Seattle
Making Value for Society
122nd ASEE Annual
Conference & Exposition
June 14 - 17, 2015
Seattle, WA

Paper ID #12584

Modeling Multi-Protocol Label Switching Networks in the Laboratory

Mr. Jeffrey Erin Cole, Acute Systems, LLC

Jeffrey Cole is a Master's of Electrical Engineering Technology graduate from Southern Polytechnic State University. His research included various configurations such as basic MPLS, AToM, MPLS Layer 3 VPNs and MPLS Traffic Engineering. Other topics included network performance measurements, network time protocols and network traffic generator analysis. Undergraduate studies were completed at the University of Detroit Mercy in Computer and Information Science. He has over 9 years of experience in the Information Technology field including various healthcare providers and AT&T. Currently, he is a Senior Network Engineer within the healthcare industry in Atlanta, GA.

Dr. Walter E Thain, Southern Polytechnic College of Engr and Engr Tech

Walter E. Thain received his BS, MS, and Ph.D. degrees in Electrical Engineering from the Georgia Institute of Technology. He is an Associate Professor in Electrical and Computer Engineering Technology at Southern Polytechnic State University and teaches courses in voice and data networking, analog and RF electronics, and communications systems. Research interests include voice and data network design and management, network security, RF communication systems, RF and microwave measurements, and digital signal processing. He worked 12 years in industry, where he designed mixed analog-digital systems, including, short-pulse radars and antennas, low-noise analog circuits, RF circuits, pulse generators, frequency synthesizers, switching power supplies, and high-speed digital circuits. He is co-inventor on a patent for the design of electronic instrumentation used to steer oil wells while drilling.

Dr. Thomas Fallon, Southern Polytechnic College of Engr and Engr Tech

Thomas J. Fallon received his BS and MS degrees in Electrical Engineering from the Georgia Institute of Technology and his Ph.D. degree in Astronomy from Georgia State University. He is a Professor of Electrical and Computer Engineering Technology at Kennesaw State University and has taught and/or worked for 20 years in the field of telecommunications, has conducted several networking workshops, and is author of the book The Internet Today. His astronomy Ph.D. research at Georgia State University involved the remote operation of a telescope array via the Internet.

Modeling Multi-Protocol Label Switching Networks in the Laboratory

Introduction

Multi-Protocol Label Switching (MPLS) is a vendor and protocol agnostic forwarding mechanism used to interconnect networks. As MPLS has evolved it has replaced traditional wide area network (WAN) protocols such as Frame Relay and ATM[1]. MPLS can be used to provide Layer 3 VPNs, seamless Layer 2 interconnection, or advanced routing to optimize traffic paths. In order to understand the significance and details that make MPLS the protocol of choice for most service providers, it is best to examine it under operation.

MPLS networks can be difficult to implement in academic labs. Cost, resource availability and knowledge are obstacles that often prohibit students from building networks to research and to investigate practical network scenarios. Simulators can be used to experiment with network concepts; however, they are no substitute for working with actual equipment.

This paper discusses a small scale lab network used to investigate the key capabilities of MPLS. This same lab network can also be used to instruct fundamental computer and data communication concepts to students, while maintaining low cost, ease of configuration, and design flexibility. The network design and concepts illustrated are taken from a master's thesis research project at Southern Polytechnic State University (now part of Kennesaw State University) that investigated the performance of MPLS networks.

The telecommunication lab at Southern Polytechnic State University is comprised primarily of several Cisco-based routers (2600, 2800, and 2900 series) and switches, a reconfigurable system of cables and patch panels, and various support equipment (UPSes, console switches, etc.) with several client- and server-class workstations. The client workstations are dual-bootable with both Linux- and Windows-based operating systems. Each workstation is configured with several open-source, network-related applications for data traffic generation and analysis, network design simulation, network security exercises, network management research, etc.

Although some laboratory exercises, and research, are conducted using network simulation tools, such as IT Guru OpNET and GNS3, the majority of the lessons are performed using actual hardware-based networking devices. Newer versions of OpNET, such as Riverbed Modeler, allow for the high-level design and simulation of some state-of-the-art technologies, such as MPLS, and are under consideration for integration into the telecommunications program. However, laboratory exercises based on the aforementioned small scale MPLS network were conducted for the first time during the spring 2015 semester. Analysis of student performance and understanding of the new MPLS-based labs are discussed and will be used to modify and improve the experience for subsequent course offerings.

MPLS Concepts

Before discussing the lab environment and associated learning objectives, it is important to review some MPLS concepts. As its name implies, the primary MPLS addressing mechanism is a label. The label is a 20 bit field found in an MPLS shim header wedged between the Layer 3 and Layer 2 protocol headers. For this reason MPLS is sometimes referred to as a Layer 2.5 protocol. Similar to Internet Protocol (IP), there are other fields that identify Quality of Service parameters and lifetime of an MPLS packet.

Labels can be statically configured or distributed by label distribution protocols. The most popular label distribution protocol is named Label Distribution Protocol (LDP). The labels are distributed and used to encapsulate ingress traffic through an MPLS network. This encapsulation mechanism is referred to as pushing labels.

Labels are forwarded through an MPLS network by Label Switch Routers (LSRs) performing an exact match lookup against an MPLS Label Forwarding Information Base. Labels are switched or swapped through the MPLS network. Lastly, when traffic is approaching its destination, the MPLS label is de-encapsulated or popped as traffic egresses the MPLS network toward the final destination network. Black provides more details about the label construct and operation of label processing through an MPLS network[2].

The encapsulation of any protocol through an MPLS network is one of the key contributors to MPLS' success. MPLS can be used to interconnect multiple Layer 2 networks of similar protocol. This form of MPLS is referred to as Any Transport over MPLS (AToM). Layer 3 VPNs can virtually and logically segment traffic across a service provider network with the use of MPLS encapsulation, Virtual Routing and Forwarding, and Border Gateway Protocol (BGP). Ghein discusses the variations of MPLS and relevant configurations[3].

Another unique characteristic of MPLS is its ability to traffic engineer dynamic Label Switched Paths (LSPs) through an MPLS network. The underlying mechanism for MPLS is a link state dynamic routing protocol such as Intermediate-System-Intermediate-System (IS-IS) or Open Shortest Path First (OSPF). Previous wide area network (WAN) switching protocols, like Frame Relay and Asynchronous Transfer Mode (ATM), allow the ability to traffic engineer paths as well.

