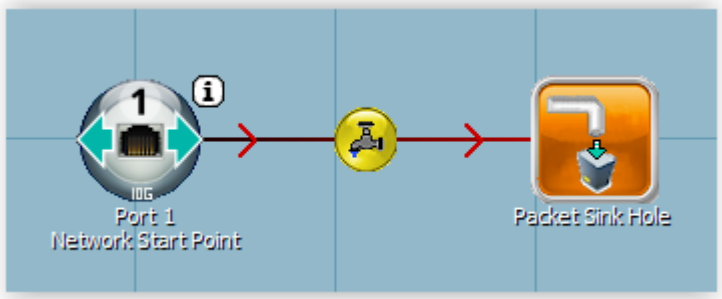
15.8. Packet Sinkhole

Impairment tool overview:

Name:	Packet Sinkhole
Description:	Drops all packets received
Network Tool Box Icon:	
Design Pane Icon:	
Available Input(s):	1 Input – Any source on same connection link
Available Output(s)	None available
Options:	None Available

Introduction

The Packet sinkhole impairment tool emulates the loss of all data on a WAN. There are no associated settings for this tool, as packets are effectively discarded once received. If a less than total drop rate is required, please refer to the Packet Drop impairment, which allows users to specify a level of data loss lower than 100%. The diagram below shows the Packet Sinkhole tool connected to a network start point, with no onward connection as no packets will remain once they enter the sinkhole.



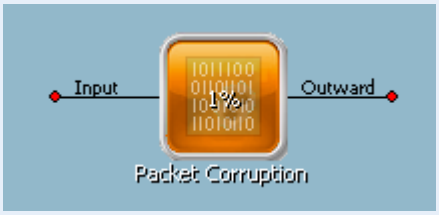
15.8.1.

Purpose

A packet sinkhole is commonly used to drop all packets after a filtering operation, or if packet duplicates are worked on/analysed but not then presented to the network (and thus dropped).

15.9. Packet Corruption

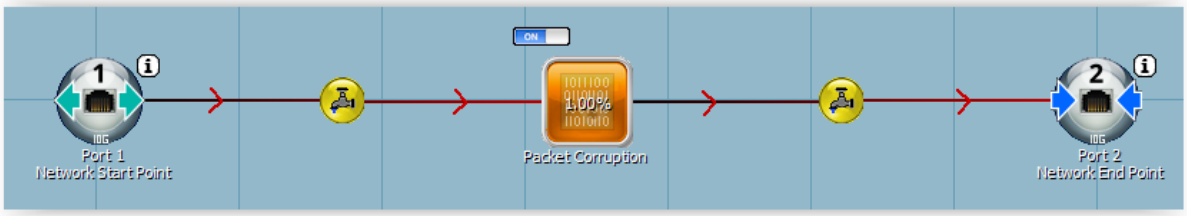
Impairment overview:

Name:	Packet Corruption
Description:	Introduces corruption (such as overwriting or rearranging data) into all packets received
Network Tool Box Icon:	
Design Pane Icon:	 Please note packet corruption setting is indicated on the Design pane icon - the example above showing 1% corruption on all packets received
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	• Bit flips (bits are rearranged) • Byte overwrite (bytes are overwritten) • Corruption on all packets or user defined corruption start and end points • Corruption scale (percentage)

15.9.1.

Introduction

The Packet Corruption impairment simulates the internal distortion that can occur to data held within packets on a WAN. This tool corrupts all packets received, through user defined settings. The diagram below shows the packet corruption tool connected between two routed connections, with 46% of each packet's contents being corrupted.



15.9.2.

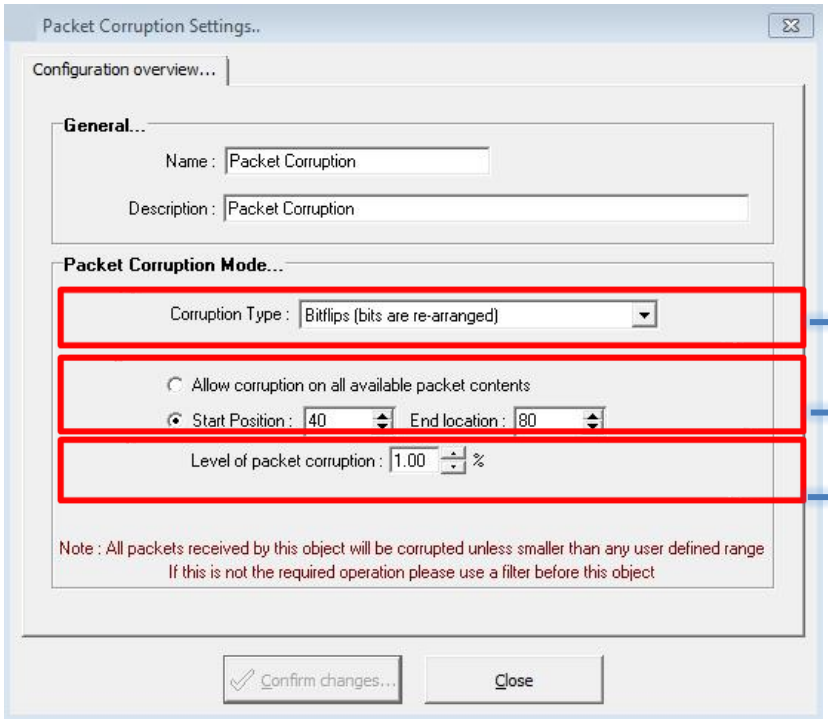
Please note: All received packets are corrupted; therefore the 'packet counting' filter is usually required to allow a certain amount of packets to be corrupted. See below for more information.

Purpose

Data corruption on a WAN, can be the result of hardware errors, satellite or microwave link problems or faulty equipment. Normally any network port would automatically drop corrupt packets (as the checksum would fail), however the SNE correctly produces the corrupt packet on the wire allowing any down-stream devices to receive it.

Settings

Once the Packet Corruption impairment has been added to your emulation map, access its settings by right-clicking on its icon and selecting Settings. The following window will be displayed:



There are two corruption modes available: Bitflips and Byte Overwrites, selectable using the drop-down menu list.

The user can select whether all contents of each packet received may be subject to corruption, or whether this should be limited to a start and end point within each packet (measured in bytes). The upper limit for the end location is 1500 bytes, as this is the byte size limit of standard data packets.

The corruption scale sets the level of corruption within each packet: if set at 20%, for example, 20% of the packets contents will be manipulated to emulate corruption

Bit Flips

This option will flip the bits within the packet, the amount and location are dependent on the other settings selected - this could be on all bits within each packet or only on bits between the user-defined start and end point (measured in bytes within each packet received). If the user, for example, selected a start point of 50 and an end point of 60, then the 10 bytes between these two values will be subject to a rearranging of their data (in every packet received).

Byte Overwrites

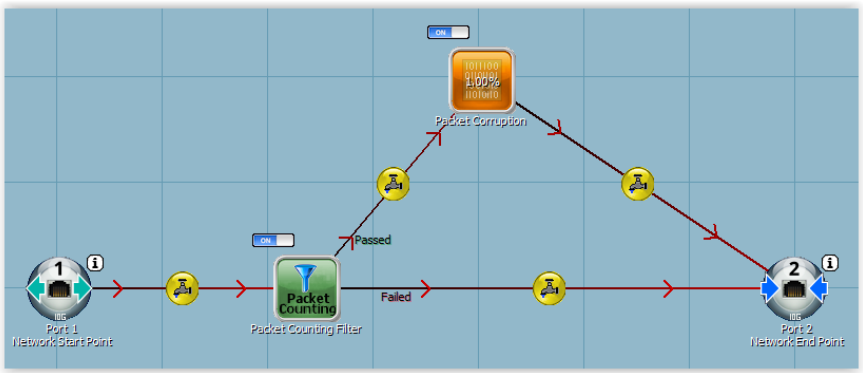
Using this option will replace existing bytes within each packet with randomly generated data, thereby overwriting the byte's information. Again, depending on the other settings selected, replacement could occur on all bytes within each packet, a certain percentage of bytes, or a certain percentage between start and end points.

Corrupting Less Than 100% of packets

The packet corruption impairment subjects all packets to corruption – if the user requires less than 100% of packets on a connection to be corrupted, a 'Packet Counting Filter' should be inserted onto the Design pane before the Packet Corruption impairment, as follows:

3 The packet corruptor will distort these 10% and then release them back onto the connection

2 10% of the packets received from port 1 will travel along the 'passed' connection to the packet corruption tool

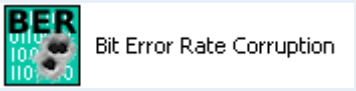


1 The Packet Counting Filter can be set to 'pass' 10% of packets, and 'fail' the remaining 90% of packets received

4 The device denoted as port 2 will receive the 90% of uncorrupted packets and the 10% corrupted packets sent from the device attached to port 1

15.10. Bit Error Rate (BER) Corruption

Impairment overview:

Name:	Bit Error Rate Corruption
Description:	Subjects packets received to duplication
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	Up-to 8 bits corrupted in 100,000,000,000,000 bits seen

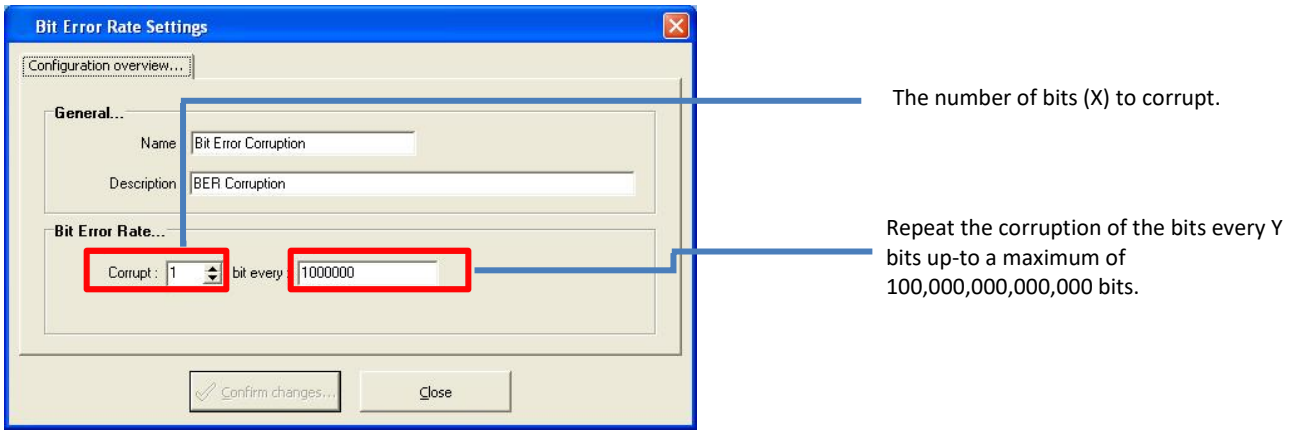
Introduction

This bit error rate corruptor simulates the bit errors likely on links such as satellite and microwave links. It can also be used to simulate problems with faulty cabling or clock drift on E1 to IP bridges, etc.

To simulate multiple bit corruptions simply connect multiple BER impairments together.

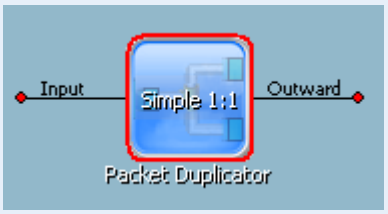
Settings

The BER Corruptor has one mode of operation and provides the ability to specify the X bits to corruption per Y bits.



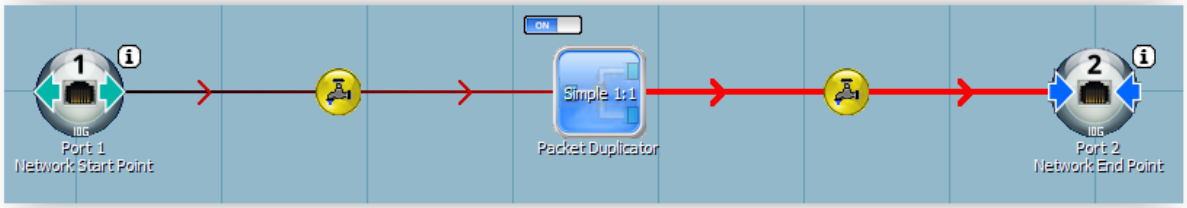
15.11. Packet Duplication

Impairment overview:

Name:	Packet Duplication
Description:	Subjects packets received to duplication
Network Tool Box Icon	
Design Pane Icon :	 Please note packet duplication setting is indicated on the Design pane icon - the example above shows a simple 1-to-1 duplication of all packets received
Available Input(s) :	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options :	• Simple (all packets received are immediately duplicated once) • Timed (packets are duplicated once every user defined number of milliseconds) • Complex (packets are duplicated a specified number of times, at intervals set by the user)

Introduction

The Packet Duplication impairment emulates the copying of packets experienced during communications over a WAN. This tool allows the user to define a wide variety of duplication scenarios, from single, immediate duplication through to multiple packet duplication at specified millisecond intervals. The diagram below shows the Packet Duplication impairment connected between ports 1 and 2, with a setting of 'simple 1:1' duplication:



Purpose

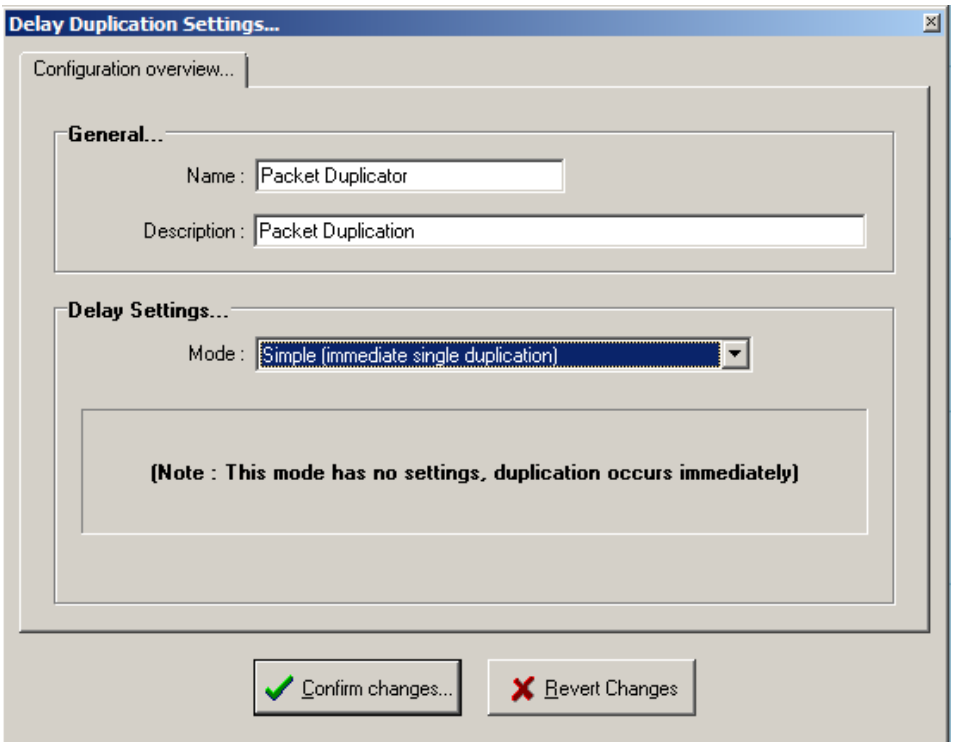
The packet duplication impairment is designed to simulate the effects of router, switch or network infrastructure issues. Under normal conditions duplicate packets are relatively rare, but when they occur their effects can be highly detrimental. This impairment is normally used to duplicate UDP or other non-guaranteed TCP/IP protocols. Certain protocols (such as TCP) automatically handle the duplication and mitigate most related application issues.

Settings

Once the Duplication impairment has been added to your emulation, access its settings by right-clicking on its icon and selecting Settings:

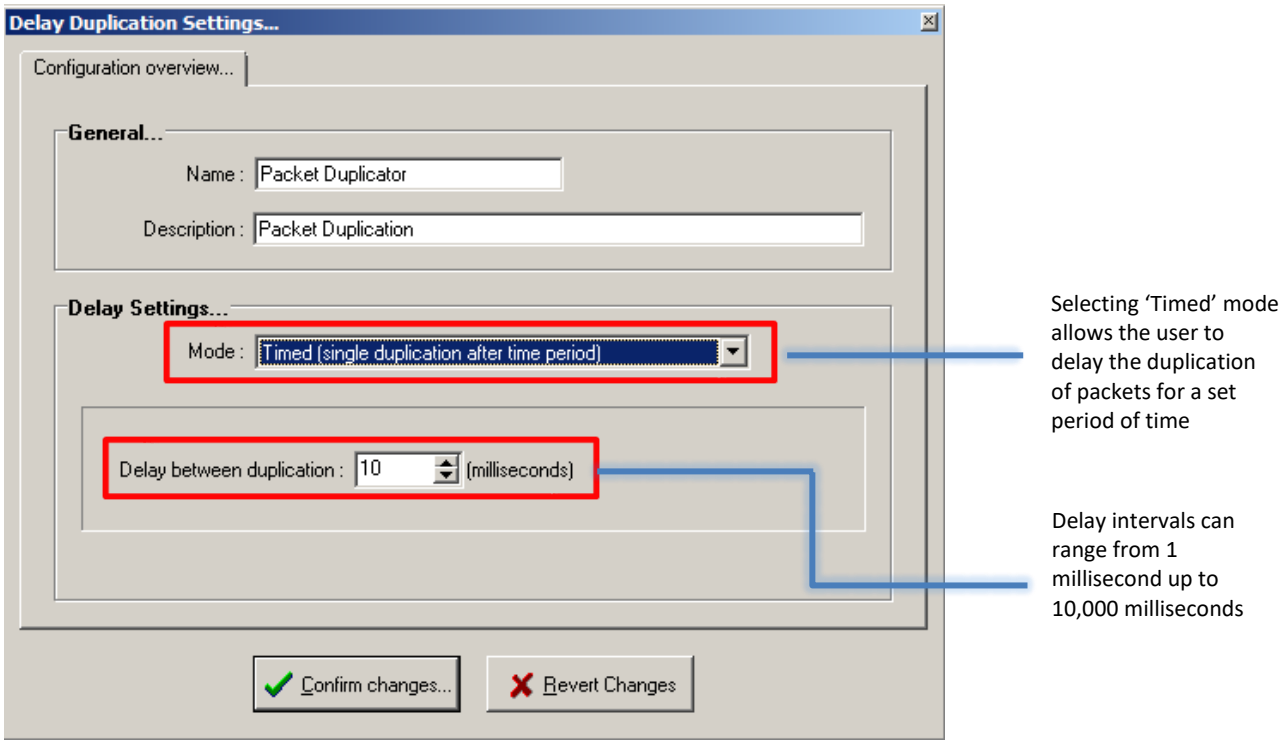
Simple duplication

On first use, this impairment's settings are opened by default in Simple Mode, as shown in the diagram below. This configuration performs a simple 1 to 1 duplication of all data packets received, so that the original data, plus an exact copy, are sent on from this impairment. There are no further settings for this mode.



Timed Duplication

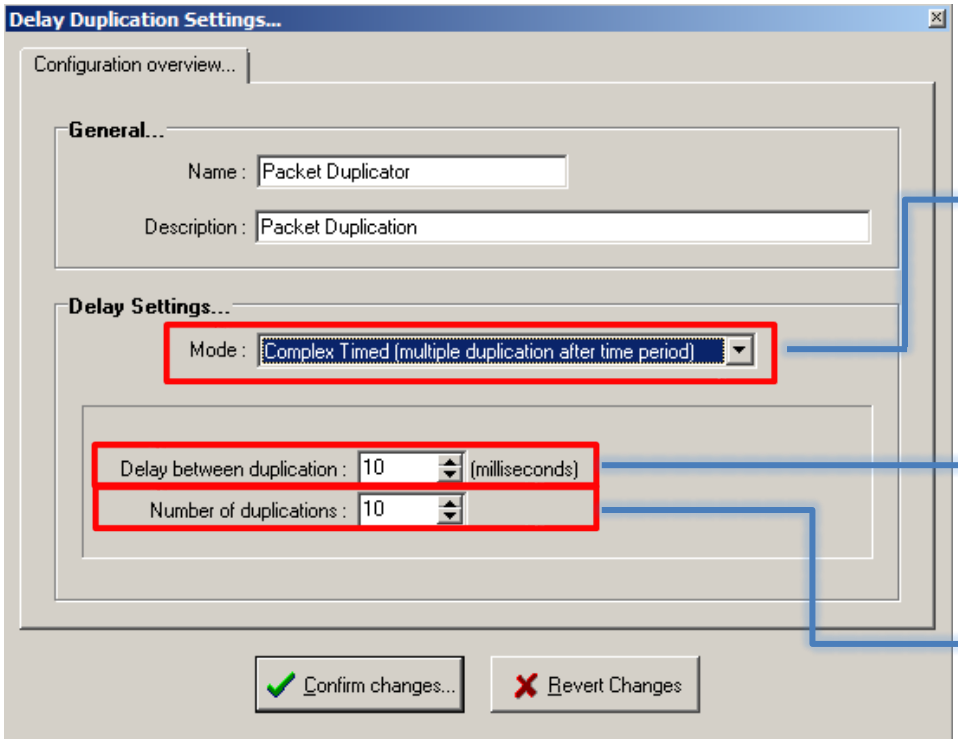
By changing the Delay mode to 'Timed (simple duplication after time period)' the user can delay the duplication of packets received by a specified time period. Please see the diagram below:



Timed mode performs a 1:1 copy of all packets received but does not release this onto the connection immediately; instead the system waits for the time entered to pass before sending on the duplicate packet.

Complex Timed Duplication

The final setting available for the Packet Duplication impairment is 'Complex Timed' – please see the diagram below:



Complex Duplication & Time Considerations

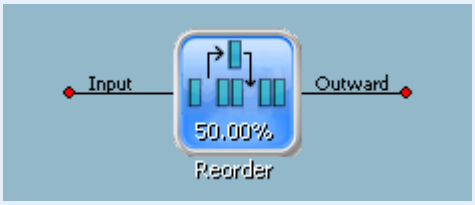
Please note that in Complex Timed duplication mode **each** duplication will be held and released sequentially. In the example screenshot above there will be a total of 10 duplications of every packet received, and each of these will be held for 10 milliseconds, before being released back onto the connection only after the previous copy was released. The total time for one packet's duplication to be completed and sent on (in the example above) is therefore 1 (packet) x 10 (duplications) x 10 milliseconds (each duplicated packet delay). It would therefore take 100 milliseconds before the full duplication process was completed for this one packet.

Users should therefore be aware that duplication may still be ongoing after the last packet of an emulation run has been sent from the source device. This is an important consideration when deciding when an emulation run is complete and can be stopped.

Similar to other impairments, if the user does not wish all packets to be duplicated, a 'Packet Count Filter' should be placed on the connection before the 'Packet Duplication' impairment, thus allowing the user to define how many (or what percentage) of packets received should be subject to any form of duplication.

15.12. Packet Reordering

This dedicated tool reorders packets based on a probability.

Name:	Packet Reordering
Description:	Reorders packets by extracting them from the flow and reinserting at a later point.
Network Tool Box Icon	
Design Pane Icon :	
Available Input(s) :	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	• Probability of reorder • Min/Max milliseconds distance • Min/Max packet distance

Introduction

The reordering tool uses a probability (for each packet) to determine if the packet should be placed a certain distance into the future. The user can either select the probability and the min/max distance the packet should be moved in milliseconds OR packet distance.

