SANDIA REPORT

SAND2009-4741
Unlimited Release
Printed August 2009

SNL Evaluation of Gigabit Passive Optical Networks (GPON)

Joseph P. Brenkosh, David H. Dirks, Bob Fischer, Steven A. Gossage, David G. Heckart, Thomas J. Pratt, Glen B. Roybal, Gerald F. Rudolfo, James A. Schutt, Sandra M. Trujillo, Betty R. Walker

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2009-4741
Printed August 2009

SNL Evaluation of Gigabit Passive Optical Networks (GPON)

Joseph P. Brenkosh
Network Design and Operations Department

Steven A. Gossage, Thomas J. Pratt, and James A. Schutt
Advanced Networking Integration Department

David H. Dirks, Bob Fischer, Sandra M. Trujillo, and Betty R. Walker
Video Conference and Collaborative Technologies Department

Glen B. Roybal, and Gerald F. Rudolfo
Telecommunications and Infrastructure Department

David G. Heckart
Cyber Security Technologies Department

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0788

ABSTRACT

Gigabit Passive Optical Networks (GPON) is a networking technology which offers the potential to provide significant cost savings to Sandia National Laboratories in the area of network operations. However, a large scale GPON deployment requires a significant investment in equipment and infrastructure. Before a large scale GPON system was acquired and built, a small GPON system manufactured by Motorola was acquired and tested. The testing performed was to determine the suitability of GPON for use at SNL. This report documents that testing.

Acknowledgements

The authors would like to acknowledge the following people for their help in making this evaluation possible.

Members of management who actively supported the GPON Test Project:
A. L. Hale (9600)
R. W. Leland (9300)
J. D. Zepper (9320)
G. K. Rogers (9330)
P. L. Manke (9335)
N. A. Marsh (9338)

Staff members who assisted in the GPON Test Project, including being a GPON beta user:
J. G. Heller (9317)
T. Holley (9335)
A. B. Leyba-Essary (9335)
J. H. Maestas (9336)
D. E. Eichert (9338)
J. H. McDonald (9341)
R. T. Jaramillo (0243)

Verizon Technical Support Team members who helped us on numerous occasions when we had questions or problems:
J. D. Avalos
J. J. Harris
E. M. Welty

Brocade (formerly Foundry Networks) Field Engineers who helped us with the NetIron MLX configuration:
C. Wright
S. Visconti

Table of Contents

List of Figures

List of Tables

Introduction

Gigabit Passive Optical Networks (GPON) is a networking technology which offers the potential to provide significant cost savings to Sandia National Laboratories in the area of network operations. However, a large scale GPON deployment requires a significant investment in equipment and infrastructure. Before acquiring and deploying a large GPON system, a small GPON system manufactured by Motorola was acquired and tested. The testing performed was to determine the suitability of GPON for use at SNL. This report documents that testing.

This report begins with a primer on GPON. Then results of host-to-hosts throughput tests using Linux test hosts are discussed. Next, it presents results of throughput tests using a Spirent AX/4000 tester. Video conferencing was also tested, and the results of those tests are then presented. VOIP testing was also performed and the results documented in the next section. GPON requires a router, and several routers were tested for compatibility with GPON, and the results of these tests are then presented. Security tests were performed and the results are contained in the next section. Because GPON is designed to be an access layer network technology, the results of the “end user experience” are then documented. Next, the operations and management of GPON are discussed. Finally, the report ends with a recommendation about GPON for use at Sandia National Laboratories.

Introduction to GPON

Without attempting to be a complete networking tutorial, this section will present an overview of access layer network technologies and also introduce Gigabit Passive Optical Networks (GPON).

In the traditional hierarchical network model, there are the core, distribution, and access layers. The functions of these layers are as follows:

- The access layer provides user access to the network.
- The distribution layer provides policy-based connectivity (routing, ACLs, etc.) for the access layer
- The core or backbone layer provides high speed transport to satisfy the connectivity needs of the distribution layer devices.

The access layer of the network can use many technologies to provide network connectivity for a user. These technologies include:

- Dialup - The user connects to the network via a modem and telephone line.
- Traditional Workgroup – The user connects to the network using a switch and/or router.
- Cable Modem Service – The user connects to the network using the CATV infrastructure.
- xDSL – Digital Subscriber Line, the "x" signifies various variants. This technology uses the existing telephone lines in the home or a business. It also uses telephone lines to transport user information to the CO where it connects to the internet.
- Wireless – The user connects via radio signal to an access point. The access point then connects to the existing wired network.
- FTTx – Fiber to the X. Possible Xs are P for Fiber to the Premises. Or B, for Fiber to the Building. Or H, for Fiber to the Home.

Access layer technologies, especially for residential customers, have been moving towards FTTx based solutions because of several factors. Fiber can provide more bandwidth for a longer distance. For example, copper can support rates up to 1 Gbps for distances of 100 meters, but fiber can support 1 Gbps rates for distances of 5 kilometers. Fiber is not susceptible to electrical noise or electrical spikes. Also, the cost of a fiber installation is decreasing with newer manufacturing technologies which allow for more factory terminated connections.

Fiber is not without drawbacks, however. Fiber is harder to splice, repair, and needs to be handled carefully. Regenerators and amplifiers are problematic and more expensive to deploy than copper. Digital signal processing requires electronics, which requires the optical signal to be converted to an electrical signal, processed, and then converted back to an optical signal. Typically switching is easier with electronics but possible with photonics. Pure fiber networks are mostly point-to-point and rings.

Optical access layer networks can be either active optical networks or passive optical networks. Active optical networks (AON) consist of a direct fiber run in a point-to-multipoint topology. It requires an expensive optical transceiver on each end of the link. Thus for N end users it would require 2N transceivers.

Passive Optical Networks (PON) implement a point-to-multipoint topology purely in optics. This avoids costly optic-electronic conversions. They use passive splitters which require no power and have virtually an unlimited Mean Time Between Failure (MTBF). Finally, Passive Optical Networks require only N+1 optical transceivers which is the minimum possible.

There are different PON standards. The current PON standard most popular in the United States is GPON (Gigabit PON) and is documented in ITU-T G.984.X. Figure 1 illustrates a typical GPON configuration.

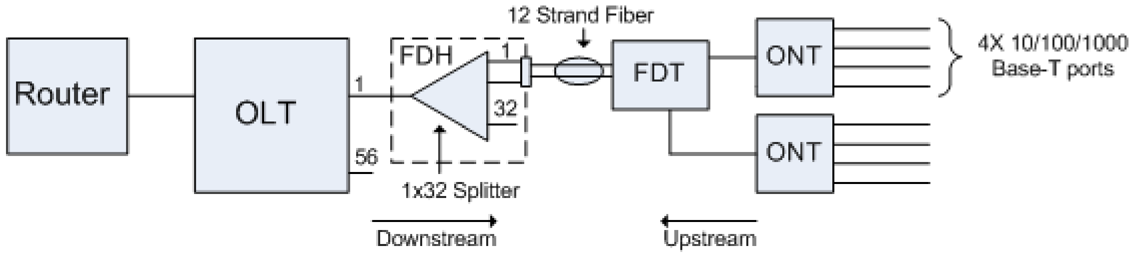

Figure 1. GPON Components

Figure 1 illustrates a typical GPON configuration. The router is used to connect the GPON network to the rest of the network. The Optical Line Terminal (OLT) is used to distribute an optical signal to the user network devices which are called Optical Network Terminals (ONTs). The OLT can not service the GPON network by itself. It needs be connected to a router capable of providing Proxy ARP services.

Depending upon the size and model, the OLT can have many ports. In Figure 1, the OLT has 56 ports. Each port connects to a single strand of singlemode fiber. The fiber connects to an optical splitter. Optical splitters come in various sizes or number of splits. Typical sizes are 32, 64, and 128. The splitter shown has 32 splits. The splitter is housed in an enclosure called a Fiber Distribution Hub (FDH). The FDH can house several splitters depending upon its size. The output of the splitter, which is 32 individual fibers connects to SC/APC (Subscriber Connector / Angle Polished Connector) connectors. Each one of these connectors has a strand of optical fiber on the opposite side. These fibers are wired in such a way that groups of 12 fibers are terminated on a MTP (Mechanical Transfer Pull Off) connector. A single cable with 12 strands of optical fiber is connected to the other side of this MTP connector. The 12 strand fiber optic cable is then run to a location close to a group of users and is terminated in a Fiber Distribution Terminal (FDT). Common sizes for FDTs are 6, 12, 24, and 48 output connectors. From the FDT a single singlemode fiber is connected to each ONT. The ONT has one or more RJ-45 ports for the connecting to a computer.

