Dancun Ogenda

Cisco and Juniper Interoperability

MPLS Layer 3 Virtual Private Network Between Cisco and Juniper

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

30 January 2016

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Dancun Ogenda Cisco and Juniper Interoperability: MPLS Layer 3 Virtual Private Network Between Cisco and Juniper 56 pages + 0 appendices 30 January 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunication and Data Networks
Instructor(s)	Matti Puska, Senior Lecturer

The goal of this project was to design, implement and verify a MPLS Layer 3 Virtual Private Network. The task included building a functioning MPLS Network that consists of the MPLS Backbone together with a Customer Edge and the Customer Site equipment's. The MPLS Backbone was to consist of the Provider Devices and the Provider Edge devices, which is used as a connection point to the Customer Edge devices. The MPLS was to only function inside the MPLS Backbone and the Provider devices were to be connected using internal BGP. For the connection between the Provider Edge and the Customer Edge, external BGP protocol was to be used.

MPLS is basically a standard used in the speeding of the delivery of packets across different platforms. By using MPLS, the area that is in the MPLS Backbone is connected using the internal BGP. This is the only area that the MPLS information is to be communicated. For the area between the Provider Edge and the Customer Edge, external BGP protocols is to be used and does not need any MPLS information or configuration. Then it is needed for an MPLS Layer 3 VPN to be built above the MPLS network; which is normally from the Service Provider. This Layer 3 VPN is used to deliver and ensure connectivity between different customers in varied geographical locations. The next task is to assume that either of two PE equipment is running the Juniper´s JunOS or Cisco IOS. This then necessitates the configuration to make the two, which can either be a router and a switch to communicate with each other and thus allow flow of packets between them.

The result of the project was that after the configurations, it was possible to get a connection from the Switch/Router running JunOS and the Switch/Router running the Cisco IOS. The goal of the project was further to delve into and achieve an end-to-end connectivity between the L3VPN´s configured on either side of the CE. This goes to prove that even though different entities might be using different networking equipment from different vendors, it is possible to make the devices communicate with or to each other and thus provide a seamless flow of traffic/packets as if the same producer made them.

Keywords	MPLS, L3VPN, CE, PE, VRF, VPN

Contents

Abbreviations

AS	Autonomous System. This is a router's unit policy for either a single or group of networks controlled by a same administrator.
CE	Customer Edge. This is the router at the Premises of the customer that connects to the service provider edge routers in an MPLS network.
CLI	Command Line Interface. A human-computer interface that relies on text input and output.
EIGRP	Enhanced Interior Gateway Protocol. An advanced distance-vector routing protocol used to automate configuration and routing decisions. It is a Cisco proprietary protocol.
IOS	Internetwork Operating System. Sophisticated operating system developed by Cisco for internetworking between routers and switches.
ISP	Internet Service Provider. It is an organisation providing services that enable the accessing of the internet possible.
IBGP	Internal Border Gateway Protocol. This is the protocol that is used between routers that are in the same Autonomous System.
IGP	Interior Gateway Protocol. A protocol that is used between gateways in the exchange of routing information between routers in an Autonomous System.
JunOS	Juniper Operating System. This is an Operating System developed by Juniper for its routers and switches.
LDP	Label Distribution Protocol. A protocol that is used by routers that support Multiprotocol Label Switching in the exchange of label information between routers.
L3VPN	Layer 3 Virtual Private Network. This is a form of Virtual Private Network that is built and whose operation depends on the Layer 3 Open System Interconnection.
MP-BGP	Multi-Protocol Border Gateway Protocol. It is a BGP extension allowing for the possibility of parallel address families distribution.
MPLS	Multi-Protocol Label Switching. A technique employed in the high-performance telecommunication networks for carrying data between different network nodes.

NLRI	Network Layer Reachability Information. This is a keyword that is used in the description of the unicast and multicast database forwarding.
OS	Operating System. This is a software that supports the basic function of the routers and switches and even computers. They help in performing tasks such as peripheral control and even activity scheduling.
OSPF	Open Shortest Path First. This a one of the routing protocols for networks in IP.
PE	Provider Edge. This is the router found in the provider core and that directly connect to the CE routers.
QoS	Quality of Service. This is the ability or the capability of a given network to offer better service for the traffic involved.
RIP	Routing Information Protocol. This is a dynamic protocol that is used when there is need to find a best path from one end of the network to the other by the use of an algorithm known as hop count.
RD	Route Distinguisher. This is basically an address qualifier that is used in MPLS networks in areas where a single network provider is involved. It is used in the route separation between different Virtual Private Network routes that are customer involved and that are connected to the service provider core network.
RT	Route Target. This is a prefix that is 64 bit long and used in the prefix tagging. Serves as an indication to the PE routers as to which prefixes are to be imported or not.
VPN	Virtual Private Network. A network construction that use the internet to connect different private networks.
VPNv4	Version 4 Virtual Private Network. These are VPNs that support IPV4 addressing. This comprises of the customer IPv4 routes being added to the Route Target to create VPNv4 routes.
VRF	Virtual Routing and Forwarding. This is a technology that allows for multiple routing instances in the same router to co-exist.

1 Introduction

The need for Virtual Private Networks (VPNs) has never been much important than at this age and time when companies as well as individuals need secure networks. Again, many individuals work from home necessitating the need for companies to provide secure connections to them. This is vital in order for them to realise their work, either from home or the business premises. This is where the VPNs comes into play in enabling service providers to give a tunnel-like connection to the customers or businesses. Depending on the management agreements and or contracts, either the customer or the service provider can see the information that flows through the tunnels and has the control of the different equipment or the configuration and maintenance of the same.

The second component here, is that, there are many manufactures of networking equipment and in this paper, since the project tend to be inclined on Cisco and Juniper, only these two will be discussed and considered at length. The choice of which vendor to purchase from, solely lies with the people the company entrust to build their networks as they make choices, differences and comparisons and provide reasons for the favourability of one vendor over the other.

The ability of a particular organisation to have switches and/or routers from different vendors then results in a situation where many different organizations will be running and using different equipment. The problem that arises is that the different manufacturers of the networking equipment, each have a different way of building their networking machines architecture-wise and they run different Operating Systems (OSs) and different vendor protocols which might be same but implemented in totally different ways. The configuration scenarios and the nature of the commands too tend to differ widely from one manufacture to the other. This thus, necessitates the situation where the routers are made to understand and communicate with each other. An instance is an illustration of where one company uses, the Cisco routers that run Internetwork Operation System (IOS) and the other uses the Juniper routers running the JunOS. When the two companies would like to connect their equipment and ensure the flow of traffic from one organization to the other, then the two equipment from the two vendors have to be configured in a way that enables them to work together and thus transfer information (interoperable).

The purpose of this project is to communicate the interoperability of a Multiprotocol Label System Layer 3 Virtual Private Network (MPLS L3VPN). In addition, technologies that assist in the interoperability and different standards that are proprietary and multivendor will be discussed. These will be discussed in this paper and different interpretations of the same offered. Terms and other important factors that are necessary for the implementation and the final results will be shown. The security of the MPLS L3VPNs, Internet Protocol Version 6 VPNs and technologies such as Cisco IOS Internet Protocol security are all left out of this project as those are advanced technologies that are not yet fully implemented and whose support are not fully developed.

The reason for the choice of this project relates to its relevance and importance. Almost everyday thousands if not millions of companies and individuals contract and buy respectively, from the service providers'; and one of the most important service they buy or contract is the VPN, which may either be Hybrid VPN, Multiprotocol Packet Label Switching VPN or even Secure Sockets Layer. So it is considered to be one of the most important services from the service provider perspective; that is offered by them and from the businesses and/ or the consumers perspective, a secure way to connect to the network and enable them achieve their goals and objectives; network wise.

The next chapter discusses the background information related to both Cisco and Juniper, their different OS, the advantages and disadvantages that necessitate the choice of one over the other and finally the historical backgrounds of the two vendors.

2 Background Information

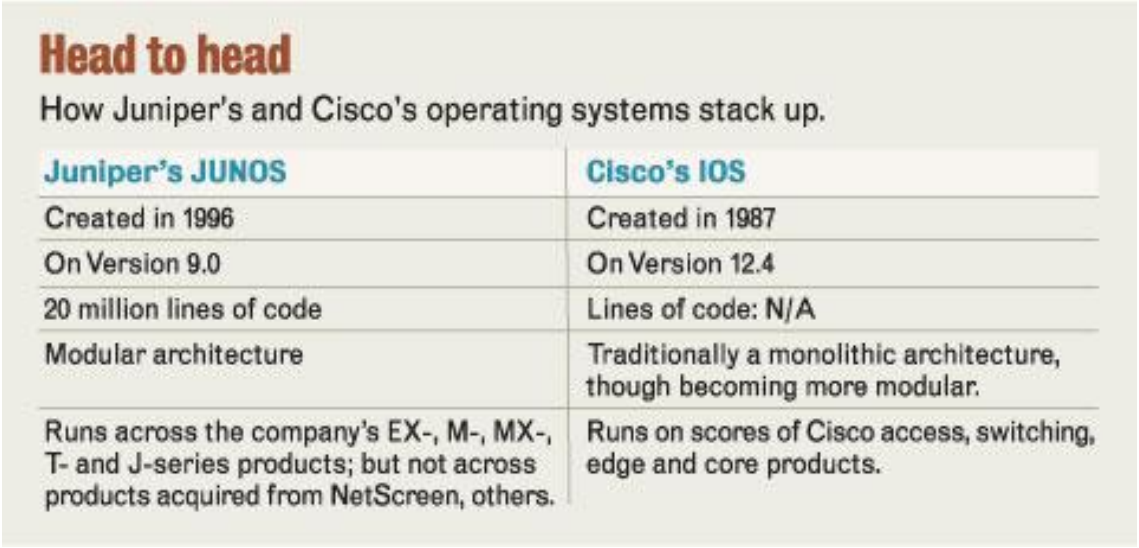
This chapter serves to offer an in-depth explanation, and analysis of the different vendors of networking (routing and switching) equipment, important background information related to them, differences between the major leading vendors (Cisco and Juniper), the different standards enabling the devices from the different vendors to work seamlessly. In addition, the benefits offered by the routers and/or switches and the disadvantages necessitation the choice of one over the other and the benefits that are offered by standards are discussed.

2.1 Cisco and Juniper Background

Since the project was about the interoperability of Cisco and Juniper, this part chapter will tend to be biased towards the two. Cisco is a pioneer in the manufacture of networking equipment and was founded in the early 1980s (1984). Three years after its inception, it developed its first IOS in 1987. Juniper on the other hand was founded in the 1990s (1996) and in the same year came up with the Juniper Operating System (JunOS). [1]

The major functions of the different networking equipment whether from Cisco or Juniper, are mainly, for routing and/or switching of packets. In this context, all routers and switches perform virtually same functions. The choice of whether to implement and build a single-vendor (i.e. all routers and/or switched being from the same vendor) or multi-vendor (i.e. the routers and/or switches being a mix from different vendors) rests solely with the network engineers or third-party-companies that are contracted to build the networks. Even though the choices and decisions rests with them, there are many factors that will influence from which networking vendor to purchase and what equipment in particular to buy.

After years of of relative success enjoyed by Cisco, with the advent of Juniper and other networking equipment vendors, competition began. The only way for Cisco to maintain the success that it enjoyed beforehand was to try and be more innovative. Later as Juniper started to cut on Cisco’s success, smear campaigns and other tactics came in. Before further description of the arguments between Cisco and Juniper each in order to justify its OS, a brief summary of the important historical information is presented as shown in the table 1 below.



Head to head

How Juniper's and Cisco's operating systems stack up.

Juniper's JUNOS	Cisco's IOS
Created in 1996	Created in 1987
On Version 9.0	On Version 12.4
20 million lines of code	Lines of code: N/A
Modular architecture	Traditionally a monolithic architecture, though becoming more modular.
Runs across the company's EX-, M-, MX-, T- and J-series products; but not across products acquired from NetScreen, others.	Runs on scores of Cisco access, switching, edge and core products.

Figure 1. Cisco and Juniper Comparison. Copied from Network World [3].