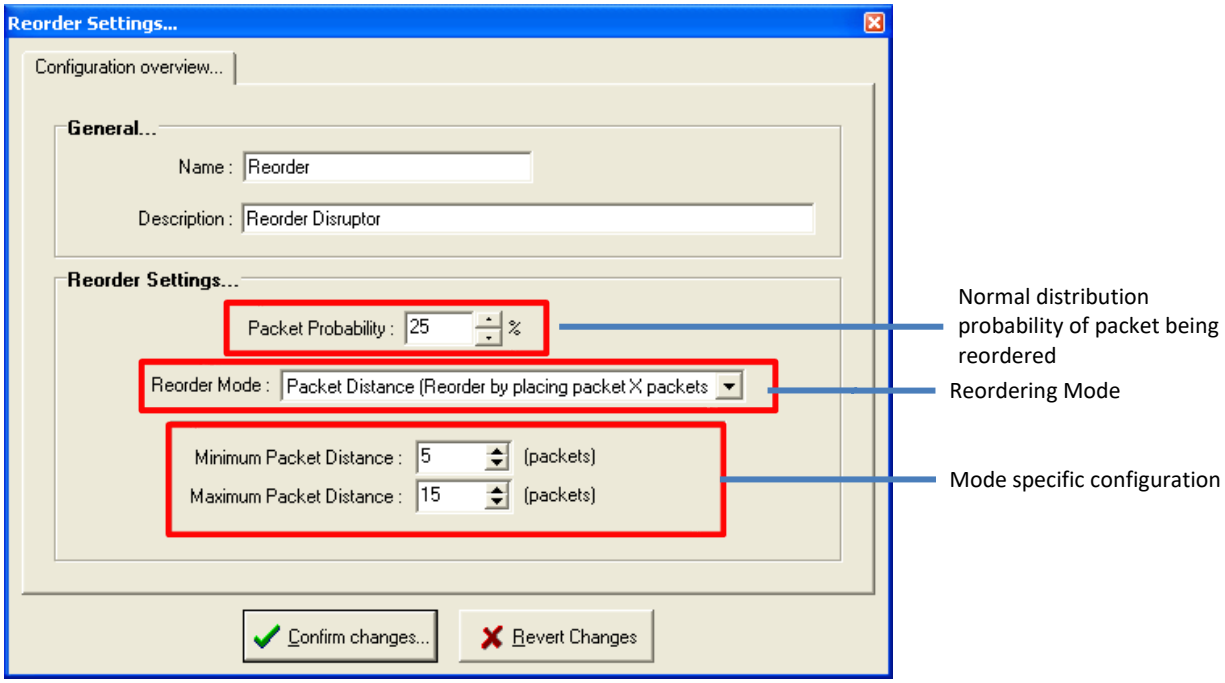
Purpose

The main purpose of this tool is to reorder a stream of packets to simulate environments where such reordering can occur, this is usually limited to switch failures or certain Internet environments. This tool can also be used to test the ability of devices under test (DUT) to cope when faced with reordering of packets (particularly IPTV, Video and Audio codecs, etc.)

Please note: you can use the Delay tool to reorder packets if required.

Settings

The reorder tool supports two reordering modes – “Packet Distance” and “Time”. The following screenshot shows the re-order tool’s settings:



General Settings

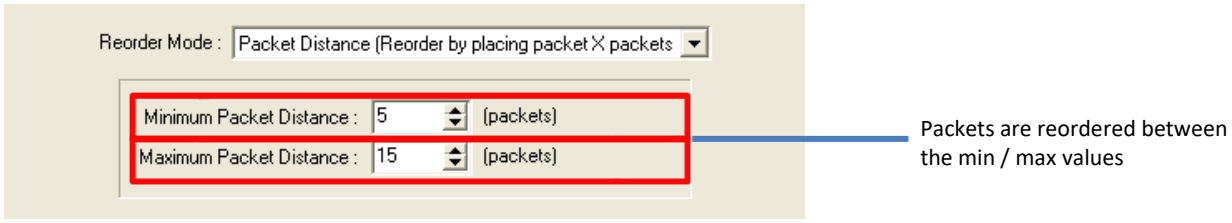
The reorder tool has two general settings; packet probability and reorder mode.

The packet probability is a percentage value used to decide if a received packet should experience a reordering event; in this case the user has selected the value of 25% - meaning that using Normal Distribution probability 25% of all packets received will be reordered.

The reorder mode is used to select whether you wish to reorder the packets using a packet distance or time specified in milliseconds.

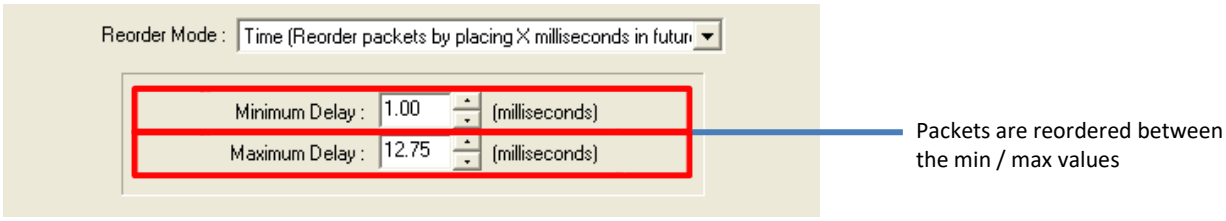
Reordering Mode - Packet Distance

In “Packet Distance” mode, any received packet will be held (and effectively re-ordered) until a set number of packets are received. The number of packets is defined as a normal distribution value between the minimum and maximum distance. If you require a constant offset please set the min and max values to be the same.



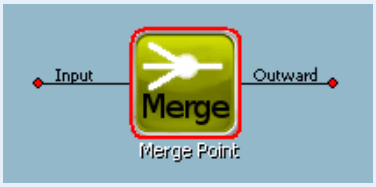
Reordering Mode - Time

In “Time” mode, any received packet will be held (and effectively re-ordered) until a time has been exceeded. The length of time the packets are held for is defined as a normal distribution value between the minimum and maximum millisecond values. If you require a constant offset please set the min and max values to be the same.



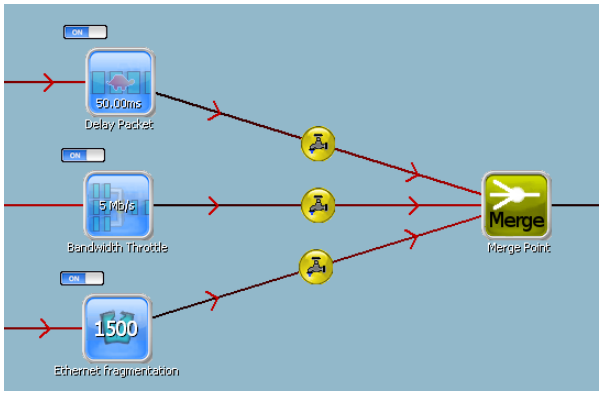
15.13. Merge Point

A merge point is used to merge together different input streams into a single output stream. There are some important rules governing the use of TAP devices after a merge point, please see below for details.

Name:	Merge Point
Description:	This tool merges together all input packets into a single output stream.
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	Unlimited Inputs
Available Output(s)	1 Output
Options:	None required

Usage

Below is sample usage of the merge tool



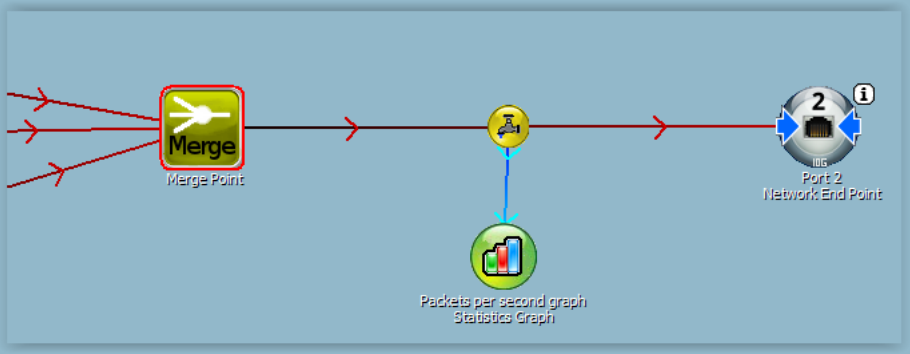
This sample usage shows the merging of 3 input streams into a single output stream using the merge tool.

The merge tool guarantees the order of packets. If a packet was received from the top path first it will be guaranteed to be delivered to the output stream first, this ensures no desequencing or reordering of your packets.

TAP Device Considerations

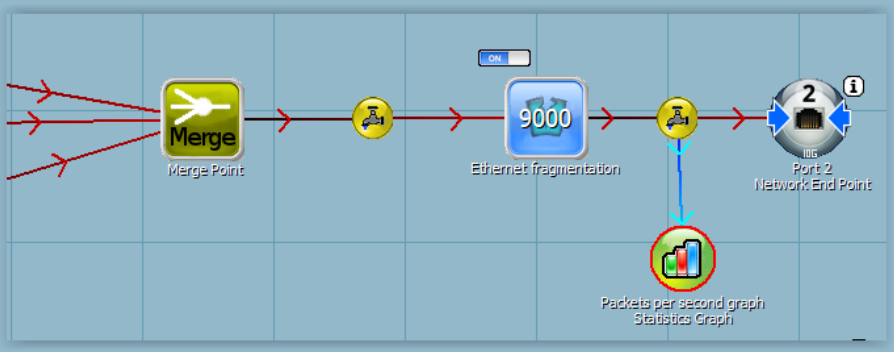
The output of the merge tool does not support any TAP device, whilst the TAP symbol is shown you ***should not*** attach any TAP device to this TAP point – you will receive inaccurate results.

The following example shows an ***invalid*** Statistical Graph:



If you require to add a add a TAP device it is recommended you add a dummy impairment (i.e. a Bandwidth Throttle set higher than you're required bandwidth or a fragmentation tool set to 9000)

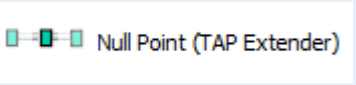
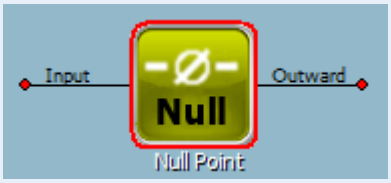
The following example shows a ***valid*** Statistical Graph, using an Ethernet Fragmentation dummy tool:



In future revisions this limitation will be lifted or show a disabled TAP device on the GUI.

15.14. Null Point (TAP Extender)

The null point is used to extend the visual aspects of the GUI and has no effects on the data traversing the emulated map. It assists visualisation and creates more TAP points for reporting purposes.

Name:	**Null Point (TAP Extender)**
Description:	Provides an extra TAP which can be used to insert further TAP devices (such as more statistics graphs, reports or Wireshark instances)
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	None required

15.15. MPEG/H.264 Corruptor

Impairment overview:

Name:	MPEG/H.264 Corruptor
Description:	Corrupts RTP based H.264 video frames
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	• IDR Frame drop and corruption settings • Non-IDR I, P and B Frame drop and corruption settings • Ability to report errors (by flashing red) • Automatically fix CRC after corruption

Introduction

The MPEG/H.264 corruptor provides the ability to both corrupt and drop H.264 frames from an incoming video stream. The impairment provides an extensive set of options to test the streaming of IPTV technologies.

Please note the following considerations:

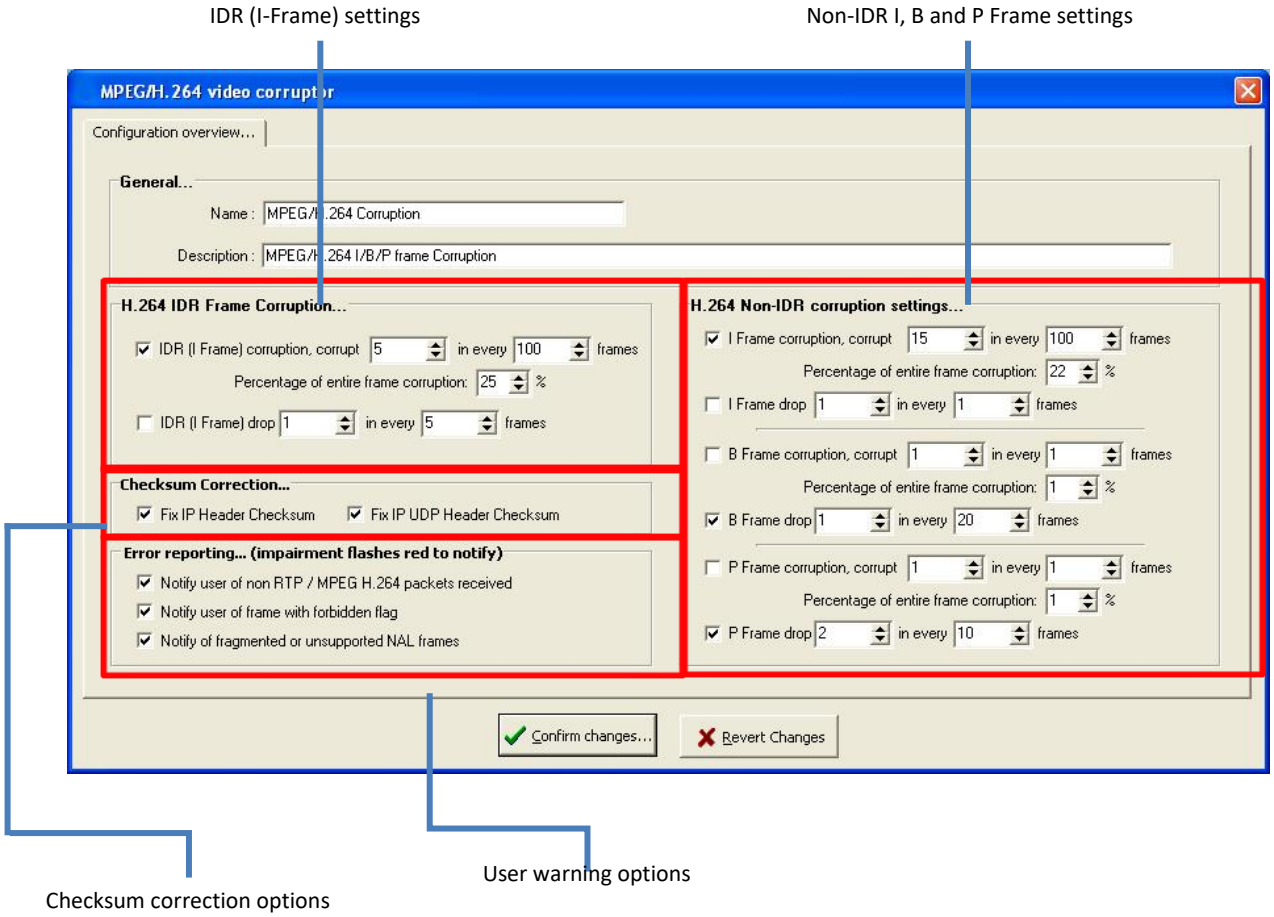
- The impairment tool will only corrupt H.264 frames contained within a RTP payload of type 104, contact should you use dynamic payload types.
- Fragmented NAL units are not supported (in practice most implementations do not use this method)

Advanced IDR / Non-IDR Operation

SNE allow full control over the corruption and dropping of both IDR and Non-IDR I Frames. For those technically minded an IDR frame is a special type of I-frame in H.264. An IDR frame specifies that no frame after the IDR frame can reference any frame before it.

Settings

The MPEG/H.264 corruptor offers the ability to drop X frames in Y frames and corrupt a certain number of frames by a percentage. It can also fix up the checksums of corrupted packets so they pass correctly through the TCP/IP stack on destination devices.
The settings are broken down into 4 different sections:



IDR Frame Corruption Settings

This section allows you to identify and corrupt/drop only H.264 IDR Frames, these frames are often used for faster seeking and glitch free playback by acting as “reference” frames. SNE allows you to clearly identify these types of frames and apply corruption, allowing you to test the durability of H.264 decoders.

In this settings panel you can enable or disable corrupt and drop separately by selecting the checkbox beside either option, in the above screenshot only the “IDR (I Frame) corruption” is enabled. Whether you are corrupting or dropping frames you can specific the amount of frames to process using X in Y method (in this example X = 5, and Y = 100 or “Corrupt 5 continuous frames in every 100 frames”). For corruption you can enter the amount to corrupt each frame, please note that this is the corruption over the entire frame length (as frames can occupy more than one physical Ethernet packet).

Non-IDR Frame Corruption Settings

This section is almost identical to the IDR Frame corruption settings, except it gives you the ability to individually impair the I, B and P frames of Non-IDR frames – as Non-IDR frames make up the bulk of H.264 frames these settings should be used to impair most H.264 streams.

Checksum Correction

When a frame is corrupted the checksums that accompany the frame are invalidated, these options allow you to correct the checksums so the corrupted frame information is passed to the H.264 device and not dropped by the TCP/IP (due to the checksum failure)

Error Reporting

The nature of H.264 (and IPTV) is such that a lot of information is present in packets, allowing the SNE to alert the user when certain conditions are detected. If selected the following options will flash the impairment red when such a condition is detected:

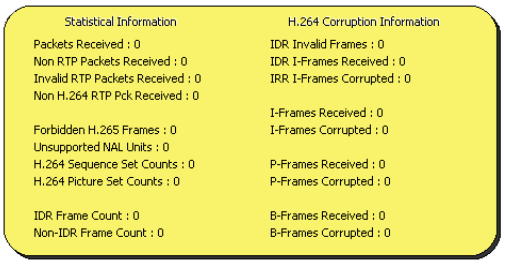
Non RTP / M-PEG H.264 – This option will indicate that the impairment had received packets that are not RTP, or do not contain H.264 frames.

Forbidden Flag – This option will alert the user that frames with the forbidden flag has been detected; these frames are not decoded by H.264 devices and are usually dropped.

Fragmented / Unsupported NALs – Certain uncommon NAL units are not supported, these include NAL units which are not video or audio related.

Real-Time Statistics

The MPEG/H.264 impairment tool allows you to view a large amount of information on the actual H.264 stream:



This information is the same as that presented in the “H.264 TAP device”, for more information on each statistic available please see the “H.264 TAP device”.

16. Load Generation

The SNE provides both simple and complex load generation, with the ability to analyse the load generated traffic against various measurements.

16.1. Background Traffic Generation

Tool overview:

Name:	**Background Traffic Generator**
Description:	Generates traffic on the link where inserted
Network Tool Box Icon:	
Design Pane Icon:	 Please note the traffic generator setting is indicated on the Design pane icon - the example above showing 64Mb/s being generated (the default)
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	1 Output – Any destination on same connection
Options:	• Fixed traffic generation rate • Percentage of available bandwidth • Generate broadcast packets

Introduction

The Background traffic generator produces packets at the point in which it is attached on the network map. The packets will leave the SNE unit through a physical port if the user has assigned the flow of the traffic generator to any physical port. It can generate a fixed amount of traffic or a percentage of the available bandwidth detected on that link.

In order to test or place load on receiving equipment under test, the generated packets can be set to a broadcast destination MAC Address. By using the broadcast address all receiving equipment will process the packets, rather than dropping them.

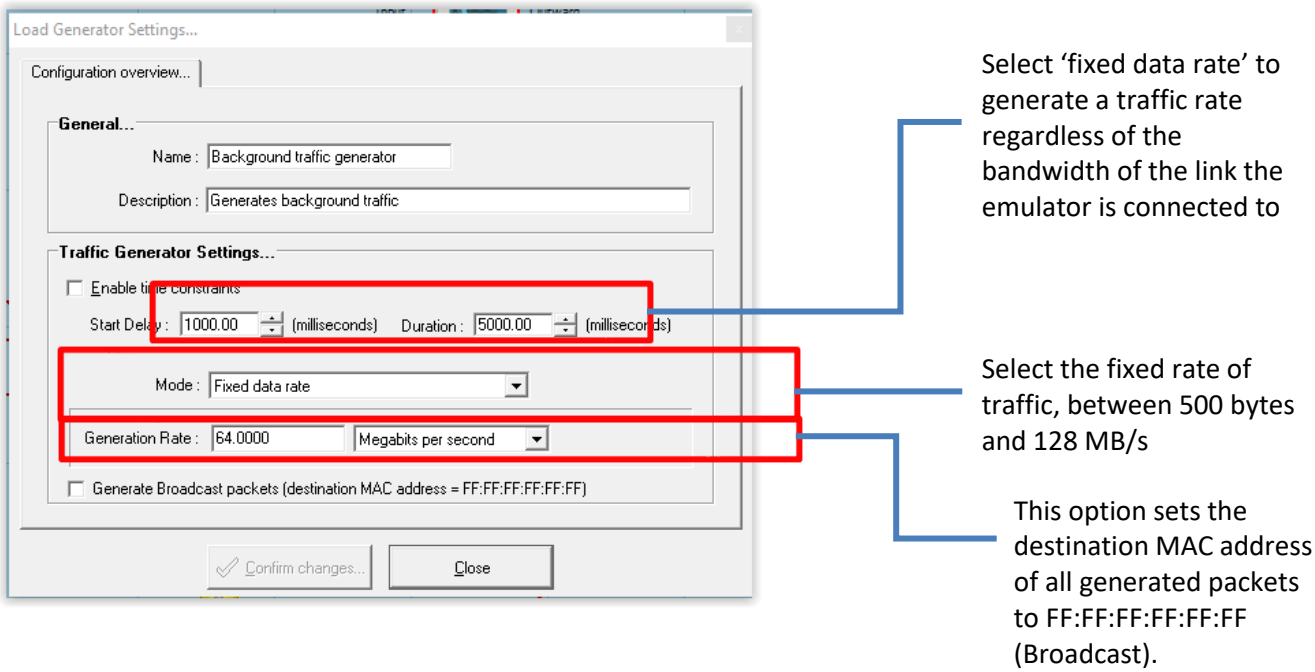
Purpose

This tool emulates other users/applications sending traffic across a network and is an important consideration for emulation. Unless fully dedicated, links should be expected to contain a certain amount of background traffic, which is delivered via this tool to an emulation.

Settings

Once the background traffic generator impairment has been added to your emulation, access its settings by right-clicking on its icon and selecting settings.

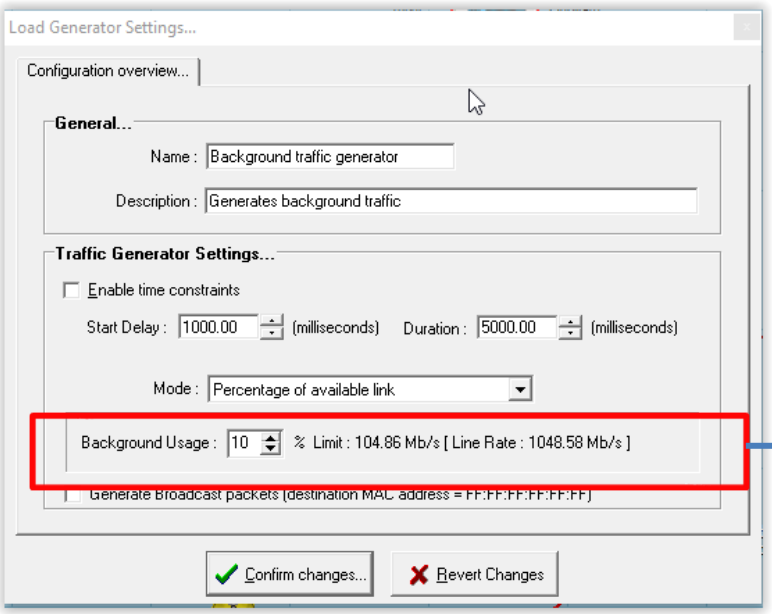
The following screen will be displayed by default:



By selecting 'percentage of available link' for the mode setting, the following screen will be displayed. This allows the user to select how much traffic will be generated based on a percentage of the link speed.

Please note that the bandwidth is calculated as follows:

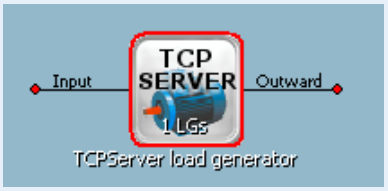
1. If a bandwidth throttle tool is inserted before the background traffic generator, the total bandwidth will be set to the bandwidth throttle value
2. If no bandwidth throttle is detected prior to the background traffic generator, the default setting will be 1 Gbps.



Select the percentage of the available link's transfer rate (from 1 to 99%). The data generation rate will be displayed to the right

16.2. TCP Server Load Generator

This tool generates simulated TCP traffic.

