MPLS IMPLEMETATION ON LAYER 3 PROTOCOLS

A THESIS SUBMITTED TO
THE FACULTY OF ARCHITECTURE AND ENGINEERING
OF
EPOKA UNIVERSITY

BY

ERIGEN HOXHA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
ELECTRONICS AND DIGITAL COMMUNICATION ENGINEERING

JULY , 2021

Approval sheet of the Thesis

This is to certify that we have read this thesis entitled **"MPLS Implemetation on Layer 3 Protocols"** and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Dr. Arban Uka
Head of Department
Date: July,28,2021

Examining Committee Members:

Assoc. Prof. Dr. Carlo Ciulla	(Computer Engineering)	_____
Dr. Maaruf Ali	(Computer Engineering)	_____
Dr. Julian Hoxha	(Computer Engineering)	_____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name Surname: Erigen Hoxha

Signature:_____

ABSTRACT

MPLS IMPLEMENTATION ON LAYER 3 PROTOCOLS

Hoxha, Erigen
M.Sc., Department of Computer Engineering
Supervisor: Dr. Julian Hoxha

This paper presents an overview of the basic operations that characterize MPLS technology and the distribution of its applications. The paper is structured in 4 chapters. It begins with a superficial description of the "MPLS world", the historical reasons for the need for this technology and its advantages as a technique that combines the labeled transfer qualities prevalent in Frame Relay and ATM technologies with the ease of distribution IP networks. Next is an overview of the MPLS tag architecture, how to transfer them to the MPLS network and some of the working methods in this network. Given that the field of MPLS technology applications is very wide and would require much longer work, only two of its applications have been studied in more detail: ATM as one of the earliest applications and MPLS VPN as its most widespread and popular application. Finally, the implementation of this technology in the network of the company ALBTELECOM is presented in detail.

The new method of packet transfer offered by MPLS technology led to the successful invention of many new applications that realize the transmission of packets based on tags such as: MPLS VPN, Traffic Engineering, AToM and VPLS. In this context, since MPLS is a mature technology, it is expected that in the future it will have further developments just as successful as those of the present.

The purpose of this paper is to provide the most understandable and practical information about MPLS technology and its applications, laying the foundations for the formation of a network engineering in the field of MPLS networks.

The methodology used is that of theoretical-practical treatment where the theoretical part is accompanied by practical examples, configuration schemes, details on how to implement and solve the problems of MPLS and its applications. This methodology makes it easy to understand what the paper deals with and at the same time makes it faster and easier to be assimilated by the reader.

Keywords: MPLS; VPN; ATM; IP networks.

ABSTRAKT

IMPLEMENTIMI I “MPLS” NË PROTOKOLLET E SHTRESËS SË TRETË

Hoxha, Erigen

Master Shkencor, Departamenti i Inxhinierisë Elektronike dhe Komunikimit Dixhital
Udhëheqësi: Dr. Julian Hoxha

Ky punim bën një paraqitje të operacioneve themelore që karakterizojnë teknologjinë MPLS dhe të shpërndarjes së aplikacioneve të saj. Punimi është strukturuar në 4 kapituj. Në fillim bëhet një përshkrim sipërfaqësor i “botës së MPLS -së”, arsyeve historike që sollën nevojën për këtë teknologji dhe përparësitë e saj si një teknikë që kombinon cilësitë e transferimit të etiketuar të përhapura në teknologjitë *Frame Relay* dhe ATM me lehtësitë e shpërndarjes së rrjeteve IP. Më tej bëhet një paraqitje e arkitekturës së etiketave MPLS, mënyrës së transferimit të tyre në rrjetin MPLS dhe të disa prej metodave të punës në këtë rrjet. Duke qënë se fusha e aplikacioneve të teknologjisë MPLS është shumë e gjerë dhe do të duhej një punim shumë herë më i gjatë, janë marë në studim më të detajuar vetëm dy prej aplikacioneve te saj: ATM-ja si një ndër aplikacionet më të herëshme dhe MPLS VPN-ja si aplikacioni më i përhapur dhe më popullor i saj. Në fund paraqitet në mënyrë të detajuar implementimi i kësaj teknologjie në rrjetin e kompanisë ALBTELEKOM.

Metoda e re e transferimit të paketave që ofron teknologjia MPLS çoi në shpikjen e suksesshme të shumë aplikacioneve të reja që realizojnë transmetimin e paketave bazuar në etiketa si: MPLS VPN, Inxhinieria e Trafikut, AToM dhe VPLS. Në këtë kuadër, duke

qënë se MPLS është një teknologji e maturuar, pritet që në të ardhmen të këtë zhvillime të mëtejshme po kaq te suksesshme sa ato të së tashmes.

Qëllimi i këtij punimi është që te japë një informacion sa më të kuptueshëm dhe praktik rreth teknologjisë MPLS dhe aplikacioneve të saj, duke hedhur bazat e formimit të një inxhinieri rrjeti në fushën e rrjeteve MPLS.

Metodologjia e përdorur është ajo e trajtimit teoriko-praktik ku pjesa teorike shoqërohet me shembuj praktik, skema konfigurimesh, detaje për mënyrën e implementimit dhe zgjidhjes së problemeve të MPLS-së dhe të aplikacioneve të saj. Kjo metodologji e bën lehtësisht të kuptueshëm atë çka punimi trajton dhe njëkohësisht bën që të asimilohet më shpejt dhe më thjeshtë nga ana e lexuesit.

Fjalët Kyçe: MPLS; VPN; ATM; rrjetet IP.

ACKNOWLEDGEMENTS

I would like to express my special thanks to my supervisor Dr. Julian Hoxha for his continuous guidance, encouragement, motivation and support during all the stages of my thesis. I sincerely appreciate the time and effort he has spent to improve my experience during my graduate years.

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENT

CHAPTER 1

INTRODUCTION

1.1. History of MPLS

Multiprotocol Label Switching (MPLS) has been around for many years in the modern world. Today it is one of the most popular technologies implemented in networks, which uses "labels" to transmit packets across the network.

Before MPLS arrived the most important WAN networks were ATM and Frame Relay. WANs, cost-effective, were built to maintain different types of protocols. With the popularity of the internet, IP became the most popular protocol. VPNs were being created over these WAN protocols. [1] Customers rented ATM lines or Frame Relay lines or other lines to set up private networks on the WAN. Since ISP routers used layer 2 services and the client used routers that worked in layer 3, sharing and isolation between different client networks was guaranteed. These networks were called overlay networks. They continue to be used today, but many users use MPLS VPN services.

Cisco systems began to put tags on the head of IP packets and at that time this was called Tag Switching. The first implementation took place on Cisco IOS 11.1 (17) CT in 1998. Tag was the name for what are now called labels. This implementation could define the network tags from the routing table and place these tags at the head of each packet destined for that network. Labeled routing built a TFIB (Tag Forwarding Information Base) which is essentially a table which contains the map of the labels from entry to exit. Each labeled routing router must match the incoming packet tag, replace it with the outgoing tag, and transfer the packet further. [2]

The IETF later standardized the labeled transfer by naming it MPLS and issued the first RFC on MPLS-RFC2547, "BGP / MPLS VPNs" - in 1999. The result was that much of the existing terminology changed. Table 1 shows a difference between the new and the old terminology. [3]

Table 1. New and Old terminology for Tag Switching/MPLS

Old terminology	*New terminology*
Tag switching	MPLS
Tag	Label
TDP => Tag Distribution Protocol	LDP => Label Distribution Protocol
TFIB => Tag Forwarding Information Base	LFIB => Label Forwarding Information Base
TSR => Tag Switching Router	LSR => Label Switching Router
TSC => Tag Switch Controller	LSC => Label Switch Controller
TSP => Tag Switched Path	LSP => Label Switched Path

Many of the labeled transfer technology was adopted to MPLS standards. TDP was used as the basis for LDP. LDP has the same function as TDP but they are different protocols. The first release of the labeled transfer on Cisco IOS allowed traffic engineering, and it was originally called Routing with Resource Reservation (RRR). [4]

The first implementation of traffic technology was static, which meant that the router operator had to configure all the hops that a traffic flow had to follow on the network. A subsequent implementation made traffic technology more dynamic using extensions in the connection state routing protocols and thus the operator was no longer obliged to configure the tunnels step by step. Connection state routing protocols carried extra information so that tunnels could be created dynamically. This reduces the work that the operator had to do and at the same time made MPLS traffic engineering very popular.

Until the advent of the MPLS VPN, tagged transfer, or MPLS, was not widely distributed. When Cisco came out with Cisco IOS 12.0 (5) T, the first software that had support for MPLS VPN in 1999, it became an immediate success because many SPs started implementing MPLS VPN immediately. MPLS VPN application is the most popular MPLS application.

The newcomer to the MPLS application family was AToM. Cisco implemented AToM on Cisco IOS 12.0 (10) ST, released in 2000, to carry ATM AAL 5 over MPLS backbone. Later many encapsulation types were added to AToM on Cisco IOS. Examples of the layer 2 encapsulation types that can be carried over the AToM network today are: Frame Relay, ATM, PPP, HDLC Ethernet and 802.1Q. In particular, Ethernet porting over the MPLS backbone has had a successful growth nowadays. Anyway AToM hesitates in this part that it carries the Ethernet frame over the MPLS backbone in a point-by-point style. Virtual Private LAN Service (VPLS) allows the transmission of Ethernet frames in a point-to-multipoint style. [2] VPLS is basically a Layer 2 service that emulates a LAN over the MPLS enabled network. The first implementation of VPLS on Cisco IOS was in 2004 on the 7600 platform in Cisco IOS 12.2 (17d) SXB.

1.2. Definition of MPLS

1.2.1. Multiprotocol Label Switching

MPLS (Multiprotocol Label Switching) is a mechanism in high performance telecommunications networks that directs and carries data from one network node to another with the help of so-called "labels". MPLS simplifies the creation of "virtual connections" between remote nodes and can also encapsulate a variety of network protocols. [5]

1.2.1.1. MPLS tags

MPLS tags are predefined between routers so they can build a tag-on-tag map. These tags are attached to the IP packets causing the router to transmit traffic based on this tag and not based on the destination IP address. Packets are transmitted by label transfer and not by IP. The technique of label-based transmission is not new. Frame Relay and ATM use this technique to move frames or atm cells on the network. In Frame Relay frames can have any type of length, while in ATMs the cells have a well-defined length and are composed of a 5-byte head and a payload of 48 bytes. The head of an ATM cell and the Frame Relay frame refers to a virtual circuit that the cell or frame must traverse to get to the destination. [6] The similarity between Frame Relay and ATM is that in each jump across the network the value of the "label" on the header changes. This is different from transfer based on IP addresses, as in the latter we have no change of IP address when transferring the packet to the destination node. The fact that MPLS tags are used to transfer packets and not their IP addresses has led to the popularity of MPLS. These benefits are addressed below.

1.3. Advantages of MPLS

MPLS like any other technology has its benefits and advantages, but also its disadvantages. In the first place, the benefits should be evaluated as they are the main criteria for evaluating a new technology before implementation by different companies in the market. [7] The benefits of MPLS are:

- Use of a unified network infrastructure Better IP integration over ATMs
- BGP (Border Gateway Protocol) - free core
- Peer-to-peer model for MPLS VPN Optimal traffic flow
- Traffic Engineering

1.3.1. Use of a unified network infrastructure

The idea of MPLS is to label all incoming packets based on their destination address or other predefined criteria and to transfer traffic over a common infrastructure. This is a huge advantage of MPLS. One of the reasons why IP became the dominant protocol was because many technologies can be transported through it, not only data but also the phone is transferred over IP.

Using MPLS with IP expands the possibility of what can be transported over the network. By adding labels to packages, this makes it possible to maintain protocols other than IP over the third-layer IP-MPLS backbone, similar to what was possible with Frame Relay and ATM in the second layer. MPLS can transport IPv4, IPv6, Ethernet, High-Level Data Link Control (HDLC), PPP and other second-tier technologies. [8]

The above feature through which each second layer frame is held along the MPLS backbone is called AnyTransport over MPLS [AToM]. Routers that transfer AToM traffic do not need to be informed about MPLS "load"; they just need to transfer the labeled traffic by looking at the label at the beginning of the packages. Basically labeled MPLS transfer is a simple method to transfer many different protocols over a network. There should be a transfer table, which contains the input labels which will be exchanged with the output labels and the other hop. So AToM allows the service provider (Service Provider) to provide the same second tier service to the customer as with any non-MPLS network and at the same time, the service provider only needs a unified network infrastructure for keep all types of client traffic.

1.3.2. Better IP integration over ATMs

In the past decade IP has won the battle with all third-tier network protocols such as AppleTalk, Internetwork Packet Exchange (IPX), and DECnet. IP is relatively simpler and present as a single type. A very advanced protocol at the time in the second tier was ATM. However, the idea that an ATM was a bottom-up or desktop-to-desktop protocol never occurred. ATM was a huge success, but its success was limited by its use as a WAN protocol in the service provider's network core. [9]

Many service providers distribute IP backbone. Several solutions were proposed to better integrate IP over ATMs. One solution was to implement IPs over ATMs based on the well-known RFC 1483 “Multiprotocol Encapsulation over ATM Adaptation Layer 5,” which specifies how to encapsulate protocols. multiple routing or bridges over the ATM adoption layer (AAL). In this solution the ATM circuits are set manually and the routes between the other IP hop and the ATM endpoint must be manually configured for each ATM placed on the network.

Another way is to implement LAN emulation (LANe). Ethernet is a very popular second-tier technology on the network, but it has never achieved the scalability and security required by SPs (service providers). [10] LANE in the basic concept makes the network look like an emulated ethernet network, which means that many ethernet segments are connected to each other as if the ATM WAN in the middle was an ethernet switch.

Eventually the Multiple ATM Protocol (MPOA), which is a specification from the ATM forum, provides the closer but also more complex IP integration over ATMs. All of these methods were unsuitable for implementation and improvement. A good solution for IP integration over ATMs was one of the main reasons for establishing MPLS. The requirements for MPLS over ATMs were to make ATM transfer more intelligent. The

ATM transfer had to be executed over an IP routing protocol and implement a labeled delivery protocol. [11]

1.3.3. BGP – Free Core

When the Service Provider's IP network needs to transfer traffic, each router must look at the destination IP address of the packet. If the packet must be transferred to a destination located outside the SP network then the external IP prefixes must be present in the routing table of each router. BGP maintains external prefixes such as client prefixes or Internet prefixes. This means that all routers in the Service Provider network must execute BGP. [12]

MPLS transfers packets by looking at the labels and not their IP addresses. MPLS allows the label to be associated with an outbound router instead of the packet destination IP address. The label summarizes all the information about which terminal output routers the packet should transmit and this information is attached to the packet. The kernel router no longer needs to rely on the IP address to transfer packets and so the kernel routers in the SP network no longer need BGP execution. [13]

The router at the edge of the MPLS network still needs to see the packet IP address, so it still needs to execute BGP. Each BGP prefix on MPLS incoming routers has a BGP IP address of the other hop associated with it. This BGP IP address of the other hop is an IP address of the MPLS output router. The tag associated with the IP packet is a tag associated with this BGP IP address of the other hop. Since each kernel router transfers packets based on the MPLS tag attached to the packet, which is associated with the BGP IP address of the next step, each BGP IP address of the next step of the MPLS output router must be recognized by all kernel routers . Any internal routing protocol like OSPF or ISIS can do the job.

An ISP (Internet Service Provider) that has about 200 core routers in its network must execute BGP across all of its 200 routers. If MPLS is implemented on the network only edge routers, which may be 50 need to execute BGP.

All routers in the network kernel transfer labeled packets regardless of IP address, so they are no longer forced to execute BGP. Given that the entire network has about 150,000 routers then the lack of obligation to execute BGP in each of them is an important consideration. Routers without the full routing table need less memory, and kernel routers can work without having to execute BGP. [14]

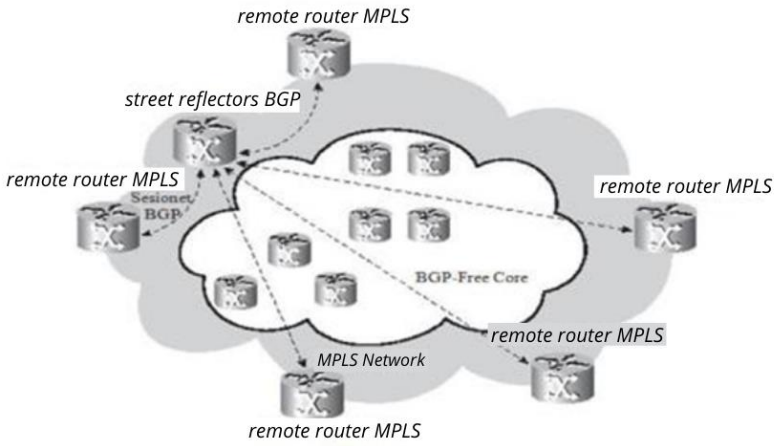


Figure 1. MPLS Network BGP Free Core

1.3.4. Peer-to-peer VPN model versus VPN overlay model

A VPN is a network that simulates a private network over a shared infrastructure. The private network requires that all customers be able to connect and be completely separate from any other type of VPN. The VPN usually belongs to a company which has a number of interconnected locations along the common SP infrastructure. SPs can distribute two types of VPN models that provide VPN services to their clients:

- Overlay VPN model
- Peer to peer VPN model

1.3.4.1. Overlay VPN Models

In the overlay model SP supplies a point-to-point or virtual circuit connection service across its network between client routers. Client routers form peer routing between them directly via connection or virtual circuits from the SP. Routers and switches hold client data across the SP network, but no peer routing occurs between an SP router and a client. [15] The result of this is that SP routers never see the client routing. This point-to-point service can be of layer 1, 2 or 3.

Examples of layer 1 are: TDM E1, E3, SONET and SDH connections. Examples of layer 2 are virtual circuits created by X.25, ATM or Frame Relay. Figure 1.2 shows an example of an overlay network built on Frame Relay. In the SP network are Frame Relay switchers who place virtual circuits between client routers at the ends of the Frame Relay network.

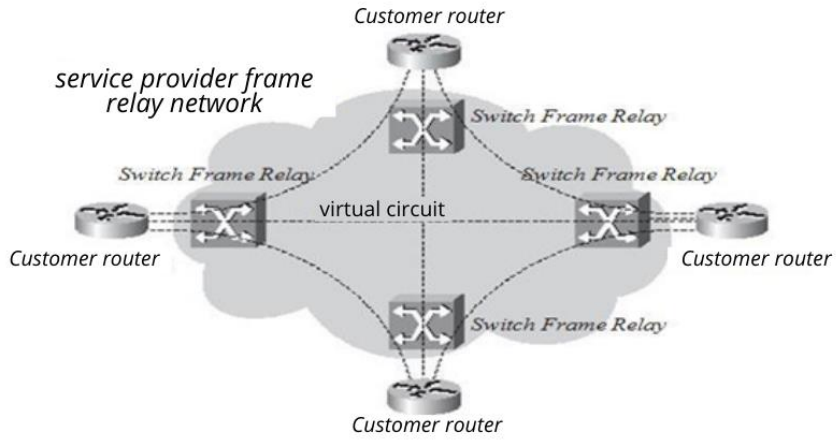


Figure 2. Overlay network in frame relay

Considering layer 3 routing (IP) and peer-to-peer from the client's point of view, the client routers appear to be directly connected. Figure 3 shows this:

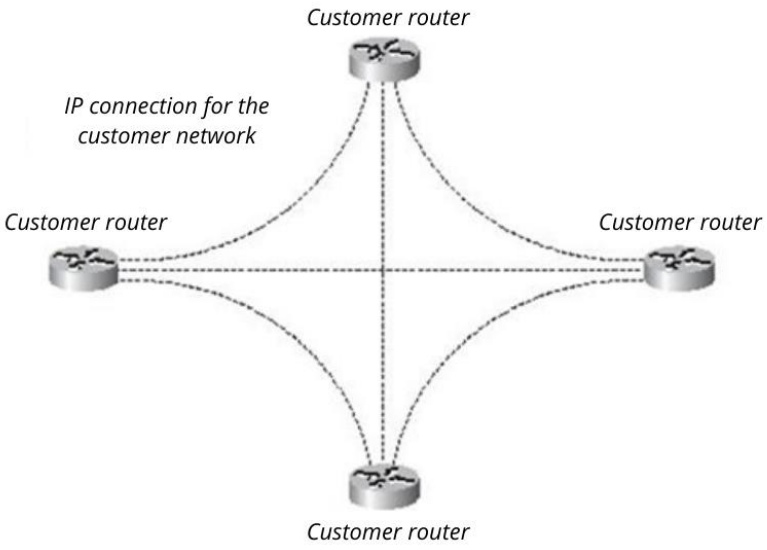


Figure 3. Overlay network: Customer peer routing

Overlay service can also be provided in Layer 3 IP protocol. The common tunnels used to build the overlay network over IP are GRE (Generic Roting Encapsulation) tunnels. These tunnels encapsulate traffic with a GRE header and an IP header. The GRE header shows, among other things, what the transport protocol is. IP header is used to route packets across the SP network. Figure 1.4 shows an example of an overlay network with GRE tunnels. One advantage of GRE tunnels is that they can route traffic in addition to IP traffic. It is possible to use IP sec over GRE tunnels and thus provide security through data encryption.

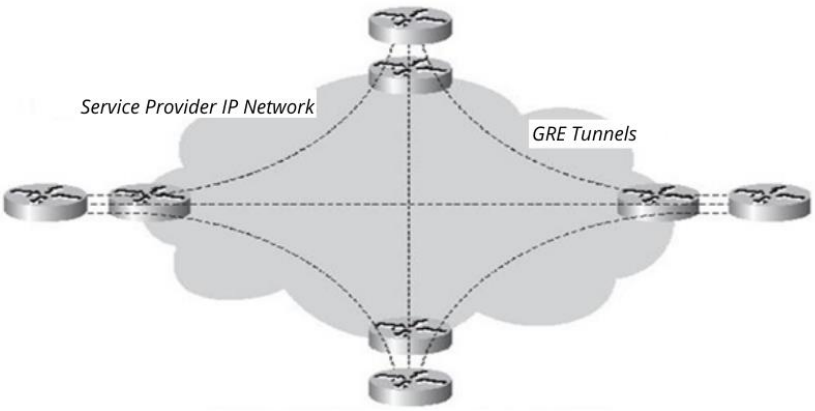


Figure 4. Overlay network in GRE Tunnels

1.3.4.2. Peer-to-peer VPN model

In the VPN model peer-to-peer, the SP routers carry client data across the network, but they also participate in user routing. In other words, SP routers connect directly to the client layer 3 routers. The result is that a proximity or neighborhood routing protocol exists between the client and the SP router. Figure 1.5 shows the concept of the peer-to-peer VPN model. [16]

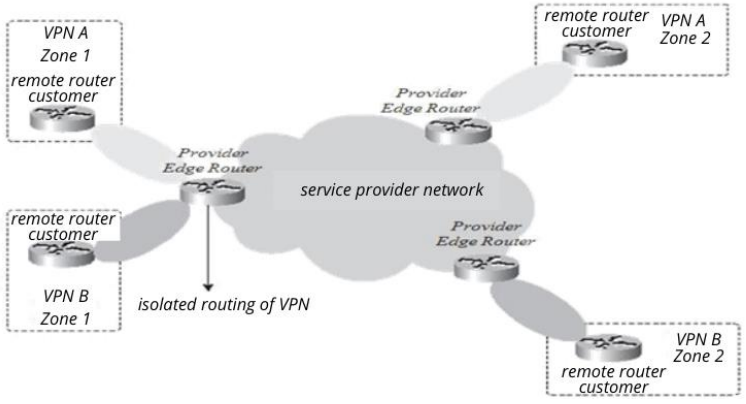


Figure 5. Peer-to-peer VPN Model

Before MPLS existed, the peer-to-peer VPN model could be achieved by creating an IP peer route between the client and the SP routers. The VPN model required privacy or isolation between different clients. This could be achieved by configuring packet filters (access list) to control the data going in or out of the client routers. One way to achieve some form of security was to warn the road or stop the road from being warned on the way to the customer. Another possibility was to implement both methods simultaneously.

Before it was MPLS, the overlay VPN model was more distributed than the peer-to-peer VPN, but it required more supplies because to add a new client many configurations had to be made in different parts. The peer-to-peer model did not have these problems. MPLS VPN is an MPLS application that made the peer-to-peer VPN model easier to implement. Adding or removing a client is easier to configure and requires less time and effort. With MPLS VPN a client router called CE (costumer edge router) connects to the IP layer at least one SP router called PE (provider edge router).

