All LANforge-FIRE Cookbooks

The LANforge-FIRE Cookbook provides a set of high-level examples of how to setup useful test scenarios in LANforge-FIRE for traffic generation. Each example intends to give the reader a brief introduction to the test scenario and a set of step-by-step instructions on how to use the LANforge-GUI to configure the test.

All of the following examples will work on Linux systems running the LANforge software with the LANforge kernel and a sufficient license. If you are running another Linux kernel, you will not be able to exactly duplicate some of the examples, but there are usually work-arounds available to assist you. Please contact us at support@candelatech.com if you have any questions.

If you are using the Windows version of LANforge, you will have to modify ports using the Windows utilities. Everything else should work approximately the same, but the performance is limited to 10Mbps speeds.

LANforge-FIRE Traffic Generation

Before attempting the examples below, ensure that you have successfully followed these software installation guides:

- LANforge-GUI Installation
- LANforge Server Installation

It is also recommended that you back up your current running LANforge Server database so that you may safely return to your current operating state.
1. Switched Network Testing
2. Routed Network Testing
3. Firewall Testing
4. Webserver Testing
5. Introduction to Layer 4-7 Traffic
6. Scripted Cable Modem Testing
7. DSLAM Testing
8. VoIP Testing
9. Armageddon Testing (Accelerated UDP testing)
10. Armageddon Testing with Random MAC Addresses
11. Scripted Layer-3 Test (RFC-2544)
12. Scripted Armageddon Test (RFC-2544)
13. 5000 TCP Connections on unique IP addresses
14. Multiple Thousands of TCP Connections
15. Multiple Thousands of UDP Connections
16. Layer-3 UDP Traffic Generator
17. Armageddon Random MAC Generation
18. Dual Windows Host Layer 3 Testing
19. File IO Endpoint Testing
20. Providing HTTP service on a Port
21. Generating FTP Traffic Between Two Physical Ports
22. Table Report Builder
23. Displaying Sequence Gaps
24. Scalability Testing with NFS File-IO

Generating Traffic to a Switched Network

Goal: Set up and run traffic on a routed network.

In this test scenario, LANforge-FIRE is used to generate traffic to a basic router in order to test throughput.
1. Connect two available data generating ports of your LANforge server to the DUT, an unmanaged switch.

2. Set up the LANforge ports so that they have valid IP addresses.
   A. Go to the Port Manager

   ![LANforge Manager](image1)

   All Ethernet Interfaces (Ports) for all Resources.

   | Port | Pha. | Down | IP   | SEC | Alias | Parent Dev | RX Bytes | RX Pkts | RX Pps | RX bps | RX RX | TX Bytes | TX Pkts | TX Pps | TX bps | RX TX |
   |------|------|------|------|-----|-------|------------|----------|---------|--------|--------|-------|----------|---------|--------|--------|--------|-------|
   | 1.1.0|      |      | 192.168.100.102 | 0    | eth0  |            | 49,388   | 412     | 4      | 1,120  | 184,397 | 233     | 2       |
   | 1.1.1|      |      | 192.168.100.103 | 0    | eth1  |            |          | 0       | 0      | 0      | 0     | 0        | 0       | 0      | 0      | 0      |
   | 1.2.0|      |      | 192.168.100.104 | 0    | eth2  |            | 70       | 1       | 5      | 0      | 0     | 0        | 0       | 0      | 0      | 0      |
   | 1.3.0|      |      | 192.168.100.105 | 0    | eth3  |            | 70       | 1       | 5      | 0      | 0     | 0        | 0       | 0      | 0      | 0      |
   | 1.4.0|      |      | 192.168.100.106 | 0    | eth4  |            |          | 0       | 0      | 0      | 0     | 0        | 0       | 0      | 0      | 0      |
   | 1.5.0|      |      | 192.168.100.107 | 0    | eth5  |            |          | 0       | 0      | 0      | 0     | 0        | 0       | 0      | 0      | 0      |

   Logged in to: 192.168.100.103:8002 as: Admin

   ![eth2 Configure Settings](image2)

   B. Modify port for Endpoint A (eth2)
C. Modify port for Endpoint B (eth3)

D. Verify the port configuration

For more information see LANforge User’s Guide: Ports (Interfaces)

3. Create a Layer-3 connection using the two configured ports.
A. Go to the **Layer-3** tab

B. Create a new Cross-Connect

C. Verify the new Cross-Connect
4. Run traffic and observe results.
   A. Select the cross-connect on the Layer-3 tab, click Start and then Display

   ![Image of LANforge Manager with cross-connects selected]

   Logged in to: 192.168.100.103:4002 as: Admin

   B. View the Layer-3 cross-connect display

   ![Image of Layer-3 cross-connect display]

   For more information see LANforge User's Guide: Layer-3 Cross-Connect Display

5. In this case, the overall throughput of the DUT is approximately 76Mbps. The Report Manager can also be used to record the throughput over time.
A. Select **Reporting Manager** from the **Reporting** pull-down menu.
B. Record test data by following these steps:

A. Select the GUI Data Collection tab.
B. Choose a directory to save raw (.csv) data.
C. Click Save to start the data collection.
D. After desired test duration, click Stop.
E. NOTE: Your report will look cleaner if you stop traffic about 2 minutes before you stop saving data.

C. In the Generate Report tab, choose a directory to save the HTML report. NOTE: Make sure your directory name does not include any special characters such as apostrophes.

A. Click Generate Report.
D. Select the entities to be included

E. Click **Generate Report** to start the report generation
F. This window lists all the reports being generated. The last line indicates the location of the HTML report.

G. View the HTML report

For more information see LANforge User’s Guide: Reporting

Generating Traffic to a Routed Network

Goal: Set up and run traffic on a routed network.

In this test scenario, LANforge-FIRE is used to generate traffic to a basic router in order to test throughput.
1. Connect one LANforge-FIRE port to the router's LAN port.

2. Connect another LANforge-FIRE port to the router's WAN port.

3. Set up the LANforge ports so that they have valid IP addresses.
   A. Go to the Port Manager.
B. Modify port for Endpoint A [eth3]. Set a valid network IP Address and Gateway IP.
C. Modify port for Endpoint B (eth4). Set a valid network IP Address and Gateway IP.

D. Verify the port configuration

For more information see LANforge User's Guide: Ports(Interfaces)
4. Create a Layer-3 connection using the two configured ports.
   A. Go to the **Layer-3** tab

B. Create a new Cross-Connect

C. Verify the new Cross-Connect

For more information see [LANforge User's Guide: Layer-3 Cross-Connects (FIRE)](link)
5. Run traffic and determine router throughput.
   A. Select the cross-connect on the **Layer-3** tab, click **Start** and then **Display**

   ![Layer-3 Cross-Connect Display](image)

  Logged in to: 192.168.10.129:4002 as: Admin

B. View the Layer-3 cross-connect display

   ![Layer-3 Cross-Connect Display](image)

   For more information see **LANforge User’s Guide: Layer-3 Cross-Connect Display**

6. For this example, a low performance router was used to illustrate poor throughput, variable latency, and dropped packets.
   A. Go to the **L3 Endps** tab

   ![Layer-3 Endpoints](image)

   Logged in to: 192.168.106.130:4002 as: Admin
B. Scroll to the right to view Latency and Dropped Packets

For more information see LANforge User's Guide: Layer-3 Endpoints (FIRE)

Generating Traffic to a Firewall

Goal: Set up and run traffic to test a firewall.

In this test scenario, LANforge-FIRE is used to generate traffic to a firewall DUT in order to measure the following benchmarks:

- **UDP Throughput** - Maximum payload bits per second with a UDP traffic flow.
- **TCP Throughput** - Maximum payload bits per second with a TCP traffic flow.
- **TCP Concurrent Connections** - Maximum number of simultaneous TCP connections.
- **TCP Connections per Second** - Maximum number of established TCP connections per second.

**NOTE:** If you are attempting to run this test scenario, you will need a LANforge license key that enables the correct number of ports and multi-connections. Please contact us at support@candelatech.com for assistance.

1. The **UDP Throughput** test will use a scripted Layer-3 connection to vary the rate and payload size to determine the bi-directional UDP throughput of the DUT across the scripted parameters.
A. On the Port Manager tab, set up the LANforge ports with valid IP addresses.

<table>
<thead>
<tr>
<th>Port</th>
<th>IP Address</th>
<th>Alias</th>
<th>RX Bytes</th>
<th>RX Pkts</th>
<th>RX Pkts</th>
<th>TX Bytes</th>
<th>TX Pkts</th>
<th>TX Pkts</th>
<th>Collisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00</td>
<td>192.168.100.173</td>
<td>132.397</td>
<td>1.219</td>
<td>7</td>
<td>6.644</td>
<td>846.575</td>
<td>1034.6</td>
<td>33.572</td>
<td>0</td>
</tr>
<tr>
<td>1.02</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.03</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.04</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.05</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.06</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.07</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.08</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.09</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.10</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.11</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.12</td>
<td>192.168.100.173</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
B. On the Layer-3 tab, create a UDP connection.

A. Set Endpoint A to use the DUT WAN port.
B. Set Endpoint B to use the DUT LAN port.
C. Make sure CX Type is LANforge / UDP then select Apply.

C. Select the Script button to set up the scripting parameters.

A. Set up the script to iterate over the rates.
B. Specify the payload sizes to be tested.

For more information see LANforge FIRE Cookbook example: Scripted Layer-3 Test
D. Highlight the connection and select the **Start** button.
The final test report shows the results of the test run. Here we can see that the DJT has the best bi-directional throughput with 460Byte payloads at 24.9Mbps.

### Script Report for Endpoint: udp-test-A

#### Endpoint Information:
- **Endpoint ID:** udp-test-A
- **Type:** LANMAN_UDP
- **Peer Endpoint ID:** udp-test-B

#### Summary Data for each iteration:

<table>
<thead>
<tr>
<th>#</th>
<th>pld-size</th>
<th>cfg-rate</th>
<th>tx-bps</th>
<th>rx-bps</th>
<th>tx-bps-L</th>
<th>rx-bps-L</th>
<th>tx-pps</th>
<th>rx-pps</th>
<th>tx-pkts</th>
<th>rx-pkts</th>
<th>ca-drops</th>
<th>dropit</th>
<th>nx-iat(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>60</td>
<td>10000000</td>
<td>1313632</td>
<td>1313632</td>
<td>0</td>
<td>7757</td>
<td>7757</td>
<td>1043165</td>
<td>1043165</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>1</td>
<td>128</td>
<td>10000000</td>
<td>2787447</td>
<td>2787447</td>
<td>0</td>
<td>2722</td>
<td>2722</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>256</td>
<td>954632</td>
<td>954632</td>
<td>954632</td>
<td>0</td>
<td>2694</td>
<td>2694</td>
<td>1661194</td>
<td>1661194</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>205</td>
</tr>
<tr>
<td>3</td>
<td>512</td>
<td>999987</td>
<td>999987</td>
<td>999987</td>
<td>0</td>
<td>2640</td>
<td>2640</td>
<td>168596</td>
<td>168596</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>260</td>
</tr>
<tr>
<td>4</td>
<td>1024</td>
<td>999957</td>
<td>999957</td>
<td>999957</td>
<td>0</td>
<td>2220</td>
<td>2220</td>
<td>73109</td>
<td>73109</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>2048</td>
<td>9994381</td>
<td>9994381</td>
<td>9994381</td>
<td>0</td>
<td>676</td>
<td>676</td>
<td>98962</td>
<td>98962</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>4096</td>
<td>993019</td>
<td>993019</td>
<td>993019</td>
<td>0</td>
<td>856</td>
<td>856</td>
<td>51334</td>
<td>51334</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>8192</td>
<td>994447</td>
<td>994447</td>
<td>994447</td>
<td>0</td>
<td>849</td>
<td>849</td>
<td>50923</td>
<td>50923</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>16384</td>
<td>1137869</td>
<td>1137869</td>
<td>1137869</td>
<td>0</td>
<td>2425</td>
<td>2425</td>
<td>104701</td>
<td>104701</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>443</td>
</tr>
<tr>
<td>9</td>
<td>32768</td>
<td>252959</td>
<td>252959</td>
<td>252959</td>
<td>0</td>
<td>7757</td>
<td>7757</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>329</td>
</tr>
<tr>
<td>10</td>
<td>65536</td>
<td>5537149</td>
<td>5537149</td>
<td>5537149</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>11</td>
<td>129096</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>12</td>
<td>257656</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>13</td>
<td>515312</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>14</td>
<td>1030640</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>15</td>
<td>2061280</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>16</td>
<td>4122560</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>17</td>
<td>8245120</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>18</td>
<td>16490240</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>19</td>
<td>32980480</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>20</td>
<td>65960960</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>21</td>
<td>13192192</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>22</td>
<td>26384384</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>23</td>
<td>52768768</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>24</td>
<td>10553752</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>25</td>
<td>21107504</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>26</td>
<td>42215008</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>27</td>
<td>84430016</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
<tr>
<td>28</td>
<td>168860032</td>
<td>1693226</td>
<td>1693226</td>
<td>1693226</td>
<td>0</td>
<td>2677</td>
<td>2677</td>
<td>165827</td>
<td>165827</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>268</td>
</tr>
</tbody>
</table>

For more information see Full script report for the UDP test.
2. The TCP Concurrent Connections test will measure the maximum number of simultaneous TCP connections that the DUT can maintain at once.

   A. On the Port Manager tab, create 5 MAC-VLANs on the LANforge port connected to the DUT LAN port.
B. Verify that the MAC-VLANS have correct IP addresses.
C. Create a Layer-3 connection that has a low-speed rate with **Multi-Conn** set to 10000 and **Min IP Port** to 0 (zero) on **Endpoint-A**. **Multi-Conn** should be set to 1 on **Endpoint-B**.

