RESEARCH ARTICLE OPEN ACCESS

MPLS layer2 VPN any carrying over MPLS (AIOM) Ethernet to PPP

Karthikeyan P M.C.A., M.Phil., (Ph.D)[1], Iswarya.S [2]

1(Assistant Professor, Department of Computer Science, Ponnaiyah Ramajayam Institute Of Science And Technology Prist University, And Thanjavur)

2 (M.C.A., Scholar Department Of Computer Science, Ponnaiyah Ramajayam Institute Of Science And Technology Prist University, And Thanjavur)

Abstract:

Multiprotocol Label Switching (MPLS) has evolved from being a catchphrase in the networking industry to a widely deployed technology in service provider (SP) networks. MPLS is a contemporary solution to address a multitude of troubles faced by present- day networks: speed, scalability, quality of service (QoS) supervision, and traffic engineering. Service providers are realizing larger revenues by the implementation of service models based on the flexibility and value added services provided by MPLS solutions. MPLS also provides an elegant solution to satisfy the bandwidth management and service requirements for next-generation IP–based backbone networks.

Keywords — **Multiprotocol Label Switching (MPLS), keywords service provider (SP), IP.**

I. INTRODUCTION

Over the last few years, the Internet has evolved into a ubiquitous network and inspired the development of a variety of new applications in business and consumer markets. These new applications have driven the demand for increased and guaranteed bandwidth requirements in the backbone of the network. In addition to the traditional data services currently provided over the Internet, new voice and multimedia services are being developed and deployed. The Internet has emerged as the network for providing these converged services. However, the demands placed on the network by these new applications and services, in terms of speed and bandwidth, have strained the resources of the existing Internet infrastructure. This transformation of the network toward a packet-and cell-based infrastructure has introduced uncertainty into what has traditionally been a fairly deterministic network.

In addition to the issue of resource constraints, another challenge relates to the transport of bits and bytes over the backbone to provide differentiated classes of service to users. The exponential growth in the number of users and the volume of traffic add another dimension to this problem. Class of service (CoS) and QoS issues must be addressed to in order to support the diverse requirements of the wide range of network users.

In sum, despite some initial challenges, MPLS will play an important role in the routing, switching, and forwarding of packets through the next-generation network in order to meet the service demands of the network users.

II. TRADITIONAL ROUTING AND PACKET SWITCHING

The initial deployment of the Internet addressed the requirements of data transfer over the network. This network catered to simple applications such as file transfer and remote login. To carry out these requirements, a simple software-based router platform, with network interfaces to support the existing T1/E1 – or T3/E3 – based backbones, was sufficient. As the demand for higher speed and the ability to support higher-bandwidth transmission rates emerged, devices with capabilities to switch at the Level-2 (data link) and the Level-3 (network layer) in hardware had to be

deployed. Layer-2 switching devices addressed the switching bottlenecks within the subnets of a local-area network (LAN) environment. Layer-3 switching devices helped alleviate the bottleneck in Layer-3 routing by moving the route lookup for Lyer-3 forwarding to high-speed switching hardware.

These early solutions addressed the need for wire-speed transfer of packets as they traversed the network, but they did not address the service requirements of the information contained in the packets. Also, most of the routing protocols deployed today are based on algorithms designed to obtain the shortest path in the network for packet traversal and do not take into account additional metrics (such as delay, jitter, and traffic congestion), which can further diminish network performance. Traffic engineering is a challenge for network managers.

III. UNI CAST IP FORWARDING IN TRADITIONAL IP NETWORKS:

In traditional IP networks, routing protocols are used to distribute Layer 3 routing information. depicts a traditional IP network where network layer reach ability information (NLRI) for network 172.16.10.0/24 is propagated using an IP routing protocol. Regardless of the routing protocol, packet forwarding is based on the destination address alone. Therefore, when a packet is received by the router, it determines the next-hop address using the packet's destination IP address along with the information from its own forwarding/routing table. This process of determining the next hop is repeated at each hop (router) from the source to the destination.