MPLS leverages the IP protocol in order to packet-switch traffic through a service provider network. Switching IP packets enables more attributes than a traditional Layer 2 mechanism such as ATM and Frame Relay. Not only does IP introduce routing attributes associated the underlying dynamic link state routing protocols, but MPLS traffic engineering utilizes Resource Reservation Protocol (RSVP). The underlying dynamic link state routing protocols combined with RSVP empowers MPLS traffic engineering to use multiple path attributes; therefore, efficiently making use of the best path. Osborne provides more explanation of MPLS traffic engineering with relevant configuration data[4].

MPLS traffic engineering, AToM, Layer 3 VPNs were configured, simulated and performance tested using the lab environment discussed in the next section. Benchmarking and testing performance testing details were based from RFCs 2544 and 5695 [5,6]. As previously mentioned, pre-requisites such as dynamic routing protocols, network analysis, and other concepts can be explored by collapsing or expanding on the lab network discussed.

Initially, a proof-of-concept network was designed and configured using Graphical Network Simulator 3 (GNS3)[7]. An interesting feature of GNS3 is its use of actual Cisco router software images, allowing most of the router commands and configurations to be implemented. Each router is executed as a virtual machine within the GNS3 environment. However, it was found that only basic MPLS connectivity could be effectively simulated. Network stress performance simulations yielded inaccurate results due to workstation memory and processor resource limitations. Nevertheless, simulators such as GNS3 and OpNET are great tools to assist in understanding basic protocol functionality when actual network hardware resources are scarce. Because of these limitations, a hardware-based experimental lab network using Cisco routers was used to explore MPLS and develop instructional lab exercises.

Lab Environment and Experimental Network Configuration

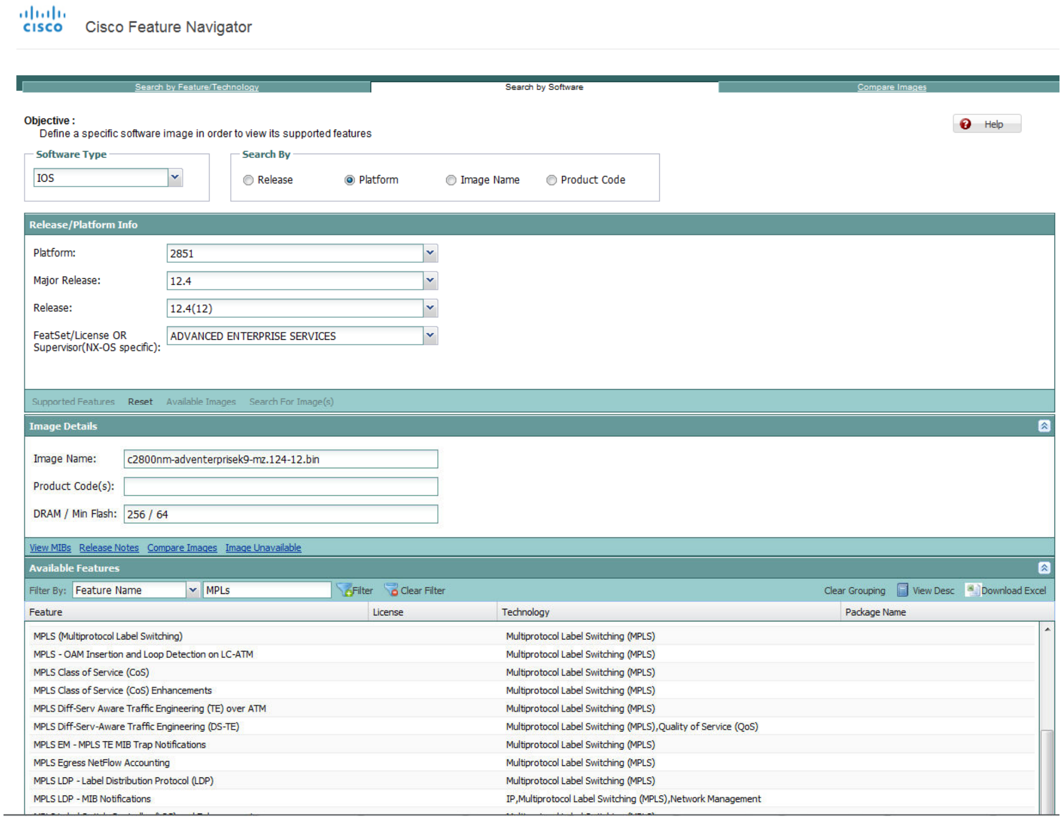
The telecommunication lab equipment consisted of various options for routing and switching. Routers included Cisco 2621s, 2621XMs, and 2851s. Switches included Cisco Catalyst 2900, 2950, 3550, and 4948 switches. Cisco products have a license structure that is based on a software feature set per Cisco hardware platform. Not all platforms support the desired features.

For example, Cisco 2621XMs supported some basic MPLS capabilities, while they did not support advanced MPLS capabilities such AToM, Layer 3 VPNs and traffic engineering. The Catalyst 3550 and 4948 Layer 3 Cisco switches support dynamic routing protocols, but not MPLS advanced features. After determining the hardware platform that can support a software feature set, other requirements such as minimum memory requirements needed to run the IO S image must be met.

Consideration of router platform and IOS is restricted to Cisco products since they are very popular and were used in the development of the methodology described in this paper. MPLS is a WAN-specific protocol and finding lower-cost routers with the capability of running it can be challenging. Cisco's integrated services or multiservice routers are designed for branch office applications and some support IOS images with MPLS capability.

Generally, MPLS first became available for certain 3600- and 2800- series branch routers starting with IOS version 12.4(1). These routers are now obsolete though the 2800 is still supported into 2016. Presently Cisco's branch router product line has moved to 3900-, and 2900-series. Determining an appropriate combination of platform and IOS feature set can be done by contacting Cisco representatives or by using the online Cisco Feature Navigator[8]. The navigator permits searching by combinations of router platform, image release, and feature. Figure 1 is a screen shot of the navigator window for a search of MPLS features for a 2851 router in IOS release 12.4(12) with the Advanced Enterprise Services feature set. Other IOS feature sets supporting MPLS can be found iteratively. IOS images are priced by feature set and MPLS features are found on the more expensive images.