<table>
<thead>
<tr>
<th>CK Name</th>
<th>CK Type</th>
<th>Resource</th>
<th>Port</th>
<th>Min Tx Rate</th>
<th>Max Tx Rate</th>
<th>Min PDU Size</th>
<th>Max PDU Size</th>
<th>IP ToS</th>
<th>Pkts To Send</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 Gbps</td>
<td>1 Gbps</td>
<td>1 k</td>
<td>1 k</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 (Gbps)</td>
<td>1 (Gbps)</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 k</td>
<td>1 k</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
<td>Same</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Best Effort</td>
<td>Best Effort</td>
<td>Infinite</td>
<td>Infinite</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A. **Endpoint-A** will be one of the MAC-VLANs and **Endpoint-B** will be the port connected to the DUT WAN port. This setup will initiate the TCP sessions from the LAN side of the DUT.

B. Low-speed depends on the DUT, we could also set the rate to zero which would allow the TCP connections to be set up without payload data to be transmitted, but this would not give an accurate picture of the firewall performance. Here we are using 1 Kbps connections with 1KB size payload.

C. This is an iterative test, the number of TCP connections to use will depend on the DUT capabilities. Modify the number of connections as necessary to find the most accurate measurement.

D. The DUT should be power-cycled to reset it before each test run.
D. Select the Batch-Create button to create 4 more copies of this connection each with a new MAC-VLAN port.
E. Highlight and start each set of 10000 connections until the target max simultaneous connections are running.
F. On the Layer-3 Endpoints tab, highlight the Running A-Side Endpoints, then right-click and select Calculations.
G. The top line, Sum, is what we are interested in for Maximum Concurrent TCP Connections.

<table>
<thead>
<tr>
<th>Calculation</th>
<th>Tx Rate</th>
<th>Tx Rate(l)</th>
<th>Rx Rate</th>
<th>Rx Rate(l)</th>
<th>Rx Drop %</th>
<th>Tx Pkts</th>
<th>Rx Pkts</th>
<th>Delay</th>
<th>Dropped</th>
<th>T:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sum</td>
<td>794,202.0</td>
<td>863,665.1</td>
<td>730,812</td>
<td>602.1</td>
<td>543,657.7</td>
<td>75,631</td>
<td>44,928</td>
<td>8.99%</td>
<td>0.55</td>
<td>8.11</td>
</tr>
<tr>
<td>Mean (Average)</td>
<td>708,417.7</td>
<td>613,222.10</td>
<td>296,068.1</td>
<td>45,182.41</td>
<td>72.62</td>
<td>108,731.4</td>
<td>15,122.2</td>
<td>8.99%</td>
<td>0.55</td>
<td>8.11</td>
</tr>
<tr>
<td>Median</td>
<td>744,526</td>
<td>535,911</td>
<td>101,837</td>
<td>141,546</td>
<td>72.25</td>
<td>114,265</td>
<td>15,136</td>
<td>9.55%</td>
<td>0.55</td>
<td>8.11</td>
</tr>
</tbody>
</table>

H. Scroll right to the CX Active and CX Established columns and select the Refresh button. This DUT can maintain a maximum of 41,864 simultaneous TCP connections.

<table>
<thead>
<tr>
<th>Calculation</th>
<th>Tx Bytes</th>
<th>Rx Bytes</th>
<th>TCP Pkt</th>
<th>Dup Pkt</th>
<th>QDD Pkt</th>
<th>RX Wrong</th>
<th>CRC Fail</th>
<th>RX BER</th>
<th>CX Active</th>
<th>CX Estab</th>
</tr>
</thead>
<tbody>
<tr>
<td>ped</td>
<td>596,764</td>
<td>580,113,568</td>
<td>16</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>41,864</td>
<td>47,633</td>
</tr>
<tr>
<td>ped</td>
<td>111,340,16</td>
<td>15,026,313</td>
<td>3,2</td>
<td>0,2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8,372,8</td>
<td>9,526,8</td>
</tr>
<tr>
<td>ped</td>
<td>137,067,15</td>
<td>15,005,164</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>9,088,10</td>
<td>10,128</td>
</tr>
</tbody>
</table>

- CX Active is the metric we are attempting to measure for Maximum Simultaneous TCP Connections. It will fluctuate with the DUT's ability to maintain the number of active TCP connections.

- CX Established is the number of TCP connections LANforge has established since the start of the test. It will continue to increase as the DUT closes the TCP connections it cannot maintain.
3. The **TCP Connections per Second** test will measure the rate of TCP connections that can be set up through the DUT.

   A. Create a Layer-3 TCP connection with the Duration and IP Port set to zero.

![TCP Connections per Second Test Setup](image)
B. Highlight and Start the connection.
C. View the **CX-Estab/s** rate on the Layer-3 Endpoints tab. This DUT can set up about 120 connections per second.

For more information see LANforge GUI User's Guide

**Generating Traffic to a Web Server**

**Goal: Set up and run traffic to a web server.**

In this test scenario, LANforge-FIRE is used to generate traffic in the form of URL requests in order to determine the maximum number of URLs/second the web server can process.

Please note that the web server used in this example is an isolated Linux system running Apache.

1. Connect one LANforge-FIRE port to the server's network.
2. Set up the LANforge port so that it has a valid IP address.
A. Go to the Port Manager

B. Modify the port connected to the web server. Set a valid network IP address and Gateway IP.
C. Verify the port configuration

For more information see LANforge User's Guide: Ports (Interfaces)

3. Set up the URL requests.
   A. Go to the Layer 4-7 tab
B. Create a Layer 4-7 Endpoint:

A. Enter a name and select the port configured in the previous step.
B. URLs per 10m should be set to around 1,200,000 which is 2,000 URLs/second.
C. Leave the SSL Cert alone as we are not using it in this example.
D. UL/DL should be set to Download.
E. URL should be set to the web server's IP address and file that you wish to download. In this example, index.html is a small test file.
F. File is the designated location that the downloaded file will be stored. In this example, we use /dev/null which will essentially throw the file away so that it does not slow down the LANforge system with writing files.
G. Select the 'Allow-Reuse' checkbox to maximize the number of URL requests LANforge can make per connection.
H. Click Apply or OK to create the Layer 4-7 endpoint.

C. Create 9 more Layer 4-7 endpoints by opening the previously created endpoint and clicking Batch-Create.

A. Set the Quantity to 9, Number of Digits to 2, and Port Increment A to 0. Then click Apply.
B. Each of the 10 Layer 4-7 Endpoints will attempt to generate 2000 URLs/second, effectively generating 20,000 URLs/second.

For more information see LANforge User's Guide: Layer 4-7 Endpoints
4. Run traffic and determine web server performance.

   A. On the Layer 4-7 tab, select one Layer 4-7 endpoint, click Start, then repeat for all 10 Layer 4-7 endpoints:

   ![Layer 4-7 Endpoints Table]

   A. As each endpoint is started, the rate of URLs/second will start to converge on a rate that the web server is capable of providing. Finding the final web server performance rate is a matter of adding up the rates of all running Layer 4-7 endpoints.

   B. Several Layer 4-7 endpoints (10 in this case) are used so each endpoint can make an independently large number of URL requests without having to wait for too many replies. Each URL request is waiting for a reply from the web server, so if only one Layer 4-7 endpoint was making requests, it would spend too much time waiting for replies instead of generating more requests. Spreading the URL requests over several endpoints allows each LANforge connection to the web server to maximize its rate of URL requests.
B. Layer 4-7 Endpoint Results:

For more information see LANforge User’s Guide: Layer 4-7 Endpoints

**Introduction to Layer 4-7 Traffic Generation**

**Goal: Use LANforge to emulate layer 4-7 download traffic**

Creating web browsing and movie watching is a common task with LANforge. This cookbook will introduce HTTP download examples and describe the difference between the Layer 4-7 and Generic traffic generation techniques. We will begin on a CT520a with 20 stations. There are two methods of emulating web browsing:

1. **Layer 4-7 connections**: these are workers doing downloads using `curl`

2. **Generic connections**: these are scripts call programs that can download or upload. Not just any program can be used, these programs need to be able to bind to a specified network interface.

If you want to:

...load test a web server, you will use mostly use **Layer 4-7 connections**.

...multiple video streams, you would use **Generic connections** that call `c-clive`

...upload files, you would use **Generic connections** that call `curl`

The following examples do not assume your LANforge has a route to the Internet, but are pointing at a webserver at an IP address. We are going to show making a common mistake in the first example.
Simple HTTP Get

2. Check your Port Mgr tab and note we have 20 stations on resource 2, radio wiphy0.

3. Move to the Layer 4-7 tab
4. Create a new connection, this example is named `www1`, on resource `sta1000`. Next, consider the **URLs per 10 minute** field.

A. Hover your mouse over the **URLs per 10 min** field to see the tooltip. If you wanted to create five connections a second, that would be **3000** connections in 10 minutes. This differs from the Max Speed field, which sets the maximum bit per second of the connection.

5. Continue with other settings. We are purposely going to make an error and diagnose it.
A. Set the request rate, choose the number of URLs per 10 min to **3000**

B. DNS Cache Timeout: 600

C. Select **Gzip**

D. Set URL to [http://10.136.0.1/](http://10.136.0.1/)

E. Set Destination file or directory to `/dev/null` if you are on Linux. (If you are on Windows, you need to use `NUL`)

F. Select **Enable 4XX** to show errors in logs

G. Select **Bind DNS** so that hostnames are resolved over **sta1000** (not over our management port)

H. Click **Apply**. Do not close this window.

6. Back in the Layer 4-7 tab, select the connection

7. **Start** the connection
A. ... then click Display

8. Watch the www1 endpoint window...

A. Notice how there is no traffic to ctweb; because the hostname won't resolve over our test network. This is a common mistake. Let's use the IP of our other LANforge hosting our test network instead.

9. Change the URL to use an IP address: http://10.136.0.1/
A. Click **Apply**

B. Do not close the window.

10. The endpoint display now shows traffic.
A. Not having DNS resolution is a common problem in test networks.
B. It can cause problems when connecting to a https website and getting certificate errors.
C. Click Close

11. It is pretty simple to create a connection per WiFi station on our LANforge. Return to our Create/Modify L4Endpoint window for www1.

A. Click Batch-Create

12. In the Batch Create window, create 19 more connections.
13. Back in the Layer 4-7 lab, observe all our connections

14. Highlight them, and click Start
15. Note that if we were to Right Click → Display to show dynamic report

16. Right Click → Dynamic Report to show dynamic report

A. This shows throughput for all the connections.

B. Notice how crowded this graph is. There is a simpler way to display overall throughput.

17. Next, select the Port Mgr tab.
   A. Select resource 2, radio wiphy0
B. Right Click → Dynamic Report to show dynamic report

C. See the overall throughput through the radio
Scripted All-in-One Cable Modem Testing

Goal: Use LANforge to test CMTS and cable-modem network (DUT).

LANforge will serve DHCP and TFTP to the DUT, generate TCP traffic to measure upload and download speeds on each modem, and generate reports. In this example, eth0 is the management port, eth1 is the upstream network port (connects to CMTS), and ports eth2-eth9 are connected to cable modems. Eth2-9 are configured for DHCP, and eth1 is configured with static IP. Eth1 is also configured to serve DHCP requests to the cable modems and other LANforge ports.

1. Set up the network interfaces.

2. Configure eth1 to serve DHCP and TFTP.
   A. Go to Status panel in LANforge GUI. Click 'Netsmith' button on the resource.
   B. Right-click in empty space and select New Router. Use default values and click OK.
   C. Drag eth1 into the virtual router. Then double-click the virtual eth1 icon to configure DHCP. DHCP files for CMTS setups must be hand-written by the user. Configure LANforge to use this custom-dhcp config file.

   ![DHCP Configuration](image)

   D. When Netsmith setup is complete, click Apply on the main Netsmith window to start up the DHCP service, etc. This screenshot was taken after the Layer-3 connections were set up.

3. Configure eth2-9 to use DHCP.
   A. Go to Port-Mgr tab, double-click each port, and make sure the DHCP option is selected. Apply changes.

4. Set up Layer-3 connections to generate the throughput tests.
A. Go to the Layer-3 tab, and click Create. Many cable modems are configured to do NAT and/or some firewalling, so normally you will need the connections to be TCP and to originate out from the client-side port. So, choose the LANforge/TCP connection type, and make the ‘B’ side eth1. Everything else can stay at the default values because we will use a script to automate the settings.

B. Create 7 similar connections, always with B side port of eth1, and use A side ports eth2-eth9. In the Create/Modify window you can just change the name, change the port, and press apply. This will make copies of the connections.

A. You can also use Batch-Create (located in the Create/Modify window) to create these connections.

5. Create Test-Group to control the 8 Layer-3 TCP connections.
A. Go to the Test Group tab, and click Create. Give your test group a name, select the 8 Layer-3 TCP connections you just created in the previous step and add those to the Test Group. Click Apply and make sure the new group shows up in the Test Group table.

B. We need to add a script to automate the test. Click the Script button in the Test Group create/modify window. Choose RFC 2544 script type. In this scenario, we want to test each modem one at a time, so we select the Sequential option for Group Action. The rates sections determine the speeds for each iteration. In this case, the first iteration will send from B to A at 35Mbps. This is the download test. The next iteration will upload from A to B at 17Mbps. When the two iterations are complete, the script will repeat on the next Layer-3 connection.

6. Run the test.
A. To start the test, select the Test Group in the table and click the Start button. You should see a script-report window pop up, and the state should go to running. To see a live report of throughput and other values, right-click on the Test Group table and select the Dynamic Report option.

B. View the individual connections from the Layer-3 tab.

7. Gather reports.
A. When the script completes, a summary of each iteration will be shown in the Script Report window. The text may be converted to HTML, but for this particular script, the graphs are not useful because we are using Sequential mode, so just saving the text to a file or printing it is probably the best option. Note that some of these tests failed the constraints configured in the script. In this case, it is because those moderns were not capable of the requested speeds.