The table above show the different historical achievements by both Cisco and Juniper, the different ways that the OSs were coded, the nature of their architectures and the different platforms that the OSs run on. As the writer claims, Cisco had an overhead of 20+ years before Juniper was founded. After 10 years, Juniper's aim was to cut Cisco's dominance in the market share. Juniper has to maintain a standard and taint Cisco's IOS as fragmented while presenting their JunOS as fixing the problems that were posed by IOS. Juniper created JunOS in 1996 and the first version was 9.0. JunOS was written on close to about 20 million lines of code and it runs across different products such as the EX, M, MX, T and even the J series. As for Cisco, it was founded in 1984 and developed its first IOS in 1987 as version 12.4. At the time of writing this paper, the releases 12.4 and a vast majority of 12.4T had announced the end of sale and Cisco recommended customer migration to the Cisco IOS Software release 15.0(1) M. Lines of code were not applicable. The IOS runs across a score of Cisco's access, edge, switching and core products. [2,3]

The battle between Cisco and Juniper stem from the belief on Juniper's part that Cisco has many variations of its IOS. To counter the argument, Cisco claims that Juniper has more than one version of JunOS contrary to Juniper's claim of having one. Juniper has a modular OS that it says when used across its platforms help in cost cuts and ease of management and operation. Cisco with the dawn of each product, brings with it a new IOS thus, making the previous IOS almost forgotten with continuous advent.

This claim by Juniper seems to be working in their favour, as in 2007, Cisco had 82% of the market share categorised at 4.2 billion USD of the enterprise-router, 4.7 billion USD of the service-provider edge-router market and 2.7 billion USD of the service provider core routers that in percentages translate to 54% and 55% respectively of the total market share value. Juniper came a second close to Cisco, with 5% of enterprise-router market, 18% of SP edge router market and 30% in SP core-router market. As for LAN switching, Cisco was in control of 71.5% of the market valued at 18 billion USD in the year 2007. Juniper had no control at the time the report was conducted, but with the invention of its EX line of products, it is on the verge of competing for this market [3].

The following subheadings serves to go into detail and further explore each of the vendor's OS individually and provide a detailed review.

2.2 Cisco's IOS

The Cisco IOS in the simplest terms is the proprietary networking software that is used in the Cisco equipment which might be the router or switches. The function of the Cisco IOS is the provision of unification principles that can be used to maintain the network with the smallest amount of cost-outlay over a given period of time. It is in essence software and it can be differentiated from the hardware and it can be upgraded or changed to make it workable with the different technologies that are developed at varied time intervals. It is the most important part of the internetworking components [4].

The major task of the Cisco IOS is to ensure that, in between the network nodes data can be communicated. Apart from the well-known functions of the Cisco IOS, the network administrator to achieve the desired functions and results, can use additional capabilities and services. It also serves to minimize the operation costs and offer maximum returns all with a view of increasing productivity. The range of the additional services offered by the Cisco IOS are the encryption of data, authentication of users, firewall configuration to enable select traffic and deny unwanted and unsolicited ones, deep packet inspection which might be used by researchers to further study and analyse the contents of the different packets and even the abilities to offer the tuning of different network services; Quality of Service [4;5].

The Cisco IOS comes under different variations, firstly, is the IOS XE which functions on the Cisco ISRs which are basically enterprise-grade, then, secondly, the IOS XR which

is run only on the service provider's equipment for example CRS routers and lastly, the Nexus OS which runs on data centres switches which are of the Cisco Nexus family. [4]

2.3 Juniper's JunOS

Just like the Cisco IOS, Juniper's JunOS aims to address the deployment time of the new services and acts to ensure that the cash outlay for the network operation are maintained at a reasonably fair value. The definition of JunOS according to the Juniper Networks, is that, "JunOS is a reliable, high-performance network operating system for routing, switching and security". [6]

JunOS in addition to its core functions will also make the automation of the operations that are related to the network possible. If some services are automated, this leaves enough time for the deployment of up-to-date services and applications. The advantage that JunOS has over the Cisco IOS is that, it is possible to program and control the JunOS, a concept that is known as the Software Defined Networks (SDNs). This SDN is very important in huge networks that are operated by the service provider as it makes the automation of complex services possible, and it orchestrates frameworks. When the software achieves these complex functions, the service provider is left with clearly cut-out business functions and the power to be innovative and create new services. [6]

2.4 Differences Between Cisco's IOS and Juniper's JunOS

Cisco's IOS and Juniper's JunOS are very different and each has different capabilities. One has a competitive edge over the other, but all these depend on the different needs of separate businesses and customers. According to the writers claim, Cisco and Juniper tend to disagree with the OS the competitor uses. Cisco claims that contrary to Juniper's claim of a sole JunOS; Juniper in essence has more than one version of their OS. Juniper on the other hand claims that Cisco has way too many versions of their OS [2].

There has been debate; fervent as some might choose to call it that has pitted Cisco and its close competitors HP and Juniper about the pros and cons of both multi-vendor and single-vendor networks. Cisco commissioned the top consulting company, Deloitte to conduct a report to show the benefits of single-vendor networks. Depending on what side you are talking to, each will tend to have a different answer to the question, "Which between a single-vendor and a multi-vendor network is the best?" [2,3] The advantages

or the reasons why an organization might choose to implement a multi-vendor network depend on a number of reasons. One of the main reasons is that, when using multi-vendor equipment, one can shop and choose equipment with the lowest value/price. This will then ensure that the total ownership cost/operational cost are kept as low as possible. This is difficult to achieve in a single-vendor network since the business/people contracted to develop the networks have no choice, and will be forced to buy the equipment from the manufacturer no matter how high the prices will be. [2]

The Gartner report claimed that organization that had multivendor networks had less complexity when they were compared to those organizations that used all Cisco equipment. The Deloitte report says otherwise and disagrees with this claim. [2,3]. Thirdly, there are several risk that are associated with a single-vendor network and this are mitigated by the use of a multi-vendor network. An error in an all-Cisco-run business that occurs in one data centre will affect all the other data centres and this might cause the business to run into huge losses. On the other hand, when the data centres are each from a different vendor, then they can be implemented in a way that enables others to continue working even if a few are shutdown/attacked or even having errors. [2,3]

The sole decision of whether to move to a multi-mode network depends on a variety of findings and impacts that will be encountered by that change to the organization. Important questions need to be asked, whether the choice to have a multi-vendor is really that important and worth it to a business organization, how much costs will this actually add to the initial budget assuming that a primary single-vendor network was already running, how long will the networking equipment that will be bought last among many others factors. [3]

The major differences between the IOS and JunOS are the span from their heritages, the different versions they have on the market and lastly, their architectures. The first major difference is that IOS runs as single operation and all the processes use the memory. The disadvantage that this faces, is that if there is a bug in one operation, then this will cause all the other processes to be corrupted. For the JunOS, the principle behind its operation was the modular OS, which means that on the kernel, the processes actually run on top of the kernel and they are separated into different protected memories. This thereby, allows for a bug to only affect a single process and not all the processes running in the kernel. [3]

The next big thing between the two is the Command Line Interface (CLI) principle of Cisco and Juniper. There are different modes involved with both when the need to configure and even troubleshoot. Cisco has the User, Global and Privileged and one subcommand mode. Juniper on the other hand, which has JunOS CLI, which will be the software used in connecting to a device that is enabled with and running the JunOS. JunOS CLI is a network tailored for Juniper and runs above the FreeBSD, which is UNIX-like. The JunOS CLI provides sets of commands that are used in monitoring and configuring all the devices that run JunOS. [3]

Juniper's JunOS uses a UNIX shell. The UNIX shell can be simply started by entering the **`exit`** command followed by **`start shell`** command in the privilege level of the router. The command to start the shell was released before JunOS Release 7.4 and works in Releases 9.0 and 11.1 for EX and QFX series respectively. The issuance of the **`start shell`** command demands the user have all the necessary login privileges. A few of the options that can be completed using the command are **`start shell csh`** which serves to create a C UNIX shell and **`start shell sh`** meant for the creation of a Bourne UNIX shell among other many commands. To denote that the user is in the shell level, then the terminal will look as follows.

```
root_username@hostname%
```

There is no rocket science involved with the CLI interface. Just like the Cisco's CLI, when a command is simply entered on a single line and upon hitting the enter tab the commands are then executed. Unlike Cisco IOS, which has three modes and a sub mode, Juniper's JunOS has two modes and below each there are many hierarchies. The two are the operational and the configuration modes. The following modes will be discussed albeit longer and important differences between the two CLIs will be shown.

In Cisco the commands that are provided by the User Exec enables the connection to devices remotely, temporary terminal changes, basic tests performance and even the listing of information relating to the system. The commands that are at the EXEC user level are just a fraction of those at the privilege. When Cisco devices are connected via Telnet or even Secure Shell (SSH) then the first interface that appears in which commands can be entered is the User EXEC mode, and it allows the users to look and find most things but they cannot enter or make any changes of and to the configuration respectively.

The Privilege EXEC mode is the second, and this is the most powerful of the exec mode since most things can be done when the user is at this level. The commands in this level are those which were in the User EXEC and other configuration commands that enable further visibility of additional configuration options. Other capabilities of this are debugging. Through this level and by entering different commands, the router or switch can either be reloaded or even rebooted. Under this level the most important command or that which is popular is the enable secret password, which will set any password the user chooses. Further security is enabled in this level as users who access the router by SSH or even Telnet are not allowed in if the password is not set. Listing 1 below shows the commands that are under the privilege EXEC mode in Cisco routers.

```
PE-R7#enable
PE-R7#?
Exec commands:
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  access-template  Create a temporary Access-List entry
  alps             ALPS exec commands
  archive          manage archive files
  audio-prompt     load ivr prompt
  auto             Exec level Automation
  bfe              For manual emergency modes setting
  calendar         Manage the hardware calendar
  call             Voice call
  cd               Change current directory
  clear            Reset functions
  clock            Manage the system clock
  cns              CNS agents
  configure        Enter configuration mode
  connect          Open a terminal connection
  copy             Copy from one file to another
  crypto           Encryption related commands.
  ct-isdn          Run an ISDN component test command
  debug            Debugging functions (see also 'undebug')
  delete           Delete a file
```

Listing 1. Cisco Privilege EXEC mode commands.

The other is the Global configuration mode, which entails those features that can affect or impact the whole system. The user mode shows the users the display information after they enter simple commands. The Privilege mode has the capability to support a lot more commands. These commands as compared to the User mode commands that have no harm, can cause huge damage to the system. Not any of the commands in the

privileged or the user mode changes the configuration of the device. The configuration modes tell the commands that are to be accepted which in turn commands or directs the device what they should do with the received commands, and how to do what it receives with the commands. Those commands that are entered in the configuration mode make necessary changes to the running configuration when enter button is pressed. Listing 2 shows a sample of the command under this level as shown below.

```
PE-R7#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
PE-R7(config)#?
Configure commands:
  aal2-profile       Configure AAL2 profile
  access-list        Add an access list entry
  alias              Create command alias
  alps               Configure Airline Protocol Support
  appletalk          Appletalk global configuration commands
  application        Define application
  arap               Appletalk Remote Access Protocol
  archive            Archive the configuration
  arp                Set a static ARP entry
  async-bootp        Modify system bootp parameters
  atm                Enable ATM SLM Statistics
  banner             Define a login banner
  bba-group          Configure BBA Group
  boot               Modify system boot parameters
  bridge             Bridge Group.
  call               Configure Call parameters
```

Listing 2. Cisco's Global Configuration Mode.

Lastly, is the subcommand, which is the Context. The settings under this level, tells the device firstly, the topic and what to do under that specific topic. An example of the topic is the interface, under which we might enter commands to configure, modify or delete either to a specific interface or to a range of interfaces. By simply entering a question mark after the topic, the router or switch will show the different actions that can be performed under that topic. An example would be to just type interface and then put a question mark, and this will show the different interface types whether fast Ethernet or serial and in what numbers they are available to be configured. These are the important details that involve the Cisco IOS CLI and it is quite simple to use as compared to the Juniper's JunOS, which is quite complicated to say the least.