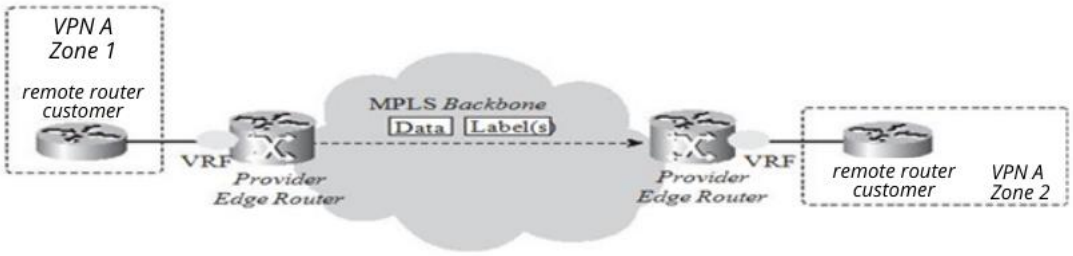


Figure 6. MPLS VPN with VRF

MPLS VPN privacy is ensured using the virtual routing and forwarding (VRF) concept and the fact that data is transferred to the backbone as a labeled packet. VRF ensures that information routing from different clients is kept separate while MPLS in the backbone ensures that packets are transferred based on the information on the label and not on the IP header. Figure 1.6 shows the concept of VRF and labeled packet transfer to the backbone of a network running MPLS VPN. Figure 1.7 shows the concept of the peer-to-peer VPN model applied to MPLS VPN.

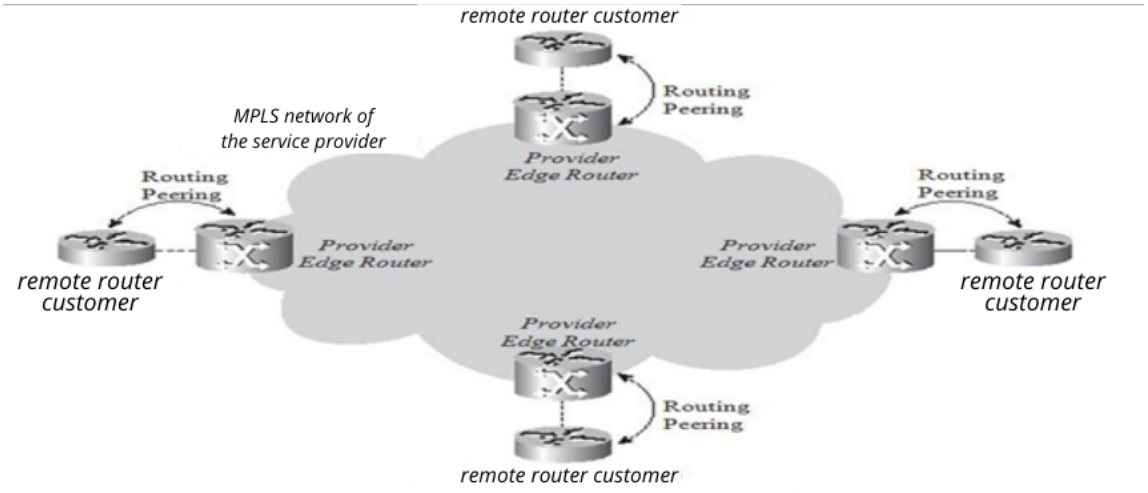


Figure 7. Peer-to-peer MPLS VPN Model

Adding a new client means that only the connection to the CE router should be added to the PE router. It is not necessary to create virtual circuits as in the VPN overlay model or to configure packet filters or routing filters with the peer-to-peer VPN model over the IP network. This is the best MPLS VPN for SP.

Many SP clients have a hub-and-spoke network, while others have a "full mesh" network around the SP backbone. While some others have something secondary. The benefits of MPLS VPN for the client are at a maximum when the client has a full mesh network. We refer to Figure 1.2 to see a full mesh client network around a Frame Relay network and compare it to the same client network with MPLS VPN in Figure 1.7. In Figure 1.2 each client router is connected to n-1 router routers of other clients, where n is the total number of client routers. In Figure 1.7 each client router is connected to only one SP router. Another good thing about SP is that it only needs to provide a connection between the PE and CE router. With the overlay model the SP must provide a connection or a virtual circuit between the parts. It is much simpler to predict traffic and also bandwidth requirements for one part than to completely predict the traffic pattern between

all parts of the client. The disadvantages of the peer-to-peer VPN model compared to the VPN overlay model are:

The client must share the responsibility of routing with the Service Provider
to the SP end devices have an added load

- The first disadvantage is that the client must have a routing connection with the SP. The client no longer controls its network end to layer 3 thanks to IP routing as with the overlay model.

- The second disadvantage is for the SP. The load for the SP is in addition to the terminal equipment, to the PE router. The SP is responsible for the routing and convergence of routing for the client network because PE routers must be able to maintain all client routers ensuring continuous routing convergence over time.

1.3.5. Optimal traffic flow

Since ATM and Frame Relay switchers are layer 2 devices, routers are interconnected through them, ie through the virtual circuits created between them. For each router to start traffic to any other remote router a virtual circuit must be created directly between them. Creating virtual circuits manually is tedious. In any case if it is required that all the parts be connected to each other there should be a network of virtual full mesh circuits between the parts, which is tedious and expensive. If the parts are connected as in figure 1.8 the traffic from CE1 to CE3 should first go to CE2. The result is that traffic passes to the ATM backbone twice and follows a transverse path to the CE2 router. Using MPLS VPN flows directly, in the most optimal way between clients of different parts. For traffic to flow normally between parts in the case of a VPN overlay model, all parts must be interconnected requiring a "full mesh" connection or virtual circuit design.

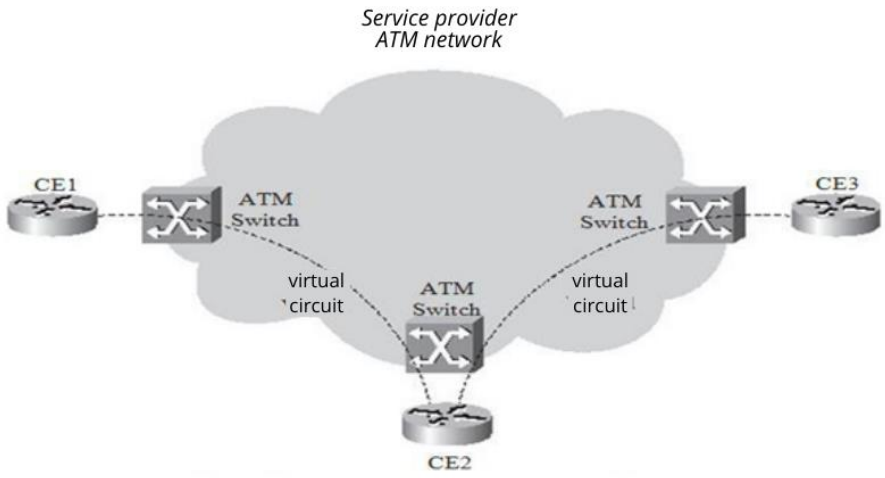


Figure 8. ATM overlay network no "Fully Meshed"

1.3.6. Traffic Engineering

The basic idea behind traffic engineering is the optimal use of network infrastructure including connections that are less used because they are not part of the preferred route. This means that traffic engineering must provide the ability to extend network traffic to different routes from preferred routes, which is the least costly route provided by IP routing. The least cost route is the shortest route calculated by the dynamic routing protocol. With traffic engineering implemented in the MPLS network we can have a traffic flow destined for a specific prefix or with a specific service quality from point A to point B through a route, which is different from the lower cost route. The result is that traffic can be spread more evenly over available connections on the network and making those connections that are less used on the network more usable. Figure 1.9 shows such an example:

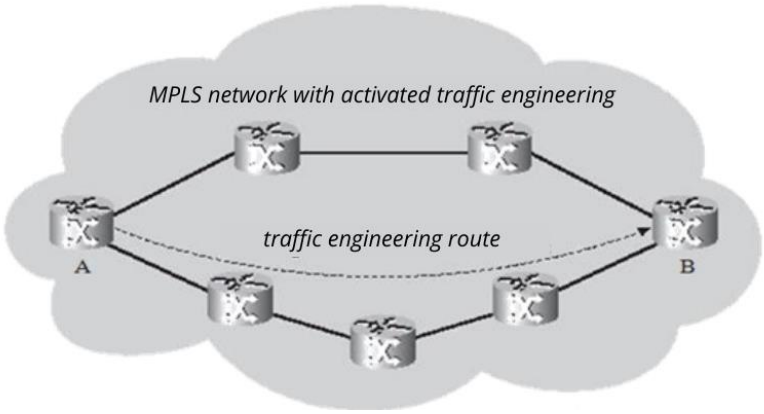


Figure 9. Traffic engineering - Example 1

As an MPLS network operator with executed traffic engineering it is possible to distribute traffic from A to B over the bottom road, which is not the shortest route between A and B (4 steps down versus 3 steps up the road) . Traffic in this network goes to the bottom path by changing the routing protocol matrices. Consider Figure 1.10:

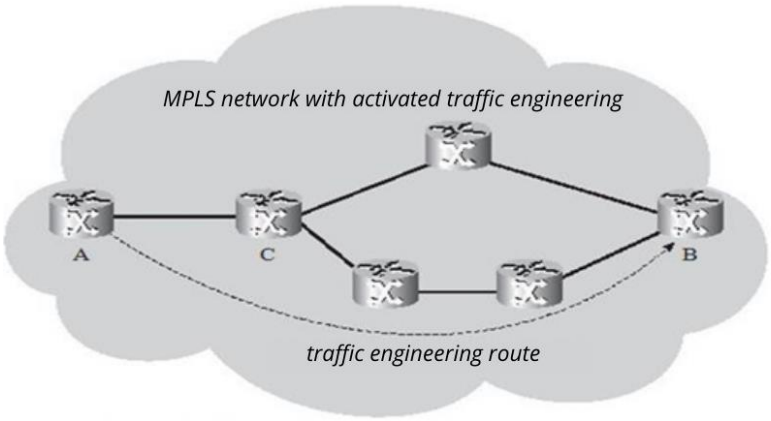


Figure 10. Traffic engineering - Example 2

This is an IP only network and it is not possible to pass traffic down the path by configuring something on router A. The router's decision to pass traffic down or up is only the router's decision C. If traffic technology is enabled MPLS in this network, then router

A can pass traffic to router B via the bottom path, as it is this technology which forces router C to pass traffic between AB to the bottom path. This is possible due to the label transfer mechanism. The road head end router in this traffic technology, which is router A, is the router that specifies the full path that traffic will carry on the MPLS network. And since it is this router that specifies the full path, then we refer to traffic technology as source-based routing. The label, which is attached to the packet by the remote head router, causes this packet to pass through that path as specified by this router. No intermediary router transmits the packet to other routes. A major advantage of MPLS traffic technology is the ability for fast re-routing (FFR). FFR allows tag traffic to be re-routed around a connection or router which has become unusable and this happens in less than 50ms, which is very fast time by today standards.

1.4. False advantages

One of the first reasons for a labeled protocol was the need for speed. The transfer of packets by IP to a CPU was considered to be lower than the transfer of packets based on labels, as it was sufficient to look only at the label at the top of the packet. A router further transfers a packet by looking at its destination IP address in the IP header and finding the most suitable path for that packet. This foresight depends on the implementation of a specific "vendor" on the router. However since the IP address can be unicast or multicast and has 4 octets, farsightedness can be complex.

A complex foresight implies that the decision to further transfer the IP packet may take time. Some people think that foresight based on the value of a label on a spreadsheet may be a faster way to transfer packages than it is based on IP addresses, but advances in IP addressing technique have made this argument somewhat suspicious. Today the connections in the routers have a bandwidth that goes up to 40 Gbps. A router that has some high-speed connections will not be able to make the transfer of IP packets simply based on the CPU decision, as the CPU mainly deals with the control plan. The control

plan is a set of portals that helps to place data in the transfer plan. The main components of the control plan are routing protocols, routing tables, and other controls or signal protocols used to supply the data plan. The data plan is the path that packets follow when transferring across a router or switch. The data transfer or transfer plan is located on specific built-in hardware or integrated application-specific circuits (ASICs). The use of ASICs in the router transfer plan has led to the transfer of IP packets just as fast as tags. So the reason for implementing MPLS in the network as a consequence of high speed is a false reason.

CHAPTER 2

MPLS ARCHITECTURE

2.1. Introduction to MPLS tags

An MPLS tag is a 32-bit field with a definite structure. Figure 2.1 shows the syntax of an MPLS tag. In an MPLS tag the first 20 bits are the label values. This value can be between 0 and 220–1, or 1,048,575. Anyway the first 16 values are released from normal use; they have a special meaning. Bits 20 to 22 are three experimental bits (EXP). These bits are used for quality of service (QoS) only. These three bits have been called experimental for historical reasons because at first no one knew what they would be used for.

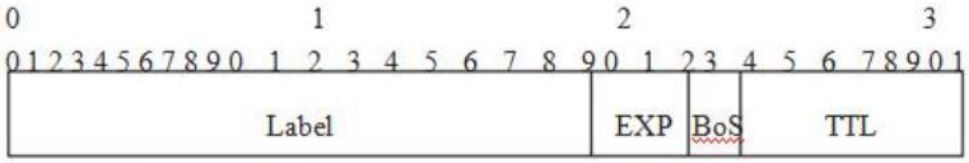


Figure 2.1 Syntax of an MPLS tag

Figure 11. Syntax of an MPLS tag

The 23rd bit is the last bit of the BoS (Buttom of Stack) stack. It is 0, unless it is the end of the label on the stack. If this happens BoS becomes 1. The stack is the collection of labels, which are located at the top of the package. The stack may even consist of just one package or there may be many. The number of labels (which is the 32 bit field) that can be found on the stack is unlimited, however you can rarely see a stack that has 4 or

more labels. Bits 24 to 31 are the eight bits used for TTL (Time To Live). This TTL has the same function as the TTL found in the IP header. It decreases by 1 in each step and its function is to avoid a packet getting stuck in a routing loop. If a routing loop occurs and no TTL is present, the packet leaks into the loop permanently. If the TTL of the label reaches 0 then it is discarded.

2.1.1. Label Stacking

Capable MPLS routers may need more than one tag at the packet header to route packets over the MPLS network. This is done by packing the labels in "stacks". The first label on the stack is called the top label and the last label is called the bottom label. There may be a number of labels between them. Figure 2.2 shows the structure of the label stack.

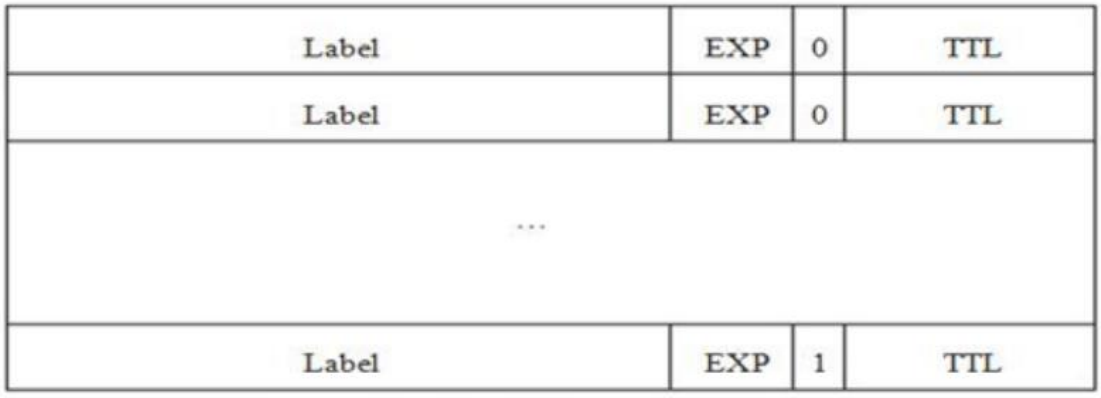


Figure 12. Stack of labels

Note that the stack label in Figure 2.2 indicates that the BoS bit is 0 for all labels except the bottom label for which the BoS bit is 1. Some MPLS applications currently need more than one label in the label stack to transfer labeled packages. Two examples of MPLS applications are MPLS VPN and AToM, which place both tags on the tag stack.

2.1.2. Coding of MPLS

Where does this label stand? -> The label stack is placed on top of the Layer 3 package, before the transport protocol header, but after the Layer 2 header. Because of its location, the MPLS label stack is often called the shim header. Figure 2.3 shows the location of the label stack for labeled packages.

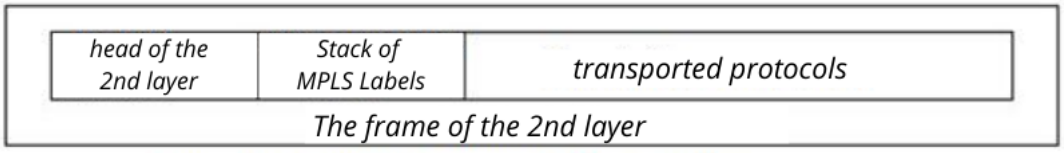


Figure 2.3 Encapsulation for labeled packages

Figure 13. Encapsulation for labeled packages

Layer 2 connection encapsulation can be any type of encapsulation that Cisco IOS supports: PPP, HDLC (High-Level Data Link Control), Ethernet, and so on. Assuming the transport protocol is IPv4 and the binding encapsulation is PPP, the label stack is present after the PPP header but before the IPv4 header.

Since the label stack in the Layer 2 frame is placed in front of the Layer 3 header or other transport protocols, new values must be created for the data link layer's protocol field, indicating what follows the layer 2 header is a packet labeled MPLS. The data link layer protocol field is a value that indicates what type of payload the layer 2 frame is holding.

ATM uses a unique way of encapsulating labels. For Frame Relay, the NLPID (Name Layer Protocol Identifier) is 0x80 indicating that a SNAP IEEE (Subnetwork Access Protocol) header is used and it is used here to tell the recipient what the Frame Relay protocol carries. The SNAP header contains an OUI (Organizationally Unique

Identifier) of type 0x000000 and an Ethertype of type 0x8847 indicating that the transport protocol is MPLS. The transport protocol can theoretically be any type; Cisco IOS supports IPv4 and IPv6. In the case of AToM, the transport protocol can be any of the most popular second layer protocols such as: Frame Relay, PPP, HDLC, ATM and ethernet.

2.2. MPLS and OSI reference model

The OSI reference model consists of seven layers. The OSI model is shown in Figure 2.4. The bottom layer is layer 1 or the physical layer and the top layer is layer 7 or the application layer. The physical layer is connected to the cable and to the mechanical and electrical characteristics. The second layer is the data link layer, which is centered on the frame format. Examples of the data link layer are Ethernet, PPP, HDLC and Frame Relay. The importance of the data link layer is only in a line between two machines, but no further. This means that the data link layer header is replaced by the machine on the other side of the link. The third layer, the network layer is concentrated in the end-to-end packet format. It has value beyond the data link. The best known example of protocols operating in the third layer is IP.

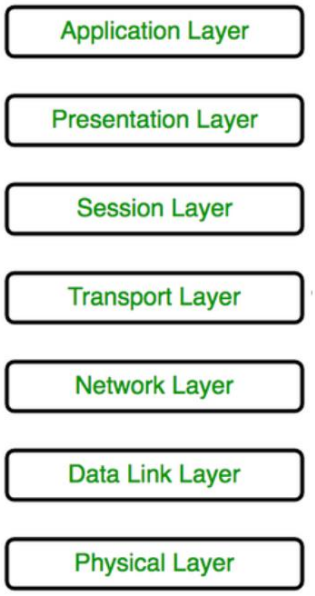


Figure 14. OSI Model

What adjustment does MPLS make in the meantime? MPLS is not a Layer 3 protocol because Layer 2 encapsulation is still present with labeled packets. MPLS is also not a second tier protocol because the third tier protocol is still present. So MPLS does not fit so well in the OSI layered model. Perhaps the best way is to view MPLS as a layer 2.5 protocol.

2.3. Label Switch Router (LSR)

A Label Switch Router (LSR) is a router that supports MPLS. It is capable of understanding MPLS tags and receiving and transmitting a tagged packet to the data link layer. There are three types of LSRs in the MPLS network:

- Igress LSR - waits for a package that has not been tagged yet, puts the tag at the top of the packet and launches it in the data link layer

- Egress LSR - cuts labeled packages, removes the label and launches them in the data link. Ingress LSR and Egress LSR are extreme LSRs.

- Intermediate LSR - Medium LSR, takes the labeled packets, performs an operation on them,
transfers packets and sends the packet to the data link correctly.

An LSR can do all three operations: insert, push or shift. He must be able to insert one or more tags (remove one or more tags from the head of the tag stack) before transferring the packet out of it. An LSR must be able to push one or more labels into the label stack and transfer the packet out. If the package is not yet labeled, LSR creates a label stack and pushes it towards the package. An LSR must be able to change a label. This means that when a tagged packet is received, the top tag of the tag stack is replaced with a new tag and the packet is transferred to the output of the data link.

An LSR that pushes labels toward unlabeled packets is called an imposing LSR because it is the first LSR to label a package. One such LSR that is imposing is an ingress LSR. An LSR that removes all tags from labeled packets before packets are transferred is called an LSR remover, and these are LSR egress. In the case of MPLS VPN, LSR ingres and egres are terminal security routers (PE). Intermediate LSRs are referred to as security routers (P). The term PE and P routers have become so popular that they are used even when the MPLS network does not work on the MPLS VPN.

2.4. Label-Switched Path (LSP)

The label switched path LSP is a sequence of LSRs that transfers the labeled packet to the MPLS network or part of the MPLS network. In the basic sense LSP is the path that packets follow in the network. The first LSR of the LSP is an ingress LSR (ingress LSR) for that LSP, while the last LSR is the exit LSR (egress LSR). All LSRs between the input and output LSRs are medium LSRs.

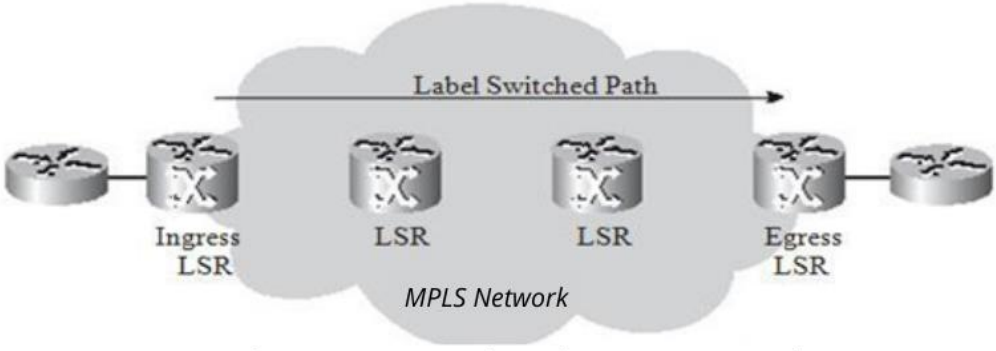


Figure 2.5 An LSP through an MPLS network

In Figure 2.5 the arrow at the top indicates the direction because the LSP is one-way. The flow of labeled packets in other directions such as. from right to left among the same extreme LSRs would be another LSR. The LSR of an LSP entry is not necessarily the first router to label a packet. The package may be pre-labeled by a predecessor LSR. Such a case is called a nested LSP, which is an LSP within an LSP. Figure 2.6 shows a LSP lying horizontally across the width of the MPLS network. Another LSR starts at the third LSR and ends at the next LSR at the end. Thus, when the packet enters the second LSP in its input LSR (this means the third LSR), it is already labeled. The nested LSR input LSR then pushes a second label towards the packet. Now the package label stack in the second LSP has two labels. The top label belongs to the nested LSP and the bottom label belongs to the LSP that surrounds the entire MPLS network. A TE (backup traffic engineering) tunnel is an example of a nested LSP.