One low-cost solution for building an MPLS network is to purchase older, unsupported or obsolete platforms with high-end IOS feature sets from a refurbished equipment reseller. Significant cost savings are available by doing this but the latest router performance capabilities


Cisco Feature Navigator
Search by Feature/Technology
Search by Software
Compare Images
Help

Objective :
Define a specific software image in order to view its supported features

Software Type: IOS

Search By: ○ Release ● Platform ○ Image Name ○ Product Code

Release/Platform Info

Platform: 2851

Major Release: 12.4

Release: 12.4(12)

FeatSet/License OR Supervisor(NX-OS specific): ADVANCED ENTERPRISE SERVICES

Supported Features Reset Available Images Search For Image(s)

Image Details

Image Name: c2800nm-adventerprisek9-mz.124-12.bin

Product Code(s):

DRAM / Min Flash: 256 / 64

Available Features

Filter By: Feature Name MPLs

Feature	License	Technology	Package Name
MPLS (Multiprotocol Label Switching)		Multiprotocol Label Switching (MPLS)	
MPLS - OAM Insertion and Loop Detection on LC-ATM		Multiprotocol Label Switching (MPLS)	
MPLS Class of Service (CoS)		Multiprotocol Label Switching (MPLS)	
MPLS Class of Service (CoS) Enhancements		Multiprotocol Label Switching (MPLS)	
MPLS Diff-Serv Aware Traffic Engineering (TE) over ATM		Multiprotocol Label Switching (MPLS)	
MPLS Diff-Serv-Aware Traffic Engineering (DS-TE)		Multiprotocol Label Switching (MPLS),Quality of Service (QoS)	
MPLS EM - MPLS TE MIB Trap Notifications		Multiprotocol Label Switching (MPLS)	
MPLS Egress NetFlow Accounting		Multiprotocol Label Switching (MPLS)	
MPLS LDP - Label Distribution Protocol (LDP)		Multiprotocol Label Switching (MPLS)	
MPLS LDP - MIB Notifications		IP,Multiprotocol Label Switching (MPLS),Network Management	

Figure 1. Screen shot of Cisco Feature Navigator showing MPLS features.

will be sacrificed. This can be an acceptable solution if instructing students about MPLS protocol capabilities is the main objective.

One must be careful when selecting an older platform and IOS image. Of the 3600-series platforms, the 3640 has MPLS capabilities with IOS image 12.4(1) and above. However, the 2600XM series, popular with Cisco certification instructional labs, does not support MPLS even though it can run 12.4 Advanced Enterprise images. Note that with each major release, additional commands within the MPLS features may be added or bugs with existing commands may be fixed. Key features needed to implement the MPLS networks discussed here were “MPLS (Multi-Protocol Label Switching”, “MPLS LDP - Label Distribution Protocol (LDP)”, “MPLS Traffic Engineering (TE)”, and “MPLS Virtual Private Networks (VPN)”.

The Cisco 2851 router with 12.4(20)T IOS image supported the MPLS functionality of a Provider (P) and Provider Edge (PE) router. The P routers are involved in MPLS label swapping and PE routers push and pop MPLS labels. The router wide-area network connections were implemented using serial links running High Level Data Link Control (HDLC) as shown in Figure 2. The figure indicates the link speeds and DCE (originates link synchronous clock) or DTE interface configurations.

In retrospect, only three routers are required to demonstrate basic MPLS functionality. The three routers would include one router to push labels, one router to swap and pop labels and the third router for egress from the MPLS network. Referring to MPLS examples during the exploration of MPLS and traffic engineer design planning resulted in the topology of three P and two PE routers. The combination of three P and two PE routers provides multiple Label Switched Paths (LSPs). Figure 3 demonstrates a sample of permutations for multiple LSPs distinguished by dashed and solid arrow flows, respectively.

The numbers in circles indicate flows 1 through 4 sourced from and destined to computers that have open source traffic generator software installed. The computers are labeled TG1 through TG4, which are traffic generator computers 1 through 4. The traffic generating computers are connected via Cisco 4948 Catalyst switches, which in turn connect to the Cisco 2851 PE routers, PE1 and PE2. The core of the MPLS network is composed of the three P routers that enable multiple LSPs labeled P1 through P3. More flows can be created when more routers are added to the topology. For example, flow number 4 would not exist without P2 and P3. If two PE and one P router were used, a subset of the flows shown would be available for testing and demonstrating the benefits of MPLS.

During a practical network design phase, device interface configuration is one of the many details planned. Students seldom have practical network design experience; therefore, interface configuration can easily become an afterthought during a lab or research exercise. This level of detail is often omitted in high-level simulators. By using actual hardware, students gain valuable interface configuration experience.

For example, the Cisco 2851 router serial interface Layer 2 protocol and clock rate were initially selected and configured. Because the serial links could not be tapped with equipment available in