Basic GPON operation begins with an IP packet sent from the router to the OLT. The OLT takes the IP packet and encapsulates it within a GPON frame along with some management information and it is broadcast out the correct GPON port. When ONTs are discovered by the OLT, the OLT maintains a database of ONTs and the OLT port to which they are connected. Because all 32 ONTs on the splitter receive the same broadcast, the transmission is encrypted using AES-128. This prevents eavesdropping. The encryption key is negotiated after the ONT is discovered by the OLT. In GPON terminology, transmissions from the OLT to the ONT is classified as downstream.

When information is sent from the ONT to the OLT, the operation is different. Each ONT gets a time slice to transmit using TDMA (time division multiple access) technology. The transmission is sent unencrypted. The ONT may have multiple Ethernet ports. However, an ONT can not act as a stand alone device. It must be connected to an OLT. Also, because of the need for Proxy ARP, an OLT requires a router to perform that function.

Note that there is only one fiber optic cable that connects to an ONT. This is possible because the downstream wavelength is typically 1490 nanometers. The upstream wavelength is 1310 nanometers. Therefore only one cable is needed per ONT.

GPON Host-to-Host Performance Testing

The main purpose of all testing is to expose problem areas (if any) before the new technology is placed into a production environment. One of the most important criteria for the evaluation of a new network technology is performance. Although there are specifications on the amount of bandwidth that GPON is capable of supplying, actual throughput tests were performed to verify it. Tests were conducted with actual hosts as described below.

Host-to-Host Baseline Testing

Host-to-host testing was performed to determine what actual performance could be expected between hosts. Before testing any GPON equipment, a basic test was performed to determine the performance of the hosts, their TCP stacks, and the test program.

The test program used was developed by James A. Schutt (Org. 09336). It used non-blocking socket I/O. It was capable of either unidirectional or bidirectional data transfer across each direction.

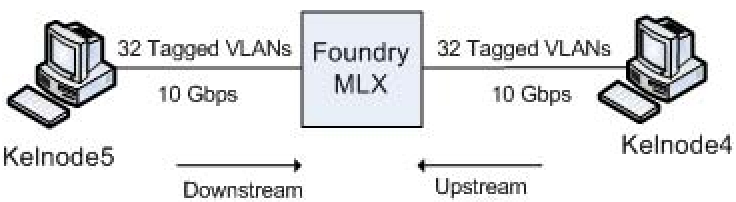

Figure 2. Host-to-Host Test Setup

The test setup for the first set of tests is illustrated in Figure 2. The testing was performed using two hosts named *Kelnode4* and *Kelnode5*, each configured as stated in Table 1. Although the NICs used have TCP offload capability, the host Linux TCP stack was used for all tests.

Table 1. Host Configuration

Hardware	
CPUs	**2 AMD Opteron (2600 MHz, 1 MB L2 Cache)**
RAM	**1 GB**
10 Gig NIC	**Chelsio T310**
Software	
Kernel	**2.6.23.14 from kernel.org**
OS Kelnode4	**Red Hat WS 4 Update 5**
OS Kelnode5	**Red Hat WS 5 Update 2**
NIC	**Version 1.0.113**
Test Utility	**A2a_bs.c**

For this test procedure, the 10 Gbps NICs on both Linux hosts were configured as trunks carrying multiple 802.1q VLANs. The test program was used to start a TCP connection on each VLAN, and measured the data transfer rate on each connection simultaneously. Multiple VLANs were used to simulate up to 32 hosts, one per VLAN.

In order to establish a performance baseline for the host TCP stacks and test application, the upstream and downstream hosts were connected through a 10 Gbps capable device. For these tests, a Foundry Networks (now Brocade) NetIron MLX switching router was used. Table 2 presents the test results for the host-to-hosts tests.

Table 2. Host-to-Host Test Results Through a Foundry NetIron MLX

Host-to-Host Test Results Through a Foundry NetIron MLX				
	Unidirectional		Full Duplex	
Number of Streams	Upstream Throughput in Mbps	Downstream Throughput in Mbps	Upstream Throughput in Mbps	Downstream Throughput in Mbps
1	311.819	368.639	217.090	217.042
2	329.942	388.944	228.032	228.035
4	327.923	383.017	234.561	234.575
8	321.365	378.915	218.099	218.129
16	340.668	398.565	197.349	197.410
24	348.558	442.933	184.535	184.594
32	348.442	442.380	195.272	195.409

Cisco 1 Gbps Uplink Testing

In order to have valid comparison of existing network technologies, another test was performed using a Cisco Catalyst 6509. This test was similar to the first test, but had a 1 Gbps connection between the Cisco Catalyst 6509 and the Foundry MLX. This configuration would be similar to what a user would experience when a 1 Gbps Uplink was used on an access switch that connects to the computer of the user.

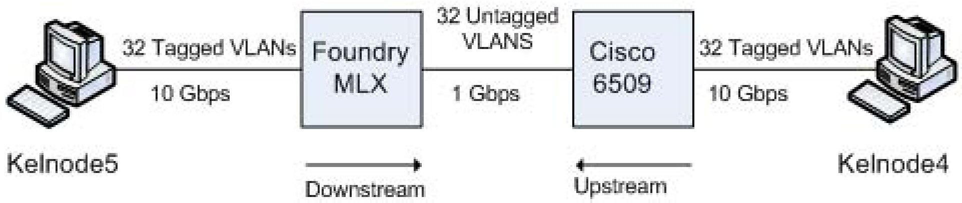

Figure 3. Host-to-Host Test Setup Using a Cisco 6509 with a 1 Gbps Uplink

The results of the Host-to-Host Tests using a Cisco 1 Gbps Uplink are shown in Table 3.

Table 3. Host-to-Host Test Results Using a Cisco 1 Gbps Uplink

Host-to-Host Tests Results Using a Cisco 1 Gbps Uplink				
	Unidirectional		Full Duplex	
Number of Streams	Upstream Throughput in Mbps	Downstream Throughput in Mbps	Upstream Throughput in Mbps	Downstream Throughput in Mbps
1	116.916	114.906	111.899	111.896
2	116.947	114.934	110.400	112.126
4	116.952	114.924	111.077	112.060
8	117.272	114.938	111.556	111.908
16	117.217	114.941	108.288	112.453
24	117.124	114.946	106.607	112.503
32	116.793	114.926	104.219	112.667

GPON Testing

After performing host-to-host tests as previously described, the GPON host-to-host tests were performed. The test setup is shown in Figure 4. In this configuration the Juniper EX 4200 is a router which provides the OLT with the necessary services such as proxy arp and provides the interface between the production network device (in this case a Foundry MLX) and the GPON network which includes the OLT, FDH, FDT, and ONTs. The Foundry X448 switch on the right side is used to take the data stream from *kelnode4* and, based upon the VLAN tag, switch it to the port which connects to the designated ONT.

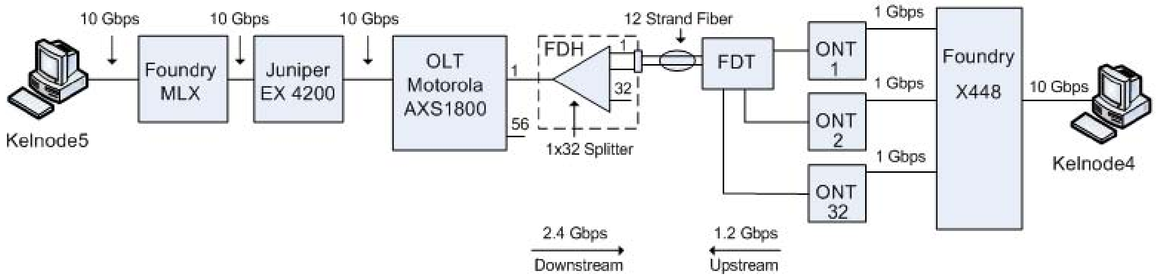

Figure 4. Host-to-Host Test Setup using GPON

The equipment used in the test is shown in Table 4.