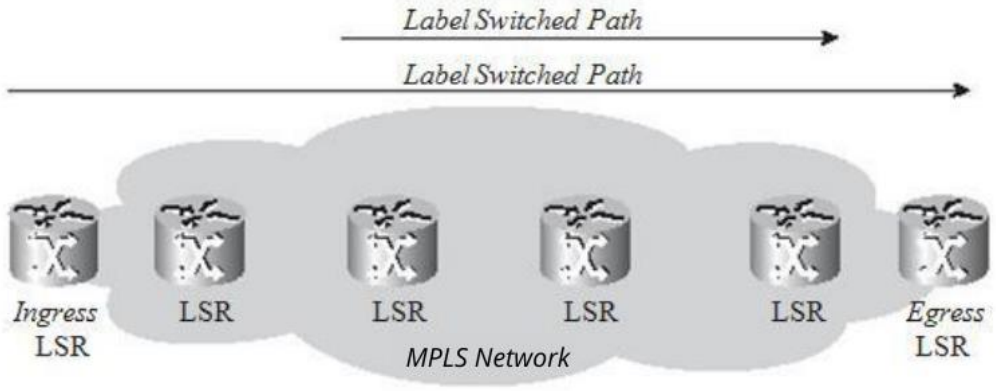


Figure 15. Nested LSP

2.5. Forwarding Equivalence Class (FEC)

An FEC (Forwarding Equivalence Class) is a group or flow of packets, which are transmitted through the same path and treated equally thanks to the transmission care. All packages belonging to the same FEC have the same label. However, not all packages with the same label belong to the same FEC because their EXP values may be different. Care for transmission may be different and so they may belong to a different FEC. The router that decides which FEC each packet belongs to is the incoming LSR. This is logical because the incoming LSR classifies and labels packets. Some examples of FEC are:

- Packets with IP address (layer 3) as destination address have a certain prefix Multicast packages belonging to a certain group
- Packets with the same transmission care based on precedent or IP DSCP (DiffServ Code Point)

- Frames (layer 2) carried along the MPLS network received at a VC or interface to the incoming LSR and transmitted over a VC or at an interface to the outgoing LSR.
- Packets with destination IP address (layer 3) belonging to a set of BGP (Border Gateway Protocol) prefixes all with the same BGP in the next step.

The latest FEC example is a very interesting example. All packets in the incoming LSR for which the destination IP address points to a set of BGP routes in the routing table (all with the same BGP address in the next step) belong to the same FEC. This means that all packets entering the MPLS network receive a label depending on how the BGP of the next step is. Figure 2.7 shows an MPLS network in which all terminal LSRs execute an internal BGP (iBGP).

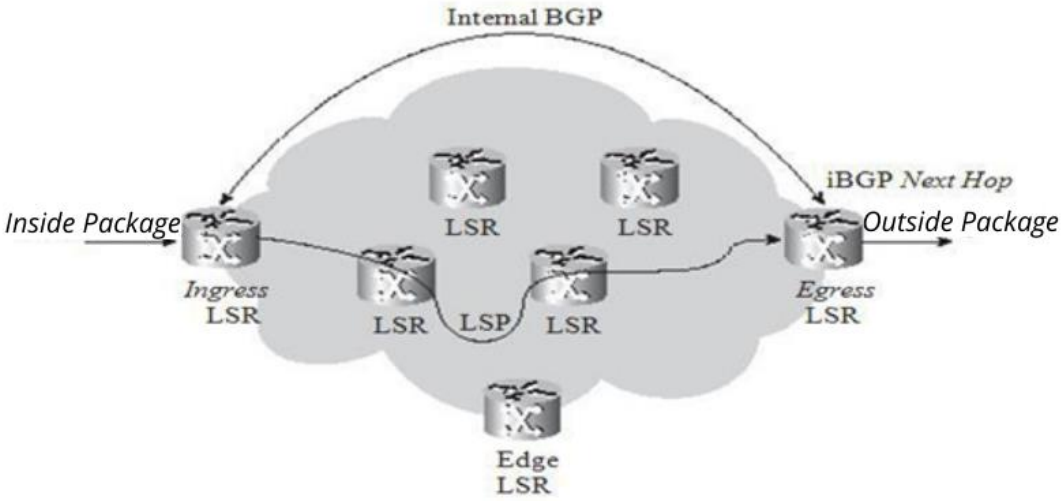


Figure 16. An MPLS network that executes iBGP

The destination IP address of all IP packets entering the incoming LSR will be set in the IP transmission table. All of these addresses belong to a set of prefixes, which are known in the routing table as BGP prefixes. Many BGP prefixes in the routing table have the same BGP address of the next step, designated as an output LSR. All packets with destination IP address for which the IP setting in the routing table belongs to the same

BGP address of the next step will be mapped to the same FEC. All packages belonging to the same FEC receive the same label imposed by the same incoming LSR.

2.6. Distribution of labels

The first label is placed on the incoming LSR and the label belongs to a single LSP. The packet path through the MPLS network is connected to a single LSP. The difference is that the top label stack label changes at every step. The incoming LSR places one or more labels on packets. The intermediate LSR changes the label of the receiving packet labeled (or as it is called the incoming label), switches this to another label, and then transmits the packet to the external connection. The LSP output LSR removes the labels from the LSP and transmits the packet further. Consider a clear example, IPv4 over MPLS, which is the simplest example of an MPLS network. IPv4 over MPLS is a network consisting of LSRs which execute an IGP (Internal Gateway Protocol) (for example Open Shortest Path First [OSPF], Intermediate System-to-Intermediate System [IS-IS] and Enhanced Interior Gateway Routing Protocol [EIGRP]). The incoming LSR looks at the destination IPv4 address of the packet, places a label, and transmits the packet further. The other LSR and any other intermediate LSR receives the labeled packet, replaces the incoming tag with an output tag, and transmits the packet further.

The output LSR removes the label and transmits the unlabeled IPv4 packet to the external connection. For this to work, nearby LSRs must agree on which labels to use for each IGP prefix. Thus, any intermediate LSR should be able to figure out which output label to replace with an input label. This means that a mechanism is needed to tell the router which labels to use to further transfer packets. Tags are local to any nearby router. Labels have no global meaning across the network. For nearby routers to agree on which label to use for each prefix, they need some form of communication between them; in contrast, routers do not know which output tag to put in front of each input tag. So you need a protocol for distributing labels.

Labels can be distributed in two ways:

- Platform transport of labels over an existing IP routing protocol
- Have a separate protocol for distributing labels

2.6.1. Platform transport of labels over an existing IP routing protocol

The first method has the advantage that it is not necessary to execute a new protocol on the LSR, but any existing IP routing protocol needs to be extended to hold the labels. This is not always an easy thing to do. The biggest advantage of having a routing protocol to keep labels is that the routing and distribution of labels is always synchronized, which means that a label can not exist if the prefix is missing or vice versa. This also eliminates the need for another protocol to be executed over the LSR, which distributes the labels. Implementation for remote vector routing protocols (like EIGRP) is regular because each router originates a prefix from its routing table. The router then simply connects a label to a prefix. Connection state routing protocol (like IS-IS and OSPF) does not work this way. Each router creates updated state connections, which are then transferred unchanged from all routers within the area. The problem is that for MPLS to work, each router needs to distribute a label for each IGP prefix (even routers that are not creators of those prefixes). Connection state routing protocols need to be increased immediately to be able to do so. The fact that a router needs to announce a label for a prefix, which it does not create itself, is against the intuitive way in which the connection state routing protocol works. Thus, for the link state routing protocol a separate protocol is preferred to distribute the labels.

None of the IGPs has been changed to establish the first method. However, BGP is a routing protocol that can maintain prefixes and distribute labels at the same time. However, BGP is not an IGP; it is used to hold external prefixes. BGP is used primarily for the distribution of tags on the MPLS VPN network.

2.6.2. Execute a separate protocol to distribute labels

The second method has the advantage of being an independent routing protocol. Whatever the IP routing protocol, whether it is capable of distributing tags or not, a separate protocol distributes the tags and lets the routing protocol distribute the prefixes. The disadvantage of this method is that a new protocol is needed in LSR. The choice of local routers was to have a new label distribution protocol to distribute labels for IGP prefixes.

This is LDP (Label Distribution Protocol), which is not the only protocol capable of distributing MPLS tags. Some other protocols that distribute labels are:

- TDP (Tag Distribution Protocol)
- LDP (Label Distribution Protocol)
- RSVP (Resource Reservation Protocol)

TDP, which precedes LDP, was the first label delivery protocol developed and implemented by Cisco. Anyway TDP is owned by Cisco. The IETF later formalized the LDP. LDP and TDP are similar in the way they operate, but LDP has more functions than TDP. With the rapid spread of LDP on the Cisco IOS model, TDP was quickly replaced by LDP. The result is that TDP is obsolete. Distribution of labels by RSVP is used only for MPLS TE.

2.6.3. Distribution of labels with LDP

For each IP IGP prefix in the IP routing table itself, each LSR creates a local connection; it associates the label with the IPv4 prefix. The LSR later distributes this link to all neighboring LDPs. Received connections become remote connections. Neighbors store these remote and local connections in a special LIB (Label Information Base) table. Each LSR has only one local connection for the prefix, at least when the label space is for the platform. If the label space is for the interface, a local labeled link may exist for the interface prefix. So we can have a prefix label or a prefix label for the interface, but the LSR takes more than one remote connection. It usually has more than one nearby LSR. Out of all remote connections for a prefix, the LSR needs to take only one and specify the output tag for that IP prefix.

The routing table sometimes called RIB (Routing Instance Base) defines what is the next step of the IPv4 prefix. The LSR uses the remote connection obtained from the downstream LSR, which is in the next hop in the routing table for that prefix. It uses this information to set its own LFIB (Label Forwarding Information Base) where the local link tag serves as an input tag and the single remote link tag selected by the routing table serves as the outbound tag. So when an LSR receives a labeled packet, it is capable of changing the input label given to it with the output label given by the nearest LSR of the other hop. Figure 2.8 shows the notification from the LDP of the connection between the LSR for the IPv4 prefix 10.0.0.0/8. Each LSR assigns a label to the IPv4 prefix where the local connection is this unique prefix and its associated label.

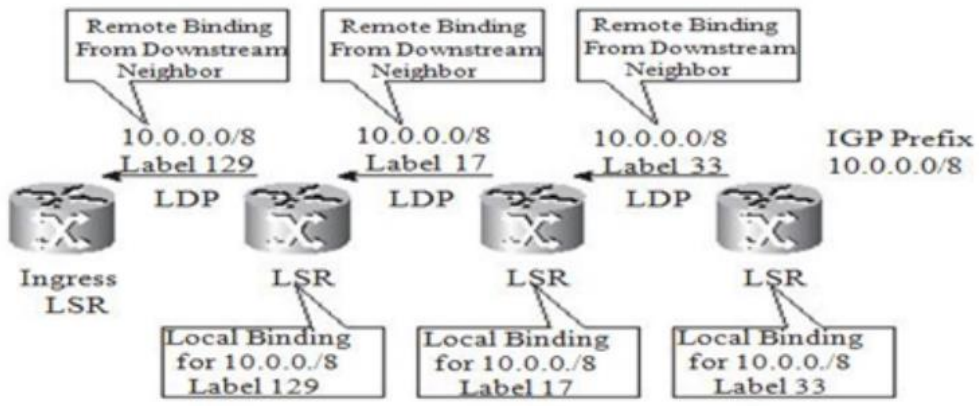


Figure 17. An IPv4 network over MPLS that executes LDP

Figure 2.9 shows the IPv4 packet (intended for 10.0.0.0/8) entering the MPLS network in the incoming LSR when it is labeled 129 and then transferred to the other LSR. The second LSR changes the input label 129 to the output label 17 and transfers the packet to the third LSR, which switches the input label 17 to the output label 33 and transfers the packet to the other LSR, and so on. On Cisco IOS, LDPs do not associate labels with BGP IPv4 prefixes.

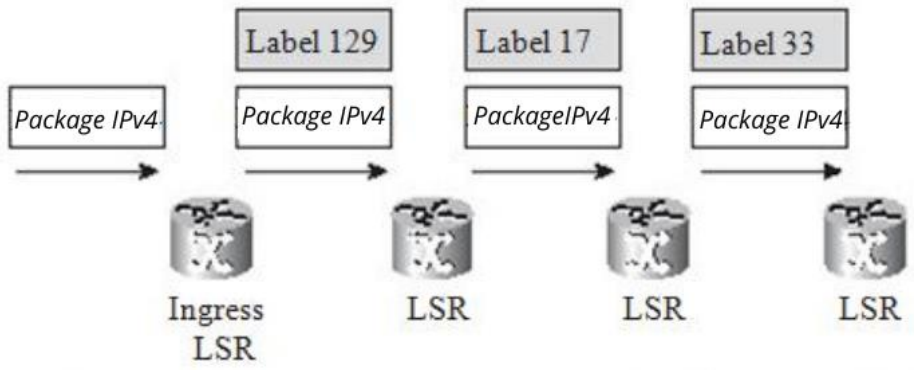


Figure 18. An IPv4 network over MPLS that executes LDP: packet transmission

2.6.4. Label Forwarding Information Base

LFIB is a table used to transfer labeled packets. It is populated with entry and exit labels for LSP. The input tag is a tag from the local connection to a separate LSR. The output tag is a label for the remote connections selected by the LSR from all possible remote connections. All these remote connections are found in LIB. LFIB selects only one of the possible output tags from all possible remote connections in LIB and installs it in LFIB. The remote label selected depends on which route is the best route found in the routing table. In the IPv4 example over MPLS, the tag is associated with an IPv4 prefix. However LFIB can be populated with labels which the LDP does not affix. In the case of MPLS traffic engineering, the labels are distributed by the RVSP, while in the case of the MPLS VPN the VPN labels are distributed by the BGP. In each case LFIB is used to transfer the labeled incoming packets.

2.6.5. MPLS Payload

The MPLS tag has no scope for identifying the network level protocol. This field is present in all Layer 2 frames to indicate what the Layer 3 protocol is. How does LSR know what the protocol is behind the label stack? or in other words, how does LSR know what MPLS Payload has ?? Many LSRs do not need to know because they will pick up a labeled package, change the label at the top, and launch the package at the exit line. This is a matter for intermediate LSRs or routers P. Intermediate LSRs do not need to know what the MPLS payload is because all the information needed to transfer the packet is known by looking only at the labels on the upper part. If the label stack consists of more than one label, the labels below the top one are not set by the LSR and thus the LSR has no knowledge of what they might be. Further, the LSR does not know what MPLS payload is shipped because the intermediate LSR only looks at the top label to make a broadcast decision and this is not a problem.

For the upper label-based transmission to be correct, the intermediate LSR must have a local and remote connection for the upper label. An outgoing LSR that removes all tags at the top of the package should know what MPLS payload is because it needs to transmit it further. The output LSR must know what value to use for the network level protocol identification field in the output frames. That outgoing LSR is the only one that makes that local connection, which means that it places a local label on the FEC and is the label used as an input label on the package. So the output LSR knows what the MPLS payload is by looking at the tags because it is the output LSR, which creates the tag link for that FEC and knows what the FEC is.

2.6.6. MPLS label spaces

In Figure 2.10, LSR A can report the L1 label for FEC 1 of LSR B and the L1 label for FEC 2 of LSR C, but only if LSR A can distinguish from which LSR the package labeled L1 was obtained. In case LSR B and LSR C are directly connected to LSR A via point-to-point connection, this can be easily achieved by implementing MPLS over LSR. The fact that the L1 tag is unique to the interface gives its name to the purpose of this tag: interface tag space. If the latter is used, the packet is transmitted not only based on the label, but based on both: the label and the input interface.

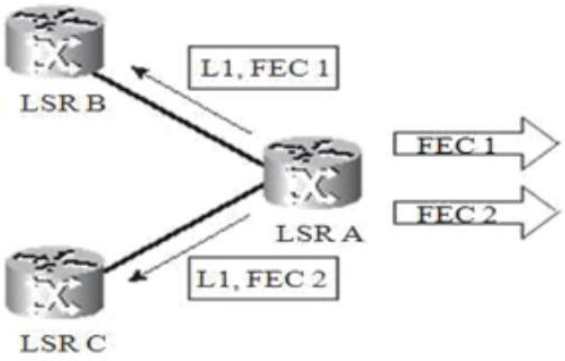


Figure 19. Interface label space

The other possibility is that the label is not unique to the interface, but over the LSR that labeled it. This is called the label space for the platform. In this case LSR A distributes FEC1 with the L1 label of LSR B and C as shown in Figure 2.11. When LSR A distributes a label for FEC 2, this label must be a different label from the L1 label. If the label space for the platform is used, the packet is transmitted based on the label, regardless of the input interface.

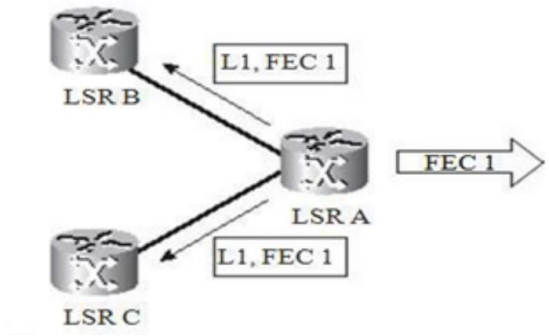


Figure 20. Label space for platforms

On Cisco IOS, all LC-ATM (Label Switching Controlled-ATM) interfaces have an interface label space, where all ATM frames (based or not) and ATM interfaces have a platform label space.

2.7. Different MPLS methods

An LSR can use different methods when distributing labels to other LSRs. There are three distinct ways:

- The Labels distribution method
- The Labels conservation method
- LSP control mode

Each mode has its own characteristics.

2.7.1. The Labels distribution method

The MPLS architecture has two ways of distributing tag links:

- The Labels distribution method DoD (Downstream-on-Demand)
- The Labels distribution method UD (Unsolicited Downstream)

In the DoD method, each LSR requires its next LSR step (which is downstream) over an LSP and a label link to that FEC. Each LSR receives a connection to the FEC only from the LSR downstream over that FEC. The downstream LSR is the other hop router shown by the IP routing table. In UD mode, each LSR distributes a link to its nearest LSR, without the label requirement of other LSRs. In UD mode, an LSR receives a remote tag connection from any nearby LSR. In the case of DoD, LIB indicates only one remote connection, whereas in the case of UD there is more than one. The way the labels are distributed depends on the interface and the implementation. On Cisco IOS, all interfaces except the LC-ATM interface use the UD mode of label distribution. All LC-ATM interfaces use the DoD method of label delivery. [17]

2.7.2. The Labels conservation method

Two ways of storing labels are possible:

- LLR Mode (Liberal Label Retention)
- CLR Mode (Conservative Label Retention)

In LLR mode, an LSR holds all incoming remote connections to the LIB. One of these connections is the remote connection taken from downstrem or the other hop for that FEC. The label from that remote connection is used in LFIB but none of the labels from other remote connections are placed in LFIB; so not all are used to transfer packets. Why not use the surrounding packages? Routing is dynamic on the network. At any time the routing topology may change (for example from a connection being broken or from a router being removed) so the router of the next hop for a particular FEC may change. At this time, the label for the next hop router is already in LIB and LFIB can be updated quickly with a new output label. [18]

The second way of keeping labels is the CLR method. An LSR being executed in this way does not store all remote connections in the LIB, but only stores those remote connections which are associated with the other hop LSR for a particular FEC. So in short, the LLR method provides a quick adaptation to routing changes, while the CLR provides fewer labels to store and a better use of the memory available on the router. In Cisco IOS, the holding mode for the LC-ATM interface is the CLR method. The LLR method is for all other types of interfaces.

2.7.3. LSP control method

LSRs can establish a local connection to an FEC in two ways:

- LSP standalone control method
- LSP sorted control method

The LSR can establish a local connection to an FEC independently of other LSRs. This is called the LSP independent control method. In this control method, each LSR establishes a local connection to a particular FEC once it recognizes the FEC. Usually this means that the prefix for an FEC is on the routing table. In the LSP-listed control method,

the LSR only creates a local connection to an FEC if it realizes that it is the output LSR for the FEC or if the LSR has received a label link from the other hop for that FEC.

The disadvantage of the LSP stand-alone control method is that some LSRs start labeling the transferred packets before the complete LSP is finally deployed; so the package is not transferred properly. If the LSP is not fully deployed, the package may not receive the necessary correction for transfer anywhere or may even be thrown away. An example of both control methods, the LDP can be viewed as a distribution method for IGP prefix label bindings. If LSRs are executed in the LSP independent control method, a local link for each IGP prefix will be placed in the routing table. If the LSR is executed in the LSP-listed control method, that LSR will only place a local label link for the IGP prefix, which is marked as linked in its own routing table, and also for the IGP prefix for which it is already has received a local connection to the other hop router (as noted in the routing table). Cisco IOS uses the independent LSP control method. ATM transfers that run on Cisco IOS use the LSP-listed control method as recommended. [19]

CHAPTER 3

TWO OF THE IMPLEMENTATIONS OF MPLS

3.1. MPLS and ATM Architecture

ATM is an oriented connection protocol, which was distributed by ITU-T. It is connection oriented because virtual circuits are signaled to hold ATM traffic. ATM traffic consists of a cell with a fixed size of 53 bytes, 5 bytes is the cell header and 48 bytes are cell data. ATM success was superior to WAN networks. Many locals built ATM transfers that could deploy virtual circuits on WANs. The advantages of ATM are as follows:

- A fixed-size package results in a low-jitter transmission
- QoS guaranteed
- High flexibility

The success of the ATM was limited to its use in WANs. Since IP became the standard network protocol used by everyone, many attempts were made to pass IP traffic over the core of the ATM network. Several schemes were compiled:

- Encapsulation based on RFC 1483
- Online emulation (LANE)
- Multiprotocol over ATM (MPOA)

RFC 1483 specified how to encapsulate highly routed or bound protocols over the ATM (AAL) compatibility layer. LANE specified how to hold the ethernet frames over the atm cloud. The MPOA provided close IP integration over ATMs, but it was a complex solution. None of these solutions was perfect to ensure a fit between IP and ATM. One of

the reasons for the introduction of MPLS was exactly this: a better integration of IP and ATM. With MPLS, the ATM transfer needed to execute an IP routing protocol and a label distribution protocol to exchange IP prefixes and labels between them and the router. The result would be that the IP overlay model over the ATM would no longer be needed. With MPLS, he became a peer model. [20]

3.1.1. Brief introduction of ATMs

An ATM cell is made up of a 5-byte header and the remaining 48 bytes are for data. The following figure shows the UNI ATM cell format.

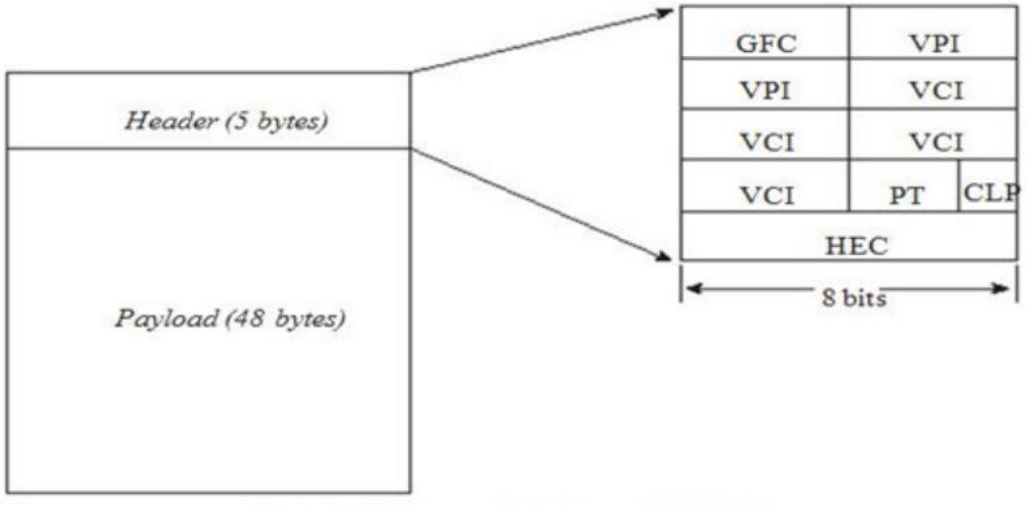


Figure 21. ATM UNI cell format

The cell format shown in the figure above is that of the UNI (User-Network Interface) cell. The NNI (Network-Node Interface) header is almost identical to this, except for the GFC field, which is forgotten. The VPI field occupies the first 12 bits and is 4 bits long, which allows the ATM transfer to place a large number of virtual path

identifiers (VPIs). The table below shows the names and meanings of each field of the ATM cell header.