As for the Juniper's JunOS, on the other hand, firstly, is the operational mode which only shows the device status and the commands that can be entered are those used in the monitoring and troubleshooting of the JunOS, the connectivity to the network and other devices connected to it. The other is the configuration mode, which is for the device that runs the JunOS, and the commands are stored in a hierarchical form. The commands that are entered in the configuration mode define all the JunOS properties that encompasses the different interfaces, routing information in general, the different routing protocols, and even the properties of the hardware just to mention a few.

The big indicator to assist in identifying what mode the router is in is by looking at the CLI. When the CLI ends in > in front of the base prompt of the router, then that shows the operational mode and not so many actions or operations can be done under this mode. The commands under this mode are used for the verification and troubleshooting. When in the configuration mode, the # appears in front of the base prompt. In this mode so many configuration processes and the different hierarchical levels can be seen.

```
root@PE-R2> ?
Possible completions:
  clear            Clear information in the system
  configure        Manipulate software configuration information
  file             Perform file operations
  help             Provide help information
  monitor          Show real-time debugging information
  mtrace           Trace multicast path from source to receiver
  op               Invoke an operation script
  ping             Ping remote target
  quit             Exit the management session
  request          Make system-level requests
  restart          Restart software process
  show             Show system information
  ssh              Start secure shell on another host
  start            Start shell
  telnet           Telnet to another host
  test             Perform diagnostic debugging
  traceroute       Trace route to remote host
```

Listing 3. JunOS Operational Mode possible commands.

When a command is entered under this level, what is actually happening is that, the candidate configuration is being viewed and changed. This file enables the operational changes to remain the same even when configuration changes are made. These changes that are made to the candidate file will not be implemented until a commit statement or command is entered. This concept differs from the Cisco IOS, that has

every command after being typed in a line, then by merely hitting the enter tab/button, the commands are immediately executed and implemented. The advantage of the candidate configuration over Cisco's every-line-hit-enter-to-execute is that changes can be made to the JunOS, without the potential of damaging ones whole current networking operations. This tends to be not possible in the Cisco IOS, as if an interface or protocol information is altered or even deleted, then all the features that were configured with the same information will be disabled.

In the operational mode, there are two commands that neither designated for monitoring the router nor the network. These are the quit which is used when logging out from the router and the CLI. Second is the configure which is used to enter the configuration mode so that the router can be configured. The command and statements are the two basic components found at the configuration mode. In the creation or the modification of the configuration in the router, the commands available in the configuration mode are used in statement additions to the particular configuration that's defines the behaviour of that particular router. Typing a question mark (?) in this mode at the topmost level that is the [edit], offers/displays a broad view of the different commands used in the router configuration. On the contrary, during the creation or the eventual modification of a router's configuration, edit and the set commands are used in controlling which configuration statements are to be included. The edit is used to move to that particular portion of the configuration that one wants to modify. The set command on the other hand is used in a specific-item configuration. The up command will move the hierarchical one level up while, the top returns to the [edit] hierarchy. Figure 3 below shows the JunOS operational mode and the command under it as follows.

```
root@PE-R2> configure
Entering configuration mode

[edit]
root@PE-R2# ?
Possible completions:
  <[Enter]>            Execute this command
  activate             Remove the inactive tag from a statement
  annotate             Annotate the statement with a comment
  commit               Commit current set of changes
  copy                 Copy a statement
  deactivate           Add the inactive tag to a statement
  delete               Delete a data element
  edit                 Edit a sub-element
  exit                 Exit from this level
  extension            Extension operations
```

```
help                    Provide help information
insert                  Insert a new ordered data element
load                    Load configuration from ASCII file
prompt                  Prompt for an input
protect                 Protect the statement
quit                    Quit from this level
rename                  Rename a statement
replace                 Replace character string in configuration
run                     Run an operational-mode command
save                    Save configuration to ASCII file
set                     Set a parameter
```

Listing 4. JunOS Operational Mode.

The JunOS CLI is arranged in a hierarchy. This means that those commands that are involved with the performance of similar tasks are put together under the same hierarchy level. An example is all the command displaying system information and information about system software are put together under the command show system command, and all those commands relating to display information regarding the routing table will all be put under the command show route command. For command execution, the full name of the command is entered, from the top hierarchy. This is different from Cisco IOS, which has no specific or particular hierarchy apart from getting to the enable mode from which commands can be entered [7;8, 2-12].

That sub-chapter served to explain the major differences between the Cisco IOS and the Juniper JunOS, from the CLI, software-wise, architecture-wise and the other important bits that makes both of them unique and stand out.

2.5 Proprietary and Multivendor Standards and Benefits

For the interoperability to be attained between the Cisco and the Juniper routers, different standards that are either proprietary or multivendor have to be taken into consideration. These standards are adhered to by the manufacturers of the networking equipment. A standard is basically a given guideline setup of specifications that enable the interoperability and has to be agreed, adopted and approved either by a particular large group or universally. Open standards are those standards which are made available publicly and whose implementation is open to anyone. What are encompassed in standards are many ideas from different areas, concepts that enable compatibility, interoperability and agreements. [9]

The different networking equipment from different vendors must adhere to set regulation and standards. There are standards that are vendor specific to ensure that the equipment is different from the others in the marketplace and these are called proprietary standards. Some of the standards have to be universal to enable separate vendor equipment's to be able to get configured and work seamlessly with equipment from other vendors. These are some of the reasons for a particular choice or preference when faced with a hard choice about vendor networking equipment.

Networks and the different networks standards have evolved over the last few decades. A world without the possibility of either the Ethernet or even the internet seem unliveable today. It is not so far that the different tasks in the workplace such as destination computer, communication paths among other things were defined by the network and not the user. Fast forward today, when most of these same services can be controlled by the user and not the network. To achieve these, standards which aim to ensure flexibility and even the establishment of baseline functionality that have to be always maintained. Standards are everywhere and a lot of work is put in the different committees and the engineering laboratories and eventually to the testing facilities. All these play a part to achieve a plug and play status. Even though, most people taking and plugging an Ethernet wire into the Ethernet outlet and getting immediate access to the internet take it all for granted, standards development tend to consists of a lot of research.

The benefits, rewards of adoption and adherence to standards for the network operators and the different connected users are as follows: -

- Integration and Testing – by using standards, the networking pilot phase is greatly shortened and simplified.
- Deployment – adherence to already implemented standards ensure that installations and even upgrades are ready and available in time.
- Operations – adherence and adoption of standards ensure streamline in the operations that might be related to either the continuing administration and maintenance.
- Availability – standards support and strengthen both the dependability of exchanges plus connections.
- Security – they (standards) ensure that the integrity of different devices besides applications relating to connection and even connected resources or devices are secure.

- Accessibility – the ease of reaching a network and using it is greatly extended by standards
- Open Systems – business and technical flexibility is greatly heightened when standards are implemented and used.
- Cost Saving – Operation expenses and capital are lowered when standards are implemented and adhered to.
- Choice – ability of vendors to be independent and ensure a variety of product availability is achieved when standards are used as they promote such.

Both the service providers and the different technology vendors enjoy returns with the adoption of standards. This further helps to make the development of different products easy and testing that adheres and conforms to such, makes efforts for support requirements quite easy and not so complicated as there is a standard upon which these are to be gauged. Standards entails technological advances that are known and widely accepted and those that are implemented by many and different service providers and vendors.

In today's world, technological advancements and innovations happen so quickly and the different network operators have to be in tune and respond adequately to these changes which might be in the form of either new IT innovations or varied and improved demand by businesses. Furthering of better standards helps the different networks operated by separate entities to provide full potential and in return boost the performance, security, service intelligence among other things. Vendor extensions serves in promoting technological innovations. The purpose of vendors in such situations is to ensure and prove that the new innovations can be both robust and ensure possible delivery of real returns before their introduction to the standardisation process and eventual acceptance by both the vendors and customers.

The main objective that sets out to be attained by the network operators and the different vendors of technology is creation and operation of networks that use formal standards to the best potential, and at the same time exploiting the full potential of defacto vendor extensions and standards. Extensions are value-added services because of the solutions that they do offer. Vendor do not use one specific standard and extensions but rather mix these with the solutions that they offer. Technological extensions serve as a base on top of which formal standards are implemented.

The two types of standards that will be discussed in this part are the vendor specific standards and then the multivendor specific standards. Each will try to explain the standards in Cisco and Juniper. Cisco has some standards that it has defined, developed and enhanced over the past couple of years and across the many different critical areas in networking. These are discussed as follows: -

- Standard for Network Connectivity: IEEE 802.3u Fast Ethernet – Marked its first introduction back in 1995 and it ensured the increase in the speeds of the Local Area Network (LAN) Ethernet to 100 from 10 Mbps. To further increase speeds to different business needs, Cisco has developed Gigabit Ethernet, 10 Gigabit Ethernet and eventually 40/100 Gigabit Ethernet. This serves to ensure the continual maintenance of the status quo of the Fast Ethernet as a primary mode of connection for the many networked and networking devices.
- Interior IP Routing: Open Shortest Path First (OSPF) and Routing Information Protocol Version 2 (RIPv2) – Are used in single Autonomous Systems (ASs) and are called dynamic routing protocols. Used in quite big enterprise networks.
- Exterior IP Routing: IETF Border Gateway Protocol (BGP) – Serves to maintain the IP networks table and makes the routing decisions as where the packets should be forwarded, deals with policies of the network among others. It is a core routing protocol.
- LAN Switching: IEEE 802.3ad EtherChannel – it's a technology of link aggregation that was developed in the early 1990s that involves grouping various many Ethernet physical links to come up with a single logical Ethernet link. The main function of this is for fault tolerance in situations where some links have problems, then the remaining good once can ensure connectivity. It also provides high speed connections since the different speeds of each link are aggregated together to become one. The standard on which they are based is the 802.3ad.
- Internet Protocol (IP) Traffic Direction: IETF Multiprotocol Label Switching (MPLS) – MPLS is highly very scalable an independent Data Link Layer that is concerned with the the direction and carriage of data from a given network node to the next. The work on the standard started in 1996 and the first deployment that was massive was in 2001. Label switching is what drives MPLS final standard.
- Management of Traffic: IETF IP Multicast – A technology of bandwidth-conservation designed with the aim of traffic reduction as it advertises a single traffic stream to thousands of customers or homes. Cisco routers in the beginning were developed to support Protocol Independent Multicast (PIM) that would in

turn result in the formation of an efficient distribution tree that were to be sued in to transmit multicast content. The IETF adopted the technology to become one of its standards. It is not only for Cisco anymore but available for other vendors like Juniper and it is widely used in large business organizations/enterprises and by service providers.

These are just but to name a few, some of the additional standards are Network Availability: IETF Virtual Router Redundancy Protocol, Wireless LAN: IEEE Control and Provisioning of Wireless Access Points, Wireless WAN: IEEE 802.16WiMAX, Data Center Networking: American National Standards Institute T.11 Virtual Storage Area Networks, Network Security: IEEE 802.1Q Virtual LANs, Network Power: IEEE 802.3af Power over Ethernet just to name a few [10].

On the Juniper part, the more generic multivendor open standards that are important to the Network Access Control (NAC) and that have to be adhered to for the enterprise equipment to communicate with those from a different vendors and even maintain security when connected with other vendor's equipment are Trusted Network Connect (TNC) and the Unified Access Control. The NAC is the ability in controlling the network access and it is based on compliance with different network policies. It ensures the appropriate connection to the necessary and appropriate network by the user and device. Because of its capability breath, NAC solutions cut across a large number of entities in the enterprise network.

The open multivendor standards that are applicable to both Cisco and Juniper are OPSF, RIP, BGP among others. As for the open proprietary, for a long time EIGRP was a Cisco proprietary standard and could be implemented and offered by Juniper. EIGRP is now an open standard and Juniper has started implementing it in some on its routers.

The next chapter focuses of the MPLS L3VPNs that involves the different components that make the L3VPN, MPLS and the advantages that it offers in comparison to ancient technologies, the positioning of the MPLS L3VPN and how the MPLS L3VPN works.

3 MPLS L3VPNs

MPLS allows a vast majority of additional services to be provided and operated over it. One of this is the L3VPN which will be discussed in this chapter. There are many ways through which a L3VPN may be implemented, but for this paper, MPLS will be used. The chapter serves to describe and discuss the most important components that relates to the successful running of the MPLS L3VPN, the different technologies that help it work, the components that make it, and other important information such as where the L3VPN positioning should occur and be conducted/implemented and what factors affect how it is implemented and built all in the context of this paper.