Table 4. GPON Equipment

GPON Equipment	
OLT	Motorola AXS 1800 Version R6_0_1 software
ONT	Motorola ONT1100GE
Splitter	ADC 1x32
FDH	ADC 288 fiber
FDT	ADC 24 port

The results of the Host-to-Host Tests using the GPON Test Network are shown in Table 5.

Table 5. Host-to-Host Test Results Using the GPON Test Network

Host-to-Host Test Results Using the GPON Test Network				
	Unidirectional		Full Duplex	
Number of Streams	Upstream Throughput in Mbps	Downstream Throughput in Mbps	Upstream Throughput in Mbps	Downstream Throughput in Mbps
1	51.096	96.272	49.777	37.448
2	102.177	116.261	40.444	40.444
4	119.880	116.190	44.527	44.527
8	122.474	115.601	39.218	39.218
16	126.955	114.355	33.682	33.682
24	132.696	113.662	32.215	32.215
32	136.770	112.715	32.470	32.470

Analysis of Test Results

These test results have suggested that GPON equipment contains buffers that may be shared, and are sufficiently small that TCP performance under multiple contending streams may be adversely affected in the following ways:
1) full utilization of the downstream optical data path cannot be achieved by a significant margin;
2) committed information rate guarantees cannot be met for TCP traffic;
3) under competing upstream and downstream TCP traffic, utilization of the downstream optical data path is even more severely compromised than under the presence of only competing downstream TCP flows.

Spirent AX/4000 Testing

The next set of tests performed were using a Spirent AX/4000 tester. This tester was used in a way similar to the host-to-host testing described in the last section. The difference was that the AX/4000 was not using TCP based flows but rather IP flows. Therefore there was no TCP backoff due to lost packets. Therefore the throughput results were somewhat higher than with the TCP based flows with the host-to-host testing.

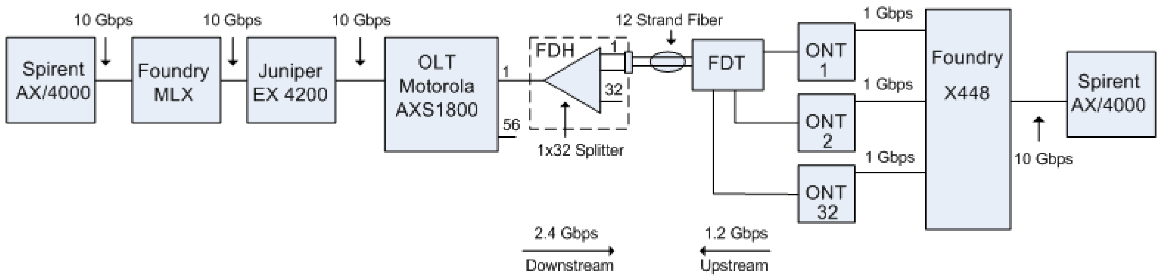

Figure 5. Spirent AX/4000 Test Setup

Figure 5 illustrates the test setup used with the Spirent AX/4000. Note that in the illustration there are two Spirent AX/4000s shown. However, they are separate ports on the same AX/4000.

The first set of tests performed involved sending IP packets downstream (left to right in Figure 5) for packet sizes of 64, 512, and 1500. For those packet sizes, the number of streams were also varied from 1 to 32. The purpose of the test was to determine how many packets could be sent without incurring any lost packets. The results are shown in Table 6.

Table 6. Spirent AX/4000 Test Results Downstream Without Loss

Spirent AX/4000 Test Results Downstream Without Loss			
Number of Streams	64 byte packets	512 byte packets	1500 byte packets
1	692	846	862
2	1394	1518	1701
4	1615	1924	1965
8	2160	2418	2426
16	1615	1924	1965
24	1384	1652	1684
32	1289	1541	1574

The next set of tests performed involved sending IP packets upstream (right to left in Figure 5) for packet sizes of 64, 512, and 1500. For those packet sizes, the number of streams were also varied from 1 to 32. The purpose of the test was to determine how many packets could be sent without incurring any lost packets. The results are shown in Table 7.

Table 7. Spirent AX/4000 Test Results Upstream Without Loss

Spirent AX/4000 Test Results Upstream Without Loss			
Number of Streams	64 byte packets	512 byte packets	1500 byte packets
1	390	416	418
2	562	863	847
4	896	962	967
8	447	734	997
16	314	734	977
24	429	866	997
32	524	962	1057

The next set of tests performed involved sending IP packets downstream (left to right in Figure 5) for packet sizes of 64, 512, and 1500. For those packet sizes, the number of streams were also varied from 1 to 32. The purpose of the test was to determine how many packets could be sent even while incurring loss. The results are shown in Table 8.

Table 8. Spirent AX/4000 Test Results Downstream With Loss

Spirent AX/4000 Test Results Downstream With Loss			
Number of Streams	64 byte packets	512 byte packets	1500 byte packets
1	699	848	869
2	1398	1697	1738
4	1622	1927	1968
8	2212	2423	2435
16	2210	2403	2435
24	2200	2405	2435
32	2114	2395	2435

The next set of tests performed involved sending IP packets upstream (right to left in the Figure 5) for packet sizes of 64, 512, and 1500. For those packet sizes, the number of streams were also varied from 1 to 32. The purpose of the test was to determine how many packets could be sent even while incurring loss. The results are shown in Table 9.

Table 9. Spirent AX/4000 Test Results Upstream With Loss

Spirent AX/4000 Tests Upstream With Loss			
Number of Streams	64 byte packets	512 byte packets	1500 byte packets
1	396	432	426
2	708	865	856
4	913	996	1007
8	928	1016	1027
16	969	1060	1067
24	1003	1098	1112
32	1040	1144	1157

The final set of tests is the packet burst test. For these tests, consecutive 1400 byte packets are sent at line rate until a packet is lost. Table 10 presents the results.

Table 10. Spirent AX/4000 1400 Byte Packet Burst Test Results

Spirent AX/4000 1400 Byte Packet Burst Test Results			
	Downstream		Upstream
1400 byte packet	10 Gbps line rate	1 Gbps line rate	1 Gbps line rate
Max Burst Size Without Loss	33 packets	50-75 packets	175 Packets

Analysis of Test Results

The results suggest a small amount of effective buffering in the downstream path. All downstream performance issues are tied to the effectively small buffer in the OLT. Tripling of that buffer size or an effective fine rate shaping capability on the attached switch/router is required to effectively deploy this GPON system. An order of magnitude increase in effective buffer size is needed to be competitive with the currently deployed Gigabit Ethernet switches.

However, this system can be recommended for replacement for most users who are currently connected via a 100 Mbps port. Gigabit Ethernet connected users should be looked at closely as the peak performance for that class of user will likely drop by about 10% assuming a 1 Gbps or faster attached server. Far worse for potential users of GPON, the sustained performance delivered can be reduced by more than 50% for some heavy network users during peak usage times. Another category of users to be concerned with are those users whose main work role involves remote computing, which will be especially vulnerable when connected via this GPON equipment. As performance guarantees in the current network are undefined, the impact of GPON upon those users will be highly subjective. Heavy users will probably perceive that performance has been reduced. Users currently receiving service via a 100 Mbps connection will most likely perceive GPON as an upgrade.

Performance concerns can be divided into two categories, performance to/from core services and “on subnet” performance issues. The core services performance issue is being constrained primarily by the small per port buffer in this OLT. This small buffer also impacts the “on subnet” performance, but this issue is primary an architectural issue when using GPON as compared to our existing switch infrastructure. This system would not be advised for users that have large local subnet resources. Possible categories of these users are HPC (computational science), manufacturing, radar imaging, and satellite. To satisfy the needs of all users, a general networking design should be implemented that is flexible enough to allow for an expected 10-20% of users to run outside the GPON environment.

Video Conferencing Testing

Before deployment of GPON in the Sandia network infrastructure, additional testing was needed for applications such as collaboration technology (e.g. videoconferencing and audio conferencing) to determine their suitability within the GPON environment. Video and audio conferencing are real-time communications tools that, when operating in an IP network, require that packets arrive on time (not out of sequence) with a minimum of latency and jitter. If IP packets arrive out-of-sequence or outside the bounded latency required, human communication is interrupted or disrupted to the point that little or no effective communication can take place. Additionally, video and audio transport requires a symmetrical network. Differentials between uplink and downlink can cause disruption in the communication path in the same manner that lost packets and latency affect it. These tests were performed by the VACT Videoconference and Collaborative Technologies (VACT) team in the GPON test bed and were designed to affirm suitability of GPON for transport of video and audio real-time traffic.