Name:	TCP Server Load Generator
Description:	Generates simulated TCP traffic
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	1 Output – Any destination
Options:	• Load Generators (Src IP, Dst IP, Ports and Data-Rate)

Purpose

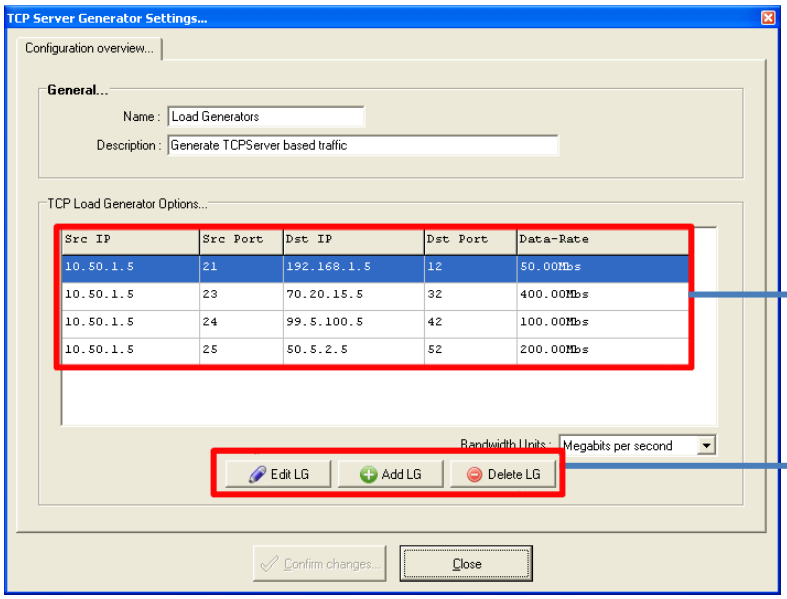
The TCP Server load generator creates traffic designed to simulate TCP server activities. It creates a continuous loop of TCP packets to simulate extremely high bandwidth server activities. These packets correctly emulate the three-way hand-shake as created by any real TCP connections.

Settings - Screenshot

The load generator has settings that provide up-to 5 load generators per instance. This means that each load generator can create 5 unique streams (each with unique addressing information).

General Settings

The load generator provides an overview of the current streams being generated. The following example shows 4 streams being generated from a source IP address of 10.50.1.5 to 4 separate destination IP addresses (with unique TCP ports and data-rates).

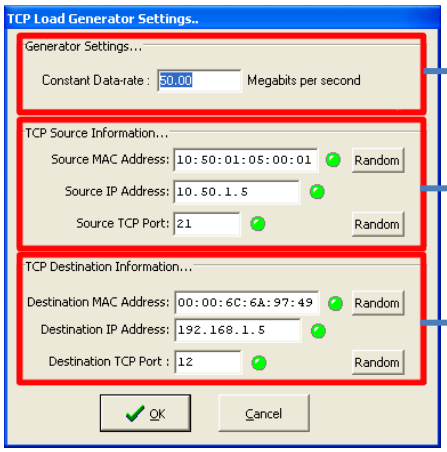


List of current load generation streams.

Add, Delete and modify load generators

Adding or modifying a load generation stream

By clicking the “Edit LG” or “Add LG” you are shown a number of options to control the load generation stream. The following screenshot gives an overview of the operation:



The data-rate of this stream in Mb/s

Source information (i.e. where the packets will appear to be “from”)

Destination information (i.e. where the packets will be transmitted to)

Analysing Generated Traffic Streams

You may wish to learn more about how your load generators are being affected by impairments or other network traffic. The Network Emulator provides a TAP device called a “Load Generation Analyser.”

Please see the **TAP device section** for more information.

Virtual Router Warning

The load generators create packets that will not have their TTL reduced whilst the packets exist inside the emulation map - if the packets are transmitted on the wire they will have their TTL reduced at each hop on the external network.

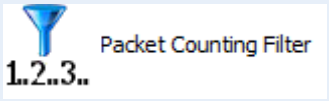
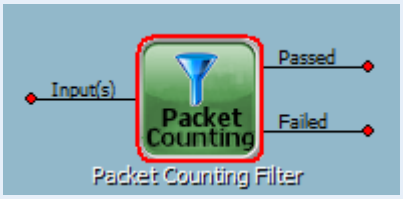
You should therefore be careful not to create circular loops with load generated packets as the emulator will enter a closed loop of forwarding on packets, whilst generating more packets. At some point this will consume the finite hardware resources and cause packets to be dropped (i.e. an overload condition).

17. Filter Tools Overview

Network filters allow the user to specify what data, or how much data, should traverse an emulation map. These are powerful tools that provide a significant degree of control to the user as they design the WAN to be emulated.

17.1. Packet Counting Filter

The packet count filter provides the user with control over how much data should be sent to other impairments on an emulation map and is one of the most commonly used filters within the SNE. The user decides how much data should be 'failed' (either as a percentage or 'X in every Y packets' format) with the 'failed' data taking a different route than the 'passed' data.

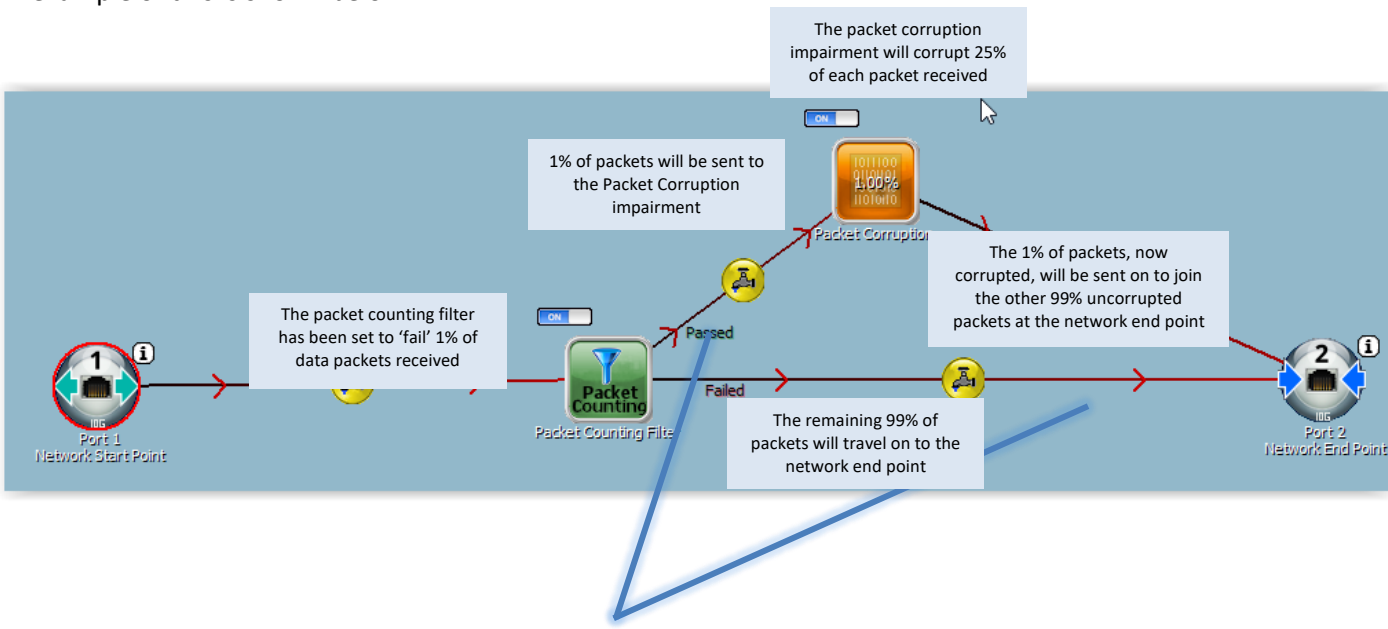
Name:	**Packet Counting Filter**
Description:	Separates packets received into 2 new streams of data, one that has 'passed' and one that has 'failed' depending on the number of packets received.
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source on same connection
Available Output(s)	2 Outputs – packets received will be routed down a 'passed' or a 'failed' connection
Options:	• Fail a set number of packets in a user defined total (fail X packets for every Y packets received) • Fail a percentage of packets received

Purpose

The packet counting filter ensures the user can select a number of packets that are to be subjected to impairments through its "pass" or "fail" filters.

If, for example, the user only wishes to corrupt 1% of data received, they would place the 'Packet counting filter' before the 'Packet Corruption' impairment, set the former to fail 1% of all data received and send this down a connection to the Packet Corruption impairment. The remaining 99% 'passed' data would continue on a different connection to the network end point.

An example of this is shown below:



Note the 'failed' and 'passed' labels on the two connections coming out of the packet counting filter, showing which direction the 1% 'failed' and 99% 'passed' packets will take in the above example.

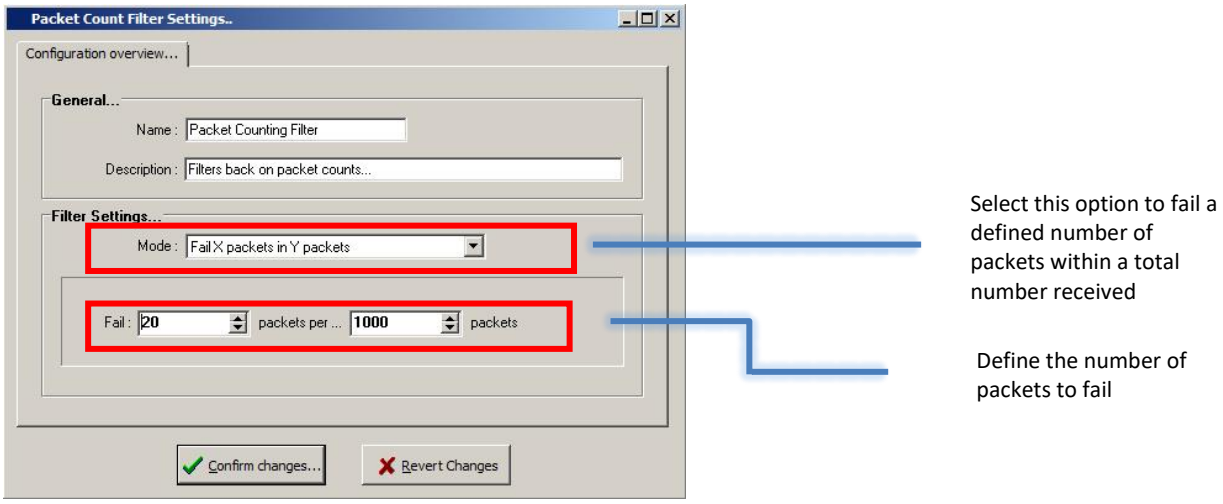
The packet counting filter should therefore be used in advance of other impairments, to direct traffic towards or away from that impairment.

Settings

There are two settings for packet counting, as described below. Right-click on the Packet Counting Filter after it has been added to the Design pane and click on 'Settings' to access.

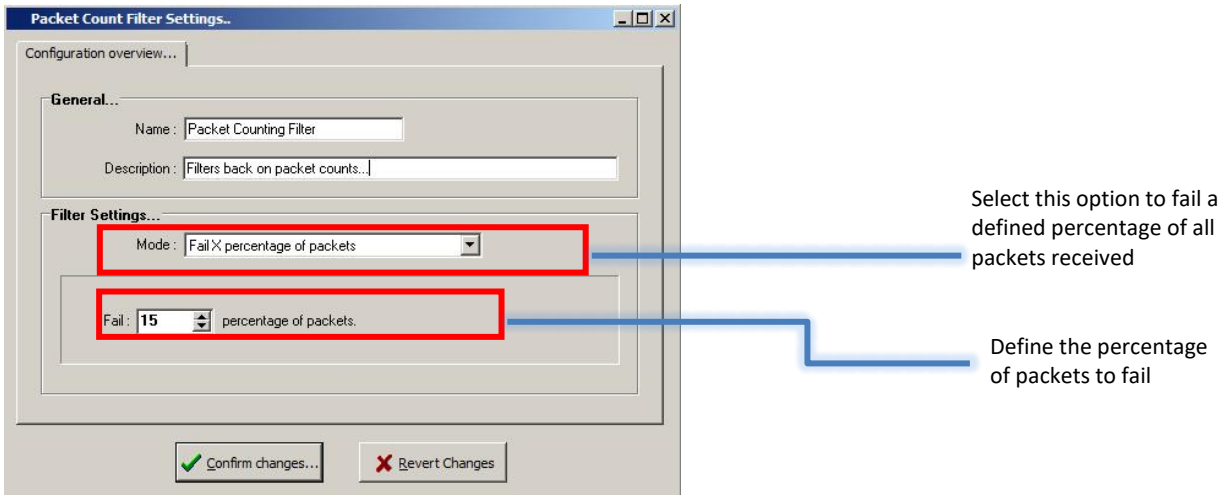
Fail 'X' in 'Y'

Using this setting, the user selects how many packets received should be failed, out of the total number received.



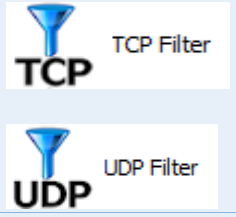
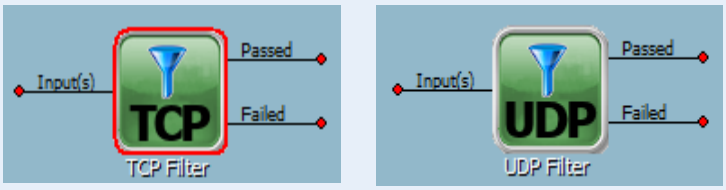
Percentage Fail

Use this mode to set a percentage on how many packets received via the Packet Counting Filter should be failed.



17.2. UDP/TCP Filters

Users can also filter network traffic based on whether the received packets is a UDP (User Datagram Protocol) or TCP (Transfer Control Protocol). These filters also contain advanced settings as described below.

Name:	**UDP / TCP Filter**
Description:	Separates packets received into 2 new streams of data, one that has 'passed' and one that has 'failed'. This is based on an assessment of whether the received packet is either TCP or UDP
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s) :	1 Input – Any source on same connection
Available Output(s)	2 Outputs – packets received will be routed down a 'passed' or a 'failed' connection
Options:	• Simple (pass/fail based on whether a packet received in UDP or TCP) • Advanced (provides advanced routing to identify a specific stream of data between 2 devices)

Purpose

TCP and UDP filters are used to differentiate packets on a connection between a network start and end point (i.e. ports) so that the user can impair traffic that has either passed or failed the TCP/UDP filter. Both failed and passed data (e.g. data that is not TCP traffic and data that is) can be subjected to impairments following the filter.

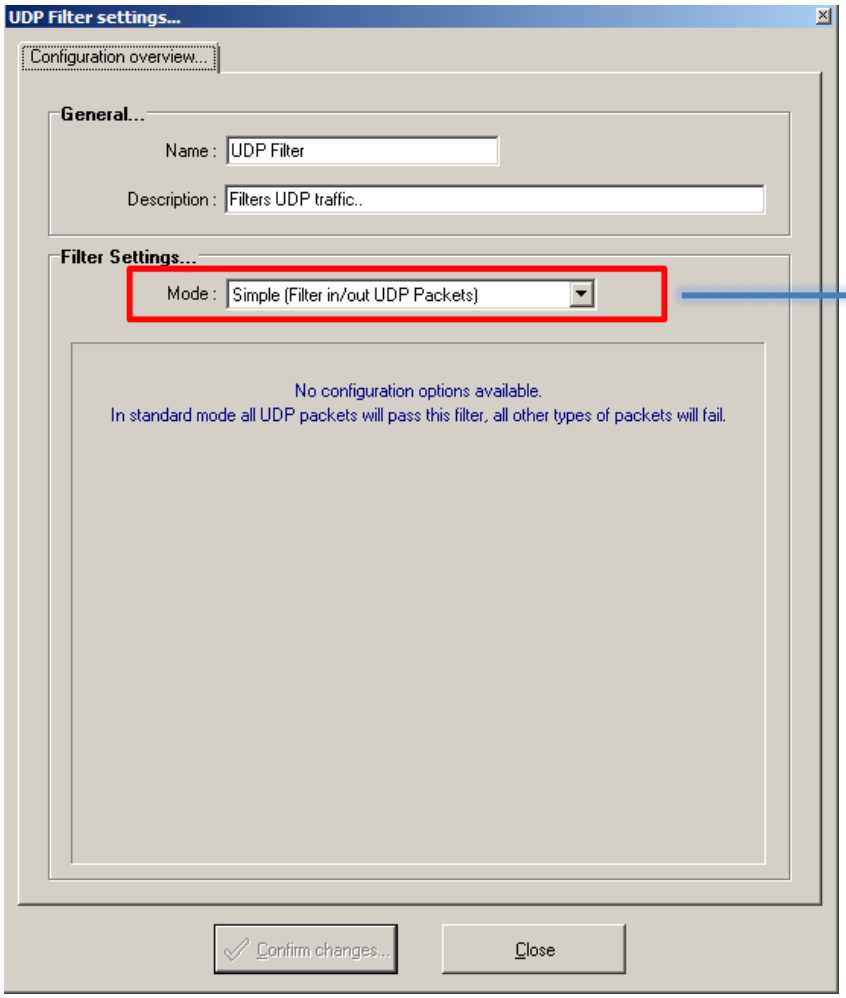
Please Note: Dropping all non-UDP traffic may not be beneficial, as many of the underlying protocols such as ARP are required before UDP communications can occur.

Settings

UDP and TCP filters contain similar settings, as described below.

Simple Mode

Simple mode interrogates all packets received by both these filters and determines if they are TCP or UDP packets. If this is the case, the packet is 'passed' and is released onto the outgoing connection which is marked 'passed'. Similarly, if the packet is not a TCP or UDP packet, it is failed and sent out on the 'failed' connection from the filter. Please note, that only one outgoing connection is required from either a TCP or UDP filter if desired (which can either be 'passed' or 'failed'). Any passed or failed data that is not subsequently passed on to another impairment or the network end point, will be dropped automatically.



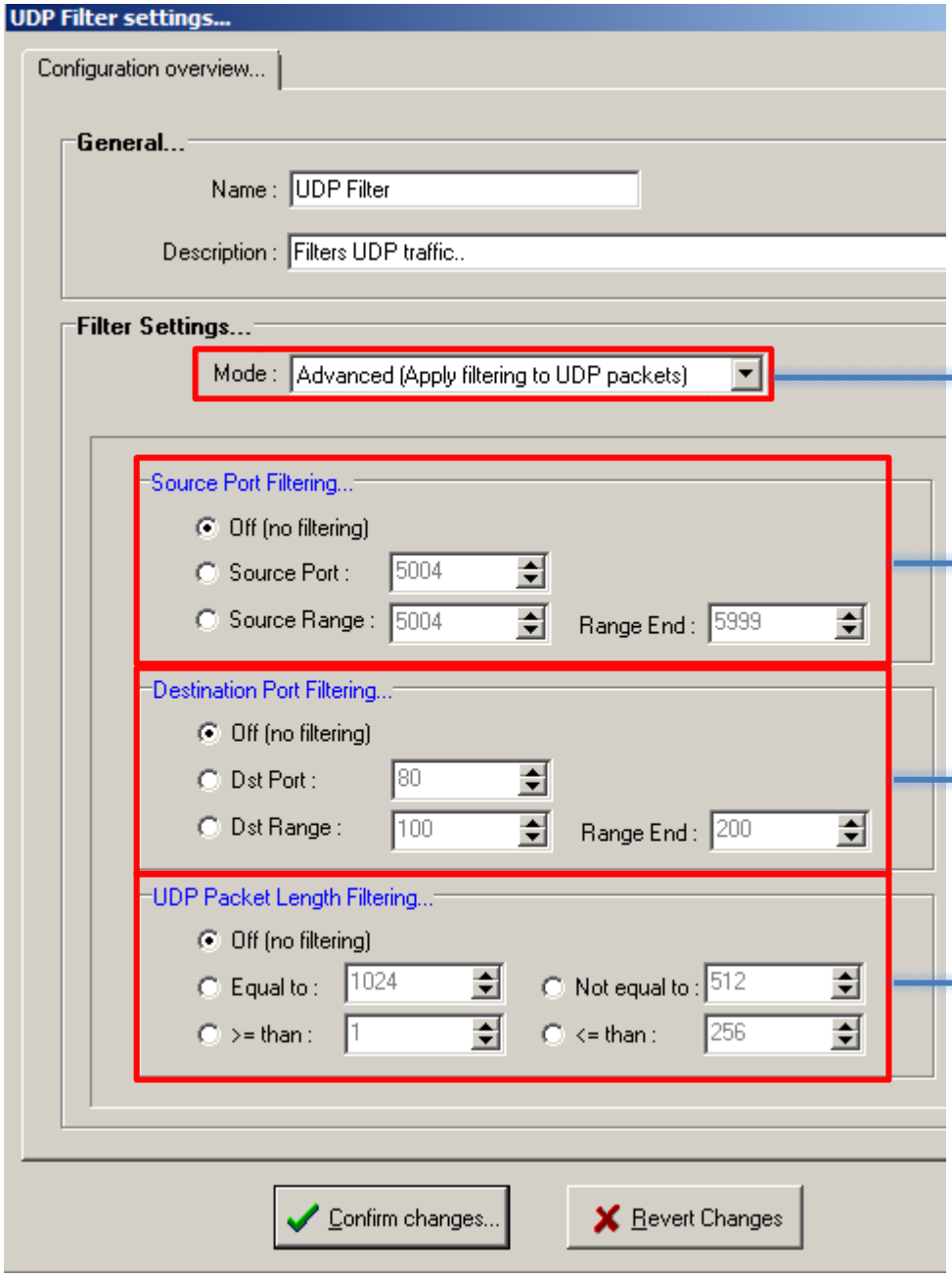
Simple mode performs a check to determine if received packets adhere to the UDP or TCP protocol.

If a packet is UDP or TCP, it is sent out on a 'passed' connection (if one has been set up by the user). If a packet fails this test, it will be sent out from this filter via the 'failed' connection.

Advanced Mode - Data Stream Filtering

The advanced mode allows the user to identify a specific UDP/TCP data stream from all data traversing the network. The user can then subject this stream to various impairments, while leaving all other packets sent/received by devices connected to the SNE untouched (or perform a different impairment on it).

Advanced settings are described below – please note these settings are identical in their appearance and operation for both the UDP and TCP packet filters (aside from the name and description of each).



Selecting Advanced filter mode activates the settings shown below

See Point 1 below

See point 2 below

See point 3 below

1. **Source Port Filtering**
   - **Off (no filtering):** Select this option if the source port is not of interest
   - **Source Port:** Setting this value will make sure the packet's source port is set to the specified value. Only packets from this source port will be 'passed'
   - **Source Range:** Allows a specific range of source ports to be included, if the packet's source port is within the range they will be 'passed'.

2. **Destination Port Filtering**
    - **Off (no filtering):** Select this option to ignore the UDP or TCP packets' destination port.
    - **Destination Port**: Setting this value will ensure the packets' destination port is set to the specified value. Only packets to this destination port will be 'passed'
    - **Destination Range:** Allows a specific range of destination ports to be included, if the packets' destination port is within the range they will be 'passed'.

3. **UDP/TCP Packet Length Filtering**
    - **Off (no filtering):** Packet length is ignored
    - **Equal to:** If the total packet length is equal to this value, then the packet is "passed"
    - **Not Equal To:** if the total packet length is not equal to this value, then the packet is "passed"
    - **Less than Equal To (<=):** The packet is passed if its length if less than or equal to the supplied value.
    - **Greater than or Equal to (>=):** The packet is passed if its length is greater than or equal to the supplied value.

17.3. Ethernet MAC Address Filter

The Ethernet MAC filter allows the user to filter all incoming IP packets for source and destination MAC addresses.