Most of the details that may be smaller but albeit important will be left out, as this aims not to serve as step-by-step guide to the configuration and the working of the MPLS L3VPN.

For this part of the paper, a step-by-step style of describing the important details that relates to the L3VPN needs to be followed. The components are important altogether and the order in which they occur serves not to indicate which is more preferred or much important than the rest.

Important Request for Comments (RFC) standards that are related to the architecture of MPLS as well as those that discuss MPLS L3VPN will be discussed in detail as they form a foundation to the further understanding of how a MPLS L3VPN works. IETF developed MPLS which is a switching protocol with the main objective of incorporating the important benefits of the network switching equipment/devices into an IP network. MPLS works with different standard IP protocols such as OSPF and BGP among others. To support MPLS, these protocols have been extended. The first RFC documents to be established for MPLS were RFC 3031 and RFC 3032 that were released in the early 2000s (2001). These serve to provide a definition of the most-basic architectural framework of MPLS, provides a description of labels and how the labels are operated and passed in the MPLS traffic across the different label-switched paths (LSPs). [9,479]

3.1 MPLS L3VPN Positioning

Before a L3VPN is even configured, there are details that have to be considered in the initial designing and planning of the network. These details may either be from the people contracted by the service provider to build their networks or even experts who might have been paid to provide advice. Businesses expand and every now and then there is need for expansion of existing businesses, closure of old ones, opening up of new sites among other needs. For any and/or all of these, the service provider will at a given point be contracted to build either from the ground a new network, or expand a one that might already be existing so that it caters for the new needs of different businesses.

A properly defined network and that which was built with the future in mind is very important and needed when building networks. For this purpose and for this part of the project, the place where the L3VPN will be placed and who the business chooses to provide them with that service are of great importance. This is necessary since a properly built network serves to reduce costs over time or when the network need to be improved at some point.

MPLS technology was originally meant for the service providers because of the big sizes of their networks. MPLS is based on the separation of traffic inside the provider's core. With time however, enterprises, which are very large business organizations, started using it as well. The model that is usually used consists of the MPLS being inside the service provider's core and the customers or business organization in most cases or some do not have to configure MPLS at all. Then the service provider delivers/provides some connection for example, a switched Ethernet port to the premises where the customers reside. The customer in return routes all traffic generated from its premises to that port. The customers thus need to not know any information or detail to do with MPLS. The customer or business organization thus, needs to work closely with the service provider in order to ensure the smooth implementation of the different features that the customer might want for the business. However, all this depends on the structure and how the network is built.

The MPLS L3VPN positioning to a much extent seem to be largely dependent on the customer since the service providers core tend to be in most cases universal or standard and do not change that much. The customers on the other hand have much say as to what the positioning will entail depending on the different desires or functions and even additional services that they might want to be achieved.

IP packet operate over MPLS. The main reasoning behind MPLS entails assigning a label to a packet and the label is eventually used for switching the packet across a network. In L3VPN, rather than using the traditional IP addressing mechanism involving the router looking at the details of the destination IP address, the routers in L3VPN look at current and previously assigned/applied labels as a basis of forwarding packets. The contents of a packet as such seems not to matter in L3VPN. In the event that a packet has been labelled, the intervening routers simply forward it based on the signalling information.

In L2VPN however, the packet from a particular interface has label added to it and it is eventually forwarded. The packet might be an Ethernet frame or High-Level Data Link Control (HDLC) frame. The differences between the L3VPN and L2VPN regards the signalling mechanism and the network set-up overlay. L3VPNs (RFC2547bis) allows for the BGP protocol extension thus allowing the PE routers to signal the available routes within a given VPN. For the L2VPN on the other hand, there are many ways of constructing it for example using Point-to-Point (P2P) links as mechanisms of signalling.

3.2 Components of the MPLS L3VPN

There are quite many components that all come together to be known as a MPLS L3VPN. Before diving to define and describe the different components in detail, it is of utmost importance to first and foremost know what a VPN really is. Directly quoting from Cisco [12], which states that a VPN, “Is a set of sites that are allowed to communicate with each other privately over the Internet or other public or private networks”.

MPLS can either be a technology or protocol dealing with the data transmission from a particular network to the other. MPLS uses path levels and not the conventional long network addresses. “An MLPS L3VPN consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge routers attach to one or more provider edge routers”. [13,23-24] Layer 3 basically is the level at which the VPN will be implemented. This can be done as well in the layer 2.

The figure below copied from Cisco shows the components and the different terminologies that are involved with a basic MPLS VPN. The following subchapters aims to describe and provide an in-depth analysis of these components as follows: -

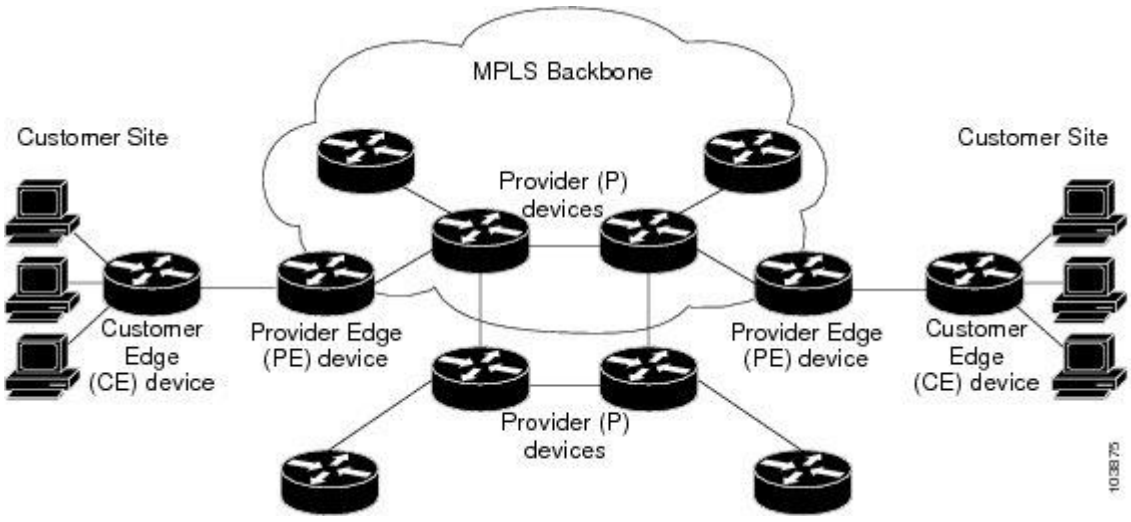


Figure 2. Components of L3VPN. Copied from Cisco [13].

As the figure above shows, the L3VPN consists of different components all of which work together to achieve end-to-end connectivity and exchange of routing information. The terminologies that will be shortly described follow RFCs as follows, for the MPLS architecture the RFC3031, and for the document that describes MPLS L3VPN the RFC4364.

The different components that make the L3VPN are discussed and presented as follows:
-

- CE router – This is a device that is at the customer site/side of the network. In the whole network, the CE router will be connected to the PE router, which is at the service provider edge. An interface is required between the CE and the PE router.
- PE router – It is the provider device that connects to the CE router. Its function is to attach labels to incoming packets from the CE device and remove the labels for outgoing packets to the CE device. The PE router has to be always updated whenever a new site has been added to the MPLS L3VPN.
- P router – These are routers found in the core or backbone of the service provider core. In the MPLS L3VNP, the P routers function is the participation in the control plane for the different customer prefixes. It is also known in some cases as Label

Switching Router (LSR). This name comes from the fact that it sometimes in its primary role in the service provider's backbone performs the switching of the labels or even the swapping of the traffic that is related to MPLS.

- C router – These are the customer devices that are connected/attached to the CE device. They provide the end users with the service that the business has contracted from the service provider for example enable users to access the VPN services.
- Multiprotocol- Border Gateway Protocol (MP-BGP) – This is an extended BGP protocol allowing for carriage of routing information that comes from different network layer protocols such as the VPNv4, IPv6 by BGP. It allows for the existence of a unicast topology for routing that is different from the multicast routing one, and this helps in controlling the resources and the network.
- Managed CE service – These are those services which are offered by the service providers alongside the MPLS L3VPN. The operations of the CE device, their management and even administration at one or more sites might be conducted by the service provider who may take advantage of this in offering additional services.
- VPNv4 – This is the when the Route Distinguisher (RD) and the IPv4 customer prefix is combined together. The IPv4 prefixes are extracted from the customer advertised routes that come from the CE routers and are combined with the RD that is configured on the PE devices. The resultant VPNv4 prefixes are then passed into the MP-BGP and transported to the other(adjacent) PE router.
- VRF – This is a short hand notation of Virtual Routing and Forwarding table. The VRF is quite separate from the table that exist on the PE routers that is used for the global routing. Routes that come to and from the routing protocols configured in the CE-PE devices are injected inside the VRF plus any other announcements from the MP-BGP that will match the VRF defined Route Targets (RT).
- Label – This refers to the frames that are MPLS based that travel from the PE routers, through the P core routers to the other PE routers.
- RD – RD is a 64-bit value that is uniquely defined for each and every group of users. It is combined with the IPv4 customer prefix information that comes from the routes advertised by a given CE router and in the end guarantees the uniqueness of the resultant VPNv4 prefix.
- RT – Route Target just like the RD is also a 64-bit value that is used as an extended community attribute for BGP. The function of the RT is to distinguish or determine what VPNv4 routes are supposed to be entered into the routing table.

These are the some of the components that make up the MPLS L3VPN [8, pg.1069-1072;11, pg. 4-6;13, pg. 4-5].

3.3 Architecture of MPLS L3VPN

Most customers prefer for their internal networks to be functioning as a single network. This is necessary and serves to ensure that the employees can be communicating and accessing different corporate services regardless of their geographical location. The service providers depending on the needs of different businesses can create and provide private networks that can join all the different customer sites into a big single network. The connection of these sites is achieved by use of P2P links. The model involves overlaying of the private network over the public internet. This type of model puts all the work relating to the design and operation of the backbones which are virtual and that are customer-related with the service provider.

This type of model has many scalability problems. There are too many virtual backbones which grow with each service that is contracted from new and even old customers. Scalability problems thus arise. This is because the service provider has to ensure the support for the proportionately larger virtual backbones and increasing customers. The addition or removal of different customers present a lot of work to the service provider as reconfiguration of nearly all existing sites, providing support to those existing sites, and maintenance of the private network all provide much work that becomes so complex over time.

This scalability problem necessitated the use of MP-BGP VPNs, that according to the RFC 2547bis is called L3VPNs mostly because of the BGP component. L3VPNs can ensure support of VPNs in their thousands and ensure that each VPN has hundreds of sites. Additional support is the overlapping of addresses. VPNs serves as connectors for geographical sites that are different and in separate locations. They offer the exactly same services that are offered by private networks. To ensure that the best architectural design of the network is followed, RFC standards provide the best tools for the people who design networks to work with [8, pg. 552].

The RFC3031 in short specifies the MPLS architecture. This states that that a packet travelling from one router to the next, which may be of connectionless network layer protocol, when it gets to the other router, then that router will conduct the forwarding decision of the packet which is independent. The routers have routing algorithm that is

based on the network layer that it uses in forwarding the packets. The packet header tends to contain too much information just for choosing the next hop. To divide the packets into smaller parts when doing the next hop forwarding the following two processes are conducted, firstly, the packets are divided into Forwarding Equivalent Classes (FECs). Secondly, the FECs are mapped into next hop sets. Then all packets that belong to a particular class of FECs will be allowed to travel to a particular path from a given node. IP forwarding in the conventional way follows the principle that router will consider two packets to belong in the same FEC when the address prefix contained in either of them has a prefix in the routing table of that particular router, so that the prefix seems to be the longest match for the destination of each of the packets.

