LANforge GUI Users Guide

Table of Contents

Overview

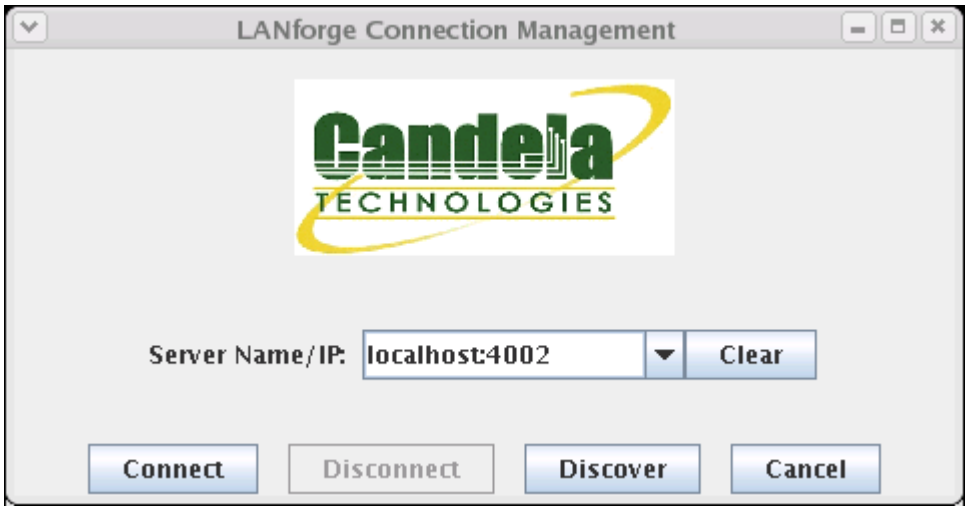
The LANforge GUI is a Graphical management interface to the LANforge system. The GUI connects to the LANforge manager process, which automatically discovers the LANforge Data Generators (also called 'Resources') on it's management network. Because the connection to the server is a standard TCP/IP interface, the GUI can access the server remotely, even over a low bandwidth connection. The GUI has extensive 'tooltip' support, so if you are unsure of what a particular field or option box does, hold the mouse cursor over it for about 3 seconds and you should see a small description of that field.

You can press the Help button on each screen and it will give you a help page relating to that screen using your default browser.

For a some ideas on how to test specific architectures and protocols, see the:
LANforge Overview

1. Getting Started & Logging In

After installing the LANforge GUI, you are ready to begin. First, start up the LANforge GUI. It should pop up two windows, one being a login screen that looks something like:

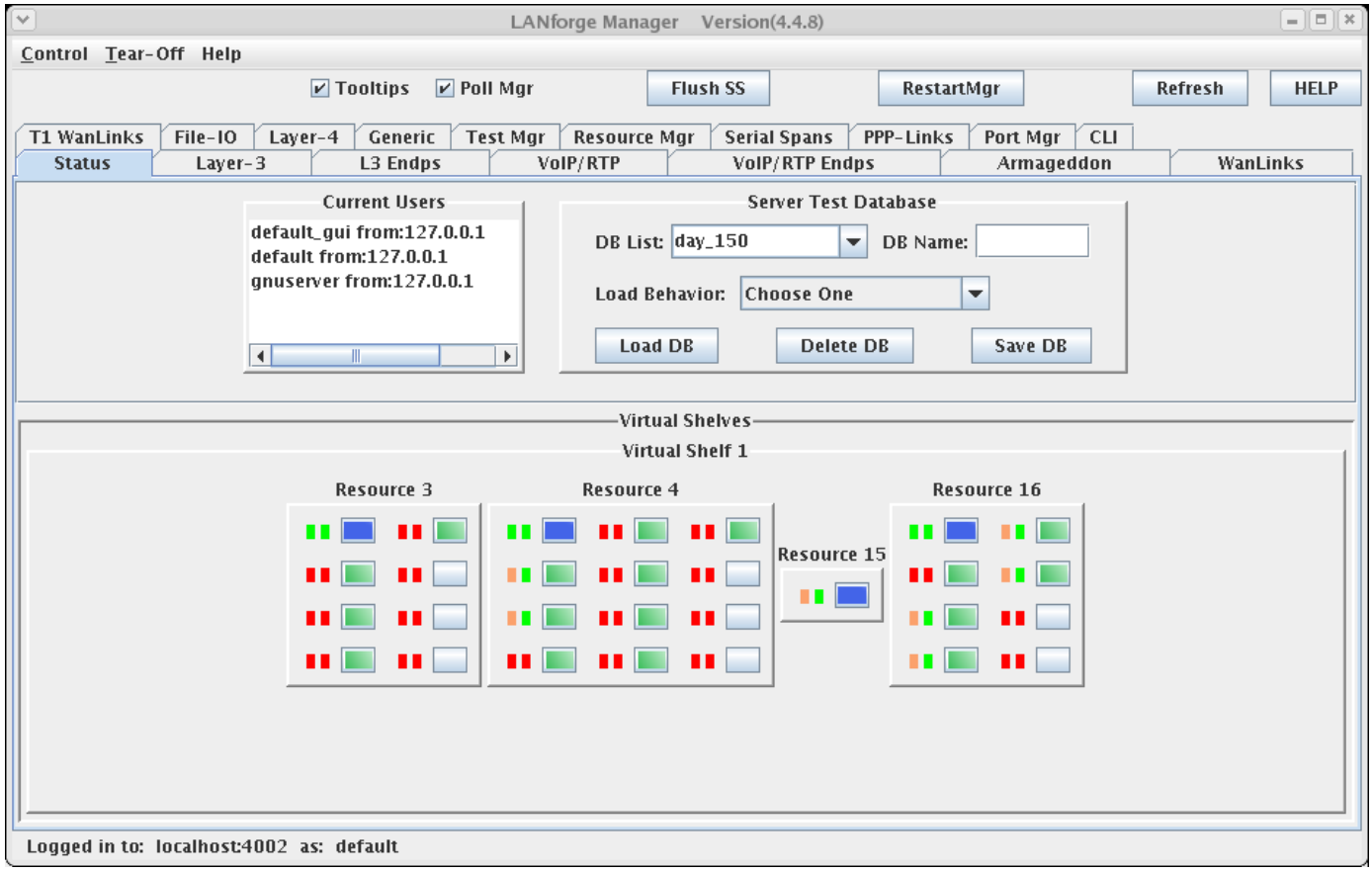


Enter the name or IP address of the LANforge server that you wish to connect to. If you are running the GUI on the same machine as the LANforge server, then you can enter 'localhost' here. The other important field is the port that the server is running on. The default port is 4002, but could be different depending on how the LANforge server was installed. You can also click the Discover button to have the GUI discover other LANforge systems on the local subnet. After you have entered the correct information, press the Connect button, and the GUI will attempt to connect to the server. If the server is re-started, or connection from the GUI to the server is lost for any other reason, the GUI will continue to try to reconnect to the server every 5 seconds.

The last 20 servers that you logged into will be placed into the drop-down box for ease of use when re-connecting. If you ever want to re-initialize the list, remove the lfcnf.txt file that is in the LANforge GUI installation directory and re-start the GUI.

2. Status Pane

After you have connected to the server, the splash screen will disappear and you will be looking at the status pane:



This pane holds several small management panes and the bottom part will display a high level view of every virtual shelf, LANforge Data Generator, and port on the generators.

- The first panel shows the "Current Users" who are logged into the LANforge Server. Because the LANforge system can be used by multiple simultaneous users, this panel will help you coordinate and understand the current usage of the LANforge system. Some of the 'users' are other LANforge processes.

- The "Server Test Database" panel displays the current list of test databases that may be found on the LANforge Server. Using this panel, you can load, save, and delete test databases. When loading, you are given the option of overwriting the current configuration with the database you are loading, or you can just append the new database to the existing configuration. Note that if you append databases that conflict, (for example, they each have a cross-connect named "cx1"), then the last one wins, and it may look a little messy. The database files are stored in plain text, and are human readable. It is possible, though not necessarily advisable, for you to edit the databases by hand, or auto-generate them with a custom script. To find the actual database files, look in the `/home/lanforge/DB/` directory.

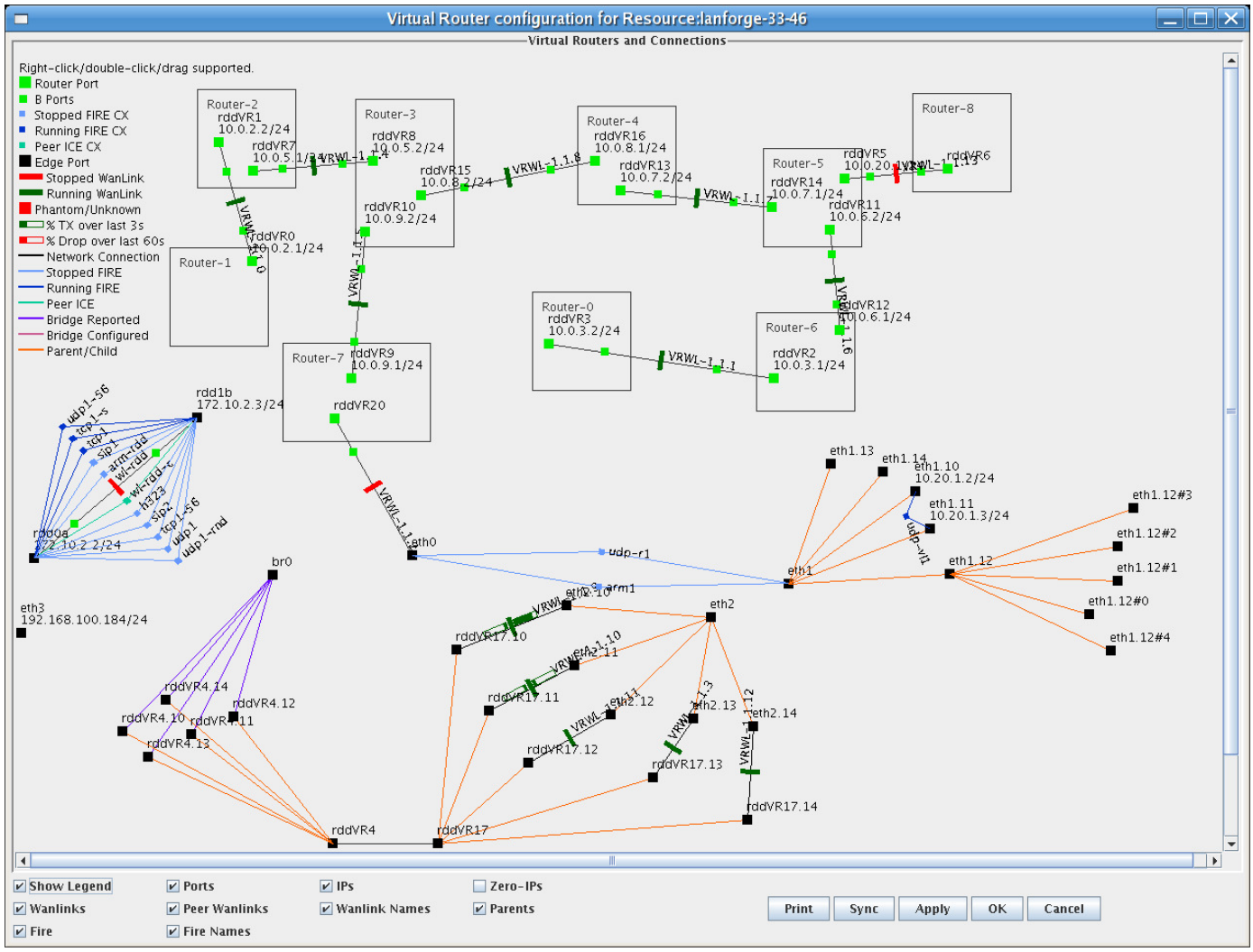
- The bottom of the Status panel lists each of the virtual shelves and LANforge data generating units (Resources). Each unit will have a certain number of 'ports' on it. The green ports are the data generating ports, yellow ports are configured in the database, but non-existent (or not yet discovered) on the real hardware, red ones are configured to be ignored by the client, and the blue ports are the management ports. The layout of the ports is specified by a config file on each of the data-generating units, and should have been configured correctly at installation time. If you click on the ports, you will be taken the the Ports panel which has much more detailed information.

  The two small colored boxes to the left of each 'port' signify the link status. The left box shows the speed: Red means no link, yellow is 10Mbps, green is 100Mbps, and orange is 1Gbps. The middle box displays green for full duplex, yellow for half duplex, and red for no link at all. The tool-tip for each port will be updated to show the correct speed as well.

  The virtual shelves are just a method of grouping the data generating units into logical collections. The membership of a data-generating unit to a shelf is specified during the configuration of the unit.

3. Netsmith: Virtual Network Configurator

With release 5.0.1 and higher, LANforge includes the Netsmith graphical configurator for virtual routers, LANforge-FIRE, and LANforge-ICE testing scenarios. Please be aware that the Virtual Router functionality only works when the LANforge resource servers are running on Linux. The updated iputils program and the Candela kernel (or a kernel with the Candela patch applied) is also required. If you purchase one of the appliances, this will all come pre-installed. If you are installing the software on your own system, please read the install guide(s) carefully.



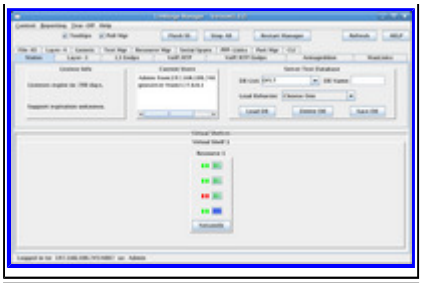
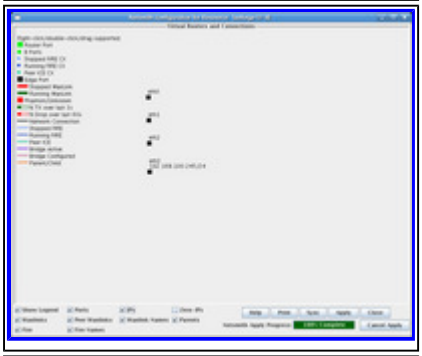
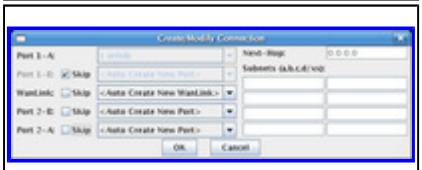
When the Netsmith tool is first opened, it will auto-create as much as possible based on the current system configuration and resources. The positioning of the objects will most likely need to be changed. For most objects, just click-and-drag them to the new location using the mouse. Some objects, such as FIRE cross-connect representations are not independently draggable, but you can drag the port endpoints to reposition the FIRE CXs.

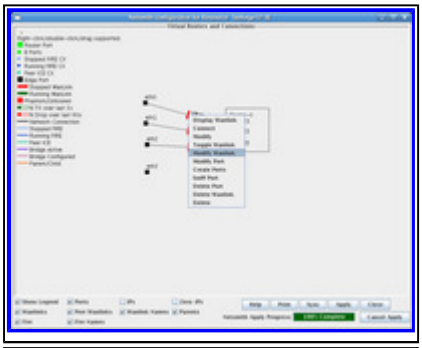
You can left-click and drag to create a selection box, and then drag or modify all of the objects inside or intersecting the box at once.

In general, you can click-and drag to move, double-click to modify, and right-click on objects to get a menu of specific tasks for each object or group of objects.

Here is an example of how to create a simple routed network emulation using three physical ports and one virtual router. This will emulate a central location with a 10Mbps network connection, and 2 remote sites with 1.54Mbps T1 connections, all connected through a routed network. (Some of these steps may require LANforge release 5.0.2 as they depend on some bug fixes introduced in the 5.0.2 release.)

Step	Screenshot

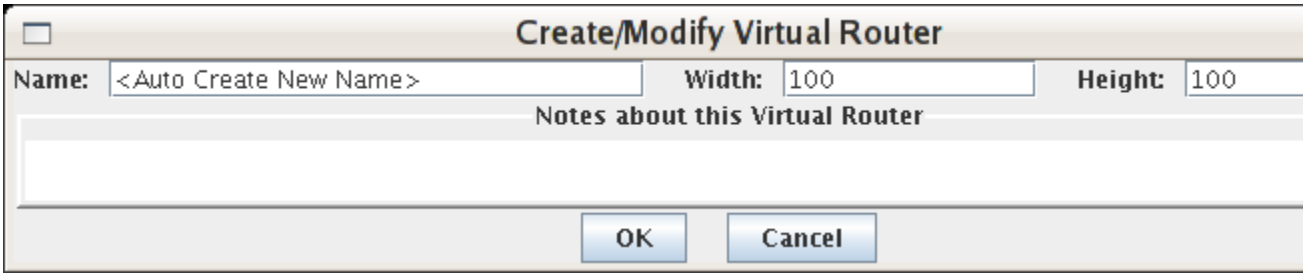
1. Go to the Status panel in the LANforge-GUI and open the Netsmith tool.	
2. We will be using 3 ethernet interfaces for use: eth0, eth1, eth2 in this example.	
3. Double-click eth0 to modify it's connection. Un-skip WanLink, Port 2-B and Port 2-A. Leave the WanLink and port settings as they are to automatically create new entities as needed. When done, click 'OK' to save the changes.	
4. Double-click eth1 and eth2 and follow the same step as above.	
5. Right-click in empty space and choose New Router. Set the name if desired and click OK.	
6. Drag the rddVRXX sides of the connections into the newly created virtual router.	
7. Click 'Apply' at the bottom-right of the Netsmith windows. This will actually create the new ports and WanLinks. You should see the newly created objects go from red squares to green and black boxes. The WanLink will be a red rectangle, and will go green when you start it (below).	

	
8. Right-click and modify the port for each of the rddVRXX interfaces in the virtual router, adding appropriate IP and MASK.	
9. If this is to be part of a larger routed network, then you can double-click the port(s) in the virtual router and set the Next-Hop and up to 8 subnets that will be using this next top. Please note that 0.0.0.0/0 is a valid subnet, and simply means 'ANY'. This is one way to set the default gateway for all unknown traffic. Press OK when done modifying the Virtual Router.	
10. When all of the ports in the Virtual Router have appropriate IPs, and the connection has the proper next-hops and subnets, press Apply to flush the changes to the LANforge server. This will create the proper routing tables.	
11. Modify the WanLinks (red or green rectangles) by right-clicking them. Set the bandwidth to 10000000 (10Mbps) on one, and 1.54Mbps on the other two. Set latency and other changes as required.	
12. Start the WanLink with right-click and Toggle WanLink.	
13. Connect your network equipment to ports	

eth0, eth1, and eth2. For each port, the default gateway will be the IP address of the corresponding rddVRXX port in the virtual router.	
14. At this point, your network equipment should be able to ping through LANforge and you should see the latency that you configured in the WanLinks.	

Virtual Routers

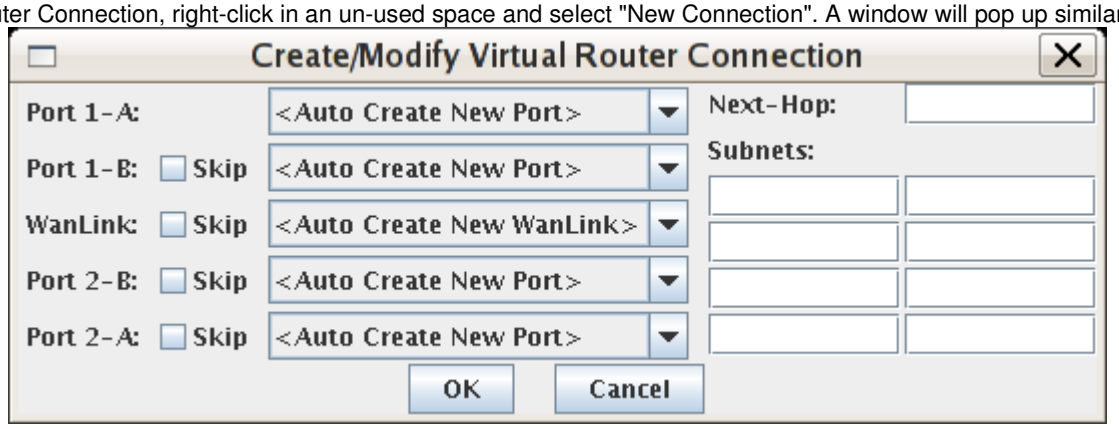
To create a new Virtual Router, right-click in an un-used space and select "New Router". A window will pop up similar to this:



After creating a virtual router, you can drag existing interfaces into it and also create new virtual devices and associate them with the virtual router. In order to be accessible to outside objects, the Virtual Router must either contain an interface (Port) that connects to the outside world, to connect to another Virtual Router that eventually connects to the outside world.

Router Connections

Router Connections are used to connect routers to each other, and to connect routers to the out-side world. To create a new Router Connection, right-click in an un-used space and select "New Connection". A window will pop up similar to this:



You can choose up to 4 ports and one WanLink to be part of this connection. What you choose and how many are active changes the behaviour significantly. In the example below, it is assumed that Port-1 will be the 'outside' port, but Router Connections do not have an inherent direction...it all depends on how you configure it.

- **Port 1-A** will be the name of the local port. If you want this connection to connect to the outside world, use a real device such as eth1 or perhaps an 802.1Q VLAN device for this value. If you want to use this connection to connect two virtual routers, then choose the default "Auto Create New Port" option and a redirect-device will be created for you when you apply the changes.
- **Port 1-A** will be the name of the local B port. If you want this connection to connect to the outside world, this should be skipped. If you want to use this connection to connect two virtual routers with a WanLink (Network Impairment) included, then choose the default "Auto Create New Port" option and a redirect-device paired with Port 1-A will be created for you when you apply the changes.
- **WanLink** will be the name of the WanLink (LANforge-ICE) that connects the local ports to the remote ports. If you skip one of the B ports, then the WanLink will connect to the A port. If you skip both B ports, the WanLink will connect the two A ports directly. If both B ports are active, the WanLink will connect the two B ports (this assumes the B ports are Redirect devices associated with the A ports, so that logically, the A ports are connected to each other through the B ports and WanLink bridge.) If you want to connect two routers without using a WanLink (to save WanLink licenses, for instance), then you can skip both B ports and the WanLink. This last case assumes that the A ports are (or will be) a pair of Redirect devices.
- **Port 2-B** will be the name of the remote B port. If you want the remote side of the connection to connect to the outside world, skip this port. Otherwise, choose the default "Auto Create New Port" option and a redirect-device

paired with Port 2-A will be created for you when you apply the changes.

- **Port 2-A** will be the name of the remote A port. If you want the remote side of the connection to connect to the outside world, this should be a real interface, such as eth2 or perhaps an 802.1Q VLAN device. If you want to use this connection to connect two virtual routers, then choose the default "Auto Create New Port" option and a redirect-device paired with Port 2-B will be created for you when you apply the changes. If you want to associate a port to a virtual router, without any WanLink emulation, you can skip Port 2-A and have a stand-alone port that can be dragged into a router. This is the default case newly discovered non-redirect device interfaces.
- **Next Hop** is the next router gateway to be used by packets leaving on a router-connection. This can only be specified for connection endpoints not associated with a virtual router. If a port is configured with a Default Gateway, that may be used as the next-hop instead (whichever is found first will be used).
- **Up to 8 additional Subnets** can also be specified to lie beyond this connection. This will influence the routing tables for the virtual routers, and should coorespond to the subnets in the user's network-under-test. The **Next Hop** gateway will be used for packets destined for these subnets. Please note that 0.0.0.0/0 is a valid subnet, and efectively means the default gateway for the entire cluster of virtual routers.

Right-Click Menus

Most objects have right-click menus associated with them to perform various actions. You cannot click on the connecting lines or the 'B' ports at this time.

- **Connection Endpoints** support Display Wanlink, Connect (to a previously selected endpoint), Modify, Toggle Wanlink (on/off), Modify Wanlink, Modify Port, Create Ports (create vlans on the selected interface), Sniff Port (with Wireshark protocol analyzer), Delete Port, Delete WanLink, Delete (Router Connection). Please note that if you delete a connection endpoint, any previously auto-created WanLinks or virtual devices associated with that connection will also be deleted when you apply the changes. **Deleting ports and WanLinks take affect immediately, so be careful!**
- **Virtual Routers** support New Connection, Modify, Show Routing Table (as is currently configured in the kernel), and Delete. Deleting a Virtual Router will not delete any Router Connections.
- **Fire CXs** (various traffic generating LANforge cross-connects) cannot be dragged, but they do support right-click actions: Display, Toggle (on/off), Start, Stop, Modify and Delete. **WARNING: There is no confirmation for these actions, including 'Delete', and they are applied immediately upon choosing the action.**
- **Peer ICE CXs** are WanLinks that are associated with a particular connection but which are not running. If you have 3 WanLinks between the same two ports, only one can be running at a time: One will be shown as the central connection, and the other two will be shown as Peer ICE CXs. The Peer ICE CXs support these right-click actions: Switch (to running this WanLink), Modify, and Delete. **WARNING: There is no confirmation for these actions, including 'Delete', and they are applied immediately upon choosing the action.**
- **A Selection Box** can be created by clicking on an empty space and dragging and releasing the mouse. One can then drag the selection box and everything it includes to a new location. It also supports some group actions, including: Display, Toggle, Start, Stop, Modify and Delete. Not all objects contained in the box will support every option, and in that case, they will be silently ignored with no ill affect. **WARNING: There is no confirmation for these actions and they are applied immediately upon choosing the action.**

Visual Display

The Netsmith window provides a real-time view of WanLinks and other LANforge entities. A legend for each type of entity is show in the top-left of the Netsmith window. Any objects drawn as a red square are not currently found in the LANforge system, even though the Netsmith has been configured such that they (should) exist. This can happen if interfaces or WanLinks were removed after Netsmith had discovered them, or if new WanLinks or connections have been created in Netsmith, but the changes have not been Applied yet. If these should really be deleted, just right-click and delete the offending objects and Apply the changes.

- **For WanLinks**, a vertical green bar represents it is running, and a vertical red bar indicates it is stopped. A horizontal traffic-throughput graph is also drawn if there is activity over the last 3 seconds through the WanLink. The green graph indicates the percentage of network utilization flowing **towards** the interface it faces. The red graph reports the percentage of dropped packets v/s transmitted packets over the last 1 minute.
- **LANforge-FIRE** connections are shown associated with their endpoint interfaces. They are drawn light-blue if stopped, and darker blue if running.
- **Port Relationships** ports will have orange connections to their parent object (for instance, an 802.1Q VLANs parent will be the the ethernet or other lower-level network device.) Bridge devices will be connected to the interfaces contained in the bridge device by dark blue lines. If the bridge is configured to own a device, but it is not currently configured as such by the kernel, then that line will be a purplish color. The purple color indicates not all may be as desired, so you may need to modify or reset the bridge device.

Drawing Options

There are several checkboxes at the bottom left of the Netsmith window. These can be used to enable and disable the drawing of various entities to suit the user's preferred level of detail. Changing these flags does not affect the actual configuration of LANforge in any way.

Netsmith Buttons

There are several buttons at the bottom-right of the Netsmith window.

- **Help** shows this help information in a web browser.
- **Print** will print the entire diagram, forcing it to fit onto a single page. One might choose to print it to a PDF printer and expand the PDF for very high-resolution viewing of a complex network configuration.

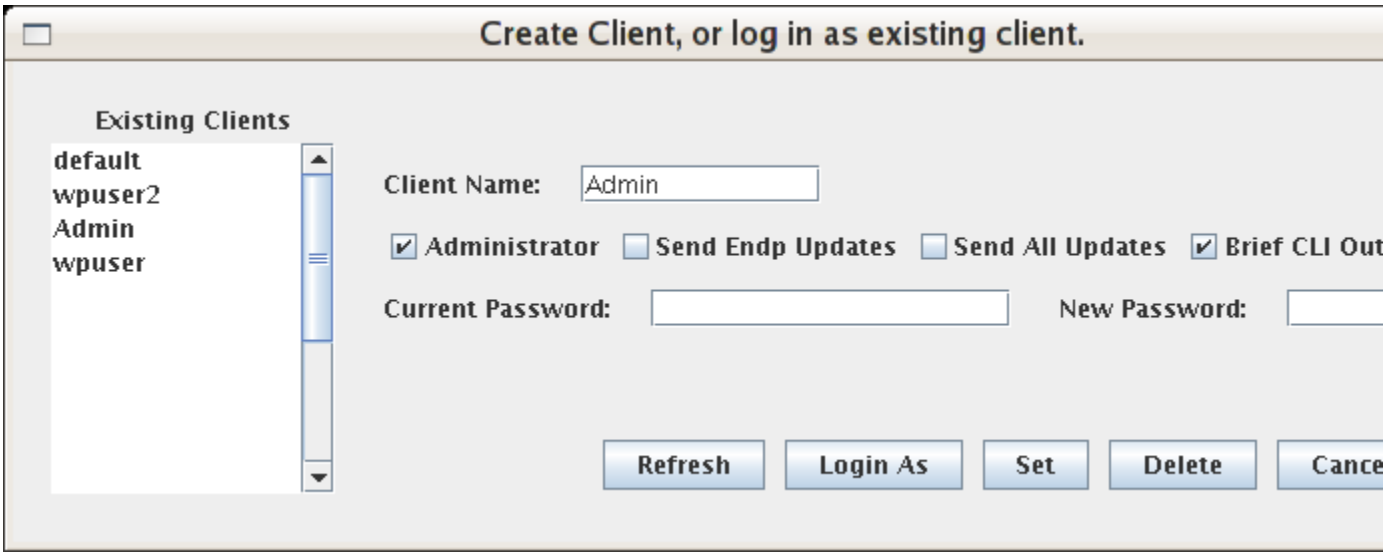
- **Sync** will re-read the current LANforge configuration and re-draw the Netsmith window appropriately. This will cause un-saved changes (such as Virtual Router and Router Connection modifications and positional changes to be lost. Sync may be needed to have newly created WanLinks and virtual interfaces to appear in the Netsmith window.
- **Apply** will force all changes to the LANforge server. It will auto-create any virtual devices and WanLinks that have been added to Netsmith since the last Apply. It will also cause the router to re-calculate all of the Virtual Router routing tables and configuration. You must Apply the changes after creating, deleting, changing virtual-router/connection associations, and when you change the port IP addresses for the changes to take full affect. For large numbers of virtual routers, Apply can take several minutes. The progress bar will update as the work completes.
- **Cancel Apply** stops the current 'Apply' process. This can often leave the virtual router configuration in a bad state, so you should make whatever changes you require and then re-apply.
- **Close** closes the Netsmith window without applying any further changes.