- R4 receives a data packet destined for 172.16.10.0 network.
- R4 performs route lookup for 172.16.10.0 network in the forwarding table, and the packet is forwarded to the next-hop Router R3.
- R3 receives the data packet with destination 172.16.10.0, performs a route lookup for 172.16.10.0 network, and forwards the packet to next-hop Router R2.
- R2 receives the data packet with destination 172.16.10.0, performs a route lookup for 172.16.10.0 network, and forwards the packet to next-hop Router R1.

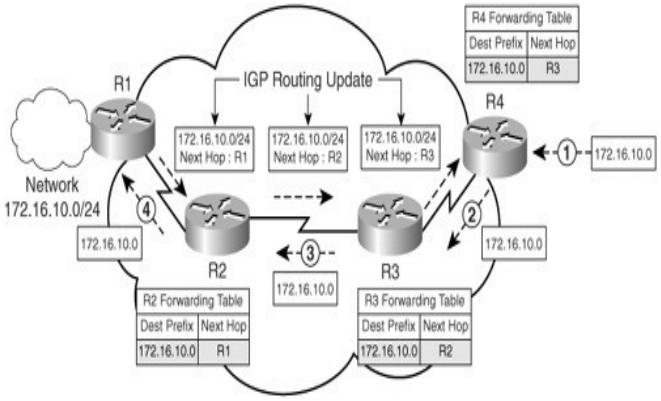

Fig.1. IP Forwarding in network

Because R1 is directly connected to network 172.16.10.0, the router forwards the packet on to the appropriate connected interface. MPLS forwarding where route table lookups are performed only by MPLS edge border routers, R1 and R4. The routers in MPLS network R1, R2, and R3 propagate updates for 172.16.10.0/24 network via an IGP routing protocol just like in traditional IP networks, assuming no filters or summarizations are not configured.

IV.MPLS ANDITCOMPONENTS MPLS:

MPLS is an Internet Engineering Task Force (IETF) – specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

A. *MPLS performs the following functions:*

- Specifies mechanisms to manage traffic flow of various granularities, such as flows between different hardware, machines, or even flows between different applications.
- Remains independent of the Layar-2 layer-3 protocols.

- Provides a means to map IP addresses to simple, fixed-length labels used by different packet-forwarding and packet-switching technologies.
- Interfaces to existing routing protocols such as resource reservation protocol (RSVP) and open shortest path first (OSPF).
- Supports the IP, ATM, and frame- relay Layer-2 protocols.

In MPLS, data transmission occurs on label-switched paths (LSPs), LSPs are a sequence of labels at each and every node along the path from the source to the destination. LSPs are established either prior to data transmission (control-driven) or upon detection of a certain flow of data (data-driven).

. The labels, which are underlying protocol-specific identifiers, are distributed using label distribution protocol (LDP) or RSVP or piggybacked on routing protocols like border gateway protocol (BGP) and OSPF. Each data packet encapsulates and carries the labels during their journey from source to destination. High-speed switching of data is possible because the fixed-length labels are inserted at the very beginning of the packet or cell and can be used by hardware to switch packets quickly between links.

V. LSRs AND LERs

The devices that participate in the MPLS protocol mechanisms can be classified into label edge routers (LERs) and label switching routers (LSRs).

An LSR is a high-speed router device in the core of an MPLS network that participates in the establishment of LSPs using the appropriate label signaling protocol and high-speed switching of the data traffic based on the established paths.
An LER is a device that operates at the edge of the access network and MPLS network. LERs support multiple ports connected to dissimilar networks (such as frame relay, ATM, and Ethernet) and forwards this traffic on to MPLS network after establishing LSPs, using the label signaling protocol at the ingress and distributing the traffic back to the access networks at the egress. The LER plays a very important role in assignment and removal of labels, as traffic enters or exits an MPLS network.

B. FEC:

The forward equivalence class (FEC) is a representation of a group of packets that share the same requirements for their transport. All packets in such a group are provided the same treatment en route to the destination. As opposed to conventional IP forwarding, in MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network. FECs are based on service requirements for a given set of packets or simply for an address prefix. Each LSR builds a table to specify how a packet must be forwarded. This table, called a label information base (LIB), is comprised of FEC–to–label bindings.