Background

Real-Time Communications IP Transport Requirements Overview[1]

The International Telecommunications Union (ITU) is responsible for establishing standards related to communications technologies including the requisite standards that manufacturers use to build audio and video codecs (coders/decoders). Video and audio conferencing systems that comply with ITU standards will interoperate system to system. The ITU H.323 umbrella standard was adopted in 1996 in support of audio (telephony) and videoconferencing transport in "non-QoS" IP networks. QoS (Quality of Service) defines the network parameters necessary to guarantee real-time packet delivery, end-to-end. Since the adoption of H.323, bandwidth and connectivity requirements for LANs and WANs have increased in orders of magnitude. Today, all real-time communications protocols must compete for bandwidth with web surfing, email, chat, FTP and many other application services. To address network congestion, standards setting organizations have defined the requirements for managed networks in support of real-time communication. ITU-T Recommendation H.361 *"End-to-end Quality of Service (QoS) and Service Priority Signaling in H.323 System"* is adopted in Version 6 release of ITU H.323. As expressed in H.361 and in recommendations from Cisco, the IP network should emulate a circuit switched network in support of real-time communications. Emulating circuit switching requires that the non-deterministic elements of the IP network be managed to provide a deterministic network.

[1] For a more complete discussion of the topic refer to *VACT Network and Telecommunications Requirements for Real-Time Collaboration and Videoconferencing*, SAND 2007-7358P, by David H. Dirks.

A real-time communications network supports[2]:

- Isochronous connectivity: In an isochronous network, all packets arrive in time and on time with no variation. The loss of frames produces unacceptable results. There is no opportunity to makeup time or to replace lost or corrupt packets.
- Low jitter: There must be minimal time variation between packets and therefore low jitter within the network.
- Low delay: Latency must be bounded. End-to-end delay should not be more than 150 ms including video encoding time[3]. Excessive delay produces unintelligible audio. Most users rate audio quality as exceedingly important.
- QoS Markings: Routers should honor QoS markings that have been set in the TOS Byte. These markings could be either by Differentiated Services (Diffserv) or IP Precedence, and these packets should be given some sort of priority queueing.

GPON as Infrastructure for Real-Time Communications

GPON technology was originally designed for the consumer home market as a replacement for DSL and cable modem service. The drivers for the consumer market are high bandwidth downlink (TV, movies, data) and low bandwidth uplink (computer data, subscription information, voice) which is descriptive of an asymmetrical network. The uplink is typically (but not necessarily) bandwidth limited and constrained by a time division multiplexing process. Both factors could contribute to the interruption or disruption of real-time traffic. At the same time, GPON can support QoS with Diffserv (64 levels of QoS), or IP Precedence (8 levels of QoS). Another key factor is the ability to reserve bandwidth for certain traffic within the network and assign it a Committed Information Rate (CIR). Both factors can help alleviate some of the “first blush” problems associated with using GPON real-time traffic. There was not a great deal of data in the industry associated with testing real-time, symmetrical traffic within GPON. Therefore, participation in the test bed was essential.

GPON Tests for Videoconferencing

Lacking access to an integrated software package that objectively tests and affirms the robustness of the GPON environment, it was determined that a combination of objective and subjective testing would be performed with existing equipment similar to a production environment. To do this, we selected the current model of Tandberg codecs. The Tandberg codec is a robust platform for testing and conveniently provides some

[2] Refer to ITU-T Recommendation H.361 “*End-to-end Quality of Service (QoS) and Service Priority Signaling in H.323 Systems*” for a complete description of network requirements.
[3] Any round-trip delay beyond 300 ms will produce lip sync timing errors. The conference becomes annoying above 400ms. Greater than 700 ms is intolerable.

useful network diagnostics such as end-to-end audio and video packet loss and jitter. The Tandbergs were upgraded to the latest firmware to provide the most current error correction capability. Codec encoding and decoding error correcting algorithms have improved significantly in the last few years. Current codecs can sustain a significant packet loss prior to any noticeable subjective picture degradation. By analyzing both objective data from the codecs and subjective information in the form of a large screen display for video and high-quality headphones for audio, it could rapidly be determined whether or not network congestion affected the user experience.

Test Equipment

A special rack for use in the GPON Test Bed was constructed as illustrated in Figure 6 and Figure 7. The rack consists of two Tandberg videoconference codecs and a combination of both standard definition and high definition cameras. Audio transmission and monitoring was accomplished through the use of the Symmetric audio preamp and headphone amplifier. BeyerDynamic DT 290 headsets were selected to isolated room noise from subjective audio test signals.

Test Codec #1 - specifications
Tandberg 3000 MXP codec, Firmware F7.2 NTSC, 1.5 Mbps bandwidth option, Natural Presenter Package (NPP) option, IP enabled
Sony EVI-D100 standard definition camera
Symmetric 302 microphone preamp
Symmetric 304 headphone amplifier
BeyerDynamic DT 290 headset

Test Codec #2 - specifications
Tandberg 6000 MXP codec, Firmware F7.0 NTSC, 1.5 Mbps bandwidth option, Natural Presenter Package (NPP) option, IP enabled
Sony EVI-D100 standard definition camera
Tandberg Precision HD high definition camera
Tandberg VideoSwitch
Symmetric 302 microphone preamp
Symmetric 304 headphone amplifier
BeyerDynamic DT 290 headset

