Migration of an ATM Network Core to MPLS/IP

ELG 5369 Course Project

Group 4

Technology review

Case :

Company D has a country-wide network that uses leased Asynchronous Transfer Mode (ATM) PVCs in order to mesh their various sites located in different cities across the country. Until recently, the network design has proven extremely reliable and has met the bandwidth requirements of the business applications used by the company. As the company has experienced significant growth over the past few years, however, the bandwidth requirements have increased and the network is quickly approaching the point where a capacity upgrade will be required. The current ATM network will not scale well under these conditions, especially since cost has become a pressing issue as the network increased in size.

The IT department of ***company D is considering migrating to an Ethernet-based network, but has to take into account the difference in reliability and flexibility between the two technologies. They have decided to use an MPLS-over-IP network in order to be able to set up redundant tunnels.*** *You will have to examine the current design, provide a new network design that meets their requirements and provide a transition strategy.*

Contents

List of Figures

1 INTRODUCTION

The purpose of this technology review is to highlight the technologies and concepts needed to do a network core migration of Company D from Asynchronous Transfer Mode (ATM) in to IP/MPLS network. In the first chapter, it discusses ATM technology in brief and advantages & disadvantages of ATM technology in general. Most importantly, it outlines the inherent constraints of ATM, that limits its ability to cater the increasing IP traffic demand.

Technology, key concepts and advantages of IP/MPLS networks were described in the second chapter. Also it will key out the strengths of IP/MPLS technology that provide solutions to inherent ATM limitations. Main points that should be considered at the network core migration and initial migration strategies are also briefly discussed in this chapter.

2 EXISTING SYSTEM

Company D is currently using a leased ATM core network to connect business sites scattered across the country. This chapter provides brief overview and key concepts of ATM technology.

2.1 ATM Technology

Asynchronous Transfer Mode (ATM) is a (ITU-T) standard which used cell relaying for the transfer of voice, video, and data over computer networks. It provides data link layer services employing both circuit switched and small packet switched networking, making it suitable for data networking as well as real-time media transport. Circuit switching provides constant transmission delay, guaranteed capacity and better for delay sensitive traffic whereas packet switching provides flexibility and efficiency for intermittent traffic (1). ATM has following features;

- Fixed size cells: ATM fragments data packets and A/V streams into 48-byte chunks, add 5 byte routing header and end with 53 byte cell (see Fig 1). This fixed size makes it possible to do more efficient and fast hardware switching.
- Connection-oriented service: virtual circuits such as Switched virtual connection (SVC) and Permanent virtual connection (PVC) allow fast routing of cells through ATM network

- Asynchronous multiplexing: The ATM Adaptation Layer (AAL) allows ATM to multiplex varied traffic types according to delay and throughput sensitivity requirements of each type of stream. AAL conversions were done at network end points. Thus transporting core doesn't have any conversion overhead.

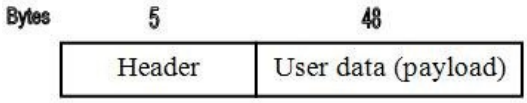


Figure 1 ATM Cell

Virtual circuits serves as logical pipes that connect end devices of ATM core. Permanent Virtual Circuits (PVCs) are built by administratively hard-coding a specific static path through the back bone. It works similar to a leased line between end points. Switched virtual connections (SVCs) are dynamically built by intelligent access devices using ATM signaling. There are three types of ATM traffic paths namely transmission path, a virtual path (VP), or a virtual channel (VC). Virtual connection needs to be established across the ATM network prior to any data transfer. Virtual Path consists several virtual Channels (see Fig 2), in a common traffic characteristics and route through the network. Although ATM switches are capable of switching these VPs and VCs transparently.

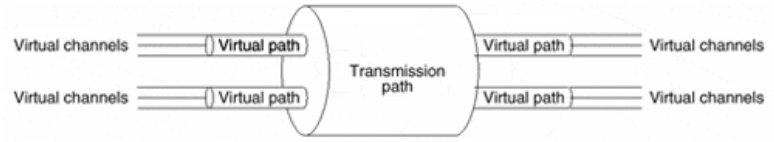


Figure 2 Virtual paths and channels

2.2 Limitations and Disadvantages of ATM Technology

2.2.1 Route instability

Routing in the ATM was done by both Layer 3 and layer 2. If one physical link failed, both layer 3 routing protocol (ex IGRP) and layer 2 ATM Private Network to Network Interface (PNNI) protocol will start to reestablish paths for new cells. During the time that PNNI reestablish the path, Layer 3 protocol try to exchange information and after PNNI establish a path, L3 protocol still need to exchange routing information do calculations to build up L3 connectivity. If any unstable link was there in between the path, it will stress the routers and will take large processing time (2).

2.2.2 Delay added to IP data transmission

IP packet propagation time depends on how they were transferred over the network. If external IP routes were interconnected with PVC's as a solution, every packet may need to route at every node adding significant propagation time at every node. Also packets will be forced to follow PVC path although it is not the topologically best path. ATM - LAN Emulation, multiprotocol over ATM and MPLS are solutions to this problem.

2.2.3 Header overhead

In ATM network IP traffic induce a significant overhead due to the small and fixed size of an ATM cell. An ATM cell has 53 bytes, 48 bytes usable data and 5 bytes for the head. Since the ratio of header size to data chunk size is more than 10%, overall header overhead per maximum size IP payload will be considerable.

2.2.4 Overhead due to cell drops

Another major issue of data transferring over ATM occurs when accidentally one cell of a data packet dropped or damaged. Since data packets are highly sensitive to throughput, the whole packet will be useless. But all the rest of cells need to pass the whole distance to the destination and re assembled to find that one cell is missing. If that packet had maximum IP payload, re trans mission of that packet will generate over 300 ATM chunks and also header overhead will again added to the network.

3 PROPOSED SYSTEM

Multi-Protocol Label Switching (MPLS) is considered as most efficient and cost effective alternative for ATM and Frame relay. It enables Service Providers to offer enhanced services for their customers, expand their current services, and have a higher degree of control over their growing networks by using its traffic engineering capabilities. MPLS solutions are used to support a wide range of applications including VoIP, email, file sharing, data backup and remote access by mid-sized businesses and large enterprises that operate out of multiple locations (3).