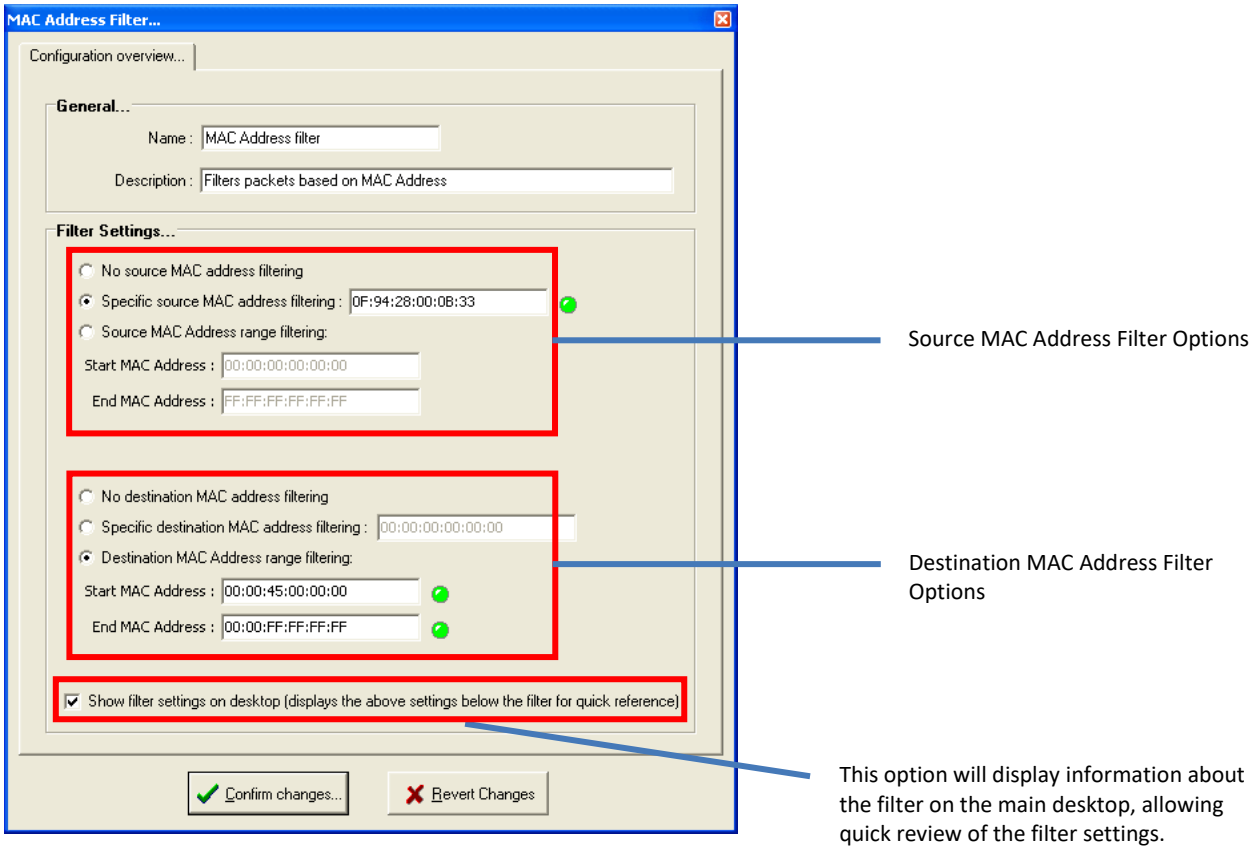
Name:	**Packet Counting Filter**
Description:	Tests a received packet against a single or range of source and/or destination MAC addresses.
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a 'passed' or a 'failed' connection
Options:	• No source MAC address filtering • Single source MAC address • Range of source MAC addresses • No destination MAC address filtering • Single destination MAC address • Range of destination MAC addresses

Purpose

The main purpose of this filter is to test the received packet for a matching MAC address in its Ethernet frame header. The filter provides both source and destination MAC address filtering and 3 different ways to provide those addresses.

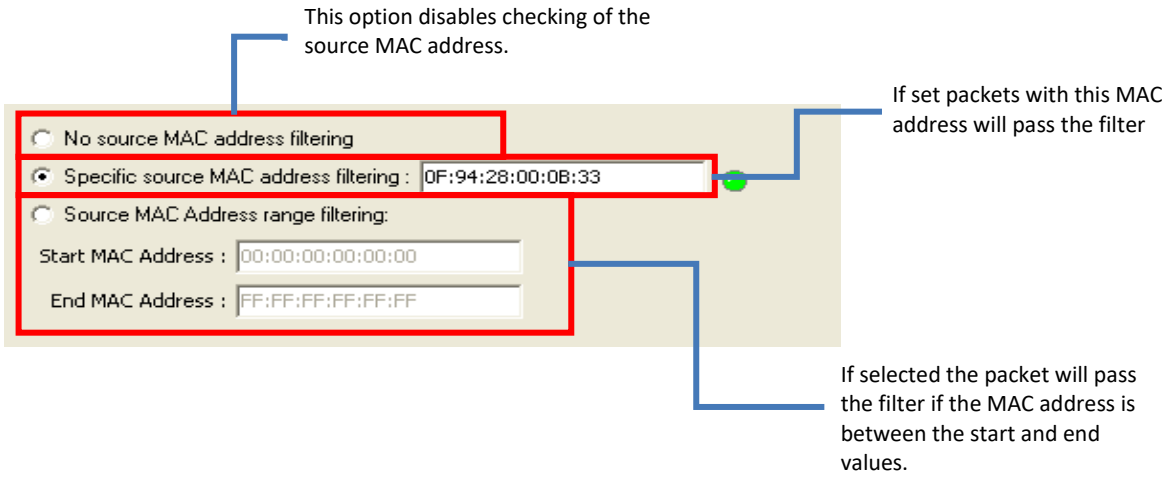
Settings

The settings window provides all the available options on one window. The top section of the filter settings deals with the Source filter options, whilst the bottom half deals with the destination filter options.



Source and Destination Options

The filter provides separate settings for both the source and destination; however they are functionally identical. Therefore, we will focus on the source options:

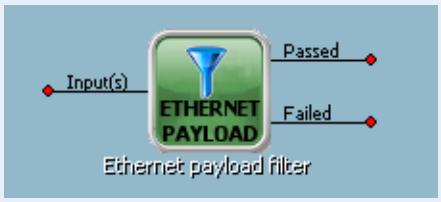


All MAC addresses are validated to ensure they conform to the standard colon delimited format (i.e. “aa:bb:cc:dd:ee:ff”). The green LED’s are used to indicate any problems with the MAC address, and an on-screen error message will give further instructions.

The destination options perform exactly the same roles, except they take effect on the destination MAC address field in the Ethernet frame.

17.4. Ethernet Payload Filter

The filter scans the Ethernet payload field of any received packets.

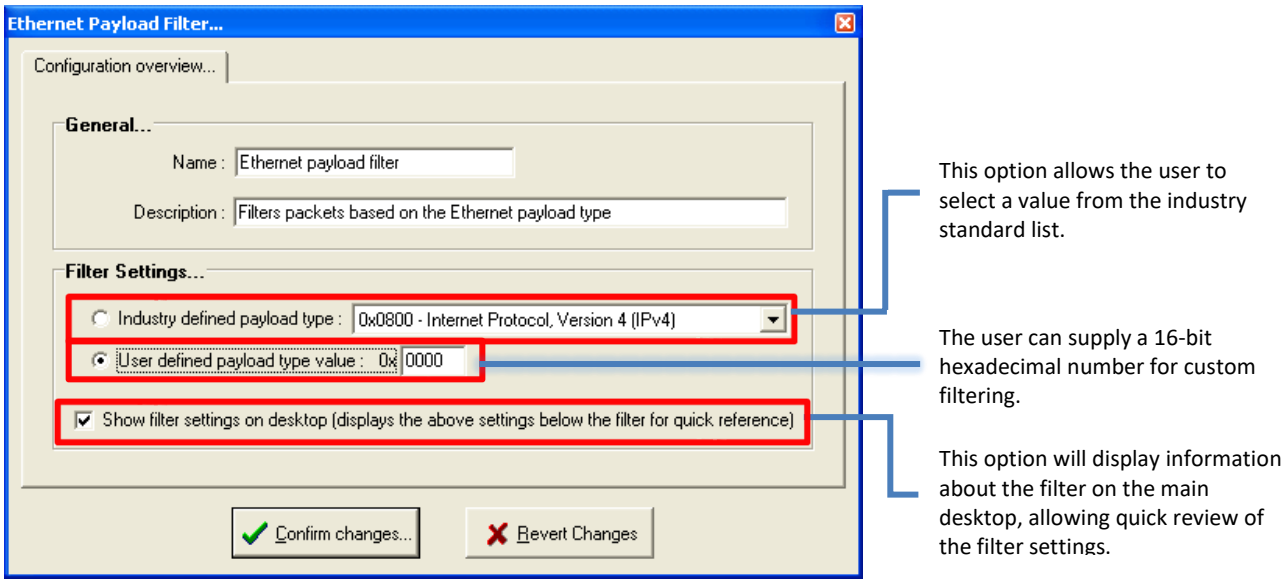
Name:	**Packet Counting Filter**
Description:	Tests against a set value in the Ethernet payload field.
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a ‘passed’ or a ‘failed’ connection
Options:	• Industry defined payload type • User defined payload type

Purpose

This simple filter checks the 16-bit value stored in the Ethernet Payload filter against the user selected value. The tool allows you to select from industry defined types or enter a user defined value.

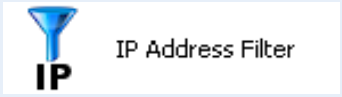
Settings

The settings window provides all the available options in one window:



17.5. IP Address Filter

The IP filter allows the user to filter all incoming IP packets for source and destination IP addresses.

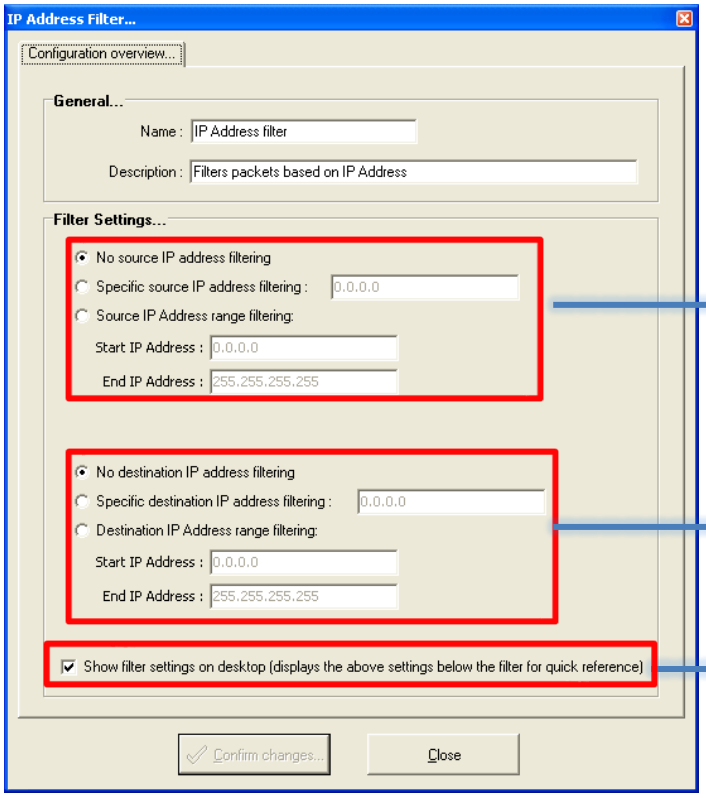
Name:	**Packet Counting Filter**
Description:	Tests a received packet against a single or range of source and/or destination IP addresses.
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a ‘passed’ or a ‘failed’ connection
Options:	• No source IP address filtering • Single source IP address • Range of source IP addresses • No destination IP address filtering • Single destination IP address • Range of destination IP addresses

Purpose

The main purpose of this filter is to test the received packet for a matching IP address in its IP frame header. The filter provides both source and destination IP address filtering and 3 different ways to provide those addresses.

Settings

The settings window provides all the available options on one window. The top section of the filter settings deals with the Source filter options, whilst the bottom half deals with the destination filter options.



Source IP Address Filter Options

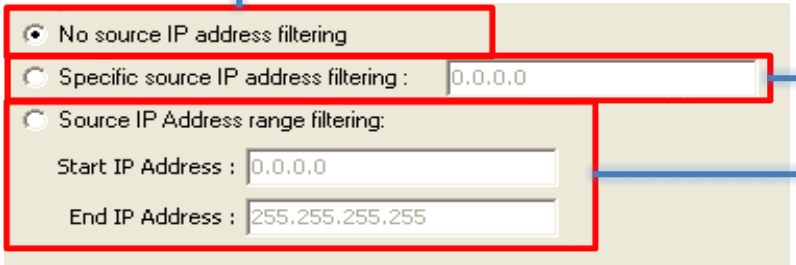
Destination IP Address Filter Options

This option will display information about the filter on the main desktop, allowing quick review of the filter settings.

Source and Destination Options

The filter provides separate settings for both the source and destination, however they are functionally identical. Therefore, we will focus on the source options:

This option disables checking of the source IP address.



If set packets with this IP address will pass the filter

If selected the packet will pass the filter if the IP address is between the start and end values.

All IP addresses are validated to ensure they conform to the standard “dot” delimited format (i.e. “192.168.1.6”). The green LED’s are used to indicate any problems with the IP address, and an on-screen error message will give further instructions.

The destination options perform exactly the same roles, except they take effect on the destination IP address field in the IP frame.

17.6. IP Protocol Filter

The filter scans the IP protocol field of any received packets.

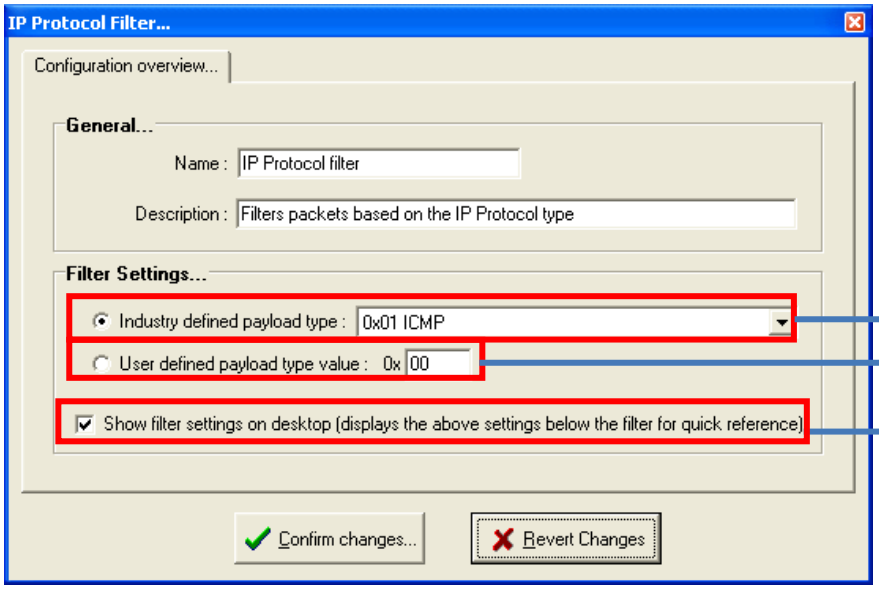
Name:	**Packet Counting Filter**
Description:	Tests the IP Protocol field of any received IP packets
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a ‘passed’ or a ‘failed’ connection
Options:	• Industry defined protocol type • User defined protocol type

Purpose

This simple filter checks the 8-bit value stored in the IP protocol field, of any received IP packets. The field is checked against a user supplied value. This tool allows you to select from industry defined type or enter a user defined value.

Settings

The settings window provides all the available options on one window.



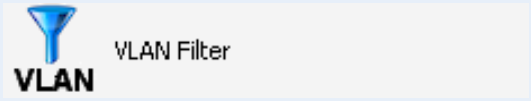
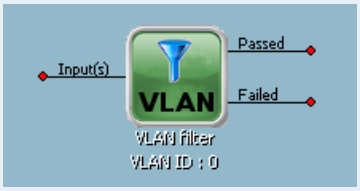
This option allows the user to select a value from the industry standard list.

The user can supply an 8-bit hexadecimal number for custom filtering.

This option will display information about the filter on the main desktop, allowing quick review of the filter settings.

17.7. VLAN Protocol Filter

The filter scans the VLAN field of any received packets.

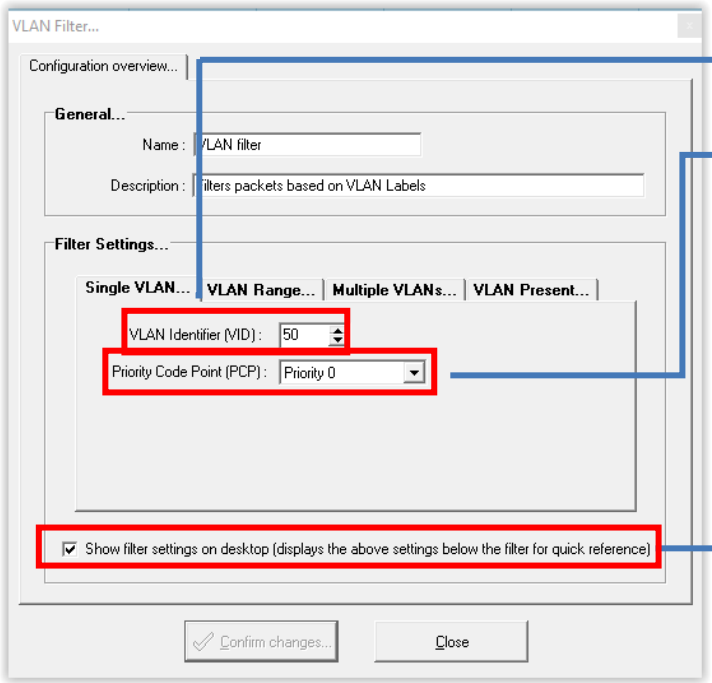
Name:	VLAN Protocol Filter
Description:	Tests the VLAN field of any received IP packets
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a 'passed' or a 'failed' connection
Options:	• VLAN ID • Priority

Purpose

This filter checks for a VLAN labelled packet, if the packets match the user supplied VLAN ID (tag) and priority they will pass the filter.

Settings

The settings window provides all the available options on one window.



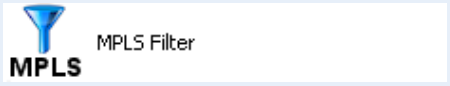
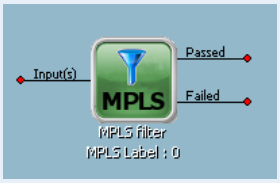
VLAN ID (tag) the packet must match to pass the filter

The VLAN User priority the packet must match to pass the filter

This option will display information about the filter on the main desktop, allowing quick review of the filter settings.

17.8. MPLS Protocol Filter

The filter scans the MPLS field of any received packets.

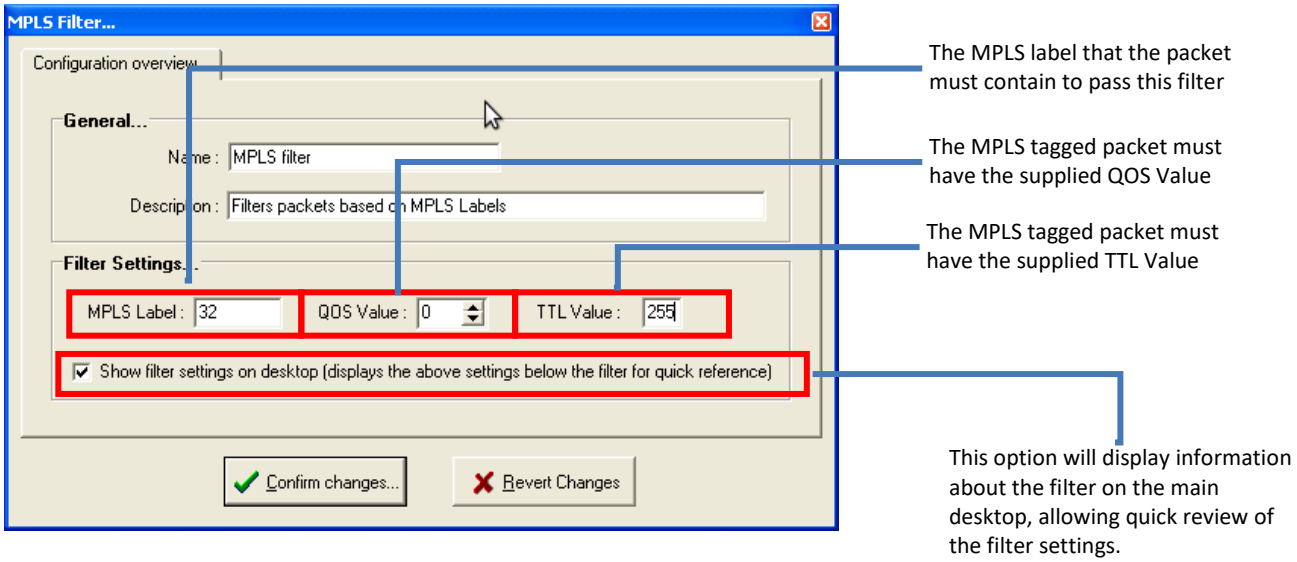
Name:	VLAN Protocol Filter
Description:	Tests the MPLS field of any received IP packets
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a 'passed' or a 'failed' connection
Options:	• MPLS Label • QOS • TTL

Purpose

This filter checks for a MPLS labelled packet. If the MPLS labelled packets matches the supplied values it will pass the filter.

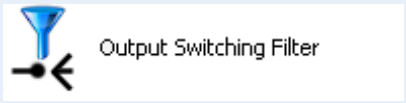
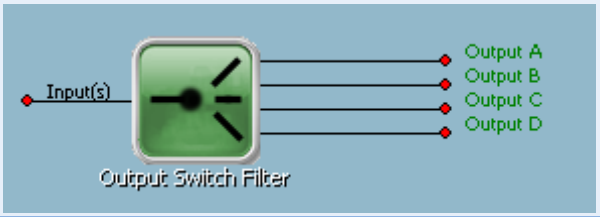
Settings

The settings window provides all the available options on one window.



17.9. Output Switching Filter

The filter can switch incoming packets to several outgoing streams.

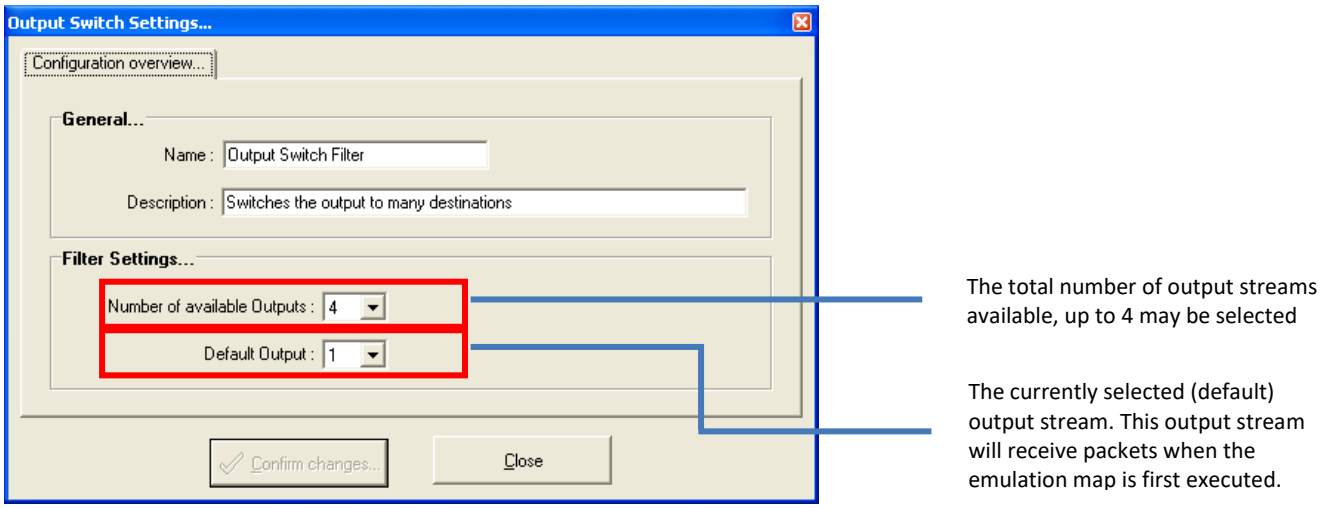
Name:	Output Switch Filter
Description:	Switches incoming packets to one of many outgoing streams
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	Up-to 4 output paths
Options:	• Number of output paths • Default output path

Purpose

This filter will switch the incoming packet stream to one of the available output streams; it performs no further operation on the packets and adds no latency or other impairments. When the emulation map is running the user can click on the output switch filter to manually change the flow of packets.
Please Note: The selection of output streams is currently not supported in the time-line feature.

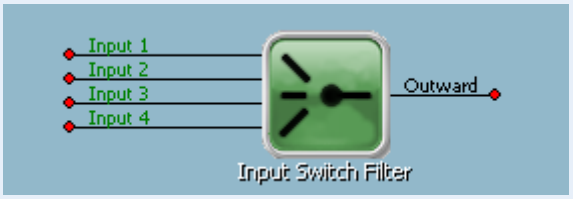
Settings

The settings window provides all the available options on one window.