RFC3031 in regards to MPLS states that assigning a given packet to a particular FEC is just done once. The FEC is then encoded into a label, and when the packet is then sent to the next hop, then the label is sent alongside the packet. This is the labelling of the packets before they are sent. As the packet moves to subsequent hops, the packet is not analysed anymore i.e. network layer header is not analysed. The label at this stage points to the table which tell more about the next hop, and since at each next hop there is a new label, it also displays/specifies the new label. The new label takes place of the old one and the packet is hence forwarded. In conclusion when a packet has been assigned to a particular FEC, there is no more analysis of the header by the routers that will receive the packet. The forwarding of the packets is label based.

In regards to the architecture of the MPLS, RFC3031 offers no specific definition of it but rather states the reasoning behind it being named multiprotocol since the techniques it offers can be applied to any network layer protocol. Label Switch Routers (LSR), are those routers with the capability to support MPLS [14, pg. 3-11].

RFC4364, which provides information about the L3VPN in the start, states how the service provider while using the IP backbone can provide VPNs to the customers. The method used by the service provider is the peer model. In the peer model, this consists of the customer edge (CE) routers sending all their routes to the service provider's edge (PE) routers. The service provider then uses Multiprotocol Border Gateway Protocol (MP-BGP) in exchanging the routes that belongs to a specific VPN to the different directly attached PE routers. This has to be done to ensure that routes that come from different VPNs stays separate and distinct even when the two have an addressing space that is

overlapping. The PE routers send routes that form a particular VPN to the CE routers. As for the CE routers, they are not allowed to pair with each other at all.

RFC4364 further goes on to state that for each given route that is within a given VPN, a MPLS [MPLS-ARCH, MPLS-BGP, MPLS-ENCAPS] label is assigned to it. Since BGP also distributes the VPN routes, it will distribute an MPLS label for that specific route too when distributing the VPN routes. When a data packet that comes from the CE travels across the service provider's backbone, it is first encapsulated with an MPLS label corresponding to the destinations packet best match. The next step is the further encapsulation of the MPLS packet either with an additional MPLS label, an IP or even Generic Routing Encapsulation (GRE) for it to be transported/tunnelled to the proper PE router while traversing the service provider's backbone. This serves to indicate that the core routers inside the backbone need to have no idea of the VPN routes.

The primary reason for having the backbone not know any VPN routes information is to ensure the support in cases where the client would like to obtain services that are related to the IP backbone from a service provider in situation where they maintain a contractual relationship between them. The advantages offered by this are that it offers simplicity in cases where the clients who might be groups of enterprises interested in contracting an extranet from the service provider, or even just another VPN from another service provider using the same methods in offering VPN services to its own clients, want the use of the services provided by the backbone, its scalability and flexibility is another benefit it affords the service provider and lastly, it allows value addition by the service provider.

A VPN according to the RFC4364 is a subset of all the sites that contain the same IP connectivity and are connected to the backbone. For two sites to have IP connectivity when they share a common backbone, then they have to contain some VPN common to both of them. If that does not hold then the two sites cannot be connected. So in further explaining the L3VPN, regarding VPNs, the above condition needs to hold for different sites to be able to communicate with each other. If all the sites making the VPN are owned by one enterprise, then the network is referred to as "intranet". If they are from different enterprises, they are called "extranet" as this means different parts might be owned and managed by different organizations/enterprises. In an extranet, the different sites can be in more than one VPN.

The customer's policies will always determine whether a collection of particular sites either form a VPN or not. Some customers will prefer that the service provider to implement all the policies while for others they might prefer the sharing of the responsibilities with the service provider. The policies that will be discussed further will help the service provider to either implement these policies themselves or together with the customers. The mechanisms that will be discussed further will enable a further implementation of different policies possible. The policies through a given VPN can involve creating links to each and every router inside the provider's core thus resulting into a full mesh topology.

About the connection of the PE and CE routers, RFC4364 states that the routers can be attached facing each other in many different ways such as Point-to-Point Protocol (PPP), frame relay among others. An attachment circuit refers to a way that the CE and the PE routes are connected and its only function is to enable connection of the two devices, which might be routers to connect over the network layer. Then each of the VPN sites needs to at least have one CE devices. The CE devices can be more than one and each of them had to be attached to the PE device by the means of an attachment circuit. The P routers, which are the routers inside the service provider's network, do not have to be connected to the CE devices.

The circuit that a packet takes from the CE to the PE device is called the ingress attachment circuit while that which a packet travels from the PE to the CE device is the egress attachment circuit. A given PE device will only be associated with a particular VPN if it attaches to a given CE device located at that sites VPN and the same applies to a PE device that must be attached to a given CE router/device. A CE device can either be a router or a switch. In instances where the CE device is a router, it becomes a routing peer to the attached PE device. It is however not a routing peer to other CE routers that may be located at other sites. The CE routes at different sites are not involved in the direct exchange of packets or communication with each other and each does not need to know that the other even exists. This makes a situation where there is no backbone for the customer to manage. The benefit of this is that the customer does not have to deal with routing that involves different sites. Regarding the management of the different edge devices, the service provider is not required to access the CE devices and the customer is not required to access or have knowledge of the PE and the P devices.

As for the service provider's backbone, this consists of the PE routers and the P routers. The PE routers only maintain the routing information about the VPNs. The P routers need to not know of any routing information related to the VPNs. This has the advantage of avoiding problems that are related to scalability of the network. Adding information of new VPNs thus needs to be only done for the PE routers only [15, pg.2-10].

3.4 MPLS L3VPN Operation

The operation of the MPLS L3VPN contains many steps that have to be configured in sequence. It also depends on the management control that either the service provider or the customer might be having over their equipment. In this paper, the assumption is that the service provider has all the management control and the customer thus does not need to configure anything for example the CE routers.

Before the configuration is undertaken, the service provider routers should be running and configured with Label Distribution Protocol (LDP) and Multi-Protocol Label Switching (MPLS). The first step will be the configuration of the backbone. The PE devices that are used inside the backbone too needs to LDP and MPLS. Edge routers are preferred over ordinary routers in the backbone, as the most basic routers do not support MPLS.

The choice of the signalling can be between LDP and Resource Reservation Protocol (RSVP). The main reason for the choice of LDP relates to it being the fastest start to MPLS that entails having the minimal configuration and the decisions to be made. When LDP is enabled inside the service provider core in all the core interfaces, this will automatically build the Label Switched Paths (LSPs) to all the egress from the ingress points.

RSVP offers more control as compared to LDP and comes with additional configuration statements. Manual configuration is required for all the LSPs on each of the ingress nodes. The number of the PE devices in the service provider core dictates the overhead in the network. When traffic engineering and fast restoration are set out to be achieved in the network, then it is a good idea/move to go with RSVP over LDP. LDP is thus suitable for simple networks.

Secondly, at the edge of an MPLS network which is the place where the MPLS VPN is always enabled at the PE, the processes that occur there are, firstly the PE and the CE devices exchange the routing information. The PE translates the routing information

(IPv4) that comes from the CE device into VPNv4 and lastly ensure that the VPNv4 routes are exchanged between the PE devices through the help of MP-BGP. Creation of the Virtual Routing and Forwarding (VRF) tables, distribution of the routing information and forwarding of the MPLS information all need to occur and be configured on each of the PE routers.

In different MPLS L3VPN architectures, depending on the customer's needs that may be to have different VPNS for different departments or for varied geographical locations, many instances of the VPN can be configured. In some instances, there can be a direct one-to-one association between a given VPN and a VRF or more. A VRF generally describes the ownership/membership to a given customer site that is attached to a given PE device. VRF is made up of an IP routing table, parameters for the given routing protocol and a given set of rules that are used in controlling the information in the routing table.

Sometimes there exists a one-to-one relationship between the created VPNs and the customer sites. This means that there a direct relation between the created VPN and the customer site that it should service. This depends on the service that the customers contract from the service provider or how many sites the customer has. The reason behind this one-to-one relationship may be traffic differentiation and categorisation. This however, is not the case as a given customer site can be associated with more than one VPN. This means that a single customer site can be connected with two or more VPNs. The reason for this is a situation where the categorization of the traffic is not necessary. An exception to the above however, is that a single customer site will always be associated with a single VRF. The content of a VRF that is associated with a single site is all the routers that are available from the VPNs that belong to the site.

The information relating to the packet forwarding is present in the CEF and the IP routing tables where they are stored for each and every instance of a VRF. It is worth noting that a separate set of CEF and IP routing information is maintained for each of the VRF. The function of this is twofold, one it to ensure that routing information is not routed/forwarded to the outside of a VPN or to prevent route information leakage and second to ensure that the device within a given VPN does not receive outside VPN packets.

After the creation of different VPN to a given site and a VRF, distribution of the information related to the VPN in the MPLS L3VPN is next. VPN Route Target (RT)

communities control the distribution of the VPN routing information and its implementation is through BGP with extended communities. The distribution of the routing information occurs in two phases, firstly, when a VPN route that is injected into BGP is learned from the CE device, then a VPN list target route of the extended community attributes will be associated with it. The list that it is associated with basically is set from a bigger export list of all the RTs that are associated with the VRF instance from which it was learned.

Secondly, each VRF is related to an import list of the RT extended communities. To expand on this, import lists in essence defines the attributes of the route target extended community that a route should possess so that it is imported to the VRF. The RTs help in the distribution of routing information related to the VPN through BGP extended communities. The routing information through the help of BGP is done when the PE device learns of a new VPN route from the CE, that route will be put/injected into BGP, and it will be associated with VPN RT community attributes. The PE router will learn the IP prefix of either a CE router, or a BGP neighborship session or through Customer IGP exchange with the CE router.

The IP prefix will be from the version 4 address family. The PE router will then convert that IP from IPv4 to VPNv4 through combination with the 8-byte long Route Distinguisher (RD). What is generated with is a VPNv4 prefix which is a member of VPN-IPv4. Its function is the unique identification of the customer address. The RD commands that will be entered in the PE routers will be associated with a given VRF. The function of BGP at this point will be the distribution of information related to reachability for the VPNv4 prefixes of the different VPNs. The Provider-IGP serves to move to VPN-IPv4 routes between the PE devices.

After the L3VPN routing information has been distributed in the MPLS L3VPN, the next step is for the MPLS information to be forwarded. The LDP automatically causes the generation and exchange of labels between the service provider routers. Each router automatically generates local labels for its different prefixes and eventually advertises the labels to its neighbors. This is based on Tag Distribution Protocol (TDP) which has now been replaced by LDP.

For the label distribution, first a User Datagram Protocol (UDP) Multicast hello packet are sent in order to discover neighbors. After the two routers have established a neighbor

adjacency, a Transmission Control Protocol (TCP) connection neighbor adjacency is built. The connection serves as a way to exchange label information. Loopback addresses are normally used for this neighbor adjacency. An example is shown by the following figure.

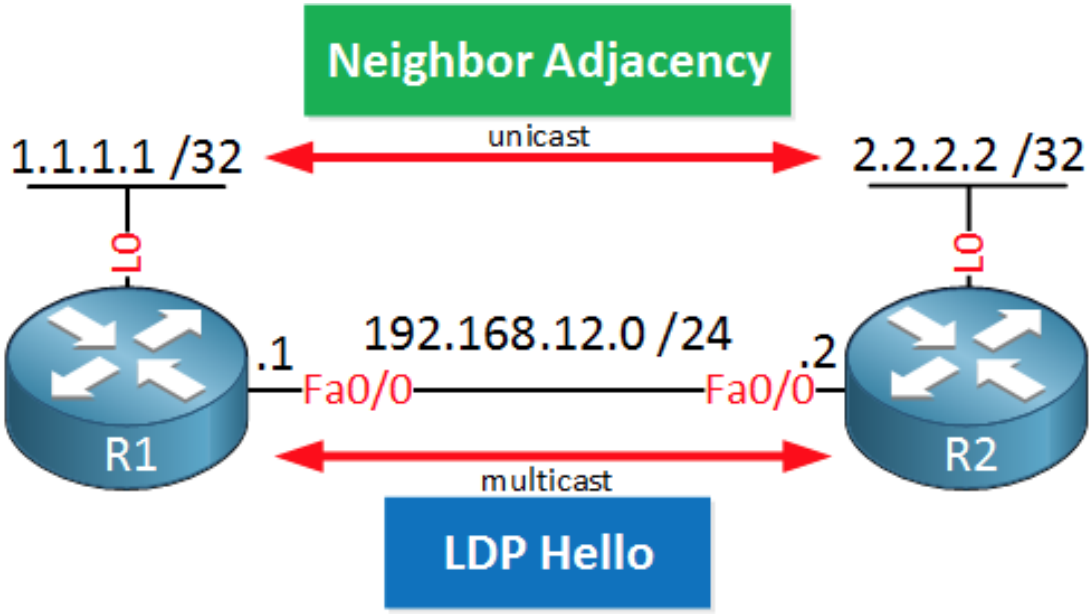


Figure 3. Neighbor Adjacency. Copied from Network Lessons. [18]

The two routers (R1 and R2) shown above sends multicast hello packets on the interfaces that is configured between them (FastEthernet). The hello packet serves to advertise a transport IP address that will be used in the establishing of a TCP connection between the routers R1 and R2. A sample of the hello packet as seen through a packet tracer is shown below.