3.1 MPLS Technology

MPLS has become the first choice of service providers as rapid changes in the type of traffic and the exponential growth in the number of internet users are continuously increasing the strain on the Internet's infrastructure. To meet these new demands, MPLS moves away from simple hop-by-hop routing, by enabling devices to specify paths in the network based on traffic types and bandwidth needs of the applications. Therefore with MPLS, Layer 2 attributes are also considered to select best path.

MPLS Switching enhances IP data transmission with additional functionalities of connection oriented data transmission networks. Labels were attached to the IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. Thus the packets are forwarded by label switching instead of by IP routing. Although Frame Relay and ATM use label switching to move frames or cells throughout a network, MPLS differs significantly as it doesn't change the label value at every HOP. The MPLS has become a more challenging competitor to Frame Relay and ATM due to the fact that MPLS uses labels to forward the packets instead of destination IP address. In a nutshell, MPLS has following benefits;

- The use of one unified network infrastructure
- Better IP over ATM integration
- Border Gateway Protocol (BGP)-free core
- The peer-to-peer model for MPLS VPN

- Optimal traffic flow
- Traffic engineering

Usually IP packets were routed from source to destination in WAN's by forwarding to next hope after matching IP header entries with previously calculated stored routing table entries. This Process needs high processing power and time.

3.2 MPLS Architecture

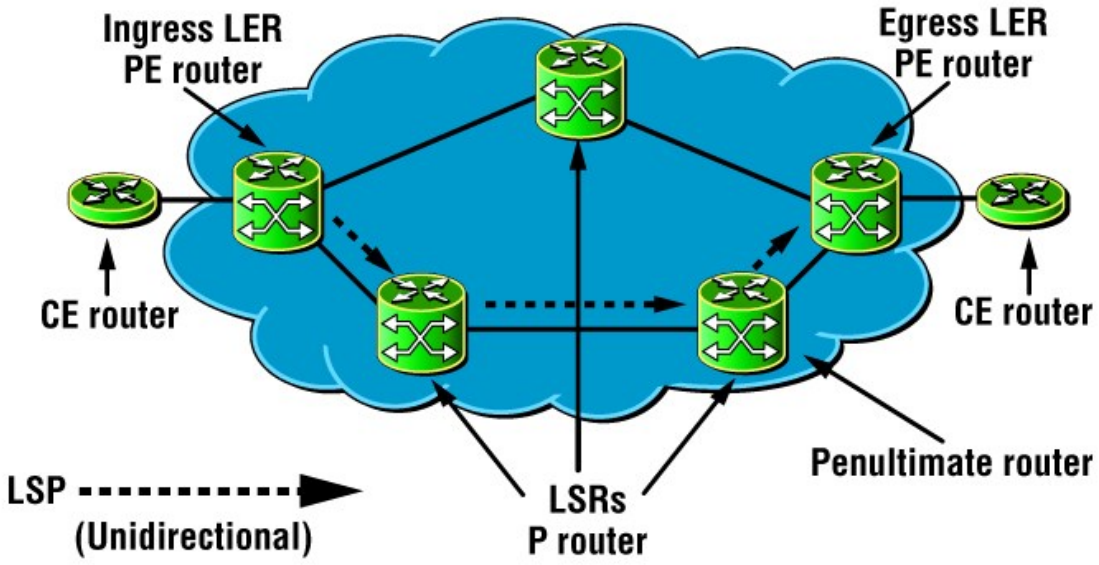


Figure 3 MPLS Architecture

- Label edge router (LER): This is a device in between non MPLS and MPLS networks. The ingress LER is the device that will add a label to incoming data. The egress LER will remove a label from an MPLS-labeled packet and act according to the encapsulated data. Therefore these router need to scan through IP network layer and add label to data units according to IP header information.
- Label switching router (LSR): This is a device capable of performing label switching as well as forwarding IP packets. LSRs are usually found in the core of the MPLS network. In the context of MPLS VPNs, an LSR is called the provider (P) router.

- Label switched path (LSP): The virtual circuit established across the MPLS network. The LSP defines the path that a unidirectional flow of data takes between LERs and across LSRs in the core of the network. Since this is a unidirectional flow, at least two LSPs must be established to achieve bidirectional traffic flow. The LSP is defined by mapping labels from an incoming interface to an outgoing interface.

- Penultimate hop popping (PHP): Endmost router in the MPLS LSP that removes the label and forwards the packet unlabeled, to the last router. This saves the egress LER from receiving the incoming labeled packet, performing the label lookup, deciding the label must be removed, removing the label and finally performing another lookup on the encapsulated packet to find how to forward it over non MPLS network.

3.3 MPLS Tag-Switching, Controlling and Forwarding

MPLS technology deals with two major functions (4);

- Forwarding- labels carried by packets and the label-forwarding information maintained by an LSR to perform packet forwarding.
- Control- responsible for maintaining correct label-forwarding information among a group of interconnected label switches (LSRs).

3.3.1 Forwarding

Forwarding decision is based on the exact-match algorithm using a fixed-length, short label as an index. When a packet with a label is received by an LSR, the switch uses the label as an index in its label information base (LFIB). Each entry in the LFIB consists of an incoming label and subentries such as outgoing label, outgoing interface and outgoing link-level information. If the switch finds an entry with the incoming label equal to the label carried in the packet, then, for each component in the entry, the switch replaces the label in the packet with the outgoing label, replaces the link-level information (such as the MAC address) in the packet with the outgoing link-level information, and forwards the packet over the outgoing interface. Forwarding based on exact match algorithm enables a simplified forwarding procedure, relative to longest-match forwarding traditionally used at the network layer. This provides several benefits;

1. Higher forwarding packets per second. The forwarding procedure is simple enough to allow a straightforward hardware (ASIC) implementation.
2. Forwarding decision is independent of the label's forwarding granularity. The same forwarding

algorithm, for example, applies to both unicast and multicast: A unicast entry would have a single (outgoing label, outgoing interface and outgoing link-level information) subentry, while a multicast entry might have one or more subentries.