17.10. Input Switching Filter

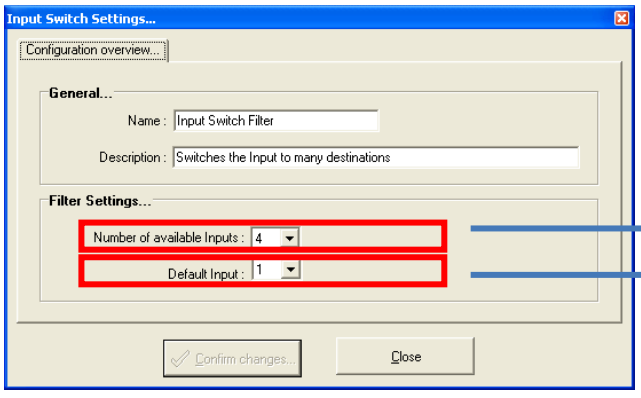
The filter can select one of up-to 4 incoming packet streams; essentially, it is the opposite of the Output Switching Filter.

Name:	Input Switch Filter
Description:	Switches one of multiple input streams to the output.
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	Up-to 4 Inputs – Any sources
Available Output(s)	One single output
Options:	• Number of input paths • Default input path

Purpose

This filter will switch one of the 4 incoming packet streams to the output streams; it performs no further operation on the packets and adds no latency or other impairments. When the emulation map is running the user can click on the input switch filter to manually change which input is used.
Please Note: The selection of output streams is currently not supported in the time-line feature.

Settings

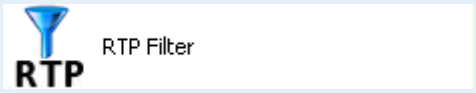
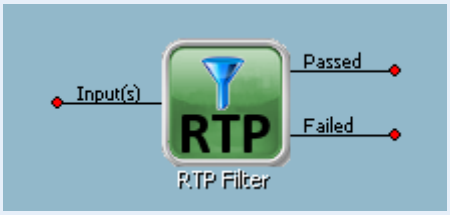


The total number of input streams available, up to 4 may be selected

The currently selected (default) input stream. This is the default stream that will be outputted by this tool when the network map is started.

17.11. RTP Filter

The RTP Filter forms part of the Multimedia Service Solution Pack (MSSP), if you would like to try this feature please contact.

Name:	**RTP Filter**
Description:	Filter RTP packets based on SSRC or Payload Type
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a 'passed' or a 'failed' connection
Options:	• Standard (all RTP packets) • Advanced (Filter by SSRC ID and/or Payload identifier)

Purpose

This filter allows you to extract (and therefore apply impairments to) RTP packets using either a standard or advanced mode.

Settings

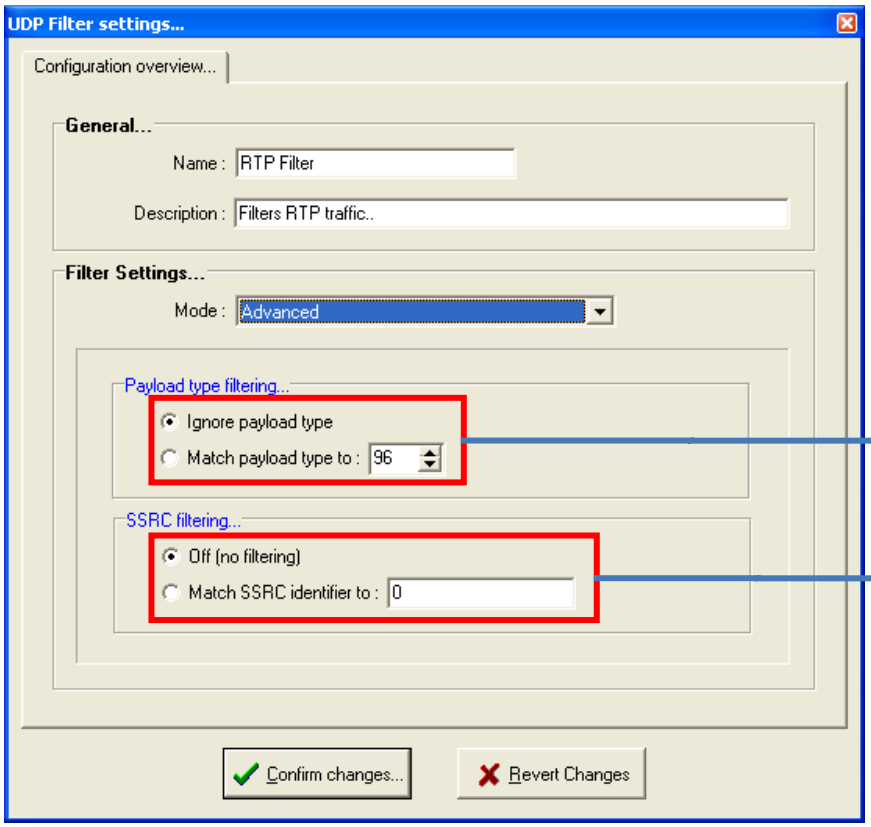
This filter has two modes of operation; standard and advanced mode.

Standard Mode

In standard mode all packets are tested to simply see if they are RTP packets and "Passed" if they conform to basic RTP structures. RTP packets have no formal header or major structural information to 100% identify the packet as RTP or not, therefore the analysis of the packets is performed as a "best effort" analysis. It is therefore recommended you use the "Advanced" mode to better guarantee correct filter by using an SSRC or Payload type.

Advanced Mode

In advanced mode an additional two options become available, namely filtering RTP packets using the RTP payload type and/or the RTP SSRC.

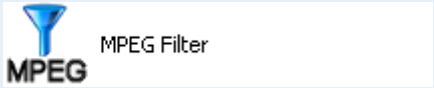
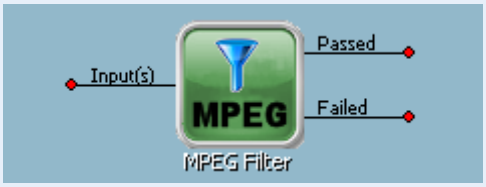


Select the payload type here, this value is checked and any packets that match the specific payload type are "Passed" by the filter

Select the SSRC identifier here, this value is checked and any packets that match the specific SSRC are "Passed" by the filter

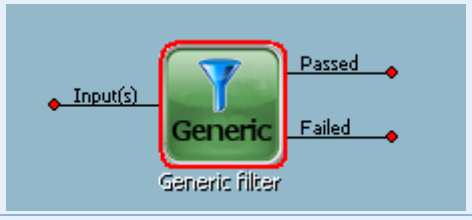
17.12. MPEG Video Filter

The MPEG Video Filter forms part of the Multimedia Service Solution Pack (MSSP), if you would like to try this feature please contact us.

Name:	**MPEG Video Filter**
Description:	Filter MPEG video packets based on contents
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a ‘passed’ or a ‘failed’ connection
Options:	• MPEG Transport Container • MPEG Video Version (v2 or v4) • Frame selection • UDP/RTP Source and Destination ports

17.13. Generic Filter

The Generic Filter allows you to filter against bit or byte patterns within packets received.

Name:	Generic Filter
Description:	Generic filter for bit/byte pattern matching
Network Tool Box Icon	
Design Pane Icon:	
Available Input(s):	1 Input – Any source
Available Output(s)	2 Outputs – packets received will be routed down a 'passed' or a 'failed' connection
Options:	• Up-to 6 filter "components" with extensive options

Purpose

This filter allows you to pattern match bits or bytes in a received packet, it allows for complex pattern testing (with logical operations) to ensure a correct match.

Settings

This filter provides a comprehensive interface for create, modifying and deleting filter components. Filtering is performed by applying a mask to a location in the packet; this mask will allow you to test bits or whole bytes against a user supplied value. If the packet value and user value match, the packet is "passed" by the filter. Each filter component has the following settings:

- Filter Name
  - This is a human readable name for the component; it is not used by the emulator.
- Offset
  - The offset (in bytes) from the start of the packet. A value of 0 means start of packet.
- Length
  - This is the number of bytes to test
- Mask
  - A hexadecimal value which will be applied to the data in the packet
- Value
  - A hexadecimal value that the packet data will be tested against
- Operation
  - The logical operation that specifies how the value will be compared against the packet (such as equals, not equals, greater or less than)

Technical Operation

When a packet is received by the filter, each filter component will be tested against the packet. If all filter components test correctly then the packet is “passed”.

During this operation the SNE Network Emulator will extract X bytes (specified in the components “length”) starting at the byte offset.

The bitmask will now be applied to the bytes, this allows certain bits to be tested for individual values rather than whole bytes. Please see the bitmask technical explanation below for more information.

After the bitmask is applied the remaining values are tested against the user defined value.

Understanding the bitmask in detail

Technically the bitmask is logically NOT-ed and then logically AND-ed with the actual value to be tested.

In order to understand the bitmask fully, the following example shows the bitmask of FF0FF0AA as a binary representation, being applied to 4 sample bytes.

	Byte One	**Byte Two**	**Byte Three**	**Byte Four**
Input (Sample) Packet Bytes	6F 01101111	FF 11111111	DD 110111101	F0 11110000
Bitmask Value	FF 11111111	0F 00001111	F0 11110000	AA 10101010
Resulting Test	6F 01101111	0F 00001111	D0 1101000	A0 10100000

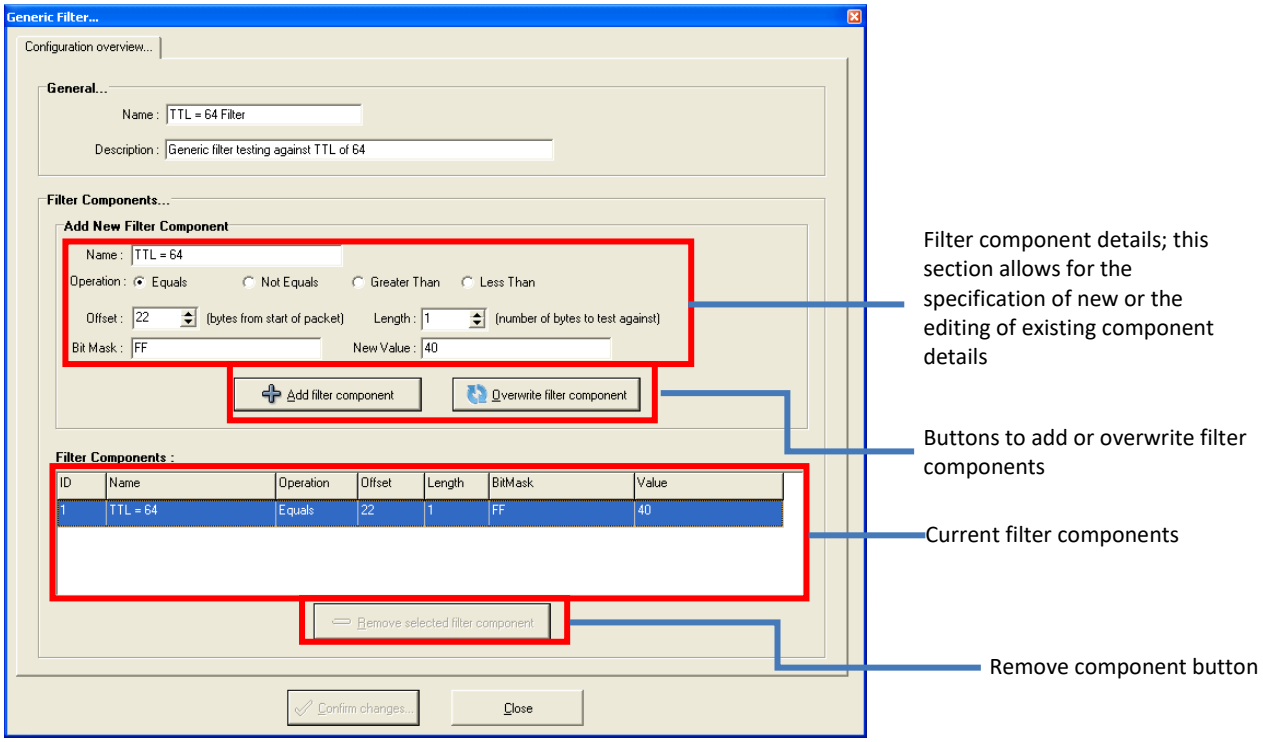
Byte One – The bitmask of FF means that all bits are to be tested against, therefore the result is the same as the input.

Byte Two – The bitmask of 0F means that only the 4 lower bits are to be tested against, this means the resulting output has only the bottom 4 bits shown for testing against.

Byte Three – The bitmask of F0 means that the upper 4 bits are to be tested against, this means that the input of DD loses its lower four bits becoming the D0 result.

Byte Four – The bitmask of AA has every other bit set, but the input byte has only the upper four bits set (F0) – therefore the output is A0.

Filter Settings



Adding a filter component

To add a new filter component, you must firstly enter all the details for the component; its name, operation, offset, length, bitmask and value properties. For examples please see below. Once you have entered all the information click the “Add filter component” button and the component will be added to the list of filter components.

Modifying a filter component

In the “Filter Components” list, click on the filter you wish to modify. Its settings will be copied to the section above so you may modify them. Once you have made your changes click “Overwrite filter component” and the changes will be made.

Copy and creating a new filter component

In the “Filter Components” list, click on the filter you wish to duplication. Its settings will be copied to the section above so you may modify them. Once you have made your changes click “Add filter component” and the new filter will be added.

Deleting a filter component

To delete a filter component, simply select it in the “Filter Components” list and click “Remove Selected Filter Component.”

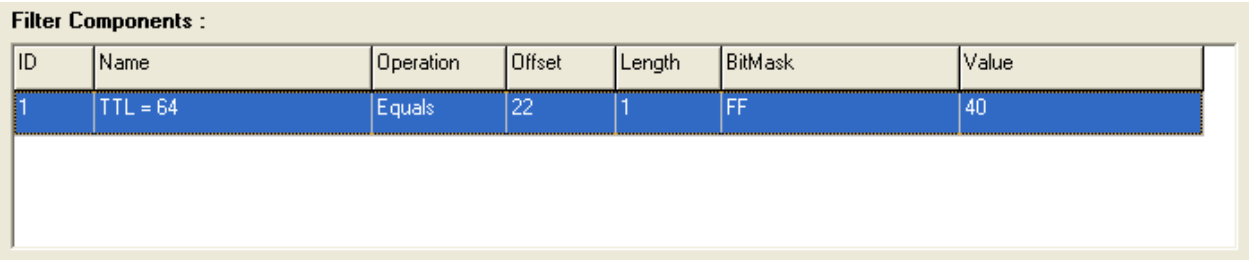
Please note – no changes are saved until you click “Save Changes” at the bottom of the window.

Example

Filtering packets with a TTL of 64

In this example we wanted to “pass” all packets that have a TTL value of 64, in this case our filter component must “look” at the TTL byte within the packet and compare it against the value of 64.

The filter component will be set as follows:



We want to test for an exact match of 64, therefore the operation is a “equals”; as the TTL has an offset of 22 bytes from the start of the packet we set the offset to 22.

The TTL value is also 8 bits wide so we set the length to 1 byte. The Bitmask is set to (hexadecimal) FF, this means we will to test all 8 bits in the 22nd byte against our value. Finally we have the value of (hexadecimal) 40 which is 64 (base 10).

18. Virtual Routers

18.1. Feature set

The SNE provides “Virtual Routers”. These virtual routers are designed to exist both at the edge (or “Entry / Exit” point) and internally (representing “hops” within the WAN).

Normally these are used to simulate ADSL / cable modems, ISP gateways, cloud systems, data centres or large distributed Wide Area Networks.

It should be noted that there are some minor limitations with Virtual Routing:

- There is no support for address translation (NAT/PAT); if you should require this functionality please contact us.

Each virtual router supports:

- A “physical interface” connection from any emulator port (this can be impaired, filtered, etc. by simply connecting those impairments into the inbound connection)
- Up-to 6 virtual interfaces, allowing you to interconnect Virtual Routers to each other. This is used to form the WAN links and can take any network topology format (ring, star, mesh, double ring, etc.)
- Dynamic and static IP address allocation.
- Automatic, static and OSPF built routing tables.
- Advanced settings such as MAC address options, ARP table time-out values, etc.
- Simulation of “Virtual Computer” end-points (called “Load Generator Targets”) which are connected directly to each Virtual Router. These virtual computer targets simulate the TCP/IP stack of a computer and allow load generators to send traffic to them.
- Multiple “Traffic Analysers” to decode and grade the quality of any load generation received by the virtual computers.

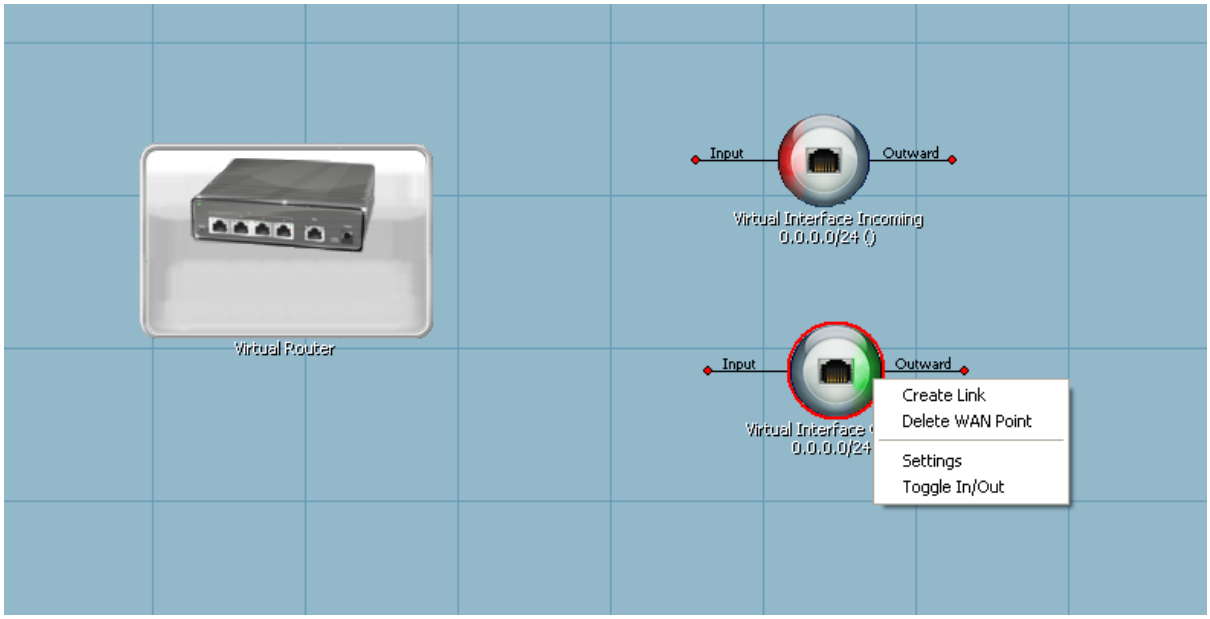
18.2. Virtual Routing

18.2.1. Introduction

To create a new “Virtual Routed” network map please right-click on the “Device/Map Navigation” window and select “New routed mode map > Create blank virtual router map” (see the “creating network maps” section for more information).

18.2.2. Using Virtual Routing

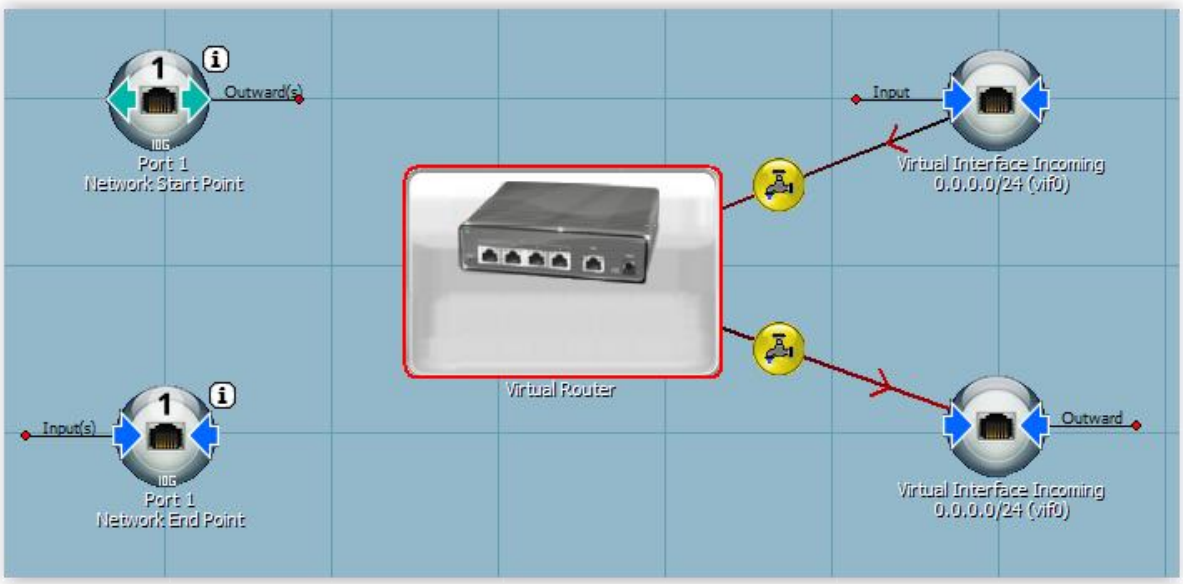
In the tool box you will see the “Virtual Routers” tool. Please drag one of these onto your network map along with 2 x “VR Virtual Interface”. Please select one of the WAN Points and toggle it as “In”:



Let’s go ahead and link up the “Virtual Router” (VR) and “Virtual Interfaces” (VI) – click on the “Virtual interface Incoming” and “Create Link”, finally click on the VR and the link should be created. Now right-click on the VR and select “Create WAN output Link” and click on the “Virtual Interface Outgoing.”

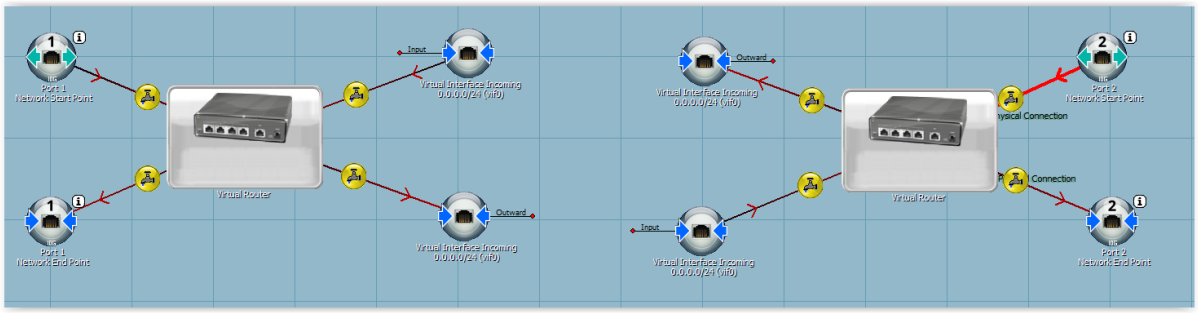
At this point we have connected the VR to its VI’s, this allow the virtual router to know which interfaces are virtual and will be used to talk to the WAN.

Now we want to connect the physical ports so that the VR can communicate with your actual hardware devices. Add “Port 1 – Incoming” and “Port 1 – Outgoing”, you should see:



We link up the physical side in a similar way as to the WAN side; right-click on the “Port 1 – Incoming” and select “Create Link”, then click on the VR. Likewise right-click on the VR and select “Create Physical Output Link” and select the “Port 1 – Outgoing”. After these operations you should have a fully connected EVR.

Go ahead and create a second VR but this time use Port 2 instead of Port 1, you should have the following network map:



18.3. Configuring Your Virtual Routers

Each VR has its own settings and routing table. It is critically important to configure this information correctly or you could create circular packet loops or cause an invalid operation.

VR – Understanding the settings

The Virtual Router must be configured correctly for normal operation.