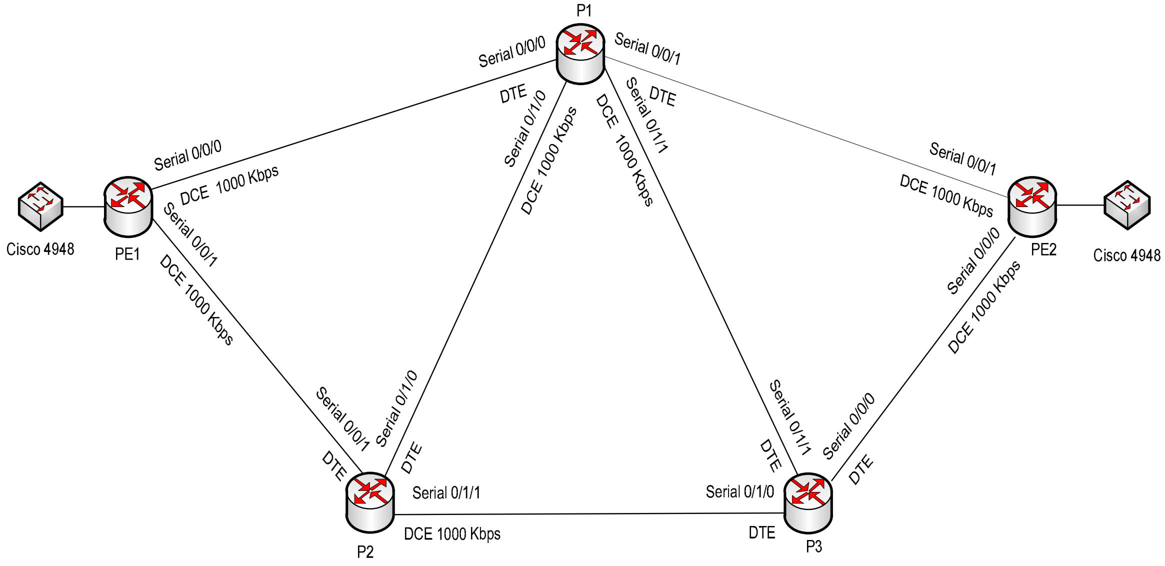


Figure 2 – Layer 2 Configuration and Topology for MPLS

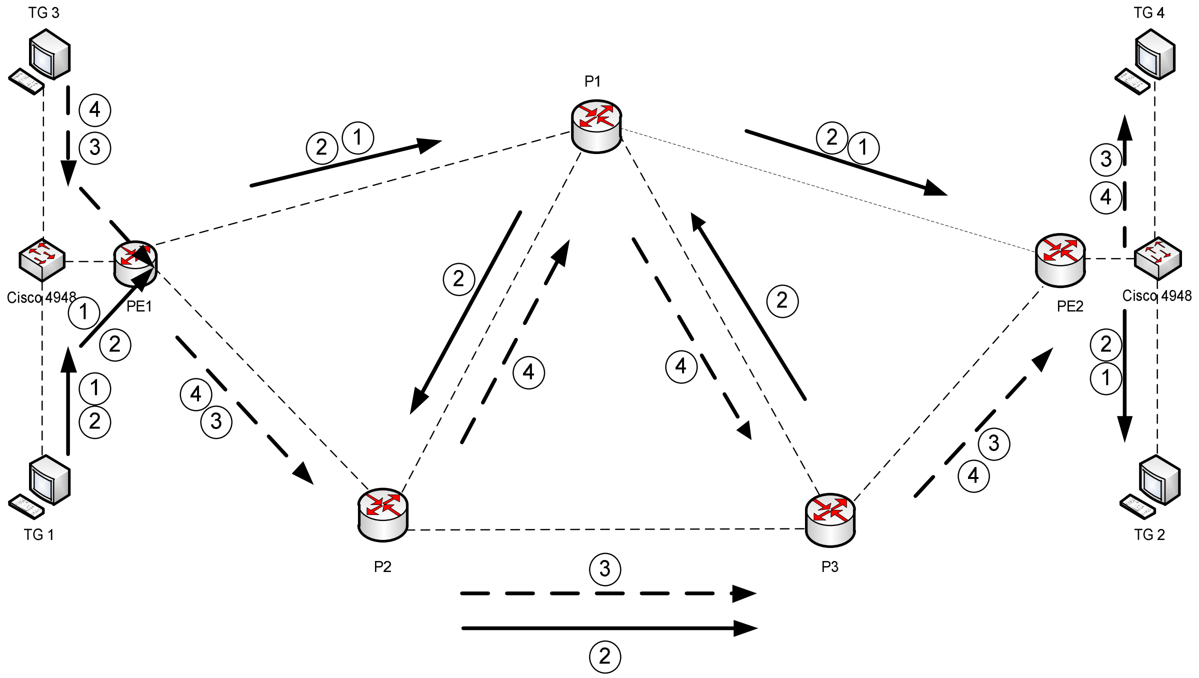


Figure 3 – MPLS provider (P) and provider edge (PE) topology with multiple LSPs

the lab, only end-to-end performance across the network could be analyzed. Therefore, MPLS protocol behavior on the links could not be observed directly. Furthermore, during performance analysis the bit-per-second overhead associated with the HDLC header had to be taken into consideration.

Cisco routers can capture and export monitored IP traffic to another collecting interface using IP Traffic Export and IP Traffic Capture. Unfortunately, these tools would only capture Layer 3, IP traffic and did not work with MPLS since it encapsulates IP headers.

To address the analysis of the MPLS protocol behavior, selected serial links were replaced by Ethernet. Routers that performed MPLS operations of pushing, swapping and popping, were connected via Cisco Ethernet switches. Two Cisco Catalyst 4948 switches were located in series with the Ethernet link between P to P and P to PE router combinations and mirrored through traffic to monitoring ports. Workstations connected to the mirrored ports analyzed packets and packet headers using Wireshark. MPLS operations of pushing, swapping and popping were readily observed. The ability to dissect MPLS packets on the Ethernet link enabled quantizing the amount of protocol-related overhead. This information was used to set up the traffic generator packet sizes when running performance tests across serial links.

In order to examine ingress and egress traffic to and from the MPLS network, Linux and Microsoft Windows workstations were attached via Ethernet directly to the PE routers. Since the emphasis of the research was focused on MPLS behavior from the wide-area network perspective, less time and research was spent on local area networks and interconnectivity to PE routers. Further investigation of customer enterprise networks acting autonomously or interconnected to the MPLS network could be performed by expanding the local area networks with other routers or Layer 3 switches.

Students may be interested in learning about enterprise network engineering and design. In this scenario, interfacing a customer network to an MPLS network will emphasize connectivity to the MPLS network rather than MPLS functionality. Less capable routers or Layer 3 switches that support basic link state or distance vector routing protocols can be used for this purpose. Key concepts such as customer network routing protocol redistribution across an MPLS network can be readily demonstrated. The ability to emphasize MPLS network concepts from the service provider or the customer perspectives are features of the chosen lab network configuration.

As previously discussed, the lab network can be expanded or contracted to meet various MPLS learning objectives. The pre-requisite for constructing an MPLS network is establishing Layer 1 through 3 network connectivity. Interfaces and cabling, Layer 2 protocols, IP and dynamic link state routing protocols have to be configured first. Therefore, the same physical network topology can be used to illustrate these concepts.

Implementing AToM involves establishing MPLS Layer 3 VPNs and using path vector based dynamic routing protocols such as external and internal Border Gateway Protocol (eBGP and iBGP, respectively). Simulation of AToM was done by connecting Ethernet networks through the MPLS network. Behavior such as end-to-end Ethernet broadcast propagation across the MPLS network can be observed. The Layer 3 VPN configuration provides the foundation for other advanced MPLS based technologies such as Virtual Private LAN Service (VPLS) and Ethernet Virtual Private Network (EVPN).