The simple forwarding procedure is thus essentially decoupled from the control component of label switching. New routing (control) functions can readily be deployed without disturbing the forwarding paradigm. Therefore it is not necessary to modify either hardware or software for optimization, as new routing functionality is added.

3.3.2 MPLS Label

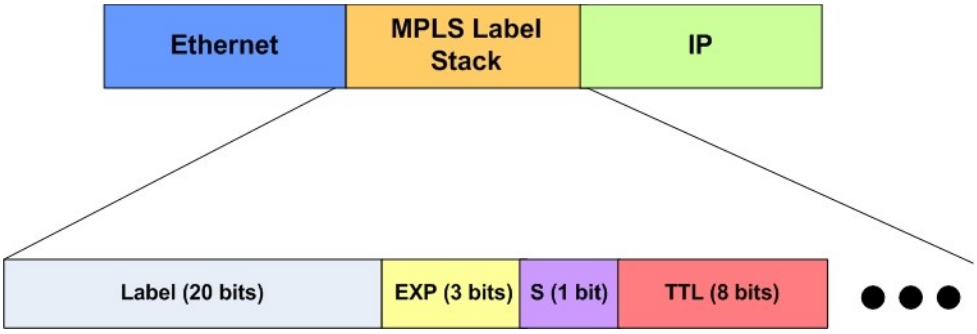


Figure 4 MPLS Label

A label consists of four fields:

- Label: Label value of 20 bits. Used as the pointer for forwarding.
- Exp: For QoS, three bits in length.
- S: Flag for indicating whether the label is at the bottom of the label stack, one bit in length. 1 indicates that the label is at the bottom of the label stack. This field is very useful when there are multiple levels of MPLS labels.
- TTL: Time to live (TTL) for the label. Eight bits in length. This field has the same meaning as that for an IP packet.

Similar to the VPI/VCI in ATM and the DLCI in frame relay, an MPLS label functions as a connection identifier. If the link layer protocol has a label field like VPI/VCI in ATM or DLCI in frame relay, the MPLS label is encapsulated in that field. Otherwise, it is inserted between the data link layer header and the network layer header as a shim. As a result, MPLS can be implemented over any media type, including point-to-point links, multi-access links, and ATM. The label-forwarding component is independent of the network layer protocol. Use of control components specific to a particular network layer protocol enables the use of label switching with different network layer protocols.

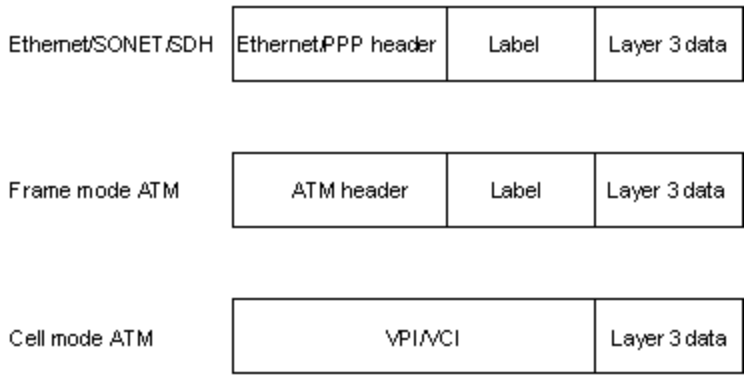


Figure 5 MPLS Label in other L2 data units

3.3.3 Control Function

MPLS need a binding between a label and network layer routes. Label could be bind either to the network layer reachability information of the routes in the group or it could be bound to an individual application flow such as an RSVP flow, or it could be bound to a multicast tree. The control component creates label bindings and then distributes the label-binding information among LSRs using a Label Distribution Protocol (LDP).

Label Distribution Protocols

There are four protocols that can perform the label distribution function:

1. Label Distribution Protocol (LDP)

   LDP relies on the underlying routing information provided by an IGP in order to forward label packets. The router forwarding information base is responsible for determining the hop-by-hop path through the network.

2. Resource Reservation Protocol with Traffic Engineering Extensions (RSVP-TE)

   RSVP-TE allows the establishment of MPLS label switched paths (LSPs), taking into consideration network constraint parameters such as available bandwidth and explicit hops.

3. Constraint-Based Routed LDP (CR-LDP)

   CR-LDP is an extension of LDP that adds signaling capabilities almost identical to those of RSVP-TE. It is not commonly used by MPLS vendors dominating the market.

4. Multiprotocol BGP

   Multiprotocol BGP supports label distribution through the IPv4 and IPv6 labeled unicast address families and it is a specialized function in support of Layer 3 MPLS VPNs

Using its signaling element, RSVP-TE sets up an LSP end-to-end (ingress-to-egress). So label distribution is coordinated among all the LSRs along a path. LDP, on the other hand, has no signaling element. It sets up LSPs hop-by-hop, and labels can be distributed between neighbors independently of what other LSRs along the path are doing. Because it has no signaling element, LDP depends on the network's IGP to determine the path an LSP must take, whereas RSVP-TE can set up paths independently of what the IGP determines to be the optimal path to a destination - hence the Traffic Engineering part of the protocol (5).

4 MIGRATION TO MPLS

MPLS/VPNs are attractive to both Customers and service providers. For enterprises, they enable right-sourcing of WAN services and provide operational cost savings. For service providers, they offer a higher level of service to customers and lower costs for service deployment serving their primary goal of providing a scalable network that is easy to manage. Many Large scale and growing enterprise networks can benefit from the migrating to MPLS infrastructure. Migrating in to MPLS provides access to higher speed technologies including, Gigabit Ethernet, OC-48c/STM-16 SONET/SDH, and 10-Gbps technologies (6).