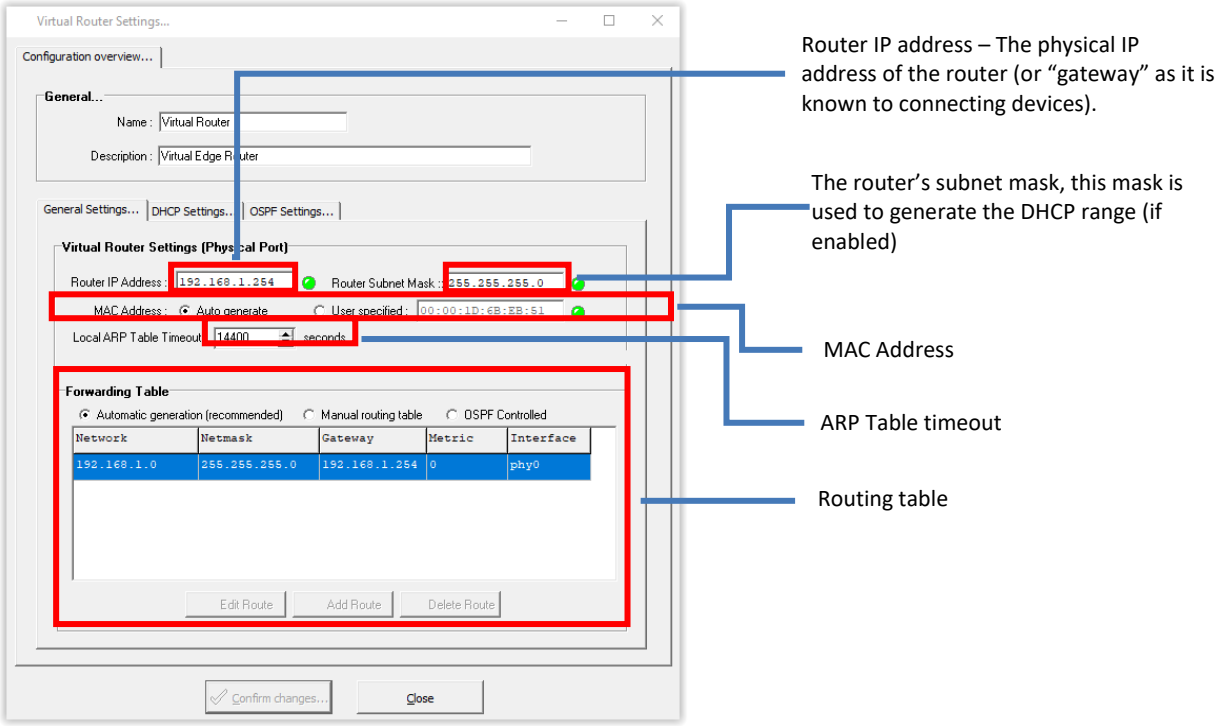
It is recommended that you allow the virtual router to automatically select certain functions (such as the routing table). Modifying these settings should only be performed with expert knowledge or active assistance from us.

Failure will result in incorrect operation of the virtual routers, the entire network map or cause the emulator to quickly reach maximum load (in the case of invalid circular links, where packet rates rise exponentially).

Virtual Router Settings

The Virtual Routers have quite a number of options. A large number of these settings can directly affect the operation of your network maps, and **therefore changes should only be made by knowledgeable personnel**.

18.4. General Settings



Virtual Router – Physical Port Settings

If the VR is connected to a physical port it must present itself as an IP addressable device on the physical network. This allows the Virtual Router to become the "gateway" for devices to communicate across the WAN. Under these settings you can see the following options:

Router IP Address – The IP address the virtual router will "exist" at. All devices connected to the physical port will talk to this IP address (as the Gateway) to access the VR and WAN beyond it.

Router Subnet Mask – This subnet mask allows the Router to generate an acceptable DHCP range (if enabled). Changing this value will automatically update the DHCP Start and End Range.

MAC Address – Allows you to choose an automatic or manually set MAC address.

Local ARP Table Timeout – You can specify the ARP time outs to trigger a flushing of the Virtual Router's ARP tables.

Virtual Router – Routing Table

The main purpose of the Virtual Router is to act as a gateway to other WAN's through other Virtual Routers. This functionality requires the routers to forward (or route) packets to the correct destinations through one (or more) virtual routers.

This table is therefore paramount to the successful configuration and execution of virtually routed networks.

You have three options when configuring the routine table:

- Automatic (recommended)
- Manual (user configured)
- OSPF (use Open Shortest Path First routing protocol, see below)

The forwarding table provides the ability to add, remove and edit each of the routes. Each route has the following information:

Network (or destination) – This is the network address to which this routing table entry exists. It provides, along with the network mask, the ability for the Virtual Router to know if the packet received is for this destination.

Netmask – This is the netmask applied to packets to see if they are allowed under the Network (or destination).

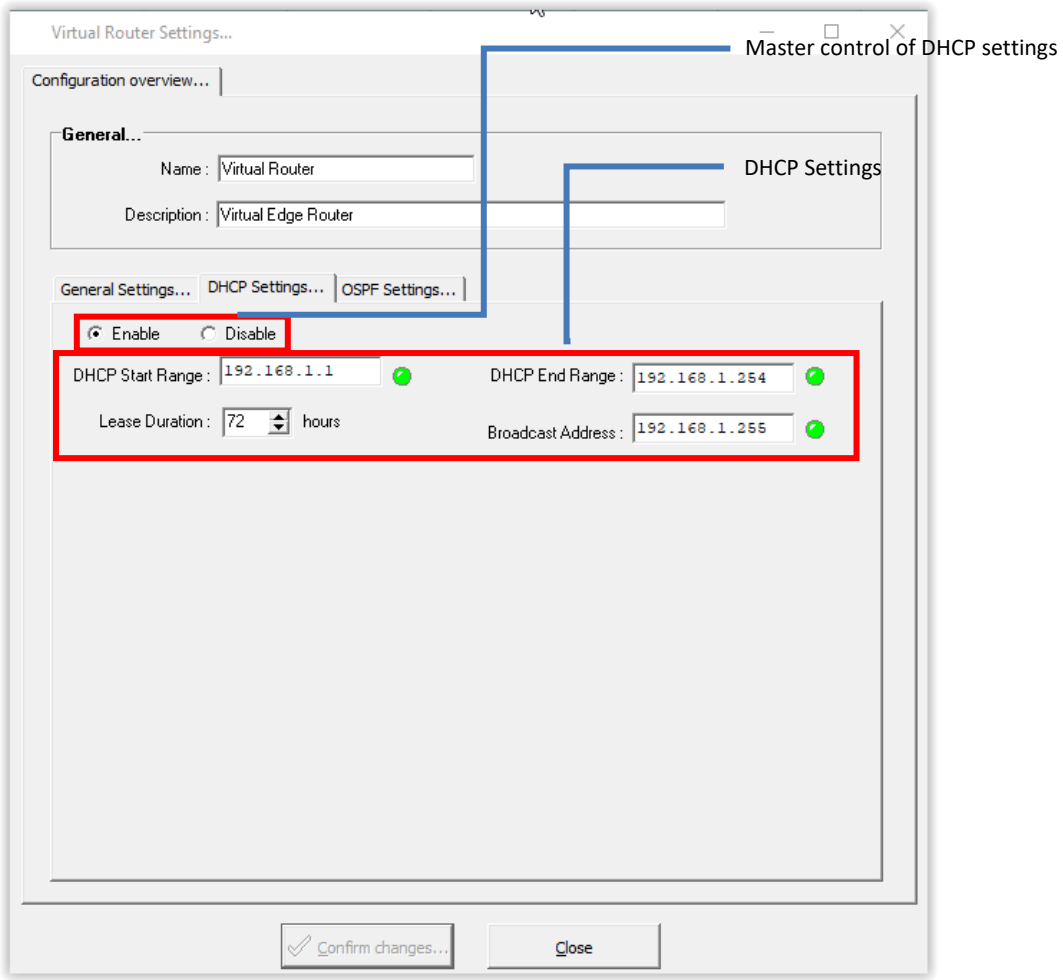
Gateway – The gateway located at the first (or next) hop in the packet's journey

Metric – If duplicate routes exist for the same packet, this metric is used to decide which route is the preferred path. This value can be changed in real-time to affect the routing.

Interface – The interface to which the packet should be routed, the destination Gateway must be present on this interface.

It is highly recommended you leave this on "automatic" for most networks.

18.5. DHCP Settings



DHCP Settings – If enabled the router will accept DHCP requests and assign IP addresses from the available DHCP pool. If DHCP is disabled on the router, the router will still act as a gateway to any device that communicates with it. These devices will normally use static IP addresses that is within the subnet range of the virtual router.

Disabling DHCP

If you disable DHCP then you must manually assign static IP addresses to your devices.

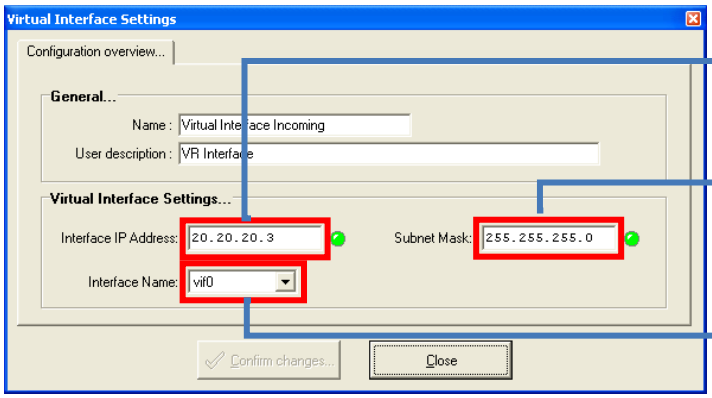
In addition, you must also set-up any routes to direct any gateway traffic to the Virtual Router. For example, under Linux you should issue "`route add default gw 192.168.1.254 eth0`"

Virtual Router – OSPF

The OSPF (Open Shortest Path First) protocol allows Virtual Routers to automatically build routing tables by detecting the paths between routers. In addition, this protocol also supports the rerouting of packets when any link loss or degradation occurs.

For more information on using the OSPF protocol please view the included Sample Network Maps.

18.6. Virtual interface Settings



The IP address of this interface, at present this is only required for OSPF (it can be left as “0.0.0.0” if OSPF is not used)

Subnet mask of the virtual interface, at present this is only required for OSPF (it can be left as “255.255.255.0” if OSPF is not

Interface name **(required)**

The Virtual Interface provides the connectivity link between Virtual Routers, with each Virtual Router being able to route packet through the Virtual Interface.

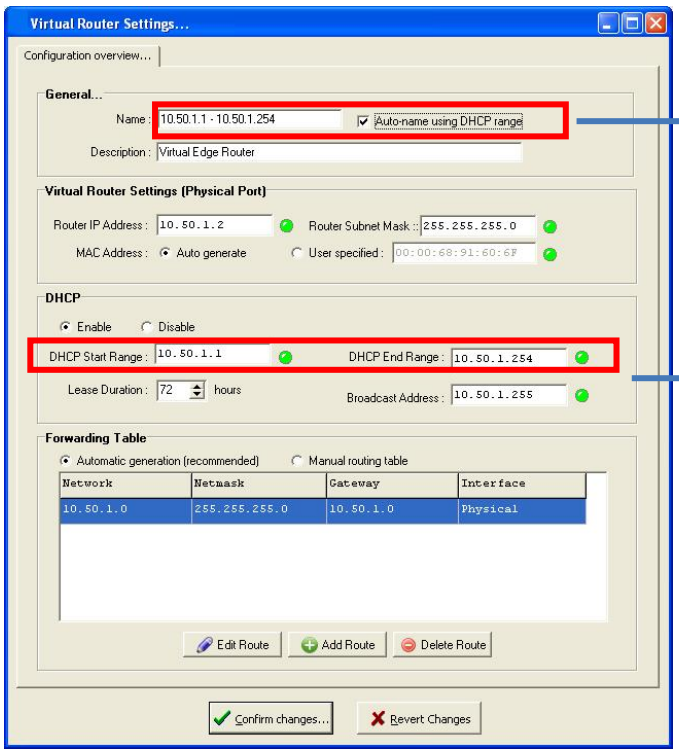
A virtual router requires **two** virtual interfaces that share the same Interface name (vif0, vif1, etc) – This is the only **required** field that you must set on the Virtual Interface.

The Interface IP Address and Subnet mask are used in OSPF to populated OSPF routing tables and are not required if a manual or automatic routing table is used.

Configuring an example Virtual Router

Having assumed you have followed the previous section detailed “Using Virtual Routing”, we will now configure your virtual router.

Right-click on the first VR (located on the left side of the network map), change its IP to “10.50.1.2”. You will notice the DHCP Range will automatically change to show:



Notice the selection of “Auto-name”, this allows the EVR IP range to be clearly visible on the network map.

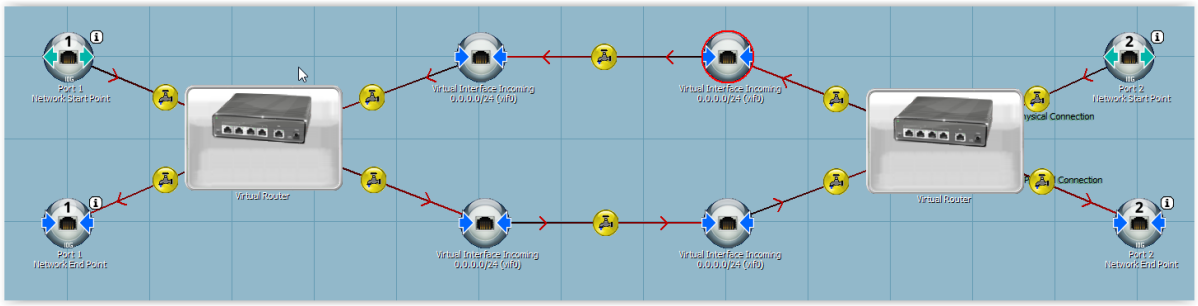
The DHCP range now reflects the IP address

You will also note that the forwarding table now has a physical interface entry for the 10.50.1.x network.

We will leave the second VR with its default settings (192.168.1.x Range).

Connecting up your Virtual Routers

Simply right-click on the “Virtual Interface Outgoing” tool and select “Create Link”, and then select the remote “Virtual Interface Incoming” tool. You have created your first VR network map with a non-impaired WAN, you should see the following network map:



Configuring

Forward Table Changes

Now that you have connected the two VR’s together the routing tables for both EVR’s will **automatically** change to show the WAN links (assuming you left the routing table on “automatic”). If you now view the routing table you will see the link to the remote VR.

Adding your impairments

The process for adding WAN impairments is the same as normal bridged mode; simply add the impairments you wish to the link between Virtual Interfaces, a quick example is shown below:

In the above screenshot you can see the simulation of a simple ADSL connection with 20Mb/s down rate and 1Mb/s up rate (from the 192.168.1.x network).

18.7. Real Time Stats

After a network map has been started each virtual router will present information to the user for diagnosis and information purposes.

DHCP Leases

When operating, the VR will show a “DHCP Leases” button which can be clicked to show DHCP lease information. When this information is available the VR will look like:

The information presented includes the DHCP assigned IP addresses, the devices MAC address along with the lease duration and expiry time.

DHCP and stopping Virtual Routing Maps

Due to the nature of the Network Emulator you may start and stop network maps at will. If you stop a network map the VRs are lost; meaning that the routed traffic stops flowing and you experience an outage. In addition to this outage the VRs lose their DHCP tables meaning that all DHCP leases are lost (but often “held” by the physical IP device until the lease is up).

This outage and loss of DHCP leases cannot be prevented (you are removing the Virtual Routers so routing cannot take place).

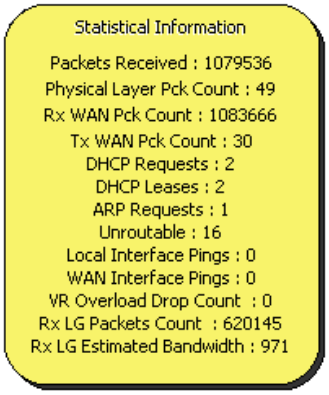
In order to counter the problem of missing DHCP leases each Virtual Router will not attempt to issue new DHCP assigned IP addresses to any connected machines or IP devices, instead it will accept packets from any host in the DHCP range and only issue new DHCP addresses if an IP device specifically asks for one.

This means in practice after a network map is stopped and started the flow of IP traffic will commence as it did when the DHCP leases were first issued.

The net result is that the DHCP leases window shows ONLY the DHCP addresses that have been assigned during this active session, if you stop and start the network map you will lose this information.

Run-Time Stats

By hovering your mouse over the small “gear icon” you will see a number of real-time stats, these can be used to understand the flow of packets in your network map and troubleshoot any invalid configurations. The following statistical information is presented for each VR:



Packets Received – The total number of packets received on all interfaces regardless of origin.

Physical Layer Packet Count – The number of packet received by the physical interface. This allows you to see if the computers or IP devices connected to the physical port are communicating correctly with the EVR.

Tx/Rx WAN Layer Packet Count – The total number of packets transmitted or received on all WAN links out of the EVR, this shows that the forwarding tables on any connected EVR’s are correct.

DHCP Requests – The total number of DHCP requests that have been received by the EVR

DHCP Leases – The total number of valid DHCP requests that have resulted in a lease being granted to a physical IP device.

ARP Requests – The number of ARP requests received by this virtual router.

Unrouteable – The total number of packets that were received (on WAN or Physical Interface) that were not routable because no entry existed in the forwarding table (for example trying to access a machine outside the virtual router’s subnet range)

Local Interface Pings – The number of pings to the Virtual Router received on the physical interface.

WAN Interface Pings – Number of pings received across the WAN to the Virtual Router.

VR Overload Drop Count – Depending on your SNE Network Emulator model you can flood the Virtual Router with more traffic than it can handle (i.e. through background traffic generation, or a large amount of duplicate packets). This count lets you know of the number of packets dropped due to this condition and gives you an indication of performance limitations.

Rx LG Packets Count – Total number of SNE Network Emulator load generator packets received, this does not count any external load generators and does not count “Background Traffic Generators”

Rx LG Estimated Bandwidth – A **rough** estimate of the current bandwidth in-use by the virtual router to forward on SNE Network Emulator load generator packets. This is the total bandwidth of all load generated packets received (but not external or background traffic generators). This is a rough estimate and should only be used for guidance.

Unrouteable counts and background traffic generation

If you have background traffic generation on your network map you will notice the unrouteable packet count increasing in line with the traffic generation. This is simply a by-product of this sort of traffic generator and should be ignored.

18.8. Virtual Routers and Load Generators

Protocol based load generators (TCP, RTP, etc.) can use Virtual Routers to simulate traffic flowing around the area of the WAN. This can be used as contention against real traffic or to understand how the flow of packets occurs on most networks.

Additional Tools

Virtual routers will be able to handle the flow of packets from any load generator by nature of their routing activities. This means without any real set-up a Virtual Router will be able to route traffic (internally) based on the load generators destination IP address.

However, to get the most from the functionality two additional tools are required.

The “Load Generator Target” is a special tool that allows virtual routers to simulate a computer (or IP device) connection to the virtual router. This target is used to “sink” (or consume) all the packets from the load generators and **prevents flooding of packets.**

Load Generation Warning

If you use a protocol-based load generator (TCP, RTP, etc.) it will generate packets that cannot have their TTL reduced. This requirement is due to performance reasons but has a knock-on effect of causing circular loops in which the network emulator may consume all resources.

You must be sure that all Load Generators have “Load Generator Targets” configured for them, failure to do this may consume all resources and cause an outage of the emulator.

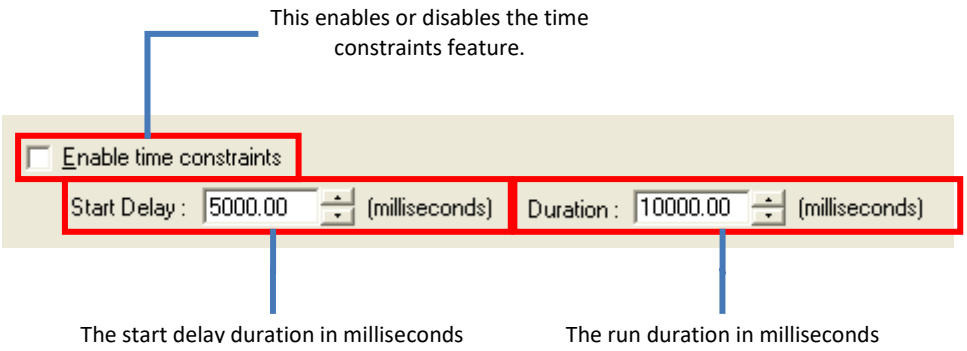
19. Time Constraints

Introduction

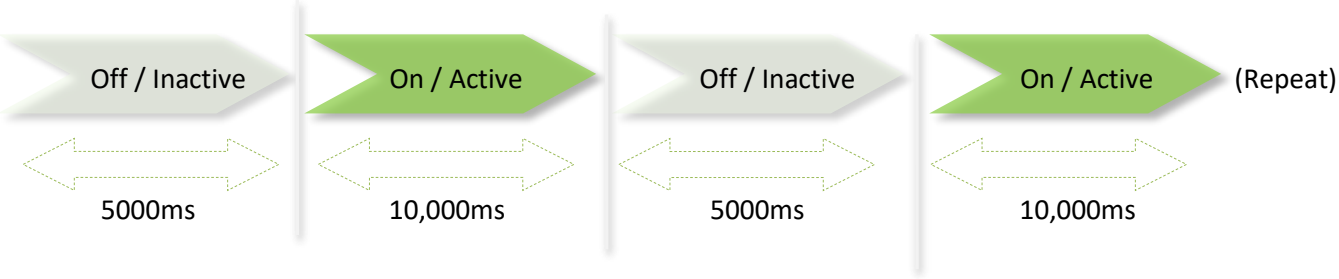
Some impairment tools provide time constraints; notably packet drop, delay and bandwidth throttle. Time constraint options allow you to provide a time period in which the tool should remain inactive (or off) and a time period in which the tool should be active (or on).

Settings

Tools that support time constraints present settings such as the following:



Using the above settings as an example, if a network map was executed or played the impairment would not start for 5 seconds (5000ms). Once the 5 seconds has passed the impairment would then operate for 10 seconds (10,000ms) at which point it would go back to inactive for 5 seconds. The process repeats as shown below:



20. Advanced Operations

20.1. Introduction

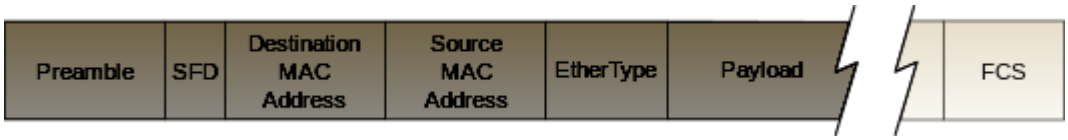
This section contains details on advanced tools, or advanced functionality offered by some tools.

The functionality and features offered by these tools are not available on all models and are **optionally licensed**. If you require the functionality please contact us.

20.2. Frame Check Sequence (FCS)

The FCS is a 4-byte value that exists at the end of the Ethernet frame, it provides a method of validating the packet's contents are correct and have not been altered.

The 4 bytes are usually generated by the Ethernet hardware and are not visible to higher level Ethernet devices (such as computers, etc.).

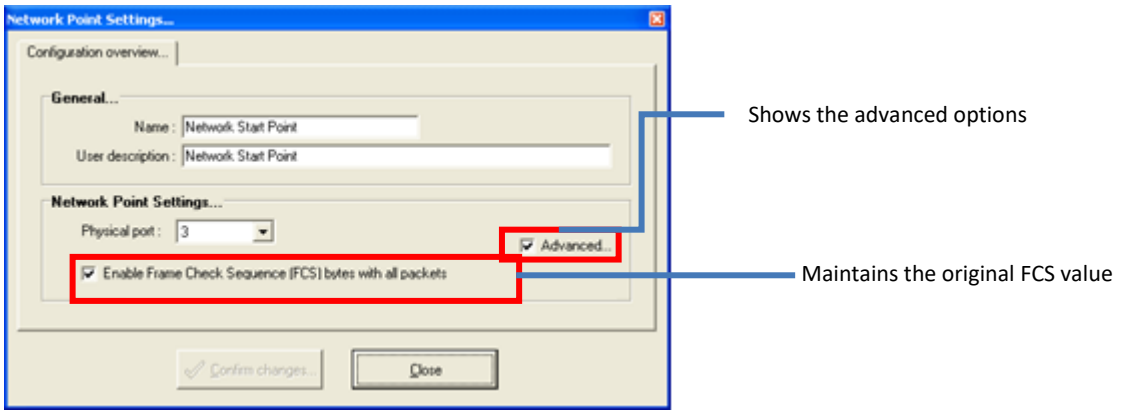


20.2.1. **FCS - Normal Operations**

Under normal (default) operation the FCS is transported transparently by the emulator and automatically recalculated on transmission out of a physical port. This ensures that the downstream connected device still receives a valid packet, even if it was modified by the SNE. However, in some scenarios it may be desirable to modify packets and not recalculate the FCS.

20.2.2. **FCS - Enabling**

Recalculation of the FCS can be enabled or disabled through a single checkbox on the Start Point settings window.