MPLS traffic engineering introduces the simultaneous use of route metrics to influence path selection through an MPLS network. Route metrics are relevant for students in understanding dynamic routing protocols since the routing protocols use them to determine optimal paths. MPLS traffic engineering advances the use of one route metric by reserving bandwidth along LSPs.

Concepts associated with LSP configuration, establishment and selection have similarities to Software Defined Networking concepts such as controller based networks. Large MPLS networks optimize network bandwidth utilization through MPLS traffic engineering LSPs. The MPLS traffic engineered LSPs can be managed dynamically by vendor proprietary controller based applications.

MPLS traffic engineering performance was observed during network congestion produced by traffic generators. MPLS traffic engineering is a congestion management technique that can provide a certain Quality of Service (QoS) without typical queuing and traditional Type of Service (ToS) techniques. The MPLS traffic engineering configuration influences traffic by using RSVP bandwidth reservations optimize underutilized paths through the MPLS network. Higher prioritized traffic can make use of higher reserved paths, while best effort traffic can traverse other paths simultaneously leveraging the same LFIB. Implementing MPLS traffic engineering can be used to show students congestion cause and effect.

For example, when congesting an MPLS Layer 3 VPN network simulated in the network lab environment, it was observed that TCP reliability would suffer when UDP traffic flooded the network. When TCP could not keep alive connection-oriented sessions, iBGP adjacencies were lost. This caused MPLS Layer 3 VPN connectivity failure and MPLS reverted to traditional link state routing across the lab environment. This type of congestion behavior can only be demonstrated on a physical network.

Traffic generators are useful tools for confirming contracted service levels in a production environment or for lab network testing and it is important for students to know how to use them. Commercial traffic generators are available but can be expensive. Open source, workstation-based generators like Iperf[9] and D-ITG[10] can be good candidates for simulating production level traffic as can real time applications such as Media Streamer. Media Streamer was used in a similar network in the telecommunications lab for testing real-time video traffic jitter performance[11].

Testing throughput, delay, jitter, and packet loss on the MPLS network lab was done using Iperf and D-ITG. Both generators use a client-server paradigm and proper operation requires efficient communication of control information between the client and server. Interesting traffic generator behavior anomalies were observed under congestion. For instance, D-ITG could not initiate traffic flow when the network was flooded with UDP traffic from Iperf due to breakdown of its TCP-based control mechanism.

Both jitter and delay are time-sensitive network performance metrics. Measuring time becomes very important, particularly with low-latency networks such as the MPLS lab network. Experimentation demonstrated the need for more accurate time references for the workstations running Iperf and D-ITG than what Network Time Protocol (NTP)[12] could provide. It was found that Precision Time Protocol (PTP)[13] provided more accurate timing results; therefore, more accurate delay and jitter measurements.

Lab Exercises

Research conducted with the lab network showed that several lab exercises could be developed to illustrate numerous learning objectives. Implementing a basic MPLS configuration is a good starting point. Students can dive deeper into common problems faced by service providers in order to provide transport solutions between companies spread across non-contiguous geographical areas leveraging Ethernet over MPLS. Multiplexing multiple unique customers, while preserving isolated integrity of data over one physical medium via MPLS Layer 3 VPNs provide another tool for service provider scenarios. Traffic engineering and maintaining service level agreements (SLAs) are what preserve the service provider’s financial investment and promises to their customers.

Students can take the enterprise networking approach by observing requirements for a local area network to interconnect to a service provider’s MPLS network. Expanding the network with less expensive routers or switches can provide a different perspective on what network engineers plan and design when connecting to a service provider network.

Prior to working with MPLS, students should already have experience with basic router configuration, including cabling the network, configuring IP on Ethernet (LAN-to-router) and serial (router-to-router) interfaces, setting up simple routing protocols such as RIP, analyzing routing tables, and establishing access lists. Table 1 summarizes concepts that can be explored with MPLS-focused lab exercises.

Table 1 – Lab Exercise Concepts

Lab Exercise	Concepts
Configuring a basic MPLS network	Physical layer cabling Layer 2 protocols (Ethernet, HDLC) Layer 3 (IP) protocols, subnetting strategies Dynamic Route protocols (OSPF, IS-IS, BGP) MPLS label pushing, swapping and popping
Demonstrating connectivity Ethernet networks using Ethernet over MPLS (EoMPLS)	Basic MPLS concepts Layer 2 VPNs Virtual Channel IDs
Using VRFs to virtually segment networks with MPLS Layer 3 VPNs	Basic MPLS concepts VRFs Layer 3 VPNs iBGP, eBGP Route targets/BGP communities Network segmentation
Deploying MPLS in a corporate enterprise network	Basic MPLS concepts Network route redistribution
Optimizing network performance in a WAN with MPLS traffic engineering	Basic MPLS concepts Layer 2 or 3 MPLS VPNs Advanced routing, RSVP
Traffic generation and analysis	Protocol analysis Traffic management Congestion and congestion management Test methodologies Open source tools, D-ITG, Iperf
Measure Network Performance Metrics	Measurement strategies Accuracy, precision Network timing protocols (NTP, PTP)