Most networks use ATM or LANE/ATM as a means of connecting backbone routers together. When using ATM connectivity between devices, MPLS use cells as carriers for data plane information. When ATM labels are used in an MPLS core, the operating mode of MPLS is called cell-mode MPLS. Frame mode MPLS can also implemented in ATM for routing between LSRs (via routed ATM PVCs). In cell-mode MPLS, the LSRs in the core of the MPLS network are ATM switches that forward data based on the ATM header. Data link layer connectivity in a frame-mode MPLS domain is established using serial HDLC/PPP, Ethernet, or ATM. ATM brings us to another aspect of Layer 2 connectivity where cells are used to transport IP packets. Note that although there might be ATM links in the MPLS domain, it is possible to run regular IP point-to-point links (routed PVCs). In such cases, it is still considered frame-mode MPLS and not cell-mode MPLS, although the Layer 2 protocol is ATM (7). In frame-mode MPLS, routers running MPLS exchange pure IP packets and labeled IP packets with one another in an MPLS domain. In an MPLS domain, label switching is done by parsing the frame header and then adding (push) & removing (pop) label by Edge LSRs and label swapping & frame forwarding by non-edge LSRs. For service providers and organizations currently having ATM backbone

infrastructure, can move in to ATM/MPLS solution or complete MPLS solution with on Layer 2 IP/MPLS VPNs.

4.1 Label Switching with ATM

MPLS technology can be applied to ATM switches by implementing the control component sine the label information needed for tag switching can be carried in the ATM VCI field. If two levels of labeling are needed, then the ATM VPI field could be used as well, although the size of the VPI field limits the size of networks in which this would be practical. The VCI field, however, is adequate for most applications of one level of labeling (8). Implementing MPLS on an ATM switch would simplify integration of ATM switches and routers. An ATM switch capable of MPLS would appear as a router to an adjacent router. That would provide a scalable alternative to the overlay model and would remove the necessity for ATM addressing, routing, and signaling schemes.

4.1.1 MPLS deployment models

- Label-Controlled ATM
- Tunneling Through ATM
- Ships in the night with ATM

Most convenient MPLS to the existing ATM network the deployment model proposed is "Ships-in- the-Night". This means that the ATM control plane and MPLS control plane will operate simultaneous without interference using the existing ATM switch hardware. This allows a single device to simultaneously operate as both an MPLS LSR and an ATM switch (9).

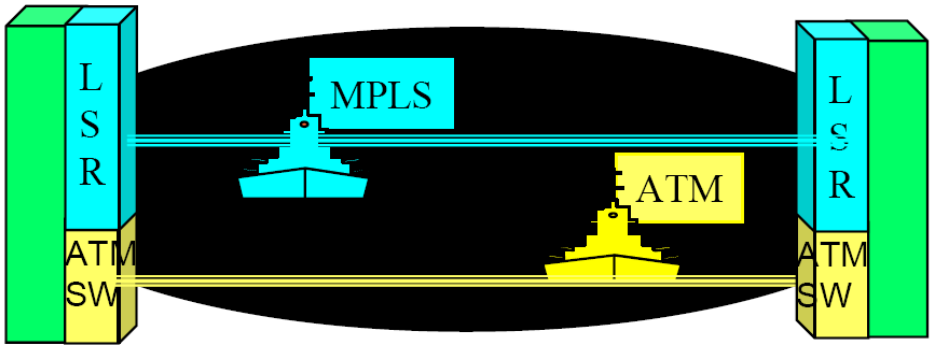


Figure 6 "Ships in the night" deployment model

MPLS could be deployed in two major ways:

- Cell switched MPLS - IP packets are still split into cells and transported using ATM infrastructure
- Frame based MPLS - cell are no longer used and another layer 2 protocol is used, such as POS (Packets over Sonet) and old ATM hardware may still be used.

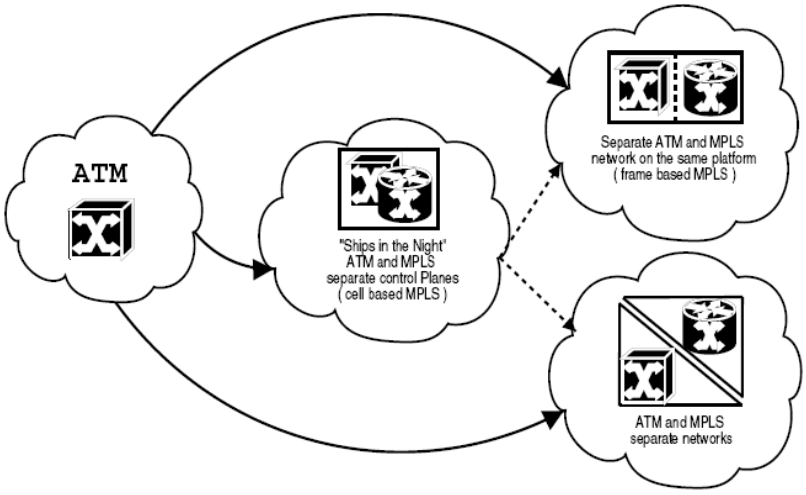


Figure 7 ATM to MPLS migration PATH

The migration to cell switched MPLS is convenient and it requires a software upgrade of the ATM network. Cell switched MPLS offer some advantages such as: reducing IGRP stress, reducing management complexity and simplifying the Class of Services management. The need to establish PVC's at the ATM layer will eliminated and IGRP stress situation will no longer occur. Although it is possible to connect ATM MPLS devices over traditional ATM equipment, in a hybrid ATM network, it is undesirable due to several disadvantages;

- Hybrid ATM networks are inefficient at providing IP services such as multicast.
- Hybrid ATM networks have routing scaling problems similar to those of IP-over-PVC networks.
- Hybrid ATM networks are more difficult to manage than pure MPLS networks.

However hybrid ATM networks can support MPLS services such as Virtual Private Networks, and may be necessary as a migration step before introducing a full MPLS network.

4.2 IP/MPLS-Based VPNs

There are two main MPLS based VPN types

Layer 3 MPLS-based VPNs

- BGP/MPLS VPNs (RFC 2547bis)

Layer 2 MPLS-based VPNs

- Virtual Private Wire Service (VPWS) – For Point-to-point connections
- Virtual Private LAN service (VPLS) – For Point-to-multipoint connections

A virtual private network (VPN) is a network in which customer connectivity to multiple sites is deployed on a shared infrastructure with the same administrative policies as a private network. The path between two systems in a VPN, and the characteristics of that path, may also be determined (wholly or partially) by policy. Whether a system in a particular VPN is allowed to communicate with systems not in the same VPN is also a matter of policy (10). In MPLS VPN, a VPN generally consists of a set of sites that are interconnected by means of an MPLS provider core network, but it is also possible to apply different policies to different systems that are located at the same site.