Table 2. Fields of the head of the cell ATM

Field	*Name*	*Height bits)*	*Meaning*
GFC	*Generic Flow Control*	4	*Provides local functions*
VPI	*Virtual path identifier*	8	*Identifies the next destination of the cell*
VCI	*Virtual channel identifier*	16	*Identifies the next destination of the cell*
PT	*Payload type*	3	*Indicates user data or control data*
CLP	*Cell Loss Priority*	1	*Indicates whether the cell should be discarded In the event of congestion*
HEC	*Header Error Control*	8	*Provides a checksum calculated on the header*

The GFC field provides local functions for the ATM cell. Local means there is no end to it and intermediate transfers do not accept this field. Local functionality means leak control and multi-station identification in a single ATM interface. The VPI and VCI fields are used together and identify the next destination of the ATM cell. [21]

The three bits of the PT field are defined as follows:

- The first bit indicates whether the cell contains user data or control data.
- The second bit indicates when there is an influx
- The third bit indicates if the cell is the last cell in the AAL 5 frame (PDU)

ATMs have determined that PVCs, or private network-network interfaces (PNNIs) can deploy virtual circuits dynamically. PNNI is a routing protocol for the connection state hierarchy that distributes virtual circuits through the ATM network. For the cells to be interpreted correctly and to be used by the above layer protocols, the ITU-T specified

a layer between the ATM layer and the top layer protocols. This layer is called AAL and has 5 categories. AAL1 is connection oriented and is used for services with delay in sensitivity and circuit emulation. AAL3 / 4 is unrelated and used mainly for older SMDS. AAL5 can be connection oriented or offline and is used for different bit rate requests and is mainly used for IP and LANE. To keep IP traffic on the ATM slot, routers at the ends of the ATM WAN are interconnected along the PVC ATM.

In order to make the connection in the most efficient way of the routers, they must be connected directly to each other along the PVC. This is necessary so that IP traffic does not pass through the ATM twice. So routers should be connected in "full mesh" mode. This is called the overlay model because all routers have an IGP close to the others in the ATM range. Figure 3.2 shows an overlay network of routers along the ATM cloud. The result is a number (n – 1) / 2 of the virtual circuits needed for n routers that are connected to ATM routers. MPLS solves this problem. When ATM switches are informed of the presence of routing, they form a CLOSE IGP between them and in the direction of the routers.

Not every router needs to form an IGP close to all routers but only to the nearest ATM switch. Figure 3.3 shows the ATM network where ATM switches are made LSR (Label Switching Routers); this means that they have become aware of the presence of MPLS. This is called the peer model because routers that are LSR terminals connect to nearby ATM switches which are now LSRs.

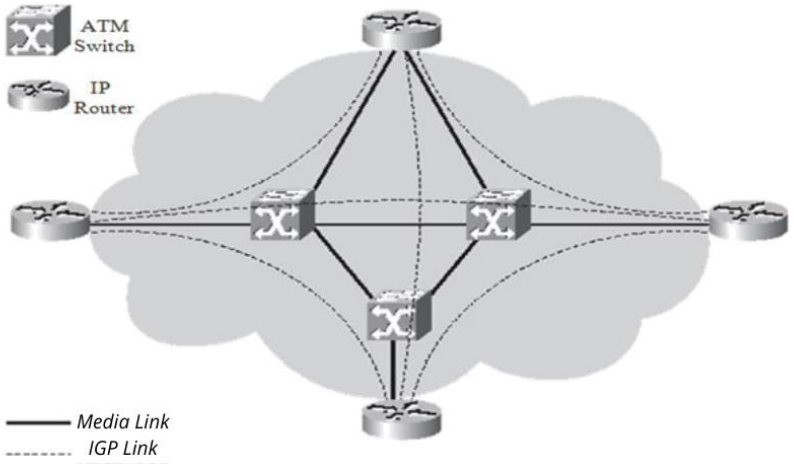


Figure 22. ATM Network Overlay

For traffic to be transmitted correctly across the LSR ATM, traffic must be encapsulated by the MPLS and MPLS tag values must be mapped to VPI / VCI values. This is because ATM switches also need to map the MPLS label values of a VC, they first need to learn the label values. So the ATM switch must execute a label distribution protocol. An LSR ATM consists of:

- A routing protocol in the control plan
- A label distribution protocol in the control plan
- ATM transfer cell in the data plan

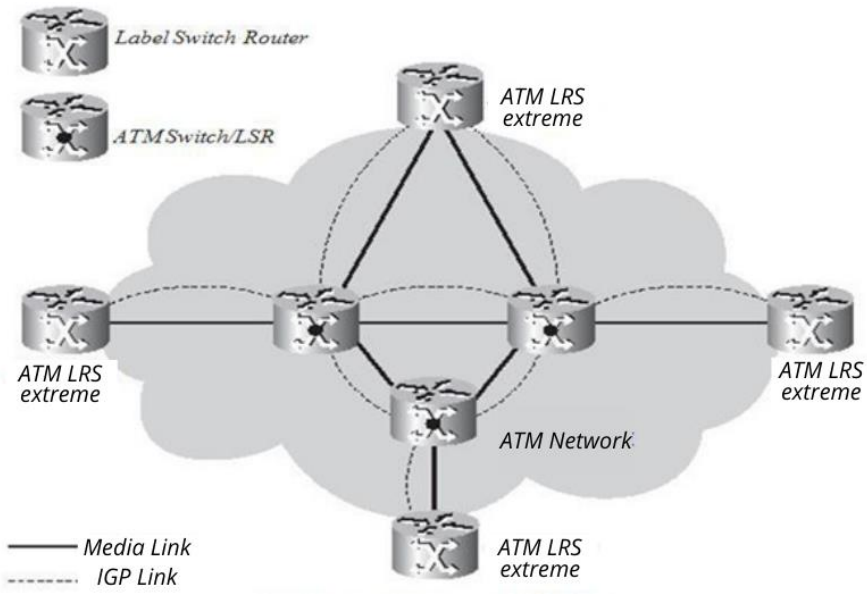


Figure 23. Peer ATM LSR network

Cisco ATM switches support OSPF (Open Shortest Path First) as routing protocol and LDP as a label delivery protocol. The Cisco ATM LSR delivers the routes to OSPF and the labeled connections associated with the routes and to the LDP. Input and output tags are mapped as VPI / VCI input and output pairs. The result is that in the data plan, the ATM switch simply needs to transfer cells from the virtual input circuit to the output one, just like a normal ATM transfer. The ATM switch never transfers IP packets. If this is necessary, then the ATM switch needs to reassemble all the input cells initially into the frame. Every ATM switch along the way needs to do this. This is undesirable for preformance reasons.

3.1.2. Label Coding

ATM switches that run MPLS are still transferring ATM cells. So they can not transfer labeled frames. Since MPLS tags are mapped to VCs in ATMs, the value of the

MPLS tag is mapped to the VPI / VCI pair. If the tagged packet has a tag stack with more than one tag, only the value at the top of the tag is mapped to the VPI / VCI field. Figure 3.4 shows the mapped MPLS tag of VPI / VCI values.

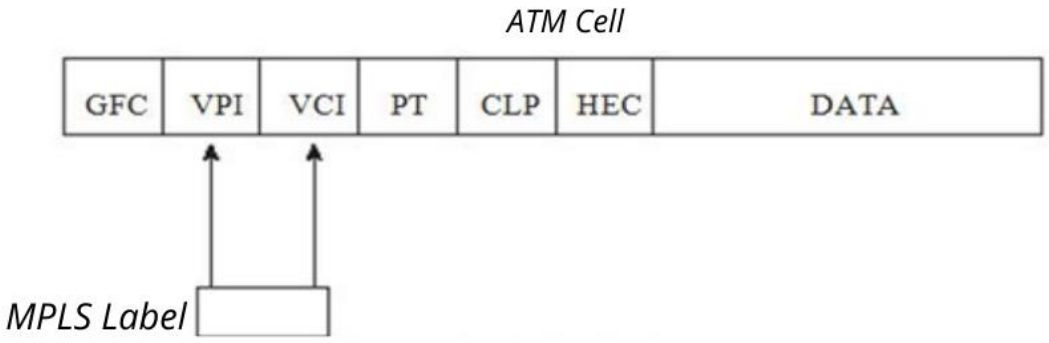


Figure 24. Label coding

When the LSR ATM edge takes a frame, the frame is split into several cells. Only the upper label value is encoded as a VPI / VCI value. The rest of the labels in the label stack are not needed to transfer the cells. However, the complete stack of labels is present in the frame. These tags will be needed again when the ATM cells are reunited in one frame and the frame needs further MPLS transfers outside the ATM network. The upper label value is encoded in the VPI / VCI field which varies at each LSR ATM and the upper label value in the label stack is set to 0. This label is held for the other three fields: TTL, EXP and the last bit of stack. TTL sets the output TTL when the packet is reconnected to the outgoing LSR ATM LSR. The EXP bit sets the packet QoS to the outgoing LSR ATM. Although the label stack consists of only one label, it is held throughout the ATM cloud in the first cell. This allows the outgoing LSR ATM to know when the package has a label stack or not. Since the VCI value is 16 bits, then there could be 216 or 65635 tags. Considering that the number of toilets is limited to ATM switches, this single value is sufficient for all the required labels on an interface. The VPI value is 12 bits, so it can be 212 or 4096 label.

3.1.3. Announcement of labels

IGP and LDP in LSR ATMs cannot be executed directly on the ATM interface and establish a neighborhood. A control VC is required for IGP and LDP to run between two neighboring ATM LSRs. When the IGP proximity is built, IGP can exchange IP prefixes which are placed in the routing table. Once the LDP places a session along the control toilet, it can exchange tag links. This in turn allows the LSR ATM to populate the connected LIB. As it repeats, a link is a prefix and an associated tag. Each IGP prefix in the routing table must be labeled. Each label value is mapped to a VPI / VCI value and a virtual circuit is built for each label. Such a virtual circuit is called LVC (Label Switched Controlled Virtual Circuit) or TVC (Tag Switching Controlled Virtual Circuit). To create these LVCs the ATM interface must be configured on the ATM switches and a labeled interface transfer control (LC-ATM) must be installed on the routers. Each LC-ATM interface must have a virtual control circuit. On routers and ATM switches running Cisco IOS, this is the recommended 0/32 virtual circuit. The encapsulation for it should be LLC / SNAP. To change the LDP of the control VC from 0/32 to another VPI / VCI pair, the interface command is used: mpls atm control-vc vpi vci. In ATM LSR, the VPI / VCI range that MPLS uses for LVC can be changed for the ATM interface. The recommended VPI range used for MPLS is 1. The Cisco IOS interface command that changes the VPI / VCI range is: mpls atm vpi vpi [-vpi] [vci-range low - high]

Each prefix present in the routing table creates a virtual network on the network. So in the interest of scalability, it is best to limit the number of prefixes in the routing table. One way to do this which is highly advisable is to have the ATM interface as an unnumbered IP interface. Need a loop interface like LDP ID for the router and IGP ID for the router and unnumbered IP interfaces that point to the loop interface. When unnumbered IP interfaces are not used, a label and a virtual circuit are allocated to each IP prefix that is configured in a connection. These trivial prefixes do not transfer traffic to the ATM network, so LVCs are set.

3.1.4. VC Connection

As mentioned the upstream LSR requires a label for a prefix from the downstream LSR and so on until it reaches the outgoing LSR. However, without a VC merger, labeled requests are propagated by the incoming LSR to the outgoing LSR, even though an intermediate LSR has already received an outgoing LSR tag from its own downstream LSR for that prefix. In Figure 3.5, where the ATM LSR Brussels atm has already received a label for the prefix 10.200.253.6/32 from the downstream LSR of Brussels. This first label came out 1/34 from atm brussel to brusel. For traffic from Washington atm to brussels, a second tag will be required by brussels for brussels bridges. This is tag 1/33.

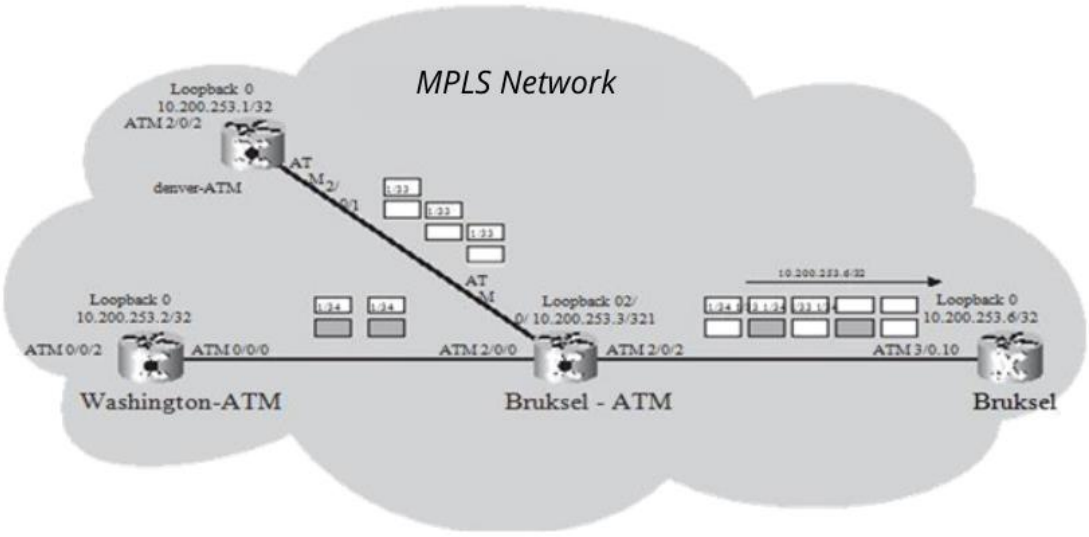


Figure 25. Two LSR Upstreams

Why does the same destination 10.200.253.6/32 over Brussels atm have a second exit label? One toilet is from denver atm in brussels and the second toilet is from washington atm in brussels. What if the Brussels LSR does not require a second label for the second upstream washington atm LSR but uses the label already received from the Brussels LSR? There would be a problem. Figure 3.6 shows the problem of cell overlap.

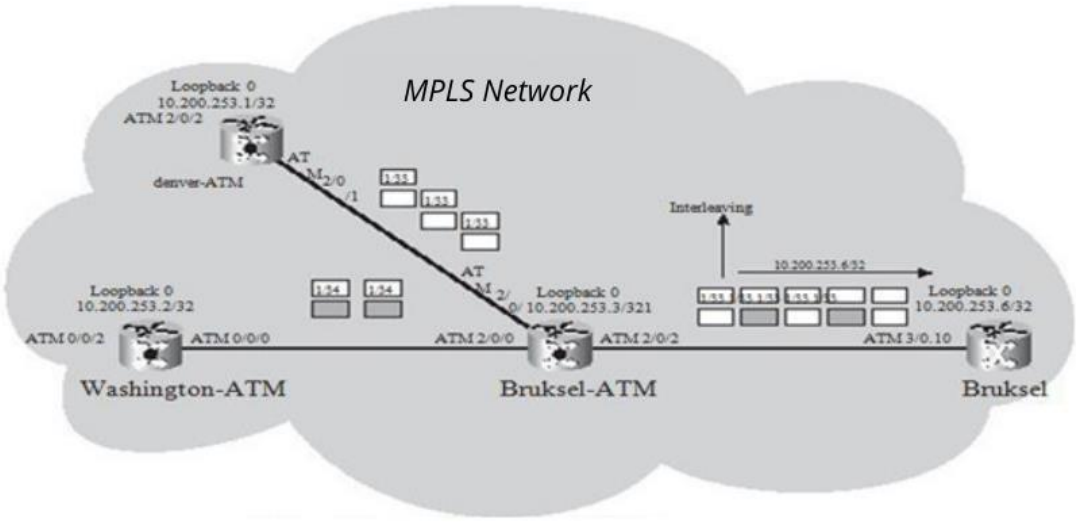


Figure 26. Cell separation

LSR Brussels atm has two incoming labels - one for each upstream LSR and only one outgoing label to LSR Brussels. Thus, cells from both denver atm LSRs and washington atm LSRs were cross-layered on the same LVC; this means that they have the same VPI / VCI value in terms of LSR Brussels. The outgoing Brussels LSR — which needs to rejoin the atm cells in the frame — does not know which stream the respective cells belong to. This is not a good idea. It can work if the cells that form a frame are not stratified with cells from another frame from another upstream LSR. This can be done if the coupling LSR (here LSR Brussels atm) buffers the cells until it detects that it has taken all the cells from the frame. This detection can be completed by bit at the end of the frame in the cell header. The coupling LSR can start cells without cell stratification from an upstream LSR.

Cells need to be buffered, which requires extra memory in the LSR ATM. The procedure of buffering cells and using only one output label per prefix for all upstream LSR ATMs is called VC. LVC merging different inputs merge into one outgoing LVC. Figure 3.7 shows the VC connection.

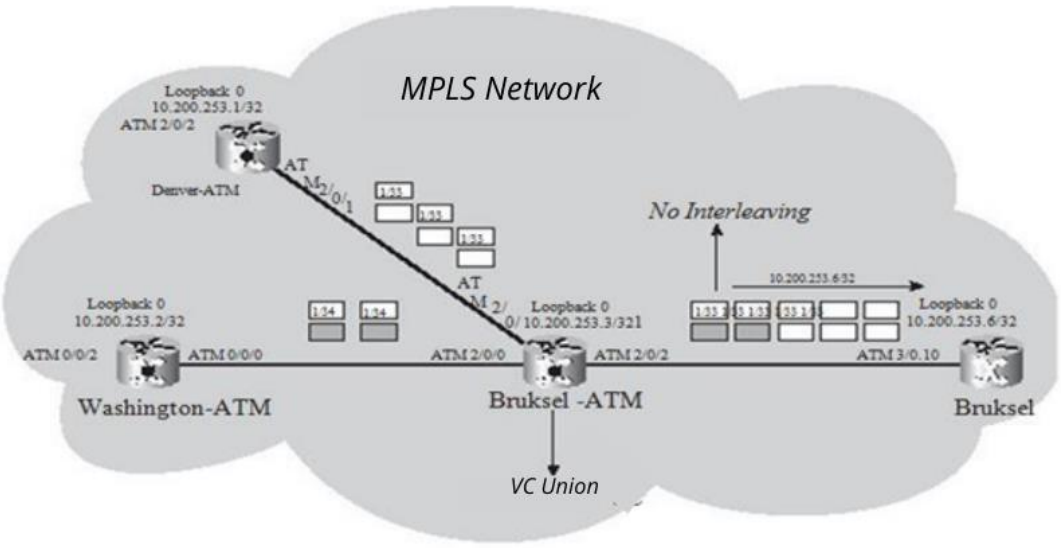


Figure 27. VC Union

The obvious advantage of the VC connection is that the number of toilets needed is reduced. If the Brussels amt router had 5 upstream LSRs for a set of 50 prefixes, it would be

(5-1) * 50 = 200 LVCs less in this simple example.

Command to enable VC connection in Cisco IOS: ***mpls ldp atm vc-merge***.

The VC connection is enabled by default on Cisco ATM switches.

3.1.5. Label Switch Controller

The label switch controller (LSC) is a hardware designed to perform the functions needed in the control plan to make the ATM switch an ATM LSR. The Cisco BPX is an ATM switch that needs an LSC to become an LSR ATM. The LSC takes care of the functions of control plans such as IGP, routing table and LDP.PBX still performs switching of ATM cells to the data plan. In the case of BPX, the LSC is a Cisco 7200 router. The LSC controls the BPX via an ATM interface over which the VSI (Virtual Switch Interface) protocol is running. The VSI allows the router to control gateways, main

lines or virtual main ones in BPX. The result is the same as if the LSC were internal to the ATM switch. When a PBX has an LSC attached to it, it becomes an LSR ATM for all purposes and purposes. The LSC establishes intermediate connections at the BPX switch factory for LVC. Interfaces are introduced in Cisco IOS as XTagATM (ATMs with extended label) interfaces over LSC.

3.1.6. Multi Virtual Circuit Target Bitrate

With Multi Virtual Circuit Target Bitrate (Multi VC TBR) many VCs are deployed to the same destination to provide different service classes (CoS). Over 4 parallel LVCs can go to the same destination. Switches can handle cells in different ways based on which LVC they are located.

Incoming IP packets are mapped to the bits of their corresponding LVC outgoing IP (DiffServ) precedent. Labeled packets are mapped based on the EXP bit values of the upper label in the corresponding LVC. At the LSR ATM terminal input there are many VC outputs from the LC ATM interface. All these toilets have the same route which is defined by IGP as the road with the lowest cost. Out-of-one toilets are activated by the mpls atm multi-vc interface command. This is configured at the ATM LSR remote so it requires 4 LVCs set for prefix. The default map of incoming packets to the parallel outgoing LVC is shown in Table 3.2.

Table 3. Default Multi-VC Map

LVC Type	CoS	*IP/MPLS EXP precedent*
Available	0	*0 and 4*
Standard	1	*1 and 5*
Premium	2	*2 and 6*
Control	3	*3 and 7*

The IP precedence of the incoming IP packet or the EXP bit value of the labeled incoming packet can be changed via MQC (Modular QoS Command Line Interface). MQC is a flexible and feature-rich component of Cisco IOS that controls QoS. Here it is used to set or change the QoS of packets before they are sent to the ATM kernel. In addition to packet classification, MQC can control and regulate incoming traffic.

To support VC TBR LVCs on atm switches, 4 CoS classes have been defined which are achieved with effort which means that bandwidth is not guaranteed. These 4 TBR service classes are shown in Table 4.

Table 4. TBR Classes

ATM Forum Service Class	CoS	*Relative weight of the class*	*LVC Type*
CBR	2	—	
VBR-RT	2	8	
VBR-nRT	3	1	
UBR	4	1	
ABR	5	1	
TBR_1 (WRR_1)	1	1	*Available*
TBR_2 (WRR_2)	6	2	*Standard*
TBR_3 (WRR_3)	7	3	*Premium*
TBR_4 (WRR_4)	8	4	*Control*

There is no CAC (connection admission control) for LVCs because they are hard-to-reach virtual circuits and bandwidth is not guaranteed. It appears that LVCs do not share the same CoS in the VC ATM forum (VBR-RT, VBRnRT, ABR and UBR). Each TBR class indicates the CoS treatment that ATM cells will receive of each LSR ATM.

Since the cells are in different toilets, they end up in different rows. ATM cells receive CoS treatment in two ways:

- Scheduling based on the relative weight of the class
- WEPD - Weighted Early Packet Discard

The command to change the relative class for a particular service class is: atm service-class service-class ***wrr-weight*** weight. You can set each service class (1-8) a weight from 1 to 15. Unless Multi VC TBR is used, each prefix has only one LVC and WEPD cannot be used. However, WERD (Weighted Random Early Detection) can be used in remote LSRs.

3.1.6.1. MPLS CoS

CoS classes can be mapped to LVC. When Multi VC TBR is used, it is required to map CoS classes differently from LVCs set by Multi VC TBR features. CoS class mapping can reduce networked toilets. Just need to design some classes of a Multi VC type TBR LVC: possible, standard, premium and control. In example 3.1 each of the 2 types of LVC possible and premium takes two defined classes. This reduces the number of LVCs from 4 to 2 per prefix. With an access list, one can specify for which prefix the CoS map is applicable.

3.1.7. ATM frame mode

The ATM can also be used in the frame mode on remote routers. In this case, a PVC is configured between the end routers. Configuration on routers consists of the PVC ATM subpage. LDP is activated on the subpage with the mpls ip command. The ATM switch in this case is not designated to hold MPLS. Routers at the ends peer to each other

— both for OSPF and LDP instead of with ATM switches. This is the overlay model. The label space used in the ATM subdomain is a wide label space platform instead of the label space interface used in the LC-ATM interface.

```
!
hostna me washingt on
!
mpl s label pr otocol ldp
mpls ldp router -id Loopba ck0 force
mpls prefi x-map 1 ac cess-list  1 0 cos-map 1
mpls cos- map 1
 class 0 av ailable
 class 1 available
 cla ss 2 premiu m
 cl ass 3 prem ium
!
a ccess-list 10 permit any
!
          swashington#show mpls atm-ldp bindings 10.200.253.2 32
 Destination: 10.200.253.2/32
     Headend Router ATM1/0.10 (1 hop) 1/47          Active, VCD=323, CoS=available
     Headend Router ATM1/0.10 (1 hop) 1/48          Active, VCD=324, CoS=premium

          swashington#show mpls forwarding-table 10.200.253.2 detail
Local   Outgoing      Prefix              Bytes tag     Outgoing      Next Hop
tag     tag or VC     or Tunnel Id        switched      interface
17      Multi-VC      10.200.253.2/32     0             AT1/0.10      point2point
          available 1/47(323), standard 1/47(323),
          premium 1/48(324), control 1/48(324)
          MAC/Encaps=4/8, MRU=4470, Tag Stack {Multi-VC}
          00078847 00007000
          Feature Quick flag set
     Per-packet load-sharing
```

Figure 28. MPLS CoS configuration

3.1.8. Reducing the number of LVCs

The following measures can be taken to reduce the number of LVCs:

- Reducing the number of IP prefixes
- Using the VC connection

- CoS classes of LVCs
- Deactivation of VC heads and bottoms in LSC
- Block label request messages for IP prefixes

The number of IP prefixes can be reduced by using loopback with IP addresses for IGP and LDP. All connections are configured as unnumbered IPs of the loopback IP address interface. IP prefixes that are not configured in LSR ATMs but are still in the same routing domain cause LVCs to be deployed. IP prefixes can also be reduced by using unnumbered interfaces. VC connection causes the connection of VCs to an LSR ATM. Without the VC merger, a VC is set for the upstream neighborhood and for the destination. With VC merger, this is reduced to a destination VC, thanks to the number of upstream neighbors at the LSR ATM. In the case of Multi-VC TBR, 4 LVCs are placed for the destination. This can be reduced by configuring a mapping of LVC CoS classes.