VI. LABELS AND LABEL BINDINGS:

A label, in its simplest form, identifies the path a packet should traverse. A label is carried or encapsulated in a Layer-2 header along with the packet. The receiving router examines the packet for its label content to determine the next hop. Once a packet has been labelled, the rest of the journey of the packet through the backbone is based on label switching. The label values are of local significance only, meaning that they pertain only to hops between LSRs.

Once a packet has been classified as a new or existing FEC, a label is assigned to the packet. The label values are derived from the underlying data link layer. For data link layers (such as frame relay or ATM). Layer-2 identifiers, such as data link connection identifiers (DLCIs) in the case of frame-relay networks or virtual path identifiers (VPIs)/virtual channel identifiers (VCIs) in case of

ATM networks, can be used directly as labels. The packets are then forwarded based on their label value.

Labels are bound to an FEC as a result of some event or policy that indicates a need for such binding. These events can be either data-driven bindings or control-driven bindings. The latter is preferable because of its advanced scaling properties that can be used in MPLS.

Label assignment decisions may be based on forwarding criteria such as the following:

- destination Unicast
- routing traffic engineering
- Multicast
- virtual private network (VPN)
- QoS

The generic label format.. The label can be embedded in header of the data link layer (the ATM VCI/VPI and the frame –relay DLCI or in the shim (between the Layer-2 data- link header and Layer-3 network layer header.

VII. CONFIGURING OAM CELL EMULATION FOR ATM AAL5 OVER MPLS:

If a PE router does not support the transport of Operation, Administration, and Maintenance (OAM) cells across a label switched path (LSP), you can use OAM cell emulation to locally terminate or loop back the OAM cells. You configure OAM cell emulation on both PE routers, which emulates a VC by forming two unidirectional LSPs. You use the oam-ac emulation-enableand oam-pvc managecommands on both PE routers to enable OAM cell emulation.

After you enable OAM cell emulation on a router, you can configure and manage the ATM VC in the same manner as you would a terminated VC. A VC that has been configured with OAM cell emulation can send loopback cells at configured intervals toward the local CE router. The endpoint can be either of the following:

- End-to-end loopback, which sends OAM cells to the local CE router.
- Segment loopback, which responds to OAM cells to a device along the path between the PE and CE routers.

The OAM cells include the following cells:

- Alarm indication signal (AIS)
- Remote defect indication (RDI)

These cells identify and report defects along a VC. When a physical link or interface failure occurs, intermediate nodes insert OAM AIS cells into all the downstream devices affected by the failure. When a router receives an AIS cell, it marks the ATM VC down and sends an RDI cell to let the remote end know about the failure.

VIII. CONFIGURING ATM CELL RELAY OVER MPLS IN PVP MODE:

VP mode allows cells coming into a predefined PVP on the ATM interface to be transported over the MPLS backbone to a predefined PVP on the egress ATM interface. You can use VP mode to send single cells or packed cells over the MPLS backbone.

To configure VP mode, you must specify the following:

- The VP for transporting cell relay cells.
- The IP address of the peer PE router and the VC ID.

When configuring ATM cell relay over MPLS in VP mode, use the following guidelines:

- You do not need to enter the **encapsulation aal0** command in VP mode.
- One ATM interface can accommodate multiple types of ATM connections. VP cell relay, VC cell relay, and ATM AAL5 over MPLS can coexist on one ATM interface. On the Cisco 12000 series router, this is true only on the engine 0 ATM line cards.

- If a VPI is configured for VP cell relay, you cannot configure a PVC using the same VPI.
- VP trunking (mapping multiple VPs to one emulated VC label) is not supported. Each VP is mapped to one emulated VC.
- Each VP is associated with one unique emulated VC ID. The AToM emulated VC type is ATM VP cell transport.
- The AToM control word is supported. However, if a peer PE does not support the control word, it is disabled. This negotiation is done by LDP label binding.
- VP mode (and VC mode) drop idle cells.