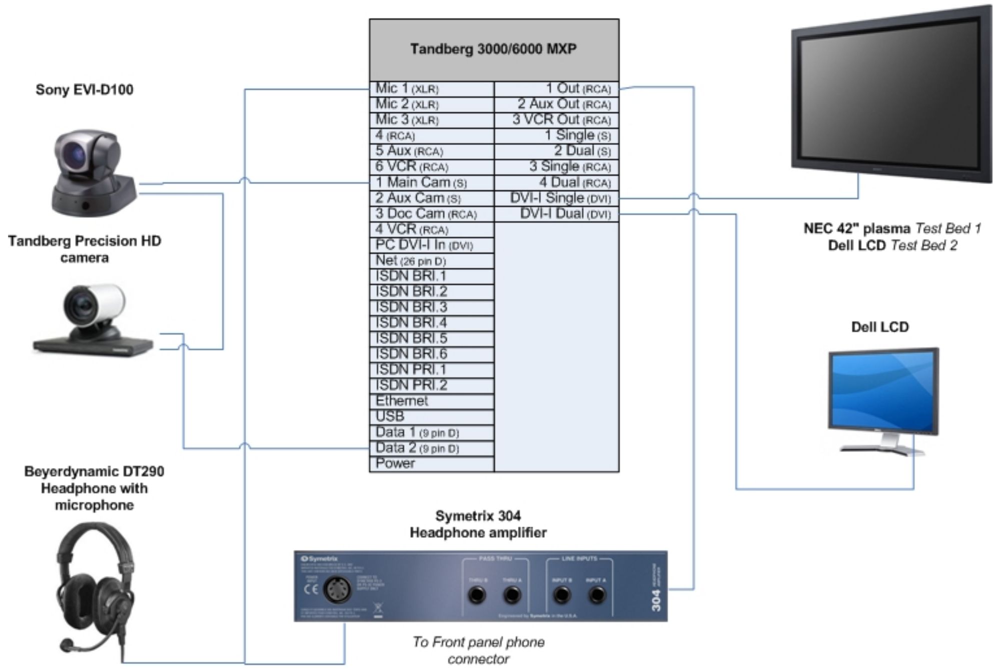

Figure 6. Codec Test Rack Setup

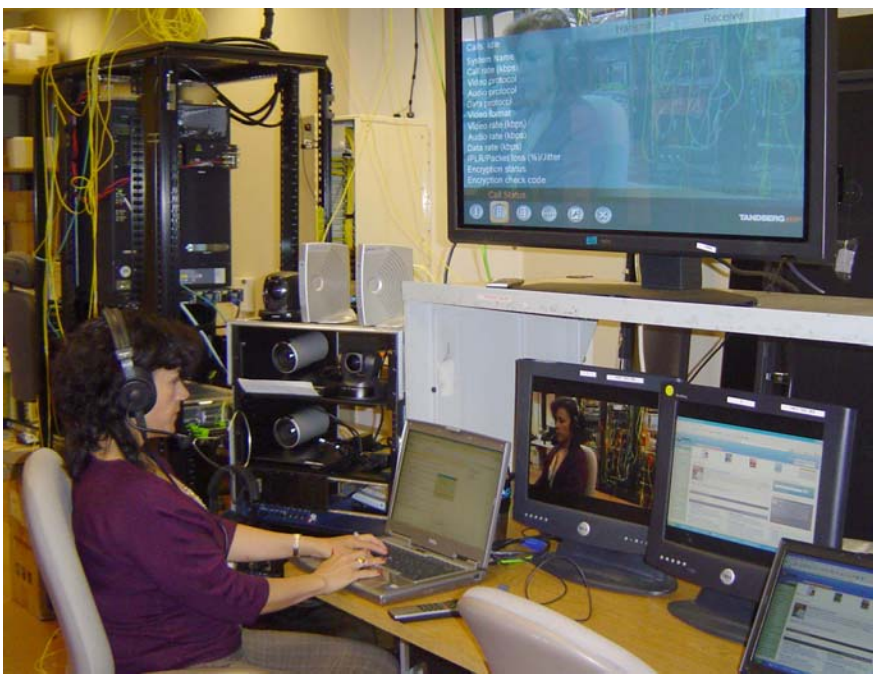

Figure 7. VACT GPON Test Bed Setup

Test Setup

The VACT Test Rack as shown in Figure 6 was connected to the GPON Test Bed ONTs as shown in Figures 8 and 9 for objective and subjective tests.

Objective Data Tests Goals

The process to obtain objective test data included: test various call speeds (data rates); watch for packet loss or any call anomalies; test with video and audio only, then test with H.239 invoked with 1024x768 PPT and test patterns; note any signs signal degradation. Signal degradation is represented in the picture by digital pixilation of the image or macro-blocking[4].

Subjective Data Tests Goals

The process to obtain subjective test data included: analyze video and audio quality – rate quality; analyze H.239 signal with test system – rate quality; the quality rating – 1 through 5 (1=worst, unusable; 5=best, no discernable degradation in signal quality e.g. perfect).

Test Processes

Test Process #1 – QoS OFF
Codecs on different ONTs / same OLT blade
CALL: 6000 to 3000; 3000 to 6000
Place series of calls – record data
384Kbps; 768Kbps; 1 Mbps; 1.5 Mbps

Test Process #2 – QoS OFF
Codecs on different ONTs / different OLT blade
CALL: 6000 to 3000; 3000 to 6000
Place series of calls – record data
384Kbps; 768Kbps; 1 Mbps; 1.5 Mbps

[4] Macro-blocking is often referred to as "blocking". Macro-blocking refers to the DCT encoding algorithm's sample block size of 8x8 pixels. Those discrete 8x8 blocks are very evident in the picture as the picture degrades in quality.

Test Process #3 – QoS ON
Codecs on different ONTs / same OLT blade
CALL: 6000 to 3000; 3000 to 6000
Place series of calls – record data
384Kbps; 768Kbps; 1 Mbps; 1.5 Mbps
Load and overload the network with other traffic

Test Process #4 – QoS ON
Codecs on different ONTs / different OLT blade
CALL: 6000 to 3000; 3000 to 6000
Place series of calls – record data
384Kbps; 768Kbps; 1 Mbps; 1.5 Mbps
Load and overload the network with other traffic

Network Setup

To simulate possible real-world scenarios, the GPON Test Bed was setup as illustrated in Figures 8 and 9. Test processes 1 and 3 were conducted on different ONTs connected to the same OLT blade as illustrated in Figure 8. Test processes 2 and 4 were conducted on different ONTs connected to different OLT blades as illustrated in Figure 9.

Tests were conducted in a pristine environment, no other network traffic, to develop baseline performance data. To simulate real world conditions, when other applications on the network will cause congestion and packet contention, the test network was loaded with various levels of data traffic from additional ONTs. The load was provided by the Spirent AX/4000.

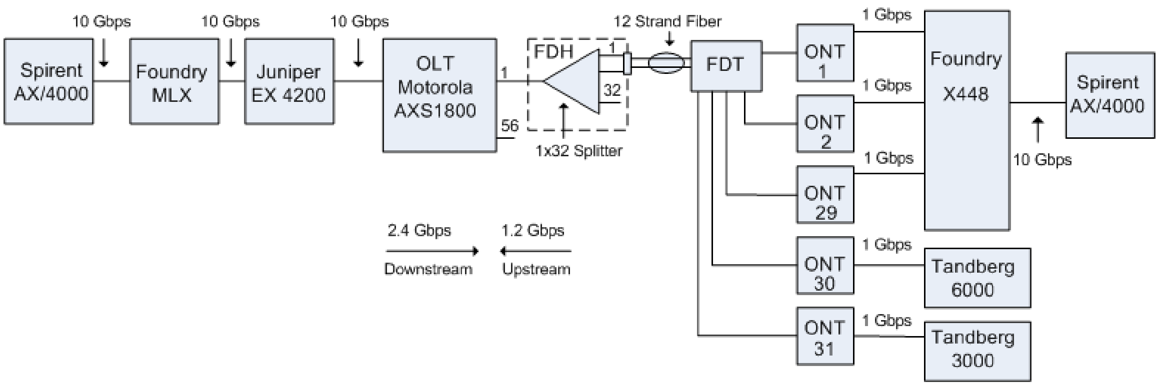

Figure 8. Test Setup: Different ONT, Same OLT blade

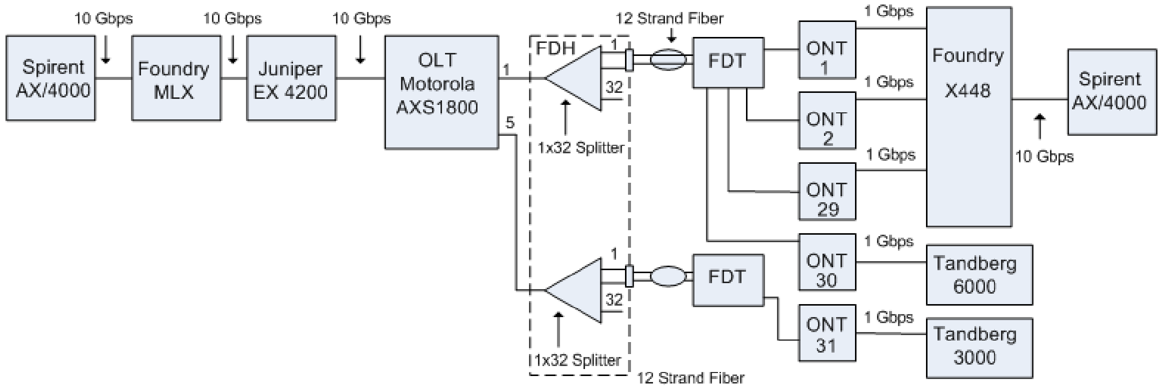

Figure 9. Test Setup: Different ONT, Different OLT Blade

Test Results

Baseline Tests

The baseline tests established the metrics for consistent, reliable and robust real-time video traffic in the GPON environment. Videoconferencing performed at the highest level with no perceivable loss of quality or significant packet loss or jitter.

Network Loading Tests

In order to save time, the loading tests were performed on the same OLT blade only with a videoconferencing data rate of 1.5 Mbps. When loading was added to the network, it was added on the same OLT blade with 29 ONTs. Note that one ONT had problems and therefore only 29 were used instead of 30. This was considered a minor deviation, and the test results are still considered valid.

Committed Information Rate (CIR) Off

The first tests were performed with Committed Information Rate (CIR) turned off. With no CIR, the videoconference downstream from the OLT remained stable up until an aggregated data rate of 3.5 Gbps. When the OLT loading reached 3.6 Gbps, the codec changed its data rate; it downspeeded[5] to maintain the call. When the OLT loading reached 10 Gbps in each direction, strong pixilation was observed and codec downspeeding occurred. Both audio and video were affected.

[5] Downspeeding – the codec analyzes network congestion and compensates for excessive congestion by changing the speed of the call in the down direction. Calls originally established at 1.5 Mbps will downspeed and renegotiate the data rate to 256 Kbps over a series of steps in order to maintain the call.

Committed Information Rate (CIR) On

With Committed Information Rate (CIR) turned on and set to 5 Mbps to protect video traffic, video calls maintained good quality. When the OLT was loaded to 10 Gbps upstream, good quality video and audio were maintained as long as the downstream load did not exceed 6 Gbps.