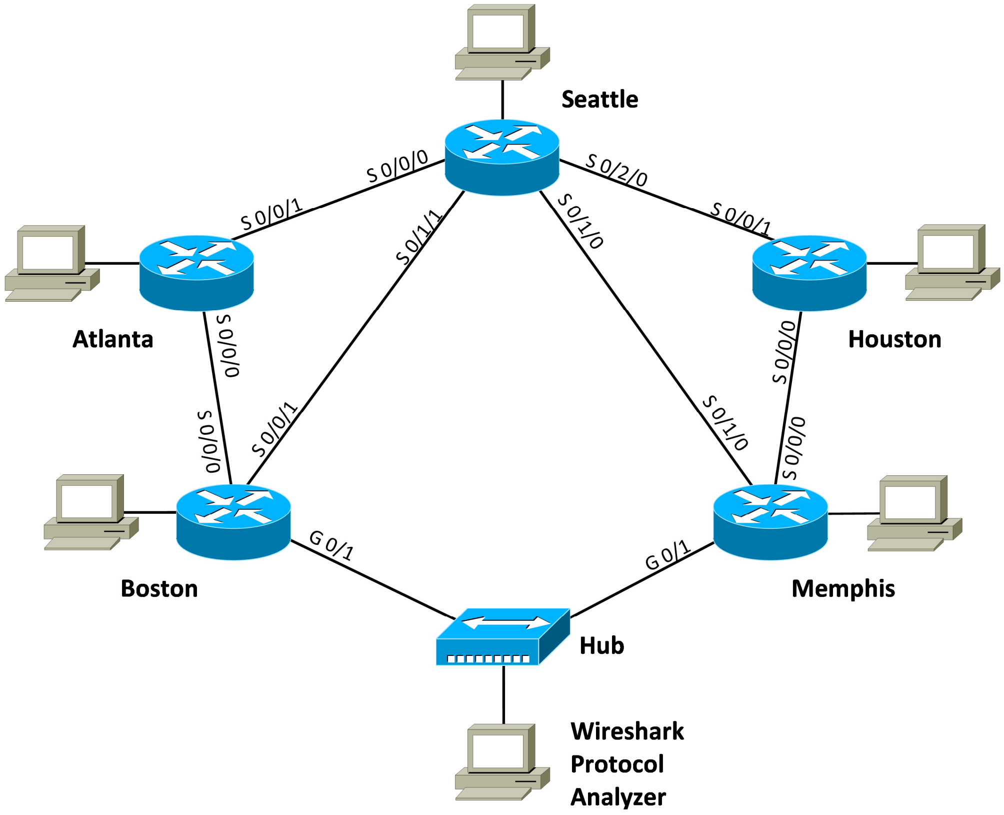


Figure 4 – Lab exercise MPLS network topology

Two lab exercises were designed and tested with students in the Advanced Telecommunications course during the spring 2015 semester. The first concentrated on basic MPLS connectivity principles and the second demonstrated Ethernet over MPLS. The network topology of Figure 2 was used for both lab exercises with one important modification. One serial link between two routers was replaced with an Ethernet link by connecting one Ethernet interface of each router to a 10 Mbps hub. A workstation running Wireshark was also connected to the hub so frames with MPLS encapsulation could be observed. The resulting topology is shown in Figure 4. Students were assigned to configure one or more routers and ensure physical-layer cabling was correct. A basic configuration was installed on the routers so students could telnet from their router's configuration workstation into the router and complete the configuration tasks.

For the Basic MPLS lab exercise, Table 2 lists student tasks, the observations they were expected to perform and questions asked. Students set up OSPF on the routers, experimented with OSPF metrics, configured MPLS and tested network connectivity by using ping and observing traffic on the Wireshark workstation. An example MPLS forwarding table is shown in Figure 5. It was observed that students' comprehension of Dijkstra's algorithm, OSPF's method of determining the shortest path, was enhanced when they had to determine how to shift the traffic path from one route to another by adjusting link metrics.

The Basic MPLS lab exercise was expanded in the Ethernet Over MPLS exercise. The same network topology was used and essentially the same steps were followed as in the Basic MPLS lab exercise up through the initial MPLS configuration, student task 8 of Table 2. While reinforcing concepts from the first exercise, these steps could be omitted if the previous network configuration was left intact. Table 3 shows the student tasks, observations and questions associated with this lab exercise.

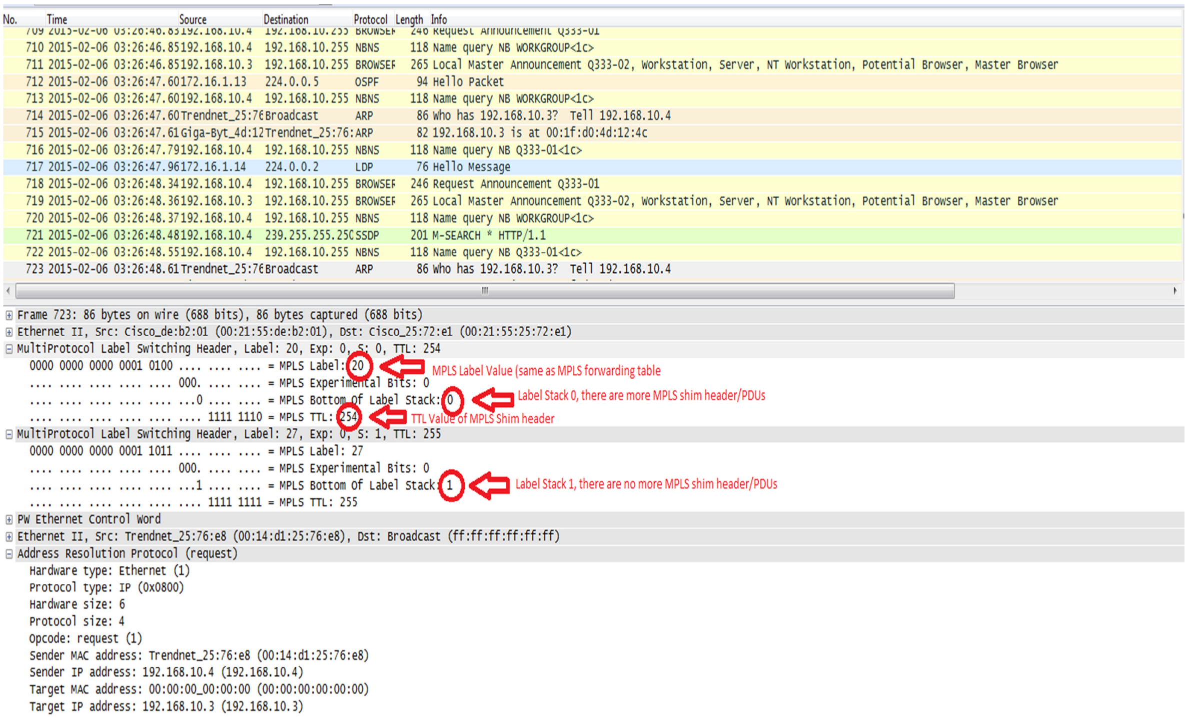
Table 2 – Basic MPLS Lab Exercise Summary