C. Configuring ATM Cell Relay over MPLS in Port Mode:

- Port mode cell relay allows cells coming into an ATM interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress ATM interface.
- To configure port mode, issue the **xconnect** command from an ATM main interface and specify the destination address and the VC ID. The syntax of the **xconnect** command is the same as for all other transport types. Each ATM port is associated with one unique pseudowire VC label.

  When configuring ATM cell relay over MPLS in port mode, use the following guidelines:

- The pseudowire VC type is set to ATM transparent cell transport (AAL0).
- The AToM control word is supported. However, if the peer PE does not support a control word, the control word is disabled. This negotiation is done by LDP label binding.

The AToM control word is not supported for port mode cell relay on Cisco 7600 series routers.

- Port mode and VP and VC mode are mutually exclusive. If you enable an ATM main interface for cell relay, you cannot enter any PVP or PVC commands.
- If the pseudowire VC label is withdrawn due to an MPLS core network failure, the PE router sends a line AIS to the CE router.
- For the Cisco 7600 series routers, you must specify the interface ATM slot, bay, and port for the SIP400 or SIP200.

IX. UNDERSTANDING ATOM OPERATIONS

AToM achieves a high degree of scalability by using the MPLS encoding method. You also read an overview of LDP in the previous section. Reading through this section, you will develop a further understanding of how MPLS encapsulation, LDP sig-naling, and pseudowire emulation work together.

The primary tasks of AToM include establishing pseudowires between provider edge (PE) routers and carrying Layer 2 packets over these pseudowires. The next sections cover the operations of AToM from the perspectives of both the control plane and the data plane as follows:

- Pseudowire label binding
- Establishing AToMpseudowires
- Control word negotiation
- Using sequence numbers
- Pseudowire encapsulation

X. Pseudowire Label Binding:

An AToMpseudowire essentially consists of two unidirectional LSPs. Each is represented by a pseudowire label, also known as a VC label. The pseudowire label is part of the label stack encoding that encapsulates Layer 2 packets going over

AToMpseudowires. Refer to Chapter 3 for an overview of an AToM packet.

The label distribution procedures that are defined in LDP specifications distribute and manage the pseudowire labels. To associate a pseudowire label with a particular Layer 2 connection, you need a way to represent such a Layer 2 connection. The baseline LDP specification only defines Layer 3 FECs. Therefore, the pseudowire emulation over MPLS application defines a new LDP extension—the Pseudowire ID FEC element—that contains a pseudowire identifier shared by the pseudowire endpoints. Figure 6-8 depicts the Pseudowire ID FEC element en-coding.

Fig.2. Pseudowire ID FEC Element.

The Pseudowire ID FEC element has the following components:

- **Pseudowire ID FEC**—The first octet has a value of 128 that identifies it as a Pseudowire ID FEC element.

- **Control Word Bit (C-Bit)**—The C-bit indicates whether the advertising PE expects the control word to be present for pseudowire packets. A control word is an optional 4-byte field located between the MPLS label stack and the Layer 2 payload in the pseudowire packet. The control word carries generic and Layer 2 payload-specific information. If the C-bit is set to 1, the advertising PE expects the control word to be present in every pseudowire packet on the pseudowire that is being signaled. If the C-bit is set to 0, no control word is expected to be present.
- **Pseudowire Type**—PW Type is a 15-bit field that represents the type of pseudowire. Examples of pseudowire .
- **Pseudowire Information Length**—Pseudowire Information Length is the length of the Pseudowire ID field and the interface parameters in octets. When the length is set to 0, this FEC element stands for all pseudowires using the specified Group ID. The Pseudowire ID and Interface Parameters fields are not present.
- **Group ID**—The Group ID field is a 32-bit arbitrary value that is assigned to a group of pseudowires.

- **Pseudowire ID**—ThePseudowire ID, also known as VC ID, is a non-zero, 32-bit identifier that distinguishes one pseudowire from another. To connect two attachment circuits through a pseudowire, you need to associate each one with the same Pseudowire ID.