The results of these tests are summarized in Table 11.

Table 11. Summarized Videoconferencing Test Results

Summarized Videoconferencing Test Results					
CIR of Test Load	**CIR of Video**	**Downstream Load**	**Upstream Load**	**Perceived Video Quality on 3000**	**Perceived Video Quality on 6000**
0	0	3.5 Gbps	10 Mbps	Good	Good
0	0	3.6 Gbps	10 Mbps	Good	Bad
0	0	10 Mbps	10 Gbps	R[6]	Good
0	0	10 Gbps	1G across 4 devices	R[7]	Bad
0	0	10 Gbps	10 Gbps	Bad	Bad
0	5 Mbps	6 Gbps	1.6 Gbps	Good	Good

Other Tests

In order to simulate a more real-world scenario, the OLT loading was changed from continuous data rate to burst mode. The downstream was loaded with a 1.8 Gbps continuous stream plus bursts applied that averaged 300 bursts/second with an average number of packets per burst of 500 at random intervals. During this test, the codecs downspeeded to adjust for congestion but did not drop the call entirely and maintained a good quality perceived image.

Analysis of Test Results

The tests demonstrate that without invoking QoS or the CIR function within GPON, traffic congestion may impair the videoconference application to a point that it becomes unstable and unusable. With CIR at 5 Mbps, there is a “fence” that protects the application so that congestion does not degrade the real-time data. But CIR appears to protect the traffic only to a point. Since testing in the lab does not exactly simulate real-

[6/7] R: Good perceived quality with codec downspeeding to accommodate network traffic.

world conditions, something other than steady state traffic needs to be used for loading the network. Bursty traffic, the type more often encountered in production networks, appears to cause some disruption in service within GPON. The disruption is not to a point of failure, but is serious enough to interrupt the human experience as the participants wait for the codec to downspeed and renegotiate the call.

These tests used loading which was far in excess of what GPON was designed to support. Also, most often the videoconferencing stream will be competing with TCP traffic. TCP traffic will "back off" i.e. reduce its transmission rate if packets are lost. Therefore, video conferencing should work with GPON at the corporate level if it is given some preferential treatment with QoS.

VOIP Testing

Although not immediately planned as a component of an initial GPON deployment at SNL, VOIP (Voice over IP) was tested for several related reasons. The first reason was to determine how well VOIP could be supported in a GPON environment. The next reason was that real time applications such as VOIP and videoconferencing can give valuable insights into how well QoS can be supported without the need for expensive test gear.

Test Setup

The test setup is shown in Figure 10. All non-VOIP connected ONTs were connected to a 1 Gbps port on the Foundry X448 switch to provide additional load that was supplied by the Spirent AX/4000. All of those connections are identical to the ONT 1 connection. Note that as in tests for other areas, there was only one Spirent AX/4000, but it had two 10 Gbps ports. One of the 32 ONTs was not working for this test. But there were 27 ONTs to supply the test load. For all tests a CIR of 5 Mbps was provisioned on all of the ONTs used for the VOIP phones and call manager.

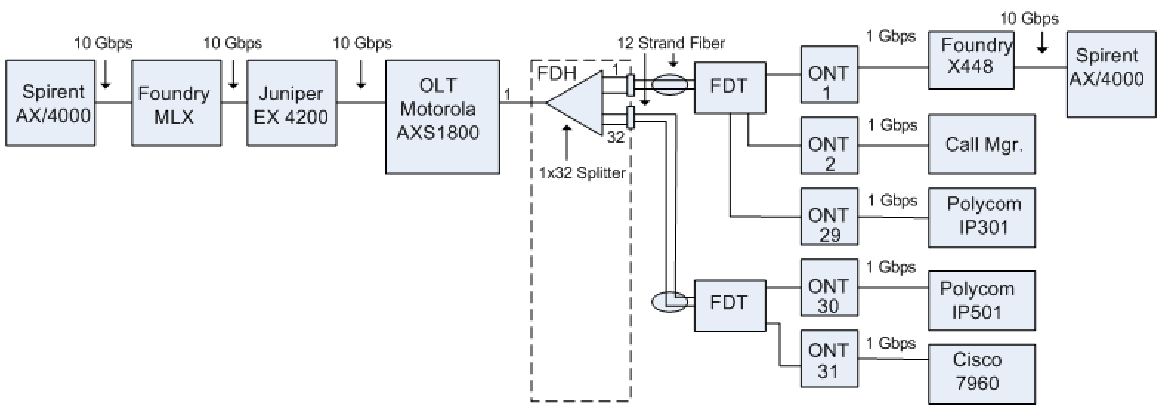

Figure 10. VOIP Test Setup

Table 12 lists the VOIP equipment details.

Table 12. VOIP Equipment Details

VOIP Test Setup Details	
Call Manager Hardware	HP xw4100
Call Manager Operating System	Linux CentOS Version 5
Call Manager Software Application	Trixbox 2.6.2.1 based on Asterisk 1.4
Telephone Protocol	SIP
IP Telephone	Polycom IP301
IP Telephone	Polycom IP501
IP Telephone	Cisco 7960
Primary Codec	G.711 Mu-law

Test Results

The objective of the tests was similar to the videoconferencing tests. VOIP calls were made between the phones while the background load traffic was increased. The load traffic was increased until the call became empirically unusable due to dropped packets, etc. For all tests a CIR of 5 Mbps was provisioned for each

The first test performed was to use a maximum upstream traffic load of 10 Gbps and to increase the downstream load. Both upstream and downstream packets where 1500 bytes in length. At the specified load levels, calls between VOIP phones were attempted. Note that because the test team did not have any special test equipment, voice quality was based upon the perception of the test team members. The results are presented in Table 13. The maximum data rate on the GPON packets downstream is 2.4 Gbps and upstream is 1.2 Gbps. Therefore, this test setup provided more downstream and upstream loads than the GPON system was designed to support. This was used to determine what combination of upstream and downstream loads would be necessary to cause errors. The results show that VOIP worked well with a 10 Gbps upstream load combined with a 5 Gbps downstream load.

Table 13. VOIP 1500 Byte Packet Test Results

VOIP 1500 Byte Packet Test Results		
Upstream Load in Gbps	**Downstream Load in Gbps**	**Results**
10	0	Voice OK. Call setup OK
10	1	Voice OK. Call setup OK
10	5	Voice OK. Slight delay in call setup
10	6	Voice OK. Delay in call setup.
10	8	Voice bad. Delay in call setup.
10	9	Voice bad, latency and jitter. Delay in call setup.
10	10	Unable to make a call.

The next set of tests used 64 byte packets. There was no upstream load. The results are presented in Table 14. The results show that with loads over 1.9 Gbps, actual calls could not be made, only voicemail was possible. At loads of 3.0 Gbps, not even voicemail was possible.

Table 14. VOIP 64 Byte Packet Test Results for Downstream Loads

VOIP 64 Byte Packet Test Results for Downstream Loads		
Upstream Load in Gbps	**Downstream Load in Gbps**	**Results**
0	1.3	Voice OK. Call setup OK.
0	1.7	Voice OK. Call setup OK.
0	1.9	Voice OK. Call setup OK.
0	2.0	Voice mail only. No call connection.
0	2.5	Voice mail only. No call connection.
0	3.0	No voicemail. No call connection.
0	4.0	No voicemail. No call connection

Another set of tests were performed using 64 byte packets, however this time there was no downstream load. The results are presented in Table 15. These results show that VOIP worked well for all loads upstream.

Table 15. VOIP 64 Byte Packet Test Results for Upstream Loads

VOIP 64 Byte Packet Test Results for Upstream Loads		
Upstream Load in Gbps	**Downstream Load in Gbps**	**Results**
5.0	0	Voice OK. Call setup OK.
7.5	0	Voice OK. Call setup OK.
8.5	0	Voice OK. Call setup OK.
9.9	0	Voice OK. Call setup OK.
10.0	0	Voice OK. Call setup OK.

Analysis of Test Results

The results of the VOIP tests presents enough data to conclude that GPON can support VOIP. It should be noted that VOIP uses low amounts of bandwidth. Depending upon the codec used, the bandwidth requirement could be between 4.8 Kbps and 64 Kbps. The tests performed for this report used 64 Kbps because the codec was G.711 Mu-law. This is not a great amount of bandwidth, but it must be guaranteed, otherwise call quality will suffer. Also SIP (Session Initiation Protocol) requires bandwidth to contact the call manager to setup the call. It should be pointed out that the test team did not have the equipment to do large scale tests of hundreds or thousands of phones.