4. User Login

The LANforge security and administration framework has a concept of Users (clients), Test-Managers, and Cross-Connects. Test-Managers are a grouping of one or more clients and 0 or more Cross-Connects. Any user belonging to a Test Manager can manage any of the Cross-Connects belonging to that Test Manager. As a special case, with release 5.0.2, WanPaths can also be assigned to a Test Manager.

When you first log into the LANforge system through the GUI, you will be logged in as the user 'default'. The GUI will then try to log you in as user 'Admin'. If a password has been set for Admin, that login will fail and the login screen will pop up to allow the user to change users and/or enter the correct password. **If there will only be a few different testers using the LANforge system at any given time, you may never need to create a new user, and if you are not worried about who uses LANforge, there is no need to set an Admin password.** However, it may be useful to do so if you have a larger group of users, or if communication between the users is not easy.

To log in as a particular user, select the **Control -> Log In** option from the pull down menus. You will get a screen that looks like this:



The existing clients are shown to the left, with the details of a particular client, including name, Admin status and some other flags. To select a client for modification, double-click it, make your changes and click 'Set'. To log in as a client, double-click it, enter a password if one is set, and click 'Login As'. To create a new account, enter the client name, set appropriate flags, enter password if desired, and click 'Set'.

Flags

Administrator
: If enabled, the user will not be restricted in what it can do.

Send Endp Updates
: If enabled, endpoint updates will automatically be sent to this user. In most cases, this should be disabled since the GUI will request updates as appropriate.

Send All Updates
: If enabled, endpoint, Port, and other updates will automatically be sent to this user. In most cases, this should be disabled since the GUI will request updates as appropriate.

Brief CLI Output
: This has only minor affect on the output of the CLI text interface. It should usually be enabled, but does not make much difference either way.

Creating a client for use by the CLI interface can be done through the GUI too. Unless you are using some sort of scripting program to control the CLI, it is advised that you turn off the Send Updates flags, or the CLI will be so noisy that you will not be able to see what you are doing!

Securing LANforge

By default, LANforge requires no password, and the GUI will log in as the super-user. The default user will also have super-user priviledges. To make LANforge more secure, remove the Administrator flag from the default user, and set a password on the Admin user. You cannot set a password on the default user, and a 'default_tm' Test Manager will always exist with the 'default' user associated. To restrict the default user's access, create a new Test Manager that does not include the default user, and add Cross-Connects to it.

Passwords may be reset by any user with Admin status. The passwords are stored in plain text in the [LANforge-Home]/DB/passwd file. If you remove this file, all users will be able to log in without a password. This password protection will help keep user's from accidentally interfering with configurations that they should not have access to, but **should NOT** be considered a serious means of securing the LANforge machine.

5. Test Managers

The Test Managers are a construct that represents a particular view into the LANforge system. In many cases, you can just use the default Test Manager and ignore this feature entirely. Each Test Manager can have a selection of cross-connects and a list of users who are authorized to use the test manager. This allows one to set up multiple different tests on a LANforge system and quickly change between the test sets. To create a new Test Manager, click on the 'Create' button. You will see this frame:

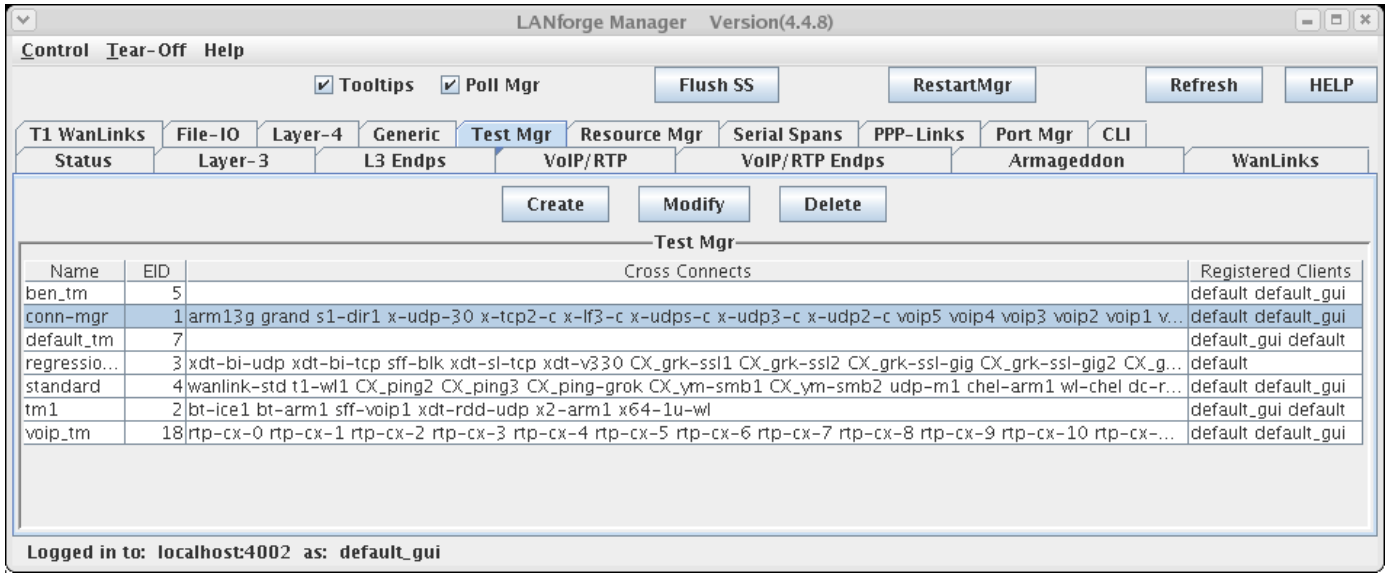
1. First, enter the name of this test manager. Almost all names in the LANforge system are restricted to 15 characters, and cannot contain spaces.

2. If you are just starting, there will be no Cross Connects to register or free, but after the system has been configured, you may adjust the Cross Connects that belong to a given test manager by adjusting the top panel of the Create/Modify Test Manager frame.

3. You will need to register at least one client with the Test Manager if you want to do any useful work. Unless you have created your own client, you should add the 'default' and 'default_gui' client at this time. If 'default_gui' is not currently listed, just add default, save your changes, and click refresh on the main GUI screen. Then select the test manager and click 'Modify'. The default_gui user should be available now.

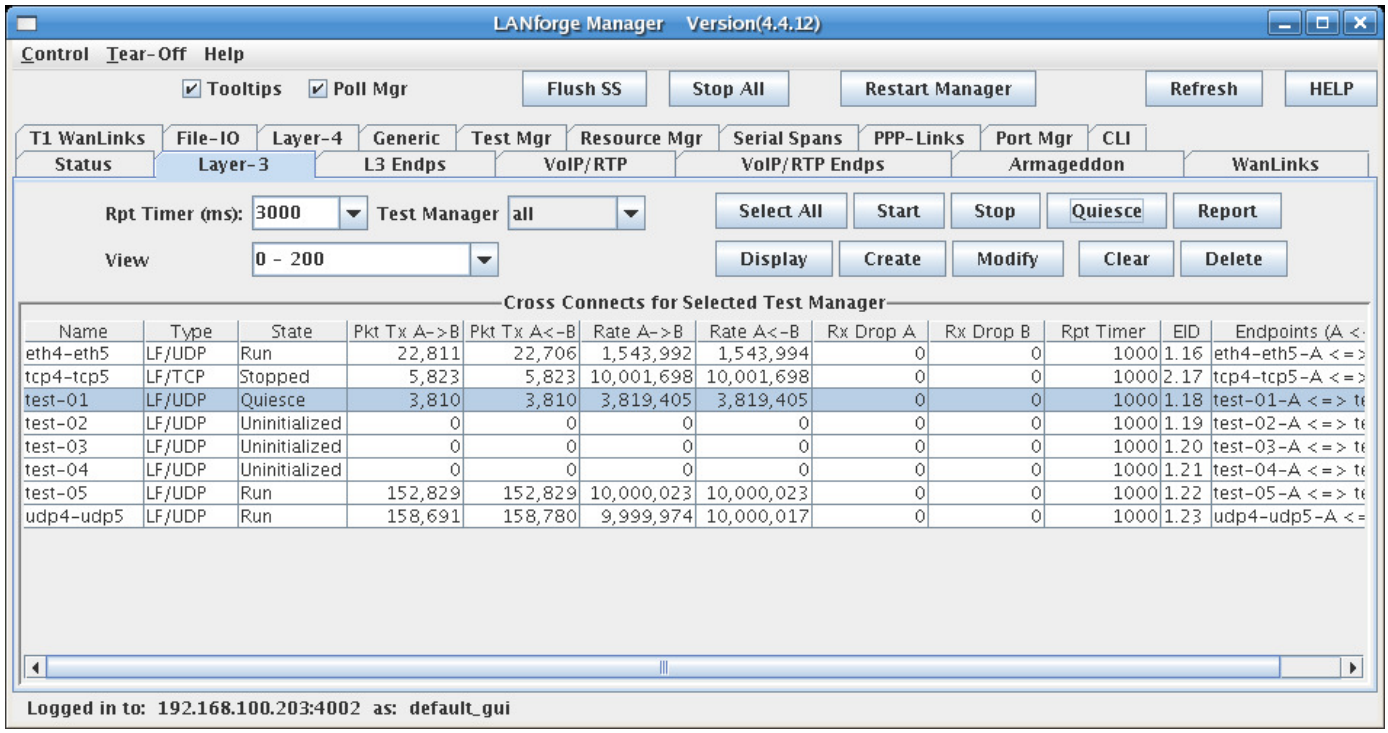
4. Press Apply to send the changes and keep the frame open for other modifications, or press OK to send the information and close the frame.

After creating the Test Manager, the Test Manager panel will display a summary of it, and all other existing Test Managers. To modify one, select it and press the Modify button. Here is what the Test Manager panel looks like:



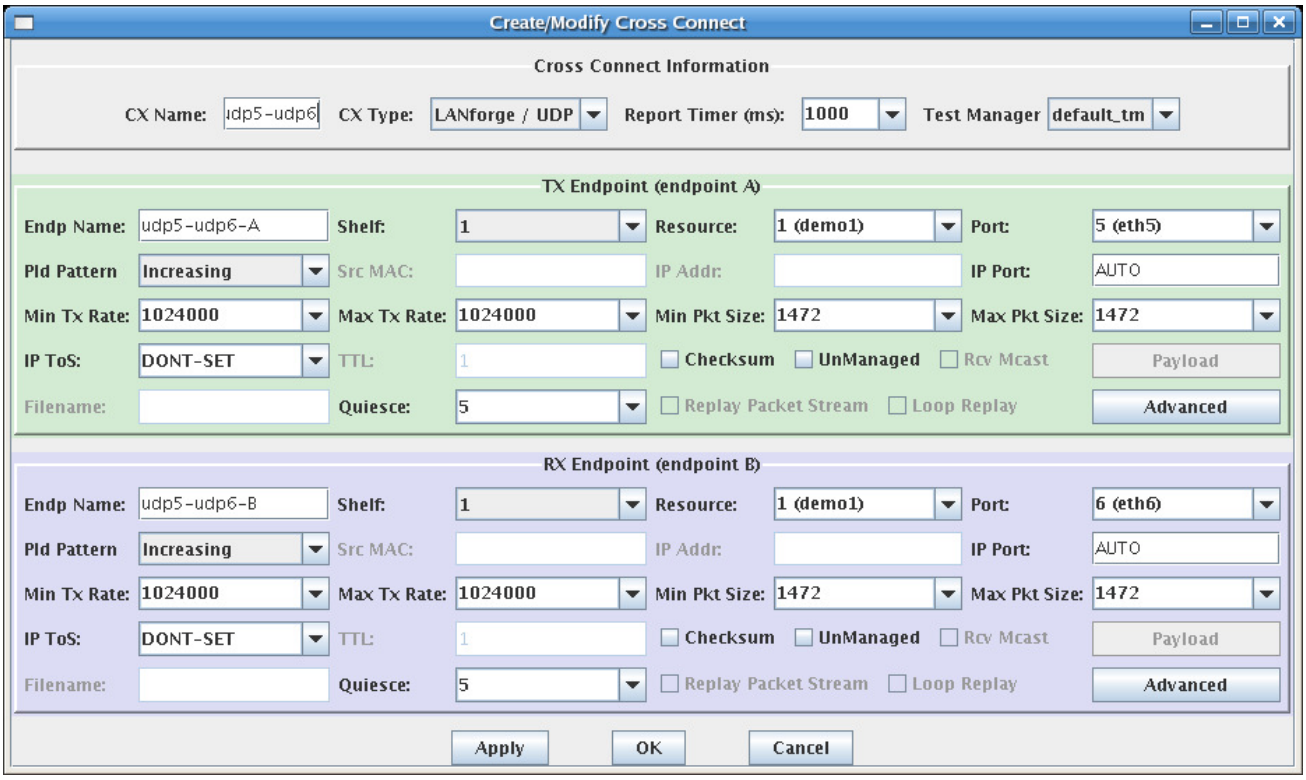
6. Layer-3 Cross Connects (FIRE)

Layer-3 Cross Connects represent a stream of data flowing through the system under test. Each Cross Connect (CX) is composed of two Endpoints, and each Endpoint is associated with a particular Port (physical or virtual interface).



1. Creating & Modifying Cross Connects

When creating a Cross-Connect (CX), you specify the details of each Endpoint, including the Shelf, Resource, and Port that the Endpoint resides on. In this way, you determine which data-generating port (which is connected to some port on the system under test) the CX's traffic will flow over. In order to create a CX, press the 'Create' button on the "Layer-3" panel.



1. The top part of the CX Creation frame contains information relating to the entire CX, including the name, CX Type, report-timer, and the test-manager this CX should belong to. The name must be unique in the LANforge system and should have no spaces and be no more than 15 characters in length. The CX Type determines the protocol that the CX will use. The current supported types are:

Ethernet
Passes a custom protocol over raw ethernet. This type of traffic is constrained to a local LAN (it cannot be routed). This is a good way to test pure packet throughput at the Ethernet level, and will show many types of link layer faults, like corrupted packets, dropped packets, and so forth that the higher level protocols might not show.

UDP/IP
UDP/IP traffic is a non-stream oriented IP protocol that is commonly used for streaming video, music, and other real-time (and possibly lossy) protocols. UDP/IP can be routed, so it is not constrained to the local LAN like the Ethernet protocol is.

TCP/IP
TCP/IP is a stream based protocol that carries the vast bulk of the Internet's traffic. It is routable, and it will re-transmit packets that are dropped, so the only packets LANforge should show as dropped are those that are still in the kernel buffers, or those in transit when the CX is stopped.

Custom Ethernet
Custom Ethernet connections let you specify the exact bytes to transmit onto the ethernet wire, including the Ethernet header. Custom Ethernet connections can also replay ethernet packets captured by LANforge ICE. When replaying, it replays the packets exactly as they were received, including the same ethernet headers, etc. To replay a capture file, select the appropriate file for each endpoint. For more information on generating the capture files, please see the **Dump Packets** notes in the LANforge ICE section.

This connection type also activates a GUI feature that allows you to build your own custom TCP/IP packets. Because LANforge has almost no control over what you send, it cannot detect received packets on the other end of the connection. You can use traffic sniffers or look at the port counters to get ideas of

how many packets were actually received. See Configuring Payloads.

Custom UDP/IP
Custom UDP connections let you specify the exact bytes to transmit as the payload of a UDP datagram. This might be useful for simulating RTP, for instance. See Configuring Payloads.

Custom TCP/IP
Custom TCP/IP connections let you specify the exact bytes to stream over a TCP/IP connection. LANforge has no way of knowing where one of your 'packets' starts or ends, so it cannot detect dropped or mangled bytes on the receive side. You can use the bytes sent and received counters to get a good idea though. See Configuring Payloads.

2. The report timer specifies how often the LANforge data-generators send updates to the LANforge server, and how often the LANforge server pushes endpoint information up to the clients (GUIs) that have requested the automatic updates. If you are running the GUI over a slow link, or have a slower machine, it is recommended to increase the report timer to 5000ms (5 seconds) or higher.

3. The Test Manager specifies which test manager this CX should be added to.

4. The Endpoints are generally symmetric for UDP and Ethernet. For TCP/IP, the TX endpoint acts as a client, and the RX endpoint acts as a server (it waits for connections). Selecting different options may enable/disable certain fields.

Endp Name
Must be no more than 15 characters, spaces and other strange characters are not allowed.

Shelf
Logical grouping for LANforge systems. In most configurations the only, and correct, choice is 1

Resource
The machine on which this endpoint should reside.

Port
The physical or virtual interface with which this endpoint should be associated.

Pld Pattern
The payload pattern for the data generated by LANforge.

Src MAC
This is only used when configuring un-managed endpoints. See below for more information on unmanaged endponts.

IP Addr
Used for un-managed UDP endpoints.

IP Port
If left 'AUTO', the LANforge system will select the IP ports. The user can also specify a particular IP port, but should be aware of potential port conflicts with other LANforge tests and third-party services running on the Linux machine.

Min Tx Rate
The minimum transmit rate that LANforge will attempt to send, in bits per second.

Max Tx Rate
The maximum transmit rate that LANforge will attempt to send, in bits per second. If this is greater than the min-tx-rate, then LANforge will vary the speed between the min and max creating a random stair-step pattern of data transmission over time.

Min Pkt Size
The minimum packet size, in bytes. The packet size includes **only** the bytes for the selected protocol. For instance, if you select a 1472 byte packet for a UDP connection, the ethernet frame will actually be 1514 bytes in length because of the addition of the 14 bytes of ethernet header, the 20 bytes of IP header, and the 8 bytes of the UDP header. When configuring an Ethernet connection, you would select a length of 1514 to create a packet of 1514 bytes since there is no underlying data protocol.

Max Pkt Size
The maximum packet size, in bytes. If this is larger than the min-pkt-size, then each packet will be a random size between min and max.

IP ToS
For IP based protocols, you can specify the ToS (aka QoS) bits in the IP header. This can be useful for testing QoS settings in the device under test.

NOTE: When running LANforge in Windows, QoS must first be setup by following the instructions in the Microsoft Knowledge Base article 248611: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q248611

TTL
This specifies the 'time-to-live' when configuring Multicast endpoints. It does not apply to other prototocols.

Do Checksum
If the Do Checksum checkbox is selected, then the payload will be checksummed with a 32-bit CRC calculation. This gives a very high degree of packet corruption detection at each layer, but due to the extra work the CPU has to do, the maximum traffic rates may be smaller. Note that TCP/IP, and the ethernet protocol itself already has CRC checks, so you may not need to enable LANforge checksumming.

UnManaged
If an endpoint is specified as UnManaged, this means that this endpoint is not controlled by LANforge. This can be used to fling UDP packets at some third-party application, for instance. It would be less useful for testing TCP in most cases.

Rcv Mcast
For multi-cast packets, this indicates that this endpoint should be a receiver of multicast instead of a sender.

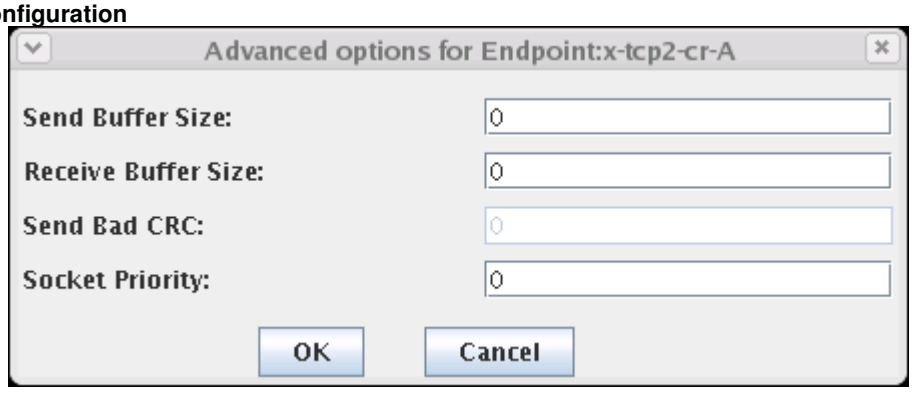
Filename
Select the file-name when replaying a previously captured stream of packets. This is only useful with Custom Ethernet connections and when the 'Replay Packet Stream' checkbox is selected.

Quiesce
Instead of stopping the receiving and transmitting endpoints, Quiesce will stop the transmitting endpoint and wait a prescribed number of seconds before stopping the receiving endpoint so that all transactions may be completed.

Replay Packet Stream
Select this to replay a previously captured packet stream. Only valid for connections of type Custom Ethernet.

Loop Replay
Select this to replay a previously captured packet stream in an endless loop. Only valid for connections of type Custom Ethernet.

5. **Advanced Configuration**



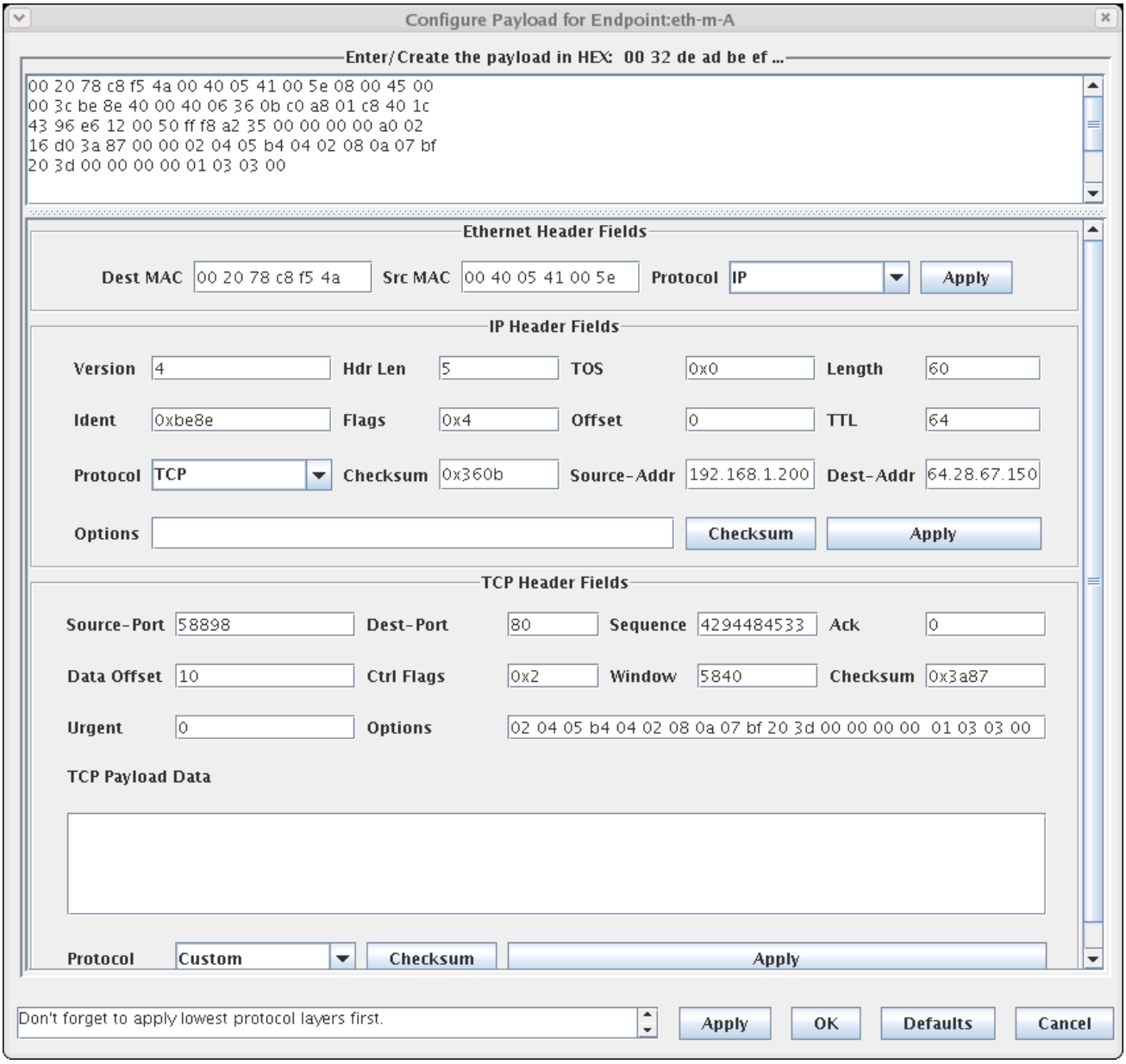
The Advanced tab allows one to configure the sending and receiving buffer sizes. For TCP connections, this correlates to sending and receiving window sizes. For layer-2 ethernet protocols one can also specify the number of frames to be generated with purposefully bad ethernet CRCs. This 'bad CRC' feature is only supported by

certain ethernet adapters and drivers. Please contact Candela if you wish to use this feature.

You can use the 'Socket Priority' field to set a particular priority for the generated packets. When used in conjunction with the priority -> .1q priority mapping supported in the 802.1Q VLAN stack on Linux, you can have packets created with particular 802.1Q priorities. You can also use other Linux tools external to LANforge to modify behaviour of the packets based on the priority.

2. Custom Payloads

To configure custom payloads on custom endpoints, click the "Payload" button on the Endpoint or Cross-Connect configuration panel. If you are configuring a Custom Ethernet Endpoint, the resulting screen will look like this:



As you fill in the lower protocol layers (for instance, the Ethernet header), other protocol builders will be added to the GUI display as selected. For example, if you choose the IP protocol in the Ethernet header, the IP builder will appear. It will parse the top HEX window if possible and initialize it's fields appropriately. From the IP protocol builder, you can choose TCP as the next layer, and the TCP builder will appear...

Protocol Builders

These are the only protocol builders supported at this time. More will be added as time permits, but please let us know if there are any in particular that you would like to see implemented first. If you wish to transmit protocols we do not have builders for, you can always paste a captured packet, or hand build one in HEX and transfer it to the text editor at the top of the Payload panel.

You can also initialize most protocols to defaults, and the resulting values will correspond to live packets gathered from our network. The ethernet protocol is slightly different, see the notes below. Make sure you initialize from the lower layers up to the higher layers.

Ethernet Header

You can specify the Source, Destination and Protocol fields in the Ethernet Header. If you tell this protocol to initialize to defaults, it will grab the MAC addresses from the two ports it is connected to. This may or may not be what you want, so be ready to re-enter the fields accordingly.

IP Header

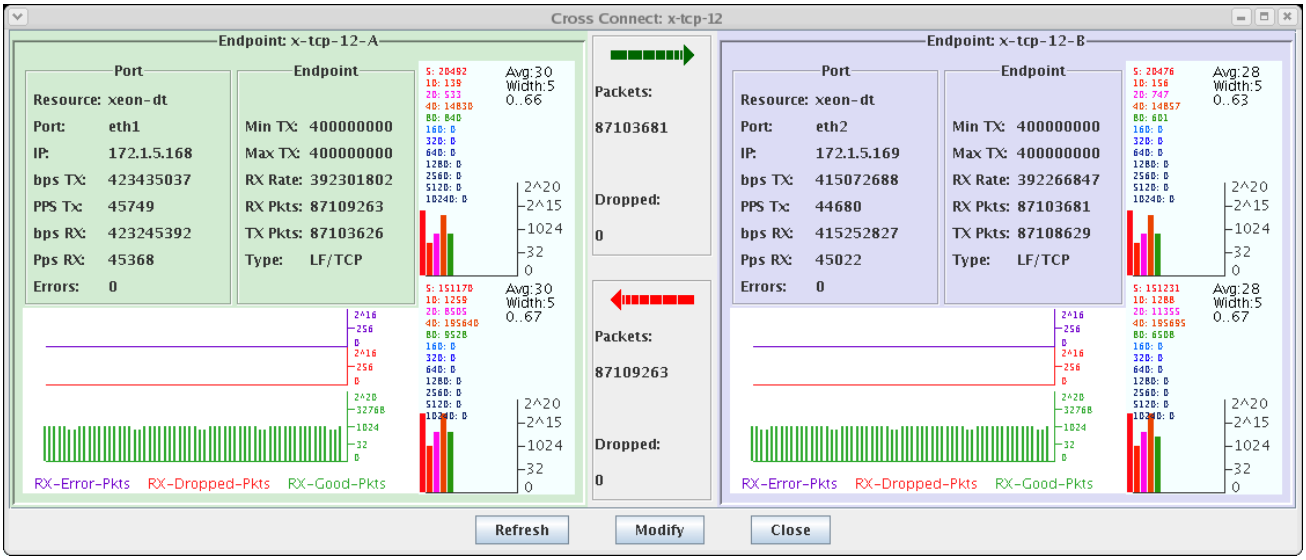
You can specify the various IP header fields. For details, look up the venerable RFC 791. If you change a field, you will probably want to re-checksum both the IP header and higher protocols too (in that order).

TCP Header

You can specify the various TCP header fields. For details, look up the venerable RFC 793. If you change a field, you will probably want to re-checksum the header with the checksum button.

3. Cross Connect Display

When you are interested in a particular Cross-Connect, you may select it and click on the 'Display' button. That will bring up a summary display for that cross-connect.



The busy graphs to the right of each pane are the latency distribution displays. LANforge detects latency with a timestamp in each LANforge protocol packet (LANforge-ETH, LANforge-UDP, and LANforge-TCP endpoint types ONLY) The precision is to 1 millisecond. If the two endpoints are using NTP protocol to keep themselves in sync, then they are usually within 0-3 milliseconds apart. Because of this, latencies may be negative at times. This just shows the difference in the clocks, and by looking at both sides of the connection, you can deduce the true latencies. For the best latency measurements, have both the sending and receiving port on the same machine. For even higher precision, consider an Armageddon endpoint, which has micro-second latency reporting.

LANforge only counts the latencies when it receives the packet. This is not exactly the time that the packet was received by the LANforge hardware because the packet must flow through the protocol stacks up to the LANforge server. This is the primary cause of the range of latencies you will see reported even on a simple and fast LAN. The average is usually very close though: It is a running average of the last 100 packets received.