B. When the script completes, you could also pause the dynamic report and print it. For an electronic copy, use a PDF printer to create PDF files instead of printing to paper.

C. The Layer-3 tab will color-code the 8 connections, with red meaning fail, and green meaning pass. You can print the connections you are interested in by selecting them in the table and using right-click → Table Report. This report can be printed or otherwise saved.
Generating Traffic for DSLAM Testing

Goal: Set up and run traffic to a DSLAM system as shown in the CT570 product description.

Please refer to the diagram in the CT570 link above. In this test scenario, the LANforge-FIRE Core is one interface on a LANforge system. The LANforge-FIRE Edge is another interface on the same LANforge system. The LF Core interface is connected to the upstream DSLAM interface either directly or through a switch. The CPEs are connected to a multi-port VLAN switch which has a VLAN trunk that is connected to the LF Edge. Traffic is sent between the LF Core and the LF Edge to achieve end-to-end network traffic testing of the DSLAM system.

1. Connect one LANforge-FIRE interface to the DSLAM upstream internet connection. This is the LF Core part of the diagram mentioned above.

2. Set up the LANforge port so that it has a valid IP address and IP mask.
   A. Go to the Port Manager
B. Modify the port connected to the DSLAM. Set a valid network IP address and IP mask.

C. Verify the port configuration

For more information see LANforge User's Guide: Ports (Interfaces)
3. Set up virtual interfaces.
   A. On the Port Mgr tab, select the port that will connect to the multi-port switch and will also be your VLAN trunk. This is the LF Edge part of the diagram.
   B. Click the Create button:

   A. Select the 802.1Q-VLAN virtual interface type
   B. The VLAN ID should correspond to your multi-port switch VLAN configuration
   C. Enter Quantity (number of virtual interfaces to be created)
   D. Enter the appropriate IP address and IP mask
   E. Click Apply to create the virtual interfaces

   C. Verify that the virtual interfaces are created and have the correct IP assignments

4. Create Layer-3 connections.
A. Go to the **Layer-3** tab

B. Click the **Create** button

A. Fill in a connection name, select a connection type and set the report timer

B. Make endpoint A the DSLAM upstream port or LF Core

C. Make endpoint B the CPE downstream port or LF Edge

D. You can make the TX/RX rates asymmetric for the connection to simulate how the connection would be used in a real-world scenario. Here we have about 5Mbps downstream (DSLAM to CPE) and 1Mbps upstream (CPE to DSLAM).

E. Click **Apply** to create the connection
C. Create multiple connections

- Click **Batch-Create** located in the Layer-3 connection's Create/Modify window to create four additional connections.
- Set **Quantity** to 4, **Port Increment A** to 0.
- Click **Apply**.

For more information see [LANforge User's Guide: Layer-3 Endpoints (FIRE)](https://example.com)
5. Run traffic.
   A. Select the connections you want to start

   ![LANforge Manager Screen]

   B. Click the Start button

   ![LANforge Manager Screen]

For more information see [LANforge User's Guide: Layer-3 Endpoints (FIRE)](http://example.com)

**Generating Traffic for VoIP Testing**
Goal: Set up and run VoIP traffic.

In this example, LANforge-FIRE is used to set up two VoIP test calls that may be used as a basis for VoIP load testing or VoIP Gateway testing.

- **Test 1**: Directed VoIP call where a LANforge endpoint calls another LANforge endpoint.
- **Test 2**: Gateway VoIP call where two LANforge endpoints register with a VoIP Gateway so that the call from one endpoint to the other goes through the gateway. The VoIP Gateway used in this example is Asterisk.

1. Set up the LANforge physical connections. The same two ports are used for both tests. Connect eth1 and eth2 from the LANforge-FIRE system to a network switch that is also connected to the VoIP Gateway. This example assumes that your VoIP Gateway is set up properly. If you need assistance, you can contact us at support@candelatech.com or you can find a basic Asterisk setup at this link: [LANforge FAQ: How do I configure Asterisk for SIP Phones?](#).

2. Set up the LANforge ports so that they have valid IP addresses and IP masks.
   - Go to the Port Manager.

   ![LANforge Manager](image)

   - All Ethernet Interfaces (Ports) for all resources:
     - Port 1.1.0
     - Port 1.1.1
     - Port 1.1.2
     - Port 1.1.3
     - Port 1.1.4
     - Port 1.1.5

   - IP addresses:
     - eth0: 192.168.100.101
     - eth1: 192.168.100.102
     - eth2: 192.168.100.103
     - eth3: 192.168.100.104
     - eth4: 192.168.100.105

   - Other details:
     - RX Bytes
     - RX PKts
     - TX Bytes
     - TX PKts
     - Pps TX
     - Pps RX
     - RX Pps
     - TX Pps
     - RX Pps
     - TX Pps

   - Logged in to: 192.168.100.103:4002 as: Admin
B. Modify eth2 and eth3 to set a valid network IP address and mask

A. If your network has DHCP service, you can select the 'DHCP-IPv4' checkbox so that each port is a DHCP client and will acquire its IP address from your DHCP server.

C. Verify the port configuration

For more information see LANforge User's Guide: Ports (Interfaces)
3. Set up Test 1, a Directed VoIP call.
   A. Go to the **VoIP/RTP** tab

   ![LANforge Manager interface](https://example.com/image)

   B. Click the **Create** button:

   ![Create/Modify Cross Connect](https://example.com/image)

   A. Enter test-1 in the **CX Name** field
   B. Select the **Multi-Call** and **Directed** buttons
   C. Endpoint A is on port eth2 in this example. If you have a PESQ licensed server available, you can select **Record** and **Enable PESQ**.
   D. Endpoint B is on port eth3. If you are using PESQ, be sure to enter a **Record File** and the IP address and port of your PESQ licensed server. Be sure to select the **Rcv Call** checkbox for this endpoint to receive the call.
   E. Click **OK** to create the VoIP Directed call

C. Verify that the test call is created

For more information see **LANforge User's Guide: VoIP Call Generator**
4. Set up Test 2, a Gateway VoIP call.
   A. Go to the VoIP/RTP tab

   ![LANforge Manager](image)

   B. Click the Create button:

   ![Create/Modify Cross Connect](image)

   A. Enter test 2 in the **CX Name** field
   B. Select the **Multi-Call** and **Use Gateway** buttons
   C. Endpoint A is on port eth2, in this example. Be sure to enter the proper username and password for the endpoint so that it can authenticate with the VoIP Gateway if necessary.
   D. Endpoint B is on port eth3. Be sure to select the **Rcv Call** checkbox for this endpoint to receive the call.
   E. Click **OK** to create the VoIP Gateway call
C. Verify that the test call is created

5. Run test-1 and test-2 individually.
   A. Select test-1 and click the **Start** button

For more information see **LANforge User's Guide: VoIP Call Generator**
B. Go to the VoIP/RTP Endps tab to see detailed results:

A. The PESQ score will be reported after the first successful call is completed and updated after each subsequent call.

B. **NOTE**: Endpoints are unregistered while the call is in progress because they are not calling through the VoIP gateway.

C. Stop test-1, select test-2 and click **Start**.
D. Go to the **VoIP/RTP Endps** tab to see detailed results:

![LANforge Manager Interface]

<table>
<thead>
<tr>
<th>Calls Attempted</th>
<th>Calls Completed</th>
<th>Calls Failed</th>
<th>CF 404</th>
<th>CF 408</th>
<th>CF Busy</th>
<th>CF Cancel</th>
<th>Calls Arr</th>
<th>Destination Addr</th>
<th>Source Addr</th>
<th>Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>02163186</td>
<td>4826976</td>
<td>348</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>04826976</td>
<td>2103186</td>
<td>348</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>09031860</td>
<td>9502721</td>
<td>114</td>
</tr>
</tbody>
</table>

- PESQ remains 0:0 when it is disabled for the call in progress
- **NOTE:** Endpoints are registered with the VoIP gateway while the call is in progress
- Calls Attempted, Calls Completed and Calls Failed can be viewed by scrolling to the right on the **VoIP/RTP Endps** tab

For more information see LANforge User's Guide: VoIP Call Generator

### Generating Traffic Using Armageddon

**Goal:** Set up and run near line-speed 1Gbps traffic using the LANforge Armageddon feature.

- For more information, see the LANforge User's Guide: Armageddon (Accelerated UDP)

In this test scenario, LANforge Armageddon is set up to run at about 80,000 packets/second full-duplex to achieve near line-speed 1Gbps traffic generation.

**Note:** In order to use the LANforge Armageddon feature, your system must have the LANforge kernel patch applied and your system must be properly licensed. Please feel free to contact us at support@candeliatech.com if you would like to obtain a demo license for the Armageddon feature.

1. Configure the physical interfaces.
A. Go to the Port Manager and select ports eth2 and eth3

B. Modify ports eth2 and eth3:

A. In this example, eth2 and eth3 are physically connected with a patch cable
C. Configure each port with a valid IP address, then click OK

For more information see LANforge User's Guide: Ports [Interfaces]
2. Create the Armageddon cross-connect.
   A. On the Armageddon tab, click the Create button

B. Enter a CX Name, select ports eth2 and eth3, then enter the speed and packet size for both endpoints

   A. For this example, 10000pps at 1514 byte packet size should generate about 121Mbps
   B. Click OK when finished
C. Verify that the Armageddon connection is created

For more information see LANforge User's Guide: Armageddon (Accelerated UDP)

3. Run the Armageddon cross-connect and view results.
   A. Select the Armageddon connection then click Start
Generating Armageddon Traffic Containing Random MAC Addresses

**Goal:** Set up and run traffic containing random MAC addresses using the LANforge Armageddon feature.

For more information, see the LANforge User's Guide: Armageddon (Accelerated UDP)

In this test scenario, LANforge Armageddon is set up to run with random MAC addresses. This is useful when performance/stress testing network devices that may not be able to keep up with high-speed traffic containing rapidly changing MAC addresses.
Note: In order to use the LANforge Armageddon feature, your system must have the LANforge kernel patch applied and your system must be properly licensed. Please feel free to contact us at support@candleite.com if you would like to obtain a demo license for the Armageddon feature.

1. Configure the physical interfaces.
   A. Go to the Port Manager and select ports eth2 and eth3

   ![LANforge Manager](image1)

   B. Modify ports eth2 and eth3

   ![eth2 (je2) Configure Settings](image2)

   A. In this example, eth2 and eth3 are connected to another LANforge system running a WanLink so that the Armageddon traffic can be sniffed off the other machine's interface

   B. **NOTE:** Be sure that both ports are in Promiscuous mode by selecting the Set PROMISC and PROMISC checkboxes
C. Configure each port with a valid IP address, then click OK

For more information see LANforge User's Guide: Ports (Interfaces)
2. Create the Armageddon cross-connect.
   A. On the Armageddon tab, click Create

   ![LANforge Manager](image)

   Logged in to: 192.168.100.100:8080 as: Admin

   B. Enter a CX Name, select ports eth2 and eth3, then enter the speed and packet size for both endpoints

   ![Create/Modify Armageddon Endpoint](image)
C. Enter values for the Source and Destination MAC addresses, specify a MAC count, and deselect Use Router MAC for both endpoints.

For more information see LANforge User’s Guide: Armageddon (Accelerated UDP)

3. Run the Armageddon cross-connect and verify results with Wireshark.
   A. Select the Armageddon connection then click Start
B. On the Port Mgr tab of the other LANforge system, select one of the physical interfaces in the Armageddon connection.

C. Click Sniff Packets to launch Wireshark and begin sniffing traffic.

A. Stop the Wireshark capture after a few seconds via the stop icon or pull-down menu (Capture>Stop)
D. Select several packets and note their MAC addresses

For more information see **LANforge User's Guide: Armageddon (Accelerated UDP)**

**Scripted Layer-3 Test**

**Goal:** Use RFC-2544 as a guide to create a Layer-3 connection that can run automatically through various payload sizes and rates for a specified duration.

In this example, LANforge is used to set up a scripted connection that will iterate through a user-defined list of payload sizes and transmission rates. Each iteration will run for a user-defined duration with a user-defined pause between iterations. A summary text report is generated at the conclusion of all iterations,
1. Create a Layer-3 connection. For more information see *Generating Traffic to a Switched Network*

2. Modify the Layer-3 connection to add the script.
   A. Highlight the Layer-3 connection and select *Modify*.

   ![Cross-Connect](image1)

   B. Select the *Script* button on Endpoint A.

   ![Add/Modify Script](image2)
C. Select the Script Type, RFC-2544.

A. **Note:** A default set of payload sizes are set up based on RFC-2544 but, can be changed by typing over the default values.

B. **Note:** For Layer-3 UDP and TCP connections, ‘payload size’ refers to size of the payload being carried by the protocol and not the ethernet frame size.
3. Set up script options. For details refer to: **LANforge User’s Guide: Scripted Cross Connect**

   A. Select **Symmetric** for the script to run both endpoints for a bi-directional traffic test.

   B. Set the **Run** and **Pause Duration**.

   A. Note the total number of **Script Iterations** and **Estimated Total Duration** to help determine how long it will take to run the script.
C. Select OK to close the Add/Modify Script window.

D. The Script Type for Endpoint B is set to NONE because Endpoint A is controlling both ends of the connection in this symmetric script example.

E. Select OK to close the Create/Modify Cross Connect window.
4. Start the Scripted Layer-3 Cross Connect.
   A. Highlight the Layer-3 connection and select Start.

   ![LANforge Manager Interface]

   Logged in as: brent@gpt:4002 as: Admin

   B. A script report window will pop up and show the details of each iteration of the scripted connection as it is run.
Goal: Use RFC-2544 as a guide to create an Armageddon connection that can run automatically through various payload sizes and rates for a specified duration.