When an LSC is used for the BPX / MGX switch, deactivating the VC may reduce the number of LVCs. This deactivates the ATM LSR which functions as a remote LSR ATM. To prevent the LSR ATM from operating as a remote LSR ATM, the ***mpls disable headend-vc*** command is used.

The label request message from an LSR can be blocked. This blocks the toilet signaling. The command to do this is ***mpls ldp request-labels*** for acl.

3.2. MPLS VPN

3.2.1. Introduction to MPLS VPN

MPLS VPN, or MPLS Virtual Private Network, is the most popular and distributed implementation of MPLS technology. Its popularity has grown since it was invented and continues to grow steadily. Although many SPs have implemented it as a replacement for

the previously popular Frame Relay and ATM technologies, MPLS VPN is seeing an increase in interest from large companies who see it as an important next step in designing network. MPLS VPN provides scalability and divides the network into small separate networks, which is much needed in large companies where shared IT infrastructure has to provide isolated networks to individual departments. Many companies that have used MPLS VPN for years are looking to connect their network to that MPLS VPN of other SPs to improve scalability and easier operation of their networks. Here comes to the fore what is called Inter Autonomus MPLS VPN and Carrier's Carrier (CsC).

3.2.1.1. Definition of VPN

VPN is a network that creates a private network over a shared infrastructure and provides communications in layer 2 or 3 of the OSI model. VPN usually belongs to a company and has different interconnection areas along the common infrastructure. The private network requires that all clients of a VPN be able to connect and be completely separate from other VPNs. This is the minimum connection requirement. Anyway the VPN model in IP layer requires more than that. They can provide connections to various VPNs when required and can also provide internet connections. MPLS VPN offers all of these. The use of MPLS has become possible as SPs execute MPLS on the backbone network, which undertakes an organization in the transmission plan and control plan, which IP does not do.

3.2.1.2. VPN models

VPN existed before MPLS and was mainly used in Frame Relay and ATM technology, offering VPN service in layer 2. The SPs had an ATM and Frame Relay backbone and established a connection in layer 2 of the client routers. This was also called the overlay model. The SP owned or managed the remote routers that were connected to

the client network. The routers were physically in client condition. Referring to the peer-to-peer model, it existed but was not popular because it was difficult to develop and maintain as distributed lists, IP packet filters or GRE tunnels were needed. MPLS VPN is a high-level scaling of the peer-to-peer VPN model.

3.2.1.3. MPLS VPN models

Figure 3.2.1 shows an MPLS VPN model figure. An SP provides a shared public infrastructure used by the client. The PE router is called the provider edge, it has a direct connection to the CE (costumer edge) router in layer 3. A P (provider) router is a router without a direct connection to the client routers. In the implementation of MPLS VPN both routers P and PE execute MPLS. This means that they must be able to distribute the labels among themselves and the packets labeled and transmitted.

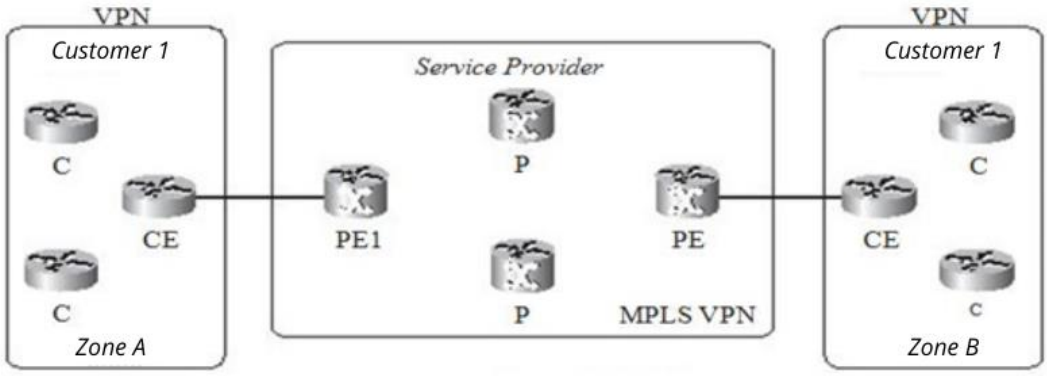


Figure 29. MPLS VPN scheme

A CE router has a direct connection in layer 3 to a PE router. A client router C is a router without a direct connection to the PE router. The CE router does not need to execute MPLS. Since the PE and CE routers interact in layer 3, they must execute a routing protocol or static routing between them. The CE router has only one peer outside its area: the PE router. If the CE router is multihome then it can be connected to many PE routers.

The CE router does not connect to any other CE router from other areas through the SP network as is the case with the overlay model. The model name peer-to-peer comes from the fact that PE and CE create connections in layer 3. P in VPN means privacy. SP clients are allowed to have their own IP address scheme. This means that they can use registered IP addresses but also private IP addresses or IP addresses used by other clients that are connected to the same IP (overlapping IP addressing). If packets had to be transferred as IP packets to the SP network, this would cause problems because it would lead to router confusion P. If neither of the last 2 schemes is allowed then each client should have a unique address range IP. In this case the packets can be transferred by forwarding the destination IP address to each router in the SP network. This means that every P and PE router should have the complete routing table of each client, which would be a very large routing table. The only routing protocol that is capable of holding a large number of routes is BGP. This means that all P and PE routers will have to execute internal BGP between them. However this is not a VPN scheme because it is not private regarding clients.

Another solution is that every P and PE router has a private routing table for each client. Various processes of a routing protocol (one process for VPN) can be executed on all routers to distribute VPN routes. Execution of the routing protocol for the VPN on each P router is not very scalable. Each time a VPN is added to the network, a new routing process will be added to each router. which private routing table will you use? If the packet is IP, this is not possible. An additional field can be added to the IP packet that specifies which VPN the IP packet belongs to, and so router P can transmit the IP packet by looking at this additional field and the destination IP address. Again P routers need to be informed about this additional field. A scalable solution would be to have an uninformed P router for VPNs. So P routers would not be loaded having routing information for VPN routes.

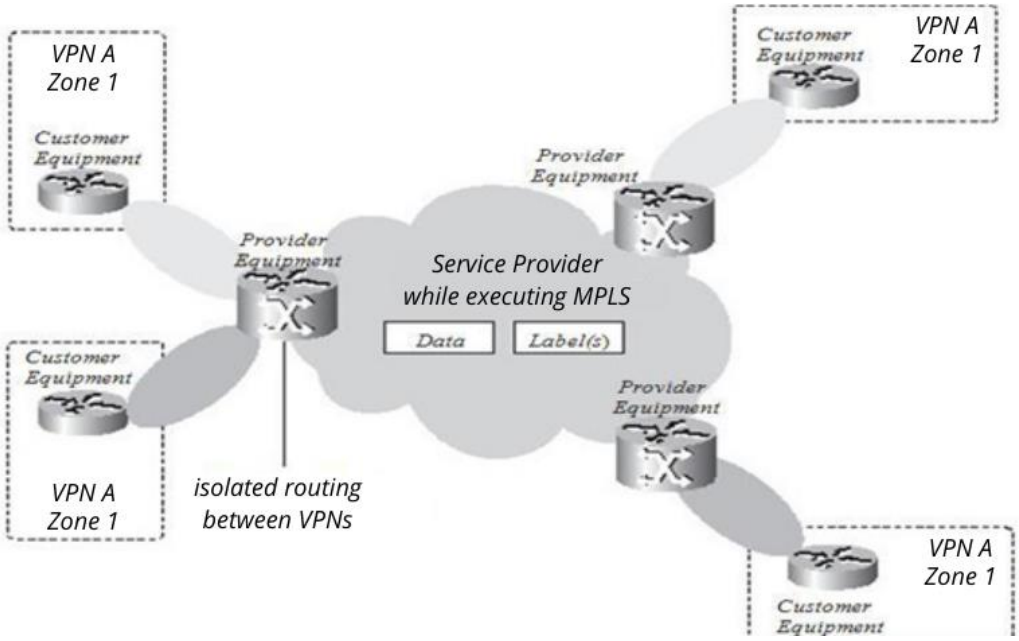


Figure 30. MPLS VPN model

Can this be achieved through MPLS? The answer is yes. Client IP packets are labeled on the SP network to achieve a private VPN for each client. Also, P routers do not need to have client routing tables using two MPLS tags. So BGP is not required in routers P. VPN routes are simply known in PE routers.

Thus VPN recognition is present only on the outgoing routers of the MPLS VPN network, which make the MPLS VPN solution scalable. Figure 3.2.2 shows the MPLS VPN model: the transfer of labeled packets to the SP network and the PE routers that are informed about the VPN.

3.2.2. Description of MPLS VPN Architecture

To achieve MPLS VPN, some basic building blocks are needed in PE routers. These building blocks are: VRF, RD (route distinguisher), RT (route targets) route propagation through MP-BGP and the transfer of labeled packets.

3.2.2.1. VRF (Virtual Routing Forwarding)

A VRF is a VPN routing and a transfer request. It is the name of the combination of VPN routing table, VRF CEF (Cisco Express Forwarding) table and IP routing protocols associated with PE routers. A PE router has a VRF request for each connected VPN. Figure 3.3.1 shows a PE router that holds the global IP routing table, but also a VRF routing table for connected PE VPNs. [21]

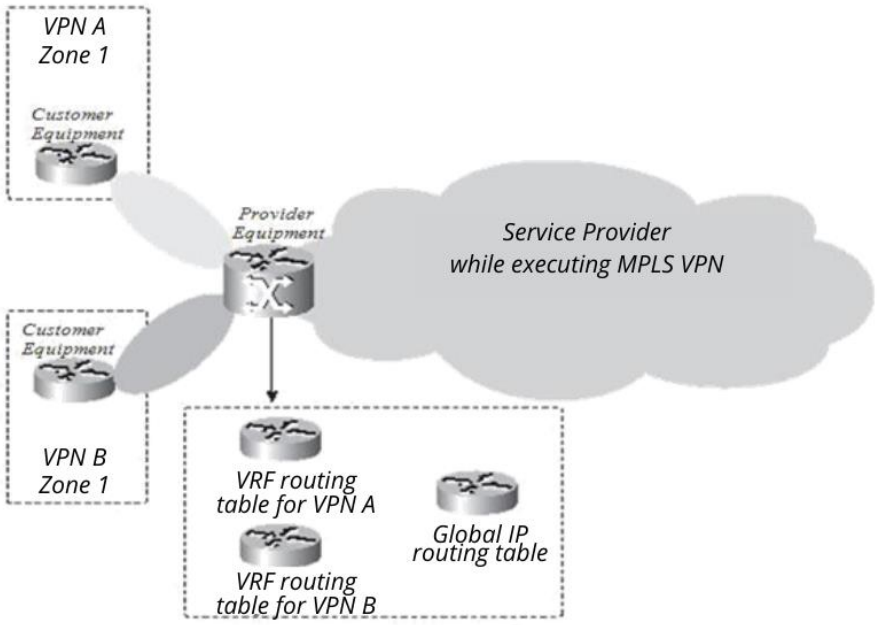
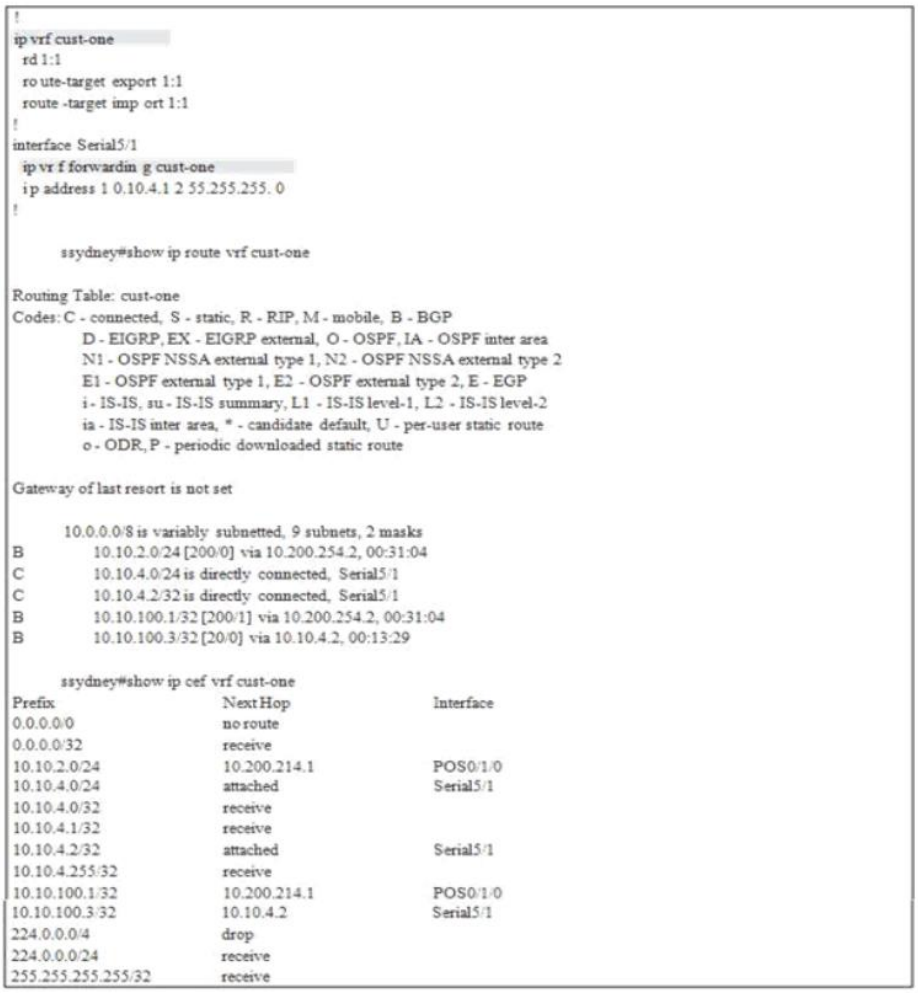


Figure 31. VRF of a PE router

Since routing must be separate and private for each client on a PE router, each VPN must have its own routing table. This private routing table is called the VRF routing table. The interface on the PE router versus the CE router can only belong to one VRF. Thus all IP packets received in the VRF interface are clearly identified as belonging to that VRF. Since we have a separate routing table for the VPN, a separate CEF table for the VPN, which transfers these packets to the PE router.

This is the VRF CEF table. As with the global routing table and the global CEF table, the CEF VRF table is derived from the VRF routing table. VRF on the PE router is created with the ip vrf command. The ip vrf forwarding command is used which establishes the PE-CE interface on the PE router of a VRF. You can set an interface to only one VRF, but you can set multiple interfaces to the same VRF. The PE router then automatically creates a VRF routing table and a CEF table. The VRF routing table is no different from a regular routing table in Cisco IOS except that it is used to deploy only one set of VPN zones and is completely separate from all other routing tables. The routing table will be referred to as the global or default routing table. Example 32 shows the configuration of the cust-one VRF.



```
!
ip vrf cust-one
 rd 1:1
 ro ute-target export 1:1
 route -target imp ort 1:1
!
interface Serial5/1
 ip vr f forwardin g cust-one
 i p address 1 0.10.4.1 2 55.255.255. 0
!

        ssydney#show ip route vrf cust-one

Routing Table: cust-one
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
           i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
           ia - IS-IS inter area, * - candidate default, U - per-user static route
           o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

        10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
B          10.10.2.0/24 [200/0] via 10.200.254.2, 00:31:04
C          10.10.4.0/24 is directly connected, Serial5/1
C          10.10.4.2/32 is directly connected, Serial5/1
B          10.10.100.1/32 [200/1] via 10.200.254.2, 00:31:04
B          10.10.100.3/32 [20/0] via 10.10.4.2, 00:13:29

        ssydney#show ip cef vrf cust-one
Prefix                  Next Hop                Interface
0.0.0.0/0               no route
0.0.0.0/32              receive
10.10.2.0/24            10.200.214.1            POS0/1/0
10.10.4.0/24            attached                Serial5/1
10.10.4.0/32            receive
10.10.4.1/32            receive
10.10.4.2/32            attached                Serial5/1
10.10.4.255/32          receive
10.10.100.1/32          10.200.214.1            POS0/1/0
10.10.100.3/32          10.10.4.2               Serial5/1
224.0.0.0/4             drop
224.0.0.0/24            receive
255.255.255.255/32      receive
```

Figure 32. A VRF configuration

This routing table has prefixes that are populated by dynamic routing protocols and static protocols, just like the global routing table. The concepts of metric, distance, other hop and so on do not change. Since the VRF request is associated with the interfaces, only IP packets that enter the PE router through those VRF interfaces are transferred according to that VRF CEF table. In Cisco IOS, CEF is the only supported method for transferring IP packets from the VRF interface. Thus CEF must be activated globally across all PE routers and all VRF interfaces.

3.2.2.2. RD

VPN prefixes are distributed over the MPLS VPN network by multi-protocol BGP (MP-BGP). The problem is that when BGP carries IPv4 prefixes throughout the SP network, they must be unique. If the client has IP addressing coverage, routing would be wrong. To avoid this problem, the concept of RD was created which sought to make the IPv4 prefixes unique. The basic idea was that each prefix from each client received a unique identifier (RD) to distinguish the same prefixes from different clients. The prefix derived from the combination of the IPv4 and RD prefix is called the vpnv4 prefix. MP-BGP needs to maintain these prefixes between PE routers. [18]

An RD is a 64 bit field used to make VRF prefixes unique when MP-BGP holds them. RD does not indicate to which VRF the prefix belongs. The RD function is not that of a VPN identifier, because some complex VPN scenarios may require more than one RD per VPN. Every VRF request on the PE router must have an RD attached to it. This 64 bit value can have two formats: ASN: nn or IP-address: nn where nn represents a number. The most used format is the first, where ANS stands as autonomus system number. Usually SPs use ANS: nn where ANS is the autonomous number system that IANA (Internet Assigned Numbers Authority) assigns to SP and nn is the number that SP assigns to VRF uniquely. RD does not set semantics; it is simply used to uniquely identify routes. This is necessary because IPv4 routes from one client can cover the routes of another client. The combination of RD with the IPv4 prefix provides a vpnv4 prefix whose address is 96 bits. The mask is 32 bits, the same as for the IPv4 prefix. If you get an IPv4 10.1.1.0/24 and RD 1: 1, the vpnv4 prefix becomes 1: 1: 10.1.1.0/24. A client can use different RDs for the same IPv4 route. [22] When a VPN zone is connected to 2 PE routers, the paths from the VPN zones can receive 2 different RDs, depending on which PE router routers are received. Each IPv4 path will take 2 different RDs and will have two completely different vpnv4 paths. This will allow BGP to look at them as different paths

and apply a different path practice. Example 3.2.1 shows how to configure RD in Cisco IOS.

```
csydney#conf t
Enter configuration commands, one per line.                End with CNTL/Z.
        isydney(config)#ip vrf ?
  WORD VPN Routing/Forwarding instance name
        isydney(config)#ip vrf cust-one
          rsydney(config-vrf)#rd ?
  ASN:nn or IP-address:nn          VPN Route Distinguisher
          rsydney(config-vrf)#rd 1:1
```

Figure 33. RD configuration

3.2.2.3. RTs

If RD was used only to indicate VPN, communication between parts of different VPNs would be problematic. An area of company A would not be able to communicate with an area of company B because the RDs would not match. The concept of having company A capable of communicating with company B is called VPN extranets.

The simple matter of communication between parts of the same company — the same VPN — is called an intranet. Communication between parts is controlled by another MPLS VPN feature called RT. An RT is an extended BGP community that indicates which route to take from MP-BGP towards VRF. Exporting an RT means that the exported vpnv4 route takes on an additional extended BGP community — this is RT — as configured under ip vrf on the PE router, where the route is redistributed from the VRF routing table in the direction of MP-BGP. Importing an RT means that the vpnv4 path taken by MP-BGP is controlled for an extended community that matches — this is a target path — to that in the configuration. If the result matches, the prefix is entered in the VRF routing table as an IPv4 route. If we do not have adaptation, the prefix is rejected. [23]

The command to configure RT for VRF is route-target {import | export | both} route-target-extcommunity. The word both means import and export. Figure 3.4.1 shows the RT controls which routes are imported in the direction of which VRF from the PE router remotely and with which RT the vpnv4 routes are exported in the direction of the PE remote routers. With more than one RT can be attached to the vpnv4 route. For each import in the direction of VRF to be accepted, only one RT from the vpnv4 path is required to be compared with the configuration of the imported RT under section ip vrf in the PE router.

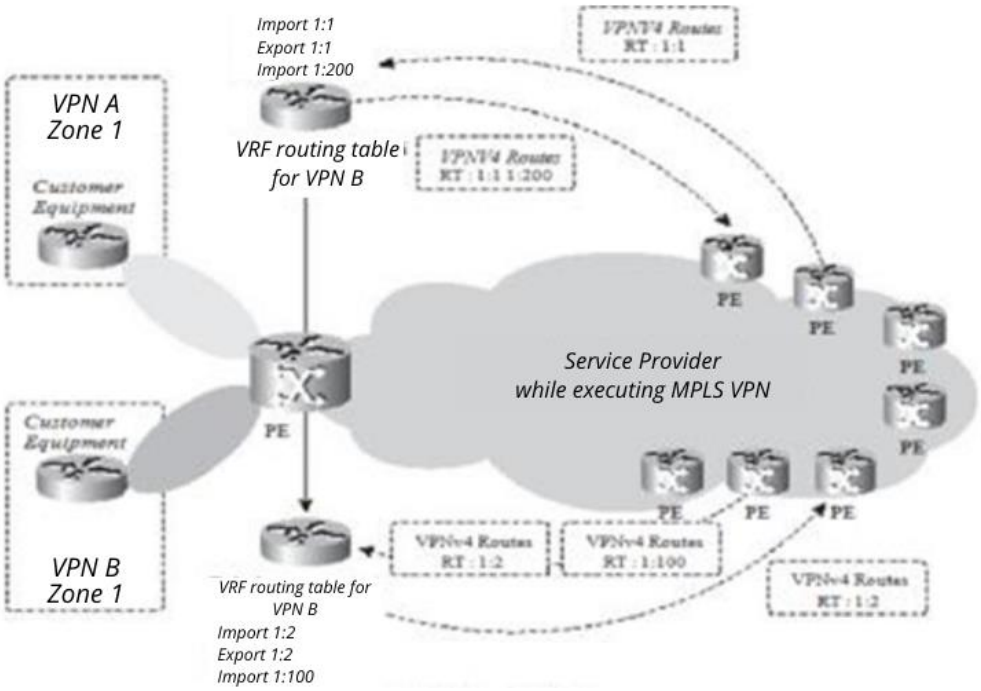


Figure 34. RT

Figure 35 shows how to configure RT on Cisco IOS.

```
csydney#conft
Enter configuration commands, one per line.   End with CNTL/Z.
isydney(config)#ip vrf cust-one
rsydney(config-vrf)#route-target
? ASN:nn or IP-address:nn   Target VPN Extended Community
  both                      Both import and export Target-VPN community
  export                    Export Target-VPN community
  import                    Import Target-VPN community
rsydney(config-vrf)#route-target both 1:1
```

Figure 35. RT configuration

When configuring a multi-zone VRF belonging to one VPN, without having to communicate with parts belonging to another VPN, simply configure an RT to be imported and exported to all PE routers with an area belonging to that VRF. This is a simple example of an intranet. When you have areas belonging to a VPN that needs to be able to communicate with areas from another VPN (extranet case), be careful how to configure the RT correctly. [24]

Figure 36 shows an example extranet.