Layer 3 MPLS VPNs are characterized by fully meshed architectures that enable, for instance, multicast conferencing in support of projects involving a dispersed work group. Layer 2 MPLS technology is limited in this area because it does not scale as well as Layer 3.Small industrial entities prefer Layer 3 options because the service provider takes responsibility of the WAN routing, whereas with a Layer 2 VPN, such as MPLS-based virtual private LAN services (VPLS), businesses would have to handle the routing (11)

4.2.1 MPLS Layer-3 VPNs

Layer 3 MPLS-based VPNs offers a routed solution and it's also referred to as BGP/MPLS VPNs because routes are propagated via BGP.
Three basic steps involve in data transmission;

1. Edge router picks up customer datagram from one site
2. Looking up the destination IP address of the datagram in a forwarding table
3. Sending that datagram to its destination across the provider's network using a LSP

BGP/MPLS VPNs approach follows the peer to peer model of VPNs. The provider edge (PE) routers exchange routes with the customer edge (CE) routers to acquire reachability information about a given customer's

networks and BGP propagates these routes to other PE routers who are catering the same VPN. However, they are never shared with the provider's core routers (P), since the PEs use LSPs to forward packets from one PE to the other. P routers do not need to know about the customer's networks in order to perform their label switching functions (Figure 8). A PE router receiving routes of a given VPN site from another PE, propagates the routes to the CE router of the connected site belonging to that same VPN, so that the CE will also learn about the networks in the remote site (12).

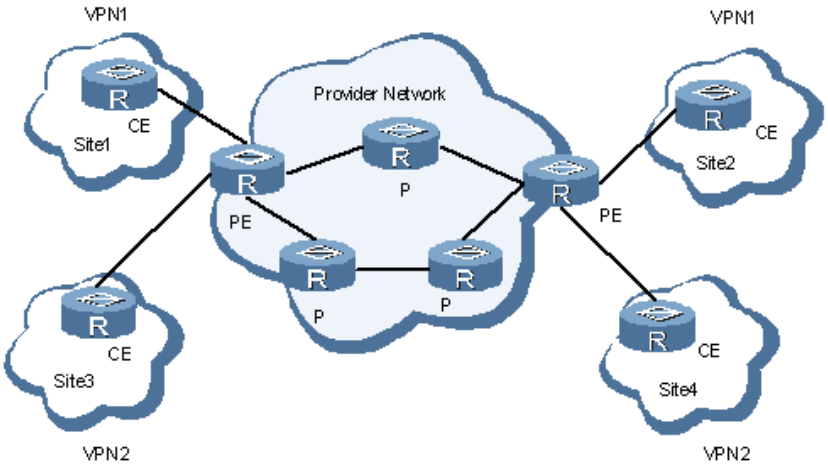


Figure 8 BGP/MPLS Architecture

BGP/MPLS VPNs has two major advantages over pure VPNs without tunneling

- Supporting globally unique IP addresses on the customer side and private non-unique overlapping addresses
- Supporting overlapping VPNs, where one site could belong to more than one VPN. The approach allows for creating overlapping VPNs when a customer needs a VPN for their intranet, and another for their extranet with a different set of routes advertised in each to control the accessibility of resources. Such a customer would rely on the service provider to perform the required route control.

Multiple VPN Routing and Forwarding (VRF) tables are created on each PE router to separate the routes belong to different VPNs on a PE router. A VRF table is created for each site connected to the PE, however, if there were multiple sites belonging to the same VPN connected to the same PE, these sites might share a single VRF table on that PE.

When advertising a VPN-IPv4 route, the PE also includes an MPLS label – representing the route – in the BGP message, and it sets the BGP NEXT_HOP equal to its own address. The provider network is MPLS enabled, and each PE router should be capable of reaching any of the other PEs via an LSP. Those LSPs could be created by any protocol like LDP or RSVP/TE.

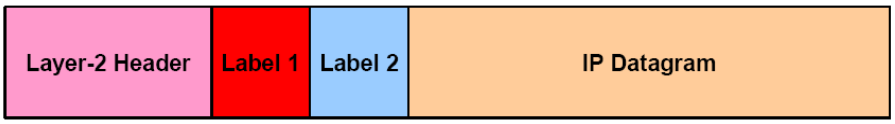


Figure 9 BGP/MPLS Datagram

When a PE router receives a packet with a destination in a remote site, it pushes two MPLS labels between Layer 2 header and payload (Figure 9) and forwards it from its relevant destination port for LSP. The frame gets label switched all the way to the remote PE. Remote PE pops the label 1, and examines the label 2. Label 1 is for the LSP leading to the BGP NEXT_HOP. Label 2 is the label associated with that destination, learned previously from a BGP update received from a peer. Label 2, in most cases, is to uniquely identify the destination, therefore, it is removed by destination PE and the packet is forwarded to its destination.

4.2.2 MPLS Layer-2 VPNs

Layer 2 MPLS based VPNs provide switched solution and allows complete separation between the provider's network and the customer's network since there is no route exchange between the PE devices and the CE devices. MPLS Layer 2 network infrastructure is completely transparent to both sending edge and receiving edge customer devices. As a result, customer devices recognize the topology as directly connected devices. Handling customer layer-2 frames allows the service provider to offer a service that is independent of the layer-3 protocols in use by the customers. The layer 2 MPLS approach facilitates both Point-to-Point and Multi-Point Connectivity.

4.2.3 Virtual Private Wire Service (VPWS) for Point-to-Point Connectivity

Luca Martini introduced this VPN technology by IETF draft commonly known as Martini Drafts. VPWS L2VPNs employ layer 2 services over MPLS to build a topology of point-to-point connections that connect end customer sites in a VPN. These L2VPNs provide an alternative to private networks that have been provisioned by means of dedicated leased lines or by means of layer 2 virtual circuits that employ ATM or Frame Relay. The service provisioned with these L2VPNs is known as Virtual Private Wire Service (VPWS) or Martini Pseudo-wires (13).