In this example, LANforge is used to set up a scripted connection that will iterate through a user-defined list of payload sizes and transmission rates. Each iteration will run for a user-defined duration with a user-defined pause between iterations. A summary text report is generated at the conclusion of all iterations.
1. Create an Armageddon connection. For more information see Armageddon Testing (Accelerated UDP)

2. Modify the Armageddon connection to add the script.
   A. Highlight the Armageddon connection and select Modify.

   ![Screenshot of Armageddon configuration interface]

   - Create/Modify Armageddon Endpoint
     - Cross Connect Information
     - TX Endpoint (endpoint A)
     - RX Endpoint (endpoint B)

   Use the configuration options to set up the desired connection and script parameters.
B. Select the **Script** button on Endpoint A.

C. Select the **Script Type** ‘RFC-2544’.

---

A. **Note**: A default set of payload sizes are set up based on RFC-2544 but, can be changed by typing over the default values.

B. **Note**: For Armageddon UDP connections, ‘payload size’ refers to the ethernet frame size.

For more information see [LANforge User’s Guide: Scripted Armageddon Cross Connect](#)
3. Set up script options.
   A. Select Symmetric for the script to run both endpoints for a bi-directional traffic test.

   ![Script Configuration Diagram]

   B. Set the Run and Pause Duration, max failure thresholds, and modify Rates and Payload Sizes as needed.
C. Note the total number of Script Iterations and Estimated Total Duration to help determine how long it will take to run this script.

D. Select OK to close the Add/Modify Script window.
E. The Script Type for Endpoint B is set to NONE because Endpoint A is controlling both ends of the connection in this symmetric script example.

F. Select OK to close the Create/Modify Cross Connect window.

For more information see LANforge User's Guide: Scripted Armageddon Cross Connect
4. Start the Scripted Armageddon Cross Connect.

A. Highlight the Armageddon connection and select **Start**.

B. A script report window will pop up and show the details of each iteration of the scripted connection as it is run.
Goal:
Quickly set up 5000 TCP connections from 5000 different IP addresses.

5000 concurrent TCP streams and IP addresses

Goal: Quickly set up 5000 TCP connections from 5000 different IP addresses.

Requires LANforge 5.2.10 or later. Use the new feature in 5.2.10 that lets multi-conn Layer-3 TCP connections use a range of secondary IPs to quickly create 5000 stateful TCP/IP connections on different IP addresses. This example uses two 10G ports on a system similar to the LANforge CT503-MIX systems but the procedure should work on all properly licensed higher-end systems. A standard LANforge license only supports 1000 concurrent connections, contact your sales representative for additional licenses. This cookbook assumes basic familiarity with LANforge.
1. Create 5000 secondary IP addresses on an ethernet port. The IP address range should be on the same subnet as the primary IP address on this interface.
   A. Go to the Port Manager tab, select the client-side ethernet port and click Modify. Ensure subnet mask is 255.255.0.0 or similar so we have plenty of room to add the 5000 secondary IPs on the subnet. Apply if changes were made.
B. Click the **Secondary-IPs** button to bring up the Secondary IP address management window. Enter the IP address range similar to the image below and click **Apply**:

C. Click **Sync** after a few minutes to make sure all of the new IP addresses were properly created.
D. Make sure a second ethernet port on the LANforge is properly configured for the server-side of the network. In this case, we are using a network-emulator in bridge mode as device-under-test, so all IP addresses are on the same subnet.

For more information see LANforge User's Guide: Ports (Interfaces)

2. Create a Layer-3 TCP connection to utilize these 5000 secondary IPs and start the traffic.
   A. Go to the Layer-3 tab and click Create. Configure the CX Name, CX Type, Ports, and PDU Size in section 1. The port in the green section should be the one with the secondary IP Addresses. In section 2, configure Min IP Port in the green section, and Multi-Conn in both. In section 3, select ‘Linear’ for the IP Addr selection box in the green section. In section 5, select the Concurrent IP Addr checkbox in the green section.
Goal:

Set up and run traffic on multiple thousands of stateful TCP connections.

As of LANforge release version 5.1.4, LANforge-FIRE has the capability to create multiple thousands of TCP connections using only two ports on one Layer-3 connection that can all run simultaneously and in a stateful manner. This feature can be used to test connection state aware devices such as firewalls, stateful packet inspection systems and intrusion detection/prevention systems.

The upper limit of the total number of concurrent connections is determined by the processor speed and total memory available on the system running the LANforge software. In addition, the packet rate and payload size of each connection will also affect performance.

NOTE: If you are attempting to run this test scenario, you will need a LANforge license key that enables the correct number of multi-connections. Please contact us at support@candletech.com for assistance.
1. For this example, two physical ports on a single LANforge system are connected together.

2. Set up the LANforge ports so that they have valid IP addresses and IP masks.
   A. Using the LANforge GUI, go to the Port Manager tab.

   ![LANforge Manager](image)

   - Logged in to: FF00:0c:1412:00:00:4002 as: Admin

   - All Ethernet Interfaces (Ports) for all Resources.

   - Port: 1.1.0, IP: 192.168.100.185.0, Alias: eth0, RX Bytes: 12,349,471, TX Bytes: 125,350, RX Pkts: 15, TX Pkts: 177,232

   - Port: 1.1.1, IP: 192.168.100.186.0, Alias: eth1, RX Bytes: 0, TX Bytes: 0, RX Pkts: 0, TX Pkts: 0

   - Port: 1.1.2, IP: 192.168.100.187.0, Alias: eth2, RX Bytes: 0, TX Bytes: 0, RX Pkts: 0, TX Pkts: 0

   - Port: 1.1.3, IP: 192.168.100.188.0, Alias: eth3, RX Bytes: 0, TX Bytes: 0, RX Pkts: 0, TX Pkts: 0

   - Port: 1.1.4, IP: 192.168.100.189.0, Alias: eth4, RX Bytes: 0, TX Bytes: 0, RX Pkts: 0, TX Pkts: 0

   - Port: 1.1.5, IP: 192.168.100.190.0, Alias: eth5, RX Bytes: 0, TX Bytes: 0, RX Pkts: 0, TX Pkts: 0

B. Assign IP addresses and masks to the two ports.

   ![Port Status Information](image)

   - Port Status Information
     - Current: LINKUP 10G-FD TSO GSO GRE
     - Driver Info: Port Type: Ethernet, Driver: ixgbe(4.1.1-k) Bus: 0000.02.00.1 Cur: 5GT/s x16 Max: 5GT/s x16

   - General Interface Settings
     - IP Address: 172.16.0.102/24, Global IPv6: AUTO, IPv6 GW: AUTO

   - Port Rates
     - 10Gb-HD, 10Gb-FD, 100Gb-HD, 100Gb-FD, 40Gb-FD

   - Offload
     - TSO Enabled, UGO Enabled, GSO Enabled, LRO Enabled, XRO Enabled, Flow-Control
C. Verify the port configuration.

For more information see LANforge User's Guide: Ports (Interfaces)
3. Set up a Layer-3 Multi-Conn TCP connection.
   A. Go to the **Layer-3** tab, and select the **Create** button.

   ![Layer-3 Multi-Conn TCP connection](image1)

   B. For Endpoint A, type in a name in the **CX Name** field, choose a **CX Type** of ‘LANforge/TCP’, choose the correct ports and set the **Report Timer** to ‘last (1 s)’.

   ![Set up Layer-3 Multi-Conn TCP connection](image2)

   C. Set the **Min Tx Rate** on both Endpoints A and B to ’9.6Kbps’. Leave the **Max Tx Rate** on both set to ‘Same’.

   ![Set up Layer-3 Multi-Conn TCP connection](image3)

   A. **NOTE**: Higher speeds and/or bursty transmit rates will require more memory to process per connection.
D. Set the **Min PDU Size** on both Endpoints A and B to '1024B'. Leave the Max PDU Size on both set to 'Same'.

<table>
<thead>
<tr>
<th>CX Name</th>
<th>CX Type</th>
<th>Resource</th>
<th>Port</th>
<th>Min Rx Rate</th>
<th>Max Rx Rate</th>
<th>Min PDU Size</th>
<th>Max PDU Size</th>
<th>IP ToS</th>
<th>Pkts To Send</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td>1 (f1005c-cs-141.20020)</td>
<td>4 (eth4)</td>
<td>Same</td>
<td>Same</td>
<td>1k</td>
<td>1k</td>
<td>Best Effort (0)</td>
<td>Infinite</td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>1 (f1005c-cs-141.20020)</td>
<td>5 (eth5)</td>
<td>Same</td>
<td>Same</td>
<td>1k</td>
<td>1k</td>
<td>Best Effort (0)</td>
<td>Infinite</td>
</tr>
</tbody>
</table>

A. **NOTE**: Larger packet sizes will use more memory, smaller packet sizes will require more CPU processing time.

E. Set **Min IP Port** to 0 (zero) on Endpoint A. Leave the Min IP Port on Endpoint B set to AUTO.

F. Leave the **Min Duration** set to Forever and **Max Duration** set to Same for both endpoints, unless you want each of the multiple TCP connections to teardown and restart after a specified duration.
G. For Endpoint A, set the Multi-Conn to the desired number of multiple TCP connections.

A. You can type in any value that your license allows here or choose one from the drop down box. The recommended approach is to create a new Multi-Conn connection for every 5000 connections.

H. For Endpoint B, set the Multi-Conn to one, then select OK to create the connection.

A. Endpoint B is the 'server' side of the TCP connection, therefore it is only necessary to have one Multi-Conn set up on Endpoint B to reply to all of the Endpoint A TCP SYN packets when the 5000 connections are being established.

For more information see LANforge User’s Guide: Creating & Modifying Cross Connects

4. Create 5 more Layer-3 Multi-Conn TCP connections.

A. On the Layer-3 tab, highlight the first connection created in the previous step and select Modify.
B. Select the **Batch-Create** button.

C. Set the **Quantity** to 5, and set **Port Increment A** and **Port Increment B** to 0 (zero).

D. Select the **Apply** button.
E. Verify that six Multi-Conn TCP connections were created.

For more information see LANforge User's Guide: Layer-3 Endpoints (FIRE)
5. Run traffic and verify results.
   A. Highlight all six connections.

   ![LANforge Manager](image)

   B. Select the **Start** button

   ![LANforge Manager](image)
C. Go to the L3 Endps tab to verify that all 30,000 connections are running.

D. Or, go to the Port Mgr tab, and sniff one of the ports while the Multi-Conn TCP connections are running.

---

A. **NOTE:** You will need a lot of memory to run a Wireshark capture on 30,000 connections. It is probably best to stop all connections, set up the Wireshark capture, start all connections and let them run for 30 seconds to 1 minute before stopping them all, then stop the Wireshark capture and wait for it to process all those packets!
**Goal:**
Set up and run traffic on multiple thousands of UDP connections.

LANforge-FIRE has the capability to create multiple thousands of UDP connections using only two ports. This example creates 1000 Layer-3 connections between two sets of 1000 MAC-VLANS that can all run simultaneously. This feature can be used to test stateless connection services such as DNS, DHCP, and file streaming systems.

The upper limit of the total number of concurrent connections is determined by the processor speed and total memory available on the system running the LANforge server software. In addition, the packet rate and payload size of each connection will also affect performance. Larger packet sizes take less CPU time to process.

**NOTE:** If you are attempting to run this test scenario, you will need a LANforge license key that enables the correct number of ports. Please contact us at support@candelatech.com for assistance.
1. For this example, we are using a CT503-MIX 1Gx4 with multiple 10 Gigabit fiber NICs. We have cabled two physical ports on this single LANforge system together. Our plan of action will be to create 1000 MAC-VLANs on each port as endpoints for 1000 Layer-3 UDP cross connections.

A. **Connection Suggestion:** If you are using the LANforge GUI Client remotely connected to your LANforge Server (like using a VPN), this process will appear rather sluggish. This sluggishness is caused by the volume of reporting traffic flowing to the GUI. We suggest you connect to the LANforge Server desktop using Remote Desktop or VNC.

B. **Reporting Suggestion:** When creating 2000 MAC-VLANs and 1000 Layer-3 connections, we are actually creating $2000 + (3 \times 1000) = 5000$ reportable entities that could generate up to $5000 \times 4kB = 20,000kB$ of traffic per reporting interval. We intentionally set our reporting intervals low (10 or more seconds) to keep the GUI client responsive.

2. Set up two physical ports so that they have 0.0.0.0 IP addresses and IP masks. We will choose eth4 and eth5 for this example. We will base our MAC-VLANs off these two physical ports. Set the reporting level for these two ports to a low frequency: 30 sec.
A. In the LANforge GUI, go to the Port Manager tab.

B. Assign IP addresses and masks to the two ports.

C. Verify the port configuration.

For more information see LANforge User's Guide: Ports [Interfaces]
3. We will use the Port Batch Create tool to create 1000 MAC-VLANs on each of the two ports. These MAC-VLAN ports should report more frequently than the parent ports; set them to report every 15 seconds. We also want to create MAC addresses that are distinct for these two groups: the first three octets will match the parent port, but we will set their fourth octets to 04 and 05 to remind us of their parent ports. The following two octets will be random (specified with ‘*’).

A. In the Ports tab, highlight port eth4 and click the Create button.

B. Follow these steps to create 1000 MAC-VLANs on the port:

1. **MAC-VLAN**
2. **B08.1Q-VLAN**
3. **Redirect**
4. **Bridge**
5. **GRE Tunnel**
6. **WIFI STA**
7. **WIFI VAP**
8. **WIFI Monitor**
9. **WIFI Virtual Radio**

**Create VLANs on Port: 1.1.4**

1. **Select Shelf:** 1
2. **Resource:** 1
3. **MAC Address:** 00:00:04:*:*
4. **MAC Quantity:** 1000
5. **IP Address:** 172.16.1.1
6. **IP Mask or Bits:** 255.255.0.0
7. **Gateway IP:**
8. **IPv6 Gateway:**
9. **STAD:**
10. **SSID:**
11. **WIFI AP:**
12. **Key/Phrase:**

A. Create a MAC Address pattern similar to the parent MAC address pattern: 00;e0;ed:30:*:*.
B. Set Quantity to 1000.
C. Set an initial IP Address: 172.16.1.1.
D. Set the IP Mask: 255.255.0.0.
E. Click Apply, this takes a second to start.
F. You do not need to close the Create window.
C. Repeat the previous step with these changes to create the next 1000 MAC-VLANs on port eth5.