The average is printed out on the top-right side of the individual latency display widgets. The min/max are displayed below the average.

There are 2 latency graphs for each endpoint. The top one is for the last 30 seconds, and the bottom is for the last 5 minutes.

The numbers on the top-left of the widget are the counters for each latency 'bucket'. The vertical graphs correspond to those numbers.

The units for the size of the buckets are milliseconds, and are exponential (2^X) in scale. The exponential values (1, 2, 4, 8, etc) will be multiplied by the bucket 'width', which is always 5 currently, and added to the minimum latency. For instance, if the minimum latency is 0 millisecond, then the buckets will be:

```
5
10
20
40
80
...
```

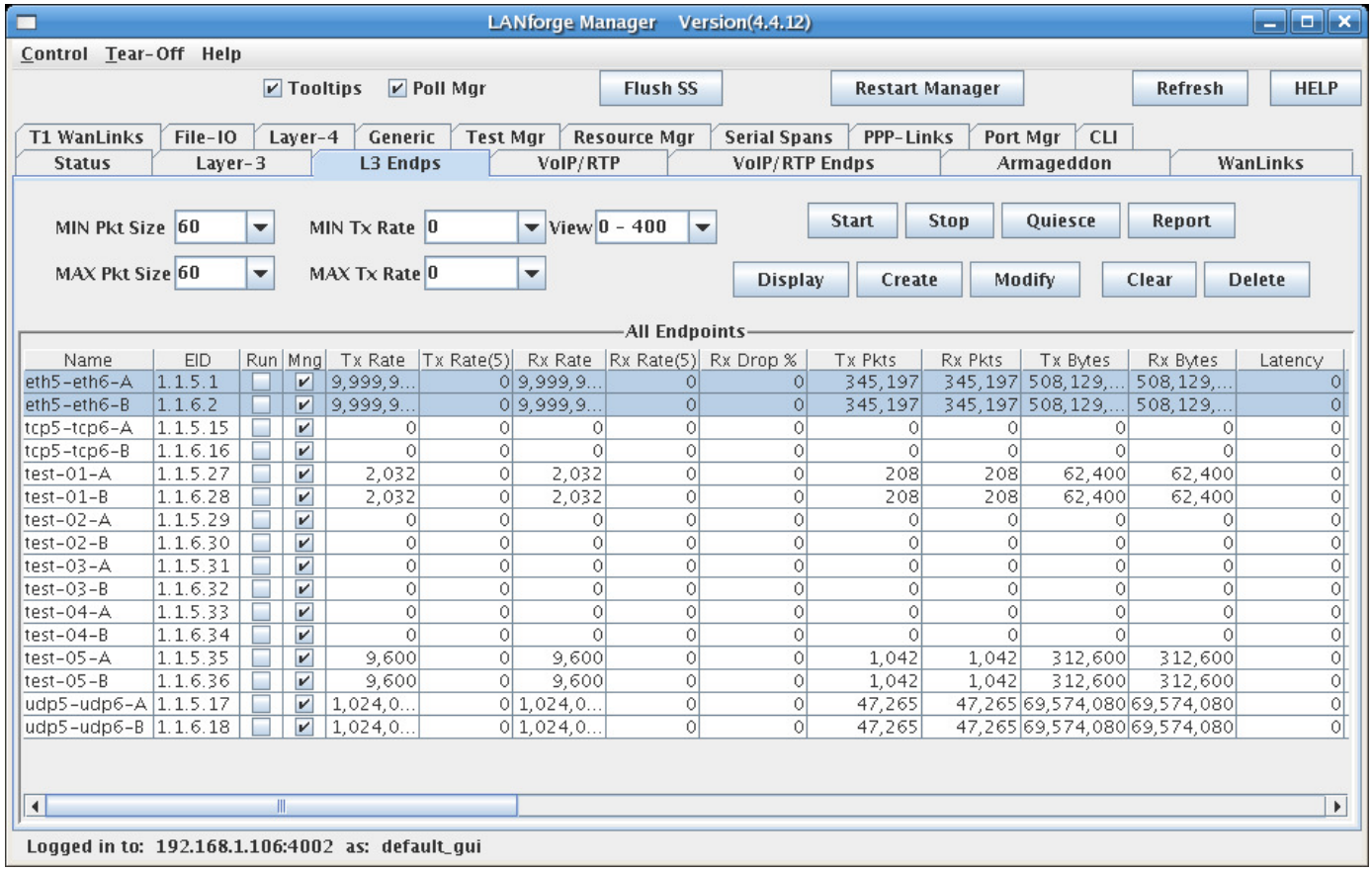
If the bucket "5" has 2000 beside it, then that means that 2000 packets have been received in the last time-period that ranged from 0 to 4 milliseconds in latency. If the bucket "10" has 30 beside it, then that means 30 packets had latency between 5 and 9 milliseconds, inclusive.

The minimum latency can change over time, which will cause the buckets to shift their values. Although this may be confusing at first, it allows LANforge to report high-precision data regardless of the latency of the system under test.

When viewing the Spread-Sheet output, the lat_0, lat_1, etc columns show the number of packets received in the last 30 seconds that fall into the buckets.

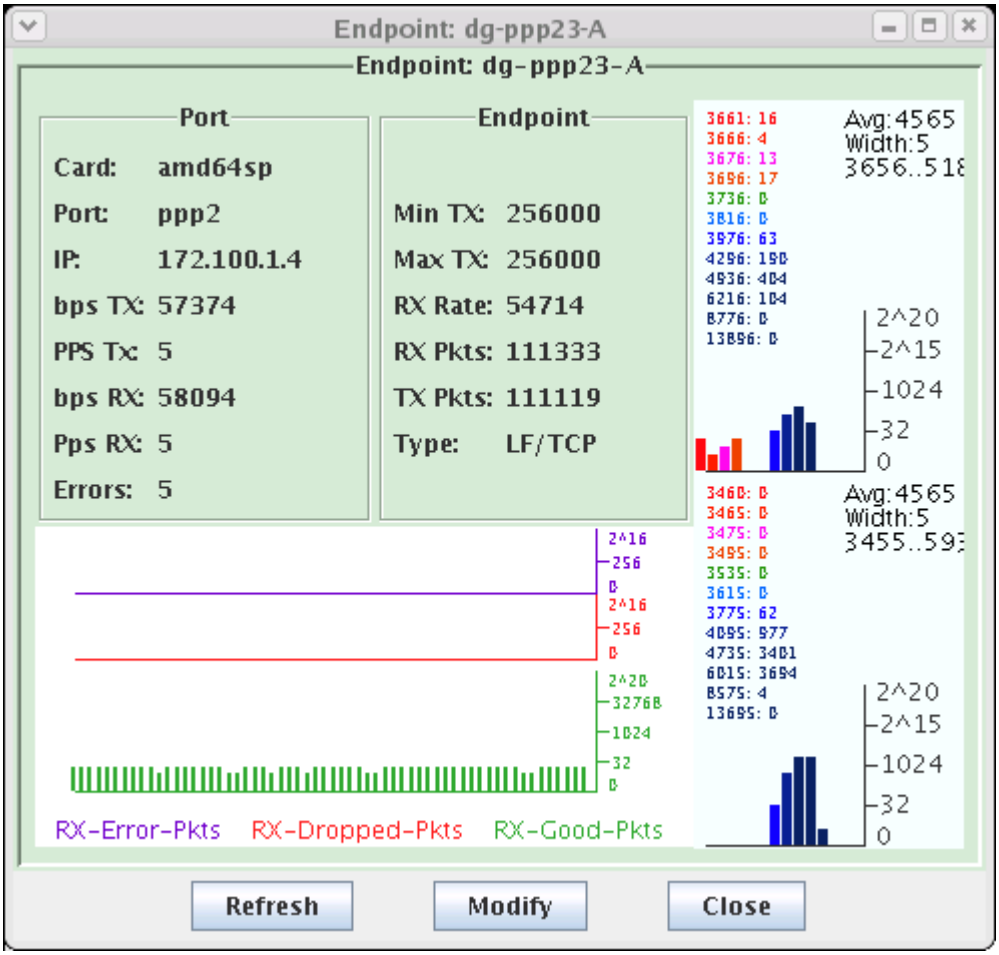
7. Layer-3 Endpoints (FIRE)

You will use the Cross Connect screen to stop/start/modify your (non IGMP) CXs, but to see the fine details of each cross-connect, you will want to look at the endpoint screen. If you select a particular CX by single-clicking on it's row, then you can move to the L3-Endps screen and see the Endpoints for that CX highlighted as well.



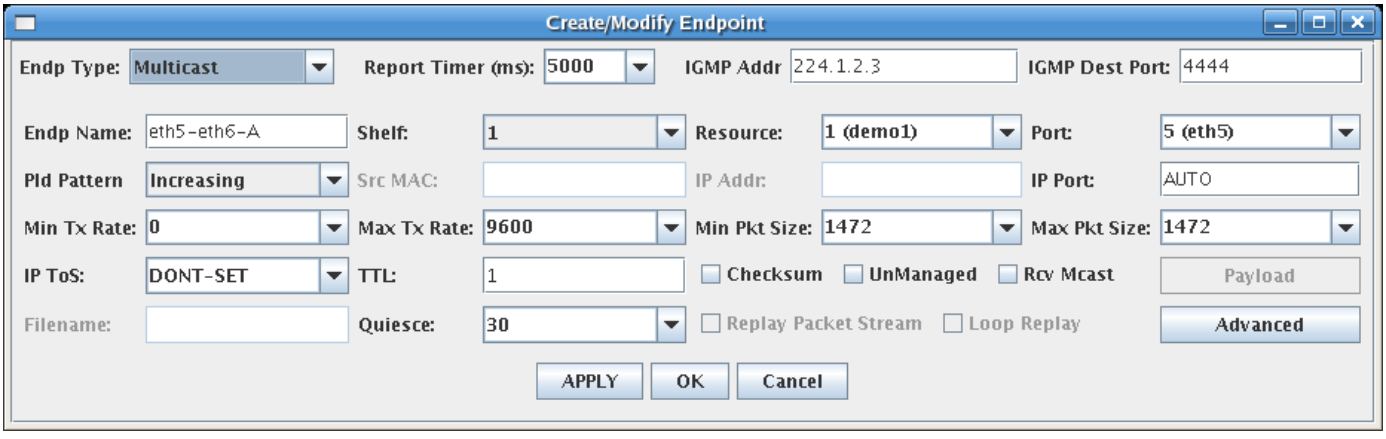
From the L3-Endp Panel you can do bulk changes to packet sizes and packet rates. For example, if you want several of your Endpoints running at 56000bps then you can select them, and use the MIN Tx Rate combo-box to set the desired value. For more specific modifications, select the endpoint in question and press the Modify button. You can also modify Endpoints through their Cross-Connect on the Cross Connects pane.

If you wish to see graphs for the received packets for a particular endpoint, you can select one or more endpoints and click on the "Display" button. Here is an the Display of an IGMP Multicast endpoint:



IGMP: Multicast UDP

LANforge now supports the IGMP UDP Multicast protocol. Because there is a one to many relationship, these endpoints are not handled by the standard cross-connect paradigm. Instead, you can create multiple endpoints, specifying one generator and zero or more receivers for a particular IGMP address/port pair. To create an IGMP endpoint, press the "Create" button. To modify an existing IGMP endpoint, select it and press the "Modify" button.



Endp Type

The Endpoint Type should be "Multicast". Custom Multicast is not supported at this time (please enquire if you are interested in this feature.)

Report Timer

The Report Timer is how often (in millisecond units) the endpoint reports to the GUI. 1000-5000 (1-5 seconds) is suggested for most cases.

IGMP Address

The IGMP Address is the 'IP' address of the multicast group. Multicast IP addresses must be in the range between 224.0.0.0 and 239.255.255.255, inclusive. The IGMP Address and Port specifies a particular multicast group.

IGMP Dest Port

The IGMP Destination Port is the UDP port that this endpoint will transmit to, assuming it is a transmitter. If it is a receive-only endpoint, then this field can be left blank ("IP Port" specifies the receiving port.)

IP Port

The IP Port is the port that the Endpoint listens to if it is a receiver. If it is a transmitter, then this field can be left at the default setting.

TTL

The Time To Live field determines how far the IGMP packet may travel. If it's 1, then it travels only to the local subnet. Larger numbers allow it to travel across routers. Be careful not to flood other networks by accident!

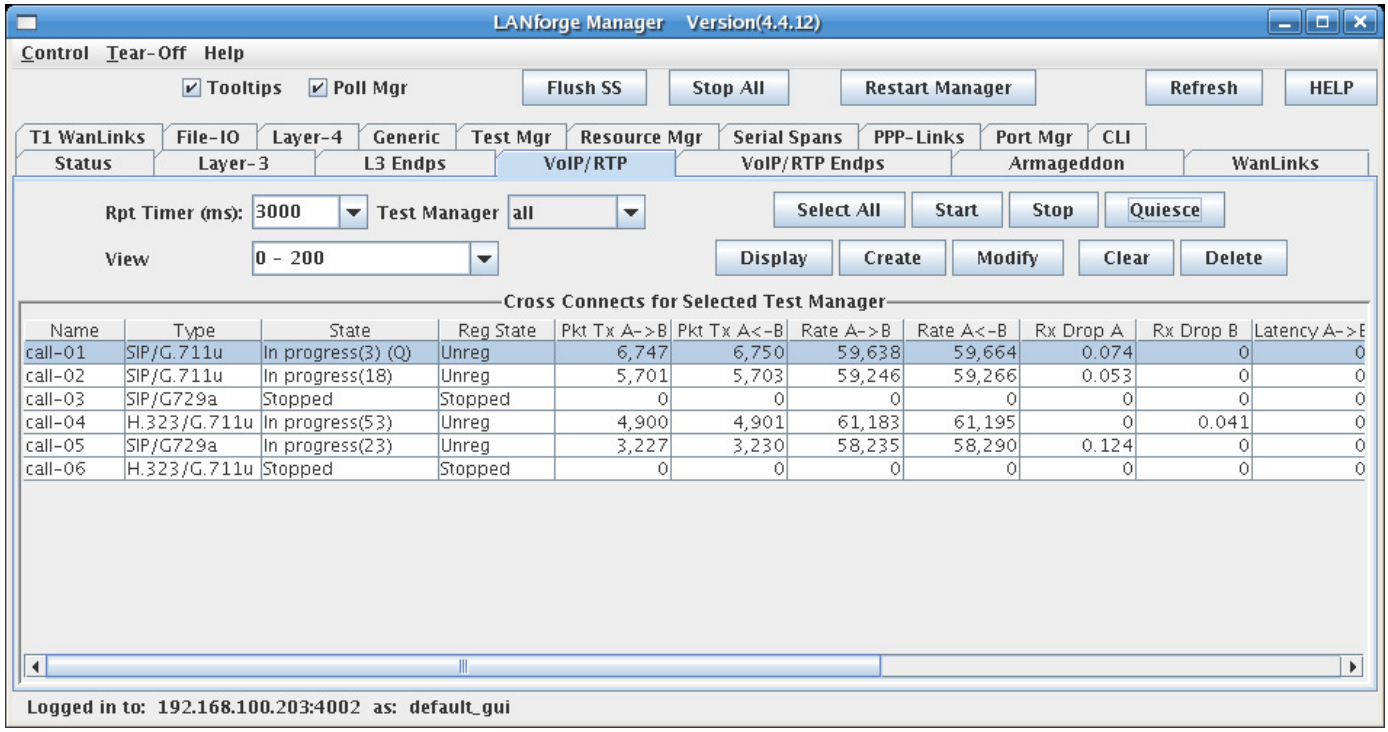
Rcv Mcast

If the Receive Multicast flag is checked, then this endpoint will be a receiver. If not, then it will be an IGMP multicast generator. You should have one generator per unique multicast IP address and port, and zero or more receivers.

8. VoIP (H.323, SIP, RTP, RTCP) Call Generator

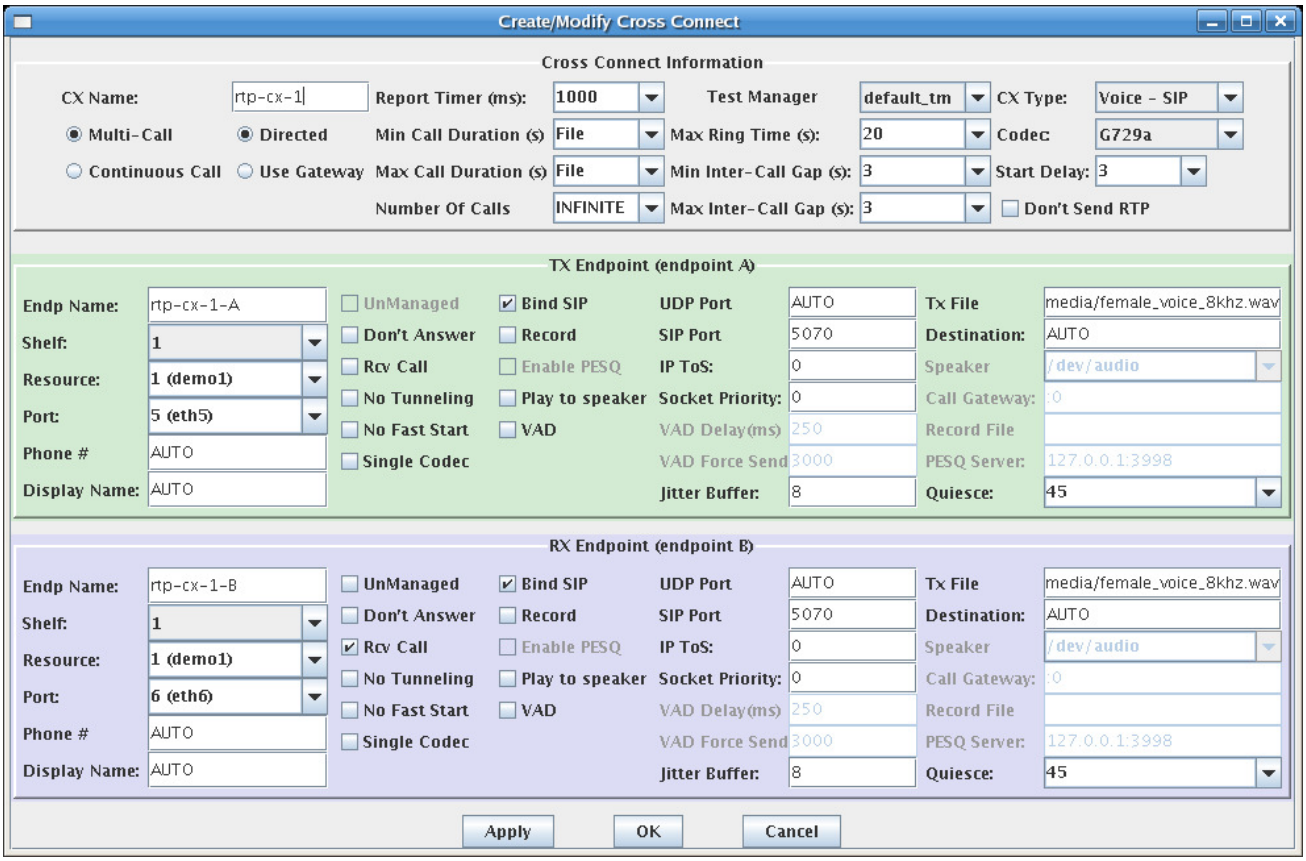
After adding a Test Manager, you may create Voice over IP (VoIP) Calls between LANforge interfaces. You may also set up third-party phones to call LANforge or be called by LANforge.

VoIP consists of several protocols. The messaging protocols currently supported by LANforge are H.323 (as of release 4.4.1) and SIP (Session Initiated Protocol). The voice payload is transmitted with the Real Time Protocol (RTP) which runs over UDP. The Real Time Control Protocol (RTCP) is used for latency and other accounting, and runs over UDP with the same priority as the RTP traffic.



1. Creating & Modifying VoIP Cross Connects

When creating a Cross-Connect (CX), you specify the details of each Endpoint, including the Shelf, Resource, and Port that the Endpoint resides on. In this way, you determine which data-generating port (which is connected to some port on the system under test) the call's traffic will flow over. In order to create a CX, press the 'Create' button on the "VOIP/RTP" panel.



The top part of the CX Creation frame contains information relating to the entire CX, including the name, CX Type, report-timer, and the test-manager this CX should belong to. The name must be unique in the LANforge system.

CX Type

The CX Type determines the protocol that the CX will use. The current supported VoIP types are:

Voice-SIP

Makes a voice call using the SIP messaging protocol. If you are using 'Directed' mode, then the endpoints can call directly to each other without using a SIP proxy server. With the 'Use Gateway' option, a SIP server will be used to handle the call routing. LANforge has been tested with a wide variety of third-party SIP gateways, including Asterisk

Voice-H323

Makes a voice call using the H.323 messaging protocol. If you are using 'Directed' mode, then the endpoints can call directly to each other without using an H.323 gateway. With the 'Use Gateway' option, an H.323 server will be used to handle the call routing. LANforge has been tested with the gnugk H.323 gateway.

Report Timer

The report timer specifies how often the LANforge data-generators send updates to the LANforge server, and how often the LANforge server pushes endpoint information up to the clients (GUIs) that have requested the automatic updates. If you are running the GUI over a slow link, or have a slower machine, it is recommended to increase the report timer to 5000ms (5 seconds) or higher.

Test Manager

Specifies to which test manager this CX should be added.

Call Modes

Three call modes are possible: With 'Continuous Call', a single call will be made and the wave file will be played in

a loop until the call is stopped by the user. In 'Single Call' mode, the wave file will be played exactly once and the call will be terminated. In 'Multi-Call' mode you can specify the number of times to loop the wave file, the number of calls to make, and the maximum time of the call. If using PESQ, you should use the 'Multi-Call' option.

Call Gateway Mode

Two different Call Gateway options are available: 'Directed' means that the VOIP endpoints directly call themselves, without registering with or using a proxy or gateway. In this configuration most of the endpoint attributes can be 'AUTO' because LANforge can determine the settings automatically. In 'Use Gateway' mode the call endpoints will register with a gateway or proxy and make calls through it.

Call Duration

Min/Max Call Duration determine the length of the call. If 'File' is selected then the call will be as long as it takes to play the chosen wave file. If Min is not equal to Max, a random value between the min and max will be chosen for each call made. If using PESQ, select 'File' for the call duration.

Number of Calls

Specifies the number of calls to make before the endpoint stops itself. Choose 'Infinite' if you want to run until the user stops the call manually.

Ring Time

Determines how long the calling endpoint will wait for the called party to pick up before deciding the call was a 'No Answer'.

Inter-Call Gap

Min/Max Inter Call Gap specifies how long to wait between calls. If min is not equal to max, a random value will be chosen between min and max for each call.

Codec

Determines the codec for the RTP voice payload. Currently G729, G711u, G726-16, G726-24, G726-32, G726-40 and Speex codecs are supported by SIP. H.323 only supports G.711u at present. By default, the phones will advertise all supported Codecs, with a preference on the one selected here. If you want to **only** advertise the single selected codec, then also enable the "Single Codec" checkbox in the Endpoint configuration sections.

Don't Send RTP

By default, LANforge will generate the RTP payload for each call. This requires significant processing resources, so if you only care about the SIP messaging, you can select this checkbox to disable sending of RTP.

Each Endpoint can be configured independently of the other. The default is to have the 'A' endpoint call the 'B' endpoint. The 'B' endpoint can be un-managed, which means LANforge assumes that it is a third-party endpoint, such as a Cisco or Grandstream SIP phone.

Name, Shelf, Resource, Port

The Endpoint name, shelf, resource, and port information determines the Port (interface) this endpoint will use.

Phone Number

The Phone Number is the SIP or H.323 identifier for the endpoint. If you are using a Gateway, then this number must be configured in the Gateway so that the endpoint can register. For directed calls, this can be 'AUTO' and LANforge will choose some random value and make it work. For SIP, if you put in a number, the SIP To/From headers will be number@IP:port. If you want LANforge to use a domain for the To/From headers, then you can enter something like: 1234@domain.com for the phone number. If you are using non-standard SIP ports, then you must specify the SIP port too: 1234@domain.com:50600

Display Name

Allows configuration of the SIP Display Name attribute.

Flags & Options

Several flags are used to enable and disable certain features and affect certain behaviour. The 'UnManaged' flag tells LANforge that this particular Endpoint is not a LANforge endpoint. Use this when configuring LANforge to call third-party SIP phones, for example. The 'Don't Answer' flag will make LANforge decline to 'pick up' the phone when called. If 'Rcv Call' is set, then this endpoint will wait for calls to be made to it, but will not originate any calls. Set the 'Bind-SIP' flag if the gateway is connected to the same (ethernet) interface that the VoIP endpoint is connected to. If you are using the management network for the gateway, then un-set this checkbox.

If the 'Record' box is checked, LANforge will record the received audio stream to the specified wav file. This must be selected if you want to enable PESQ reporting.

You can also play the received audio to the LANforge server's speaker, assuming the sound system exists and is configured correctly. The sound device is normally /dev/audio in Linux.

LANforge VOIP now supports PESQ automated voice quality reporting. You must purchase a separate PESQ license for your LANforge system in order to enable this feature. To configure the VOIP endpoint for PESQ, select the 'Enable PESQ' checkbox. You must also configure the PESQ server. The PESQ server is the LANforge machine on which you install the PESQ license. PESQ can run along side other LANforge processes, so everything can be installed on a single machine if desired. For optimal results, select the 'Multi-Call' call mode and 'File' for the call duration. You also have to enable the 'Record' feature so that the received audio is saved to the local file system for processing by PESQ.

SIP supports 'Voice Activity Detection (VAD)'. With this enabled, RTP packets will not be sent when more than 'delay' milliseconds of silence have been detected.

By default, LANforge will prefer the selected Codec, but it will also accept other codecs that it supports. If you want to only use a single selected codec, then select the 'Single Codec' checkbox.

For H.323 calls, you an configure the fast-start and tunneling modes with the two checkboxes on the bottom left.

UDP Port

UDP Port specifies the port that RTP traffic will use. RTCP will use one port higher than that, so if you choose to configure these manually, be sure to leave space. You can also use 'AUTO', in which case LANforge will allocate ports accordingly.

SIP Port

SIP Port specifies the UDP port for the SIP messaging protocol. When using H.323 protocol, this specifies the H.323 management port. The default SIP port is 5060, so if you are trying to configure an un-managed endpoint that cooresponds to a third-party SIP phone, using 5060 is a good choice. The default H.323 port is 1720.

IP ToS

You can specify the ToS (aka QoS) bits in the IP header. This value will be set on RTP and SIP packets.

Socket Priority

If you are running VOIP over 802.1Q VLAN interfaces on the LANforge system, setting the socket priority can allow you to map the priority to the 802.1Q priority. Use the external 'vconfig' Linux tool to configure the mappings between a particular socket priority and the .1Q priority. (Not currently supported by H.323.)

VAD Delay

How much consecutive silence before VAD is enabled.

VAD Force Send

Force a send of an RTP packet at least every X milliseconds. Helps keep connections from being timed out with some phones.

Jitter Buffer

Specify the jitter buffer size, in number of 20ms packets. Should be used to smooth out network jitter inherent in RTP traffic.

Tx File

The Tx File is the WAV file to play. Wave files must use single-channel 8-bit encoding. The Linux tool 'sox' can be used to convert various formats to the correct encoding. Assuming you have a sound/music file called muzak.ogg, the command syntax is:

```
sox muzak.ogg -U -c 1 -b -v 1.1 -r 8000 /tmp/muzak.wav resample -q1


# muzak.ogg == input file, can be almost any type of sound file.
# -U      == ulaw encoding
# -c 1    == one channel
# -b      == 1-byte encoding (8-bit)
# -v 1.1  == increase volume by 1.1/1.0 percent, optional
# -r 8000 == 8000 samples per second.
# /tmp/muzak.wav  == output file, has to be a .wav extension.
# resample -q1    == makes it sound better, evidently, I can't tell.
```

Destination

If the destination number/URL to be called is different from the peer endpoint's phone number, you may specify it

in this field.

Speaker

If you have a properly configured sound card, you can play the received call to the speaker real-time. Only a single call can play on a particular machine at the same time. Select the 'Play to Speaker' checkbox to enable this feature. This feature is only supported for SIP, and only on Linux.

Call Gateway

For 'Use Gateway' calls, you will need to specify the SIP Proxy or H.323 gateway. The proxy or gateway should usually be located in the system/network under test. This is a potentially complex matter, so please contact Candela Technologies or your supplier if you have any questions. For authenticated SIP registration, append the password to the front of the IP address: [password@]IP[:port]

Record File

If you want a copy of the received wav file, or if you are using PESQ, enter the file name to which to save the received audio stream. This should be unique for all endpoints so that you do not corrupt other calls' files.

PESQ

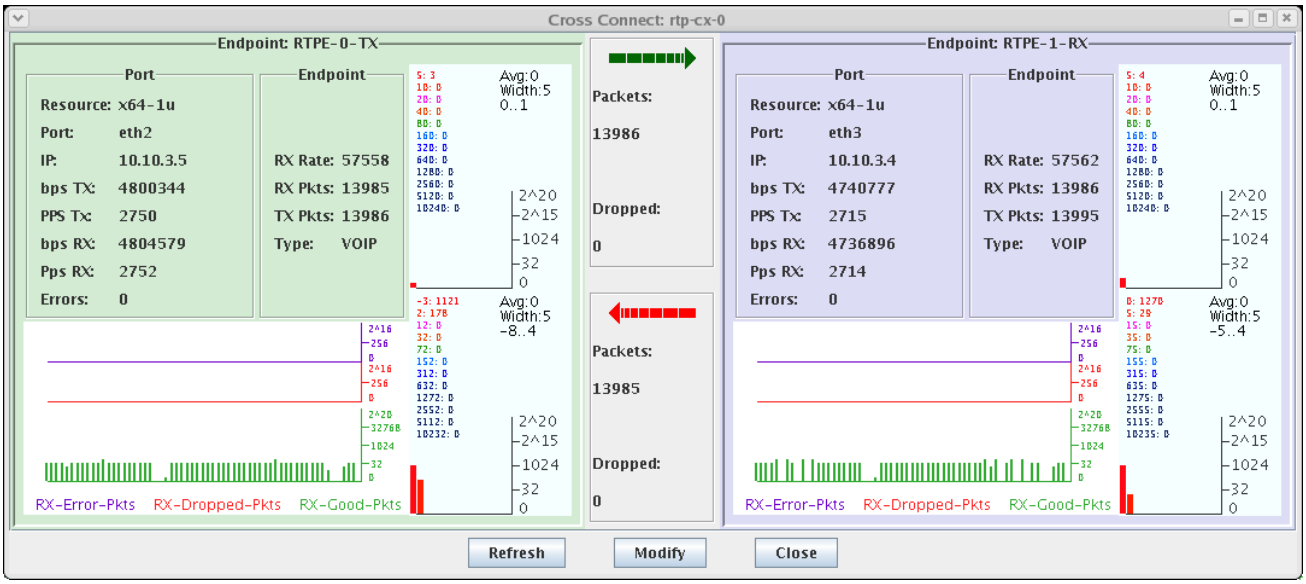
To enable PESQ automated reporting, you must have a PESQ license and/or access to a machine running a licensed PESQ server. Enter the IP address of that machine and the port (default port is 3998) in this field.