VPWS makes the integration of existing Layer 2 and Layer 3 services possible on a point-to-point basis across a service provider's IP/MPLS cloud VPN called a pseudo-wire (Figure 10). A pseudo-wire is an encapsulation of a service for transmission over a packet switched network. Two pseudo-wire technologies are available from Cisco Systems. AToM is the Ciscopseudo-wire technology that targets MPLS networks and L2TPv3 is the Cisco

pseudo-wire technology for native IP networks (14).

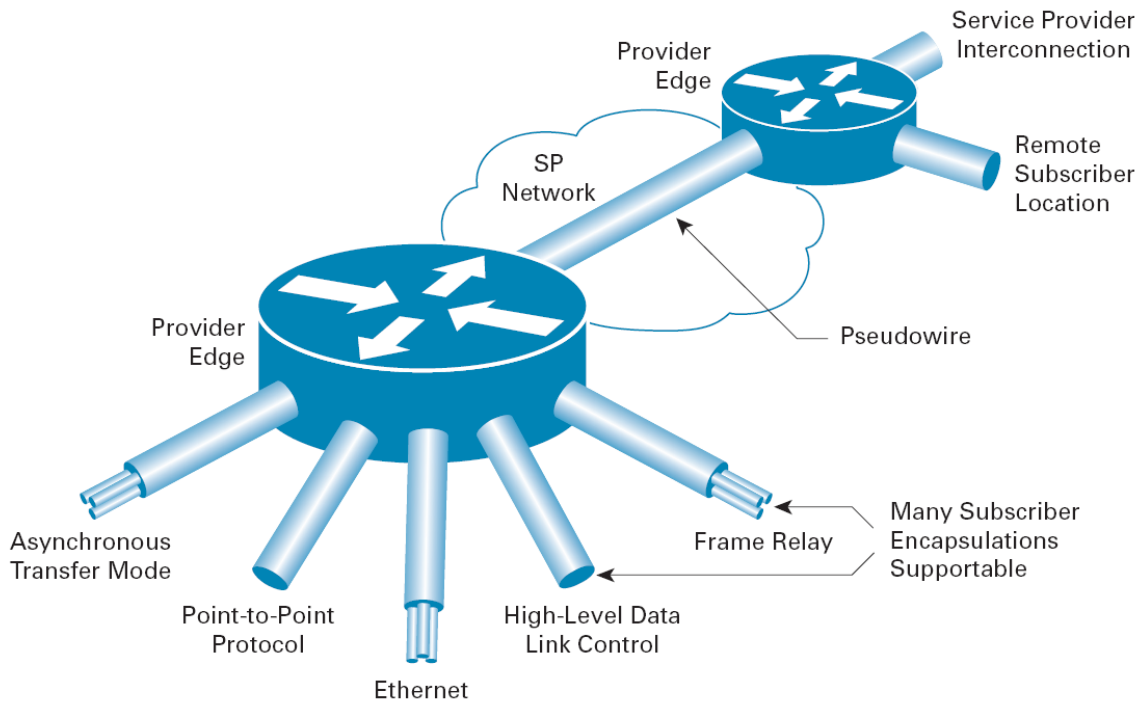


Figure 10 Pseudo-wire over MPLS network

An LSP acts as a tunnel carrying multiple VCs, whereas a VC acts like the actual circuit carrying customer layer-2 frames. A VC, actually, is just another LSP within the original tunnel LSP. The tunnel LSP provides the tunnel between two PE routers, while the VC carries frames of a given customer only. VCs are uni-directional just like normal LSPs. Hence, for bi-directional communication, a pair of VCs – one in each direction – is need. In order to create this hierarchy, an encapsulated customer frame traversing the service provider network has two labels attached to it as shown in Figure 11.

- A label pertaining to the tunnel LSP leading to a destination PE. This is called the "tunnel label".
- A label pertaining to the VC that carries the frame and leads to a certain site attached to the destination PE. This is called the "VC label".

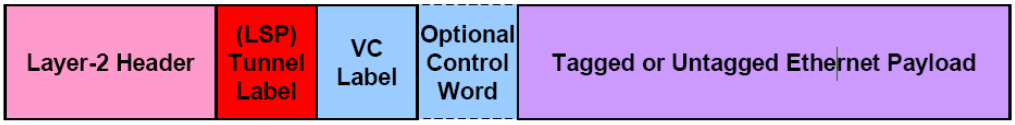


Figure 11 Labels in VPWS PDU

Tunnel LSPs between the PE routers could be created using any protocol like RSVP/TE or LDP. PE routers exchange the VC labels via LDP in downstream unsolicited mode.

At the edge of the provider network, the PE router encapsulates the subscriber layer-2 frame as per the Martini drafts, attaches a VC label and a tunnel label, and then sends the frame over the tunnel LSP. At the other end of the tunnel LSP, the receiving PE router pops the tunnel label, determines which customer port the packet should be destined based on the VC label, extracts the original layer-2 frame, and sends it out the port determined above.

4.2.4 Virtual Private LAN Service (VPLS) for Point-to-Multipoint Connectivity

VPLS is described in Kompella (15) drafts and it's an attractive option for service providers because it uses a Layer 2 architecture to offer multipoint Ethernet VPNs that connect multiple sites over a metropolitan-area network (MAN) or WAN. For efficient use of the provider's network bandwidth, a frame should be sent only to the PE that connects to the target site of the frame whenever possible, instead of being flooded. This is accomplished by switching the customer frames based on their destination MAC address. Using VPLS, service providers can create a Layer 2 "virtual switch" over an MPLS core to establish a distributed Network Access Point (NAP). The NAP allows transparent private peering between multiple ISPs and delivers robust connections to multiple sites within a specific metro region. Service provider-to-service provider VPLS can be supported using either Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP). LDP provides more granular control of communication and quality of service between VPLS nodes, more control per node, and is a consistent signaling option to support MPLS, VPLS, or VPWS. BGP is less versatile because typically it communicates the same information to all nodes participating in a VPLS (12). A PE router maintains a separate layer-2 forwarding table, called Virtual Forwarding Instance (VFI), for each VPN that it carries. Figure 5 illustrates the basic concepts behind the VPLS approach.