- **Interface Parameters**—The variable-length Interface Parameters field provides attachment circuit-specific information, such as interface MTU, maximum number of concatenated ATM cells, interface description, and so on. Each interface parameter uses a generic TLV encoding.

Pseudo wire Type	**Description**
0x0001	Frame Relay data-link connection identifier (DLCI)
0x0002	ATM AAL5 service data unit (SDU) virtual channel connection (VCC)
0x0003	ATM Transparent Cell
0x0004	Ethernet VLAN
0x0005	Ethernet
0x0006	High-Level Data Link Control (HDLC)
0x0007	PPP

Table1. **Pseudowire Type description**

XI. Establishing AToMPseudowires:

Typically, two types of LDP sessions are involved in establishing AToMpseudowires. They are the nontargeted LDP session and the targeted LDP session.

The nontargeted LDP session that is established through LDP basic discovery between a PE router and its directly connected P routers is used to distribute tunnel labels. The label distri-bution and management of tunnel labels pertains to the deployment model of the underlying MPLS network.

It can be some combination of downstream on-demand or unsolicited label advertisement, independent or ordered control, and conservative or liberal label retention. Neither pseudowire emulation nor AToM dictates any particular label distribution and management mode for tunnel labels.

The other type of LDP sessions are established through LDP extended discovery between PE routers. These sessions are known as targeted LDP sessions because they send periodic Tar-geted Hello messages to each other. Targeted LDP sessions in the context of pseudowire emulation distribute pseudowire labels.

IETF documents on pseudowire emulation over MPLS specify the use of downstream unsolicited label advertisement. In Cisco IOS Software, AToM uses independent label control and liberal label retention to improve performance and convergence time on pseudowire signaling.

XII. USING SEQUENCE NUMBERS:

Because Layer 2 packets are normally transported over Layer 1 physical media directly, most Layer 2 protocols assume that the underlying transport ensures in-order packet delivery. These protocols might not function correctly if out-of-order delivery occurs. For instance, if PPP LCP packets are reordered, the end-to-end PPP connection is unable to establish.

To avoid out-of-order packets, the best solution is to engineer a reordering-free packet network. Even though this goal is not always easy to achieve, you should make it a priority because no matter what kind of remedy you might use, network performance suffers significantly from out-of-order delivery.

Sequencing that is defined in pseudowire emulation mainly serves a detection mechanism for network operators to troubleshoot occasional out-of-order delivery problems. Implementations might choose to either discard or reorder out-of-order packets when they are detected. Because the latter requires huge packet buffer space for high-speed links and has significant performance overhead, AToM simply discards out-of-order packets and relies on the upper layer to retransmit these packets. The first step in using sequencing is to signal the presence of the control word, as described in the previous section. The control word contains a 16-bit Sequence Number field. However, the presence of the control word does not mandate sequencing. When sequencing is not used, Sequence Number value is set to 0.

After negotiating the control word, the sequence number is set to 1 and increments by 1 for each subsequent packet that is being transmitted. If the transmitting sequence number reaches the maximum value 65535, it wraps around to 1 again.
To detect an out-of-order packet, the receiving PE router calculates the expected sequence number for the next packet by using the last receiving sequence number (which has an initial value of 0) plus 1, and then mod (modulus) by 2^{16} (2^{16} = 65536). If the result is 0, the expected sequence number is set to 1. A packet that is received over a pseudowire is considered in-order if one of the following conditions is met:

- The receiving sequence number is 0.
- The receiving sequence number is no less than the expected sequence number and the result of the receiving sequence number minus the expected sequence number is less than 32768.
- The receiving sequence number is less than the expected sequence number and the result

of the expected sequence number minus the receiving sequence number is no less than 32768.