Quiesce

Instead of stopping VoIP endpoints, Quiesce will stop generating new traffic and wait a prescribed number of seconds before stopping the receiving endpoint so that all transactions may be completed.

2. VoIP Call Display Panel

When you are interested in a particular VoIP Cross-Connect, you may select it and click on the 'Display' button. That will bring up a summary display for that cross-connect.



The busy graphs to the right of each pane are the latency and jitter distribution displays. LANforge detects latency with the RTCP protocol, and jitter is determined from the timestamp on the received RTP packets. Note that the jitter calculation is made before the packet is processed by the RTP Jitter buffer.

The average values are printed out on the top-right side of the individual display widgets. The min/max are displayed below the average.

The top graph is for RTCP latency over the last 30 seconds, and the bottom graph is jitter derived from the RTP packets over the last 30 seconds.

The numbers on the top-left of the widget are the counters for each latency 'bucket'. The vertical graphs correspond do those numbers.

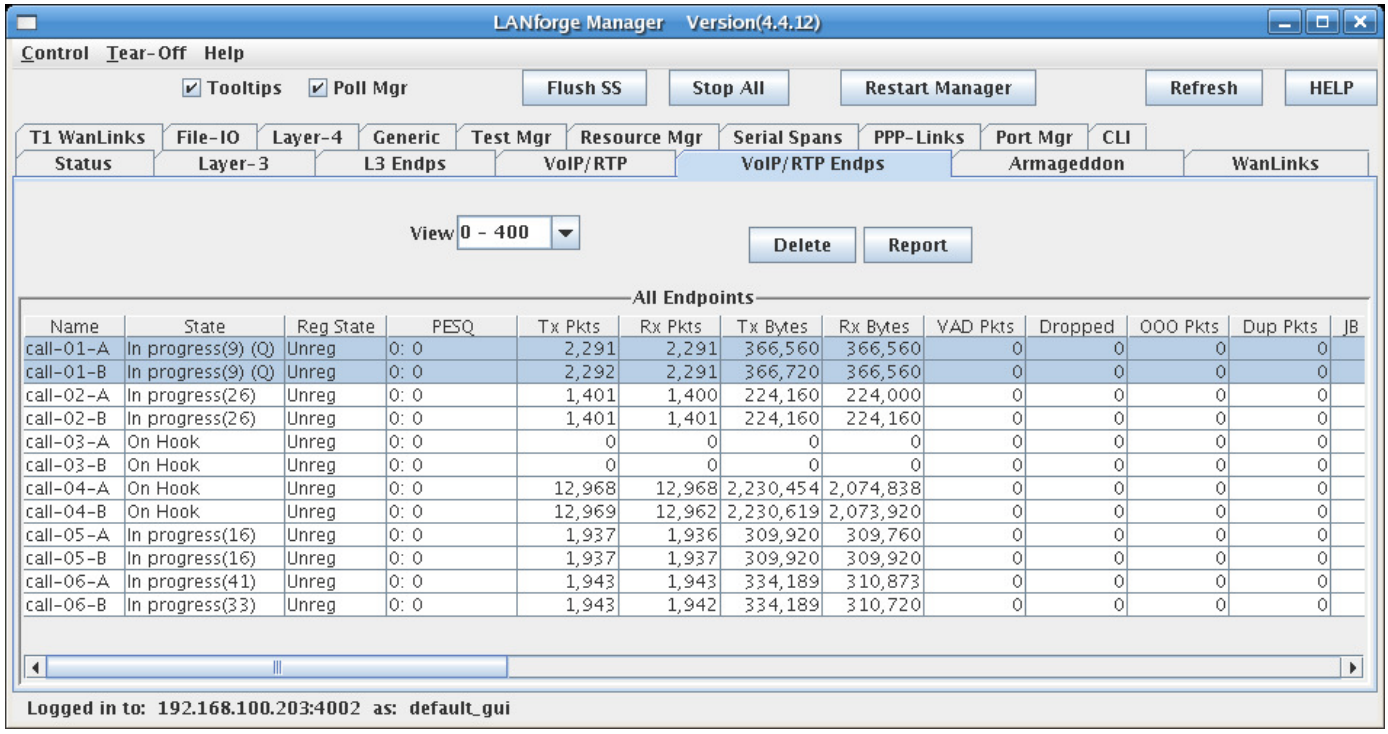
The units for the size of the buckets are milliseconds, and are logorithmic in scale. For instance, if the average latency is 0 millisecond, then the buckets will be:

```
9
19
39
79
...
```

If the bucket "4" has 2000 beside it, then that means that 2000 packets have been received in the last time-period that ranged from 0 to 4 milliseconds in latency. If the bucket "9" has 30 beside it, then that means 30 packets had latency between 5 and 9 milliseconds.

9. VoIP Endpoints

You will use the RTP Cross Connect screen to stop/start/modify your RTP Call Cross-Connects, but to see the fine details of each endpoint, you may want to look at the endpoint screen. If you select a particular call by single-clicking on it's row, then you can move to the RTP Endpoints screen and see the Endpoints for that call highlighted as well.

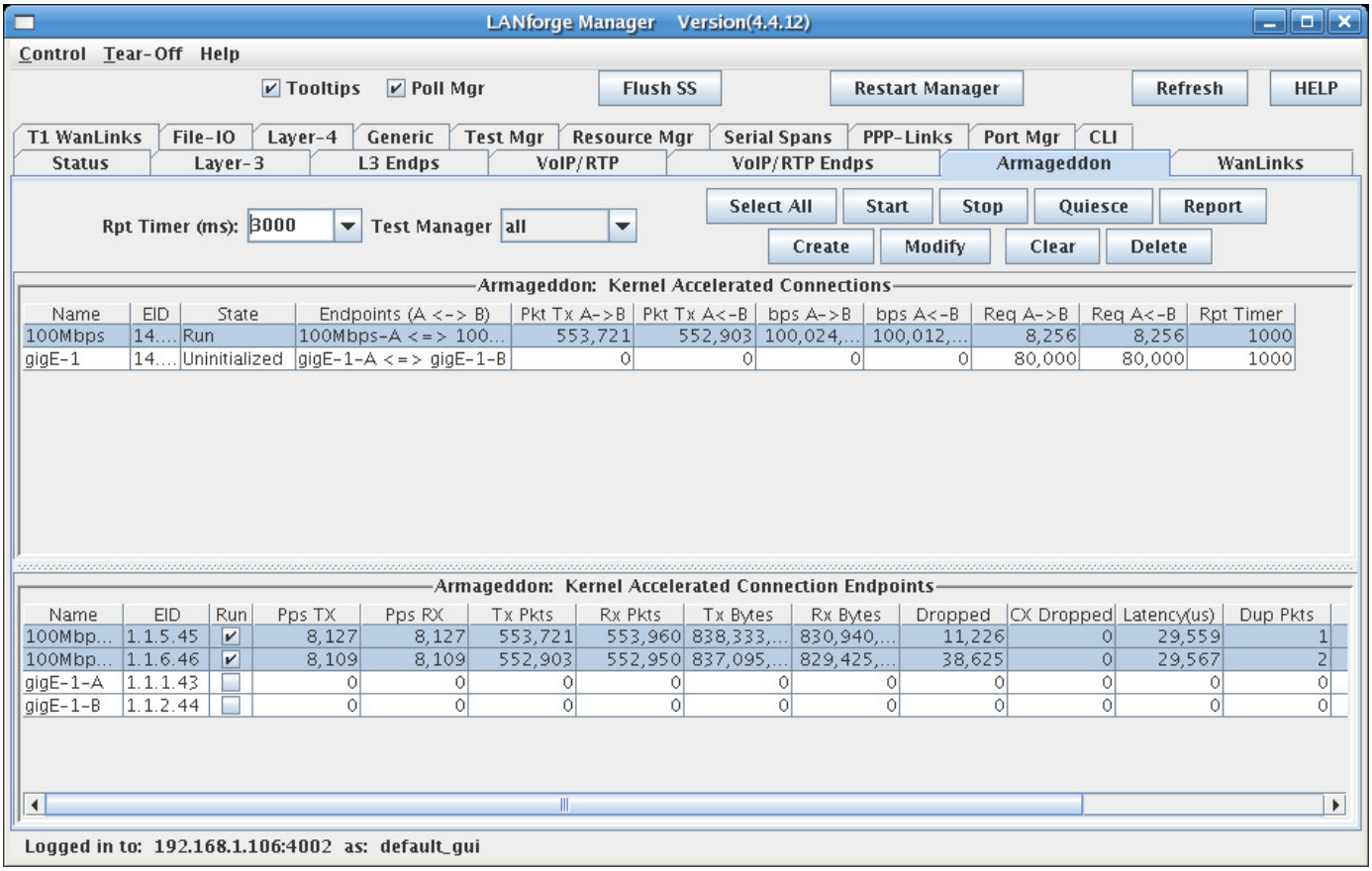


0. Armageddon (Accelerated UDP)

Armageddon Cross Connects require special Linux kernel features. If you purchased your machine from Candela, then these features will allready be included. Otherwise, you should make sure you have installed the kernel patches from Candela.

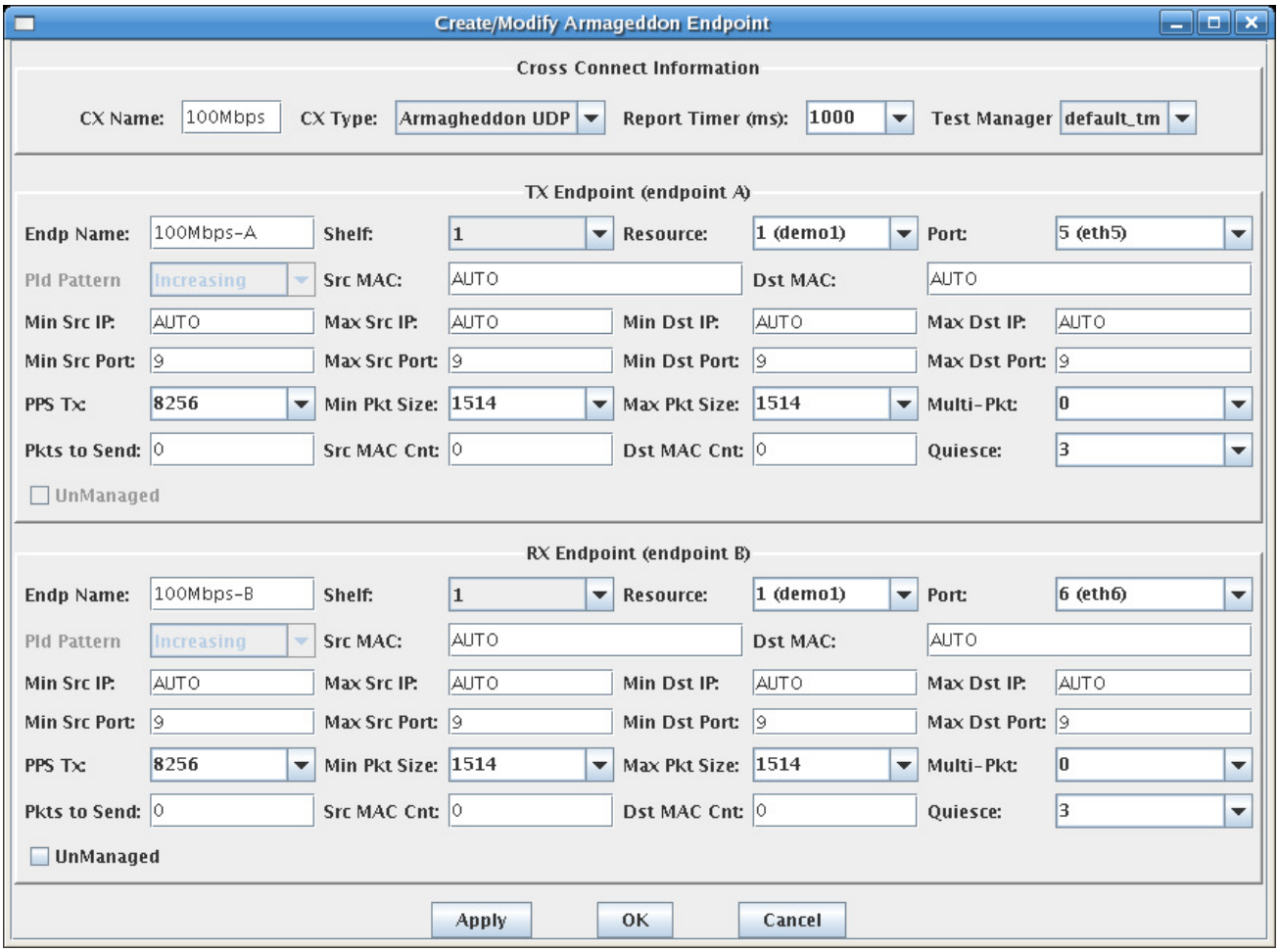
The Armageddon traffic generator can generate UDP packets with various IP and UDP header fields. More importantly, it can generate packets at line speed on 10/100Mbps and Gigabit Ethernet networks. Armageddon can also measure latency with 1 micro-second accuracy, and the sending and receiving ports can be on the same machine.

NOTE: If you are running Armageddon on a flat (non routed) network, then LANforge can figure out all the defaults for you. However, if you are running in a routed network, you will need to manually enter the MAC address of your router in the Destination MAC field of the Armageddon configuration panel.



1. Creating & Modifying Armageddon Cross Connects

When creating an Armageddon CX, you specify the details of each Endpoint, including the Shelf, Resource, and Port that the Endpoint resides on. In this way, you determine which data-generating port (which is connected to some port on the system under test) the CX's traffic will flow over. In order to create a CX, press the 'Create' button.



1. The top part of the CX Creation frame contains information relating to the entire CX, including the name, CX Type, report-timer, and the test-manager this CX should belong to. The name must be unique in the LANforge system. The CX Type determines the protocol that the CX will use. The current supported types are:

   Armageddon/UDP
   Generates and receives UDP packets. Protocol header fields will default to sane values based on the ports you select, but you can specify or randomize most fields to customize the packets that you send. For generating traffic for a routed network, you may have to over-ride the default destination MAC address with the one from your router. Currently, the payload will just be random bytes, except for a small header at the beginning of the UDP payload that LANforge uses to detect dropped and re-ordered packets.

2. The report timer specifies how often the LANforge data-generators send updates to the LANforge server, and how often the LANforge server pushes endpoint information up to the clients (GUIs) that have requested the automatic updates. If you are running the GUI over a slow link, or have a slower machine, it is recommended to increase the report timer to 5000ms (5 seconds) or higher.

3. The Test Manager specifies which test manager this CX should be added to.

4. The endpoint values are defined below.

   Endp Name
   The unique name for this endpoint. Normally, you just let this be the default value based on the CX Name.

   Shelf

The virtual 'shelf' for this endpoint. The default of 1 is the only correct answer in most configurations.

Resource
The LANforge machine that this endpoint should be associated with. Choose from the drop-down values.

Port
The network interface (real or virtual) that this endpoint should be associated with. Choose from the drop-down values.

Pld Pattern
The payload pattern is random chunks of memory, and is not currently configurable.

Src MAC
The source MAC address in the generated packets.

Dst MAC
The destination MAC address in the generated packets.

Min Src IP
The source IP address for the generated packets.

Max Src IP
The source IP address for generated packets. If this value is larger than the Min Src IP, then the generated packets will cycle through the IP address range creating traffic from each IP address.

Min Dst IP
The destination IP address for the generated packets.

Max Dst IP
The destination IP address for generated packets. If this value is larger than the Min Dst IP, then the generated packets will cycle through the IP address range creating traffic to each IP address.

Min Src Port
The source IP port for the generated packets.

Max Src Port
The source IP port for generated packets. If this value is larger than the Min Src Port, then the generated packets will cycle through the IP port range creating traffic from all IP ports.

Min Dst Port
The destination IP port for the generated packets.

Max Dst Port
The destination IP port for generated packets. If this value is larger than the Min Src Port, then the generated packets will cycle through the IP port range creating traffic to all IP ports.

PPS Tx
The desired packets-per-second to transmit. If the hardware/network cannot actually run at this speed, it will run as fast as it is able.

Min Pkt Size
The minimum packet size. This includes all ethernet headers, but does NOT include the 4 byte CRC at the end of the ethernet frame. The reported bits-per-second and bytes received WILL take the 4 byte CRC into account.

Max Pkt Size
The maximum packet size. This includes all ethernet headers, but does NOT include the 4 byte CRC at the end of the ethernet frame. If this value is larger than the Min Pkt Size, each new packet will have a random size between min and max, in a random distribution.

Multi-Pkt
This setting determines the number of times the exact same packet will be transmitted before a new one is created. Setting this value to greater than one can increase performance of the LANforge machine, but it will decrease the chance of detecting out-of-order packets. This is not usually a problem. When using

Armageddon on virtual interfaces, such as MAC-VLANs and 802.1Q VLANs, this value must be 0 due to internal driver limitations.

Pkts to Send

This specifies the number of packets to send before stopping the test. Set this value to zero to have the test run until stopped by the user.

Src MAC Cnt

If this value is greater than 1, the source MAC address will be incremented through the specified range. This allows the test to create packets from what appears to be many different ethernet NICs and can be good for stress-testing ethernet switches and other types of equipment that attempt to detect and optimize for network flows.

Dst MAC Cnt

If this value is greater than 1, the destination MAC address will be incremented through the specified range. This allows the test to create packets to what appears to be many different ethernet NICs and can be good for stress-testing ethernet switches and other types of equipment that attempt to detect and optimize for network flows.

Quiesce

Instead of stopping the receiving and transmitting endpoints, Quiesce will stop the transmitting endpoint and wait a prescribed number of seconds before stopping the receiving endpoint so that all transactions may be completed.

1. WanLinks (ICE)

WanLinks support the WAN/Network emulation feature (also called LANforge ICE). In the default configuration, two interfaces will act like a transparent layer-2 ethernet bridge. As traffic flows through this bridge, the WAN emulation is applied. The WanLinks are able to add various characteristics to the traffic flowing through them, including maximum-bandwidth, latency, jitter, jitter-frequency, dropped-packets, duplicated-packets, reordered-packets, bit & byte errors, and more! Each WanLink is composed of two WanLink Endpoints that represent one of the sides of the WAN simulation.

Overview of WanLink Configuration

A WanLink emulates a bridged Ethernet network with characteristics determined by the user. Packets are received in one Ethernet (or virtual) interface and are transmitted out the other interface. This means that when you add the LANforge machine to an existing network configuration, no routing changes are needed. When designing your network, you can think of a pair of WanLink ports as an ethernet switch or even just a pass-through cable! WanLinks can bridge 802.1Q VLAN interfaces as well.

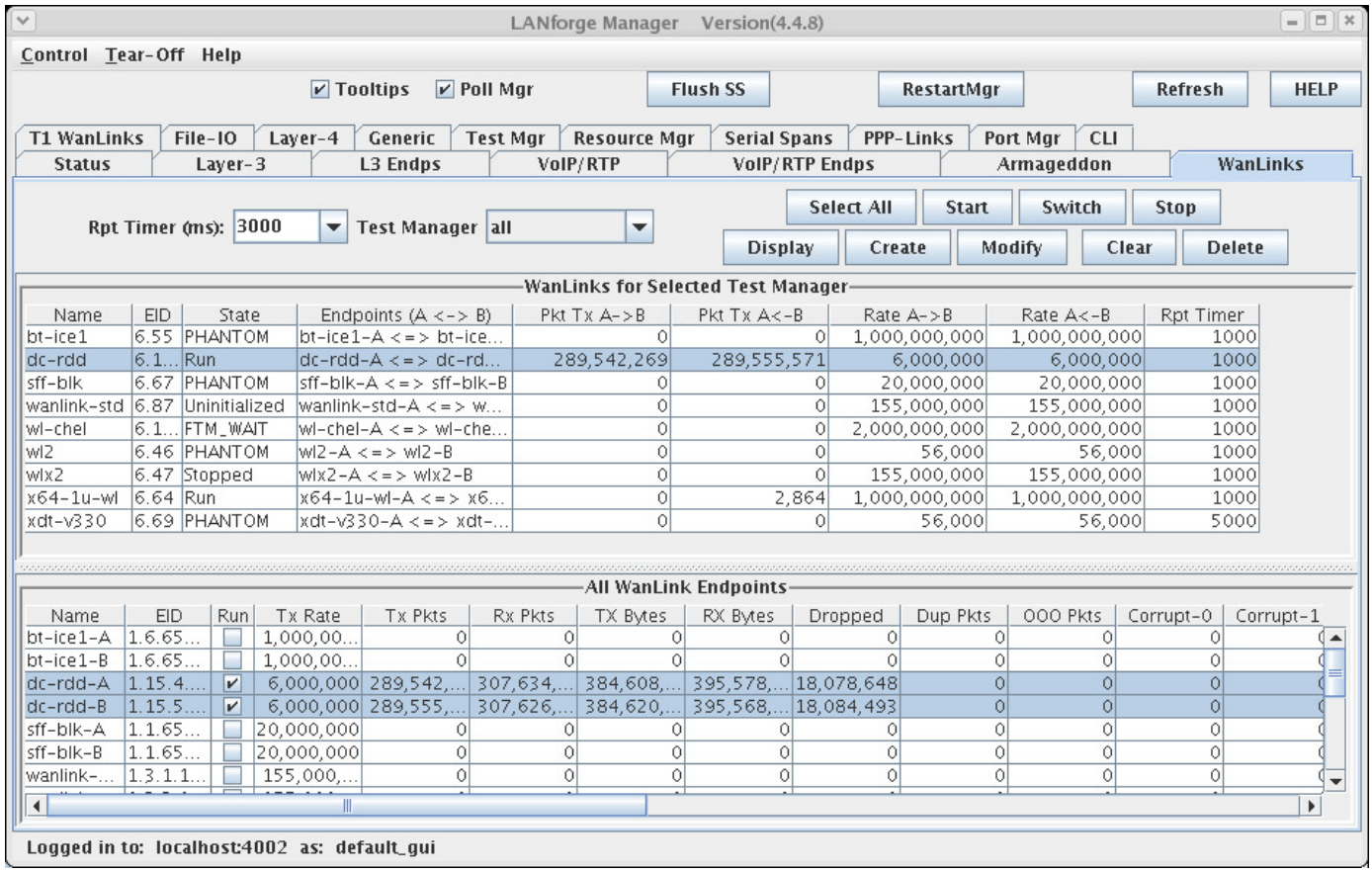
As of release 5.0.1, LANforge-ICE supports multiple virtual routers per system when LANforge is running on Linux. On Windows, only bridge-mode is supported. To configure LANforge-ICE in routed mode, the easiest way is to use the Netsmith tool, described here. If you are running an older release of LANforge, then you can configure simple routing in the method described below. Much of this is now done for you automatically with release 5.0.1, but the basic use of pairs of redirect devices is still used.

To configure LANforge ICE (version 4.2.9 - 4.4.12) as a router, you will need to create one or more pairs of a special virtual device called a 'Redirect-Device'. You can create these on the Port-Mgr tab of the LANforge-GUI. For instance, if you want to emulate a WAN connection on the ethernet interface eth1 and another on eth2, you can follow these steps:

- Create a pair of Redirect-devices called: rdd0 and rdd1 on the Port-Mgr tab.
- Create a pair of Redirect-devices called: rdd2 and rdd3 on the Port-Mgr tab.
- Assign the IP address that you would normally associate with eth1 to rdd1
- Assign the IP address that you would normally associate with eth2 to rdd3
- Create a WanLink that uses port eth1 and rdd0 for the ports (see below)
- Create a WanLink that uses port eth2 and rdd2 for the ports (see below)

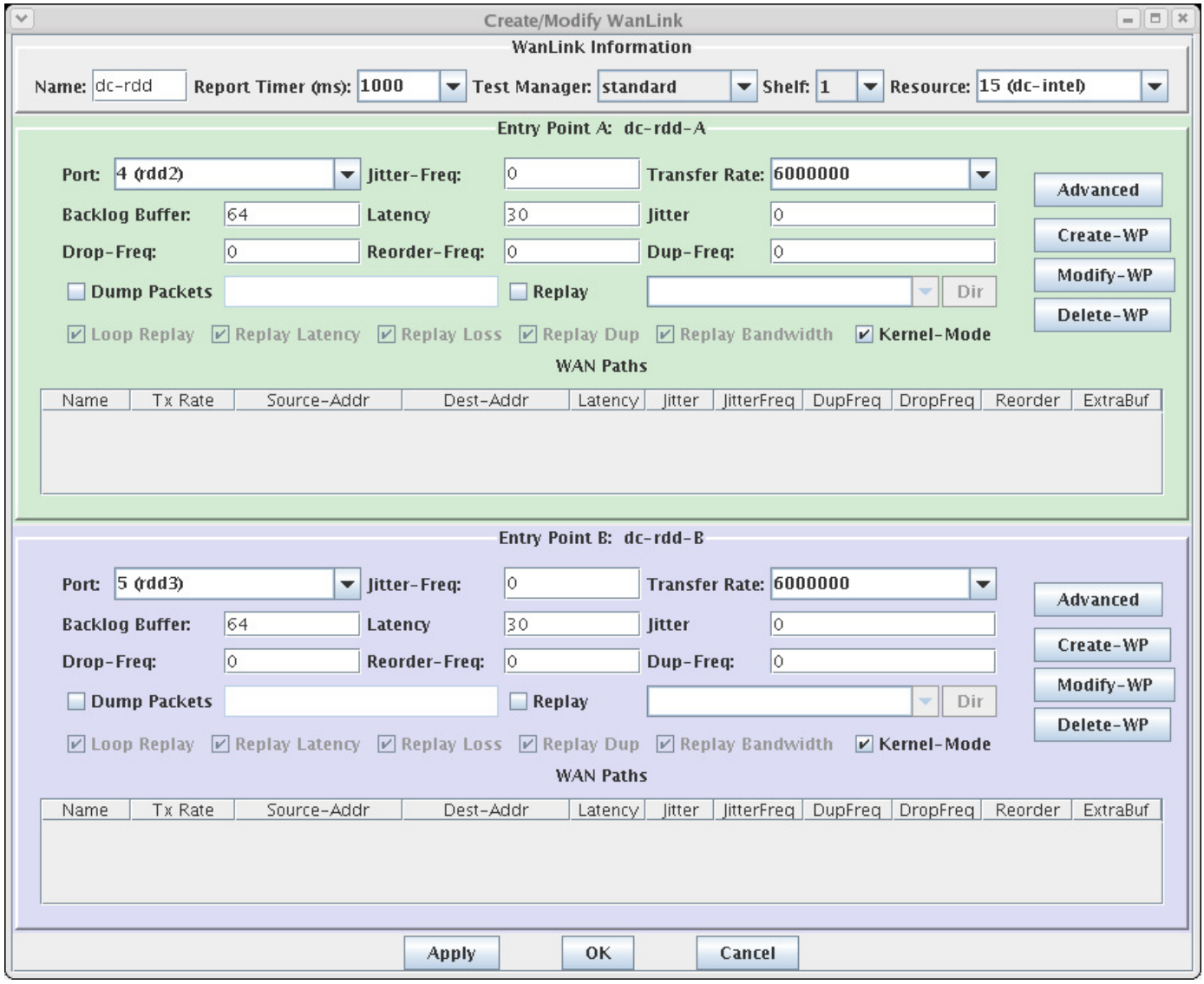
Now, when a device sends a packet to the IP address of rdd1 through physical interface eth1, the WanLink associated with eth1 and rdd0 will apply the specified WAN emulation. The LANforge machine will use the normal Linux routing rules to forward the packet destined for rdd1 to whatever other interface the routing tables select. If that happens to be rdd3, then the packet will leave through the second WanLink on eth2 and rdd2, and will have those WAN emulation values applied on that traversal as well.

To ensure that there is no interaction with the LANforge machine's protocol stacks, the IP address is removed from each WanLink port. To access the LANforge machine for management purposes, you should use a third management port. It is possible to run WanLinks on a machine with only two ports, but you will not be able to manage the machine remotely because there will be no management port. This can be useful when using an interface-constrained platform such as a Laptop.