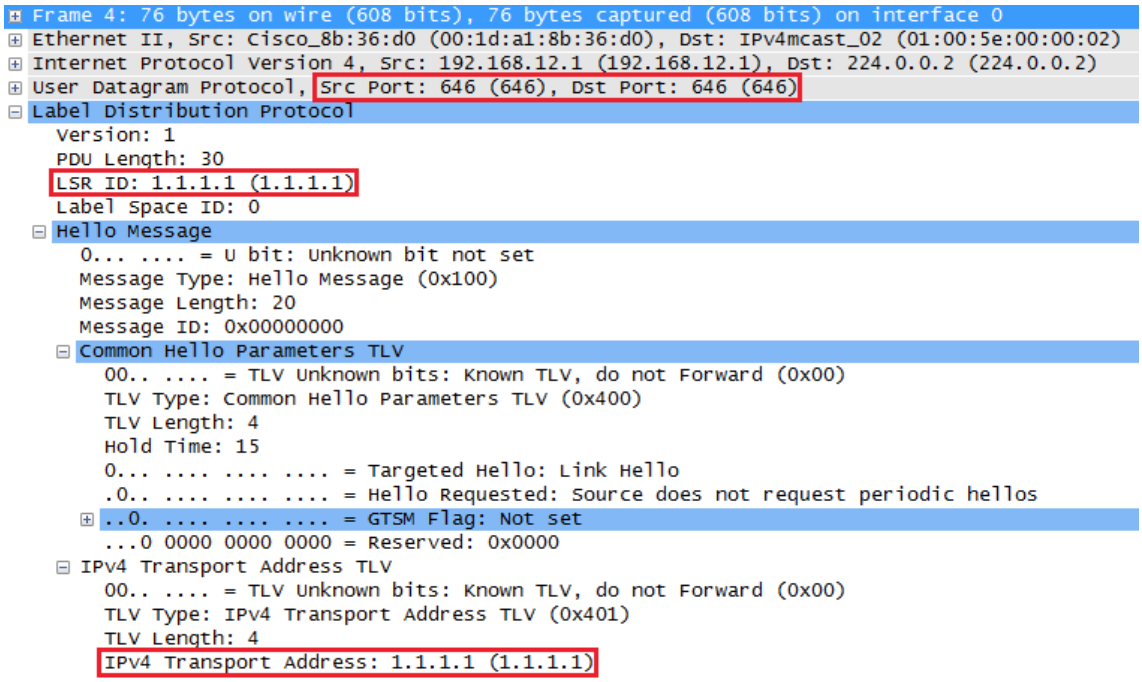


Figure 4. Hello Packet captured in Wireshark. Copied from Network Lessons. [18]

The capture shows the important details. Firstly, that the hello packets are sent to a 224.0.0.2 multicast address using a source and destination UDP port 646. Secondly, that each router possesses a unique ID known as LSR. The routing information is present and stored in the CEF and VRF IP routing tables will be used to forward packets to their destination using MPLS. The PE device after learning the customer prefix from the CE binds two MPLS labels to each prefix. The label is then included in the NLRI for that prefix. This prefix is then advertised to the other PE devices. Lastly, is the transport address that is found at the bottom and this is what will be used in the building of the actual TCP connection.

After the LPD routers have established a neighbor adjacency, the next step is the label exchange. With normal routing, EIGRP, BGP and OSPF are always used as the routing protocols as they learn prefixes from other routers. All this information is in turn stored in the Routing Information Base (RIB). The RIB acts as a routing table. The information that is in the RIB is further used in the build-up of Forwarding Information Base (FIB). The FIB is what will eventually be used in the forwarding of the IP packets. As for MPLS a different table is used. Figure 10 shown below serves to further understand the label distribution be presenting the different components.

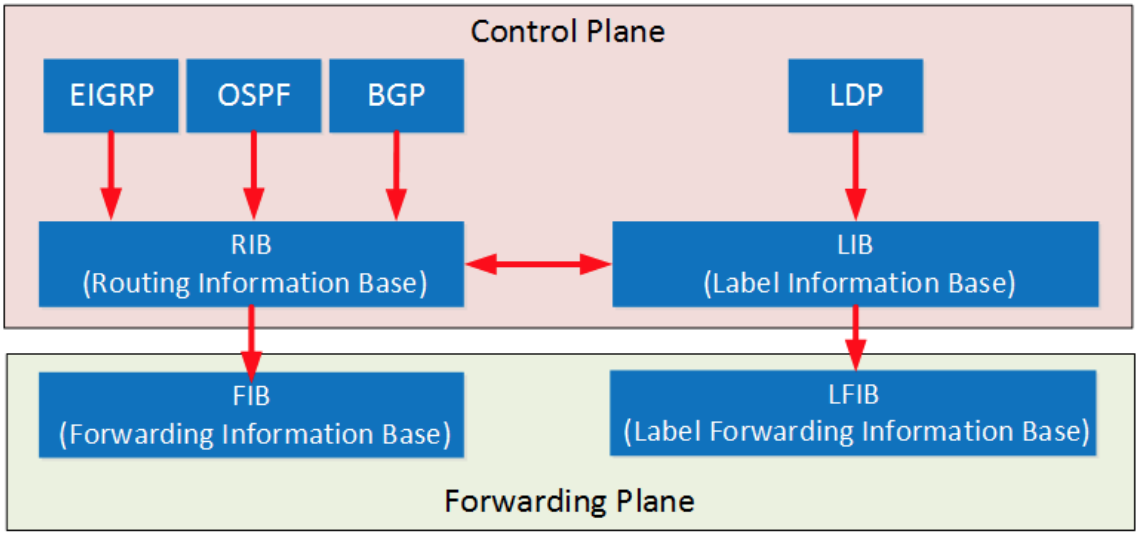


Figure 5. Control Plane. Copied from Network Lessons

LDP use generates labels which are found in the RIB. The RIB information is added to LIP. The information in LIB is further used to build the Label Forwarding Information Base (LFIB). So when a router forwards a packet that has an MPLS label on it, then the LFIB table will be used to forward that given packet across the service provider core to its destination.

In the event that a PE device forwarding a received packet from a CE device, the packet will be label learned from the destination PE device by the originating PE device. When the packet arrives at the destination PE device, the label will be popped and the PE device will use it in directing the packets to the correct VRF instance and then to the destination CE device. The forwarding described above is known as label forwarding. The basis of the label forwarding of packets is either through engineering of the traffic paths or the dynamic label switching [8, pg. 552-575;10, pg. 1069-1130;18].

3.5 Benefits and Limitations of MPLS L3VPN

Before the introduction of MPLS, routers made forwarding decisions of packets based on very complex route lookups. The root lookups were IP address defined. The problem with this was that it took too long for the lookup and this increased the time it took to forward packets. The goal of MPLS, with vanilla MPLS was to speed up the forwarding decisions of packets. This was made faster by the use of simple and not-so-complicated labels instead of the overcomplicated and use of long IP addresses as was before MPLS invention.

The use of simple labels over complicated IP lookups brought with it its benefits. Firstly, the MPLS L3VPN allows the deployment of VPNs that are scalable and this provides a platform for the further provision and delivering of additional value services, which for example are connectionless ones. This is one of the technical advantages that the MPLS L3VPN offers. TCP/IP seems to be credited with the success of the Internet today since it is packet-based built and a network paradigm that is connectionless. What this means is that prior action seems to be not necessary in establishing communication between different hosts. This makes the communication process between the different parties very easy. In order to provide privacy in the connectionless IP environment that is provided by the MPLS VPN network, then a connection oriented and a point-to-point network overlay is offered by the VPN solutions.

Secondly, there is the centralization of services since when building L3VPNs, this allows for the targeted delivery of specific services to a given user group that is represented by a particular VPN. The VPN to the service provider must be able to more than just being a mechanism used for the private connection of users to the intranet services. It must offer a platform on top of it that allows the further implementation of additional services possible. Scalability is important and critical, as the different customers each want to use services in their extranets and intranets privately. Since the MPLS L3VPN are viewed as intranets that are private, new IP services that can be used multicast, QoS, centralized services such as hosting of the web to a given VPN and support for telephony within a particular VPN. Several of these combinations can be customized for each individual customer for example to enable within a given intranet video conferencing, this is achieved by combining a low-latency IP multicast class with some other services.

Thirdly, is the scalability, which in cases where a VPN is created by the use of connection-oriented or even frame relays, the problems with these is that they aren't scalable. Not fully meshed connection-oriented VPNs that exist between different customer sites are not best/optimal. The advantage that is offered by the MPLS L3VPN is that it uses peer modelling and a connectionless architecture at the Layer 3 that enable the leveraging to a VPN network that is greatly scalable. The requirements of this peer model are that an individual customer site must peer with a single PE device and not all the CE devices that belong to the same VPN. Tunnels, which are a complicated way of doing things, are eliminated when the connectionless architecture that operates at Layer 3 is operated. Additional areas where the scalability question falls and applies are MPLS based VPNs involving VPN route partitions between a particular PE device and

partitioning further of the routes that are related to the VPN and those of an IGP between the core network routers. This requires the no VPN routes are to be maintained by the P routers and VPN routes that are members of a given VPN are to be maintained by the PE routers. This serves to ensure that no particular device in the core is a bottleneck to scalability. This ensures increased core scalability.

Fourthly, MPLS L3VPN creation is easy. The only requirement on the part of the customer for the full utilization of the VPN is for them to create new user communities and VPNs. The facts that MPLS based VPNs are connectionless means that specific P2P connection is not a requirement at all. Additional sites can either be added to the intranets or the extranets to form a user group that is closed. This manner of managing VPNs serves to provide the advantage of a given site membership in multiple VPNs thus maximising the flexibility when building/constructing both intranets and extranets.

Fifthly, the addressing is flexible as when a given VPN is being made, service provider customers are given the opportunity for designing their network addressing plan, that is not related to that used by the service provider other customer's. Following the recommendations of the RFC 1918, most of the customers prefer the use of private network addresses. This is because the prices/costs plus the time involved with Network Address Translation (NAT) hefty and time consuming and they do not want thus to do those. MPLS VPNs allows for the continued use of the customers private addressing scheme without the need for NAT by the provision of a private and public address view. The only situation that demands NAT use is when overlapping address space is used between two VPNs that need to communicate with one another. MPLS VPNs thus removes the NAT from the equation and thus enabling the customer's use of private addressing scheme in freely communicating with/across IP network that is public.

Sixthly, is the support for the Integrated QoS. QoS is one of the most important requirement that is needed by many customers who contract IP VPN. QoS fundamentally addresses VPN requirements that are twofold; one is the predictability of performance and implementation of policies and second is ensuring that support exists for MPLS VPN in many different levels. Classification of network traffic and labelling of the same done at the edge of the provider core before the overall traffic (aggregation based on the subscribed-defined policies and service provider-implemented ones) is transported across the provider core. Differentiation of the traffic either at the core network or edge

is possible into distinct and separate classes. This can be achieved by either delaying it or dropping it randomly based on probability.