When checking the “Enable Frame Check Sequence” check-box the emulator will maintain the original FCS value, i.e. it will not recalculate this value even if the packet has been modified.

FCS Warnings

Enabling the FCS option allows you to modify (or corrupt) packets whilst leaving the FCS unchanged (and therefore invalid). On most hardware this will result in a RX checksum failure error (or “RX discards”) if viewing network statistics.

It should be noted that the following tools do not support FCS:

- Traffic record – This tool does not record the additional 4 bytes
- Traffic replay – This tool does not produce the additional 4 bytes expected by an FCS enabled outgoing port.
- Background traffic generator – This tool does not generate or append the additional 4 bytes expected by an FCS enabled outgoing port.

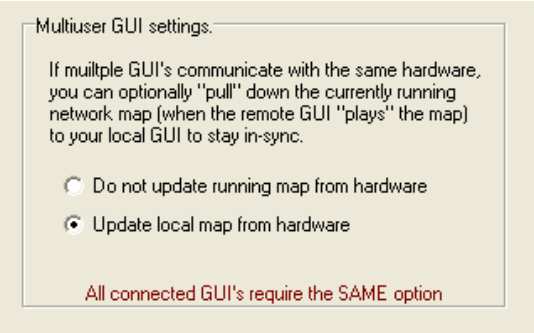
20.3. Updating maps on remote clients

As the GUI holds the network maps (locally on the machine it is installed on) you can run into mismatches between GUI's on different machines. This mismatch occurs because each GUI will have a different copy of (or completely lack a) network map that is currently executing on the emulator.

The SNE provides a way of retrieving these maps so that remote clients can all see the same network map.

20.3.1. Enabling retrieval of network maps

In order to enable the retrieval of network maps from the hardware, you must enable the "Multiuser GUI Settings" options in the IDE settings. Please click the "Tools" menu, followed by the "GUI Settings" and find the Tab Sheet marked "Map Settings". At the bottom of this window you will see the options:



To enable the option please select "Update local map from hardware"

When creating a new user, please ensure that the user name is unique.

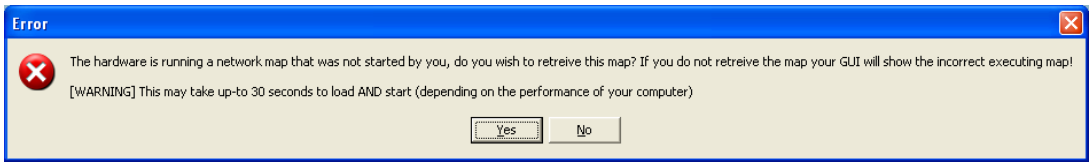
Multiuser GUI Warning

If this option is enabled, all GUI's that connect to the hardware **MUST** have this option enabled otherwise the general operation of map retrieval will fail and/or produce unpredictable results.

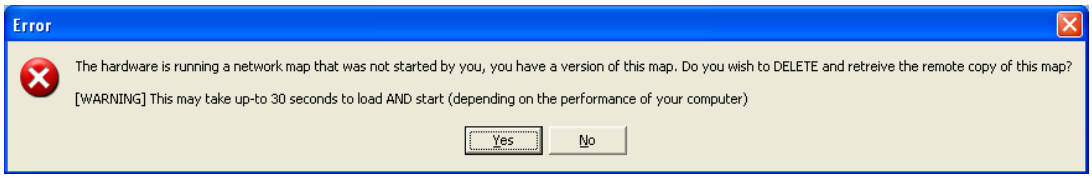
20.3.2. **Automatic retrieval**

When a network map is executed by a remote GUI, your local GUI will detect that the hardware is running a network map that it did not start. You will be asked whether you wish to update your GUI with the network map.

If the network map is new, and not available on your hardware you will see the following message:



If the network map exists on your GUI, you will need to confirm that you wish to delete and overwrite your local copy of the network map with the remote copy on the emulator.



20.3.3. **Further Information**

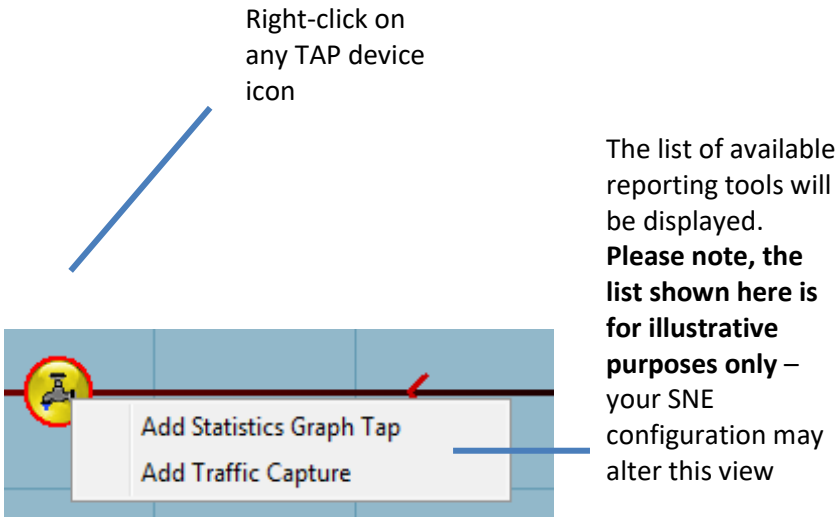
The retrieval system uses TCP port 5780 to communicate and this port must be unblocked and available for use by the GUI. The retrieval system will not transfer any auxiliary information such as time lines and is for use in the transferring of network maps only – any TAP device (Wireshark, statistical graphs, etc.) will not execute until any transferred map is launched.

21. Reporting – TAP Devices

The SNE Test Access Points (TAP) devices are automatically added in the Design pane when a connection is made between ports or impairments. The TAP device icon is shown below:

TAP devices provide the user with the ability to add reporting/analysis anywhere on an emulation map. The Network Emulator includes multiple reporting tools, which are described below.

The reporting functions which are available to you will be displayed when a right-click is performed on any TAP device on an emulation map, as shown below:



Please Note: The available TAP devices are dependent on your license key.

21.1. Reports

The SNE provides reporting through the ability to extract information from packets as they pass a Report TAP device and place them into a multi-page report (with headers, footers, etc.)

The reporting functionality is an additional extra on most installations, please contact us if you wish to license this feature.

Given the large nature of the reporting system, please see the dedicated report section.

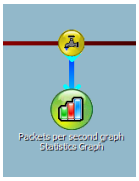
21.2. Statistical Graphs TAP

The Statistical graphs show real time information in the form of a graph. It uses metrics to extract certain information from the flow of packets. Your available metrics are as follows:

- Packet rate (packets passing the TAP point every second)
- Bandwidth

Adding a statistical graph to your emulation map

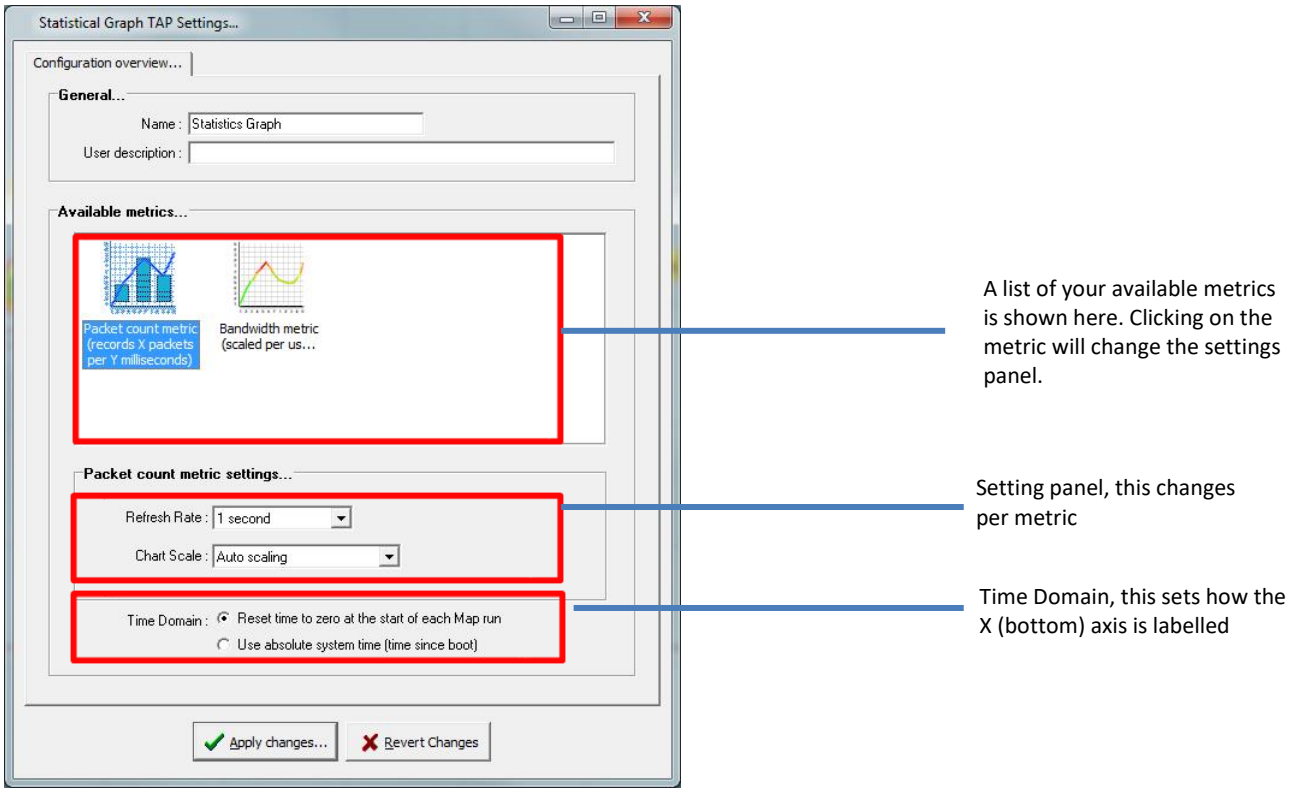
Right-click on the required TAP point, and select “Add Statistical Graph Tap”, the TAP device should appear below the TAP point as indicated in the following image:



The default stats graph added to the Design pane is the packets per second graph. This can be changed to the bandwidth graph by right-clicking on the green icon and selecting ‘Settings’.

Statistical graph settings window

The statistical graph settings window shows your available metrics. Select which type of metric you require by clicking on it.



Packets per second metric settings

Refresh Rate – This is the number of times per second the graph's details are updated.
Chart Scale – This allows you to provide a scale for the chart, auto scaling is recommended.

Bandwidth metric settings

Chart Scale – This allows you to set the scale of the bandwidth measurements

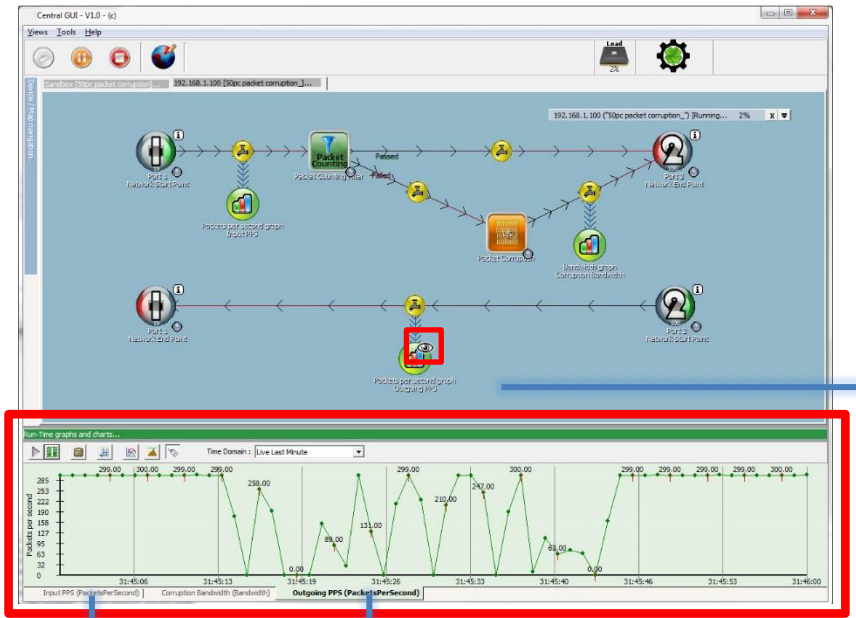
Include Framing – This option ensures that the bits before and after the physical packet (i.e. frame CRC, inter-packet spacing, preamble, etc.) are included. This allows viewing the correct full-wire rate.

Please Note: For low bandwidth applications it is possible to set the scale so low that it is not possible to see any values (values indicated as 0.00).

Running your emulation map

When your emulation map is run the Statistics Graph automatically appears at the bottom of the screen. If more than one statistics graph is available on your emulation map then a tab will be displayed that allows you to switch the view.

The following screen-shot shows an emulation map with 3 statistics graphs. It highlights the important features associated with the statistics graph feature.



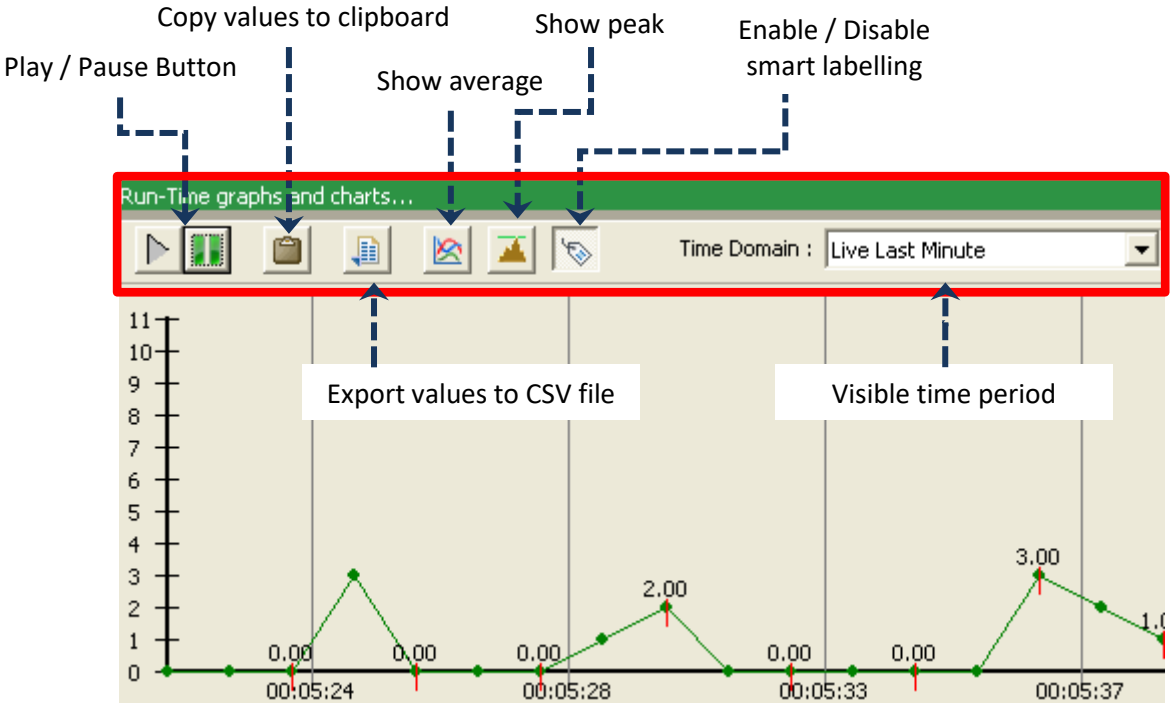
"Eye" Icon is used to show which statistics graph is being viewed.

Statistics Graph (see below for more information)

Tabs to control which statistics graph is being viewed. Current graph is in focus.

Statistics Graph Tools

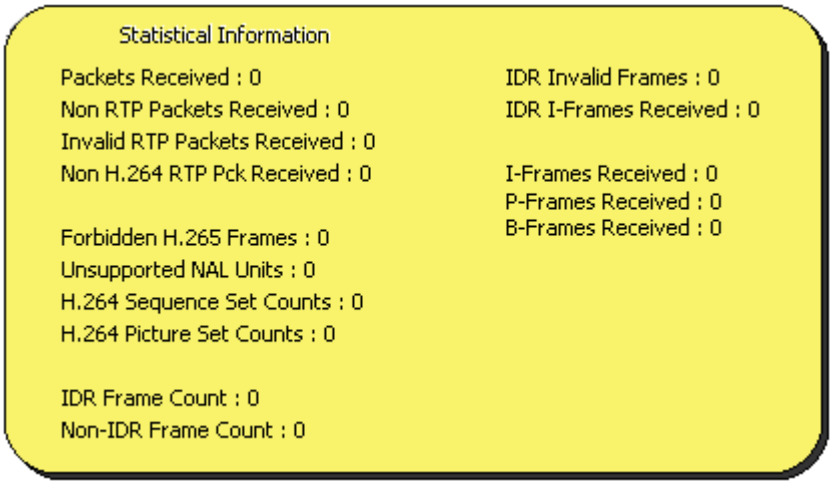
The Statistics Graph has a number of buttons and tools that allow you to obtain more information from your graphs. They are detailed below:



Please note that when exporting to a .csv file, the user defined filename must be suffixed with '.csv'.

21.3. H.264 Statistical TAP

This TAP Device provides detailed information on any H.264 (over RTP) streams that are passing the TAP device; the TAP will present the following information:



Statistics Information

Packets Received – The total number of packets received by this TAP device
Non-RTP Packets Received – Total number of non-RTP packets received
Invalid RTP Packets Received – Total number of RTP packets that are not version 2.0
Non H.264 RTP Packets Received – Number of RTP packets which do not contain H.264 frames, they could contain audio or other video formats

Forbidden H.264 Frames – Packet count of H.264 frames marked forbidden or “do not decode”
Unsupported NAL units – Total unsupported NAL units (i.e. non-video NAL units)
H.264 Sequence Set Counts – Total number of .265 “Sequence Set” NAL Units
H.264 Picture Set Counts – Total number of .265 “Picture Set” NAL Units

IDR Frame Count – Total number of Instantaneous Decoding Refresh (IDR) Frames
Non-IDR Frame Count – Total number of normal I,B or P Frames.

21.4. Root Cause Analysis – Wireshark

SNE provide the capability to capture Wireshark files (with extension .pcap) for detailed packet analysis and root cause analysis.

Wireshark is an open source tool employed by moderate/advanced technical users to analyse data packets sent over a network. The SNE provides the functionality to save captured traffic as Wireshark .PCAP files. These PCAP files can be loaded into Wireshark and provide advanced 'deep dive' analysis on packets that have been impaired by WAN conditions, thus providing the opportunity for root cause identification.

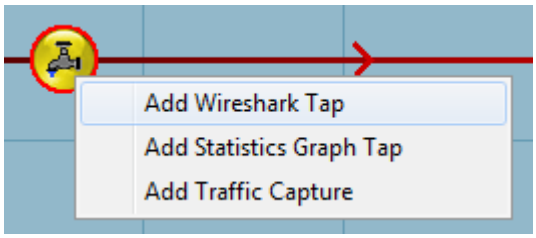
Wireshark is licensed under the GNU license agreement. We are not responsible for the supply, amendment, use or operation of the Wireshark application or its files. For information on how to install, use and analyse Wireshark file captures, please refer to http://www.wireshark.org for more information. Information on the GNU General Public License is available here: http://www.gnu.org/licenses/gpl.html

The current officially supported Wireshark version is V1.7+ (April 2015), however all versions of Wireshark should be compatible with the GUI.

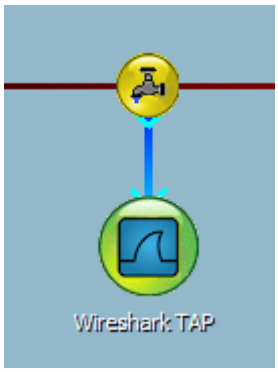
Using Wireshark

Please ensure you have downloaded the latest officially supported version of Wireshark to your Windows computer running the SNE GUI.

On the design pane, right-click any TAP device on an emulation map, and select 'Add Wireshark Tap', as shown below:



The Wireshark TAP device will be added, denoted by this icon:



When an emulation is run with a Wireshark TAP device on the link, the Wireshark application will automatically load and start to capture packets as they traverse the point on the link where the Wireshark was placed.

If at any time you close the live Wireshark capture, you may reopen the connection by clicking the green 'reopen' arrow present on the Wireshark TAP Device.

Please note: if you plan to capture traffic using a Wireshark device (as opposed to a traffic capture TAP device) it is recommended that the Wireshark programme is launched before commencing emulations. This significantly reduces the time required for the SNE to initiate the sending of traffic to the Wireshark capture file.

Performance note: There is a maximum throughput limit on the amount of traffic that can be received live from the network and sent to your Wireshark client. After this is exceeded you will be presented with a warning under the Wireshark client reading "Warning Overloaded". If this occurs use a 'traffic capture' TAP device instead to capture the packets at full-wire rate. Please see the following section for more information.

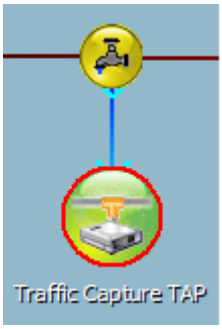
21.5. Traffic Capture and Replay

SNE provides the ability to capture impaired/unimpaired network traffic that traverses it for review in Wireshark. This differs from the Wireshark TAP device in that the captured traffic is saved to the SNE hardware for download at a later point.

SNE can capture and store up to 6GB of network traffic at any one time (the total capacity depends on the model being used). This storage (on the SNE hardware) is designed to be a temporary holding place for captured traffic, which should be subsequently saved onto local hard drives. If captured traffic files are not downloaded to a separate hard drive, the ability to capture traffic will be impaired once all available SNE memory is used by existing capture files.

Capturing network traffic

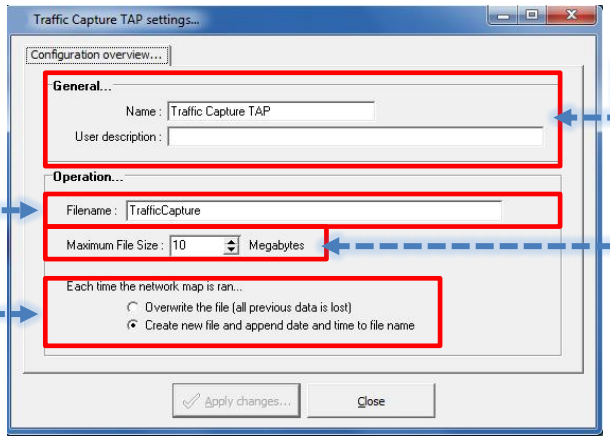
To capture traffic, please right-click on any TAP point on the Design pane and select 'Add Traffic Capture'. This will add a traffic capture tap device to your emulation map, as shown below:



Right-click on the traffic capture object, and choose 'Settings'.

This is the title that will identify the file for replay purposes

If you do not specify a new filename for each recording, decide if the previous recording with the same filename should be overwritten



Enter descriptive details if required

Set the file's maximum capture size

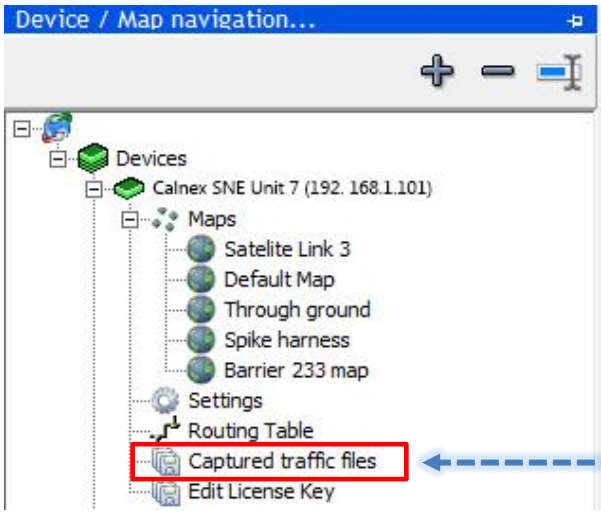
Multiple traffic capturing

The SNE allows users to add multiple 'traffic capture' TAP points to an emulation map, and therefore record traffic both bi-directionally and before or after impairments. However, it is important to note that when using more than one traffic capture device on a single emulation map, each traffic capture device must be assigned a unique filename.

This allows the system to differentiate between the traffic capture files – if the default filename is used, or all files named the same, only one file will be captured. The GUI may also report an on-screen error – if this occurs, edit the names of the traffic capture files to make them unique, and restart the emulation.