A. Create a MAC Address pattern similar to the parent MAC address pattern: 00:e0:ed:05:*:*.

B. Set Quantity to 1000.

C. Set an initial IP Address: 172.16.10.1.

D. Set the IP Mask: 255.255.0.0.

E. Click Apply, this takes a second to start.

F. When the progress bar switches to Ready you can click Cancel to close the Create window.

D. Check the Ports tab to watch the IP addresses get assigned to the MAC-VLANs. This will take 5 or more minutes.
### E. Adjust the Report Timer.

A. Click the Column header labeled **Port** to sort all the newly created MAC-VLANs to the top.

B. Select all the MAC-VLANs.

C. Change the **Rpt Timer** setting to **slow (15 s)**

D. Click Apply.
4. Create Cross Connects between the MAC-VLANS. We can create all these cross connections in two steps. First we will create the first cross-connect. Next, we will batch-create the remaining 999 cross connections using the first as a template.

A. Switch to the Layer-3 tab and click the **Create** button to see the **Create/Modify Cross Connect** window.

B. Set up the cross connection between the first two MAC-VLANS.

A. Connection name: **eg13cx**
B. **Port, TX Endpoint:** eth4#0
C. **Port, RX Endpoint:** eth5#0
D. **Min PDU Size:** 9,000 B
E. Click the **OK** button to save.
C. In the **Layer-3** tab...

   A. Select the cross-connect `eg13cx`.

   B. Click **Modify** in the **Layer-3** tab.

D. Click **Batch Create** in the **Create/Modify Cross Connect** window.
E. We can create cross connects in one batch. Using the Layer-3 Batch Creator window:

- Specify for **Quantity**: 999. This brings us to 1000 cross connects.
- **Starting Name Suffix**: 1
- **Resource Increment A**: 0
- **Port Increment A**: 1
- **IP Addr Increment A**: 0

Click the **Apply** button to create the cross connects.

F. Expect the system to work for a few minutes while it creates the cross connects.

When creating lots of entities at once, the system may be sluggish for a minute or two as it completes the request. Please be patient.

- When the process completes, the Batch Warning will disappear.
- Click the **Cancel** button on the Create/Modify Cross Connects window.
G. Update Report Timer for all cross connects.

A. The Layer-3 tab now shows the first 200 Layer-3 cross connects.
B. Use the View dropdown to display all the cross connects: select All and press Go.
C. Click the Select All button to select all cross connects.
D. Select slow (10s) in the Rpt Timer dropdown.
E. Click the Report Timer Go button to apply. This will keep the GUI responsive.

5. Start your cross connects.
   A. In the Layer-3 tab, click the Select All button.
   B. Then click the Start button.

<table>
<thead>
<tr>
<th>Tx Bytes</th>
<th>Rx Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,652,000</td>
<td>5,652,000</td>
</tr>
<tr>
<td>5,652,000</td>
<td>5,652,000</td>
</tr>
<tr>
<td>5,652,000</td>
<td>5,652,000</td>
</tr>
<tr>
<td>5,652,000</td>
<td>5,652,000</td>
</tr>
<tr>
<td>5,652,000</td>
<td>5,652,000</td>
</tr>
<tr>
<td>5,652,000</td>
<td>5,652,000</td>
</tr>
</tbody>
</table>

A. As you scroll to the left in the L3 Endpoints table, you can monitor the connection qualities.

B. Tx Bytes and Rx Bytes columns show traffic amount.

C. The Pattern column shows traffic trend.
A. To sniff the parent ports that the MAC-VLANs are associated with, you want to be connected to the LANforge server desktop using either Remote Desktop or VNC.

B. Operating this many cross connects can be taxing on many machines. To minimize the sluggishness of Wireshark, start Wireshark when none of the Cross-Connects are active, and use the LANforge client to start and stop the traffic.

C. In the Layer-3 tab, click Select All and click Stop.

D. In the Port Mgr tab, select interface eth4 and click the Sniff Packets button.

E. Wireshark will open and be capturing packets.

F. In the Layer-3 tab, click the Start button, and let your test run for one or two minutes.

G. Then click the Stop or Quiesce buttons to end the test.

H. Now you can save the Wireshark capture.

Making FIRE Chili

Goal: Make some tasty chili.

In this test scenario, LANforge-FIRE is not used to generate traffic. Instead, the test engineer should realize that all work and no play makes Homer something nothing.

Please note that this chili recipe is just as quick and dirty as the rest of the examples in this cookbook, but ever more tasty. Feel free to improvise...
1. Get yourself in a kitchen with some groceries.

2. Prep some ingredients.
   A. Chop up some onions. One should be good enough.
B. Chop up some garlic. Just a few cloves.

3. Cook it all up
   A. Brown some ground beef.
B. Heat up tomato sauce, kidney beans. 16oz of each is good.

C. Add garlic, onions, beef and spices such as cayenne, cumin, chili powder, salt and pepper.
D. Don’t forget the beer!

A. Note: The beer is for you, not the chili...unless of course you are experimenting!
E. Cornbread is also nice to have.

4. Enjoy!
   
   A. Serve with additional chopped onions, corn chips and cheddar cheese.
Layer-3 UDP Traffic Generator

Goal: Generate one-sided traffic to a network device with a fixed destination IP address.

This scenario is useful for testing switches, firewalls and data loggers that have to handle highly varied or very fast UDP packet streams with a fixed destination. A one-sided traffic stream is used to send packets to a network device under test when round-trip reporting is not required.

1. Configure an ethernet port.
   A. On the Port Mgr tab, select a port within the table and click the Modify button.

A. This example will use port eth1.
B. Assign an IP and Mask as necessary.

C. Click OK.

2. Configure the Layer-3 connection.
   A. On the Layer-3 tab, click Create.
B. Assign port `eth1` to **Endpoint-A**.

A. You will not need to assign **Endpoint-B** because that will become unmanaged.

C. Configure the attributes in section 1:

A. **Endpoint-A** Min Tx Rate: 1Gbps

B. **Endpoint-A** Min Tx Rate: Zero (0 bps)

C. **Endpoint-A** Min PDU Size: UDP PId (1,472 B)
D. Use the **All** button at the top to expand to the last detail level.

E. Configure the Layer-3 connection to the system under test (Endpoint-B) by following these steps:
A. In section 5, on the right side, Endpoint B (blue), select **UnManaged**. This will gray-out most of the Endpoint-B options.

B. In section 2, set the Report Timer to **slow (10 s)**. Also, set the Endpoint-B Min IP port: 9999. If you have a service under test this port should match, if not, this setting still needs to be present to generate valid traffic.

C. In section 3, set the Endpoint-B IP to the system under test IP address. Our example shows 198.105.254.11.

D. In section 4, set the send buffer size (Send Buff Size) to **1MB**.

E. Click **OK** at the top to commit the changes.

3. Start generating traffic.

A. In the **Layer-3** tab, select the connection udpgen.

B. Click **Start**.
Armageddon UDP Traffic Generation with Random MAC Addresses.

Goal: Generate network traffic to a network device with one or many destination MAC addresses.

These scenarios are useful for testing switches and firewalls that have to handle UDP traffic from thousands of source MAC addresses and one or many destination MAC addresses. This cookbook covers two scenarios:

1. A single destination MAC address. (This would exercise a firewall or router.)

2. Thousands of destination MAC addresses. (This would exercise a switch by overflowing the device CAM table.)

A one-sided traffic stream is used to send packets to a network device under test when round-trip reporting is not required.

1. On the Armageddon tab, click Create.

2. **Firewall Scenario:** Configure the Armageddon connection with the following values:
A. In the TX Endpoint (green box):
   A. The connection name for this example is macgen.
   B. Src MAC: 00:01:00:00:00:00. This is the starting point for emulated remote MAC addresses.
   C. Dest MAC: 00:0e:fa:12:bc:3a. Use the destination MAC address of your system under test.
   E. Max Src IP: 10.26.254.254. This emulates about 65,000 remote hosts.
   F. Min Dst IP: 10.27.0.1.
   G. Max Dst IP: 10.27.254.254. This emulates about 65,000 destination addresses.
   H. Pps Tx: 80,000. This is a 1Gbps packet rate.
   I. Min Pkt Size: 1514.
   J. Max Pkt Size: 1514.
   K. Src MAC Cnt: 65,025. This emulates 65,025 remote devices.
   L. Dst MAC Cnt: 1.
   M. Deselect Use Router MAC.

B. In the RX Endpoint (blue box):
   A. Select UnManaged. This allows us to fire and forget the packets.

C. Click OK to commit the configuration.

3. **Switch Scenario**: Configure the Armageddon connection with the following values:
### A. In the TX Endpoint (green box):

- **A.** The connection name for this example is `macgen`.
- **B.** Src MAC: 00:01:00:00:00:00. This is the starting point for emulated source MAC addresses.
- **C.** Dest MAC: 00:02:00:00:00:00. This is the starting point for emulated destination MAC addresses. This address is 4.2 billion addresses after the starting source MAC address.
- **E.** Max Src IP: 10.26.254.254. This emulates about 65,000 remote hosts.
- **F.** Min Dst IP: 10.27.0.1.
- **G.** Max Dst IP: 10.27.254.254. This emulates about 65,000 destination addresses.
- **H.** Pps Tx: 80,000. This is a 1Gbps packet rate.
- **I.** Min Pkt Size: 1514.
- **J.** Max Pkt Size: 1514.
- **K.** Src MAC Cnt: 65,025. This emulates 65,025 source devices.
- **L.** Dst MAC Cnt: 65,025. This emulates 65,025 destination devices.
- **M.** Deselect Use Router MAC.

### B. In the RX Endpoint (blue box):

- **A.** Select UnManaged. This allows us to fire and forget the packets.
- **C.** Click OK to commit the configuration.

### 4. Start traffic generation:
Layer 3 Testing on Windows

Goal: Test layer-3 connection throughput between two Windows hosts.

This scenario involves installation on one physical Windows 7 workstation with three network ports and a Windows XP virtual host with four network ports running within VirtualBox. We will create a pair of layer three connections and see test results.

1. Configure Virtual Guest Windows machine
   A. **Note:** LANforge installations on Windows are not able to change the IP of ports. Please do this before running LANforge.
B. Set up four network ports on the virtual guest. This example shows three ports connected to the host machine over bridge interfaces.

C. Set the IPs for the various ports using the Windows Network Settings control panel.
   A. Local Area Connection: DHCP This is the default VirtualBox NAT port. We’ll leave this one as a backup port for safety sake.
   B. Local Area Connection 2: 192.168.1.201, we will use this for normal LAN and LANforge communications

For more information see Windows IP Address

D. Review the IPs for the various ports using `netsh`.

```
C:\Documents and Settings\IEUser>netsh interface ip show address

Configuration for interface "Local Area Connection 3"
DHCP enabled: No
IP Address: 10.26.39.10
SubnetMask: 255.255.255.0
InterfaceMetric: 0

Configuration for interface "Local Area Connection 2"
DHCP enabled: Yes
InterfaceMetric: 0

Configuration for interface "Local Area Connection 4"
DHCP enabled: No
IP Address: 10.26.39.11
SubnetMask: 255.255.255.0
InterfaceMetric: 0

Configuration for interface "Local Area Connection"
DHCP enabled: Yes
InterfaceMetric: 0
```

C:\Documents and Settings\IEUser>
E. Set up network ports on the Windows workstation. The configuration includes one physical port on the motherboard and a four-port Intel PCIe card.
   A. **Local Area Connection**: 192.168.100.39, we will use this for normal LAN and LANforge communications.
   B. **Local Area Connection 2**: 10.26.39.2, for LANforge use.
   C. **Local Area Connection 3**: 10.26.39.3, for LANforge use.
   D. **Local Area Connection 4**: 10.26.39.4, for LANforge use.

F. Make sure your LANforge client GUI can ping the IP of the virtual guest management port.

G. Make sure your LANforge Manager can ping the IPs of the virtual guest management ports.

H. If necessary, configure the Windows firewall to allow ICMP packets. Or disable the Windows firewall.

---

2. Install LANforge Server on the Windows workstation

A. Make sure you install WinPCAP if it is not already installed.
B. At the end of the LANforge Server install, launch the LANforge Configuration Utility

LANforge-Server 5.2.11 Installer Setup

LANforge-Server 5.2.11 was installed. You should run the LANforge configuration tool and tell it to write out new config files before starting LANforge. Do you want to run the LANforge configuration tool now?

[Yes] [No]

A. Set the Realm to 1.
B. Set the Resource to 1.
C. Set the Mode to Both.
D. Set the Management port to the local LAN addressed port.
C. Apply the configuration and LANforge Server will start in Manager mode.

D. Click the Exit LANforge Config button. Leave the LANforge Server running (you may minimize the DOS windows.)
E. Desktop icons allow you to start and configure LANforge Server later.

3. Install the LANforge GUI on the Windows workstation.

A. Don't forget to install the licences.
4. Install LANforge Server on the virtual guest
   A. Make sure you install WinPCAP if it is not already installed.
   B. At the end of the system install, launch the LANforge Configuration Utility
   C. Set the Mode to Resource
   D. Set the Management port to the local LAN addressed port.
   E. Set the Realm to 1
   F. Set the Resource to 2
5. Create Layer 3 connections
   A. In the Layer-3 tab, click Create
B. In the Level-1 box, create the first cross connect:

A. Name the Cross Connect to `w7-ad1_xp-ad2`.
B. The CX Type is LANforge / TCP.
C. Set the Endpoint A Resource to Windows 7.
D. The Endpoint A Port to the first 10.x addressed port, ad1.
E. Set the Endpoint A Min PDU Size to TCP (1460 B).
F. Set the Endpoint A Min Tx Rate to 100Mbit. This is a limit of the XP guest.
H. Endpoint B Port: ad2.
I. Endpoint B Min Tx Rate: 100Mbit.
J. Set the Endpoint B Min PDU Size to TCP (1460 B).
K. Set the Endpoint B Min Tx Rate to 100Mbit. This is a limit of the XP guest.
L. Click OK to commit those settings.