Lastly, the MPLS VPN migration is straightforward. In order for the quick deployment of VPN services by the service provider, they just have to use a straightforward migration path. The advantage offered by MPLS L3VPNs is that they are unique as they can be built over many network architectures that include IP network or hybrid ones [10, pg. 1073-1074;11, pg. 6-7;13, pg. 7-9]

As for the limitations first and foremost, since MPLS L3 VPNs natively offers support solely for IP, this means that in cases where the customers need to support other protocols for example GRE or Internetwork Packet Exchange (IPX) then tunnels will have to be configured between the different CE routers. Its ability to support native IP thus, offers a disadvantage when other protocols are to be implemented. Some of the service providers offer no native IP multicast support for traffic between the different sites in the MPLS L3VPN. This means that all the traffic that is multicast has to be tunnelled between the different customers' sites by ensuring GRE configuration at each of the CE routers.

Secondly, in any given MPLS L3VPN, the Wide Area Network (WAN) routing is outside the control of the customer. The given PE routers at the service providers' core have to establish peer connectivity with the CE devices as direct routing adjacencies is not a possibility. Thirdly, the service provider core does not offer support for IPv6 in MPLS VPN. This means that the service provider core is still stuck with running IPv4 making it not possible for IPv4 customer routes to be advertised to the adjacent PE devices. Lastly, although MPLS L3VPNs are VPNs that are trusted, and offer segregation and division of traffic and even similar security as those offered by Asynchronous Transfer Mode (ATM) or Frame Relay, they do not by default/not natively offer authentication mechanism and encryption good enough in today's world full of attacks to networking equipment and software. Those offered by IPsec are considered much better [11, pg. 6-7].

Although the benefits of MPLS L3VPN seems to outweigh its limitations, no one given technology or innovation is an end in itself. All technologies are a means to an end and not an end to themselves. To ensure great satisfaction in any of the functions that each should achieve, different technologies or processes are mingled together to come up with a best alternative. MPLS L3VPN is thus just a backbone, with many other services

and processes that can be run with it to achieve different organizational needs that are in taste with the different objectives set out to be achieved by varied customers.

The next chapter discusses the practical part of the project and entails the topology of the project, the configuration of the MPLS L3VPN in both the Cisco's IOS and Juniper's JunOS.

4 Interoperability of Cisco and Juniper Routers

This is the part of the project where the interoperability of Cisco and Juniper routers is implemented. The purpose of this stage is to make the routers that are from different vendors to work seamlessly. The design of the network will be discussed, the IP networking choice will be discussed, implementation on how the routers were made to work together described and the configurations entered in the PE routers shown. The first component that will be discussed is the design topology of the project in the next subheading.

4.1 MPLS L3VPN Project Design Topology and Addressing Scheme

The figure shown below shows the topological choice of the project, the IP addressing scheme, the different protocols that are run at each site and the names that denote the different routers.

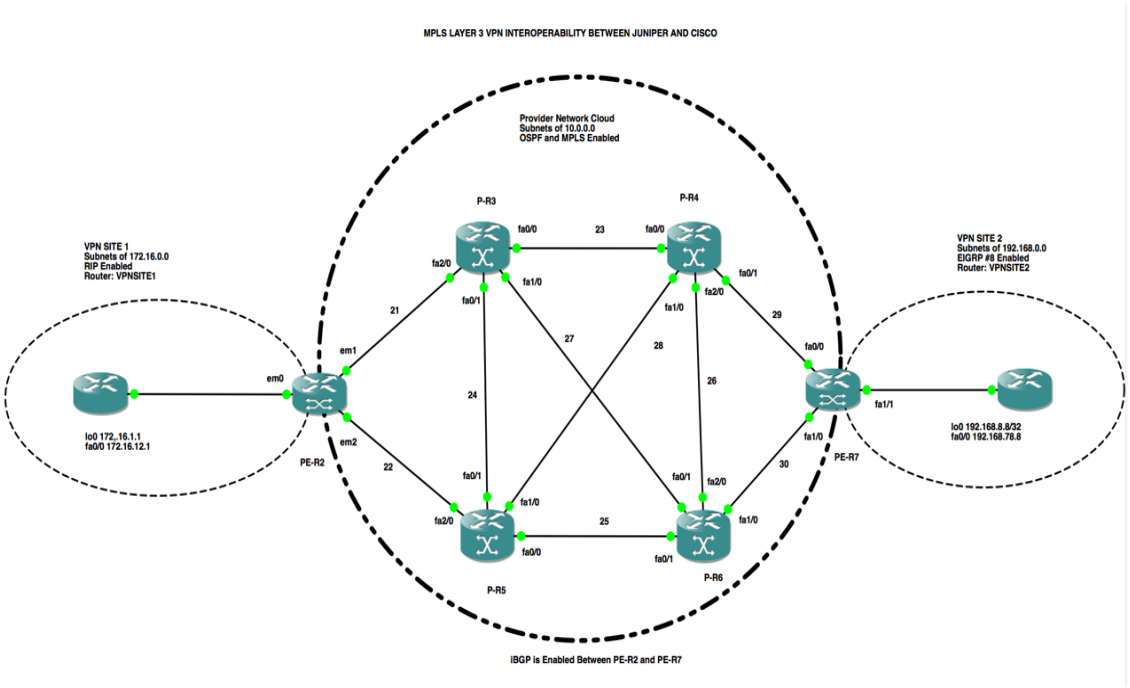


Figure 6. Project Topology.

The figure above shows the different components of the L3VPN. Shown by the same figure is the topology of the project. In as much as this is to an extent an overly smaller part of what might constitute a bigger part of the L3VPN architecture that is provided by the service provider, the same addressing scheme used in real business scenarios will be used here as well. There are two CE sites, which as is in real life scenarios, use private IP addresses of 172.16.0.0 and 192.168.0.0. As for the service provider core, a private IP address of 10.0.0.0/8 is used. So the reason for the choice of the above network is to try and simulate a real-life situation as close as possible.

Secondly, the CE routers are running the Cisco IOS and for the P routers in the service provider's core, these all run the Cisco IOS. The PE-R2 runs JunOS while the PE-R7 runs IOS. The different routers have numbers, which serve to differentiate them from each other. The IP address of each is going to have an ending that corresponds to the router number. This will serve to help while troubleshooting and make it easier to understand the origin of a particular route. The loopback addresses that will form the BGP neighborship in the provider core will have addresses of 2.2.2.2 and 7.7.7.7 for PE-R2 and PE-R7 respectively.

Thirdly, the routing protocols which serve to indicate the means through which the different routers will be communicating with each other are varied. The different CE sites will be using EIGRP and RIP. The aim of this is to make it a little bit challenging, plus in real life scenarios, not all the CE sites use the same routing protocols in the two or more sites. The PE routers use interior routing protocol OSPF and distance vector routing protocols RIPv2 and EIGRP as well as exterior gateway protocols BGP that is used in the exchange of routing information between routers in the same Autonomous Systems (AS). The reason for the choice is related to the protocols not being out-of-date or old. Plus, these protocols are widely used in the everyday activities that are related to the network configuration.

Fourthly, the topology as seen from the figure above is quite simple. But even with that simplicity, there are functions or precautionary measures that have to be fulfilled by the topology. These can be failure in links that may warrant back-up links and even use of loopback addresses in case the physical addresses fail to operate because of an error. The service provider core is fully meshed to provide different routes. Each of the PE routers in the above topology has two links, for fault tolerance and continuance of service provision to the CE devices in cases where a link may be lost or down. The same idea applies, as that is one of the reasons for the use of the loopback interfaces, so that in situations where there is a failure with the physical link, then reachability can still be sustained or tested.

Lastly, the project was about an MPLS L3VPN between Cisco and Juniper. The only way to ensure that this is achieved is by the proper placement of the different routers. The routers that are related mainly to the configuration of the MPLS L3VPN are the PE routers. So to achieve the goal of the project, one of the PE routers had to be running JunOS and the other IOS. If this is not so, then it will end in a situation where the PE routers either running JunOS or IOS, which in effect will not be satisfying the set goal and objectives of the project. So this was a major and important part to be fulfilled as it had direct relation to whether the set-out goals of the project would be attained.

4.2 Configuring IOS MPLS L3VPN

The first of the the MPLS will be the configuration of all the provider routers. There will comprise of the PE and the CE routers. From the customers site, the CE router configuration does not entail much detail. The CE router configuration to much extent is standard as same processes are followed. The only restriction that is to be adhered to is

that the routing protocol that will be used between the PE and the CE routers must be either RIPv2, EIGRP. In this case the VPNSITE1 will run RIPv2 and the VPNSITE2 will run EIGRP. The last detail is that the CE router needs not to be configured with any MPLS since MPLS information will only be communicated inside the providers' core.

The aim of the routing protocol configuration on the two CE routers is so that the routes can be advertised to the PE routers. PE routers serve to advertise customer routes to the adjacent and directly connected PE routers which in turn are transported or advertised or forwarded inside the providers' core to the other PE routers and finally to the destination CE device and vice-versa.

Secondly and the most important part of the configuration will be the PE router configuration. The PE-R2 runs IOS and the following are the configurations in a sequential manner that need to be conducted. The loopback interface that will be used for the BGP source update and the LDP router ID are configured. The IP address of the loopback addresses both have an IP mask of /32. The reason for the use of the /32 mask is to prevent errors. IGP used in the backbone of this project is OSPF thus, if the loopback is not configured to the /32 mask, then the PE router will then advertise a label binding for the specific loopback address configured with the mask configured.

The routes that are advertised in OSPF to the neighbor routes will also include a /32 mask as OSPF always advertise the /32 mask by default. This will result in a situation where the neighbouring routers create binding for labels corresponding to those advertised by the adjacent PE router. This then results in LSP failure. The way to correct this in this project was by configuring the loopback addressed on both CE routers with a /32 mask. The loopback address will act as a fall-back address and will be used to conduct test in instances where the physical interface fails to work.

The CEF has to be configured or enabled since in some routers it is not enabled by default. Failure to enable CEF will result in an error and the MPLS that will be configured or enabled later will not work. The CEF configuration is enabled by entering the **ip cef** command on the terminal in the configuration mode of IOS.

The next step is to configure the LDP protocol. The LDP protocol is used in the backbone as well. The default label distribution protocol used in the IOS routers is TDP. So to use LDP then it has to be manually configured by **mpls label protocol ldp** command.

Configuring the router ID serves to ensure the ease of troubleshooting as the LDP routers sources can be identified easily. The loopback addresses used in the PE routers will be similar to the router ID configured.

MPLS will then be configured in the core interfaces. This serves to connect the PE and the P routers. MPLS needs to be enabled globally and on individual interfaces. The next configuration that is to be conducted is to configure the backbone IGP. Any IGP can be used to establish IP reachability inside the core but the two most common ones are OPSF and IS-IS. OPSF will be used in this case. The example configuration used is shown below.

```
router ospf 1
log-adjacency-changes
passive-interface Loopback0
network 7.7.7.7 0.0.0.0 area 0
network 10.0.0.0 0.255.255.255 area 0
```

The **router ospf 1** command will enable OPSF process 1 on the PE-R2 router. All the interfaces in the backbone that fall in the network 10.0.0.0/8 are placed under OSPF area 0. The process 1 indicates the OSPF instance one and since all the core routers are in the same area that is why they are all put in the area0. The passive interface serves to prevent advertisement of OPSF packets on the interface loopback0. BGP source update should be advertised into OSPF. Failure to do advertise the source update will break the MPLS L3VPNs.

The next step is the global configuration of BGP on the IOS PE router. To advertise the customer VPN-IPV4 routes across the MPLS backbone and between the two PE routers, MP-BGP is used. MP-BGP is configured under two steps. First step is the global configuration of the neighbors and then the neighbors being activated for the MP-BGP exchange for the VPNv4 address family.

```
router bgp 27
no synchronization
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 27
neighbor 2.2.2.2 update-source Loopback0
no auto-summary
```

The first command will serve to enable on the PE router BGP and after that the no synchronization command disables IGP global synchronization. The **neighbor ip-address remote-as autonomous_system** command configures both the autonomous system and the IP address of the remote PE router. The **update-source** command ensures that the loopback address is configured as the update source of the BGP session. Lastly the **no auto-summary** serves to ensure that BGP redistributed routes are not summarized at the major boundary of the network. Though not entered in this configuration, to only allow MP-BGP which are the only routes required for VPN functionality and not the global BGP routes the command **no bgp default ipv4-unicast** can be entered.