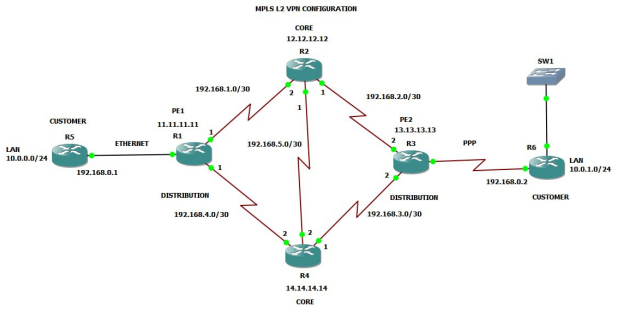

Fig.3. final configuration of deployment

If none of these conditions is satisfied, the packet is considered out-of-order and is discarded.

Sometimes the sending or the receiving PE router might lose the last transmitting or receiving sequence number because of transient system problems. This router might want to restart the sequence number from the initial value. AToM implements a set of signaling procedures to reliably resynchronize the sequence number. Although the IETF documents do not specify these procedures, the procedures are interoperable with any standard-compliant implementation. The resynchronization procedures in AToM are as follows:

- If the transmitting PE router needs to reset the transmitting sequence number, it must inform the receiving PE router to reset the receiving sequence number. AToM accomplishes this by letting the transmitting PE router send a Label Release message to the receiving PE router, followed by a Label Request message. Because the receiving PE router interprets this as a pseudowire flapping, it resets the receiving sequence number.

- If the receiving PE router needs to reset the receiving sequence number, it must inform the receiving PE router to reset the transmitting sequence number. AToM does so by letting the receiving PE router send a Label Withdraw message to the transmitting PE router, followed by a Label Mapping message. Because the transmitting PE router perceives this as a pseudowire flapping, it resets the transmitting sequence number.

XIII. CONCLUSIONS

Simulation Aims and Environment The aim of this simulation is to underline the need of integration of AToM with DiffServ. AToM rerouting is shown in this simulation as the motivating reason behind the AToM and DiffServ integration. AToM traffic engineering is an other important reason for AToM and DiffServ integration, but will not be dealt with here. The environment consists of ns-2 network simulation software in Linux operating system. Two ns-2 patches, the DiffServ patch and the MPLS patch were applied to execute the simulations.

REFERENCES

1. *Francesco Palmieri, (2003), 'VPN Scalability over High Performance Backbone Evaluating MPLS VPN against Traditional Approaches,' Proceedings of the 8th IEEE International Symposium on Computers and Communication, vol. 2, pp. 975-981.*
2. *Hiroshi Yamada (2006),'End-to-End Performance Design Framework of MPLS Virtual Private Network Service across Autonomous System Boundaries', IEEE International.*
3. *Lan jun ,Lin bi ying (2011)Research for Service Deployment Based on MPLS L3 VPN Technology, IEEE International transaction.*, M. BELLAFKIH**
4. *Li-Der Chout, Mao Yuan Hong (2006) 'Design and Implementation of Two-Level VPN Service Provisioning Systems over MPLS Networks', IEEE International Symposium.*
5. *Mahesh Kr. Porwal, Anjulata Yadav,S. V. Charhate(2008) 'Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic distribution in OSPF and MPLS', IEEE International journal.*
6. *Md.Arifur Rahman, A.H.Kabir, K.A.M.Lutfullahl, Z.Hassan(2007) 'Performance Analysis of MPLS Protocols over conventional Network', IEEE International Symposium.*
7. *Muhammad Romdzi Ahamed Rahimi,Habibah Hashim(2009) 'Implementation of Quality of Service (QoS) in Multi-Protocol Label Switching (MPLS) Networks', IEEE International .*

8. *Shu-mei LI, Hai-ying LIANG (2011) 'A Model of Path Fault Recovery of MPLS VPN and Simulation', IEEE International.*

9. *Tran Cong Hung, PhD, Le Quoc Cuong, Ph.D, Tran Thi Thuy (2010) 'A Study on Any Transport over MPLS (AToM)'Functioning and Management of MPLS/QOS In the IMS architectureA. Saika*, R. El KOUCH International.*

10. *Zakaria Bin Ali,Mustaffa Samad,Habibah (2011) 'Performance Comparison of Video Multicasting over Asynchronous Transfer Mode (ATM) & Multiprotocol Label Switching (MPLS) Networks', IEEE*