Although PE routers carry out the switching function, unlike normal layer-2 switches, they do not run STP within the provider's network to avoid switching loops. Since VPLS is based on MPLS, it leverages MPLS' traffic protection abilities in order to implement a fault tolerant service. Also, since VPLS relies on a full mesh of VCs for a given VPN without any transit PEs in between, the VPLS PEs apply a simple split horizon forwarding rule when forwarding customer frames. If a customer frame is received over a VC within a VPN, that frame could only be forwarded to an attached customer site, not back to the same VPN (over another VC). This simple rule together with the full mesh topology of VCs addresses the issue of loop avoidance without using STP. Avoiding the use of STP allows the PE routers to avoid STP scalability issues commonly encountered in pure layer-2 networks. The intention here is to make VPLS more scalable.

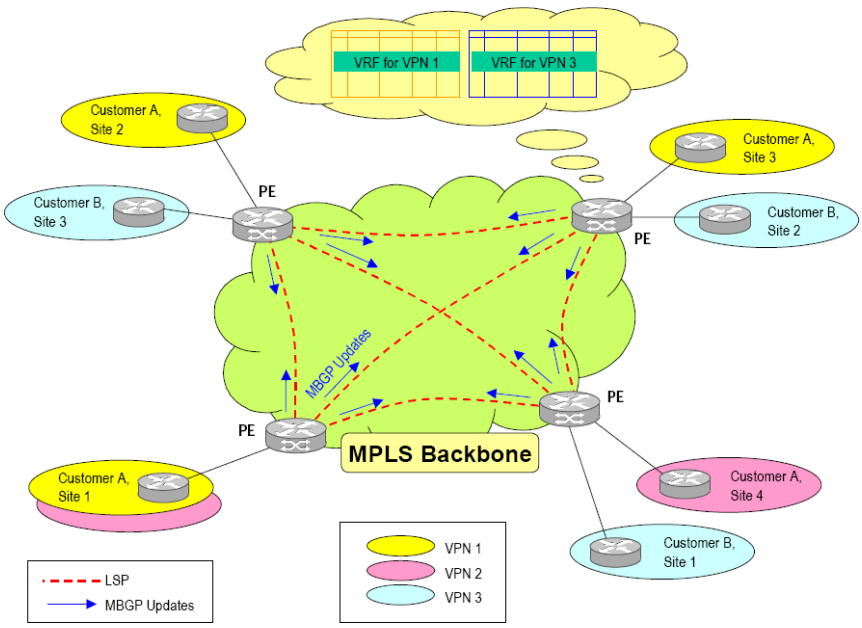


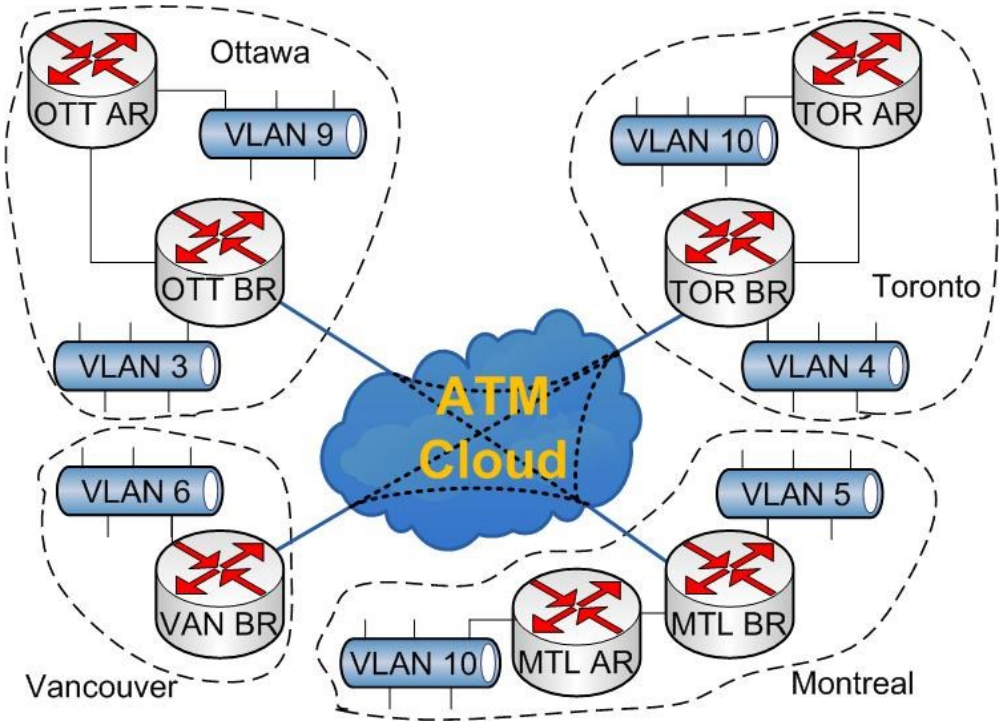
Figure 12 MPLS VPLS architecture

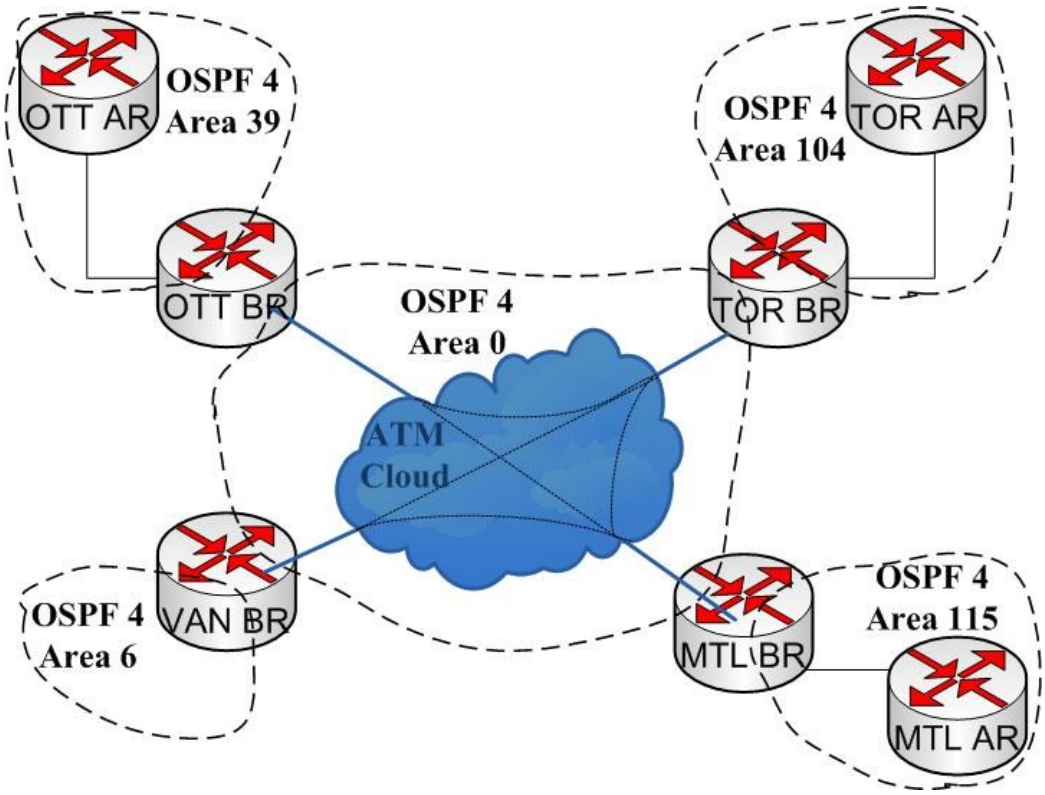
Another major advantage of VPLS is provisions to implement overlapping VPNs (Figure 12)

Customer A, Site 1 lies in both VPN 1 and VPN 2. To separate traffic belonging to each VPN, the customer site could be connected to the PE router using two access links, one for each VPN. Alternatively, traffic belonging to both VPNs could be multiplexed over the same access link using two different VLAN IDs, where one VLAN ID maps to VPN 1, the other ID maps to VPN 2. The use of more than one 802.1Q tag within a frame helps the service provider and the customer use the required service tag (VLAN ID) without having any impact on the customer's choice of their own VLAN IDs.

In contrast with the layer-3 approach, the task of controlling the routes that get advertised in each VPN remains the customer's responsibility, since the PE router does not handle any customer routes.

5 EXISTING DESIGN ANALYSIS




OSPF 4
Area 39
OTT AR
OTT BR
OSPF 4
Area 104
TOR AR
TOR BR
OSPF 4
Area 0
ATM
Cloud
OSPF 4
Area 6
VAN BR
MTL BR
OSPF 4
Area 115
MTL AR

6 BIBLIOGRAPHY