LANforge Manager Version(4.4.8)
Control Tear-Off Help
Tooltips
Poll Mgr
Flush SS
RestartMgr
Refresh
HELP
T1 WanLinks
File-IO
Layer-4
Generic
Test Mgr
Resource Mgr
Serial Spans
PPP-Links
Port Mgr
CLI
Status
Layer-3
L3 Endps
VoIP/RTP
VoIP/RTP Endps
Armageddon
WanLinks
Rpt Timer (ms): 3000
Test Manager all
Select All
Start
Switch
Stop
Display
Create
Modify
Clear
Delete
WanLinks for Selected Test Manager
Name EID State Endpoints (A <-> B) Pkt Tx A->B Pkt Tx A<-B Rate A->B Rate A<-B Rpt Timer
bt-ice1 6.55 PHANTOM bt-ice1-A <=> bt-ice... 0 0 1,000,000,000 1,000,000,000 1000
dc-rdd 6.1... Run dc-rdd-A <=> dc-rd... 289,542,269 289,555,571 6,000,000 6,000,000 1000
sff-blk 6.67 PHANTOM sff-blk-A <=> sff-blk-B 0 0 20,000,000 20,000,000 1000
wanlink-std 6.87 Uninitialized wanlink-std-A <=> w... 0 0 155,000,000 155,000,000 1000
wl-chel 6.1... FTM_WAIT wl-chel-A <=> wl-che... 0 0 2,000,000,000 2,000,000,000 1000
wl2 6.46 PHANTOM wl2-A <=> wl2-B 0 0 56,000 56,000 1000
wlx2 6.47 Stopped wlx2-A <=> wlx2-B 0 0 155,000,000 155,000,000 1000
x64-1u-wl 6.64 Run x64-1u-wl-A <=> x6... 0 2,864 1,000,000,000 1,000,000,000 1000
xdt-v330 6.69 PHANTOM xdt-v330-A <=> xdt-... 0 0 56,000 56,000 5000
All WanLink Endpoints
Name EID Run Tx Rate Tx Pkts Rx Pkts TX Bytes RX Bytes Dropped Dup Pkts OOO Pkts Corrupt-0 Corrupt-1
bt-ice1-A 1.6.65... 1,000,00... 0 0 0 0 0 0 0 0 0
bt-ice1-B 1.6.65... 1,000,00... 0 0 0 0 0 0 0 0 0
dc-rdd-A 1.15.4.... 6,000,000 289,542,... 307,634,... 384,608,... 395,578,... 18,078,648 0 0 0
dc-rdd-B 1.15.5.... 6,000,000 289,555,... 307,626,... 384,620,... 395,568,... 18,084,493 0 0 0
sff-blk-A 1.1.65... 20,000,000 0 0 0 0 0 0 0 0 0
sff-blk-B 1.1.65... 20,000,000 0 0 0 0 0 0 0 0 0
wanlink-... 1.3.1.1... 155,000,... 0 0 0 0 0 0 0 0 0
Logged in to: localhost:4002 as: default_gui

Creating & Modifying WanLinks

When creating a WanLink, you specify the details of each WanLink Endpoint, including the Port that the WanLink Endpoint resides on. In this way, you determine which ethernet port (which is connected to some port on the system under test) the WanLink will accept traffic on. In order to create a WanLink, press the 'Create' button on the "WanLinks" panel. WanLinks can be attached to physical ethernet interfaces and 802.1Q VLAN interfaces. WanLinks should NOT be attached to MAC-VLAN, 802.11a/b/g, or PPP interfaces at this time.



1. The top part of the WanLink Creation frame contains information relating to the entire WanLink, including the name, report-timer, and the test-manager this WanLink should belong to. You also select the Shelf and Resource that the WanLink will reside on. For LANforge ICE systems with only one machine, you do not need to change these values from their default of one (1).

2. The report timer specifies how often the LANforge data-generators send updates to the LANforge server, and how often the LANforge server pushes endpoint information up to the clients (GUIs) that have requested the automatic updates. If you are running the GUI over a slow link, or have a slower machine, it is recommended to increase the report timer to 5000ms (5 seconds) or higher.

3. The Test Manager specifies which test manager this CX should be added to.

4. The WanLink Endpoints entries should be fairly self explanatory, and are described in detail below.
   Port
   The external ethernet interface this Entry Point resides on. Ports used in WanLinks should have their IP address, MASK, and Gateway set to **0.0.0.0** at least when the WanLink is running. LANforge will forcefully set the IP to 0.0.0.0 as soon as you start the WanLink.

Jitter Frequency

This determines how often we will randomly apply jitter to packets flowing through this WanLink. The units are X per million. So, if you wanted about 1 out of every 100 packets to have jitter applied to them, you would enter 10000 here. Please see the Jitter section as well.

Transfer Rate

How much data will this Entry Point accept per second.

Backlog Buffer

Most (and all good) equipment that you will find in a Wide-Area-Network will contain a certain amount of buffers to smooth bursty traffic so that packets are not needlessly dropped. The backlog buffer is your way of configuring this value. The units are in 1024 bytes (1KB). The size of the buffer depends on many things, and should generally be bigger for higher-speed simulations. Due to the bursty nature of Ethernet (and ethernet drivers in common systems), we suggest these buffer sizes when trying to simulate a relatively well architected WAN:

WanLink Speed	Backlog Buffer Size
56Kbps - 256Kbps	4-16
257Kbps - 1.54Mbps	16-128
1.5Mbps - 45Mbps	128-512
45Mbps - 155Mbps	512-2048
155Mbps - 1Gbps	2048-8192

Latency

How much latency (in milliseconds) will be added to each packet as it enters this Entry Point.

Jitter

How much random jitter will be added to each packet as it enters this Entry Point. This will be a random value between 0 and the value entered here. It will not cause any packet re-ordering. Please see the Jitter-Frequency setting as well.

Drop Frequency

How many packets out of every 1 million (1,000,000) will we purposefully drop. This is used to simulate errors on the WAN.

Reorder Frequency

How many packets out of every 1 million (1,000,000) will we purposefully re-order. You can configure the min and max reorder offset in the 'Advanced' configuration screen. This is used to simulate behaviour that you will see in multi-path networks and is good for testing RTP and other streaming protocols.

Dup Frequency

How many packets out of every 1 million (1,000,000) will we purposefully duplicate. This will cause the other side of the simulated WAN to receive two identical packets. This is used to simulate errors on the WAN.

Dump Packets

If selected, then all packets received will be logged to the specified file. They can later be replayed with a LANforge FIRE custom-ethernet connection. This allows the capture and replay of packet flows and protocols that exactly fit your environment.

Replay

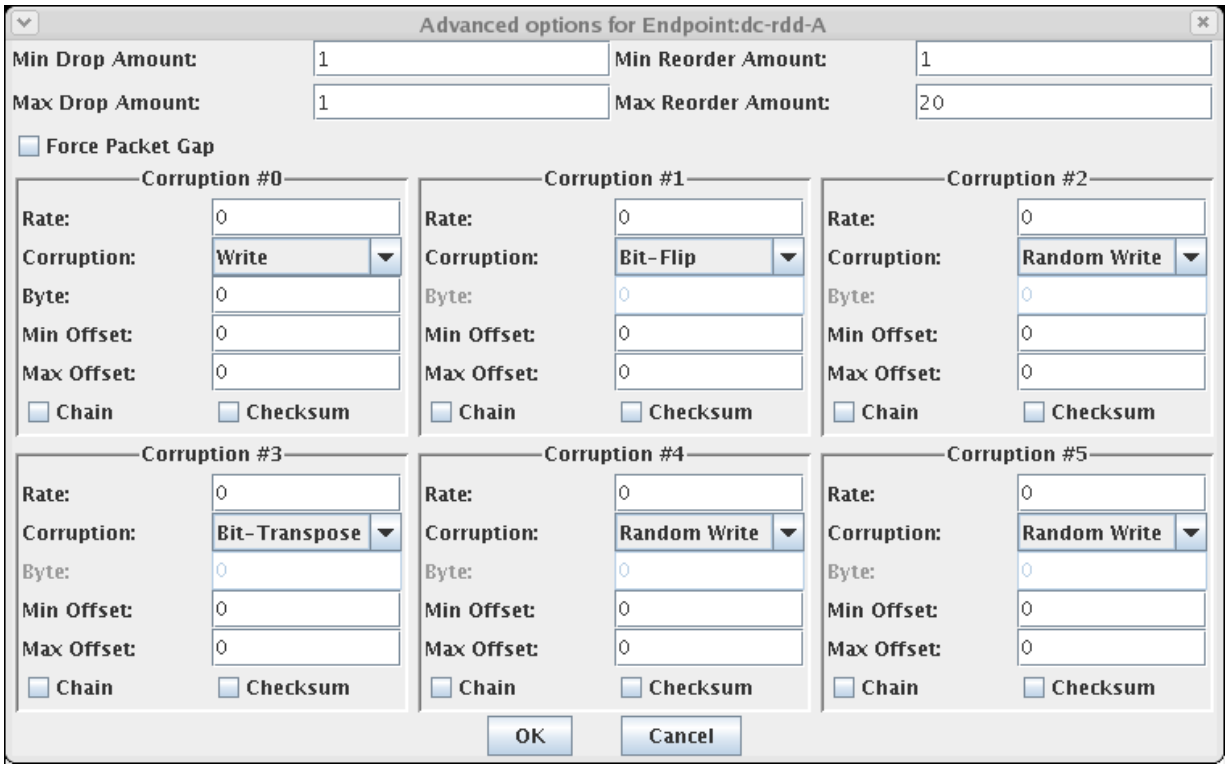
If selected, then the LANforge ICE connection will read values from an XML file and change it's values accordingly. The XML file consists of periodic samples of network characteristics. The WAN capture file can be created by the LANforge ICE-Cap tool (included free of charge). The 'Loop Replay', 'Replay Latency', 'Replay Loss' and 'Replay Bandwidth' flags pertain to this feature and determine the behaviour described by the XML file. Please note that this does not directly relate to the 'Dump Packets' feature.

Kernel Mode

If you are using a pre-compiled Linux kernel from the Candela downloads page, then you can use Kernel Mode for the WAN emulation. Kernel mode allows much higher emulation speeds and supports all features of the normal WAN emulation mode. Kernel Mode must be selected on both or neither endpoints, and may be changed only when the endpoints are stopped.

Advanced Configuration

You can use the advanced configuration window to configure LANforge to drop bursts of packets, modify the reordering behaviour, introduce bit & byte errors, and to enforce minimum packet gaps:



To create bursts of dropped packets, set the min and/or max packet drop to some value greater than 1. At each drop event (randomly selected based on the drop-per-million on the main config screen), a random number of packets between min and max (inclusive) will be dropped.

The reorder amount gives you the ability to specify how many packets will be allowed to go by before the reordered packet is re-inserted into the stream.

If the Force Packet Gap checkbox is selected, a packet gap of at least 80% of the theoretical will be enforced between every packet. The 80% allows for the system to make up for internal processing overhead. Enabling this feature can cause significant performance degradation at speeds of greater than about 2Mbps.

With release 4.4.8, LANforge ICE supports bit and byte error corruptions in ethernet frames. The **Rate** field determines how often to apply the corruption, out of 1 million. The **Corruption** drop-down lets you specify what type of corruption you want to apply.

- **Random Write:** Will write a random byte to one byte between the min and max offset into the ethernet frame.
- **Write:** Will write the byte specified in the Byte field to a location between the min and max offset into the ethernet frame.
- **Bit Flip:** Will flip one bit from 0 to 1 or 1 to zero in a byte between the min and max offset into the ethernet frame.
- **Bit Transpose:** Will transpose two bits in a byte between the min and max offset into the ethernet frame.

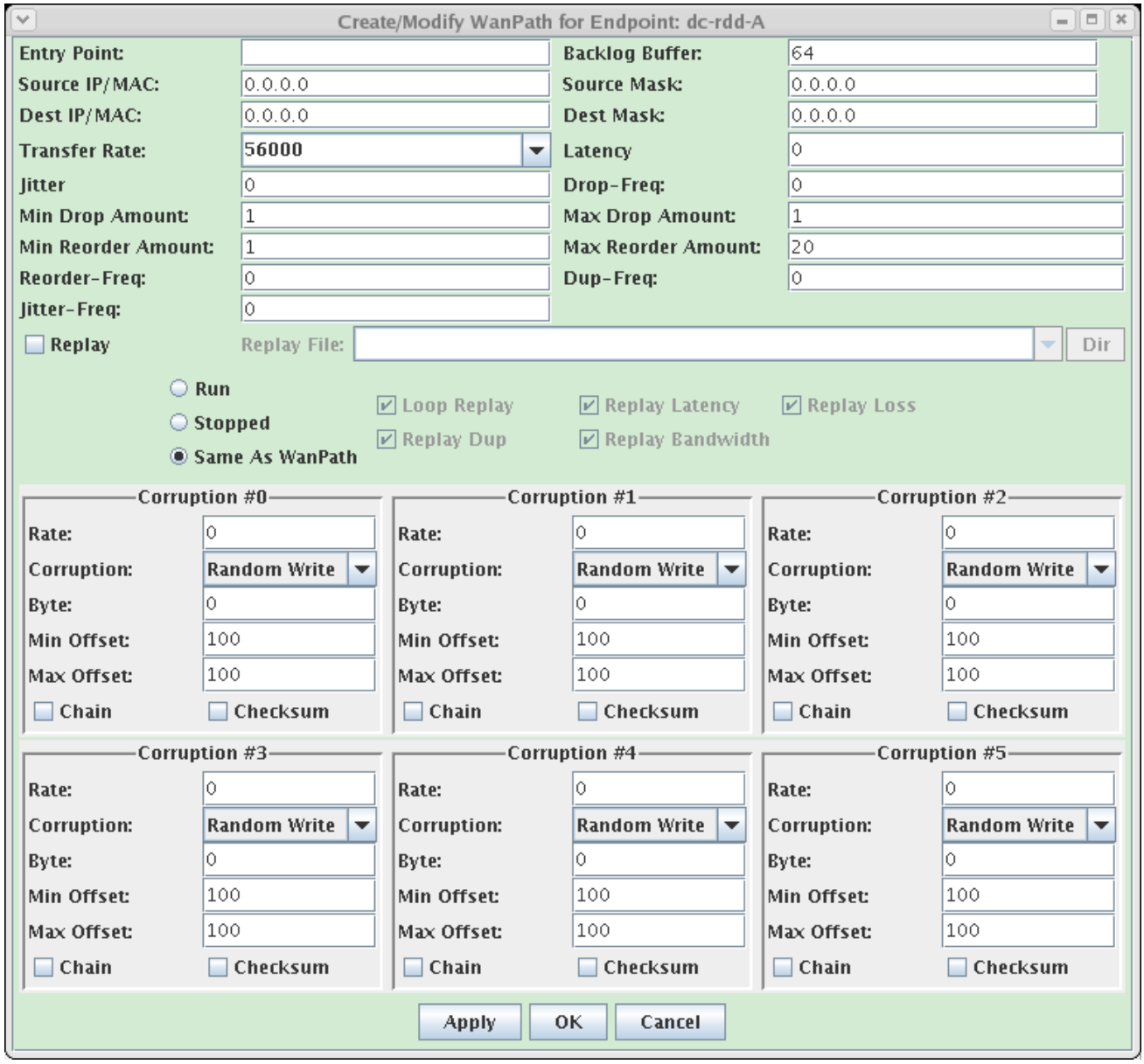
The **Min and Max Offset** fields determine the location of the corruption. If Min is less than Max, the corruption will be at a random byte between min and max.

If the **Chain** flag is selected, any time this corruption is applied, the next corruption will be applied as well. This can allow you to reliably generate multiple corruptions in a single packet.

If the **Checksum** flag is selected, LANforge will attempt to recalculate the IP, UDP, and TCP checksum for the packet after applying the corruption. This will allow the errored packet to be accepted by the stacks on the receiving machine as if the data were actually valid. This feature will only work if the UDP or TCP payload does not span more than one physical ethernet frame.

5. WanPaths represent a virtual WAN between a source and destination IP or MAC Address range. This allows you to set up one WanLink that simulates a physical pipe, and multiple WanPaths that simulate connections between different machines or sets of machines on your network. You can have up to 128 WanPaths on each WanLink endpoint.

   The configuration of a WanPath is similar to that of a WanLink, except that the WanPath belongs to a specific WanLink, and you must specify the IP Address ranges that are to match this WanLink. **Please note that when you add a WanPath to an endpoint, the patterns match with regard to packets entering the interface that the endpoint uses. If you want to match on a source IP of 192.1.1.2 and the endpoint is configured on eth0, then put that machine on the network connected to eth0.**



Entry Point
The name of this particular WanPath. Must be unique across the parent WanLink.

Source IP/MAC
The Source IP or MAC address that matches this WanPath. If using IP address matching, the number of bits that are matched are controlled by the Source IP Mask. If using MAC address matching, any non-zero mask will match exactly, and a zero mask will match all.

Source Mask
Specifies how many bits of the Source IP are significant. If this is 0.0.0.0 it will match anything. You can also enter an integer number between zero and 32, inclusive. For MAC addresses, 0 means 'ANY' and anything else means match exactly the single MAC.

Dest IP/MAC

The Destination IP or MAC that matches this WanPath. If using IP address matching, the number of bits that are matched are controlled by the Source IP Mask. If using MAC address matching, any non-zero mask will match exactly, and a zero mask will match all.

Destination Mask

Specifies how many bits of the Destination IP are significant. If this is 0.0.0.0 or 0 it will match anything. You can also enter an integer number between zero and 32, inclusive. If using MAC address matching, any non-zero mask will match exactly, and a zero mask will match all.

Replay

If checked, then the LANforge ICE connection will read values from an XML file and change it's values accordingly. The XML file consists of periodic samples of network characteristics. The WAN capture file can be created with scripts or third-party applications. Contact Candela for more information on how to generate these scripts. The remaining flags pertain to this feature and determine the behaviour described by the XML file.

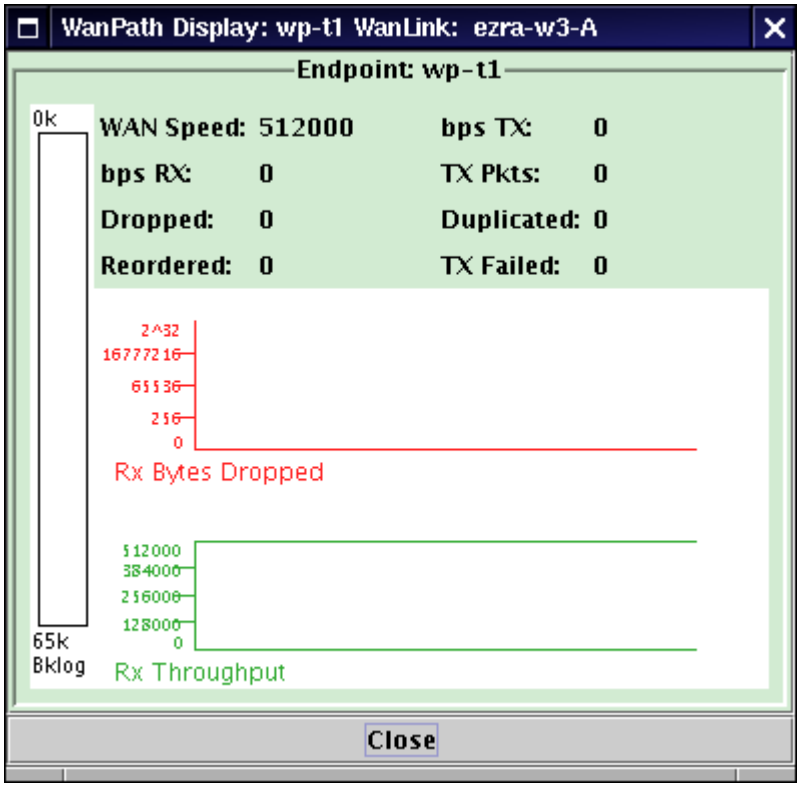
Running State

If the 'Same as WanPath' state is selected, the WanPath will be active when the WanLink is active. If 'Stopped' is selected, the WanPath will not be active, and all traffic will be handled as if the WanPath does not exist.

Displaying WanLinks and WanPaths

After creating a WanLink, you may display it to watch the flow across your emulated WAN in detail. To display one or more WanLinks, select the row(s) and press the 'Display' button.

You can also display individual WanPaths:



WanLink Endpoints (ICE)

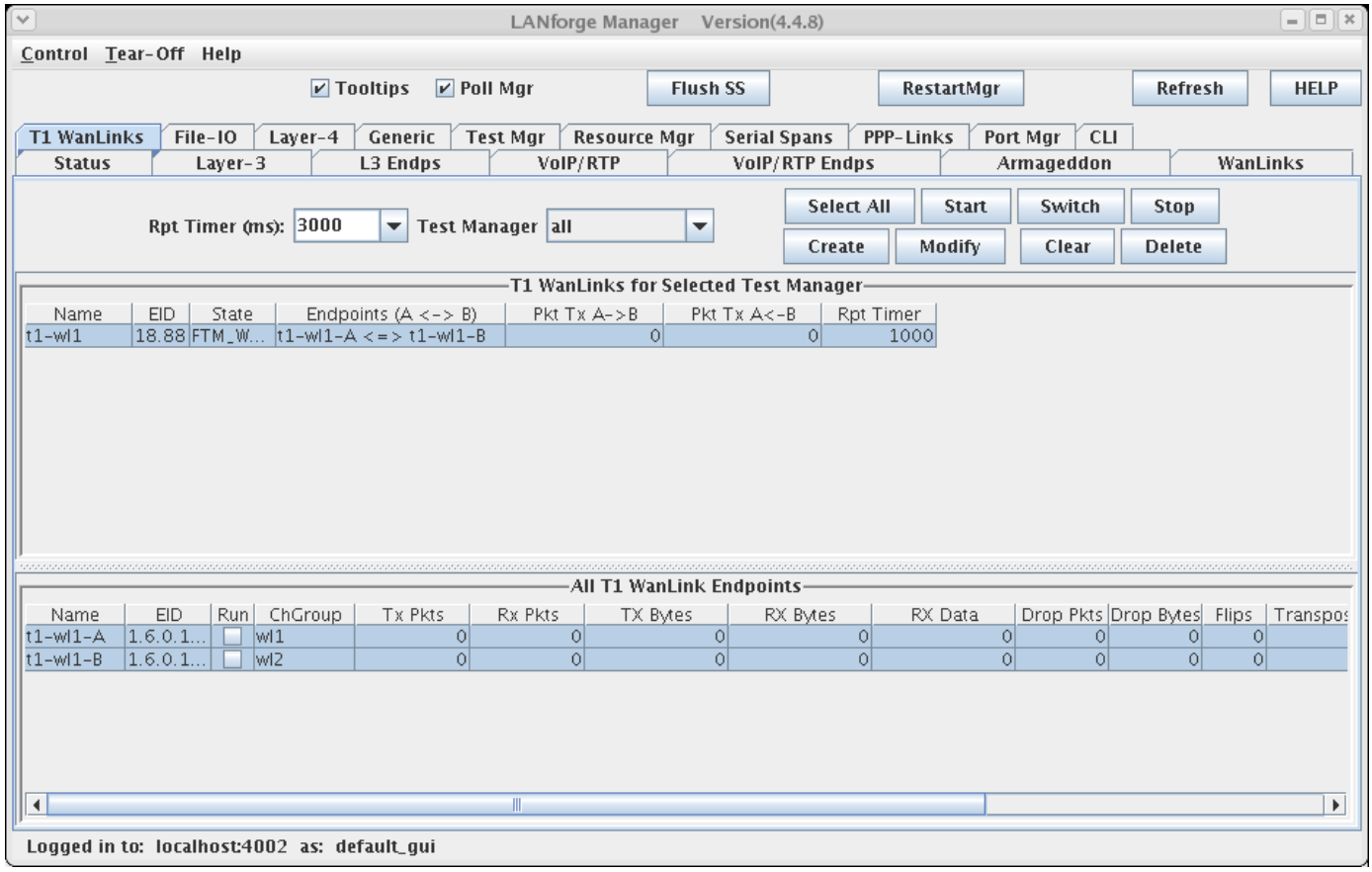
You can see the fine details of each WanLink Endpoint in the WanLink-Endpoint table. If you select a particular WanLink by single-clicking on its row, then you can see the WanLink Endpoints for that WanLink highlighted as well.

2. T1/E1 WanLinks (ICE)

After properly configuring your Serial Spans and Channel Groups, you can add T1 WanLinks, which make two T1 or E1 ports (interfaces) appear as two ends of a Wide-Area-Network (WAN). The T1 WanLinks are able to add latency, bit-flip errors and bit-transpose errors. Each WanLink is composed of two WanLink Endpoints that represent one of the sides of the WAN simulation.

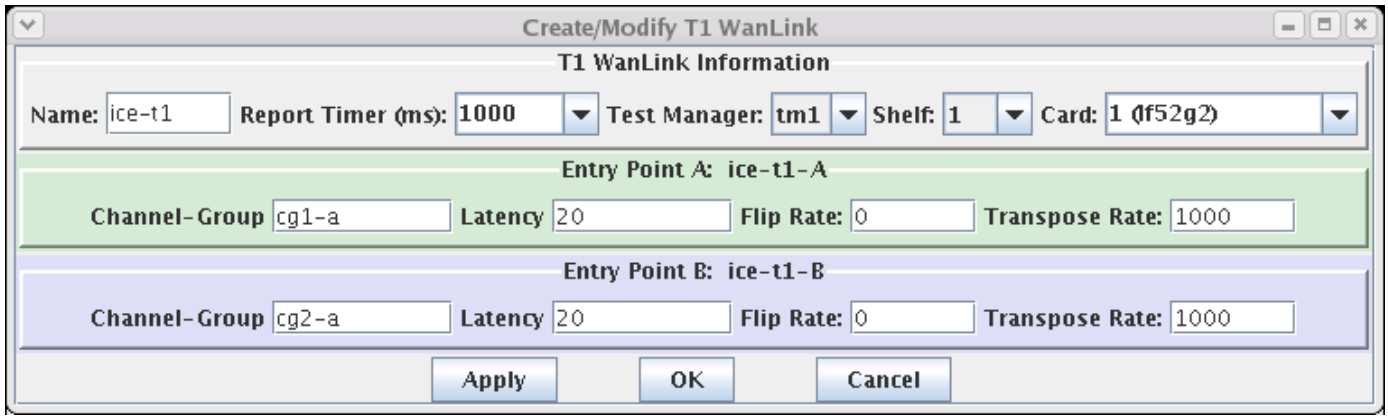
Overview of T1/E1 WanLink Configuration

A T1 WanLink emulates a T1 network with latency and bit-errors defined by the user. Bytes are received in one T1 interface and are transmitted out the other interface. All T1 channels are bridged at the same time, and all bytes (including idle bytes) are transmitted as received. It is possible for the LANforge system to become congested or over-worked, and in this case, a certain number of bytes may be dropped. If this happens, a counter is incremented and displayed in the LANforge-GUI.



Creating & Modifying T1/E1 WanLinks

When creating a WanLink, you specify the details of each WanLink Endpoint, including the Channel-Group (which is in turn associated with a particular T1/E1 Span) that the WanLink Endpoint resides on. Please see the Serial Spans section for help on creating Channel Groups. In order to create a T1 WanLink, press the 'Create' button on the "T1 WanLinks" panel.



1. The top part of the T1 WanLink Creation frame contains information relating to the entire T1 WanLink, including the name, report-timer, and the test-manager this T1 WanLink should belong to. You also select the Shelf and Resource that the T1 WanLink will reside on. For LANforge configurations with only one machine, you do not need to change these values from their default of one (1).

2. The report timer specifies how often the LANforge data-generators send updates to the LANforge server, and how often the LANforge server pushes endpoint information up to the clients (GUIs) that have requested the automatic updates. If you are running the GUI over a slow link, or have a slower machine, it is recommended to increase the report timer to 5000ms (5 seconds) or higher.

3. The Test Manager specifies which test manager this CX should be added to.

4. The WanLink Endpoints entries should be fairly self explanatory, and are described in detail below.
   Channel Group
   The T1/E1 channel-group this Entry Point resides on. Channel-groups used for T1 WanLinks MUST be configured to use 'ALL' channels on the span. For best latency accuracy, use a smaller MTU (192 is suggested.)

   Latency
   How much latency (in milliseconds) will be added to traffic entering this Entry Point.

   Flip Rate
   How many bits, per billion, should be randomly flipped. (A flipped bit goes from 0 to 1 or 1 to 0.

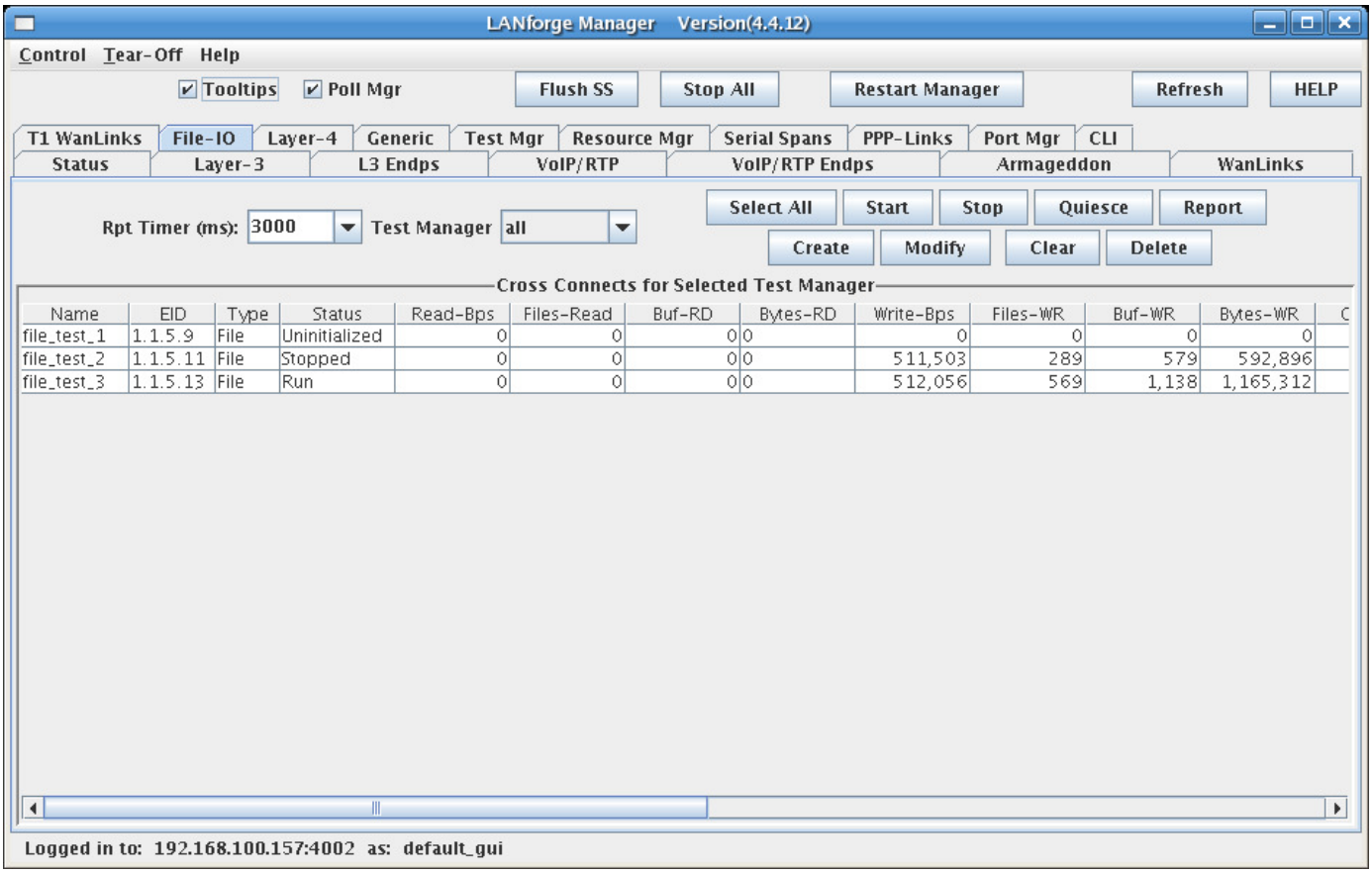
   Transpose Rate
   How many bits, per billion, should be randomly transposed. (A transposed bit exchanges the value with it's neighbour.)