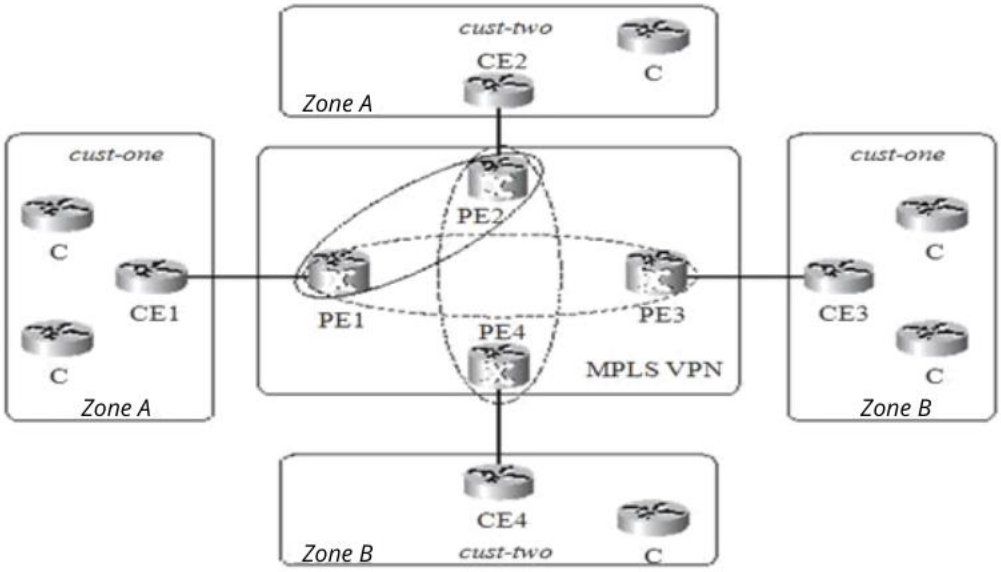


Figure 36. Extranet example

Of course, zone A and zone B from the VRF cust one must be able to communicate with each other. This also applies to zones A and B of VRF cust two. The RT that uses cust one is 1: 1, while cust two uses 1: 2. Now suppose that zone one of the VRF cust one needs to talk to zone A of the VRF cust two. This is entirely possible and is determined by configuring RT depending on this. RT 100: 1 is imported and exported from zone A of vrf cust one and cust two in PE1 and PE2 to achieve this. This is called extranet. [5]

Maybe we may not want 2 VRFs to swap all paths. The number of routes from one VRF point to another can be limited by configuring an import or export map under ip vrf, which uses a road map for other filtered routes.

3.2.2.4. Spread of VPNv4 routes in MPLS VPN network

VRF divides client routes into PE routers, but how are prefixes transported across the SP network? Being potentially multiple routes (possibly hundreds of thousands) can be transported, BGP is the ideal candidate because it is a proven and stable routing protocol to maintain multiple routes. This is understood given that BGP is the standard routing protocol to maintain a complete online routing table. Since the routes to the client are made unique by the RD of each IPv4 route (their return to vpnv4 route) all client routes can be safely transported over the MPLS VPN network. Figure 3.6.1 shows a description of the path presentation in the MPLS VPN network.

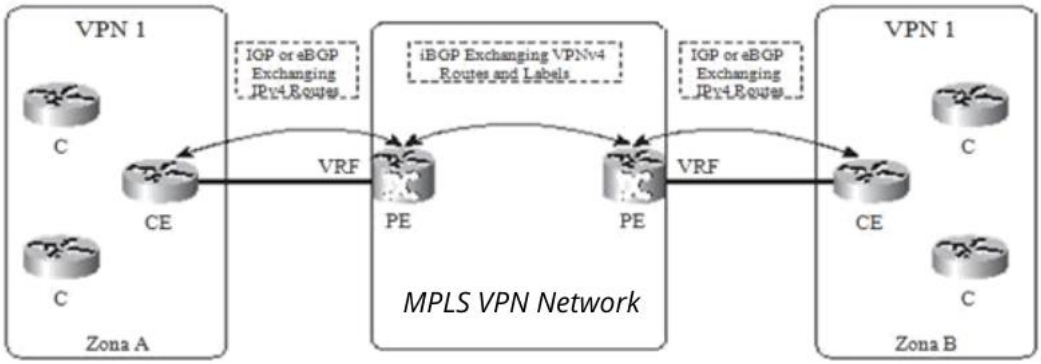


Figure 37. Propagation of VPNv4 routes in the MPLS VPN network

The PE router receives IPv4 routes from the CE router via IGP (Internal Gateway Protocol) or external BGP (Exterior Border Gateway Protocol). These IPv4 routes from VPN areas are placed in the VRF routing table. Which VRF will be used, this is determined by the VRF configured on the interface on the PE router in the direction of the CE router. These paths are attached to the RD which is marked on that VRF. So they become vpnv4 routes of all PE routers in MPLS VPN network. On PE routers, the vpnv4 paths are stripped of the RD and placed in the VRF routing table as IPv4 paths. If the vpnv4 path, after stripping RD, is set to VRF depending on whether RT allows import into VRF. These IPv4 routes are defined on the CE router via an IGP or eBGP that runs between the PE and CE routers.

Since the SP that is running the MPLS network VPN executes BGP on an autonomous system, iBGP is running between the PE router. The submission by eBGP (running between the PE and CE router) of MP-iBGP on the MPLS VPN network and vice versa is automatic and does not require extra configuration. However the redistribution of MP-iBGP to IGP that is being executed between the PE and CE router is not automatic. Joint redistribution between MP-iBGP and IGP should be configured.

3.2.2.5. Transmission of packets in a MPLS VPN network

As explained in the previous section, packets cannot be transmitted as simple IP packets between zones. P routers cannot transmit them because they do not have VRF information from every area. MPLS solves this problem by labeling packages. So router P in this case must have the information needed to transfer packets.

The most common way is to configure LDP (Label Distribution Protocol) between all P and PE routers so that all IP traffic is labeled and transferred between them. RSVP with add-ons for traffic (traffic engineering) can also be used when implementing MPLS TE, but LDP is more common for MPLS VPN. IP packets are then labeled and transmitted with a label from the PE input router to the PE output router. A P router does not have to perform a remote view of the destination IP address. This is how packets are transferred between the input PE router and the output PE router. This tag is called the IGP tag because it is the tag associated with an IPv4 prefix in the global P & PE router routing table and the IGP of the SP network warns it.

How does the PE output router know which VRF packet it belongs to? This information is not in the IP header and cannot be found from the IGP tag because it is only used to transfer packets to the SP network. The solution is to add other tags to the MPLS tag stack.

This label indicates to which VRF the packages belong. So client packets are transmitted with two tags: the IGP tag as the top tag and the VPN tag as the last tag. The VPN tag must be placed on the PE input router to indicate to the output router to which the VRF packets belong. How does the PE output router signal the input PE router to indicate which label to use as the VRF prefix? Since MP-BGP is already used to warn the vpnv4 prefix, it also signals the VPN tag (referred to as the BGP tag) which is associated with the vpnv4 prefix. Currently, the concept of having a VPN tag that indicates the VRF

to which the packet belongs is not very clear. This may be true in some cases, but in most cases it is not. A VPN tag usually indicates the next hop that the packet needs to be transferred to the output PE router. So, most of the time, its purpose is to show the correct CE router as the next packet hop.

VRF to VRF traffic has two tags on the MPLS network. The above label is the IGP label and is distributed by the LDP or RSVP for ALL between all P and PE routers hop by hop. The bottom tag is the VPN tag that is warned by the MP-iBGP from EP to EP. P routers use the IGP tag to transfer packets to the correct PE output router. PE routers use the VPN tag to transfer IP packets to the correct CE router. Figure 3.7.1 shows the packet transfer to the MPLS VPN network. The packet enters the PE router on the VRF interface as an IPv4 packet. This is transferred across the MPLS network with two tags. P routers transfer the packet by looking at the top label which is exchanged on each router P. The labels are stripped to the output PE router and the packet is transferred as an IPv4 packet to the VRF interface in the direction of the CE router. The correct CE router is found by looking at the VPN tags.

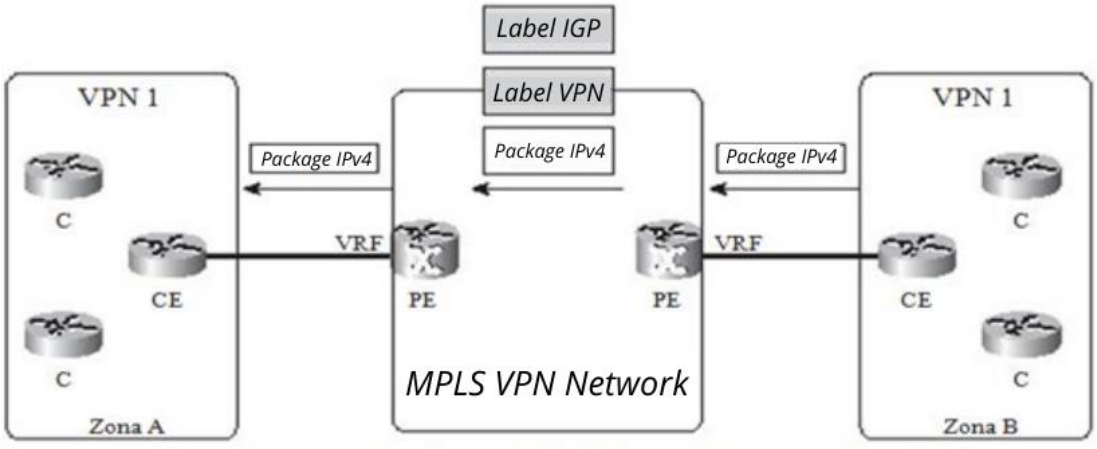


Figure 38. Packet transmission in the MPLS VPN network

3.2.3. BGP

BGP version 4 (BGP-4) has been in use for years and is a standard protocol for routing between domains. BGP is the protocol that makes the internet work so well nowadays. The SPs that make up the internet execute the BGP between them. They interact with other SPs through eBGP and execute iBGP on their network. BGP is a routing protocol that is well equipped to hold hundreds of thousands of routes and has been proven to retain this capability. BGP is a routing protocol that allows for the implementation of broad and flexible policies. This is why it is a good candidate to maintain MPLS VPN routes. As mentioned before it is the combination of RD with IPv4 prefix that creates the vpnv4 prefix and it is this prefix that iBGP needs to keep between PE routers.

3.2.3.1. Multi-protocol BGP add-ons and options

BGP-4 is described in RFC 1771, but RFC only describes the use of BGP to maintain IPv4 prefixes. BGP can do more than just maintain IPv4 prefixes. RFC 2858, "Multiprotocol Extensions for BGP-4", was created to extend BGP to allow it to hold routing information other than IPv4. Upon request, BGP-4 can maintain IPv6 prefixes and thus provide the interdomain for IPv6. A BGP speaker notifies its peers that the multi-protocol extension for BGP-4 is supported using capability alerts. BGP peers share with each other the skills they support. Options owned by all peers can then be used. Examples of possibilities are ORF (outbound route filtering), the ability to refresh the road and the extension of many protocols. RFC 3392 (BGP-4 Opportunity Notifications) describes its functions. When a BGP speaker launches an open message to its peers, it can include the optional options parameter, listing all the capabilities of that BGP speaker. BGP peers can do the same. Furthermore the capabilities match in both peers, or a BGP notification is received from the other BGP speaker indicating what capabilities it does not support.

The multi-protocol extension for BGP-4 defines two new BGP features: Multiprotocol Reachable NLRI and Multiprotocol Unreachable NLRI. These features alert or cancel routes. Each of them holds two fields: AFI (Address Family Identifier) and SAFI (Subsequent Address Family Identifier). Together they determine exactly what type of road BGP holds. To ensure BGP multi-protocol welfare in Cisco IOS, the BGP routing process has the concept of address families. The 4 address families supported so far are IPv4, IPv6, vpnv4 (VPN-IPv4) and vpnv6 (VPN-IPv6). Subsequent address families that can be specified are unicast, multicast, and VRF. Figure 39 shows the configuration of BGP address families. The vpnv4 address family is used under the router BGP process to configure the vpnv4 BGP session and the parameters that the PE router needs. The ipv4 vrf address family vrf-name is used under the BGP router process on PE routers to configure BGP session and parameters in the direction of CE routers, along the VRF interface.

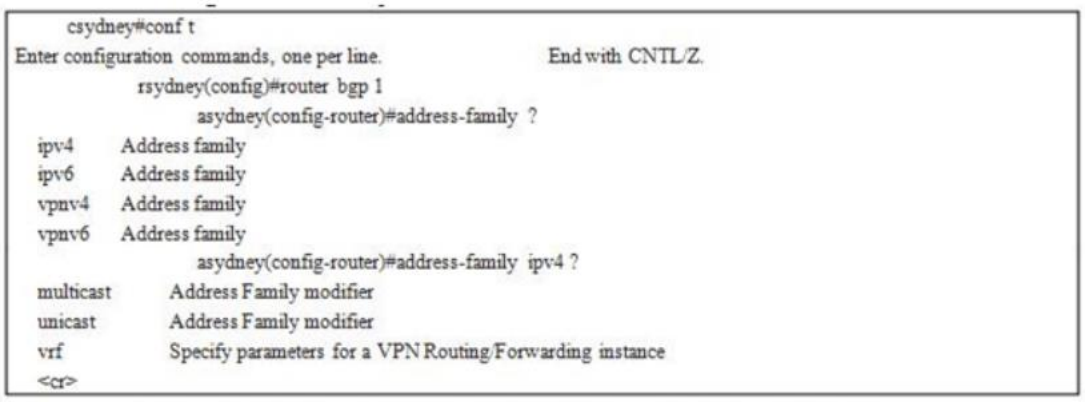


Figure 39. BGP address family configuration

3.2.3.2. VPNv4 routes

The 64 bit RD field and the 32 bit IPv4 prefix make up the vpnv4 prefix which is 96 bits long. MP-iBGP announces these prefixes between PE routers. The vpnv4 prefixes held by BGP appear in the following commands:

show ip bgp vpnv4 {all rd *route-distinguisher* **vrf** *vrf-name}*
[rib-failure] *[ip-prefix/length [**longer-prefixes**] [output-modifiers]] [network-address [mask] [**longer-prefixes**][**labels**]*

All words for this command indicate all vpnv4 paths or all paths for all RDs. With the keywords rd, only those paths with that RD can be viewed. The same can be done with the vrf keyword on a PE router. However if the command with the words vrf is used in a route reflector RR (route reflector), it may not show the routes. RR may not have VFR configured because it is simply used to reflect vpnv4 paths. In this case, the command with the keywords rd must be used to view a specific vpnv4 path. ***Debug ip bgp vpnv4 unicast updates*** lets you update vpnv4 updates to BGP. Figure 40 shows the adjustment when a VPNv4 prefix is obtained.

```
dsydney#debug ip bgp vpnv4 unicast updates
BGP updates debugging is on for address family: VPNv4 Unicast
sydney#
BGP(2): 10.200.254.2 rcvd UPDATE w/ attr: nexthop 10.200.254.2, origin ?, localpref 100,
  metric
1, extended community RT:1:1
BGP(2): 10.200.254.2 rcvd 1:1:10.10.100.1/32
BGP(2): Revise route installing 1 of 1 routes for 10.10.100.1/32 -> 10.200.254.2(main) to
  cust-
one IP table
```

Figure 40. Debug ip bgp VPNv4 Unicast Updates

The internal tag is used as an entry tag in the LFIB (Label Forwarding Information Base) for this vpnv4 prefix. It is the label that communicates to other PE routers for this vpnv4 prefix. The external label for the vpnv4 prefix from other PE routers is that of the attached vpnv4 prefix. It is the VPN tag that this EP uses when transferring traffic over the MPLS VPN network. Each vpnv4 prefix is assigned a unique MPLS tag in Cisco IOS which is also the default option.

3.2.3.3. Itinerary selection by BGP

Different BGP sockets can alert the vpnv4 route when, on request, a client area is native to two PE routers. The BGP receiving speaker should choose a BGP route as best it can. The process of selecting the vpnv4 route is the same as for IPv4 BGP routes. The only difference is that BGP itineraries are not 32 bit IPv4 prefixes but 96 bit vpnv4 prefixes. Thus if the client area is native to two PE routers, the incoming PE router takes the vpnv4 itinerary with two different BGPs of the other hop - namely the two PE dales routers. The input PE router applies the best BGP path selection process and installs one of the two BGP paths in the VRF routing table.

3.2.3.3.1. Multicast BGP

BGP selects only one path for each prefix it takes. This means that only one BGP path is installed in the IP routing table, which excludes the possibility of balanced loading. Multi-route BGP is a feature of BGP where the selection process still selects a BGP route as the best one but allows many BGP routes to be installed in the routing table.

Multicast BGP comes in three types: iBGP, eBGP and eiBGP. Multi-way iBGP is the installation of two or more internal BGP routes. Multi-way eBGP is the installation of two or more external BGP routes. eiBGP multi-path is the installation of one or more internal BGP paths and one or more external BGP paths. Not every BGP route can be chosen as many routes along with the best route. Some criteria must be met for a road to be used in multi-road BGP. The following BGP properties of alternative routes BGP must be identical to those of the best route for alternative routes to be used in parallel:

- Weight
- Local Preference Length
- AS-PATH Origin

- MED (Multi-exit discriminator)

One of the following:

- Autonom Autonomous neighborhood system (AS) or sub-AS (before many eiBGP properties to be added)
- AS-PATH (after eiBGP multi-path property is added) Metric IGP of other hop BGP

Table 3.1.1 shows what commands are used in the specific family of BGP addresses to configure multicast BGPs.

Table 5. BGP Multipath commands

BGP Multipath	*BGP address family command*
eBGP	***maximum-paths n***
iBGP	***maximum-paths ibgp n***
eiBGP	***maximum-paths eiBGP n***

- the ***"n"*** in the maximum-paths command of the BGP address family indicates how many paths can be installed in the IP routing table. The default value of n is 1, so the multipath BGP is deactivated from the recommended one.

3.2.4. Further transmission of packages

This section, illustrated with a specific example, looks at the life of an IP packet as it passes the MPLS VPN backbone from one client area to another. The MPLS VPN base blocks should be in place at the beginning. Multi-protocol iBGP must be executed between PE routers that distribute vpnv4 routers and their associated VPN tag. A DISTRIBUTION protocol should exist between all PE and P routers. This example

acknowledges that the label distribution protocol is LDP. Between PE and CE routers, a routing protocol must place the client itinerary on the VRF routing table on PE routers. And finally these itineraries should be distributed in the direction of MP-iBGP and vice versa. Figure 3.8 shows and explains this. Figure 3.8 shows the itinerary notification for the vpnv4 itinerary and the label from the outgoing PE to the incoming PE and the itinerary announcement to the IGP introducing the BGP of the other hop of the outgoing PE and the label to the incoming PE. The BGP address of the other hop in the outgoing EP is 10.200.254.2/32, where an IGP notifies the incoming EP.

The label for the IGP itinerary has been announced hop after hop by the LDP. Client IPv4 Itinerary 10.10.100.1/32 is notified by PE-CE routing protocol from CE to outgoing PE. The outgoing EP adds RD 1: 1, returns it to the vpnv4 itinerary 1: 1: 10.10.100.1/32 and launches it to the incoming EP labeled 30, via the multi-protocol iBGP.

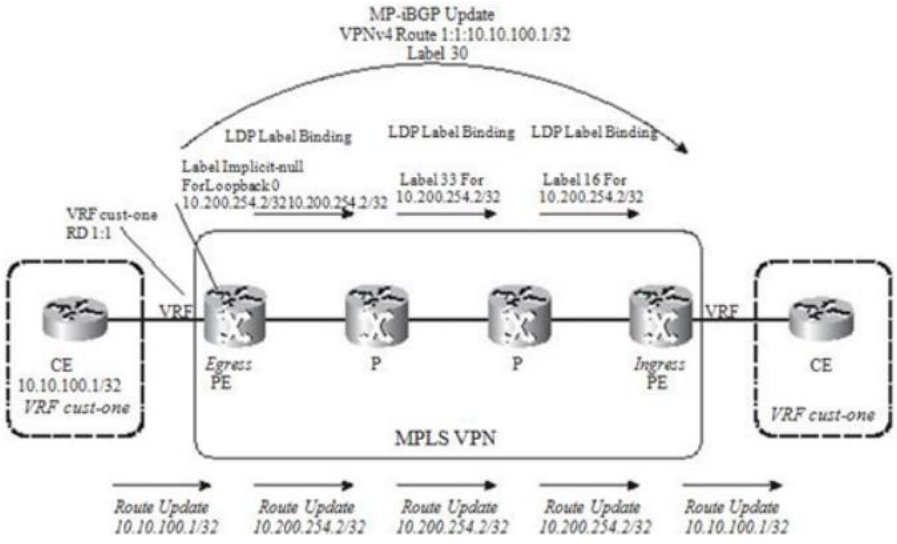


Figure 41. Life of an IPv4 packet along MPLS VPN backbone: Routes and label notifications

When an IP packet enters the PE input router from CE, the input PE router looks at the destination IP address in the VRF cust-one CEF table. The input PE router finds the appropriate VRF by looking at which interface the packet entered the PE router and with which VRF table this interface is associated. Specific entry in the VRF CEF table usually indicates that two labels need to be added.

When the input and output PE routers are directly connected, the packets will only have one VPN tag-tag. This is true as a result of PHP (penultimate hop popping). Initially the PE input router adds the VPN 30 tag as announced from the vpnv4 itinerary. This becomes the final label. The input PE router then pushes the IGP tag as the top tag. This tag is the tag associated with the IGP / 32 itinerary for the IP address of the BGP of the other hop. This is usually the IP address of the loopback interface in the outgoing email. This tag is notified hop by hop between P routers until it reaches the input PE router. Each hop changes the value of the label. its upper. The top tag — the IGP tag for the PE output router — is exchanged at each hop on the road. This tag delivers the IPv4 VPN packet to the appropriate output PE router. Usually — being the recommended behavior in Cisco IOS — PHP behavior takes place between the last P and the output PE router. Thus the IGP tag is placed on the last P router and the packet enters the output PE router with only one VPN tag on the tag stack. The output PE router looks at this VPN tag in the LFIB and makes a further transmission decision. Since the outgoing label is non-labeled, the remaining stack of labels is removed and the packet is further transmitted as an IP packet to the CE router. The outgoing PE router does not have to perform a remote view of the destination IP address on the IP header if the outgoing tag is unlabeled. The exact information of the other hop is found by looking at the VPN tag in LFIB. Only when the outgoing label is summary, then the outgoing PE router should perform an IP search in the VRF CEF table after the label looks in LFIB.

3.2.5. PE – CE routing protocols

Routing occurs between PE and CE routers. The PE-CE routing protocols supported by Cicso IOS are static routing, RIPv2, OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol), IS-IS (Intermediate System-to-Intermediate System) and eBGP.

3.2.5.1. Related itineraries

Connected itineraries are not routing protocols. However, to ensure connectivity, it is a good practice to redistribute the itineraries connected to the PE router to BGP. This way when the user executes a ping from a CE router to a remote CE router, the return packet is routed backwards. As recommended, if the user launches a ping and does not specify the source IP address, it takes as the source IP address the IP address of the outgoing interface, which in the case of the CE router is an IP address from the subnet to the PE-CE connection. So the return packet has an IP address as the destination IP address. So this prefix must be known in remote areas for ping to occur. It can be selected not to distribute subnets connected to the BGP but then a ping from CE to CE must be executed specifying a different source IP address on the CE router. This IP address will then be entered in the relevant PE-CE routing protocol. The same goes for other applications, such as Telnet.

3.2.5.2. Static Routing

Static routing is the easiest route to configure. However it can be annoying when many static itineraries have to be configured manually. To support VRF, static itineraries have been announced for VRF so they can be configured on PE routers to route traffic to VRF. Figure 42 shows a static routing for the prefix 10.88.1.1/32 indicating the next hop

10.10.2.1, which is the IP address of the interface on the PE-CE connection to the CE router. It can be seen that the static itinerary applies to the VRF cust one and that the itinerary is installed in the VRF routing table which is associated with the VRF cust-one.