C. For the second cross connect, click Create in the Layer-3 tab.
D. In the Level-1 box, create the second cross connect:

A. Name the Cross Connect to w7-ad2_xp-ad3
B. The CX Type is LANforge / TCP
C. Set the Endpoint A Resource to Windows 7
D. The Endpoint A Port will be the next free 10.0.x port, ad2
E. Set the Endpoint A Min PDU Size to TCP (1460 B)
F. Set the Endpoint A Min Tx Rate to 100Mbps. This is a limit of the XP guest.
G. The opposite end Endpoint B Resource is the XP Guest
H. Set the Endpoint B Port to ad3
I. Set the Endpoint B Min PDU Size to TCP (1460 B)
J. Set the Endpoint B Min Tx Rate to 100Mbps. This is a limit of the XP guest.
K. Click OK to commit those settings

E. In the Layer-3 tab, you will now see your two cross-connects:

A. Start Layer 3 connections
B. Highlight the connections
C. Click Start
C. You will see data transferring along the cross connects.

D. Highlight both connections and click Display to see the connection statistics for each. Here is the first:

E. Here is the second:

LANforge File-IO with CIFS and NFS

Goal: Create a series of MAC-VLAN based clients to emulate CIFS and NFS traffic.

This cookbook connects a LANforge system to a file server with CIFS and NFS shares available. The file server in this example will be 10.26.1.3. It will be sharing smb://10.26.1.3/fileio and 10.26.1.3:/home/fileio. We will create ten readers and ten writers for each file sharing protocol. This demonstrates using the Batch Create tool in the FileIO tab.
1. Create initial MAC VLANS for our emulated endpoints. In the Port Mgr tab, highlight a non-management port on your LANforge FIRE system and click Create.

A. Create 40 MAC VLANS with IPs starting at 10.26.1.10.

B. Choose either :::: or a random MAC address, like 00:26:::*:::*

C. Enter 10.26.1.10 and 255.255.255.0 for the IP and netmask.

D. Set Quantity to 40.

E. Click Apply to create the MAC VLANS.

F. Click Cancel to close the Create window.
B. See the 40 MAC VLANs in the Ports tab.

For more information see GUI Users Guide

2. Create your first FileIO NFS Endpoint. In the FileIO tab, click Create.
A. Use the following settings to create a NFS reader writer endpoint.

B. Enter nfs-writer for the name.
C. Select NFS for FS-Type
D. Use the first MAC VLAN p1p1#0 for Port
E. Select 2KB for the Min-RW Size
F. Choose 1MB for the Max-RW Size
G. For Min File Size choose 10KB
H. Then for Max File Size choose 25MB
I. The Min Write Rate is the minimum inbound line rate, start at 10Mbps
J. Then set the Max Write Rate at 1Gbps
K. The number of files written per connection: set File # to 2
L. Now we specify the NFS server: set Server to 10.26.1.3:/home/fileio
M. You can leave Directory, and Mount-Dir at AUTO

3. In the File-I/O tab, select the endpoint you just created and click Modify.
A. The File-IO Details dialog appears. Click the Batch Create button at the bottom of the screen.

B. Enter these values into the Batch Create dialog:
   A. Quantity should be 9
   B. Number of Digits should be 2
   C. Click Apply

C. Close the Batch Create window. You will see the new endpoints.

4. Create initial endpoint for CIFS writer.
A. Name the endpoint cifs-writer

B. Set FS-Type to CIFS

C. Then set the Port to the next open MAC VLAN: p1p1#10

D. Set the Min-RW Size and Max-RW Size to 2k and 1M

E. For the Min File Size and Max File Size enter 10KB and 100MB

F. The Min Write Rate and the Max Write Rate should be 10 Mbps and 100 Mbps

G. Enter //10.26.1.3/fileio for Server

H. Supply the credentials for the CIFS mount point in Options. For this example, our username and password are ‘lanforge’ and ‘lanforge’. Write them as options to the mount command: user=lanforge, passwd=lanforge

I. Click Apply

5. Use Batch Create to create nine more CIFS endpoints. You do not actually need to close the Create/Modify window. Click on Batch Create directly.

A. In the Batch Create window, Enter:

```
cifs-writer01, cifs-writer02 ... cifs-writer09
```

B. Quantity is 9

C. Number of Digits is 2

D. Then click Apply

B. In Create/Modify click Cancel
6. We will proceed to creating the same number of **NFS reader endpoints** by using a writer as a template for a reader:

7. Open the Modify window of the endpoint **nfs-writer**

   ![Modify window](image)

A. Change the **Name** to **nfs-reader**

B. Set the **Port** to the next unused MAC VLAN, plpl120

C. Change **Read/Write** to **Read**

D. Set the **Min Read Rate** and **Max Read Rate** to **10 Mbps** and **100 Mbps**

E. To match this reader to a writer, set the **Prefix** field to **nfs-writer**

F. Click **Apply**

8. Before closing the Modify windows we can use Batch Create to create nine more NFS endpoints:

9. Click on the **Batch Create** window of the endpoint **nfs-reader**
10. And we now create the same number of **CIFS reader endpoints**. Start by using **cifs-writer** as a template:
A. Open the Modify window of the endpoint cifs-writer:

B. Change the Name to cifs-reader

C. Set the Port to the next unused MAC VLAN, pl1p1#30

D. Change Read/Write to Read

E. Set the Min Read Rate and Max Read Rate to 10 Mbps and 100 Mbps

F. To match this reader to a writer, set the Prefix field to cifs-writer

G. Click Apply

B. Before closing the Modify windows we can use Batch Create to create nine more CIFS reader endpoints:

C. Click on the Batch Create window of the endpoint cifs-reader:

A. Change the Quantity to 9

B. Set the Number of Digits to 2

C. Click Apply

D. Click Close

E. In the Modify window, click Cancel

11. In the File-IO tab, we see our newly created reader endpoints.
12. Start the reader/writer testing.
   A. In the **File-IO** tab, begin by starting the NFS writers
A. Click on the Name column header to sort the rows of readers and writers.
B. You can use control-left-click and drag to select the group of writers.
C. Click the Start button at the top.
### B. Next, start the CIFS writers

```
<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>Type</th>
<th>Status</th>
<th>Read Bps</th>
<th>Write Bps</th>
<th>RxBps-Zeros</th>
<th>SxBps-Zeros</th>
<th>Files-Read</th>
<th>Buf-RD</th>
<th>Bytes-RD</th>
<th>Write-Bps</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.37.06</td>
<td>cifs-reader01</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.38.07</td>
<td>cifs-reader02</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.39.08</td>
<td>cifs-reader03</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.40.09</td>
<td>cifs-reader04</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.41.10</td>
<td>cifs-reader05</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.42.11</td>
<td>cifs-reader06</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.43.12</td>
<td>cifs-reader07</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.44.13</td>
<td>cifs-reader08</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.45.14</td>
<td>cifs-reader09</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.46.15</td>
<td>cifs-writer</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.47.16</td>
<td>cifs-writer01</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.48.17</td>
<td>cifs-writer02</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.49.18</td>
<td>cifs-writer03</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.50.19</td>
<td>cifs-writer04</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.51.20</td>
<td>cifs-writer05</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.52.21</td>
<td>cifs-writer06</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.53.22</td>
<td>cifs-writer07</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.54.23</td>
<td>cifs-writer08</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.55.24</td>
<td>cifs-writer09</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.56.25</td>
<td>nfs-reader</td>
<td>NFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

Logged in to: 192.168.100.26:4002 as: Admin

### C. Then the NFS readers

```
<table>
<thead>
<tr>
<th>PID</th>
<th>Name</th>
<th>Type</th>
<th>Status</th>
<th>Read Bps</th>
<th>Write Bps</th>
<th>RxBps-Zeros</th>
<th>SxBps-Zeros</th>
<th>Files-Read</th>
<th>Buf-RD</th>
<th>Bytes-RD</th>
<th>Write-Bps</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.37.06</td>
<td>cifs-reader01</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.38.07</td>
<td>cifs-reader02</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.39.08</td>
<td>cifs-reader03</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.40.09</td>
<td>cifs-reader04</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.41.10</td>
<td>cifs-reader05</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.42.11</td>
<td>cifs-reader06</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.43.12</td>
<td>cifs-reader07</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.44.13</td>
<td>cifs-reader08</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.45.14</td>
<td>cifs-reader09</td>
<td>CIFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.46.15</td>
<td>cifs-writer</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.47.16</td>
<td>cifs-writer01</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.48.17</td>
<td>cifs-writer02</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.49.18</td>
<td>cifs-writer03</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.50.19</td>
<td>cifs-writer04</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.51.20</td>
<td>cifs-writer05</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.52.21</td>
<td>cifs-writer06</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.53.22</td>
<td>cifs-writer07</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.54.23</td>
<td>cifs-writer08</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.55.24</td>
<td>cifs-writer09</td>
<td>CIFS</td>
<td>Run</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1.1.56.25</td>
<td>nfs-reader</td>
<td>NFS</td>
<td>Stopped</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

Logged in to: 192.168.100.26:4002 as: Admin
13. We can inspect the traffic in the Dynamic Report window and the File-IO tab:

A. Select a group of endpoints and right click on them, select Dynamic Report
B. In the Dynamic Report window, select the checkbox Rx-Bps

dynamic graph with selected options

C. In the File-IO window, we can watch for Files Written and IO Errors:

file-IO window with selected options
Providing HTTP Service on a Port

**Goal:** Configure and activate a http server bound to a specific port in LANforge.

This is useful if you want to provide an application layer target to interact with. This cookbook assumes you can access a shell prompt on the LANforge computer; the command-line instructions can be done at the system console, in a terminal over a remote desktop connection, or over `ssh`. The nginx service is only available on the Linux version of LANforge server.

**Note:** There are two web servers installed in a LANforge computer. The default web server is a stock version of Apache HTTPD that responds to all port 80 requests on all interfaces. For testing we recommend running Candela Technologies’ version of Nginx on specific ports as covered in this cookbook. In contrast, Apache cannot bind to a network-device therefore we do not suggest running it.

Nginx can also be configured to listen to IPv6 traffic. Jump to the end of the cookbook for that technique.

1. Stop and disable LANforge system Apache instance.
   A. Log into the LANforge computer as user lanforge
   
   ```
   jreynolds@jed-shuttle:~$ ssh lanforge@192.168.180.48
   ```

   B. Become super-user using the command `su` (or `sudo -s`)
   
   ```
   root@jed-f20:~/home/lanforge$ sudo -s
   ```

   ```
   [lanforge@jed-f20 ~]$ sudo -s
   ```

   ```
   [root@jed-f20 lanforge]#
   ```
C. Stop the Apache service with `systemctl stop httpd`

```
root@jed-f20:/home/lanforge - Terminal
[root@jed-f20 lanforge]# systemctl stop httpd
[root@jed-f20 lanforge]#
```

D. If you want this setting to persist after a reboot, disable the service: `systemctl disable httpd`

```
root@jed-f20:/home/lanforge - Terminal
[root@jed-f20 lanforge]# systemctl stop httpd
[root@jed-f20 lanforge]# systemctl disable httpd
rm ' /etc/systemd/system/multi-user.target.wants/httpd.service'
[root@jed-f20 lanforge]#
```

E. Set this as system default with: `systemctl daemon-reload`

```
root@jed-f20:/home/lanforge - Terminal
[root@jed-f20 lanforge]# systemctl stop httpd
[root@jed-f20 lanforge]# systemctl disable httpd
rm ' /etc/systemd/system/multi-user.target.wants/httpd.service'
[root@jed-f20 lanforge]# systemctl daemon-reload
[root@jed-f20 lanforge]#
```

2. (Optional) There are other options for running Apache if you want to have both web servers available. You would not need to stop and disable Apache, just restart it. You can change Apache to:

   A. ...listen to a different port (like 81). Edit `/etc/httpd/conf/httpd.conf` and change the `Listen` option.

```
root@jed-f20:/etc/httpd/conf - Terminal
[root@jed-f20 httpd conf]# cd /etc/httpd/conf
[root@jed-f20 conf]# nano httpd.conf
```
B. ...bind to a specific IP address, which is a good option if you configure the LANforge computer to have a fixed IP address on the management port. You would edit **httpd.conf** and change `Listen` to that specific IP address and port 80. Example: `Listen 192.168.1.40:80`

3. The demonstration test we'll create is making two ports, one for making requests and the other one for serving the protocol. Let's create two ports:
   A. Create a redirect device:
      
      A. In the Ports tab, click the Create button

      ![Create VLANs on Port](image)

      B. Select Redirect
      
      C. Enter rd0a for #1 Redirect name,
      
      D. and rd0b for #2 Redirect name.
      
      E. Click Apply and then Cancel to close the window.
B. Configure rd0a as the service port:

A. In the Ports tab, double-click the row for port rd0a

B. The Configure Settings window will appear

C. Set an IP of 10.2.0.1,

D. a netmask of 255.255.255.0

E. and the report time to faster (1 s)

F. Click OK
C. Configure r0db as a client port

A. In the Ports tab, double-click the row for port r0db

B. The Configure Settings window will appear

C. Set an IP of 10.2.0.3,

D. a netmask of 255.255.255.0

E. and the report time to faster (1 s)

F. Click OK

4. Enable HTTP service on your upstream port using the following steps.
A. Enable the nginx service on port rdoa:
   A. In the Ports tab, double-click the row for port rdoa

   ![LANforge Manager](image)

   B. The Configure Settings window will appear
   C. In the lower left column of the window, enable HTTP option.
   D. Click OK and then close the window.