Security Testing

Before deploying a new technology such as GPON, it should be tested and analyzed for security vulnerabilities, including serious vulnerabilities such as "security showstoppers." Also, GPON needed to be analyzed for the impact that it would have on current security procedures.

Strength of Security in Case of Improper ONT Relocation

In examining the GPON architecture a series of related questions arose regarding the end-node devices (ONTs). The ONTs are the only part of the GPON infrastructure which are located in the office space of an individual and thus potentially outside of the physical control of administrative processes. More specifically, the question became that of "What happens during a rogue ONT move?" To wit, if a user carries an ONT to a different location (or network drop) which is configured for a different VLAN or subnet, what happens then? Will the ONT come online, and if so with what functionality and on what VLAN or subnet?

These questions were answered by performing laboratory testing of GPON. An ONT was configured per the normal process to be a member of a particular VLAN and subnet, and subsequent host connectivity. By necessity, this includes network drop association. A client PC was attached to prove network connectivity, and packet sniffing was performed to understand network flows. Likewise, on another network drop, a different ONT was configured for a different VLAN and subnet. Then ONTs were moved per the scenario in question and behavior examined. The results of the test were very good. The ONTs were refused connection to the GPON network with no link available, and the GPON management console logged major error codes showing the events. Also, the client PC was unable to establish network connectivity, and packet sniffing indicated that no requests from the PC were ever answered. In summary, the GPON "failed closed."

Eavesdropping by Network Neighbors Addressed

All network topologies must address the potential for "network neighbors" – systems with potential access to physical transport layer shared with other systems. With Ethernet, for example, this is mitigated by switched topology, while WiFi utilizes encryption and access keys. In the case of GPON, downstream traffic is broadcast yet protected by AES-128 encryption and addressed to specific end-nodes (ONTs). Upstream traffic is not encrypted and therefore there were questions about possible eavesdropping and exposure prior to and during the key exchange process.

Examining the GPON architecture, it was determined that there was a possible exposure point, the optical splitter, where light reflections might allow neighboring drops to eavesdrop on their neighbors' traffic. Therefore, Steven A. Gossage (Org. 09336) implemented a lab test to examine this potential vulnerability. In summary, his tests indicated an extremely low likelihood of picking up enough signal from neighboring drops to assemble network packets.

Compatibility with Cyber Security Monitoring

The GPON Test Team investigated the GPON architecture in relation to monitoring "taps", and whether GPON would prevent or interfere with Cyber Security Monitoring activities. Fortunately, no problems are anticipated due to the point in the network architecture where these taps are located. Cyber monitoring data gathering is connected at a point outside of the impacted technology infrastructure; therefore no changes are needed to continue monitoring operations.

Administrative Network Management

Because almost all configuration and management operations for the GPON system tested require the management application (Motorola AXSVison). This software consists of a server and one or more clients. Several important questions needed to be answered about this application.

- Do administrative network management tools incur greater opportunity for abuse of privileged access?

Any person such as an administrator who has access to the management application can provision or change any ONT to have different parameters such as the VLAN or its QoS settings. However, this is no different than current network gear.

- What about the authentication and access controls for administration of the GPON management console and component administration? Do they support TACACS, RADIUS, 2-factor logins, and multiple authentication/privilege levels?

The Motorola AXSVison application runs on a Sun Solaris platform. Therefore all authentication features that are supported by Solaris are available for the administrator of the GPON system. In addition the application is password protected and supports multiple logins.

- Are remote administrative access protocols encrypted (i.e. ssh)?

Remote client access to the server initially sends an encrypted username and password to the server for authentication. After successful authentication, all further communication is unencrypted XML commands.

- Will administrative traffic be out-of-band?

Administrative traffic can be thought of as consisting of two main components. The first is OLT to ONT management. This is accomplished by the PLOAM field in GPON upstream and downstream packets. It is part of the G.984 standard. Although it uses the same fiber and packets, it is considered an administrative channel and therefore can be considered out-of-band. Remote client access to the server application uses the production network and is not out-of-band.

Potential Use in Classified Processing

GPON could be not be used in a classified environment without the use of approved encryption technology because the upstream traffic is not encrypted. There are currently no options in the system tested or in the G.984 standard to add approved encryption for the upstream.

Security Analysis

Security Showstoppers

When security is posed as the question of security "showstoppers," the team has found nothing to indicate cyber security threats inherent in GPON that would prevent the implementation and advancement of this technology at SNL. However, because the communications between the client and server are unencrypted in this implementation, it would be in both the best interest of the vendor and also the implementer if communications between the client and the server were encrypted. If this could not be readily accomplished, the clients should be placed on a private network, or use a VPN appliance.

Comparison to Current Network Technology

In some ways the final security topic can be summed up with the question "Is it any worse than what we have now?" Since the current technology is Ethernet over copper, and/or Ethernet over fiber, it has been determined that we have no indications that GPON is worse than the current technology. In fact, the architecture adds encryption, increased manageability, endpoint registration, and fiber optics to increase the overall security position.

Router Testing

Routers do not run any of the GPON G.984 protocols. However, a GPON system requires a router. The OLT is connected to the router. Its location can be viewed in Figure 1. The router is used to provide proxy ARP services for the OLT and ONTs. The OLT can not perform this function. Also the router needs to be able to disable gratuitous ARP replies, so it will not reply to gratuitous ARP requests.

Three routers were tested with the GPON system. They were the following:

- Juniper EX 4200 running JUNOS 9.2R1.10
- Cisco Catalyst 6509 running Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(33)SXH, RELEASE SOFTWARE (fc5)
- Brocade (formerly Foundry Networks) NetIron MLX running IronWare Version 4.0.0bT163

Analysis of Test Results

All three routers performed well. There was no user perceived difference in performance. It should be noted that the GPON test bed is a small system. Therefore only functionality was tested, not performance for hundreds or thousands of simultaneous users. Thus router selection for a GPON system should be based upon the number of users that it will need to support.

End User Experience

Although laboratory testing of GPON is useful, the end user experience is really the ultimate test. That is because GPON is designed to be deployed at the access layer of the network, which is where the end user gains access to the network. Five users volunteered to use GPON on a daily basis. These users compared GPON to the legacy network connections that they were using.

Tests Performed and Results

The tests performed included a wide variety of applications used in daily tasks. These included web access, email, saving and retrieving files to/from corporate storage systems, Secure Copy *scp* file transfers from host-to-host, corporate video, streaming audio, diskless booting and DHCP.

Web Access

Users accesed both corporate internal web sites and external web sites using Mozilla Firefox 3.0.11, Microsoft Internet Explorer 6.0, and Google Chrome 2.0. All browsers worked well.

DHCP

This test was performed by having several hosts (both Windows and Linux based) connected to ONTs in the GPON Test Bed, send a DHCP request to a server that was external to the GPON test bed, to obtain an IP address. DHCP worked fine for both Linux and Windows hosts.

Diskless Booting

This test was performed by connecting a diskless workstation to an ONT and booting. The server was external to the GPON Test Bed. There were no problems with diskless booting. However, only one machine was booted. There were not sufficient diskless workstations available to test how GPON would perform for multiple workstations booting simultaneously.

Email

This test used a Microsoft Outlook client to send and receive email from the corporate email server. All functions worked well.

Saving and Retrieving Files to/from Corporate Storage Systems

This test used a Windows based machine to save and retrieve files from the corporate storage systems. There were no problems.

Secure Copy (SCP)

This test used a Windows SCP client to connect to a Linux server and perform file transfers from client to server. The client was connected to an ONT in the GPON test bed. The server was connected to the corporate network. There were no problems. All transfers performed well.

Streaming Video

The test used both Microsoft Windows Media Player Version 11.0 and the Microsoft Silverlight plugin Version 2.0 with a Firefox 3.0.11 browser to view corporate and external video. Both Media Player and Firefox with the Silverlight plugin had no difficulty.

Streaming Audio

The test used both Microsoft Windows Media Player Version 11.0 to test streaming audio from external streaming audio sites. Streaming audio worked well.

End User Experience Summary

None of the GPON users experienced any problems whatsoever with GPON. There was no perceived latency, dropped packets, or any other network degradation that would suggest that GPON should not be deployed at the enterprise level.