Student Tasks	Observations and Questions Addressed by Students
1. Set up configuration workstation IPv4 network address, subnet mask, and default gateway to match Ethernet interface of the router 2. Configure router serial interfaces for HDLC layer-2 protocol and IPv4 addresses and subnet masks 3. Configure OSPF on router 4. Verify routing table on each router to ensure reachability to all IP networks in the topology. Test with Pings from workstations. 5. Set up Wireshark workstation to observe traffic between Boston and Memphis 6. Manipulate router OSPF link metrics to divert traffic from Atlanta-Seattle-Houston path to Atlanta-Boston-Memphis-Houston path. Verify with pings from Atlanta to Houston workstations and Wireshark captures 7. Configure MPLS on all router serial interfaces and the two Ethernet interfaces that connect Boston and Memphis 8. Verify MPLS forwarding table on each router. Look for local label, remote label, pop label, and no label 9. Ping from Atlanta to Houston and in reverse direction; observe Wireshark capture	1. How are you sure that OSPF has converged to final topology? 2. How did you know OSPF link metric changes resulted in rerouting traffic through the network? 3. How did Wireshark Ping captures change after MPLS was started? 4. From captured MPLS traffic: Did labels change when pinging from Atlanta to Houston and then from Houston to Atlanta? Why or why not? What fields are in the MPLS protocol data unit? What MPLS time-to-live values are observed and why these values? What label stack values are observed? 5. Research questions: What types of networks can connect to an MPLS network? What features or limitations do you see with basic MPLS? How does MPLS differ from ATM or Frame Relay?

```
P3_Seattle#show mpls forwarding-table
Local   Outgoing    Prefix             Bytes tag  Outgoing    Next Hop
tag     tag or VC   or Tunnel Id       switched   interface
 16      Pop tag     172.16.1.4/30      0          Se0/1/0     point2point
 17      18          172.16.1.0/30      0          Se0/1/0     point2point
 18      Pop tag     172.16.2.0/30      0          Se0/1/0     point2point
 19      Pop tag     172.16.3.0/30      530        Se0/0/0     point2point
 20      20          192.168.0.8/29     0          Se0/1/0     point2point
 21      21          192.168.0.4/30     0          Se0/1/0     point2point
 22      23          192.168.2.8/29     0          Se0/0/0     point2point
 23      Pop tag     192.168.2.4/30     212        Se0/0/0     point2point
```

Figure 5 – Example MPLS forwarding table

Students examined the Label Information Base (LIB) and Label Forwarding Information Base (LFIB) on the various routers and predicted label use along a given path. They also examined the different router forwarding tables to see how labels were manipulated along a path. Virtual circuit tunnels were configured across the network to support EoMPLS (a version of AToM) and Wireshark was used to observe the resulting label stacking. Figure 6 is an annotated example of a captured Address Resolution Protocol (ARP) broadcast packet sent by host 192.168.10.4. This packet is the last one in the list. It illustrates the placement of the MPLS shim header, the fields within the protocol data unit, the operation of MPLS Time to Live (TTL), and the feature of MPLS label stacking, or encapsulation.



```
No.   Time                   Source          Destination     Protocol Length Info
  709 2015-02-06 03:26:46.83192.168.10.4    192.168.10.255  BROWSEF  246 Request Announcement Q333-01
  710 2015-02-06 03:26:46.85192.168.10.4    192.168.10.255  NBNS     118 Name query NB WORKGROUP<1c>
  711 2015-02-06 03:26:46.85192.168.10.3    192.168.10.255  BROWSEF  265 Local Master Announcement Q333-02, Workstation, Server, NT Workstation, Potential Browser, Master Browser
  712 2015-02-06 03:26:47.60172.16.1.13     224.0.0.5       OSPF      94 Hello Packet
  713 2015-02-06 03:26:47.60192.168.10.4    192.168.10.255  NBNS     118 Name query NB WORKGROUP<1c>
  714 2015-02-06 03:26:47.60Trendnet_25:76Broadcast         ARP       86 Who has 192.168.10.3?  Tell 192.168.10.4
  715 2015-02-06 03:26:47.61Giga-Byt_4d:12Trendnet_25:76:   ARP       82 192.168.10.3 is at 00:1f:d0:4d:12:4c
  716 2015-02-06 03:26:47.79192.168.10.4    192.168.10.255  NBNS     118 Name query NB Q333-01<1c>
  717 2015-02-06 03:26:47.96172.16.1.14     224.0.0.2       LDP       76 Hello Message
  718 2015-02-06 03:26:48.34192.168.10.4    192.168.10.255  BROWSEF  246 Request Announcement Q333-01
  719 2015-02-06 03:26:48.36192.168.10.3    192.168.10.255  BROWSEF  265 Local Master Announcement Q333-02, Workstation, Server, NT Workstation, Potential Browser, Master Browser
  720 2015-02-06 03:26:48.37192.168.10.4    192.168.10.255  NBNS     118 Name query NB WORKGROUP<1c>
  721 2015-02-06 03:26:48.48192.168.10.4    239.255.255.25C SSDP     201 M-SEARCH * HTTP/1.1
  722 2015-02-06 03:26:48.55192.168.10.4    192.168.10.255  NBNS     118 Name query NB Q333-01<1c>
  723 2015-02-06 03:26:48.61Trendnet_25:76Broadcast         ARP       86 Who has 192.168.10.3?  Tell 192.168.10.4

⊞ Frame 723: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
⊞ Ethernet II, Src: Cisco_de:b2:01 (00:21:55:de:b2:01), Dst: Cisco_25:72:e1 (00:21:55:25:72:e1)
⊟ MultiProtocol Label Switching Header, Label: 20, Exp: 0, S: 0, TTL: 254
    0000 0000 0000 0001 0100 .... .... .... = MPLS Label: 20
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...0 .... .... = MPLS Bottom Of Label Stack: 0
    .... .... .... .... .... .... 1111 1110 = MPLS TTL: 254
⊟ MultiProtocol Label Switching Header, Label: 27, Exp: 0, S: 1, TTL: 255
    0000 0000 0000 0001 1011 .... .... .... = MPLS Label: 27
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 1111 1111 = MPLS TTL: 255
⊞ PW Ethernet Control Word
⊞ Ethernet II, Src: Trendnet_25:76:e8 (00:14:d1:25:76:e8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Trendnet_25:76:e8 (00:14:d1:25:76:e8)
    Sender IP address: 192.168.10.4 (192.168.10.4)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.10.3 (192.168.10.3)
```