T1/E1 WanLink Endpoints (ICE)

You can see the fine details of each T1 WanLink Endpoint in the T1 WanLink-Endpoint table. If you select a particular T1 WanLink by single-clicking on its row, then you can see the T1 WanLink Endpoints for that T1 WanLink highlighted as well.

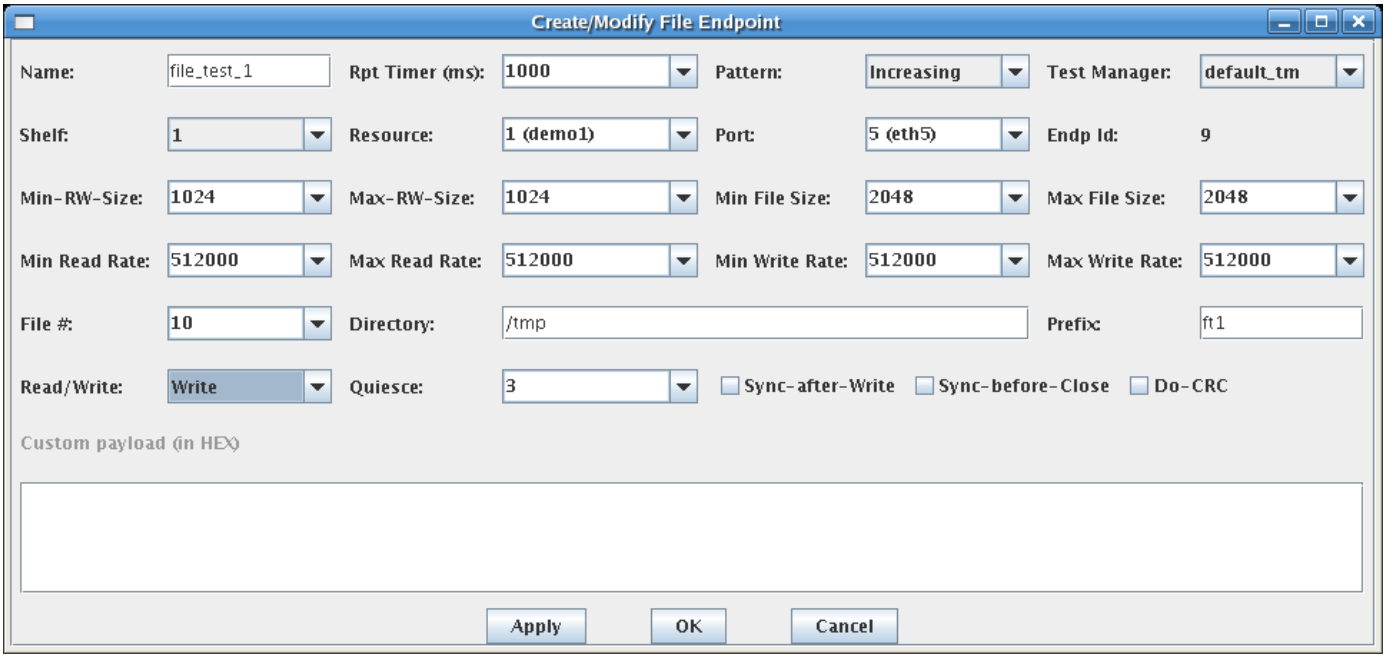
3. File Endpoints

File Endpoints are used to generate file system traffic. If you happen to configure LANforge to have file systems mounted over NFS, iSCSI, or SMB (SAMBA), then the file system tests will indirectly produce network traffic as well. A file endpoint is synonymous with a File cross-connect, because LANforge only controls or manages a single side. The other side may be the local file system, or a remote NFS server: It makes no difference to the LANforge software suite's configuration.



Creating & Modifying File Endpoints

When creating a File Endpoint, you get to specify attributes such as file size, how many files, read vs. write, chunk-size to read/write and some options relating to synchnonizing (flushing) the files to disk. A File Endpoint is a complete test by itself (you do not directly create File Cross-Connects, as you do with some other endpoint types.) In order to create a File Endpoint, press the 'Create' button on the "File-IO" panel.



Name

The name specifies the name for this File Endpoint.

Report Timer

The Report Timer is how often (in millisecond units) the endpoint reports to the GUI. 1000-5000 (1-5 seconds) is suggested for most cases.

Pattern

The pattern relates to the data that will be written to the disk. If you are using the check-sum feature, then there will also be a small header written to disk before the payload so we can do verification checks when reading.

Shelf, Resource, Port, Endpoint ID

The shelf and resource determine which machine the test will run on. The port does not make any difference at this time, but in the future may help with directing network traffic to a particular interface. The endpoint-ID is for display only, and gives the unique identifier for this endpoint.

Min-RW-Size, Max-RW-Size

The Min-RW-Size and Max-RW-Size specify the minimum and maximum read or write (depending on the mode) size in bytes for each call to the system read and/or write calls. Larger read/write sizes will give more throughput, smaller ones may stress the system harder in certain other ways. If the min and max are different, LANforge will randomly pick values between the min and max values.

Min File Size, Max File Size

The Min File Size and Max File Size specify the minimum and maximum file size in bytes only when writing. When reading, LANforge will read any size file in the specified directory.

Min Read Rate, Max Read Rate

The min and max read rate specify how fast the Endpoint will attempt to read the file(s). If the values are not the same, LANforge will randomly pick values between the min and max rate. The picked value will be used for a short (random) amount of time to simulate burstiness.

Min Write Rate, Max Write Rate

The min and max write rate specify how fast the Endpoint will attempt to write the file(s). If the values are not the same, LANforge will randomly pick values between the min and max rate. The picked value will be used for a short (random) amount of time to simulate burstiness.

File #

The number of files to create when doing the write tests. LANforge will continiously write data, but will re-use the files. For instance, if you chose to use 10 files, and let a File Endpoint run for long enough to write 15 files, then there will be 10 files in your directory, and 5 of them will have been written over once with new data.

Directory

The directory chooses the place the files will be written to, or read from. When writing, if the directory does not yet exist, LANforge will create it. When reading, LANforge will not read from a non-existent directory.

Prefix

The prefix may be used to distinguish files written for multiple endpoints. The prefix will be prepended to any file created for writing.

Read/Write

The Read/Write selection box allows you to select whether the endpoint is reading or writing. You can change at any time, but it can only be in one state or the other. To do simultaneous reads and writes, create two separate File Endpoints.

Quiesce

The Quiesce selection box allows you to set the number of seconds LANforge will wait to finish reading or writing the next file before stopping the File Endpoint. If the quiesce timer expires before the read or write is complete, the File Endpoint is stopped.

Sync-after-Write, Sync-before-Close

The Sync-after-Write checkbox determines whether or not the fsync method will be called after every write. This really slows down performance, but may be perfect for some types of tests. The sync-before-close does the fsync call right before a file is to be closed. This isn't as much of a performance killer as the sync-after-write, but it can still slow things down. It does simulate some real world tools, such as Mail Transfer Agents (MTAs), such as Sendmail.

Do-CRC

The Do-CRC checkbox allows you to tell the Endpoint to do a 32-bit CRC (checksum) on the payload and header being written to disk. If you read this with a File Endpoint that is also doing a CRC check, it will detect, with great certainty, any corruption in the file.

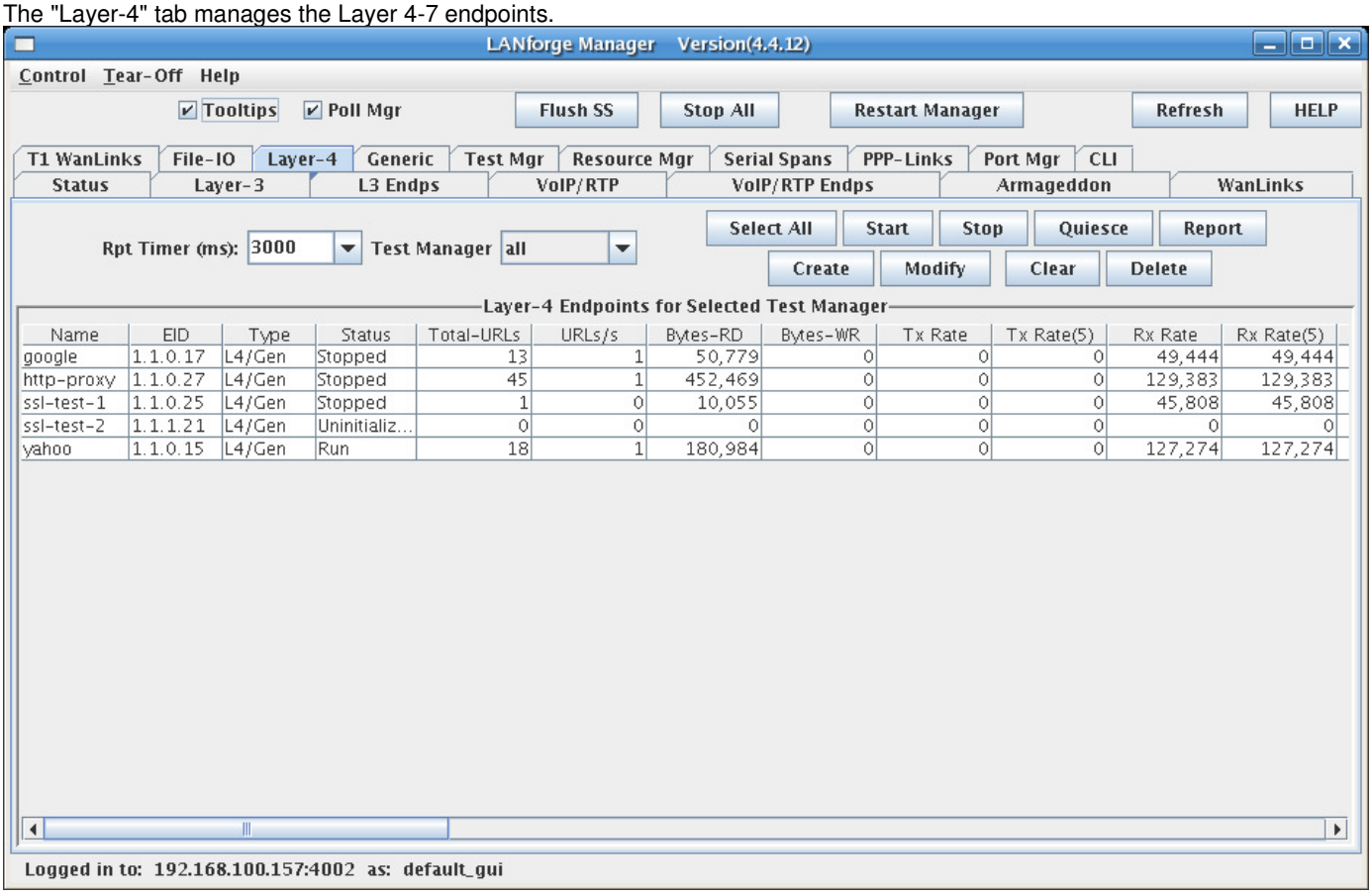
Custom Payload

If you are using a custom payload, then you can specify the payload (up to 2048 bytes) in HEX in the edit box provided. This pattern will be written to disk as entered, except that it will be prepended with the FileEndpoint header.

4. Layer 4-7 Endpoints (FTP, HTTP, ...)

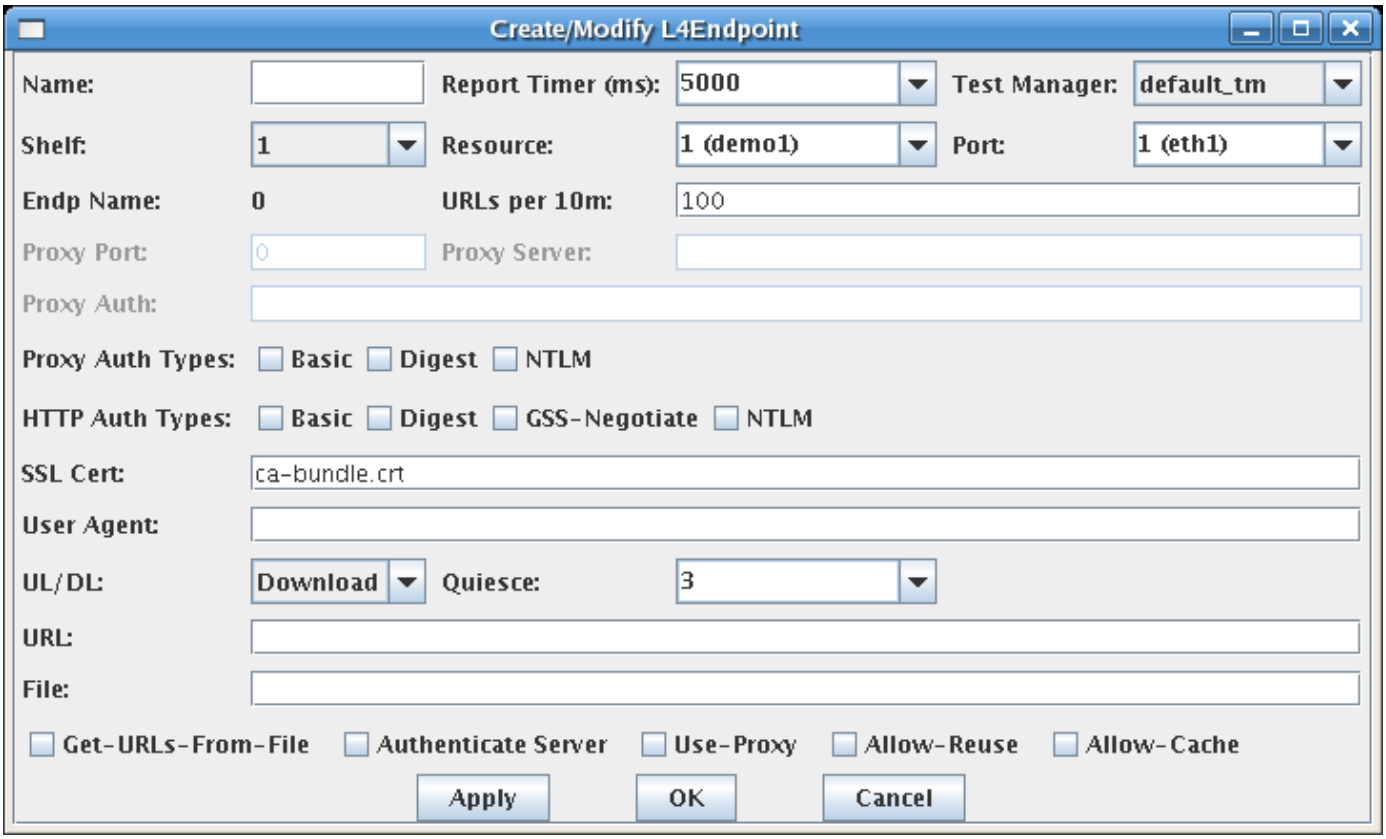
You can now create FTP, HTTP and HTTPS Layer 4-7 Endpoints that will generate real, protocol specific traffic. FTP can upload and download, the rest are only for downloading.

The "Layer-4" tab manages the Layer 4-7 endpoints.



Creating & Modifying Layer 4-7 Endpoints

To Create a new Layer 4-7 endpoint, click on the "Create" button. To modify, select the Endpoint(s) and click on the "Modify" button. You will see a frame that looks like this:



Name

The Name specifies the name of this Endpoint, and must be unique across the LANforge system.

Report Timer

The Report timer specifies how often the Endpoint voluntarily reports data (you can query it at any time).

Test Manager

The test manager specifies who 'owns' this Endpoint, and can be used to segregate a large LANforge system for use by many engineers.

Shelf, Resource, Port

The Shelf and Resource specify which machine this Endpoint will operate on, and the Port specifies which port will be used for outgoing traffic. (It will usually dictate the port for incomming traffic too, but LANforge cannot strictly enforce that if you are using a non LANforge system to serve up the Layer 4-7 data.)

Endpoint Name

The Endpoint Name is just the unique identifier for this endpoint, and may not be modified by the user.

URLs per 10m

The "URLs per 10m" field specifies the number of URLs that the endpoint will process in a 10-minute period. This is where you set your rate limiting.

Proxy Port, Proxy Server

The Proxy Port and Proxy Server relates to HTTP proxies, and will be filled in according to your network setup if you choose to use this feature.

Proxy Auth, Proxy Auth Types

If your proxy requires authentication, enter the user password in the 'Proxy Auth' input field. The proxy authentication types are:

- Basic - Sends username and password in plain text over the network.
- Digest - Described in RFC 2617, does not send the plain text password over the network.
- NTLM - NT LAN Manager, a proprietary Microsoft 'challenge/response' protocol.

HTTP Auth Types

The available HTTP authentication types are:

- Basic - Sends username and password in plain text over the network.
- Digest - Described in RFC 2617, does not send the plain text password over the network.
- GSS-Negotiate - Described in IETF draft-brezak-spnego-http-04.txt, a Microsoft implementation of SPNEGO and GSSAPI authentication mechanisms.
- NTLM - NT LAN Manager, a proprietary Microsoft 'challenge/response' protocol.

SSL Cert

If you are using SSL (HTTPS), specify the certs file in the 'SSL Cert' entry box. LANforge ships with an example certs file called 'ca-bundle.crt' which may have all the certs you need.

User Agent

Allows you to specify the user-agent string for the HTTP connection.

UL/DL

UL/DL specifies whether we are uploading to this URL, or downloading from the URL. For HTTP URLS, you must choose to download, or your results will undoubtedly be wierd. For FTP URLs, you may choose either upload or download, but you must be sure to set up your FTP server to allow the anonymous login to do what you are requesting.

Quiesce

Specify the number of seconds LANforge will wait before finishing downloading or uploading the next URL and stopping the Layer 4 Endpoint.

URL

The URL specifies the thing you are downloading from, or uploading to.
Some example URLs for Upload include:

- ftp://172.1.1.103/pub/upload/gnuserver.upload

Some URLs for Download include:

- ftp://172.1.1.103/pub/gnuserver
- ftp://user:password@ftp.my.site:8021/README
- http://172.1.1.103/index.html

Another option is to have a list of URLs in a file on the LANforge data-generator machine. In that case, you specify that file name (relative to /home/lanforge) and the Layer 4-7 Endpoint will process every URL in that file, over and over again. A file might look like:

```
# Format is:
# [ul | dl] 'URL' 'file-name'

# Get default web page from lf1
dl http://172.1.1.103/index.html /tmp/172.1.1.103_index.html

# Get default web page from lf4
dl http://172.1.1.103/index.html /tmp/172.1.1.103_index.html

# Get a file via FTP
dl ftp://172.1.1.103/pub/gnuserver /tmp/172.1.1.103_gnuserver

# Put a file via FTP
ul ftp://172.1.1.103/pub/upload/gnuserver.upload /tmp/172.1.1.103_gnuserver
```

File

The File specifies where you will save the downloaded URL, or what you will upload to the URL if you are uploading. **Be careful not to over-write any useful files! LANforge runs as root, and will happily overwrite any file you specify! We suggest you always use files in the /tmp directory for safety.**

Get-URLs-From-File

The Get-URLs-From-File checkbox tells the endpoint to treat the URL as a file on the local machine. Note that you do not (at this time), put any URL protocol on the file name. In other words, it's /tmp/foo.txt, not file://tmp/foo.txt.

Authenticate Server

If you are using SSL (HTTPS) and want to verify the server, select the 'Authenticate Server' checkbox. If your server is not authenticated, then do not select this checkbox.

Use-Proxy

The Use-Proxy checkbox turns on the use of the HTTP proxy settings.

Allow-Reuse

When selected, the Allow-Reuse checkbox allows LANforge to reuse existing connections when possible. When not selected, LANforge will create a new connection for each requested URL.

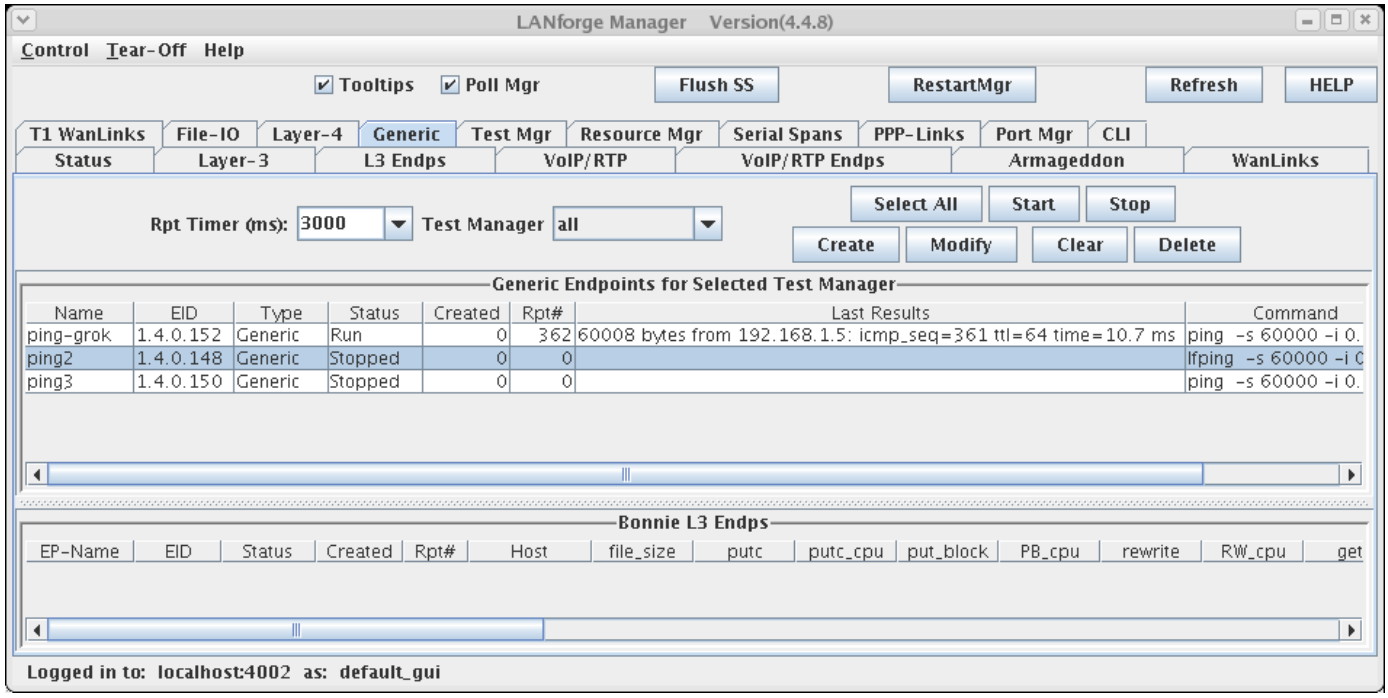
Allow-Cache

When selected, the Allow-Cache checkbox allows LANforge to use cached objects from servers.

5. Generic (User) Endpoints (bonnie++, ping, traceroute, ...)

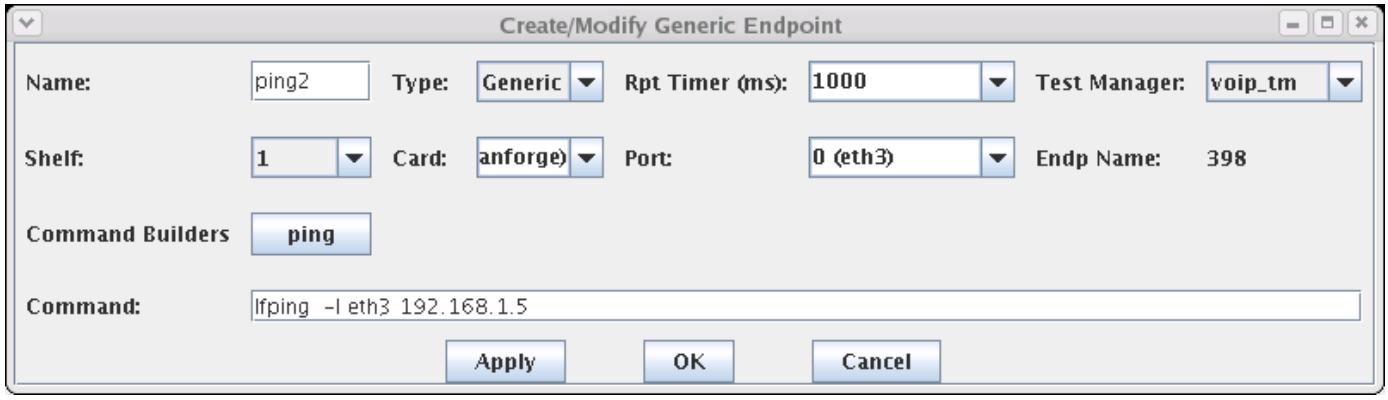
LANforge has the ability to control command line tools and collect their results. For example, the 'ping -I eth4 172.1.1.2 -s 1024' command will ping to host 172.1.1.2, using the local interface eth4. It is up to the user to specify the correct command line, but Candela Technologies will be happy to offer suggestions and help with any tools you would like to use in this manner.

Of special interest (and support), is the bonnie++ program. It is a well-respected Unix file-system tester. It is good for stressing the local LANforge generator machine, but it can also be used as a network traffic generator by running the file-system tests on a network file system, like NFS, SAMBA, or a file system mounted using the iSCSI protocol. The Generic-Endpoints have special handling for bonnie++ output, as you can see from the screen capture below:



Creating & Modifying Generic Endpoints

To Create a new Generic endpoint, click on the "Create" button. To modify, select the Endpoint(s) and click on the "Modify" button. You will see a frame that looks like this:



The Name specifies the name of this Endpoint, and must be unique across the LANforge system. The type can be used to tell the LANforge GUI how to parse the results. Currently, only bonnie++ is specifically supported.

The Report timer specifies how often the Endpoint voluntarily reports data (you can query it at any time). The test manager specifies who 'owns' this Endpoint, and can be used to segregate a large LANforge system for use by many engineers.

The Shelf and Resource specify which LANforge data-generator the command will be run on. The Port specifies which interface the traffic should go on, but at this time, LANforge does not enforce that the command-line is correct. The user must specify the correct command line arguments to whatever command is being used.

The Command is the command that will be run on the specified machine. It should be identical to what you would have to type if you were to telnet into that machine and run the command. To run bonnie++, you will want a command that looks something like this:

```
./bonnie++ -f -q -u lanforge
```

Other commands/tools you might find useful:

File System Testing

The bonnie++ tool is an excellent file system tester. An example command could look like this:

```
./bonnie++ -f -q -u lanforge
```

PING (ICMP)

You can use the standard ping program, but you may also want to consider the lfping script included with LANforge. It wraps the ping program and offers better reporting.

```
lfping -I eth1 -s 1024 192.168.1.100
```

Traceroute (ICMP)

Traceroute is a tool that is used to show each packet hop (router) for a path through a network. It utilizes ICMP response codes to determine the path.

```
traceroute www.slashdot.org
```

DNS

DNS is the protocol that programs use to resolve domain names into IP addresses and visa-versa. We provide a modified version of the standard unix 'dig' tool for generating DNS traffic:

```
./dig -b <local-ip> -B <local-iface> [@<nameserver.com>] <domain>
```

SMTP

SMTP is the Simple Mail Transport Protocol, which handles the vast bulk of email on the internet. We provide the smtp-client.pl program which is a simple client script that can talk to a third-party mail server, such as sendmail. You can get some additional help on the tool by running the command: ./smtp-client.pl --help from the Linux prompt on the lanforge machine. The text file to be sent as email can have headers, for instance:

Subject: Test Email

This is a test email.

```
./smtp-client.pl --enable-auth --verbose --user <user-name> --host <mail-server-name-or-ip> --local-host <local-ip> --local-iface <local-iface> --to <target@email.com> --from <me@domain.com> --pass <mail-server-password> --data <text-file-to-email>
```

TELNET

Telnet requires user-interaction, so we utilize an expect script. Please examine the telnet_expect_wrapper.pl and telnet.expect scripts. You will also need to use the modified 'telnet' executable that comes with LANforge.

Netcat, NMAP

Scripts to generate random netcat and nmap traffic have been donated by Daniel Berry. You will need to edit the script slightly to match your network configuration. Please see the rand_nc.pl and rand_nmap.pl scripts for details.