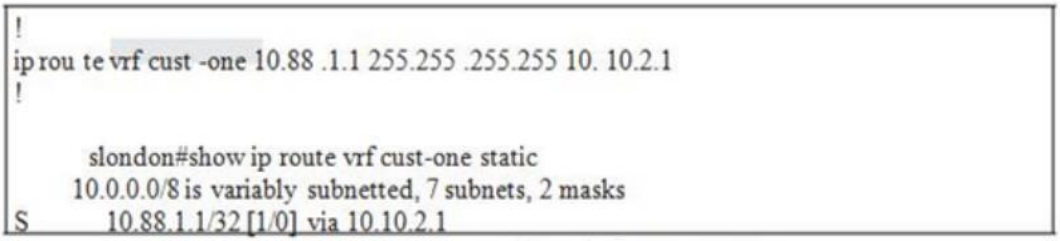


Figure 42. OSPF VRF configuration

To ensure that the static itinerary is learned from other PE routers as a vpnv4 itinerary, static itineraries to BGP should be distributed under the address family for a specific VRF.

3.2.5.3. RIP version 2

RIP (Routing Information Protocol) is a route vector routing protocol. It is limited in its use and is not a routing protocol used for wide area networks due to its slow convergence. However, it is still used in small networks as well as the quick-and-dirty routing protocols that do the job with respect to basic routing functions. RIP version 2 has seen some improvements regarding the first RIP specifications, but is still a limited routing protocol.

Some improvements are these:

- Introducing a subnet mask with prefixes
- Using milticast addresses 244.0.0.9 instead of broadcast ones 255.255.255.255
- Entering the next hop address

- Insert an itinerary label
- Use of authentication (optional)

On Cisco IOS, RIPv2 is supported as a routing protocol, but RIP version 1 is not.

3.2.5.4. OSPF

OSPF can be routing protocol in PE-CE connection. To spread the itineraries from PE to PE, OSPF is redistributed towards iBGP and vice versa to PE routers. The bottom line of this is that all OSPF itineraries become external itineraries to remote PE when itineraries are redistributed back to OSPF. The result of this would be that all OSPF itineraries that pass backbone MPS VPN will be less preferred than itineraries that do not pass backbone but that are sent through a backdoor link from an OSPF zone of another. To prevent all itineraries from turning into external OSPF prefixes, OSPF internal itineraries are reported as link-state advertisement [LSA] type 3) which are inter-zone itineraries - in PE when they are redistributed by BGP after OSPF . This is not normal behavior because PE routers redistribute BGP itineraries to OSPF and are ASBRs (autonomous system boundary routers) that must report itineraries as external OSPF itineraries (LSA type 5). In fact it looks like PE routers are ARB routers (area border routers) that announce summary itineraries to another area. However, all OSPF internal routes (intra-zone and inter-zone routes) become inter-zone routes (LSA type 3) after BGP distributes them, although the area number matches different PE routers. Figure 43 shows the distribution of OSPF itineraries along the MPLS VPN backbone.

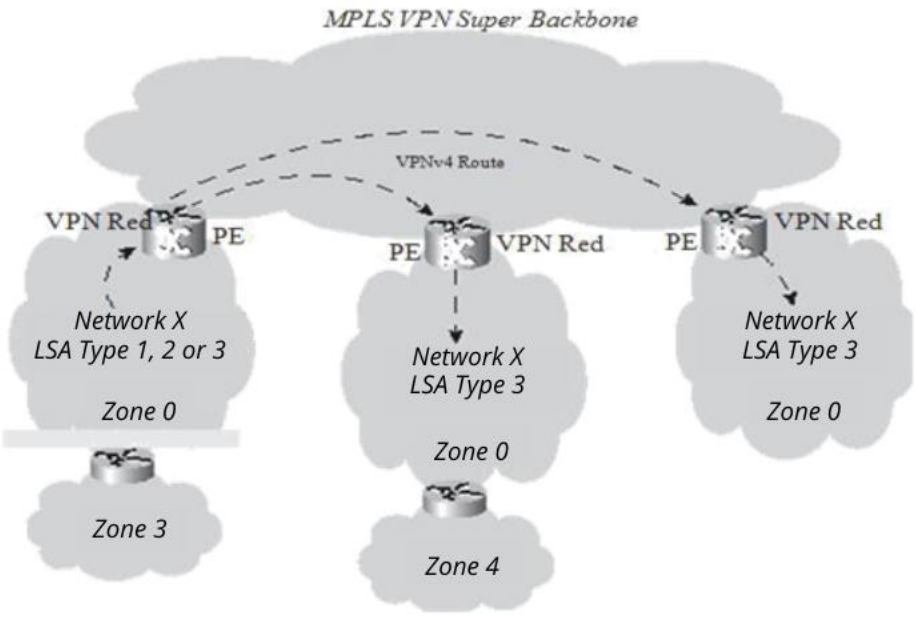


Figure 43. Internal OPSF itineraries along the MPLS VPN Backbone

The preference of normal OSPF itineraries makes intra-zone itineraries more preferable than interzonal OSPF itineraries. Since all internal OSPF itineraries become interzonal itineraries in remote areas, intrazonal itineraries can still cause a problem by becoming interzonal itineraries when a backdoor link exists between the zones. Intra-zone itineraries remain the same along the backdoor connection but become interzonal itineraries along the MPLS VPN backbone. So intra-zonal itineraries that are announced along the backdoor link are always preferred. To avoid this, a special link, called a sham link, must be configured between the PE routers. PE routers have OSPF areas interconnected. These areas can be backbone areas 0 or any other type of area. The MPLS VPN backbone can be considered as an added hierarchy that is higher than the OSPF backbone area: the MPLS VPN super backbone.

3.2.5.5. EIGRP

The EIGRP may be the PE-CE routing protocol. The usual redistribution disadvantage between iBGP and the routing protocol between the PE and the CE router is present here as well. This means that the redistribution of itineraries from BGP to EIGRP makes all itineraries external EIGRP itineraries. Anyway we have the coding of the most possible amount of EIGRP information in an extended new BGP community to solve this problem. This allows the PE remote router to rebuild the EIGRP itinerary with all its features, including metric components, AS, TAG and for extended itineraries, remote AS number, remote ID, remote protocol and remote metric. These are the EIGRP characteristics of a prefix found in the topology table. If the reported EIGRP itinerary is internal, the itinerary is reported as an internal itinerary to the remote area if the AS destination matches the AS resource held by the extended BGP community. If the AS numbers do not match the itinerary is reconstructed as an external EIGRP itinerary. Figure 44 shows how an EIGPR itinerary spreads across the MPLS VPN backbone from one EIGRP area to another.

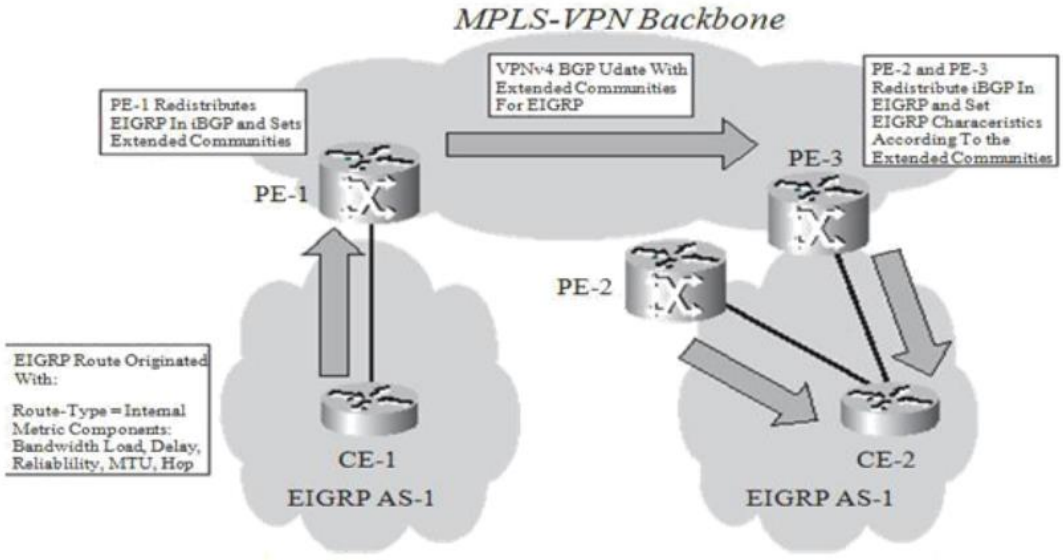


Figure 44. Distribution of the EIGRP itinerary along the MPLS VPN Backbone

On the right hand side, PE 2 and PE 3 redistribute the vpnv4 itinerary from iBGP to EIGRP. However the same itinerary can be taken as an EIGRP itinerary from the other PE router on the same side. However the vpnv4 itinerary learned from PE1 is always preferred over the EIGRP itinerary learned from another PE on the same side.

This is because the metric of the itinerary obtained is compared and the smallest metric always wins. This is always the vpnv4 itinerary from the PE remote router, if the cost of the EIGRP itinerary is calculated from the reconstruction of the metric components by the extended community. This is why EIGRP does not need a down bit as OSPF does. The indirect cost of MPLS VPN backbone is 0 for EIGRP itineraries.

3.2.5.6. Best Preliminary POI Path

The cost of community in BGP is a non-transient community which is passed on to iBGP and confederate peers but no further. It influences the choice of the best BGP route by assigning a cost value to each route. The community cost is set with the command set extcommunity cost on a route map. A community cost ID (0-255) and a cost value (0-4.294.967.295) can be set. The community cost ID indicates the preferences of this BGP route over others. The lower the ID cost, the more preferred it is.

The POI entry point is the area in the BGP route selection process where BGP considers the cost community. Best Preliminary Pathway POI indicates that BGP considers the cost of the community before each of the regular steps of comparing BGP in the well-known process of choosing the best BGP route. A cost community for the best pre-route can be configured by configuring the community cost with pre-bestpath keywords on the route map. Community cost is of the form Cost: POI: ID: value. [25]

It is the cost of the community with the best prior path that is decided when the EIGRP is redistributed to BGP. Without the community cost for EIGRP on the PE router,

the PE router always prefers the local source BGP itinerary over the iterated by the peer BGP. In the case of having a backdoor link between two EIGRP sides, this means that the backdoor link is the preferred path. With the cost community for EIGRP backdoor link on the one hand and the path learned by iBGP through the MPLS VPN backbone on the other hand, the comparison is made. The low cost EIGRP route is the preferred route. The cost control for EIGRP over MPLS VPN is automatically set in the case of EIGRP as the PE-CE routing protocol, so we do not have to configure it. POI is the best preliminary route. The community cost ID is either 128 or 129: 128 for internal EIGRP itineraries and 129 for external EIGRP itineraries. So internal EIGRP itineraries are always preferred over external one. The value of the EIGRP metric composite value is placed on the PE router that redistributes itineraries to BGP. Itineraries that have a low value are more preferred than itineraries that have a higher value. In the itinerary community cost ID the values are the same, Cisco IOS prefers the EIGRP itinerary over the BGP itinerary in the PE router.

Example 3.7 shows the cost community that EIGRP uses in MPLS VPN scenarios. The two PE routers report the vpnv4 prefix 10.10.100.1/32 and each sets the cost community of an ID equal to 128 and a value representing the EIGRP metric composite as viewed from the Sydney PE router. Sydney PE can choose the best route based on the cost community value that the PE router reports, ignoring other BGP attributes.

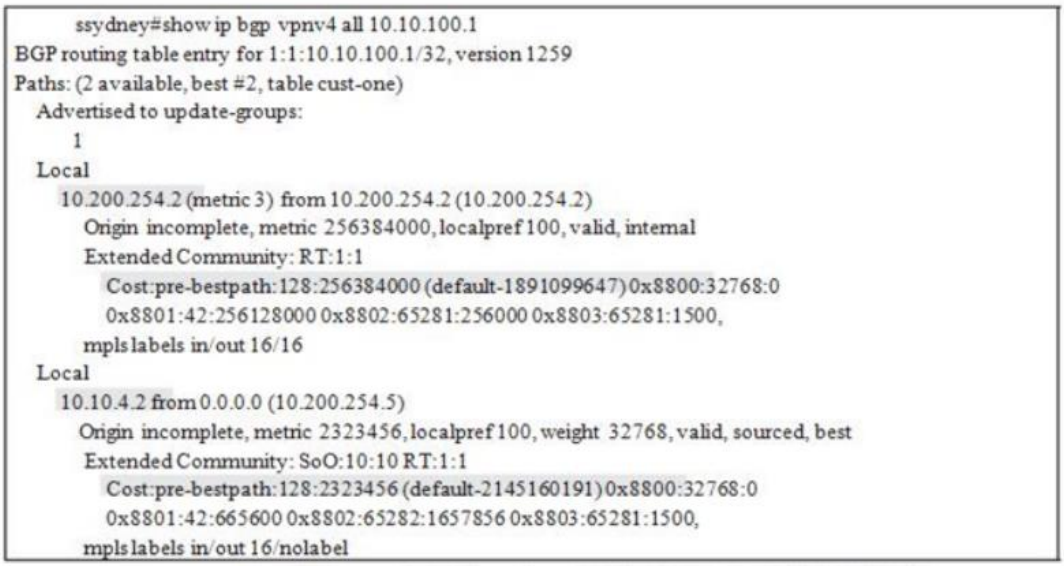


Figure 45. Cost community for EIGRP over MPLS VPN

3.2.5.7. IS-IS

A possible PE-CE routing protocol is IS-IS, which is a link state routing protocol like OSPF. However unlike OSPF, IS-IS runs directly in layer 2 and not over IP. In order for IS-IS to be executed during the PE-CE connection, ISIS is required to be notified of VRF on PE routers. ISIS can be configured for a VRF using the vrf vrf-name command under the IS-IS process. The IS-IS processes on a router differ from each other by the tag as configured with the router isis process-tag command.

The PE-CE connection to the appropriate IS-IS VRF process must be associated with the isis process-tag ip router interface command. As with OSPF, each VRF request has its own IS-IS routing processes (and SPF algorithms), IS-IS database, and routing table.

The top / bottom bit prevents routing loop when an IS-IS area is local to two locations. This bit has the same functionality as the bottom bit for OSPF over MPLS VPN. However, the top / bottom bit was not created to execute IS-IS over MPLS VPN. Introduced rapidly to prevent routing loops in the case of IP prefix notification from level 2 to level 1. (They can be called interarea itineraries). When an L1L2 router announces a level 2 prefix in LSP level 1, it must set the top / bottom bit. This way, another L1L2 router can view the set bit and does not distribute this prefix back to level 2. A PE router that distributes the learned vpnv4 iBGP itinerary to IS-IS places the top / bottom bit when announcing the prefix to IS-IS. Another PE router that looks at the IS-IS prefix with the top / bottom bit of vensour never distributes this prefix back to iBGP. [5]

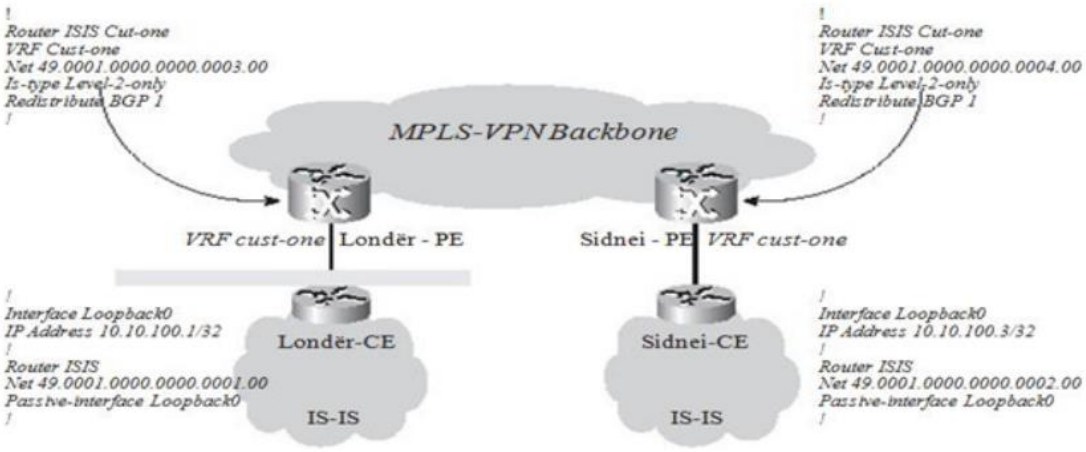


Figure 46. MPLS VPN over IS-IS

3.2.5.8. SOO

SOO uniquely identifies the area that originates an itinerary. It is an extended BGP community that prevents routing loops or subopsoinal routing, especially when a backdoor is present between VPN areas. SOO provides loop prevention in networks with dual local areas (areas which are connected to two or more PE routers). It can be used when an IGP is a PE-CE routing protocol. It can also be used when BGP is used between PE and CE, when preventing AS road bends could not be safer. [22] This happens when BGP uses an as-override or allowas. If the SOO is configured for a CE router and a vpnv4 itinerary is taught with the same SOO, the itinerary should not be placed on the VRF routing table in PE and notified in CE. In figure 3.12, the prefix vpnv4 is reported after the same area and taken in PE-3 via MP-BGP. When a PE-3 detects the same SOO in the vpnv4 itinerary as the SOO in the configuration, it does not install the prefix in the VRF routing table.

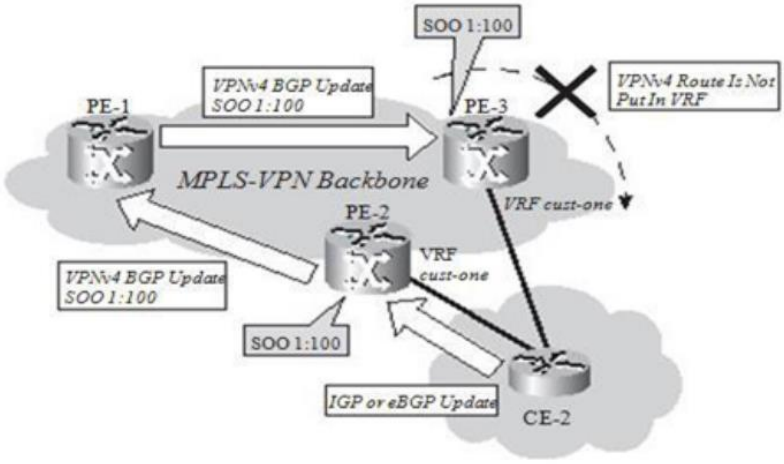


Figure 47. SOO preventing road loops

This prevents possible routing loops, but also prevents suboptional routing. The subopsional case that forces it to the local itineraries of the local dual areas, the path along the MPLS VPN backbone is preferred over the local path, is blocked. SOO can be set for

connected and static itineraries when they are redistributed to IGP. Example 3.8 shows the redistribute command with the SOO routing map.

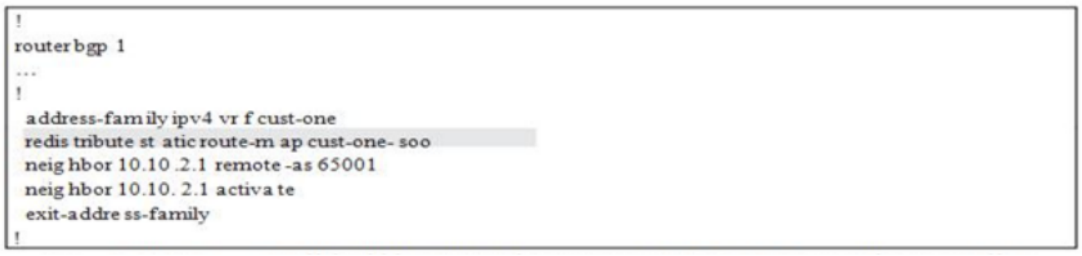


Figure 48. Application of SOO route map for the static routes

3.2.5.9. CE Management

It is often the SP and not the client who owns and manages the CE router. In this situation, SP wants management access to the CE router from a central management server. This can be done by having the PE router notified of a prefix by a CE router managed by an RT that is imported into the management VRF by the PE router connected to the VRF management. [25]

The number of prefixes reported with RT management can be limited by configuring an export map in each VRF that resets this RT management to only one prefix on the CE router. Regular VRF RTs used by VPNs can be notified with this prefix if other CE routers need to be able to reach it. Figure 3.13 is an overview of management organization. VRF management has a management station. PE router with VRF management imports all itineraries with RT 9000: 100. Sydney PE router sets the RT of a prefix in the CE router (here prefix 10.10.100.3/32; loopback prefix in the CE router) of 9000: 100.

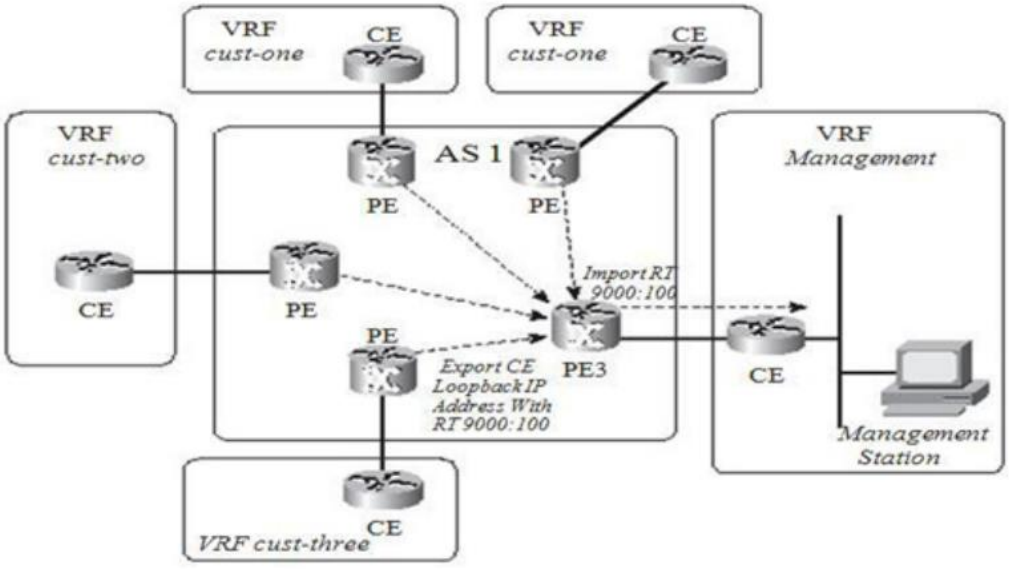


Figure 49. Example of a management access

The configuration of a PE router providing CE management access is shown in Figure 50.

```
!
hostna me sydney
!
ip vrf c ust-one
 rd 1:1
 expo rt map mana gement
 route-t arget expor t 1:1
 route-targe t import 1: 1
!
ip pr efix-list  C E-manageme nt-loopback seq 5 permit 10.10.100.3/32
!
route-map m anagement permit 10
 match ip addres s prefix-lis  t CE-managem ent-loopback
 set extcommunit y rt        9000: 100
!
```

Figure 50. Configuring an PE router that provides management access

Many SPs connect their MPLS VPN backbones. This can be done in two ways:

- Inter-Autonomus MPLS VPN
- CsC

- With Inter-Autonomus MPLS VPN, MPLS VPN networks create companions with each other and exchange client prefixes that have connected areas of each of the SPs. SPs should then provide connections between client sides even when they are not connected to just one MPLS VPN backbone. [21]

- CsC is a solution when a large carrier provides MPLS VPN services to other carriers or SPs. The service is hierarchical in nature, while the Inter-Autonomous MPLS VPN is simply an interconnection between MPLS VPN backbones that exchange client prefixes.

CHAPTER 4

RESULTS AND CONCLUSIONS

MPLS is a technology that combines the advantages of labeled transfer prevalent in Frame Relay & ATM technologies with the ease of packet delivery over IP networks. In MPLS the transmission of labels is done by looking at the label at the head of the package, which is changed hop by hop. The application of this technique by MPLS technology has highlighted a large number of advantages of this technology, which is spreading very fast nowadays. It has several advantages over previous technologies, which are:

Unified network infrastructure, which summarizes all existing networks into a single one that supports all types of services (this constitutes the so-called any type of transport over MPLS). This results in a better QoS (bandwidth guarantee, latency and burst size), real-time IP over voice (voice over IP) services, triple play, etc.

MPLS offers scalability. Transit route routing tables do not have to be complete, fast label retrieval versus long prefix matches, differentiated service classes, label hierarchy (depending on scalability), fast defect recovery in less than 50 ms. MPLS introduces connection model oriented to IP networks Creating secure virtual private networks MPLS VPN (tags "hide" IP addresses of public network users). Advantages in number of VPNs, number of members for VPN and special tunnels between parts.

Service flexibility thanks to the FEC (packages that follow the same path in the MPLS network are treated in the same way by the LSR, receive the same label). Types of services and resources can be associated with an FEC at LSP.

Implementing traffic engineering facilitates the control of a very busy traffic.