1. Guide to ATM Technology for the Catalyst 8540 MSR, Catalyst 8510 MSR, and LightStream 1010 ATM Switch Routers. [Online] Cisco Systems, Inc.170, West Tasman Drive, 2000. http://www.cisco.com/en/US/products/hw/switches/ps718/products_technical_reference_book09186a00800eb44f.html.

2. **Adrian, Minta.** ASPECTS OF NETWORK MIGRATION FROM ATM TO MPLS. *http://www.minta.ro/papers.html.* [Online] http://www.minta.ro/papers/Aspects_of_network_migration_from_ATM_to_MPLS.pdf.

3. Multiprotocol Label Switching. [Online] Hill Associates, Nov 2007. http://wiki.hill.com/wiki/index.php?title=Multiprotocol_Label_Switching.

4. MPLS/Tag Switching. *Internetworking Technology Handbook.* [Online] December 2009. http://docwiki.cisco.com/wiki/MPLS/Tag_Switching.

5. HTC IToIP Solution Experts. *MPLS Basics Introduction.* [Online] http://www.h3c.com/portal/Products___Solutions/Technology/MPLS/Technology_Introduction/200702/201197_57_0.htm.

6. **Lewis, Chris, et al., et al.** Selecting MPLS VPN Services. s.l. : Cisco Press, 2006.

7. **Jaeger, Rob.** *Transitioning from IP-over-LANE/ATM to IP/MPLS Networks.* s.l. : Juniper Networks, Inc.

8. **Lawrence, Jeremy.** Designing ATM MPLS Networks. [Online] 1999. docstore.mik.ua/cisco/pdf/Cisco.Designing.ATM.MPLS.Networks.pdf.

9. **Ionescu, Dan.** *ELG5369: Internetwork Technologies course Materials.* Ottawa : NCCT, University of Ottawa, 2010.

10. **Cisco, Systems.** Introduction to Cisco MPLS VPN Technology. *Cisco.* [Online] http://www.cisco.com/en/US/docs/net_mgmt/vpn_solutions_center/1.1/user/guide/VPN_UG1.html.

11. **Greene, Tim.** The differences between Layers 2 and 3 Cloud Security Alert. [Online] June 2006. http://www.networkworld.com/newsletters/vpn/2006/0605vpn2.html?fsrc=rss-vpns.

12. **Abdelhalim, Ahmed.** *IP/MPLS-Based VPNs.* s.l. : Foundry Networks, Inc, 2002.

13. **Networks, Juniper.** VPWS Overview. [Online]

http://www.juniper.net/techpubs/software/erx/junose93/swconfig-bgp-mpls/vpws-overview_1.html.

14. Vpls and vpws at a glance. [Online] Cisco Systems, Inc., 2004. http://www.cisco.com/application/pdf/en/us/guest/tech/tk891/c1482/cdccont_0900aecd80162184.pdf.

15. **K. Kompella et al.** Layer 2 VPNs Over Tunnels. [Online] 2003. http://tools.ietf.org/html/draft-kompella-ppvpn-l2vpn-03.