MPLS Label Value (same as MPLS forwarding table

Label Stack 0, there are more MPLS shim header/PDUs

TTL Value of MPLS Shim header

Label Stack 1, there are no more MPLS shim header/PDUs

Figure 6 - Captured ARP packet with stacked MPLS labels of EoMPLS

Table 3 – Ethernet Over MPLS Lab Exercise Summary

Student Tasks	Observations and Questions Addressed by Students
1. through 8. Same as Basic MPLS lab. 9. Observe LIB and LFIB on the different routers (basic MPLS configuration) 10. Configure virtual circuit ID numbers for MPLS network interfaces and set up tunnels across the network 11. Verify EoMPLS connectivity using forwarding table 12. Use Wireshark to verify EoMPLS label use on the Boston to Memphis segment	1. From the LIB and LFIB information, determine how forwarding labels are chosen predict label numbers used by the different routers 2. Determine which labels are pushed, swapped or popped on each router 3. How does label stacking differ between basic MPLS and EoMPLS? 4. How does PDU overhead vary between MPLS and EoMPLS?

Observations on Student Learning

Written lab reports were collected and reviewed to determine student comprehension of learning objectives. Students were asked to explain their level of understanding and answer various questions after performing the MPLS lab exercises. Overall students understood basic MPLS functionality and protocol data unit structure.

The correlation of the Wireshark packet capture and analysis to the MPLS LFIB table provided students the reinforcement of MPLS label distribution and operation. Viewing MPLS's capability to stack labels demonstrated one of the advantages of MPLS over legacy WAN protocols such as Frame Relay and ATM.

EoMPLS provided some challenges for student's understanding of bridging Layer 2 networks over MPLS. Initially, students did not recognize the significance of ARP broadcasts across a service provider's network, until students had a better understanding of ARP and its operation within a network. After further explanation of ARP and the distinct capabilities that EoMPLS could provide compared to basic MPLS and Layer 3 VPNs, students began to wonder where EoMPLS would be practically implemented. Providing relevant examples such as seamlessly bridging data centers without imposing Layer 3 boundaries gave students an idea of practical situations where EoMPLS would be applicable. Another application example is using VPNs to logically segment customer traffic.

Another topic that challenged students was the idea of generalizing ingress and egress traffic for MPLS as Forwarding Equivalent Classes (FECs). During basic MPLS overview and investigation, students quickly assumed that IP networks were the predominant application of ingress and egress traffic in and out of MPLS. Once AToM was covered, students developed a clear understanding that FECs were used to categorize the types of traffic traversing an MPLS network. EoMPLS as a subset of AToM in lab exercises and instruction provided a hands on experience for students understanding. After EoMPLS lab exercises, ATM, Frame Relay, HDLC and other Data Link Layer protocols were reiterated as potential FECs for AToM.

Quiz results demonstrated that students were able to answer questions that related to multiple aspects of MPLS. One of the questions involved an understanding of a TCP 3-way handshake and proper protocol data unit placement of MPLS shim headers. The question not only tested the student's understanding of TCP and MPLS, but emphasized what students had demonstrated in lab exercises. Other questions involved label distribution methods, MPLS operation and analyzing MPLS forwarding tables. Student performance on the quiz proved that MPLS was thoroughly investigated and demonstrated between instruction and hands on exercises.

Conclusion

Ultimately, academic curricula are designed to teach students about real-world applications, problems and solutions and prepare them for future employment. MPLS is a popular WAN protocol that should be included in a telecommunications or information technology curriculum. It was found that lab experiences significantly improved student comprehension of MPLS concepts.

Various learning objectives can be met since MPLS encompasses many LAN and WAN concepts. The lab network discussed here can be tailored to meet a wide range of learning objectives. MPLS lab exercises can be modularized to focus on desired objectives ranging from basic connectivity to advanced concepts such as EoMPLS and traffic engineering. The Basic MPLS lab exercise reinforced routing and subnetting concepts in addition to introducing students to MPLS functionality.

Using software based simulation tools is a great way to teach students about network concepts when hardware is not available, but simulators may not accurately reproduce real-world behavior. However, more details have to be considered when building an experimental hardware lab. Giving students a holistic view of factors that impact network design and performance can justify the cost of a hardware lab.

References

1. T. Green, (2007, Oct. 26). *Frame relay vs. ATM* [Online]. Available: http://www.networkworld.com/article/2287582/lan-wan/frame-relay-vs--atm.html
2. U. Black, *MPLS and Label Switching Networks*, Upper Saddle River, NJ, Prentice Hall PTR, 2002.
3. L.D. Ghein, *MPLS Fundamentals*, Indianapolis, IN, Cisco Press, 2007.
4. E. Osborne and A. Simha, *Traffic Engineering with MPLS*, Indianapolis, IN, Cisco Press, 2003.
5. S. Bradner and J. McQuaid. (1999, Mar.). *Benchmarking Methodology for Network Interconnect Devices* (IETF RFC 2544) [Online]. Available: http://www.ietf.org/rfc/rfc2544.txt
6. A. Akhter, R. Asati, and C. Pignataro. (2009, Nov.) *MPLS Forwarding Benchmarking Methodology for IP Flows* (IETF RFC 5695) [Online]. Available: http://tools.ietf.org/html/rfc5695
7. T. Li and W. Thain, "On the Use of Virtualization for Router Network Simulation," *2010 ASEE Annual Conf. and Exposition*, Louisville, KY, 2010.

8. Cisco Systems, Inc. (2015, Jan.). *Cisco Feature Navigator* [Online]. Available: http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp
9. Sourceforge.net. (2015, Jan.). *Iperf* [Online]. Available http://sourceforge.net/projects/iperf/
10. A. Bott et.al., "A tool for the generation of realistic network workload for emerging networking scenarios," *Computer Networks (Elsevier),* vol. 56, no. 15, pp 3531-3547, 2012.
11. D. Darko-Mensah, "*Performance analysis of IPv4-TO-IPv6 transition mechanisms in a content delivery network*," M.S. thesis, ECET Dept. Southern Polytechnic State Univ. Marietta, GA, 2011.
12. Meinberg Radio Clocks, (2015, Jan.). *Network Time Protocol (NTP)* [Online]. Available: https://www.meinbergglobal.com/english/info/ntp.htm
13. K. Correll et al. "Design considerations for software only implementations of the IEEE 1588 precision time protocol," *Conf. on IEEE 1588*, 2005.