Implementing MPLS technology in a telecommunications company network brings several advantages in terms of applications that can be offered by the company:

Convergence of existing networks (telephony, internet and data) into a single network. Ability to broadcast any type of service over the network.

Providing triple play services (data, internet, telephone), IP video, IPTV, intranet. Providing internet and some other broadband services. Providing MPLS VPN service with all its options.

Optimal traffic flow (Traffic engineering, BGP-free core and network scalability).

REFERENCES

[1] J. Israr, M. Guennoun and H. T. Mouftah, Credible BGP - Ectensions to BGP for Secure Networking, Porto: IEEE, 2009.

[2] W. Ming-Hao, The Security Analysis and Attacks Detection of OSPF Routing Protocol, Changsha: IEEE, 2015.

[3] U. S. Masruroh, K. Hamdi, P. Widya, A. Fiade and R. I. Julia, Performance Evaluation DMVPN using Routing Protocol RIP, OSPF, EIGRP, Parapat: IEEE, 2019.

[4] H. B. Chandana and P. Darsini, Inter-Provider VPN network using back-to-back VRF and MP-eBGP method, Chennai: IEEE, 2017.

[5] V. Jain and S. A. Gandhi, An Architecture for Implementation of IEEE1588v2 over MPLS/MPLS-TP Networks, Bhopal: IEEE, 2014.

[6] A. Bahnasse, M. Talea, A. Badri and F. E. Louhab, New Smart Platform for automating MPLS virtual private network simulation, Marrakech: IEEE, 2018.

[7] M. K. Porwal, A. Yadav and S. V. Charhate, Traffic Analysis of MPLS and non MPLS Network including Signaling Protocols and Traffic Distribution in OSPF and MPLS, Nagpur: IEEE, 2008.

[8] F. Le Faucheur, IETF Multiprotocol Label Switching (MPLS) Architecture, Colmar: IEEE, 2002.

[9] I. Hussain, Overview of MPLS technology and traffic engineering application, Lahore: IEEE, 2004.

[10] R. Zheng and W. Yang, H-MPLS: A lightweight NFV-based MPLS solution in access network, Las Vegas: IEEE, 2014.

[11] I. Joe and H. Lee, GM-MPLS: Group-based Mobile for mobility management in wired/wireless network, Gyeongju: IEEE, 2010.

[12] M. Hlozak, J. Frnda, Z. Chmelikova and M. Voznak, Analysis of Cisco and Huawei routers cooperation for MPLS network design, Belgrade: IEEE, 2014.

[13] A. Diad, R. Boringer and A. Mitschele, Optimized I-MPLS: A Fast and Transparent Micro-Mobility-Enabeled MPLS Framework, Valencia: IEEE, 2006.

[14] Y. Qiu, H. Zhu, Y. Zhou and J. Gu, A Research of MPLS-Based Network Fault Recovery, Shenyang: IEEE, 2010.

[15] N. Angelescu, D. C. Puchianu, G. Predisca, L. D. Circiumarescu and G. Movila, DMVPN simulation in GNS3 network simulation software, Targoviste: IEEE, 2017.

[16] S. Mehraban, K. B. Vora and D. Upadhyay, Deploy MPLS using VRF, Tirunelveli: IEEE, 2018.

[17] C. Jacquenet, G. Bourdon and M. Boucadair, Dynamic Enforcement of Security Policies in IP/MPLS Environments, Wiley, 2008.

[18] S. Sinha, R. Chowdhury, A. Das and A. Ghosh, Comparative Analysis Amid National and International MPLS Local Loop Optimization and Commercial Impact, Singapore: IEEE, 2019.

[19] I. J. Mohamad, T.-C. Wan, F. Y. Alzyoud and P. Sumari, Optimizing the MPLS support for real time IPv6-Flows using MPLS-PHS approach, Singapore: IEEE, 2009.

[20] S. Yadav and A. Jeyakumar, Design of traffic engineered MPLS VPN for protected traffic using GNS simulator, Chennai: IEEE, 2016.

[21] S. Yadav and A. Jeyakumar, MPLS multi-VRF design and implementation using GNS simulator, Coimbatore: IEEE, 2016.

[22] P. Chumchu, S. Sirisaingkarn and T. Mayteevarunyou, Performance analysis and improvement of mobile MPLS, Kuala Lumpur: IEEE, 2011.

[23] W. Gray, A. Tsokanos and R. Kirner, Multi-Link Failure Effects on MPLS Resilient Fast-Reroute Network Architectures, Daegu: IEEE, 2021.

[24] M. Zhang and Z. Tao, Application Research of MPLS VPN All-in-One Campus Card Network based on IP-Sec, Chongqing: IEEE, 2012.

[25] H. Hodzic and S. Zoric, Traffic engineering with constraint based routing in MPLS networks, Borik Zadar: IEEE, 2008.

[26] M. A. Rahman, Z. Hassan, A. H. Kabir, K. A. M. Lutfullah and M. R. Amin, Performance Analysis of MPLS Protocols over conventional Network, Shanghai: IEEE, 2008.

[27] R. Guedrez, O. Duegon, S. Lahoud and G. Texier, Label encoding algorithm for MPLS Segment Routing, Cambridge, MA: IEEE, 2016.

[28] W. Xie, S. Huang and W. Gu, An improved ring protection method in MPLS-TP networks, Beijing: IEEE, 2010.

[29] The design, implementation and performance analysis of transport-MPLS network, Beijing: IEEE, 2009.

[30] M. A. Rahman, A. H. Kabir, K. A. Lutfullah, M. Z. Hassan and M. R. Amin, Performance analysis and the study of the behavior of MPLS protocols, Kuala Lampur: IEEE, 2008.

In the Project below I have implemented all the mentioned tasks above.

APPENDIX A

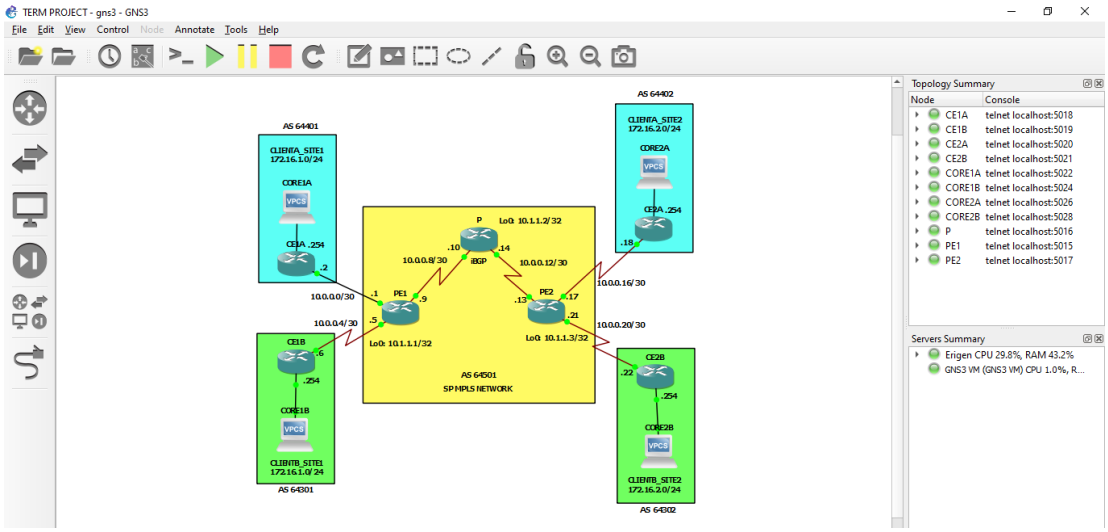


Figure 51. Project implemented on GNS3 simulator

APPENDIX B

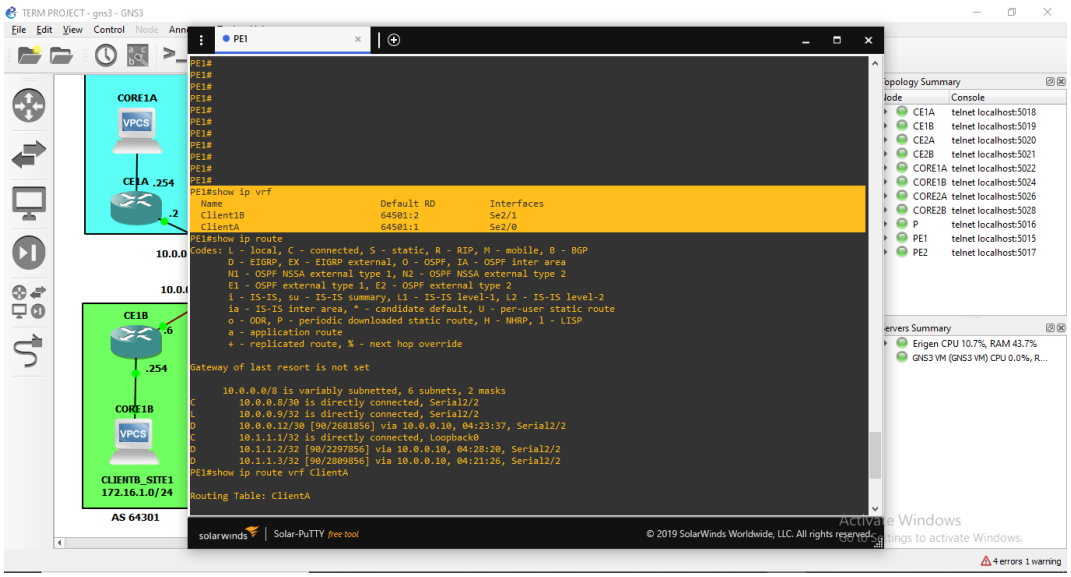


Figure 52. *"show ip vrf"* command

APPENDIX C

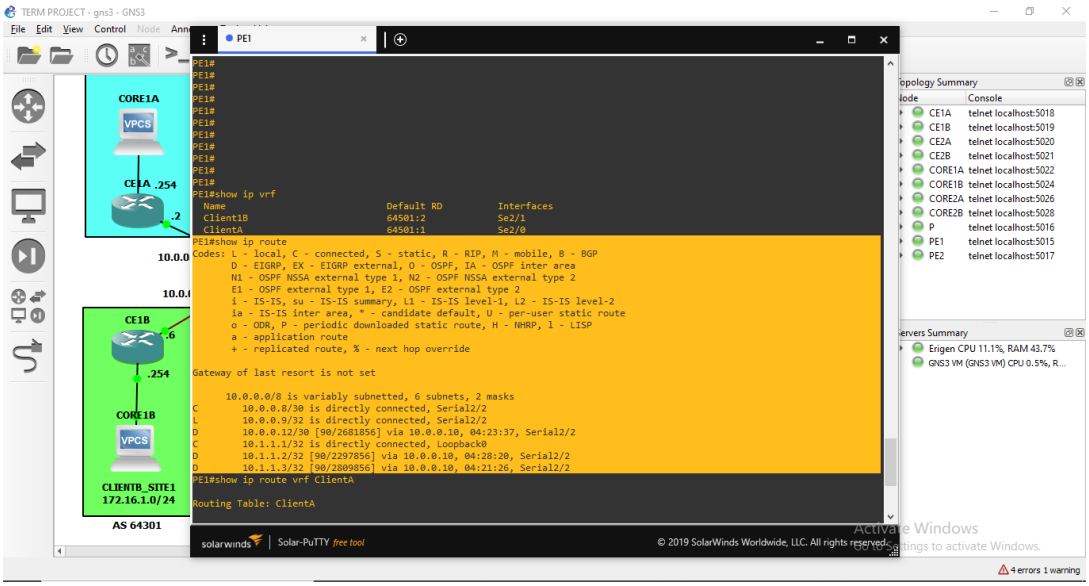


Figure 53. *"show ip route"* command

APPENDIX D

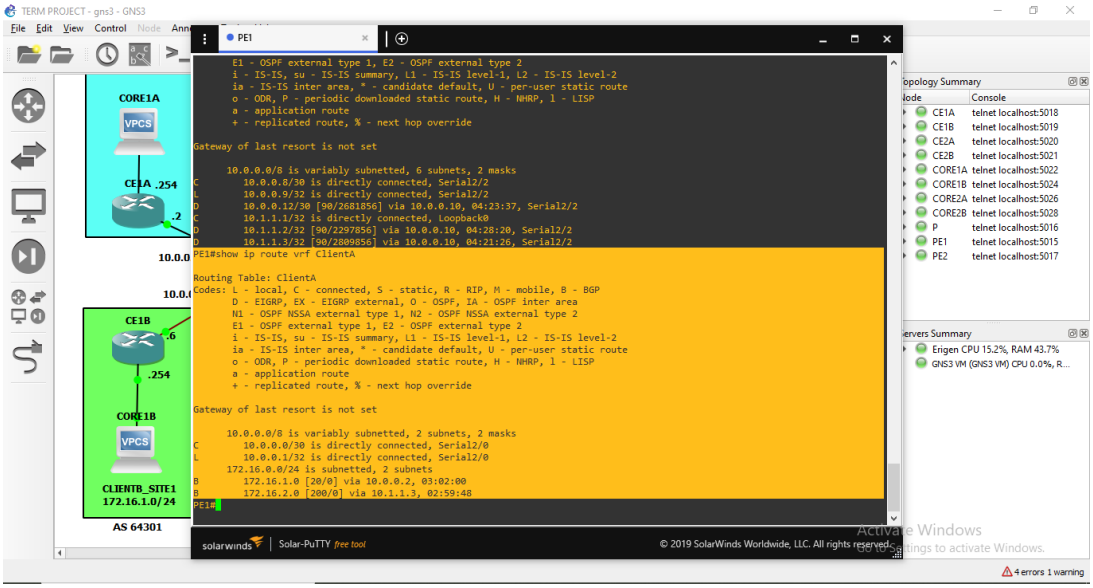


Figure 54. *"show ip route vrf [vrf-name]"* command

APPENDIX E

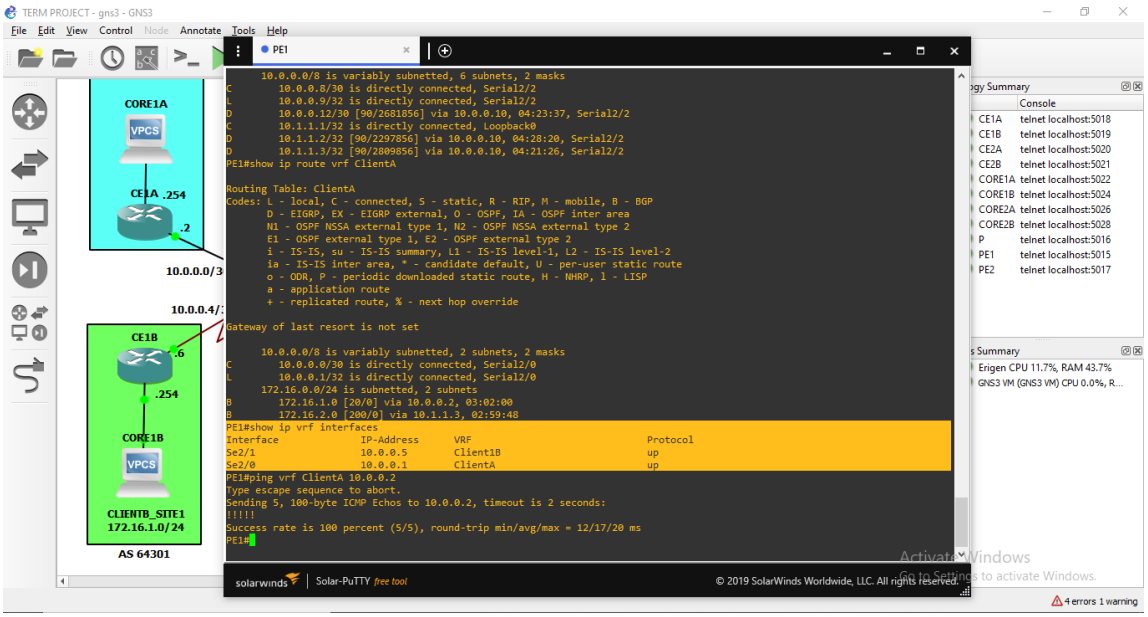


Figure 55. *"show ip route vrf interfaces"* command

APPENDIX F

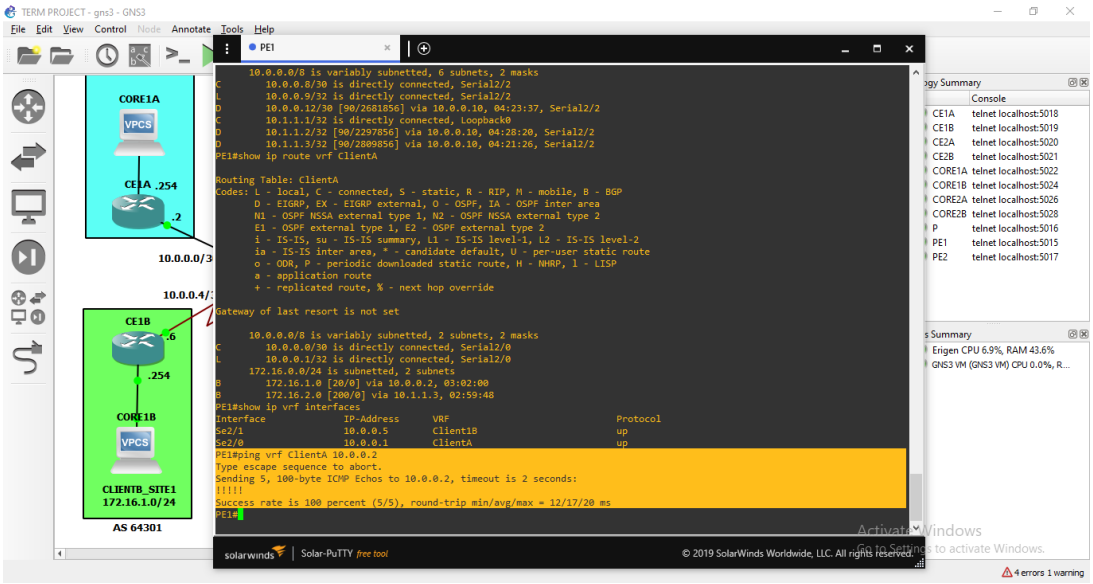


Figure 56. *"ping [vrf-name ipv4-address]* command

➔ Also I will show all my configuration commands below:

PROVIDER#show running-config

```
hostname P
no ip domain lookup
interface Loopback0
 ip address 10.1.1.2 255.255.255.255
no shutdown
interface Serial2/2
 description P -> PE1
 ip address 10.0.0.10 255.255.255.252
 mpls ip
no shutdown
interface Serial2/3
 description P -> PE2
 ip address 10.0.0.14 255.255.255.252
 mpls ip
no shutdown
!
router eigrp 1
 network 10.0.0.8 0.0.0.3
 network 10.0.0.12 0.0.0.3
 network 10.1.1.2 0.0.0.0
!
ip forward-protocol nd
!
```

```
no cdp log mismatch duplex
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
```

PROVIDER_EDGE1#show running-config

```
hostname PE1
ip vrf Client1B
 rd 64501:2
 route-target export 64501:2
 route-target import 64501:2
!
ip vrf ClientA
 rd 64501:1
 route-target export 64501:1
 route-target import 64501:1
!
no ip domain lookup
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
no shutdown
!
interface Serial2/0
 description PE1 -> CE1A
 ip vrf forwarding ClientA
 ip address 10.0.0.1 255.255.255.252
no shutdown
!
interface Serial2/1
```

```
 description PE1 -> CE1B
 ip vrf forwarding Client1B
 ip address 10.0.0.5 255.255.255.252
no shutdown
!
interface Serial2/2
 description PE1 -> P
 ip address 10.0.0.9 255.255.255.252
 mpls ip
 serial restart-delay 0
!
router eigrp 1
 network 10.0.0.8 0.0.0.3
 network 10.1.1.1 0.0.0.0
!
router bgp 64501
 bgp log-neighbor-changes
 neighbor 10.1.1.3 remote-as 64501
 neighbor 10.1.1.3 update-source Loopback0
 !
 address-family ipv4
  neighbor 10.1.1.3 activate
 exit-address-family
 !
 address-family vpnv4
```

```
 neighbor 10.1.1.3 activate
 neighbor 10.1.1.3 send-community extended
exit-address-family
!
address-family ipv4 vrf Client1B
 neighbor 10.0.0.6 remote-as 64301
 neighbor 10.0.0.6 activate
exit-address-family
!
address-family ipv4 vrf ClientA
 neighbor 10.0.0.2 remote-as 64401
 neighbor 10.0.0.2 activate
exit-address-family
!
ip forward-protocol nd
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
```

```
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
!
end
```

PROVIDER_EDGE2#show running-config

```
hostname PE2
ip vrf Client2A
 rd 64501:1
 route-target export 64501:1
 route-target import 64501:1
!
ip vrf Client2B
 rd 64501:2
```

```
 route-target export 64501:2
 route-target import 64501:2
!
no ip domain lookup
!
interface Loopback0
 ip address 10.1.1.3 255.255.255.255
no shutdown
!
interface Serial2/3
 description PE2 -> P
 ip address 10.0.0.13 255.255.255.252
 mpls ip
 no shutdown
!
interface Serial2/4
 description PE2 -> CE2A
 ip vrf forwarding Client2A
 ip address 10.0.0.17 255.255.255.252
 no shutdown
!
interface Serial2/5
 description PE2 -> CE2B
 ip vrf forwarding Client2B
 ip address 10.0.0.21 255.255.255.252
```

```
 no shutdown
!
router eigrp 1
 network 10.0.0.12 0.0.0.3
 network 10.1.1.3 0.0.0.0
!
router bgp 64501
 bgp log-neighbor-changes
 neighbor 10.1.1.1 remote-as 64501
 neighbor 10.1.1.1 update-source Loopback0
 !
 address-family vpnv4
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf Client2A
  neighbor 10.0.0.18 remote-as 64402
  neighbor 10.0.0.18 activate
 exit-address-family
 !
 address-family ipv4 vrf Client2B
  neighbor 10.0.0.22 remote-as 64302
  neighbor 10.0.0.22 activate
 exit-address-family
```

```
!
ip forward-protocol nd
!
control-plane
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
```

```
!
end
```

CUSTOMER_EDGE1_A#show running-config

```
hostname CE1A
no ip domain lookup
!
interface GigabitEthernet1/0
 description LINK-TO-LAN1A
 ip address 172.16.1.254 255.255.255.0
 no shutdown
!
interface Serial2/0
 description CE1A -> PE1
 ip address 10.0.0.2 255.255.255.252
 no shutdown
!
router bgp 64401
 bgp log-neighbor-changes
 network 172.16.1.0 mask 255.255.255.0
 neighbor 10.0.0.1 remote-as 64501
!
ip forward-protocol nd
!
mgcp behavior rsip-range tgcp-only
```

```
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
!
end
```

CUSTOMER_EDGE2_A#show running-config

```
hostname CE2A
no ip domain lookup
!
interface GigabitEthernet1/0
```

```
 description LINK-TO-LAN2A
 ip address 172.16.2.254 255.255.255.0
 no shutdown
!
interface Serial2/4
 description CE2A -> PE2
 ip address 10.0.0.18 255.255.255.252
 no shutdown
!
router bgp 64402
 bgp log-neighbor-changes
 network 172.16.2.0 mask 255.255.255.0
 neighbor 10.0.0.17 remote-as 64501
!
ip forward-protocol nd
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
```

```
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
!
end
```

CUSTOMER_EDGE1_B#show running-config

```
hostname CE1B
no ip domain lookup
!
interface GigabitEthernet1/0
 description LINK-TO-LAN1B
 ip address 172.16.1.254 255.255.255.0
 no shutdown
!
interface Serial2/1
 description CE1B -> PE1
 ip address 10.0.0.6 255.255.255.252
 serial restart-delay 0
```

```
!
router bgp 64301
 bgp log-neighbor-changes
 network 172.16.1.0 mask 255.255.255.0
 neighbor 10.0.0.5 remote-as 64501
!
ip forward-protocol nd
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
```

```
 transport input all
!
end
```

CUSTOMER_EDGE2_B#show running-config

```
hostname CE2B
no ip domain lookup
!
interface GigabitEthernet1/0
 description LINK-TO-LAN2B
 ip address 172.16.2.254 255.255.255.0
 no shutdown
!
interface Serial2/5
 description CE2B -> PE2
 ip address 10.0.0.22 255.255.255.252
 no shutdown
!
router bgp 64302
 bgp log-neighbor-changes
 network 172.16.2.0 mask 255.255.255.0
 neighbor 10.0.0.21 remote-as 64501
!
ip forward-protocol nd
!
```

```
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
!
end
```