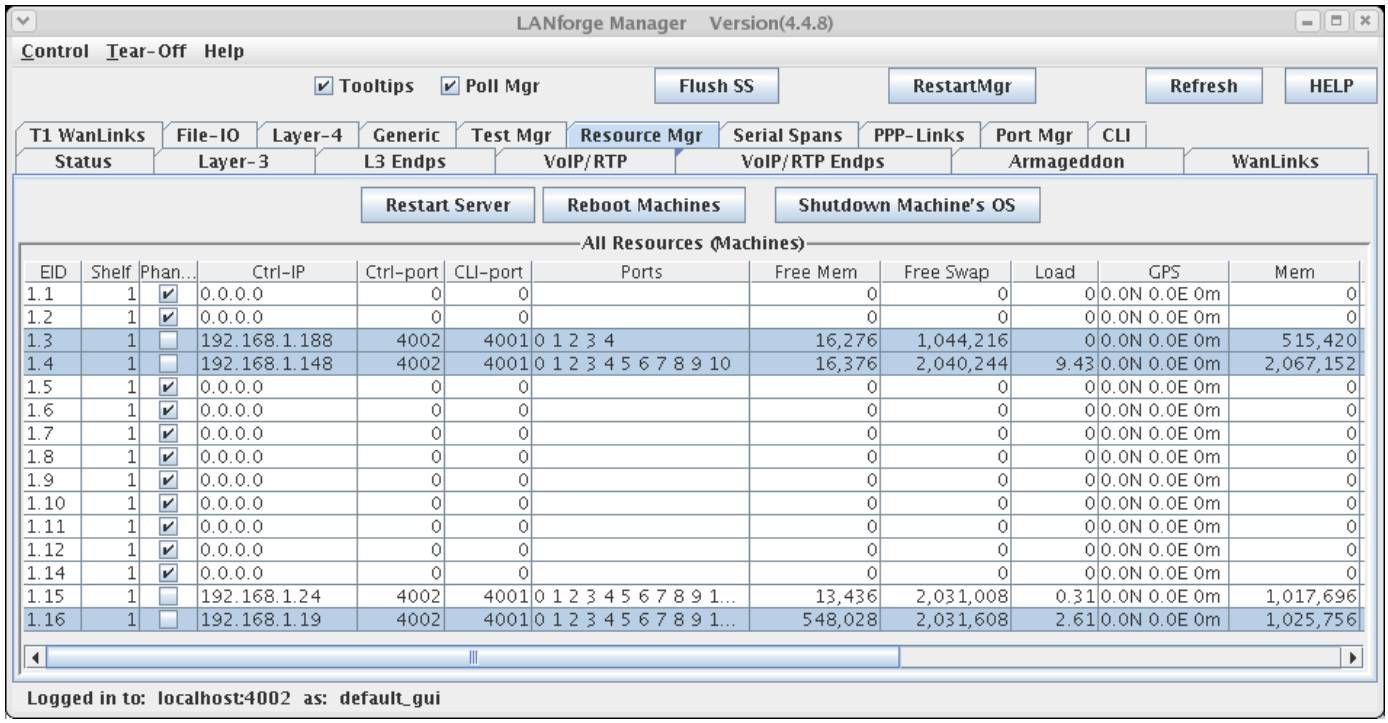
6. Resources (Data Generators)

The LANforge system uses the term 'Resource' to apply to the data-processing machines. The Resources panel gives you information on the resources the LANforge server has discovered. It also gives you the ability to restart the LANforge server on the particular resource. If the resource is PHANTOM, then the LANforge server is not running on it, or the LANforge manager is unable to communicate with it for some other reason. You will not be able to manage a Resource in this state. If it's not Phantom, then you can also reboot the Resource's OS, or shutdown the OS for good (ie until a power-cycle of the individual Resource.)

If you have LANforge systems in a geographically disperse deployment, you may wish to connect them to a GPS device to automatically obtain their location. LANforge supports this feature, and all you need to do is configure the right serial port settings using the lfconfig tool. You may also manually enter the coordinates using the CLI.

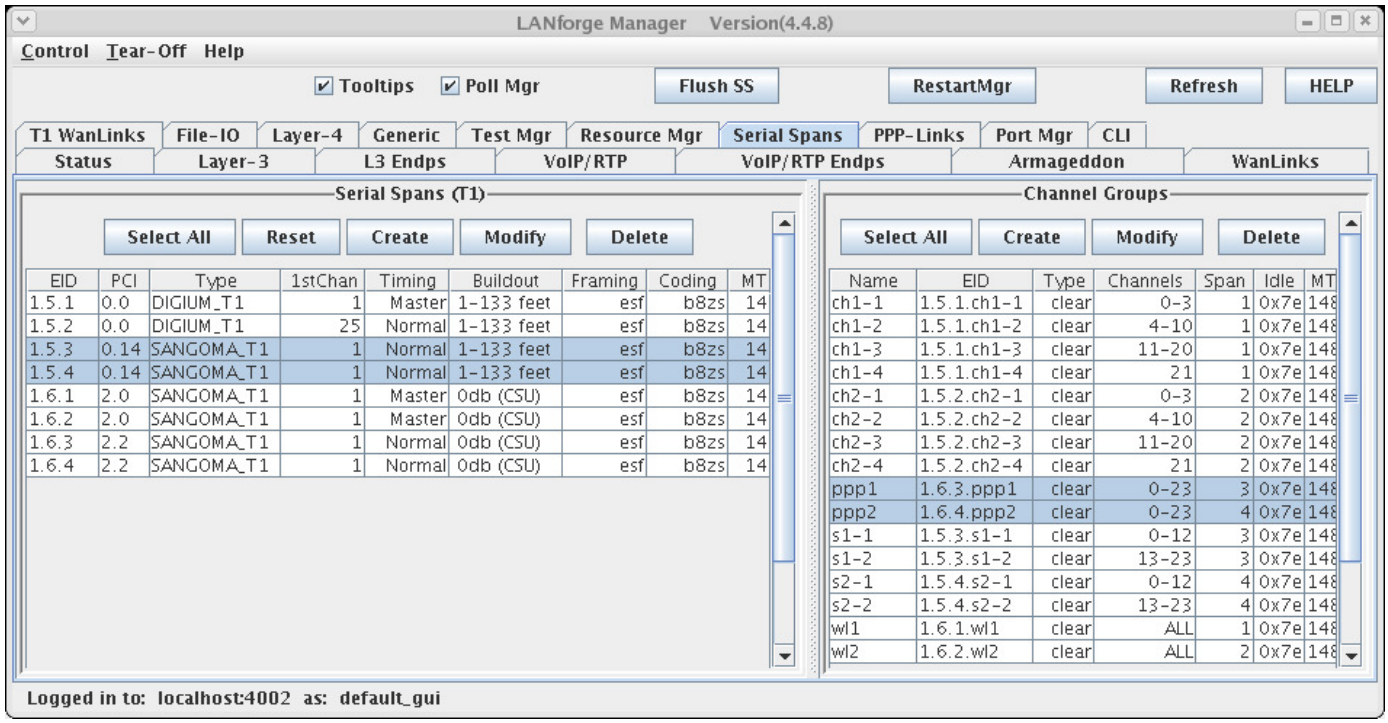
POWERING DOWN NOTE:

If you DO wish to power down a Resource, then you should ALWAYS choose to shutdown the resource first, and give it about 1 minute to take itself down gracefully.



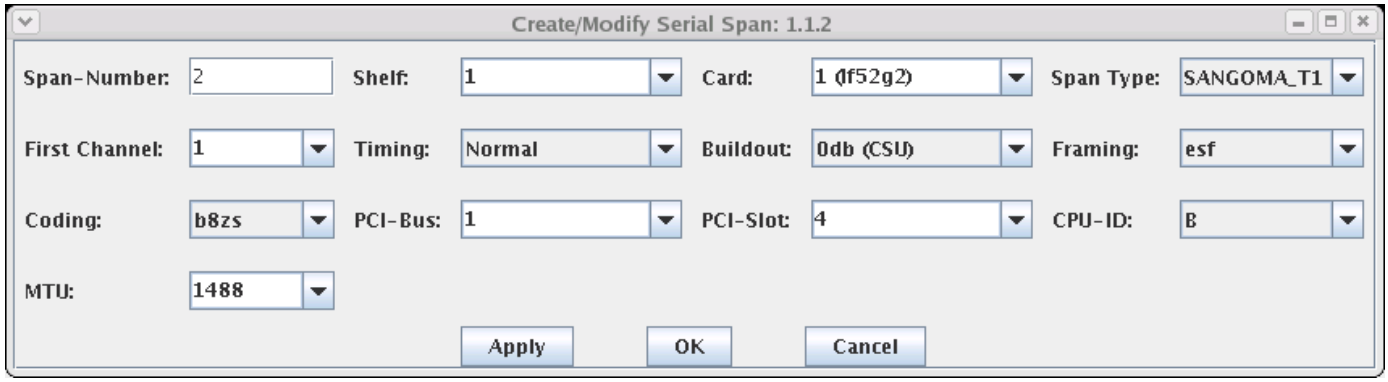
7. Serial Spans

The Serial Spans panel manages the T1 and E1 spans and channel-groups. T3 and other higher speed interfaces will be supported in the future. Currently, Sangoma T1 and E1 cards are supported.



Create & Modify Spans

LANforge cannot currently detect the T1/E1 spans automatically, so you must add them through the GUI if your system is not pre-configured. Click 'Create' in the Serial Spans section and the Create/Modify widget will appear:



Span-Number
: This number must be unique on each Resource. This number is used to configure Digium cards, so if you have a system with both Digium and Sangoma T1 adapters, you should configure the Digium interfaces with IDs starting with 1.

Shelf
: The virtual shelf for the LANforge machine that will hold the T1 interface.

Resource
: The LANforge machine that will hold the T1 interface.

Span Type
: The type of harware for this span. Sangoma-T1 and Sangoma-E1 are the only valid choices at this time.

First Channel

This is used to configure the Digium adapters. For T1 interfaces, the first channel can be calculated with this formula: span-number * 24 + 1

Timing
This influences how the T1 interface derives it's timing. The correct setting depends on the settings of the device terminating the span. If the peer is MASTER, then set LANforge to Normal, and vice versa.

Buildout
Choose the setting closest to the actual length of the T1 span this interface will be attached to.

Framing
The framing for this T1 interface. ESF is a good choice if you are uncertain and are using T1 NICs. D4 is also supported by Sangoma NICs.

Coding
The encoding protocol for this T1 interface. b8zs is a good T1 choice if you are uncertain. AMI is also supported by Sangoma.

PCI-Bus
This is needed for Sangoma T1 cards only. You can find the PCI bus by looking at the output of `wanrouter hwprobe`

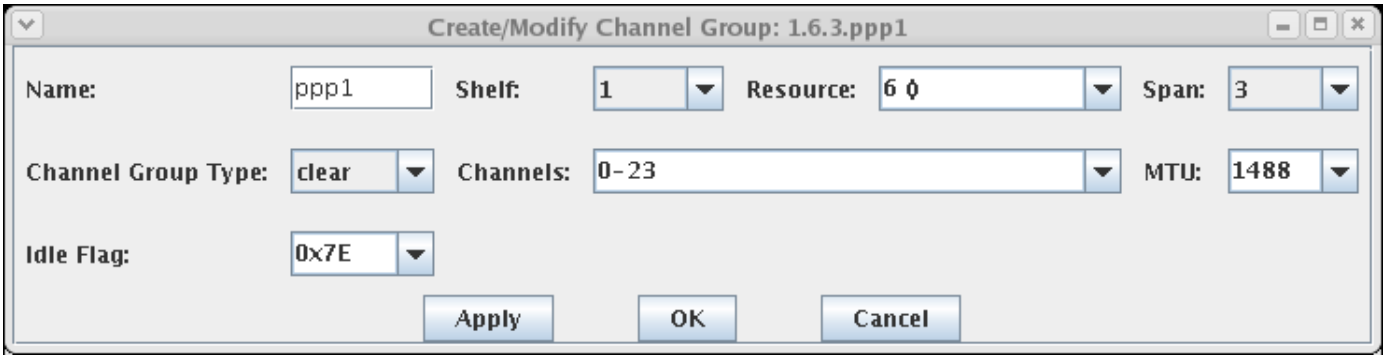
PCI-Slot
This is needed for Sangoma T1 cards only. You can find the PCI slot by looking at the output of `wanrouter hwprobe`

CPU-ID
This is needed for Sangoma T1 cards only. For a 2-port NIC, one interface will be 'A' and the other will be 'B'.

MTU
This specifies the MTU for the in-band management. This can be left at the default of 1488 and does not affect LANforge behaviour.

Create & Modify Channel Groups

After creating a Serial Span, you can now configure one or more Channel groups on the Span. The Digium T1 cards support up to 24 channel groups per Span, but the Sangoma cards we have tested with have only support 1 channel group at this time. Click 'Create' in the Channel Groups section and the Create/Modify widget will appear:



Name
A unique identifier for the Channel-Group on a particular Resource. Should not have spaces and should be less than 16 characters in length.

Shelf
The virtual shelf for the LANforge machine that will hold the channel-group

Resource
The LANforge machine that will hold the channel-group

Span
The Span number that this channel-group will reside upon

Channel Group Type

Specifies the encoding for this channel group. For PPP channel groups and T1 WanLink emulations, choose 'clear'.

Channels

Specifies the particular channels to use for this channel group. Examples of possible entries include: "ALL", "0-23", "0-4,7,9,20-23", and "1,2,3,4,5,6" If the channel group is to be used by a T1 WanLink, be sure to use 'ALL'.

MTU

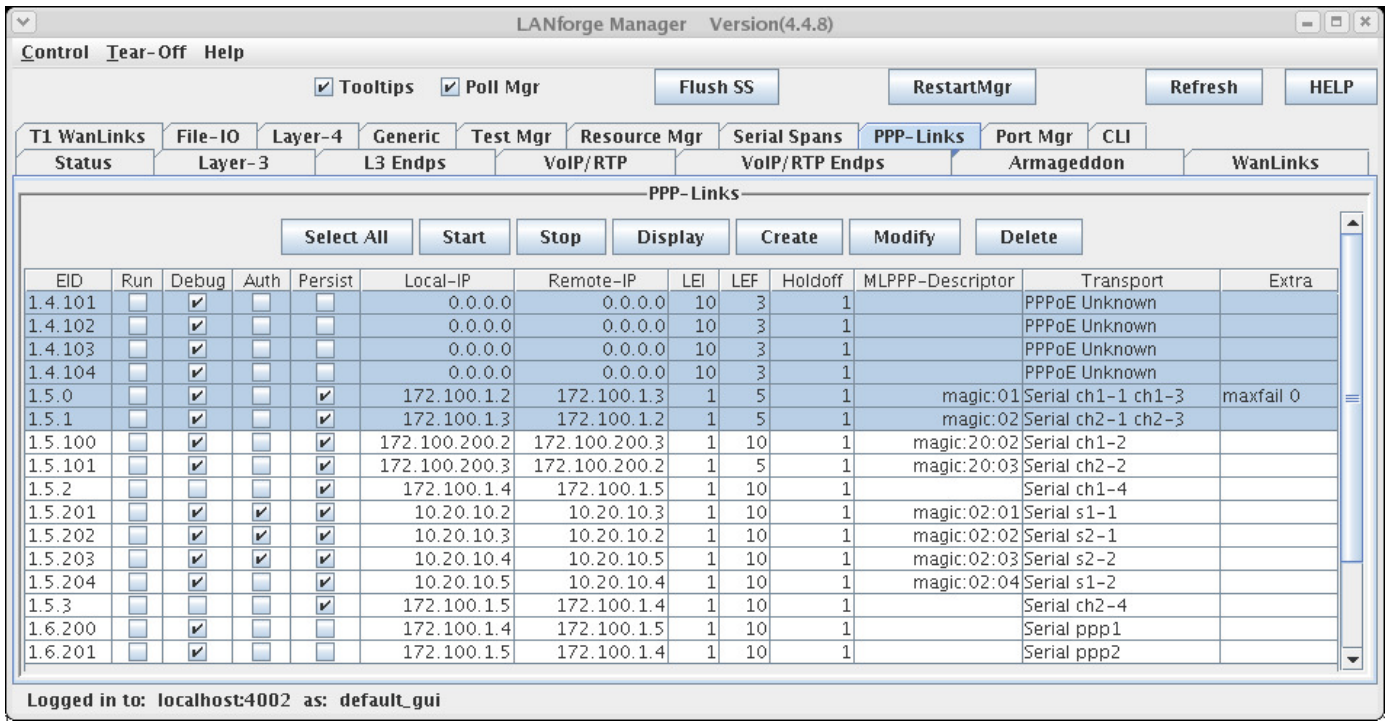
This specifies the MTU for this channel group. If the channel group is to be used by a T1 WanLink, then set the MTU to a small value (192 is suggested). The MTU **MUST** be an even multiple of the number of channels (24 in the case of a T1). The smaller the MTU, the more accurate the T1 WanLink latency will be, but the more CPU the LANforge processes will use. If your machine is being over-worked and/or dropping packets, try increasing the MTU. For PPP links, the MTU is not critical, and should be set to a larger value, like 1488 or 1500.

Idle Flag

This specifies the idle flag for this channel group. This byte pattern will be sent automatically by the T1 hardware whenever there is nothing else to send. This value should probably match the idle flag used by the peer equipment to which LANforge is attached.

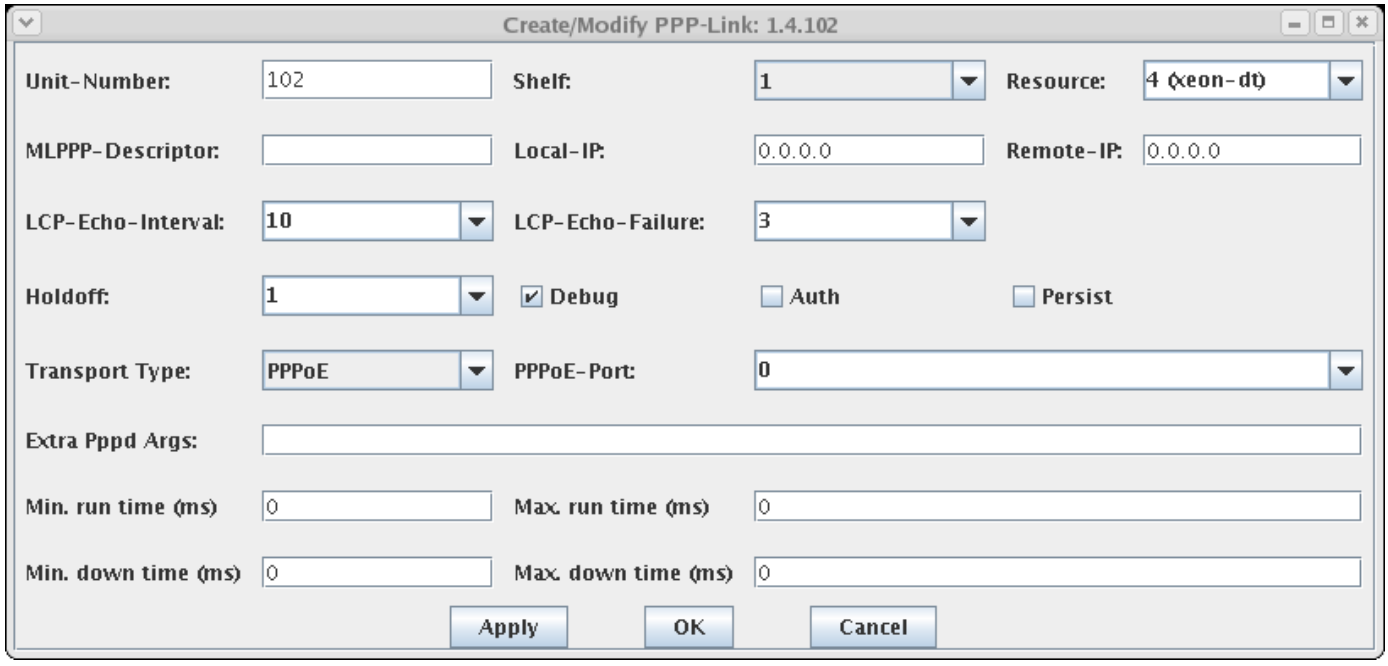
8. Create & Modify PPP Interfaces

The PPP connections will run over one or more T1 channel groups, and PPPoE interfaces can be created over regular ethernet (assuming you have a PPPoE server available.) If you choose more than one channel group, then the multi-link PPP protocol will be used.



The basic building block of the ppp daemon is the pppd server. If you only use Sangoma T1 hardware or PPPoE, the default pppd on modern distributions will work. LANforge creates a start script in the pppScripts directory. When the PPP link is started, LANforge will fork and exec this script.

Click 'Create' in the PPP-Links section and the Create/Modify widget will appear:



Unit-Number

Should be unique for a particular resource. This will be the XXX in the device name pppXXX. For instance, if the interface should be called ppp2, then set the Unit-Number to 2.

Shelf
The virtual shelf for the LANforge machine that will hold the PPP Link

Resource
The LANforge machine that will hold the PPP Link

MLPPP-Desriptor
If using Multi-Link PPP, then set the descriptor here. It should start with magic: and then be followed by asci-hex. For example: magic:01:02:ab:df The identifier should be unique for each PPP-Link on a particular machine.

Local-IP
Specify the Local-IP for this PPP Interface. Not needed for PPPoE.

Remote-IP
Specify the Remote-IP for this PPP Interface. When connecting two PPP links to each other, the Local & Remote IP addresses should be swapped. Not needed for PPPoE.

LCP-Echo-Interval
Specifies, how often, in seconds, a link control protocol echo should be sent.

LCP-Echo-Failure
Specifies how many echo failures we can have before we consider the link to be down.

Channel-Groups/PPPoE-Port
Specifies the channel group(s) to use for this PPP Link. If this is a PPPoE link, then you specify the ethernet port to use. If multiple groups are specified, multi-link PPP will be used and you must also specify a MLPPP-Descriptor.

Holdoff
How long (in seconds) to wait before trying to re-establish a PPP link that has gone down for some reason.

Debug
Select this to run the ppp daemon in debugging mode. The log files will be placed in the pppLogs directory.

Auth
Should we attempt to authenticate this PPP connection. Auth is not supported at this point, so leave this un-selected.

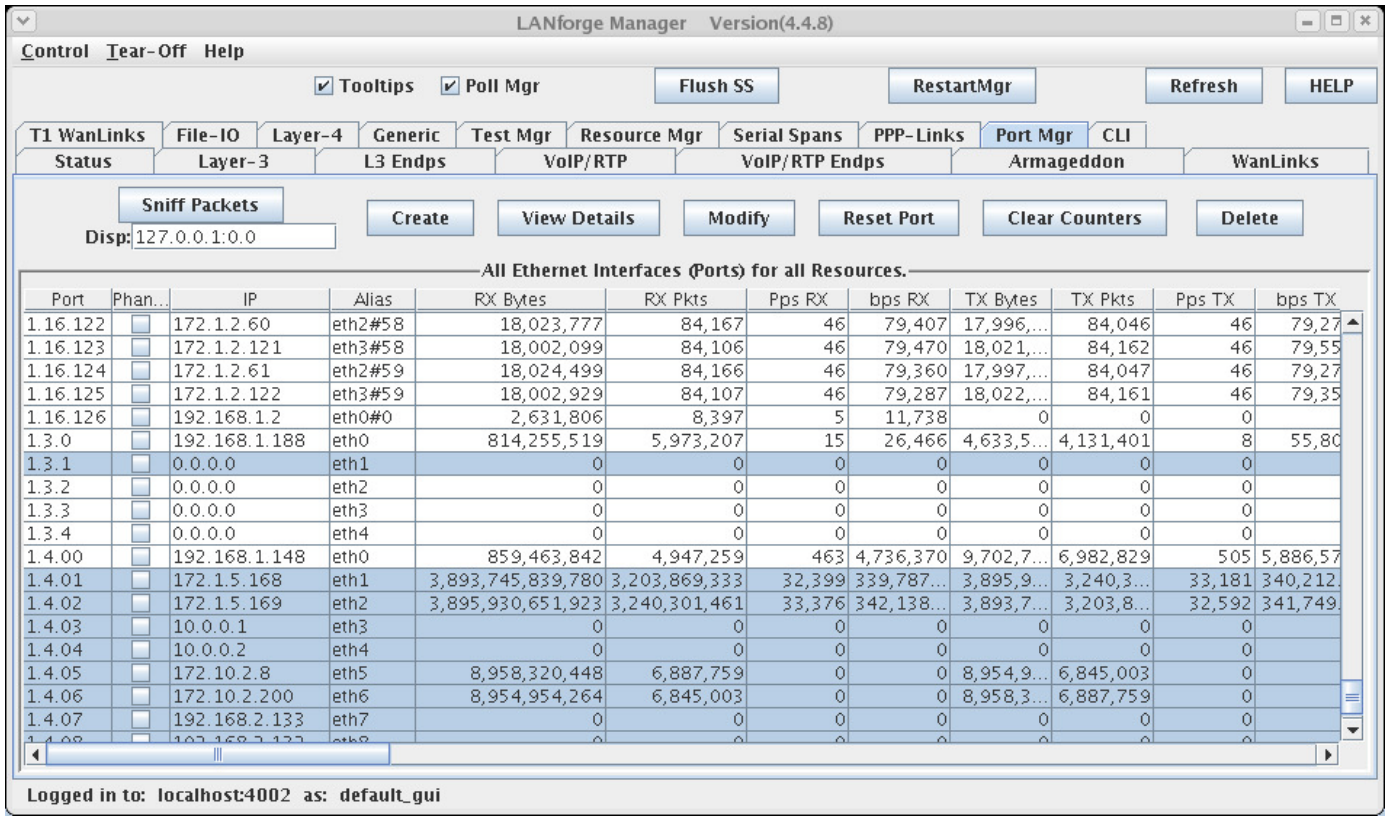
Persist
Should we attempt to re-establish the PPP link if the link goes down for some reason. In most cases, this option should be selected.

Extra Pppd Args
If you want to pass your own arguments to the pppd process, add them in this field. If you add the wrong options you can cause all sorts of problems, so use this with care.

Run Timers
If you want the PPP link to come up and down at some interval, you can set the min/max run and down timers. The LANforge traffic generation cross-connects will automatically re-start when the PPP links come back up.

9. Ports (Interfaces)

The Ports panel represents the individual Ethernet Ports on the LANforge Data Generators (Resources). It has a large number of counters who's values are acquired from the kernel drivers.



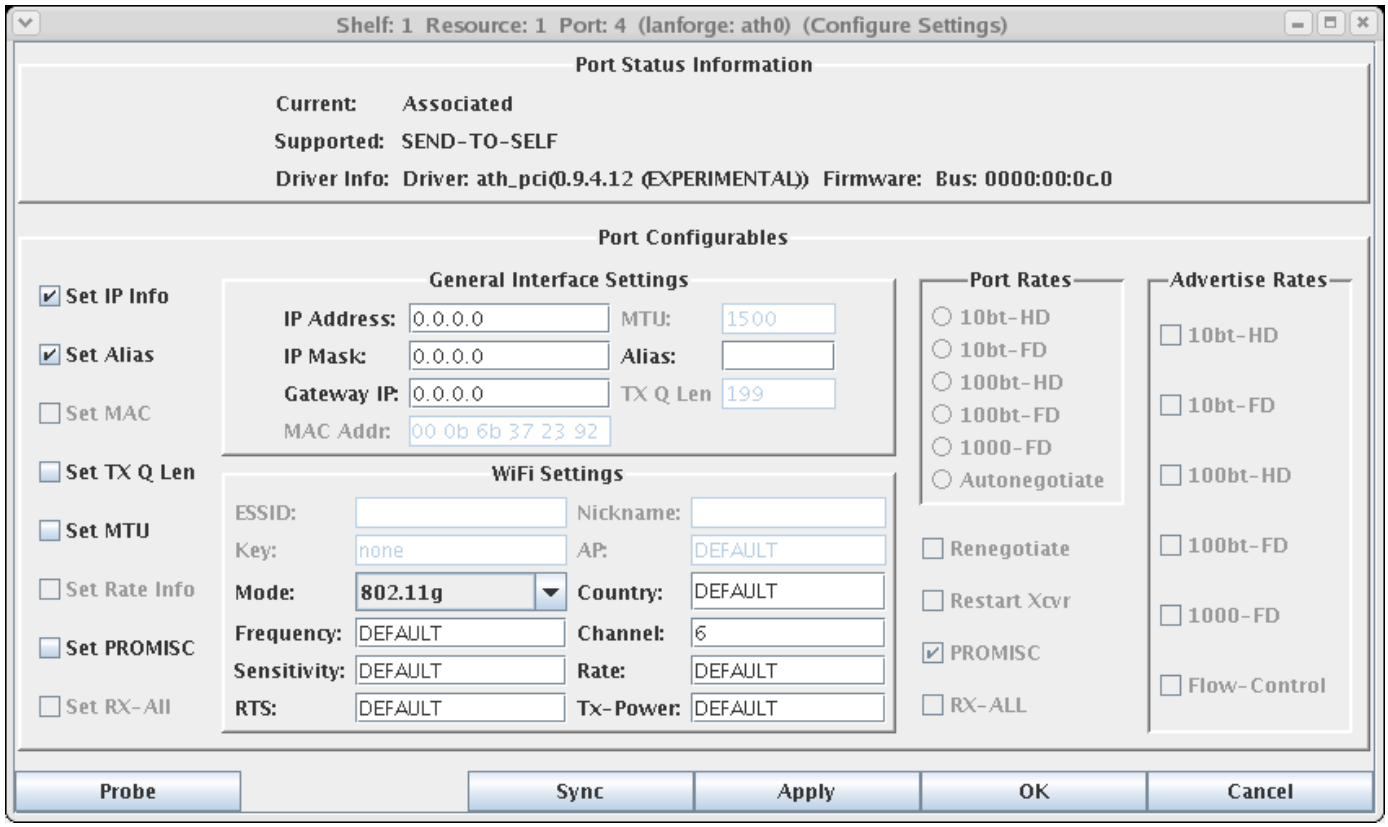
Port	Phan...	IP	Alias	RX Bytes	RX Pkts	Pps RX	bps RX	TX Bytes	TX Pkts	Pps TX	bps TX
1.16.122		172.1.2.60	eth2#58	18,023,777	84,167	46	79,407	17,996,...	84,046	46	79,27
1.16.123		172.1.2.121	eth3#58	18,002,099	84,106	46	79,470	18,021,...	84,162	46	79,55
1.16.124		172.1.2.61	eth2#59	18,024,499	84,166	46	79,360	17,997,...	84,047	46	79,27
1.16.125		172.1.2.122	eth3#59	18,002,929	84,107	46	79,287	18,022,...	84,161	46	79,35
1.16.126		192.168.1.2	eth0#0	2,631,806	8,397	5	11,738	0	0	0	
1.3.0		192.168.1.188	eth0	814,255,519	5,973,207	15	26,466	4,633,5...	4,131,401	8	55,80
1.3.1		0.0.0.0	eth1	0	0	0	0	0	0	0	
1.3.2		0.0.0.0	eth2	0	0	0	0	0	0	0	
1.3.3		0.0.0.0	eth3	0	0	0	0	0	0	0	
1.3.4		0.0.0.0	eth4	0	0	0	0	0	0	0	
1.4.00		192.168.1.148	eth0	859,463,842	4,947,259	463	4,736,370	9,702,7...	6,982,829	505	5,886,57
1.4.01		172.1.5.168	eth1	3,893,745,839,780	3,203,869,333	32,399	339,787...	3,895,9...	3,240,3...	33,181	340,212.
1.4.02		172.1.5.169	eth2	3,895,930,651,923	3,240,301,461	33,376	342,138...	3,893,7...	3,203,8...	32,592	341,749.
1.4.03		10.0.0.1	eth3	0	0	0	0	0	0	0	
1.4.04		10.0.0.2	eth4	0	0	0	0	0	0	0	
1.4.05		172.10.2.8	eth5	8,958,320,448	6,887,759	0	0	8,954,9...	6,845,003	0	
1.4.06		172.10.2.200	eth6	8,954,954,264	6,845,003	0	0	8,958,3...	6,887,759	0	
1.4.07		192.168.2.133	eth7	0	0	0	0	0	0	0	

Each port can be configured with an IP address (must be configured if you are running anything other than raw Ethernet protocols or LANforge ICE) and a default gateway. The Default Gateway will be used when the system-under-test acts as a router. LANforge is designed to make each port look as if it's a separate computer, so you are able to specify a different default gateway on each port, or the same one if you desire. You are not restricted to the use of Port IP addresses, except that you must not have duplicate IP addresses on the same Resource, and of course they must make sense in whatever testing network you have configured. TCP/IP networking is a complex subject, so if you have questions not addressed here, email support@candelatech.com and they will try to explain how LANforge can address your specific needs.