   ![rd0a Configure Settings](image)

   ![Laforge@jed-f20:/vr_conf - Terminal](image)

B. [Optional] Modify the nginx config file for port rdoa. This example assumes you are logged into the LANforge system console, or have connected to the desktop using a remote-desktop client like vncviewer. If you are familiar with editing from the command-line, you will likely know how to do this via ssh.

   A. From the desktop Accessories menu, select Terminal Emulator,
   B. Change to the LANforge nginx directory: `cd /home/Lanforge/vr_conf`

   ![Laforge@jed-f20:/vr_conf - Terminal](image)
C. Edit the file nginx_rd0a.conf. If you do not see the file, you might have connected to the wrong LANforge resource, or you might not have clicked OK/Apply when enabling the Configure Settings window for port rd0a.

D. You will see that the listen directive is already set to 10.2.0.1:80 bind_dev=rd0a:

E. If you want to change settings, delete the first line of the config file as part of your changes. This will signal LANforge not to overwrite the file.
C. To apply the changes to the nginx service on this port:

A. Disable the HTTPD service in the r60a Configure Settings window.

B. Click the **Apply** button.

C. Enable HTTPD service.

D. Click the **Apply** button.

E. Click the **Cancel** button to close the window if you are done.
D. A quick way to add a file into the nginx document root folder is to symlink the system dictionary there. You will need to be in a terminal or unix shell of the resource running nginx (192.168.100.40 in this example).  
A. Change the ownership of the document root directory to user lanforge:
B. sudo chown lanforge:lanforge /usr/local/lanforge/nginx/html

C. cd /usr/local/lanforge/nginx/html

D. ln -s /usr/share/dict/linux.words ..

E. (Optional) To load a larger payload (such as a DVD file), you can use Filezilla (or scp) to copy the file over. You will want to have changed the nginx document root directory owner to lanforge (as above):
A. From your desktop, using FileZilla

1. Quick connect to sftp://192.168.100.40 (also named jed-f20 in this example)
2. Using username Lanforge and password Lanforge

B. In the left column, choose your local directory (Y:\downloads)
C. In the right column, type in the nginx document root, /usr/local/lanforge/nginx/html and hit enter.

D. In the left column, double-click your DVD image (Fedora-20-x86_64-netinst.iso)
5. Configure application-layer traffic using the Layer 4-7 tab tools:
   A. In the Layer 4-7 tab, click the Create button,

   B. You will see the Create/Modify L4Endpoint window

   C. Create a connection named web-requests,

   D. With a Report timer of fast (1 s)

   E. from Resource (jed-20) port rd0b

   F. Let's make ten requests a second. Enter 6000 for URLs per 10m.

   G. Jump down to the URL field, and enter http://10.2.0.1/index.html

   H. and to avoid saving the result, set the Dest File to /dev/null
6. Running the traffic is simple:
   A. Select the row named `web-requests` in the Layer 4-7 table,
   B. Click the `Start` button.
C. Click the Display button to see more detail on the traffic:

7. It is also possible to verify your connection setup from the command-line:

A. To verify the Layer 3 connection, you can use ping:
   
   
   ```
   ping -I 10.2.0.3 10.2.0.1
   ```

   ![Layer-4 Endpoint web-requests Manager: jed-f20](image)

   DNS Complete
   Avg:0   0.0
   
   First RX
   Avg:0   0.3
   
   URLs Completed
   Avg:1   0.3
   
   B. To see that nginx is listening on port 80, use netstat on the resource running nginx and see what is listening on port 80:
   
   ```
   sudo netstat -ntlp | grep ':80'
   ```

   ![Terminal](image)

   ```
   [lanforge@jed-f20 html]$ sudo netstat -ntlp | grep ':80'
   tcp 0 0 10.2.0.1:80 0.0.0.0:* LISTEN 5034/nginx: master
   ```
C. To see the output of the web request, you can use LANforge's version of curl located in /home/lanforge/local/bin/curl. Since it uses bundled libraries, first type:
```
cd /home/lanforge & & . /lanforge.profile
```
This sets up all environment variables and paths to work with the binaries and libraries shipped with LANforge.

```
root@jed-f20:/home/lanforge
> cd /home/lanforge & & . /lanforge.profile
root@jed-f20:/home/lanforge
```

D. Verify it runs without complaint:
```
/home/lanforge/local/bin/curl --help
```

```
lanforge@jed-F20:-- Terminal
```

E. If you scroll up in your terminal, you will see options available in the output not found in a normal version of curl, like --dns_server, --dns_interface, --dns_ip4_addr, --dns_ip6_addr, -interface and --localaddr. We will use --interface next.

```
lanforge@jed-F20:-- Terminal
```

F. Craft your download command: cd /home/lanforge/local/bin
```
./curl --interface 10.2.0.3 'http://10.2.0.1/index.html'
```

```
lanforge@jed-F20:--local/bin - Terminal
```

```
[lanforge@jed-f20 ~]$ cd /home/lanforge/local/bin
[lanforge@jed-f20 bin]$ ./curl --interface 10.2.0.3 'http://10.2.0.1/index.html'
```
G. You will see the HTML output in the terminal:

```
[lanforge@jed-f20 ~]$ cd /home/lanforge/local/bin
[lanforge@jed-f20 bin]$ ./curl --interface 10.2.0.3 http://10.2.0.1/index.html
```

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
.body {
  width: 38em;
  margin: 0 auto;
  font-family: Tahoma, Verdana, Arial, sans-serif;
}
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
</body>
</html>
```

H. There will be a record of connections and errors in the nginx logs directory: cd /usr/local/lanforge/nginx/logs

```
[lanforge@jed-f20 logs]$ cd /usr/local/lanforge/nginx/logs
[lanforge@jed-f20 logs]$ ls -lta
```

8. [Advanced] Creating IPv6 traffic to nginx. We will assume a scenario where eth1 will serve nginx requests and eth2 will generate requests.

A. Add IPv6 addresses to your ports. We will add
- `ee::2:1/120` for eth1,
- `ee::2:2/120` for eth2,

and set the gateways for them to `ee::2:fe`. We won't actually use a gateway, but our port configuration requires it.
A. Here is eth1, and we will enable the HTTP service as well.

```
$ ping6 -I te::2:2%eth2 te::2:1
```

B. Here is eth2, notice how we added an IPv4 address to the port. Do that so that the Create Layer 4-7 dialog does not complain.

C. Here is a picture of the Port Mgr tab, with ports on two resources configured.

D. Verify your connection between ports using `ping6`. $ ping6 -I te::2%eth2 te::2:1
B. Edit your `/home/lanforge/vr_conf/nginx_eth1.conf` file. You will remove the header comment and alter the listen statements to include IPv6 addresses. You can listen for [:1] or you could listen for [::2:1]

```
worker_processes  1;
error_log logs/eth1_error.log;
pid /home/lanforge/vr_conf/nginx_eth1.pid;

events {
  worker_connections  1024;
}

http {
  include  /usr/local/lanforge/nginx/conf/mime.types;
  default_type application/octet-stream;
  access_log logs/eth1_access.log;
  sendfile on;
  keepalive_timeout 65;

  server {
    listen 0.0.0.0:80 bind_dev=eth1;
    listen [:1]:80 bind_dev=eth1;
    server_name www-eth1;
    access_log logs/eth1_host.access.log;

    location / {
      root html;
      index index.html index.htm;
    }

    error_page 500 502 503 504 /50x.html;

    location = /50x.html {
      root html;
    }
  }
}
```

C. If you provide an IPv6 address, please watch the nginx log file for errors: listening on an IPv6 address is easy to misconfigure. The log files can be found in `/usr/local/lanforge/nginx/logs`.

D. Re-start the http service on `eth1` by un-checking HTTP, clicking Apply, checking HTTP, clicking OK.

E. Configure your Layer 4-7 endpoint:

```
A. Name your endpoint
B. Set your URLs per Minute
C. Specify the URL with brackets around the address: http://[::2:1]/index.html
D. Set your output file to /dev/null
```

F. You can watch traffic on eth1 or eth2 to verify the web requests.
Generating FTP Traffic Between Two Physical ports

**Goal:** Allow LANforge to simulate a FTP connection within the same system.

This scenario is useful if you wish to generate stateful FTP traffic between two physical ports using a single LANforge system. You will need two non-management physical ports connected to each other with a loopback cable or switch.

1. Configure the physical interfaces. We will set up eth1 as a client and eth2 as a FTP server.
   
   A. Go to the **Port Mgr** tab and select eth1.

   B. Click **Modify** to configure port eth1.

   A. Set the IP Address to 10.0.0.101/24.

   B. Click **OK**.

```
C. While still in the Port Mgr tab, select eth2.

D. Click Modify to configure port eth2.

A. Set the IP Address to 10.0.0.102/24.
B. Enable FTP under Services.
C. Click OK.

2. Create a file for the FTP client to download/upload. This is optional if you already have a file in mind to test with, just make sure the file is in /home/lanforge (the default directory for FTP). Step 3 explains how to upload a file from a Windows machine.
A. First, you'll need to open a console on the LANforge system.

   A. Log into the machine directly or remotely through rdesktop. The user/password should be lanforge/lanforge for both.

   B. To log in via rdesktop type the following command into a console (replace LANforge-IP with the IP of your LANforge system):
      rdesktop LANforge-IP

C. Log in with user/password lanforge/lanforge.

D. Once you are on the system, a console should already be open. If you don't see a console, go ahead and open one by clicking the console icon in the top menu bar (shown in the below screenshot).
B. Once you have a console ready, use the below commands to create a small or large file. These files will just contain random text.

Note: These files will be created in the /home/lanforge directory. This is the default directory used for FTP on LANforge.

A. Small file (45 KB):
   ```
   dd if=/dev/urandom of=/home/lanforge/small-file.bin bs=1k count=44
   ```

B. Large file (10 MB):
   ```
   dd if=/dev/urandom of=/home/lanforge/large-file.bin bs=1k count=10240
   ```

3. Optional: Upload a file to the LANforge system for the FTP client to download/upload. There are multiple ways to do this, this step will demonstrate the upload using a Windows machine with FileZilla.

   A. On your Windows machine, download and install FileZilla. You can download the FileZilla client here:
      https://filezilla-project.org/download.php

   B. Open FileZilla.
A. Near the top left in the Host field, enter the following: sftp://LANforge-IP
(sftp://192.168.100.86 is used in this example).
B. Username: lanforge Password: lanforge.
C. Click Quickconnect.

D. In the left column navigate to your file's directory. Make sure the right column is set to /home/lanforge

D. To start transferring your file, double click it in the left column. Once the transfer is complete make sure you can find it within the right column under /home/lanforge. Your file is now on the LANforge machine!
4. Create the FTP endpoint.
   A. On the Layer 4-7 tab, click Create.

   B. Configure the FTP endpoint.
A. Name your endpoint `ftp-download`.

B. Set `Rpt Timer` to `fast (1 s)`.

C. Set `Port` to `eth1`.

D. Set `URLs per 10m` to `600 (1/sec)`.

   i. Here is a list of common values used for `URLs per 10m`.

<table>
<thead>
<tr>
<th>URLs per 10m</th>
<th>Converted</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>1/min</td>
</tr>
<tr>
<td>600</td>
<td>1/sec</td>
</tr>
<tr>
<td>6000</td>
<td>10/sec</td>
</tr>
<tr>
<td>60000</td>
<td>100/sec</td>
</tr>
</tbody>
</table>

E. To download the small file (44KB) created earlier, set `URL` to:
   `ftp://lanforge:lanforge@10.0.0.102/small-file.bin`

To download the large file (10MB) created earlier, set `URL` to:
   `ftp://lanforge:lanforge@10.0.0.102/large-file.bin`

   **Note:** The default directory for FTP is `/home/lanforge` and the default username/password is lanforge/lanforge. All files downloaded/uploaded via FTP need to be in `/home/lanforge`.

F. Optional: If you want to use another file in `/home/lanforge` you can just change the filename at the end of the URL.

   For example `ftp://lanforge:lanforge@10.0.0.102/large-file.bin` would be changed to
   `ftp://lanforge:lanforge@10.0.0.102/your-file-name`

G. Set `Source/Dest File` to `/dev/null`.

H. Click `OK`.

5. Start the endpoint and display the graph.

   A. In the **Layer 4-7** tab, select the connection called `ftp-download`.

   B. Click `Start`.  


C. Select ftp-download and click Display to see a graph similar to below.

6. **Uploading** a file from the FTP client to the FTP server.
A. Go to the **Layer 4-7** tab and modify the **ftp-download** endpoint. The below changes will need to be made:

- Name to **ftp-upload**.
- URL to **ftp://lanforge:lanforge@10.0.0.102/ftp-socket**. The upload file name in this link can be changed if needed.
- Source/Dest File to **large-file.bin**. This can be changed to a preferred file as long as it is in **/home/lanforge** (the default FTP directory).

B. Select **ftp-upload** and click **Start**.

C. This endpoint will now essentially upload the large-file.bin file in **/home/lanforge** to the same directory with a new file name (**upload-file** in this case). If you select **ftp-upload** in the **Layer 4-7** tab and click **Display**, the graph should look similar to the one below.

7. Using **SCP**, **SFTP**, and **TFTP**.
A. Go to the **Layer 4-7** tab and modify the `ftp-download` endpoint. The below changes will need to be made:

- **Name** to `ftp-scp` for `scp` or `ftp-sftp` for `sftp`.
- For `SCP`, set the URL to `scp://lanforge@10.0.0.102/~/small-file.bin`. The filename at the end of the link can be changed to another file in `/home/Lanforge`.