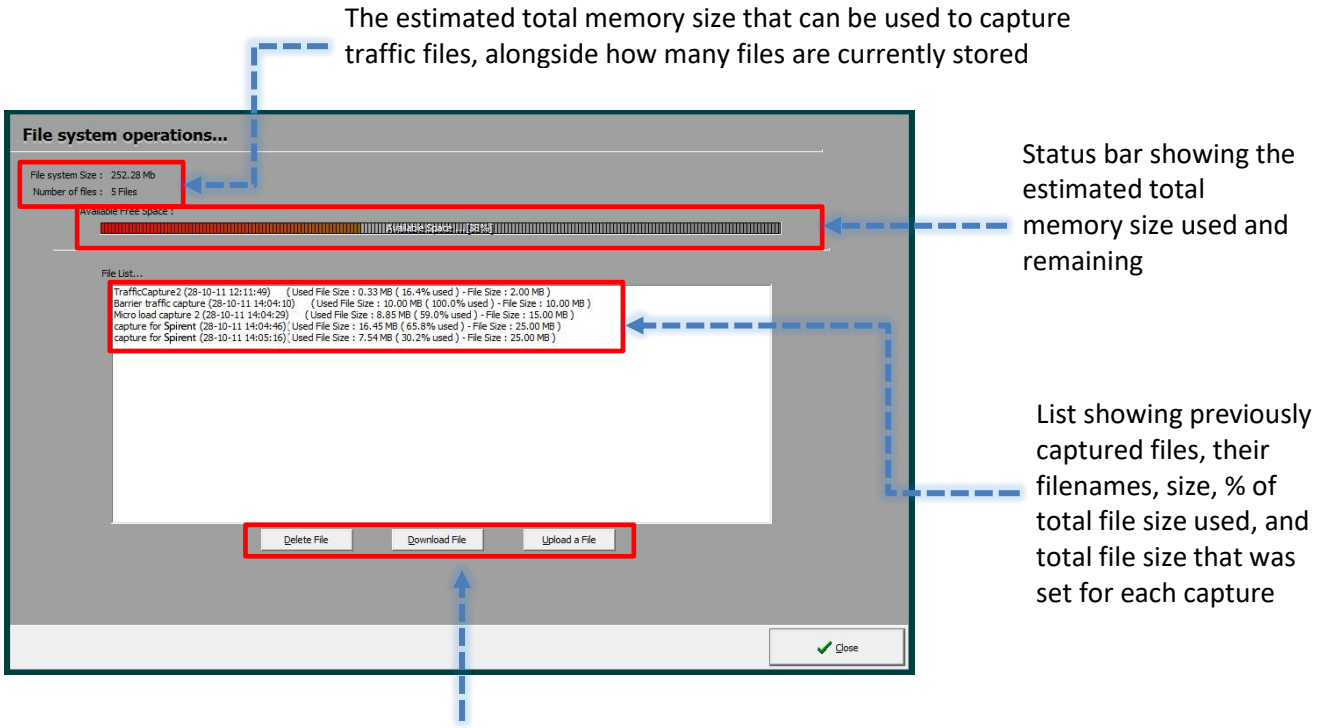
Stored traffic

Captured traffic files are stored in memory on the SNE hardware and accessed through the 'captured traffic files' option in the map/device navigation bar. Each traffic capture file is specific to the SNE hardware on which it was captured. You can access stored files as shown below:



Access previously captured files by clicking on this link in the map/device navigation bar. If you have more than one SNE hardware device, ensure you are selecting the link under the correct hardware.

The following screen will be displayed – please note that the files shown below are for illustrative purposes only (upon first use, there will be no previously captured traffic files).



- **Delete file:** the selected file will be removed permanently from the system
- **Download file:** downloads the selected file to the location specified on a local hard drive, for analysis or long-term storage
- **Upload a file:** allows previously captured files that have been downloaded to a hard drive to be uploaded and subsequently replayed (if this feature has been licensed in your version of SNE).

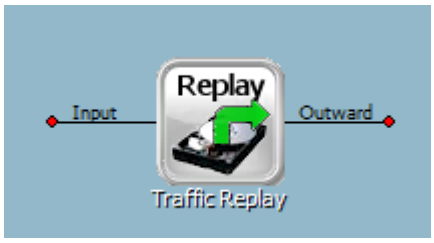
Downloaded files are stored with .pcap file extensions, which allows them to be opened and analysed via Wireshark. Users must download and install Wireshark in order to analyse .pcap files produced by SNE.

Replaying stored traffic

The user can replay stored traffic by dragging and dropping the following icon onto the main design pane (from the network toolbar):


Replay captured traffic

This will display the following icon:



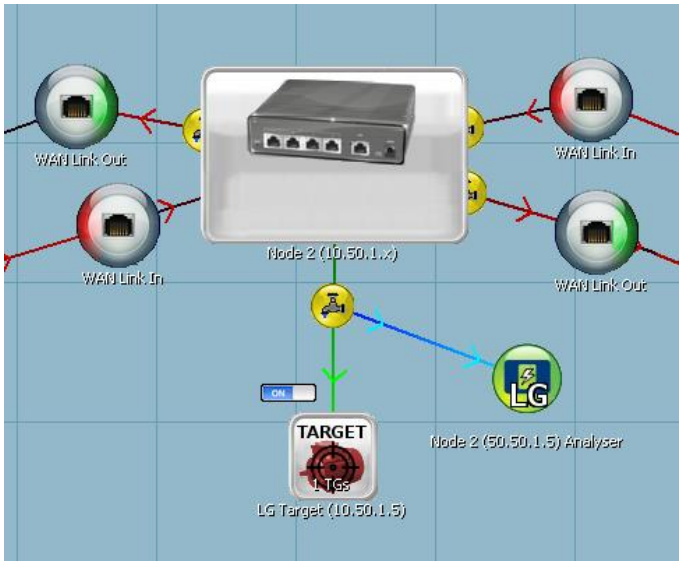
The user should right-click to open the settings of this tool and select the file to be replayed. Once the emulation is started, the traffic replay tool will send the captured packets across the selected link and allow the user to view if resolutions to application performance issues (for example) have been resolved under the exact same network conditions as when they were identified.

The traffic replay tool can optionally loop the recorded traffic.

21.6. Load Generator Analyser

This TAP Device provides detailed information on any load generated streams that are passing the TAP device. This tool is of particular interest when you are using virtual routing as it allows you to see any traffic that is arriving at the LG Target (An LG Target is a simulated “computer” on which traffic can be received).

The following screen-shot shows an example of how the Load Generator Analyser would be used in this situation.



When a network map is executed each LG Analyser will open an information panel at the bottom of the GUI, you may view the stream received along with packets rates and errors.

22. Reports

23.1 Introduction

The SNE has full reporting facilities; allowing you to design and run reports at run-time (when a map is executing) or at the end of an emulation run (when the map is stopped).

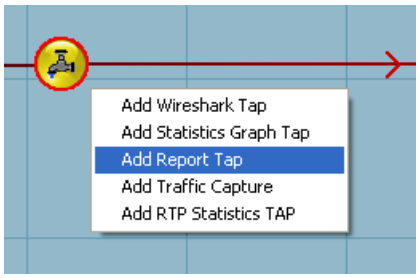
The SNE accomplishes this task by using “stream analysers” that inspect packets as they travel past a report Test Access Point (TAP). These stream analysers extract information about the packets and send this to the GUI every second. The SNE ships with two basic “stream analysers”; bandwidth and packet count.

Please Note: Reporting is a **licensed option**, if you require reporting please contact us.

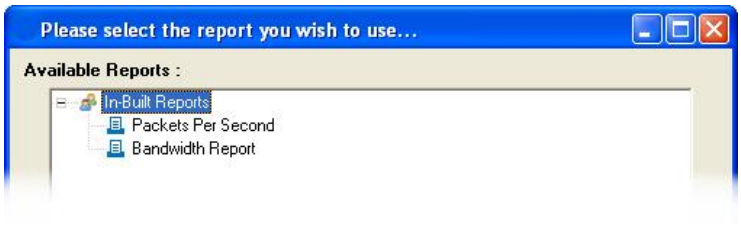
23.2 Adding an Existing Report

The unit ships with two built-in reports; bandwidth and packet counting. In this example we are going to add the “Bandwidth Report”.

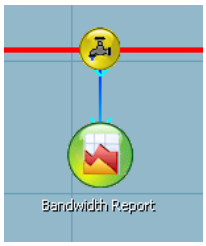
Right-click on the TAP device and select “Add Report Tap” as shown below:



After you have added the Report TAP you will be presented immediately with a selection window to show the available reports. Please select the “Bandwidth Report”.



After this the report TAP will be populated as shown:

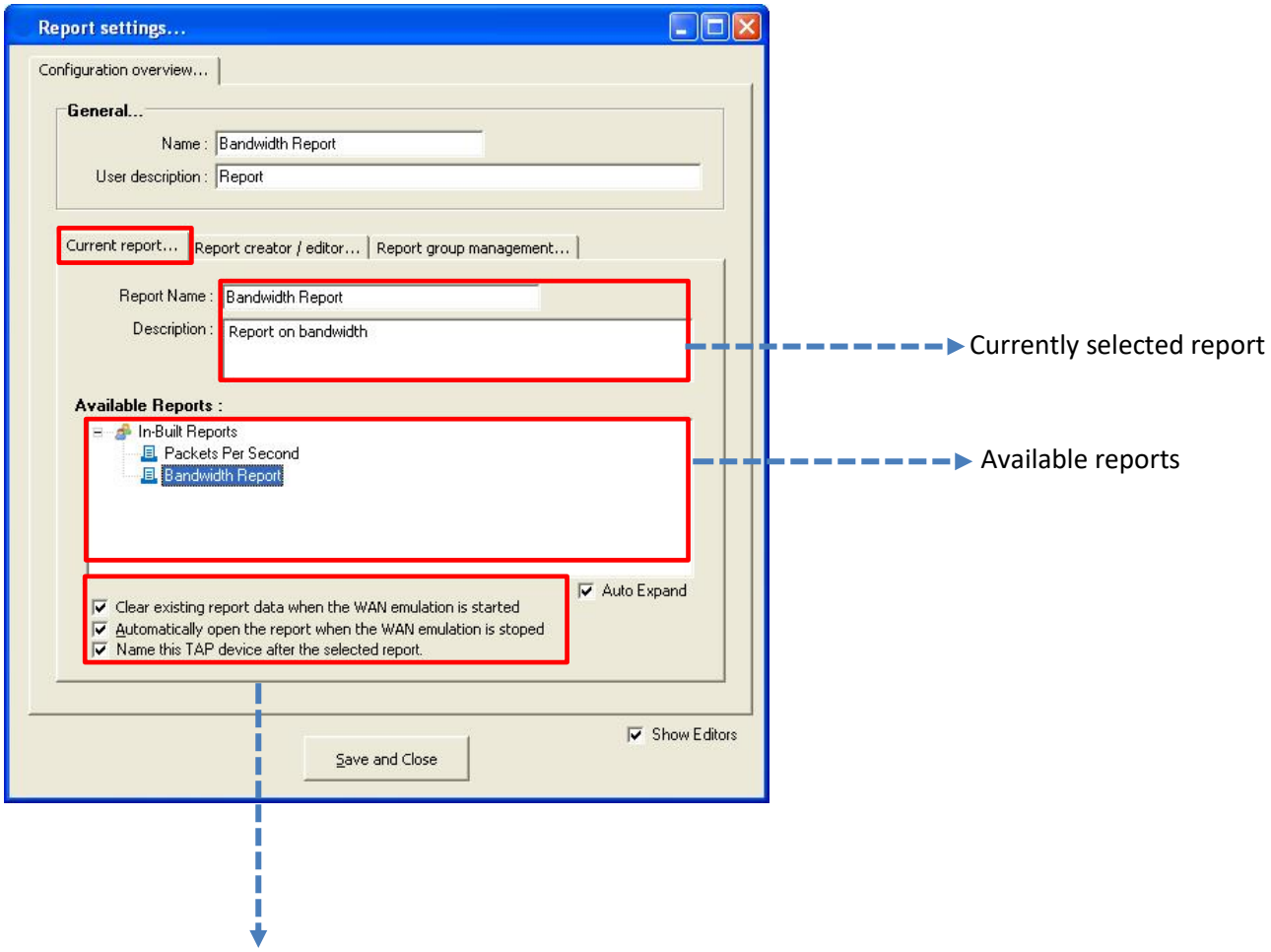


23.2.1 Report Settings

To alter the report settings, right-click on the Report TAP and select “Settings”.

23.2.3 Current Report - Settings

This commonly used panel allows you to alter the initially selected report, along with selecting some run-time options for the report generation.



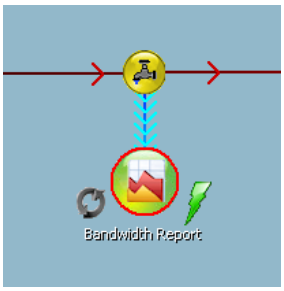
Clear Existing Report Data – This option causes the reports to clear any existing data when an emulation map is executed, you can disable this to record historical information over multiple emulation runs.

Automatically open the report – When the emulator is stopped the report is automatically disabled as an “end of emulation run” report.

Name this tap devices after the selected report – This visualisation option causes the report TAP device name to be set to the report’s name allowing for easy recognition of the selected report when the settings are closed.

23.2.4 Running a report

When the emulation or network map is run; you will notice the report TAP device has two icons beside the report TAP. Note: If you do not see these icons then there may be no packets passing the report.



Execute Report

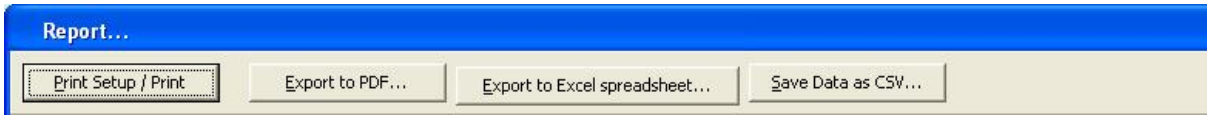
Execute report immediately, clicking this icon causes the report to be shown with whatever information has been received from the emulator (or more precisely the stream analysers).

Clear report

Clicking this icon will clear all previously received information from the report; this is handy for ensuring that the report contains only information you require from a start point.

23.2.5 Saving report information

After a report is executed you are given a number of options at the top of the report window:



Print setup / print – This option allows you to print the report
Export to PDF – This option allows the exporting of the report to PDF
Export to Excel – Generates a Microsoft Excel®.XLS file (**NOTE**: You MUST have Excel installed)
Save Data as CSV – Exports the report data as Comma Separated Values (CSV) file.

23. RESTful Remote Control API

23.1. Introduction

SNE units can be controlled using a RESTful API, allowing for automation of a wide range of tests. A list of available RESTful API commands, as well as an interface to try them out, can be accessed by navigating to http://*<ip_address>*/swagger in a web browser, where *<ip_address>* is the IP address of your SNE. See also the RESTful Remote Control API Manual for further information.

23.1.1. Operation Overview

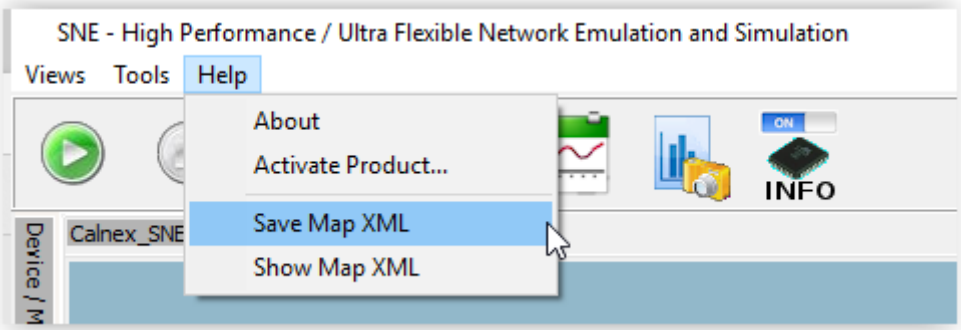
As the SNE hardware does not persist or store any network maps, **the RESTful API requires that you upload an XML version of your network map to the emulator** – this operation automatically happens when you are using the GUI.

The network map must be uploaded via the RESTful API before any changes to impairments can be made.

It is important to remember that you **may only change the settings of any impairments contained within the network map** you uploaded. For example, if your network map contains a delay impairment named "ADSLDelay" then you can modify the "delay" parameter of that impairment. If the network map does not contain any delay impairment it is not possible to add or modify the delay of any link within the network map.

23.2. Saving XML Network Maps

To save an XML version of your network map for use in the RESTful API, use the "Save Map XML" option under the "Help" menu in the GUI.

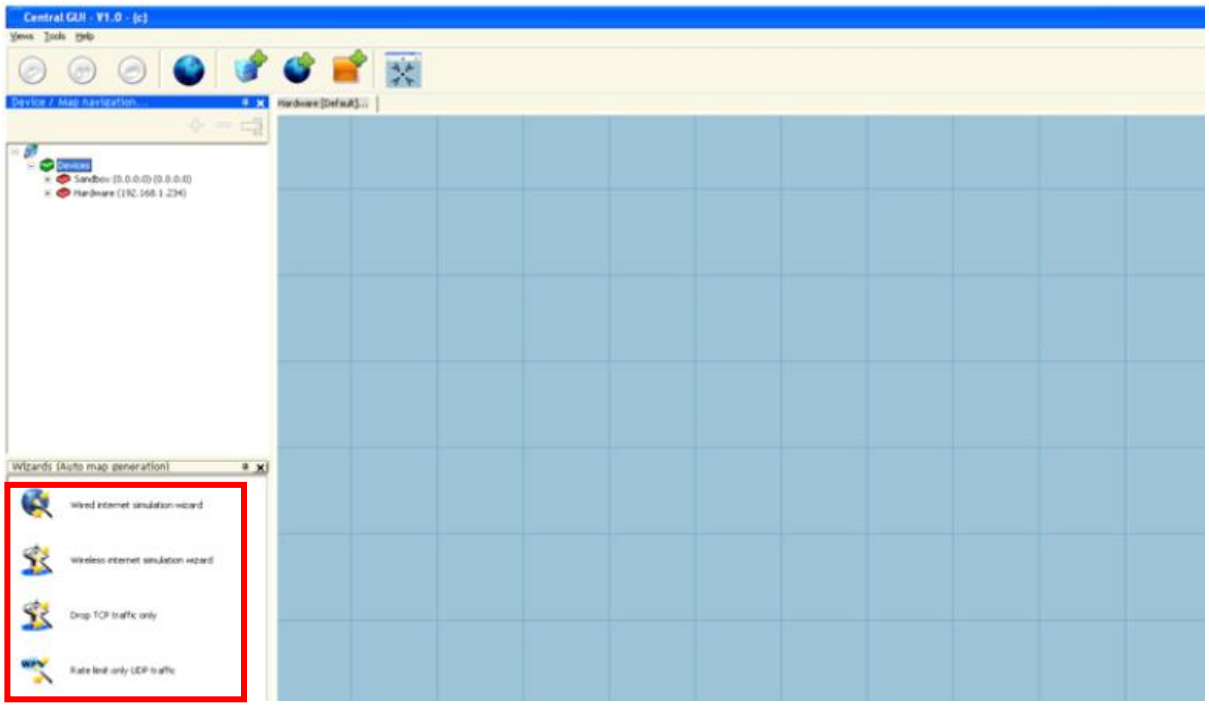


You must uniquely name any impairment in your network map that you wish to alter.

24. Wizards

The SNE is intentionally easy to set up and use. To that end, it provides wizards that can pre-populate network configurations for users without the need to draw the emulation maps from a blank canvas. These can either be supplied as standard or tailored to individual customer requirements.

These wizards are located on the left of the design pane, shown below:

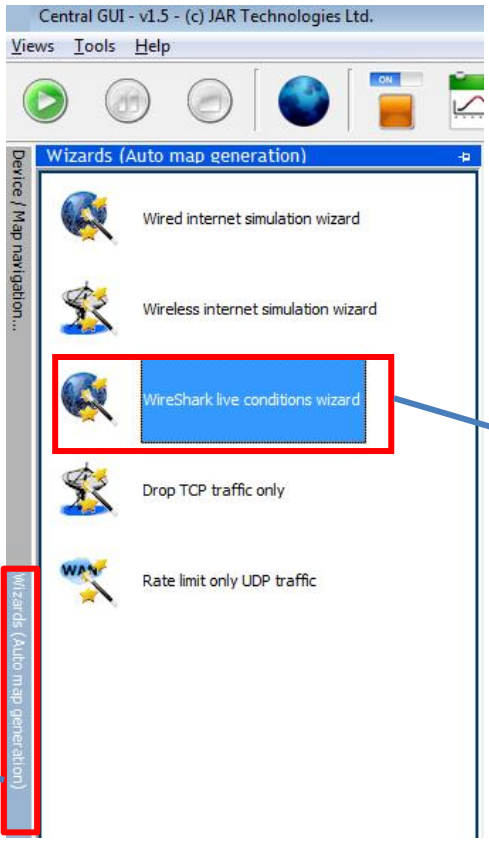


Common wizards provided include wireless, satellite and filtering map creation wizards, which guide the user through relevant questions and selections. These are then confirmed and the desired emulation map is generated.

25. Generating maps from PCAP files

SNE provides the capability to pre-populate an emulation with the conditions found on live networks, even if those conditions are unknown to the user. Traffic can be recorded (either using the emulator hardware or from a remote location), imported into the user interface and used to auto-generate emulations based on the impairments found on that network.

This facility is provided via the 'Wireshark Live Conditions wizard', as shown below:



1) Hover over the Wizards toolbar to extend this window onto screen

2) Select the 'Wireshark Live Conditions' wizard

Capturing live network conditions

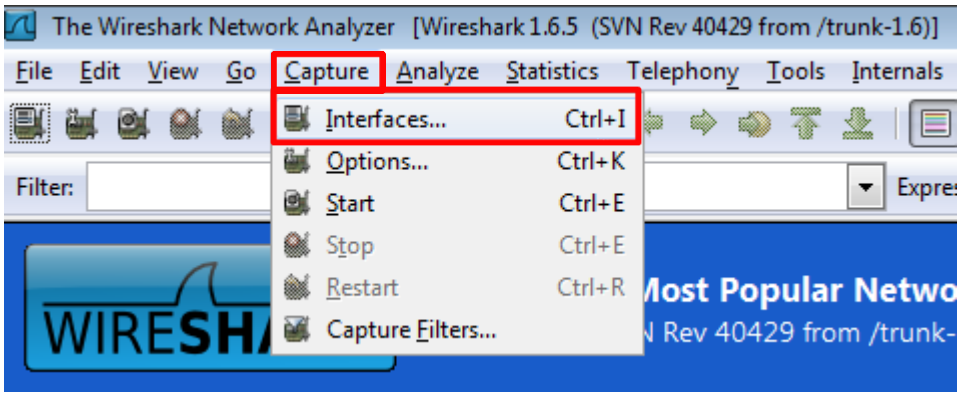
In order to capture live network conditions, SNE uses ping tests to assess the following:

- Latency
- Jitter
- Packet loss

(in both directions on the link.)
The ping test should remotely target the machine(s) on the far end of the link to be emulated. Wireshark must be capturing during this time, in order for the necessary measurements to be recorded.

In order to capture live traffic, please open Wireshark and ensure you are running it as 'administrator'. This can be achieved by right-clicking on the Wireshark application icon and selecting 'Run as Administrator').

Once Wireshark has opened, please select 'Capture' on the top menu, and select 'Interfaces' as shown below:



Select the network interface that is to be used to send/receive the ping messages, and then press 'start'.

The Wireshark application will now be capturing all traffic to and from that interface, so the user should now commence their ping test using a terminal window in Linux or a DOS dialog box in Windows. Under Windows, we recommend suffixing '-t' at the end of your 'ping <ip address>' command and allowing the ping to run for several minutes so that accurate readings can be taken and spikes/troughs do not skew the data.

Once the recording is complete, move/save the Wireshark file to the device running the SNE GUI (be sure to save it in **tcpdump** format; this can be selected from the Save As screen in Wireshark). Locate and run the 'Wireshark live conditions' wizard on this device and follow the onscreen instructions. An emulation map will be generated with the conditions found on the live network.

SNE is powered by technology from Calnex Solutions.

Contact Us

For more information, call your Spirent sales representative or visit us on the Web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defence
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com