LANforge can also give you easy access to some ethernet driver configuration options, including various link speeds and auto-negotiation settings. This will only work if you have cards and are running ethernet drivers that support these features of course. Here is a list of Ethernet cards & Drivers information.

Modifying and Viewing Ports

To configure a Port, select it and click the "Modify" button. You will see a window pop up similar to this:



The top part of the display shows the flags as reported by the ethernet drivers. These will be updated automatically for you, or you can hasten the update by pressing the "Refresh" button on the main GUI display.

The left-middle section controls which options you want to set on the ethernet driver. Select those you are interested in, and their entry fields will become active.

IP Address
Allows you to change the IP address on the interface.

IP Mask
Allows you to change the IP Mask for the interface.

Default Gateway
Allows you to change the default gateway for packets leaving from this interface.

MAC Address
Allows you to change the MAC address of the interface.

MTU
Allows you to change the Maximum Transmit Unit (MTU) for this interface. You should understand the implications before changing this. Default is 1500 for most devices. Many Gigabit Ethernet systems can handle 8k or larger MTU settings, yielding increased throughput.

Alias
Allows the user to specify a nick-name for this interface.

TX Q Len
Allows you to change the Transmit Queue Length for this interface's driver. A good range is between 100 and 2000, and you should be towards the higher end for ports expected to run at higher speed.

WiFi Settings

With release 4.4.8, LANforge supports virtual WiFi stations (Virtual STA) interfaces when LANforge is used with supported WiFi NICs. Currently, only Atheros 802.11a/b/g NICs are supported.

ESSID

The correct ESSID allows a Virtual STA to associate with an AP. *Virtual STA devices only.*

Nickname

May be used by AP to help identify Virtual STAs. *Virtual STA devices only.*

Key

Enter the WEP 64 or 128-bit key here.
For ASCII strings, prepend 's:' to the front of the key, e.g. **s:**wgU]+'j!eZlLI
For HEX keys, enter the key in ASCII HEX, for instance: 7767555d2b276a21655a6c4c49
Virtual STA devices only.

AP

Specify the station ID of the AP with which you wish this Virtual STA to associate. The station ID looks like an ethernet MAC address. To associate with any available AP, leave this blank. *Virtual STA devices only.*

Mode

Specify the Radio mode (A/B/G). This mode should match available modes on the AP you are using. *Radio devices only.*

Country

Specify the country code for the radio. *Radio devices only.*

Frequency

Specify the frequency at which the radio should transmit and receive. You may leave this blank and use the Channel to select the correct frequency. *Radio devices only.*

Channel

Specify the channel to be used by the radio. *Radio devices only.*

Sensitivity

Specify the sensitivity for the radio. See manual page for 'iwconfig' or contact Candela for more details. *Radio devices only.*

Rate

Specify the rate at which the radio should function, e.g. 54M would set the rate to 54 Mbps. Leave blank to use best possible rate. *Radio devices only.*

RTS

Specify the RTS threshold. See manual page for 'iwconfig' or contact Candela for more details. *Radio devices only.*

Tx Power

Specify the transmit power for the radio. See manual page for 'iwconfig' or contact Candela for more details. *Radio devices only.*

Port Rates

Allows you to change the rates on the ethernet driver. Normally, you will want to stay in auto-negotiate mode, which is most flexible. However, you can set to any fixed speed as well. Setting to fixed speeds may work around bugs in your driver, or in the device under test, but make sure you set the speed to the same on both ends of the connection!

Renegotiate

Allows you to force the interface to re-negotiate the link speed. This may fix a hung driver, but don't count on it!

Restart Xcvr

Allows you to restart the ethernet transceiver. This may fix a hung driver, but don't count on it!

PROMISC

Allows you to put the adapter into promiscuous mode. WiFi radio devices should **always** be in PROMISC mode.

RX-All

Certain drivers (e100, e1000) have been modified by Candela to allow them to receive packets with bad CRCs and other errors. This allows you to use a packet sniffer like Ethereal to diagnose packets with errors. This option also includes the 4-byte CRC at the end of the ethernet frame in packets received from the network. This will aid debugging of bad CRC values, but it will break certain applications (such as LANforge ICE, currently).

If you would like a verbose display of a port, select it and click the "View Details" button. It will pop up a window similar to the Port Configuration tool mentioned above, but it is read-only, and will be automatically updated as the information is received from the server. Often, it is useful to have one of these windows open as you are configuring the port because it allows you to see exactly what the server is reporting at any given time.

The Ports panel also gives you the ability to reset the port, which will tell the driver to drop the ethernet link. It will then read the TCP/IP configuration information from a file that was generated when you configured (Modified) the Port, and rebuild all of the TCP/IP information, including the default gateway, IP address, and subnet-mask.

You may also clear the Port's counters with the 'Clear Counters' button.

Create/Delete Virtual Interfaces (MAC-VLAN, 802.1Q-VLAN, Redirect-Devices, Bridge-Devices, 802.11a/b/g Virtual STA)

LANforge has the ability to create and delete virtual interfaces on the fly. There are currently five types of virtual interfaces that are supported. You must have a (virtual) port-license for each VLAN that you create: Please contact sales@candelatech.com if you need more licenses. With recent LANforge releases, there is no hard upper limit on the number of interfaces that can be created. Candela has tested up to 2000 MAC-VLANs on a high-end machine, with each virtual interface running Layer-4 HTTP requests. Support for these virtual interfaces requires the LANforge resource to be running on Linux, with the Candela kernel and updated iputils package. See the install guides for more details if you are installing LANforge on your own machines.

- **MAC-VLAN**

  The MAC-VLAN virtual interfaces allow one to create the illusion of multiple real interfaces on a single interface. From the outside world, it appears as if the physical LANforge interface is an ethernet switch with multiple machines connected to it. In other words, the MAC-VLANs are completely transparent to the other machines on the network.

- **802.1Q-VLAN**

  LANforge also supports creation and deletion of 802.1Q VLANs. Unlike MAC-VLANs, 802.1Q VLANs speak a slightly different protocol on the ethernet network. This means that the system(s) that the LANforge machine is talking to must also be configured for 802.1Q VLANs.

- **Redirect-Devices**

  Redirect devices are a pair of virtual interfaces that are logically connected with a loopback cable on the far side. If rdd0 and rdd1 are a pair, then when you transmit a packet on rdd1, the packet will be automatically received on rdd0. This feature is used for configuring LANforge ICE in router mode, and can also be used for demonstration purposes where physical interfaces are in short supply.

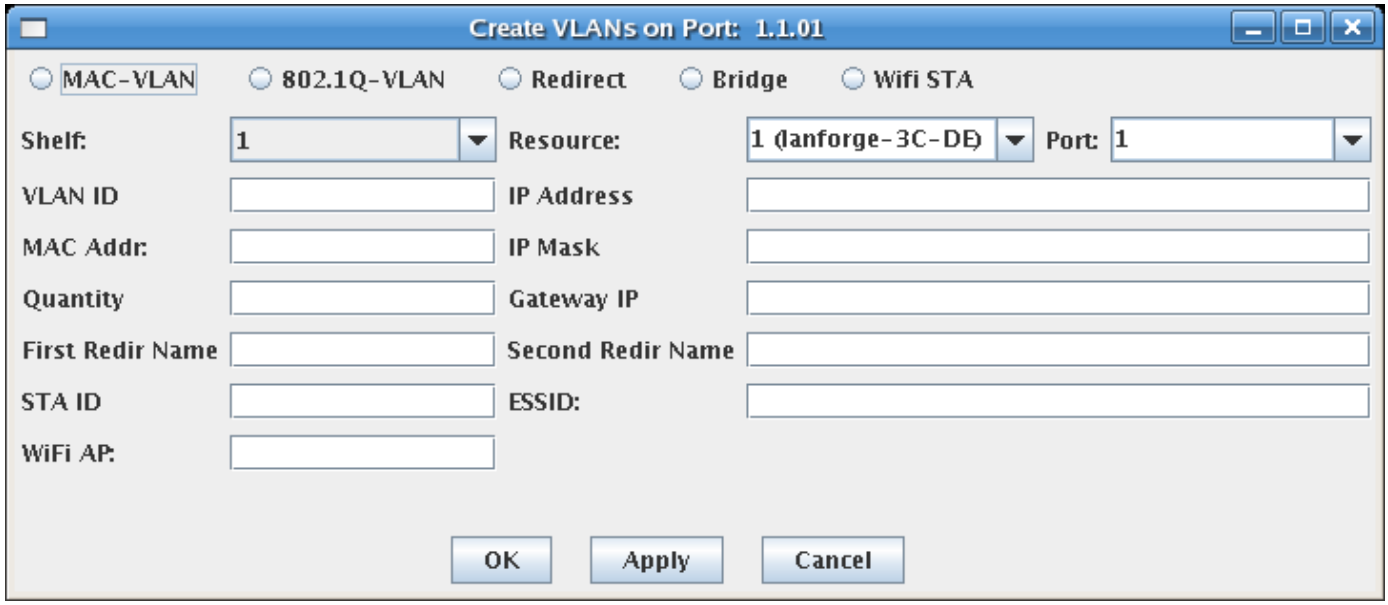
- **Bridge-Devices**

  Bridge devices are Linux network devices that allow one to aggregate other network interfaces into a single broadcast domain. After creating a bridge device, it can be modified to include the network devices that are to be associated with the bridge. Logically, bridges are very similar to an ethernet switch.

- **WiFi Virtual Station**

  The WiFi Virtual Station (Virtual STA) interfaces allow one to create the illusion of multiple distict WiFi stations (think: laptops with WiFi NICs) using a single physical WiFi radio. To the Access Point(s) (APs) it appears as if each Virtual STA is an individual station. Each Virtual STA has it's own MAC, IP address and routing table. All LANforge FIRE related traffic generation features work with Virtual STAs.

The creation of VLANs is quite simple. Select a physical port and press the "Create" button on the Ports tab. You will see a window like this appear:



Select the VLAN type (MAC-VLAN, 802.1Q VLAN, Redirect Device or Virtual STA). When creating 802.1Q VLANs you must specify the VLAN-ID. When creating a MAC-VLAN, you must specify a MAC Address to uniquely identify this VLAN. For redirect devices, just specify the two names. We suggest rdd0, rdd1, etc, but you can also name them as regular ethernet devices if you wish (eth2, eth3, etc). After creation you can change the rest of the Interface attributes like you would normal interfaces via the "Modify" button on the Ports tab. You can create multiple VLAN interfaces at once and you can have them pre-configured with IP addresses. Just fill out the appropriate fields and put in the beginning IP and/or MAC addresses.

You can create 802.1Q VLAN interfaces on physical ethernet interfaces only. You can create MAC-VLAN interfaces on physical ethernet interfaces and 802.1Q VLAN interfaces. Redirect devices are not directly associated with any physical interface.

Virtual STA interfaces may only be created on Radio Devices, and the only supported Radio Devices are the Atheros NICs using the special driver provided by the pre-built Candela kernels and appliances.

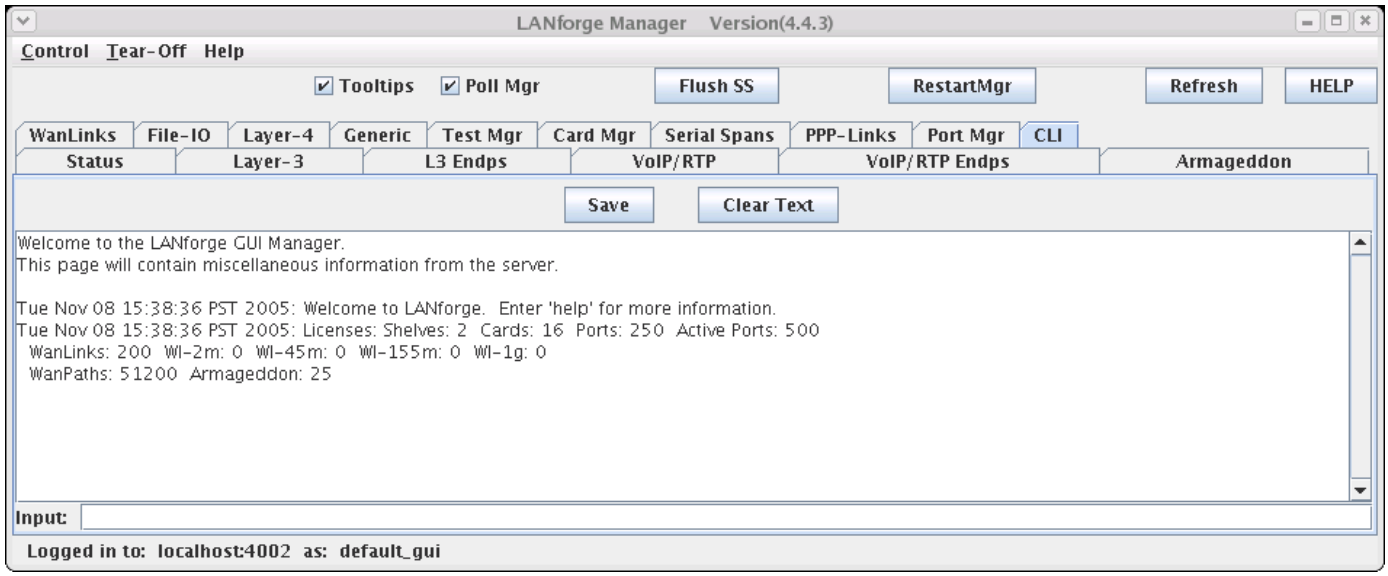
To delete a virtual interface, select it and press the "Delete" button on the Ports tab.

Sniffing Ports

If you have Ethereal installed and configured correctly on your LANforge machines, and if your machine upon which you are running the GUI supports the X-windows protocol, you may sniff a particular port. To sniff a port, select it and click the 'Sniff Packets' button. You may have to change the DISPLAY option box under the 'Sniff Packets' button if you have a non-standard setup. For example, if your LF GUI is running on one PC and your LF Server is on another, you would type in the IP address of the LF GUI machine with :0.0 at the end so that the LF Server would be allowed to display the ethereal program on the LF GUI PC. For Windows PCs running the LF GUI, the cygwin program must be installed per the GUI installation instructions. When Ethereal pops up, you can start sniffing packets by clicking on the 'Capture' menu item. For more information on Ethereal's excellent feature set, see www.ethereal.com.

0. Command Output

The Cmd Output panel is used to convey miscellaneous information from the LANforge server to the user. It can also be used to input CLI commands to the LANforge server. You can see an example of it's output here:



1. Pull-Down Options

Control

- **Connect**: Brings up the initial splash screen to Connect, Disconnect and Discover LANforge systems.
- **Log In As**: Allows you to log in as a particular user. See Client Login for more information.
- **Toggle Commas**: If you prefer to not have commas placed in large number displays within the GUI, you can toggle the use of commas through this menu item. By default, commas are turned ON.
- **Debug**: If you are having difficulty with the software, Candela Support personnel may ask you to turn on the logging, and you can do that through this menu item. For normal use, Debug may not be very useful.
- **Force-JVM-GC**: Java Virtual Machine Garbage Collection is another debugging tool that is not normally used unless you are directed to do so.
- **Exit**: An alternative way of exiting the GUI.

Reporting

- **Print (Fit to Page)**: Allows you to print the data as viewed in the GUI to a printer or PDF document which will be automatically sized to fit on one page.
- **Print (Multi Page)**: Allows you to print the data as viewed in the GUI to a printer or PDF document, splitting the columns up across several pages.
- **Brief Snapshot**: Uses the JFreeReport java class library to print the data as viewed in the GUI to a separate window where you can then export to a PDF, Excel, RTF, HTML, CSV, Text or Printer.
- **Report Manager**: Allows you to save data on reporting elements such as Endpoints, Interfaces and Resources to .csv formatted files that can be later turned into graphical HTML reports.

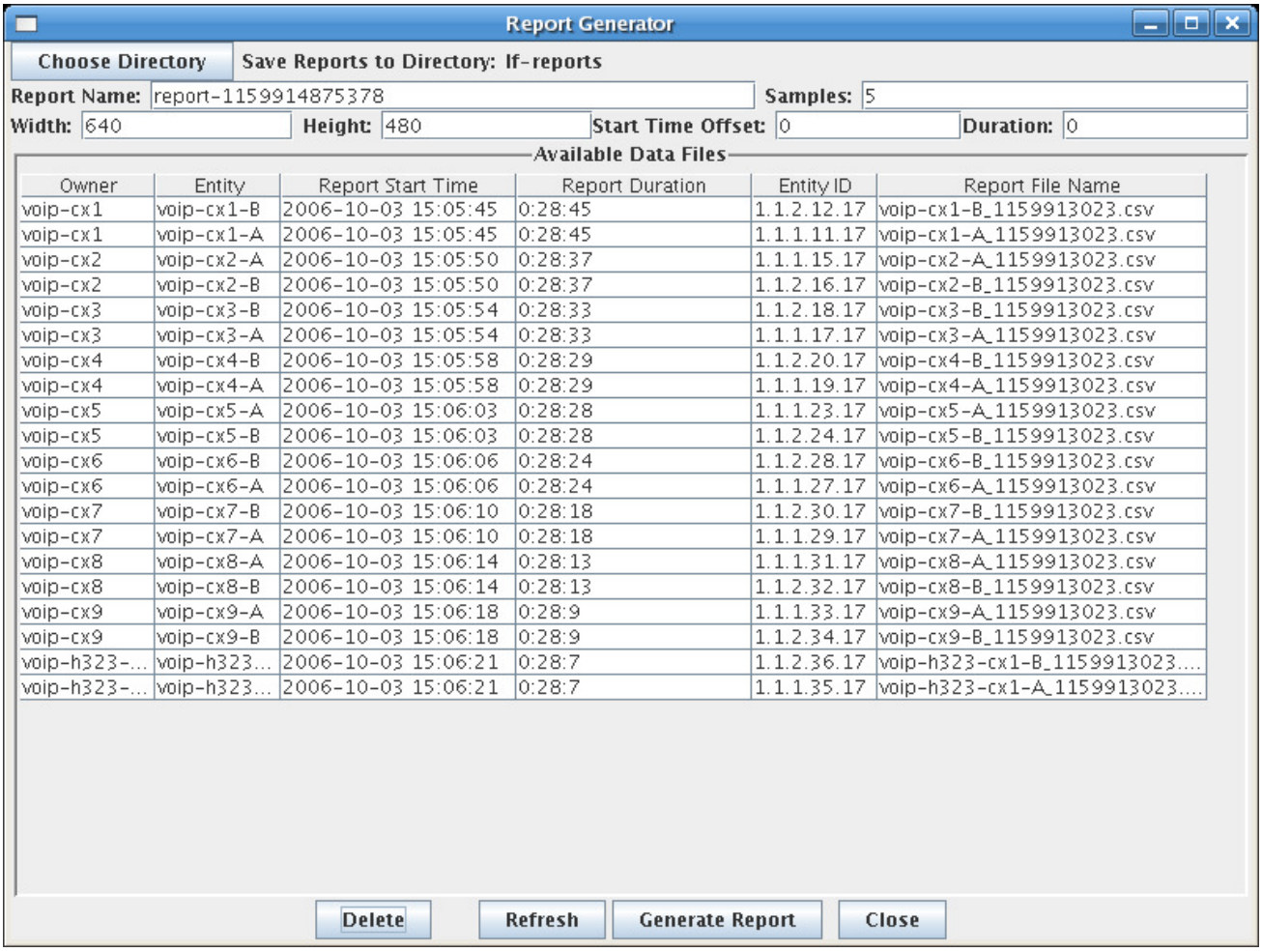
The Reporting Manager pop-up allows you to control where and when Endpoint data is stored. After your Endpoint data has been saved, the Generate Report button allows you to create customised graphical HTML reports of selected Endpoints.

Report Data Directory
Allows you to choose a directory for the .csv data reports to be stored.

Report Data Frequency
Allows you to change the rate at which Endpoint data is saved which reduces disk space usage and lowers the stress on the GUI host PC. The value, in seconds, is how often a snapshot of Endpoint data should be taken. Best Precision timing saves data at the rate of the report timer of each individual reporting element. Best Precision reporting will use the most disk space and highest processing power of the GUI host PC.

Reporting Status
Allows you to determine if data is currently being saved.

You have the option of viewing the .csv information directly by navigating to the Report Data Directory mentioned above and opening the files with a spreadsheet application. Or you can click the **Generate Report** button to create a customised graphical HTML report.



First, choose a main directory in which the GUI can save the HTML reports. This directory will be the top-level directory under which all Report Name directories will be stored.

Report Name
Allows you to choose a directory name for the current HTML report to be stored.

Samples
Allows you to specify the number of samples to average together when calculating packets-per-second and other running averages.

Width
Allows you to specify the width, in pixels, of the graphs to be generated.

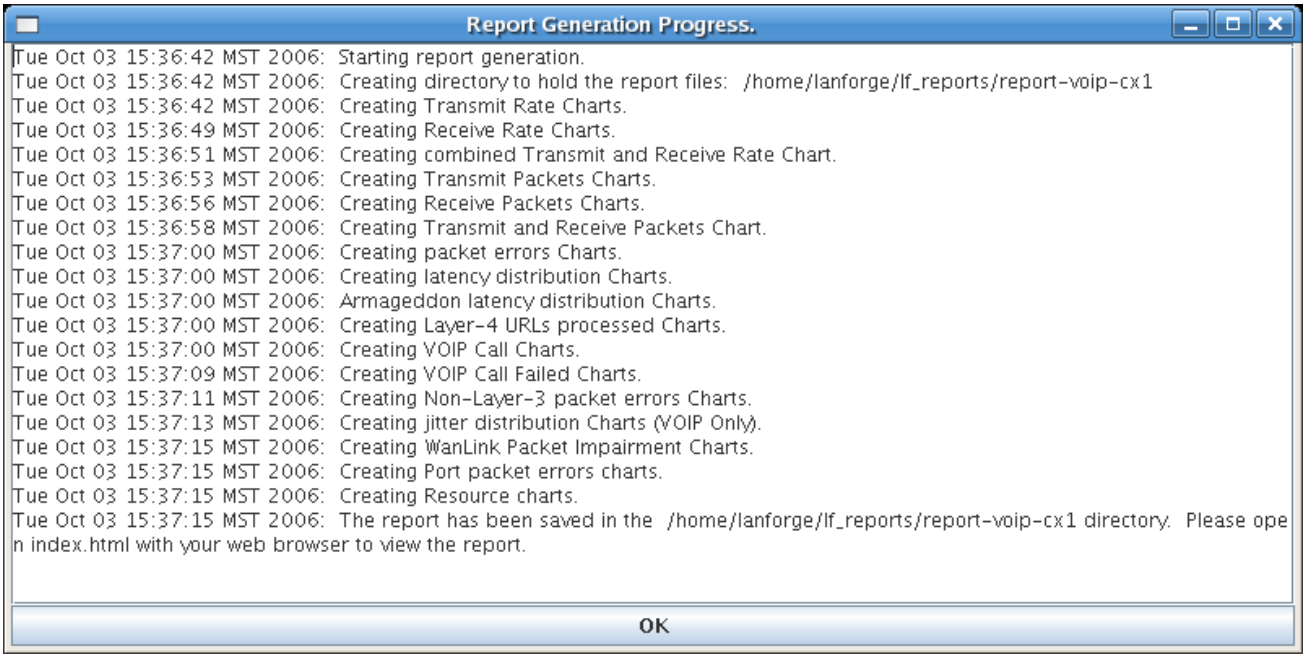
Height
Allows you to specify the height, in pixels, of the graphs to be generated.

Start Time Offset
Allows you to specify the number of seconds of data to skip before starting the report.

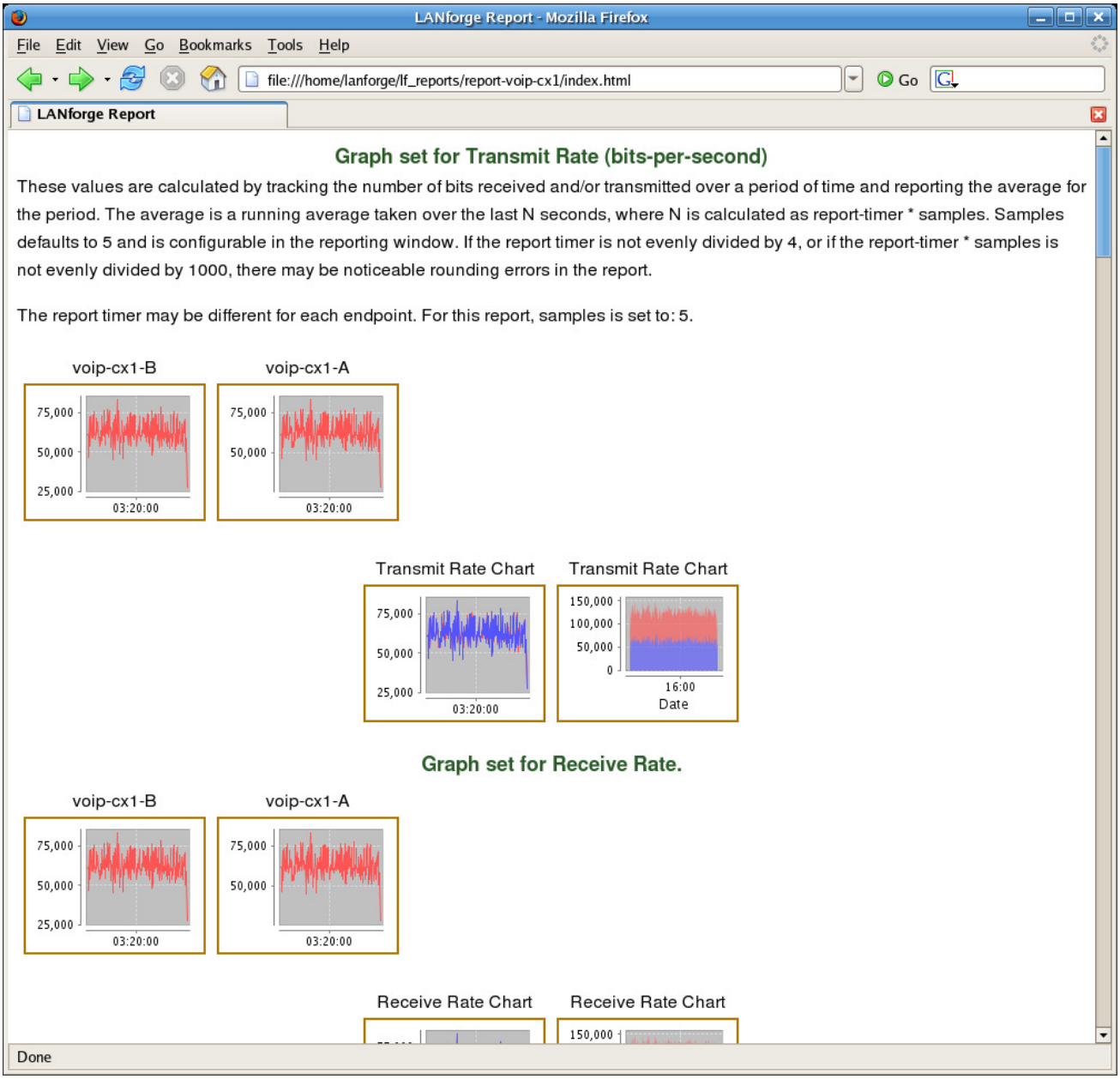
Duration
Allows you to specify the number of seconds of data to report. Zero means graph all.

After choosing your HTML report options, select the Endpoints, Interfaces and Resources that should be included in the HTML report. When you have the data files you want selected, click the 'Generate Report' button.

The Report Generation Progress pop-up will present the entire status of report generation for each Endpoint, Interface or Resource selected. The duration of report generation will depend on the size and number of .csv data files selected. At the conclusion of the report generation, the progress pop-up will confirm the name and directory of the completed HTML report.



To view the completed HTML report, navigate to the directory printed in the progress pop-up and open the index.html file in your web browser application.



Tear-Off

Up until this point, we have always shown each panel in the collection of tabs embedded in the main window. The 'Tear-Off' pulldown menu will allow you to pull off any of the tabs into their own window. This will allow you to monitor several tabs at once!

Help

Allows you to view documentation on the Current Pane you are on, as well as the LANforge Overview. The Help Menu also allows you to view which version of LANforge you are running and your current license allowances with usage information.

Candela Technologies <support@candelatech.com>
Last modified: Thu Apr 12 09:35:14 PDT 2007