B. In the **Create/Modify L4 Endpoint** window, set the following:

- **URL**: `scp://lanforge@10.0.0.102/~/small-file.bin`
- **Source/Dest File**: `default` or `dev/null`
- **Source DNS**: `dev/null`
- **Use Proxy**: `No` or `Yes`
- **FTP PASV**: `Yes` or `No`
- **FTP EPSV**: `Yes` or `No`
- **FTP Auth Types**: `NTLM` or `Basic`
- **HTTP Auth Types**: `Digest` or `Basic`
- **SSL Cert**: `ca-bundle.crt`
- **SMTP From**: `lanforge@10.0.0.102`
- **Agent/RCPT-To**: `dev/null`
- **Proxy Auth Types**: `NTLM` or `Basic`
- **HTTP Compression**: `Deflate`
- **URL Timeout**: `10000`
- **DNS Cache Timeout**: `50`
- **Max Speed**: `500000`
- **URLs per 10ms**: `600`
- **TFTP Block Size**: `65536`
- **Queue Size**: `3` (3 sec)
- **IP Addr**: `AUTO`
- **Proxy Port**: `80`
- **Proxy Server**: `dev/null`
- **Test Manager**: `default`
- **Endpt Name**: `ftp-scp` or `ftp-sftp`
- **Resource**: `l4/Lanforge`
- **Port**: `2` (eth1)

C. Click **OK**.

D. For `SFTP`, set the URL to `sftp://lanforge@10.0.0.102/~/small-file.bin`. The filename at the end of the link can be changed to another file in `/home/Lanforge`.

E. **Status**: `Stopped` or `Running`

F. **Bytes RD**: `0`

G. **Bytes WR**: `0`
E. Click OK.

B. Select the **ftp-scp** or **ftp-stfp** endpoint and click **Start**.

C. To use **TFTP**, you will first need to have a TFTP server set up and configured to serve the Layer 4-7 endpoint a file.

   A. Once the server is set up, use the below configuration to set up a TFTP endpoint.  
   
   **Note:** You will need to provide your own server's IP and file name.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>host-ip</td>
</tr>
<tr>
<td>Rpt Timer:</td>
<td>fast (1 s)</td>
</tr>
<tr>
<td>Test Manager:</td>
<td>default_tm</td>
</tr>
<tr>
<td>Port:</td>
<td>69</td>
</tr>
<tr>
<td>IP Addr:</td>
<td>AUTO</td>
</tr>
<tr>
<td>URLs per 10m:</td>
<td>600</td>
</tr>
<tr>
<td>Max Speed:</td>
<td>Infinite</td>
</tr>
<tr>
<td>URL TIMEOUT:</td>
<td>10000</td>
</tr>
<tr>
<td>DNS Cache Timeout:</td>
<td>50</td>
</tr>
<tr>
<td>Source/Dest File:</td>
<td>/dev/null</td>
</tr>
</tbody>
</table>

I. Set the **Port** to a port that can talk to the TFTP server. In this case the server was on the management network so eth0 was used.

II. **URLS per 10m** was left at the default 100, this can be set higher or lower depending on how often the file should be downloaded.

III. Set **URL** to `http://server-IP/filename`.

IV. **Source/Dest File** can be `/dev/null`.  

Generating Table-based Reports

**Goal:** Learn how to generate reports that present the data found in the table views of the LANforge GUI.

We will use the **Reporting → Table Report Generator** tool to select rows and columns present from the LANforge GUI to create an HTML report. The individual rows and columns from the Ports, Layer-3 and L3-Endpoints windows can be selected. Feature appears in release 5.3.3.

1. Beginning a New Report
   
   A. We start in the **Reports** menu, and choose the **Table Report Generator**
2. Understanding the two columns in the Table Report Builder.
A. Report Profiles are on the left. This represents your selection of Layer-3, L3-Endpoint and/or Port table columns to include in your report. These preferences are saved independently of the entity choices.
B. Entity Selections are on the right. This consists of a your combination of Layer-3 connections, L3-Endpoints and/or Ports to report on. These preferences are also saved independently from the profiles.

3. Selecting items to include
   A. The Skip button will omit a whole table from the report. Checking and un-checking the skip button will not alter your row selection check boxes.
B. The **Select** drop downs for each table are a short cut for selecting all or unselecting all items in a row.

C. The [SPACE] and [ENTER] keys are shortcuts for selecting and unselecting checkboxes. These keys will toggle highlighted groups of rows as well.

4. Saving and Loading a Report Profile
A. The Save button allows you to save your table row selections. Name your saved profile.
5. Generating the report is simple, click the **Create Report** button. Your report will be remembered with an Autosave record.
6. Saving the report as a file is easy as well. In the Graphical Script Report window, click the Save File button.

**Displaying Sequence Gaps**

**Goal: Generate and show sequence gaps (time between packets) by running traffic through a WanLink with an intermittent latency spike.**

Tracking sequence gaps can be useful in the following scenarios:
- Roaming with and without 802.11r.
- OSPF failovers.
- Cellular to WiFi handoff.

In this test scenario, LANforge will be set up to generate sequence gaps. Then the sequence gaps will be shown via the layer.3 display window.

Four physical ports will be used, two to generate traffic and two for the WanLink endpoints. This test uses a LANforge CT922 system.

LANforge will be generating UDP Traffic at 1 Mbps through a WanLink that is scripted to apply one second of latency every ten seconds. The one second latency should create a one second sequence gap. The packet size will be smaller to increase the rate of traffic and thus decreasing sequence gaps, this will make any larger sequence gaps more apparent.

1. Set IPs on traffic generating ports, eth0 and eth3 in this case.
A. In the Port Manager tab modify eth0.

B. In the Port Manager tab modify eth3.

2. Create a WanLink.
A. In Net smith, right click an open area and click New Connection.

B. Select the Skip checkboxes on Port 1-B and Port 2-B.
C. Set Port 1-A to eth1.
D. Set Port 2-A to eth2.
E. Click OK.

3. Configure the WanLink.
   A. In the WanLinks tab, modify the WanLink.

A. Set the Transfer Rate to 10Mbps for both endpoints.
B. Click the **Script** button on **Endpoint A**.

A. Set the **Script Type** to **ScriptWL**.
B. Click the **Loop** checkbox.
C. **Run Duration** = 1s
D. **Rates** = 10Mbps
E. **Latencies** = 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1000
F. **Jitter** = 0
G. **Drops** = 0
H. Click **OK**.

C. Click **OK** to close the WanLink modify window.

4. Create a Layer 3 connection.
A. In the Layer-3 tab, Click Create.

A. CX Name = udp-1m
B. Report Timer = 1s
C. Endpoint A Port = eth0
D. Endpoint B Port = eth3
E. Endpoint A and B = 1m
F. Endpoint A and B Min PDU Size = 64 B
G. Click OK.

5. Create a test group to start the layer 3 connection and WanLink at the same time.
   A. In the Test Group tab, click Create.

A. Test Group Name = tg
B. Select the WanLink and Layer 3 connection on the right and click Add Cx.
C. Click OK.
6. Start the test group. This will start both the layer 3 connection and the scripted WanLink.
   A. In the Test Group tab, select Ig and click Start. You will see the Script Report window appear.

7. Display the Layer 3 connection and analyze the Rx Gap (sequence gap).
   A. In the Layer-3 tab, select udp-1m and click Display.

   B. The Rx Gap graph is highlighted in the below screenshot. The Rx Gap for Endpoint B doesn’t show one second sequence gaps because that side of the WanLink was not scripted.

   A. The colored numbers on the left side of the colon represent time in milliseconds. The right colored numbers represent the number of times a sequence gap reached the particular time on the left side.

   You’ll notice that 9 sequence gaps hit 1024ms. These gaps were the result of the WanLink script occasionally sending one second latency.

Scalability Testing with NFS File-IO

Goal: Analyze memory usage as the number of NFS clients is scaled up, and also when NFS endpoint settings are tweaked.
Hopefully by the end of this cookbook you'll have an idea how to assess how many File-Io endpoints and associated settings your system can support. This cookbook connects a LANforge system to a NFS file server. The file server in this example will be 10.17.1.1. It will be sharing 10.17.1.1:/mnt/tmpfs1. We will create 100, 250, then 500 readers and writers and compare memory usage as we also tweak the RW Size setting.

**Note:** For this example, we are using a **CT523** with 8GB of memory. It is physically connected to the NFS file server.

1. **First, 500 MAC-VLANS will need to be created.**
   A. In the Port-Mgr tab select port eth1 and click **Create**.

   ![Create VLANs on Port: 1.png](image)

   A. Select **MAC-VLAN**.
   B. Set **Quantity** to **500**.
   C. The starting IP address is 10.17.1.2/16. For this test, if your file server is on a different network, change the IP here accordingly. Make sure not to use the file server's IP address.
   D. Click **Apply** and close the Port Create window once all ports are configured. Make sure all MAC-VLANS get IPs, this may take some time.

2. **Create 250 NFS writers and 250 NFS readers.** Batch create **50** at a time (49 for first batch of reader/writers). More information on creating File-Io endpoints can be found here: [LANforge File-Io with CIFS and NFS](#)
A. Any non-default settings for the **NFS writers** are listed below.

A. Name is `nfs-writer001`.
B. FS-Type: NFS.
C. Port is `eth1#0`.
D. Min-RW and Max-RW sizes are 4k.
E. Min/Max File sizes are 1MB.
F. Min/Max Write rates are 100Mbps.
G. Quiesce After is `Forever`.
H. Server is `10.17.1.11/mnt/tmpfs1` (use your own file server settings here).
I. Make sure `Read/Write` is set to `Write`.
J. Turn on the **Use O_DIRECT** checkbox.

B. Any non-default settings for the **NFS readers** are listed below.

A. Name is `nfs-reader001`.
B. FS-Type: NFS.
C. Port is `eth1#250`.
D. Min-RW and Max-RW sizes are 4k.
E. Min/Max File sizes are 1MB.
F. Min/Max Write rates are 100Mbps.
G. Quiesce After is `Forever`.
H. Server is `10.17.1.11/mnt/tmpfs1` (use your own file server settings here).
I. Set `Read/Write` to `Read`.
J. Set Prefix to `nfs-writer001`.
K. Turn on the **Use O_DIRECT** checkbox.

3. Start the first **50 writers** then the first **50 readers**. It's recommended to slowly start File-IO endpoints, for example, starting 25 writers then 25 readers then the same again until you have the desired amount running. The reason to do
this is because the system may become unresponsive if it can’t handle the number of File-I/O endpoints. **Note:** If you notice the system slowing down, connections not starting, or connections stuck in WAITING state, or any weirdness in general, you should stop 25 or 50 writers/readers at a time until the system clears up.

4. Now that 50 File-I/O endpoints are running, the memory will be analyzed via htop.
   A. Open a terminal on the LANforge system using a preferred method (either directly or remotely through ssh, rdesktop, or vncviewer).
B. Show a list of btservers processes (LANforge processes) by running the command:

```
htop -p `pgrep btservers | tr "\n" "," | sed 's/,$//'`
```

If htop isn't installed run: sudo yum install htop

A. The majority of btservers processes with the same or similar values here represent the running File-I/O endpoints. The RES (resident value) column represents the memory used by these File-I/O endpoints. The current test uses an average of about 10.400 KB or 10.6 MB per btservers process. These values should be monitored as the File-I/O settings are adjusted.

**NOTE:** You will need to restart htop if the endpoints are stopped/restarted. Just press q to quit out and run the above htop command again.

C. Total up the RES memory used by btservers. This is useful to compare memory usage between a different number of connections. For example you could compare how much memory 100 endpoints use compared to 500 endpoints.
A. To show the total RES memory used, run the command:
   ps aux | grep btserver | awk '{s+=$6} END {print s}'
To repeat it every second, use the below command. Press Ctrl+C to stop.
   while sleep 1; do ps aux | grep btserver | awk '{s+=$6} END {print s}'; done

B. The total memory for 50 NFS File-Io endpoints with a Min/Max RW rate of 4k is about 1,130,000 KIB which converts to around 1,157 MB.

5. While the File-Io endpoints are running, change the Min-RW and Max-RW settings.
A. Select all File-I/O endpoints and click **Batch Modify**.

![LANforge File-I/O Batch Modifier window]

A. Set the **Min/Max RW sizes** to 1MB.
B. Click **OK**

6. Analyze how the Min/Max RW size setting change has affected the memory (see steps 48 and 4C).
A. Changing the Min/Max RW sizes to 1MB increased the btserver memory use to about 11,600 Kib or 11.9 MB from 10,400 Kib or 10.6 MB. About a 1,200 Kib or 1.3 MB difference.

The total memory increased to 1,233,000 Kib, 1,262 MB from 1,130,000 Kib, 1,157 MB. About a 103,000 Kib or 105 MB difference.

7. Set the endpoints Min/Max RW size back to 4k.
A. Stop all running file-I/O endpoints by selecting them and clicking **Stop**.

B. Select all file-I/O endpoints and click **Batch Modify**.

A. Set the **Min/Max sizes** to 4k.
B. Click **OK**.

8. Repeat steps 3 through 7 for **125 writers/readers** and then again for **250 writers/readers**.

9. The results from the above tests are shown in the below tables. They show how RW size affects 100, 250, and 500 NFS File-I/O endpoints.
<table>
<thead>
<tr>
<th>RW Size</th>
<th>100</th>
<th>250</th>
<th>500</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 KB</td>
<td>10.6</td>
<td>10.8</td>
<td>10.8</td>
</tr>
<tr>
<td>1 MB</td>
<td>11.9</td>
<td>11.9</td>
<td>11.8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RW Size</th>
<th>100</th>
<th>250</th>
<th>500</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 KB</td>
<td>1.157</td>
<td>2.804</td>
<td>4.134</td>
</tr>
<tr>
<td>1 MB</td>
<td>1.262</td>
<td>3.031</td>
<td>6.013</td>
</tr>
</tbody>
</table>