Operations and Management

This section covers topics relevant to operating and managing the tested GPON system. It includes fiber infrastructure, OLT and ONT management, management via client and server, and system reliability. It finishes with an overall statement about the suitability for this GPON system to be deployed at SNL.

Fiber Infrastructure

Although the optical splitters, FDH, FDT, and cables are not manufactured by the GPON equipment vendor, they are a prerequisite for any GPON installation. Fiber Infrastructure is not specifically covered in this SAND Report. But, because of the numerous cables contained in the FDH and FDTs, cable management must be rigidly controlled. During the time when testing was being performed, there were instances when undocumented rewiring of the OLT, FDH, FDTs, and ONTs caused significant delays as the test team needed to trace fiber paths from OLT to ONT.

ONT Management

All functions pertaining to the operations and management of the ONT must be performed by the management application, in this case AXSVision. There are no administrative ports on the ONT.

OLT Management

The OLT has both an Ethernet management port and a DB9 serial port for management. The serial port is password protected and provides a CLI (command line interface). The CLI appears to be a subset of the commands needed to fully manage the OLT. Only by using the management application, can the OLT be fully managed (provisioned and monitored).

AXSVision Client and Server

The tested GPON system is fully managed with the vendor supplied application software named AXSVision. It requires both a client and a server. The server runs on a Sun Workstation running the Solaris Operating System. The client can run on the same Sun Workstation, or on a Windows PC. The management application (client and server) is a full featured system which is used both for provisioning and monitoring of the OLTs and ONTs. Because the fiber infrastructure is totally passive, it can not be managed with any system. However, AXSVision can display optical power readings from an individual ONT which can be an aid in troubleshooting. AXSVision can be used to track ONT problems by color changes. It can also gather real time statistics which is invaluable in troubleshooting.

Router Management

The router used in the GPON test bed was a Juniper EX4200. Juniper routers use JUNOS software. The CLI of JUNOS is considerably different than that of Cisco and Brocade (formerly Foundry Networks). Because of the lack of experience with JUNOS, tasks requiring provisioning of the Juniper EX 4200 took considerably longer than it would have taken if a more familiar CLI was used. Although not a showstopper, the support staff will need to be thoroughly trained in JUNOS before any routers running JUNOS can be placed in a production environment.

System Reliability

Although not deployed in a true production environment, the system overall performed fairly well. There were no failures in the OLT or management system which included the Sun Workstation and AXSVision Software. There were at 4 ONT failures. These failures were hardware failures; they could not be recovered by rebooting. Based on the fact that only 64 ONTs were acquired, that represented a failure rate of 6.25%. Also there were several times when ONTs needed to be rebooted. It is not known what caused the need for the reboot. Thus system reliability is a major concern.

Operations and Management Summary

If deployed at Sandia National Laboratories a GPON system will require a major change in the way daily operations and management are performed. Any access to the fiber infrastructure for troubleshooting or modifications must be tightly controlled and well documented. Failure to do so will lead to an inoperable network.

All operations and management to the active GPON components, i.e. OLTs and ONTs, must be accomplished by using the AXSVision client. Therefore, the support staff must be trained in its correct use. Also, concurrent troubleshooting of the same problem by several different technicians must be avoided.

When properly managed, GPON should simplify the network and make management easier. The main concerns are the high learning curve for new equipment and new procedures for operations and management.

Conclusion and Recommendations

This report presents test results of GPON system consisting of Motorola and Juniper equipment. The GPON system was tested in areas of data throughput, video conferencing, VOIP, security, and operations and management. The GPON system performed well in almost all areas.

GPON will not meet the needs of the low percentage of users requiring a true 1-10 Gbps network connection. GPON will also most likely not meet the need of some servers requiring dedicated throughput of 1-10 Gbps. Because of that, there will be some legacy network connections that must remain. If these legacy network connections can not be reduced to a bare minimum and possibly consolidated to a few locations, any cost savings gained by switching to GPON will be negated by maintaining two networks. A contract has been recently awarded for new GPON equipment with larger buffers. This equipment should improve performance and further reduce the need for legacy network connections.

Because GPON has fewer components than a typical hierarchical network, it should be easier to manage. For the system tested, the management was performed by using the AXSVison client. Access to the client must be tightly controlled, because if client/server communications are compromised, security will be an issue.

As with any network, the reliability of individual components will determine overall system reliability. There were no failures with the routers, OLT, or Sun Workstation Management platform. There were however four ONTs that failed. Because of the small sample size of 64, and the fact that some of the ONTs were used units, no conclusions can be made. However, ONT reliability is an area of concern.

Access to the fiber plant that GPON requires must be tightly controlled and all changes documented. The undocumented changes that were performed in the GPON test lab demonstrated the need for tight control and documentation.

In summary, GPON should be able to meet the needs of most network users at Sandia National Laboratories. Because it supports voice, video, and data, it positions Sandia National Laboratories to deploy these services to the desktop. For the majority of corporate network users at Sandia National Laboratories GPON should be a suitable replacement for the legacy network.

Distribution

1 Eric Welty (electronic copy)
Verizon Federal Network Systems, LLC

1 Christopher Wright (electronic copy)
Brocade Communications Systems, Inc.

1 Thomas Archuleta (electronic copy)
Cisco Systems, Inc.

1 Petra St.George (electronic copy)
Qwest Government Services

1	MS 0630	M. D. Gomez, 9611
1	MS 0630	A. L. Hale, 9600
1	MS 0630	B. V. Hess, 9610
1	MS 0671	T. C. Hu, 5627
1	MS 0671	L. G. Martinez, 5627
1	MS 0672	R. R. Olsberg, 5629
1	MS 0672	L. G. Pierson, 5629
1	MS 0781	B. C. Whittet, 6432
1	MS 0781	E. L. Witzke, 6432
1	MS 0781	G. A. Yonek, 6432
1	MS 0788	R. L. Adams, 9338
6	MS 0788	J. P. Brenkosh, 9338
1	MS 0788	D. R. Garcia, 9938
1	MS 0788	R. A. Mason, 9336
1	MS 0788	M. M. Miller, 9338
1	MS 0788	R. L. Moody, 9338
1	MS 0788	N. A. Marsh, 9338
1	MS 0788	D. L. Van Houten, 9335
1	MS 0788	J. M. Vaughan, 9338
1	MS 0788	V. K. Willliams, 9938
1	MS 0799	D. E. Eichert, 9338
1	MS 0799	J. G. Heller, 9317
1	MS 0799	B. A. Potts, 9317
1	MS 0799	M. S. Sherwood, 9317
1	MS 0801	T. L. Klitsner, 9340
1	MS 0801	R. W. Leland, 9300
1	MS 0806	S. A. Gossage, 9338
1	MS 0806	J. H. Maestas, 9336
1	MS 0806	J. H. Naegle, 9336
1	MS 0806	T. J. Pratt, 9336
1	MS 0806	J. A. Schutt, 9336
1	MS 0813	P. C. Jones, 9310

1	MS 0838	G. K. Rogers, 9320
1	MS 0813	R. M. Cahoon, 9311
1	MS 0813	D. G. Heckart, 9312
1	MS 0813	J. K. Perich, 9312
1	MS 0823	J. D. Zepper, 9320
1	MS 0831	M. O. Vahle, 5500
1	MS 0832	A. B. Leyba-Essary, 9335
1	MS 0832	P. L. Manke, 9335
1	MS 0832	T. Holley, 9335
1	MS 0947	S. M. Trujillo, 9347
1	MS 0947	B. R. Walker, 8947
1	MS 1072	L. G. Pierson, 5629
1	MS 1202	R. M. Jansma, 5631
1	MS 1202	B. A. Nuanes, 5096
1	MS 1202	D. A. Rieb, 5925
1	MS 1206	T. D. Tarman, 5632
1	MS 1204	P. R. Forbes, 5919
1	MS 1209	M. M. Mead, 5098
1	MS 1235	J. M. Eldridge, 5632
1	MS 9012	F. H. Blair, 8949
1	MS 9012	R. D. Gay, 8949
1	MS 9012	B. A. Maxwell, 8949
1	MS 9036	D. H. Dirks, 8947
1	MS 9151	C. T. Oien, 8940
1	MS 9916	B. Fischer, 8947
1	MS 0899	Technical Library, 9536 (electronic copy)