Next is the MP-BGP neighbor activation. MP-BGP is the protocol that will be used to exchange VPN routes between the PE routers. It's under the VPVv4 address family that MP-BGP must be activated. The sample configuration below shows how.

```
router bgp 27
no synchronization
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 27
neighbor 2.2.2.2 update-source Loopback0
no auto-summary
address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community extended
exit-address-family
```

The command **address-family vpnv4** is used to get to the VPNV4 address family configuration mode. The **neighbor ip-address activate** is used for the MP-BGP route exchange activation. The **send-community extended** configuration is by default and functions in enabling the BGP extended communities exchange.

The VRF are then configured next as is shown by the sample configuration below.

```
ip vrf CUSTOMER1_VPN
rd 100:100
route-target export 200:200
route-target import 200:200
```

The first line in the sample configuration above serves to indicate the name by which the VRF will be called. The **rd 100:100** is for the route distinguisher configuration for the **CUSTOMER1_VPN** configured. The configuration of the route targets is important

because they are attached to the customer routes during the redistribution into MP-BGP. The **route-target import** specifies the routes that are imported into the vrf and the **route-target export** those that are exported from the vrf. The created vrf then needs to be associated with a particular interface which will be the interface that faces the customer's CE device that is directly connected to the edge PE.

Next is the configuration of the CE-PE routing protocols. The protocol used between the VPNSITE1 and PE-R2 is EIGRP. The sample configuration and a brief explanation of what is meant by it is provided below.

```
router eigrp 1
address-family ipv4 vrf CUSTOMER1_VPN
redistribute bgp 27 metric 1 1 1 1 1
network 0.0.0.0
no auto-summary
autonomous-system 8
exit-address-family
```

The first command enables EIGRP on the PE router. Then EIGRP configuration is done under the addressing scheme of IPv4. Under the address family, redistribution is specified that is either MP-BGP or BGP into EIRGP. Customer routes are advertised between the PE routers by the use of MP-BGP and eventually imported into the respective customer's VRFs. To redistribute the routes, the command redistribute bgp is used. The network command is used in specifying the networks that are enabled for EIGRP and in this case all the networks that are from the customer site VPNSITE1 are allowed as denoted by the 0.0.0.0 network. Finally, the autonomous system command that serves to denote the EIGRP autonomous system number that was configured under the address family by default.

The final step is the customer routes redistribution into MP-BGP. The sample configuration for this part is shown below.

```
router bgp 27
address-family ipv4 vrf CUSTOMER1_VPN
redistribute eigrp 8
no synchronization
exit-address-family
```

The first command after the **router bgp 27** is used to get into the IPv4 address family configuration mode. The **redistribute eigrp 8** is for redistributing the customer EIGRP routes into MP-BGP. What should be taken into consideration is the use of the same

autonomous system number as the one that was configured under the IPv4 address family. These are the configuration that needs to be configured on the PE-R2 and they are all put together in one piece for clarity and to show how things all fall together s shown below.

```
PE-R7#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
PE-R7(config)#ip cef
PE-R7(config)#mpls ip
PE-R7(config)#ip vrf CUSTOMER1_VPN
PE-R7(config-vrf)#rd 100:100
PE-R7(config-vrf)#route-target export 200:200
PE-R7(config-vrf)#route-target import 200:200
PE-R7(config-vrf)#exit
PE-R7(config)#interface Loopback0
PE-R7(config-if)#ip address 7.7.7.7 255.255.255.255
PE-R7(config-if)#interface FastEthernet0/0
PE-R7(config-if)#ip address 10.0.29.7 255.255.255.0
PE-R7(config-if)#duplex half
PE-R7(config-if)#mpls label protocol ldp
PE-R7(config-if)#mpls ip
PE-R7(config-if)#interface FastEthernet1/0
PE-R7(config-if)#ip address 10.0.30.7 255.255.255.0
PE-R7(config-if)#duplex half
PE-R7(config-if)#mpls label protocol ldp
PE-R7(config-if)#mpls ip
PE-R7(config-if)#interface FastEthernet2/0
PE-R7(config-if)#ip vrf forwarding CUSTOMER1_VPN
PE-R7(config-if)#ip address 192.168.78.7 255.255.255.0
PE-R7(config-if)# duplex half
PE-R7(config-if)#exit
PE-R7(config-router)#router eigrp 1
PE-R7(config-router)#address-family ipv4 vrf CUSTOMER1_VPN
PE-R7(config-router-af)#redistribute bgp 27 metric 1 1 1 1 1
PE-R7(config-router-af)#network 0.0.0.0
PE-R7(config-router-af)#no auto-summary
PE-R7(config-router-af)#autonomous-system 8
PE-R7(config-router-af)#exit-address-family
PE-R7(config-router)#exit
PE-R7(config)#router ospf 1
PE-R7(config-router)#log-adjacency-changes
PE-R7(config-router)#network 7.7.7.7 0.0.0.0 area 0
PE-R7(config-router)#network 10.0.0.0 0.255.255.255 area 0
PE-R7(config-router)#exit
PE-R7(config)#router bgp 27
PE-R7(config-router)#no synchronization
PE-R7(config-router)#bgp log-neighbor-changes
PE-R7(config-router)#neighbor 2.2.2.2 remote-as 27
PE-R7(config-router)#neighbor 2.2.2.2 update-source
Loopback0
PE-R7(config-router)#no auto-summary
PE-R7(config-router-af)#address-family vpnv4
```

```
PE-R7(config-router-af)#neighbor 2.2.2.2 activate
PE-R7(config-router-af)#neighbor 2.2.2.2 send-community
extended
PE-R7(config-router-af)#exit-address-family
PE-R7(config-router)#address-family ipv4 vrf CUSTOMER1_VPN
PE-R7(config-router-af)#redistribute eigrp 8
PE-R7(config-router-af)#no synchronization
PE-R7(config-router-af)#exit-address-family
PE-R7(config-router)#end
PE-R7#wr
```

Listing 5. PE-R2 IOS configuration.

4.3 Configuring JunOS MPLS L3VPN

As for the PE-R2 that runs JunOS, although the configurations are to a larger extent similar to those entered on the IOS router, the CLI interfaces differ. In JunOS, these are the description of what is done and later a configuration of the same printed from the terminal. The assumption at this configuration is that the basic IP configuration, MPLS, LDP and OSPF has all been done. Moving from this step forward, the simplest and first part, will be the router-id configuration and the autonomous-system number that are configured under the `[routing-options]` level.

```
[edit routing-options]
root@PE-R2# set router-id 2.2.2.2

[edit routing-options]
root@PE-R2# set autonomous-system 27

[edit routing-options]
root@PE-R2# commit
commit complete
```

Secondly, in JunOS by default the RIP import policy dictates the acceptance of all routes that are received and those that pass sanity checks. As for the export policy RIP routes are not advertised by JunOS. To have this routes advertised, an export policy has to be configured and applied to advertise both direct routes and RIP-learned ones. So this will be the next step. This means that RIP in JunOS by default on the PE-R2 will import routes from the VPNSITE1, and to export or send routes to the VPNSITE1, then that function will be accomplished by the export policy that will be created and applied on the interface that faces the VPNSITE1. The routing policy is created under the `[policy-options policy-statement RIPEXPORT]` according to the configuration.

```
[edit policy-options policy-statement RIPEXPORT]
```

```
root@PE-R2# set term 1 from protocol bgp

[edit policy-options policy-statement RIPEXPORT]
root@PE-R2# set term 1 then accept

[edit policy-options policy-statement RIPEXPORT]
root@PE-R2# set term 2 then reject

[edit policy-options policy-statement RIPEXPORT]
root@PE-R2# commit
commit complete

[edit policy-options policy-statement RIPEXPORT]
```

The third step is the VRF creation, RD and route-target which are all done under the `[routing-instances CUSTOMER1_VPN]`. The route distinguisher value in this router's configuration and the vrf-target value has to be the same as those that were configured in the PE-R7 as 100:100 and 200:200 respectively. Still under the `[routing-instances CUSTOMER1_VPN]` by further editing into protocols then rip to get `[routing-instances CUSTOMER1_VPN protocols rip]`, then the RIP details are configured under here and a new group under which the earlier created export policy will be applied is configured under the same.

```
[edit routing-instances CUSTOMER1_VPN]
root@PE-R2# set instance-type vrf

[edit routing-instances CUSTOMER1_VPN]
root@PE-R2# set interface em0.0

[edit routing-instances CUSTOMER1_VPN]
root@PE-R2# set vrf-import CUSTOMER1_VPN-import-policy

[edit routing-instances CUSTOMER1_VPN]
root@PE-R2# set vrf-export CUSTOMER1_VPN-export-policy

[edit routing-instances CUSTOMER1_VPN]
root@PE-R2# set vrf-target target:200:200

root@PE-R2# set vrf-table-label

[edit routing-instances CUSTOMER1_VPN]
root@PE-R2# edit protocols rip

[edit routing-instances CUSTOMER1_VPN protocols rip]

[edit routing-instances CUSTOMER1_VPN protocols rip]
root@PE-R2# set send multicast

[edit routing-instances CUSTOMER1_VPN protocols rip]
```

```
root@PE-R2# set receive version-2

 [edit routing-instances CUSTOMER1_VPN protocols rip]
root@PE-R2# set group RIPROUTES

[edit routing-instances CUSTOMER1_VPN protocols rip]
root@PE-R2# set group RIPROUTES export RIPEXPORT

[edit routing-instances CUSTOMER1_VPN protocols rip]
root@PE-R2# set group RIPROUTES neighbor em0.0
```

The forth step is the BGP configuration, that is configured under the `[routing-options protocol bgp]` level. The beginning will to enable IPv4 capability, then next will be creating a group `PE-R2-to-PE-R7`, under which the type of BGP to be configured, which in this case would be internal, the local-address, IPv4 and VPNv4 capability will be configured. The last parameters that will be configured under the group are the peer-as and the neighbor ID or IP address.

The last step will be the creation of an export (for RIP routes) and import (for BGP routes) policy under the `[policy-options]`. The export policy will ensure the back-to-back exchange of RIP routes between the VPNSITE1 and PE-R2. The import policy will ensure the that any routes containing the policy are placed into the VRF table for transport to the other IBGP neighbor. Just like the `RIPEXPORT` policy, both the import and export policies will be applied under the `[routing-instances CUSTOMER1_VPN]`. The whole configuration for the PE-R2 is shown by listing 6 as shown below.

```
policy-options {
policy-statement CUSTOMER1_VPN-export-policy {
    term 1 {
        from protocol [ rip direct ];
        then {
            community add CUSTOMER1_VPN;
            accept;
        }
    }
    term 2 {
        then reject;
    }
}
policy-statement CUSTOMER1_VPN-import-policy {
    term 1 {
        from {
            protocol [ direct bgp ];
            community CUSTOMER1_VPN;
        }
```

```
            then accept;
        }
        term 2 {
            then reject;
        }
    }
    policy-statement RIPEXPORT {
        term 1 {
            from protocol bgp;
            then accept;
        }
        term 2 {
            then reject;
        }
    }
    community CUSTOMER1_VPN members target:200:200;
}
routing-instances {
    CUSTOMER1_VPN {
        instance-type vrf;
        interface em0.0;
        route-distinguisher 100:100;
        vrf-import CUSTOMER1_VPN-import-policy;
        vrf-export CUSTOMER1_VPN-export-policy;
        vrf-target target:200:200;
        vrf-table-label;
        protocols {
            rip {
                send multicast;
                receive version-2;
                group RIPROUTES {
                    export RIPEXPORT;
                    neighbor em0.0;
                }
            }
        }
    }
}
```

Listing 6. JunOS PE-R7 configuration.

These are somewhat in a few words the necessary configuration details on the PE routers and a vital part of the project that aims to achieve the project goals. The next chapter is the verification and troubleshooting of the configurations made in this chapter.

5 Verifying and Troubleshooting the Configuration

The configuration process of the MPLS L3VPNs tend to be in most cases complex. In the adoption of the end-to-end and to a further extent a step-by-step configuration approach, the verification tends to be relatively faster and more efficient. The troubleshooting process of an MPLS L3VPN can be divided into two basic and quite important elements. Firstly, is the troubleshooting of the route advertisement between the two customer sites and secondly, troubleshooting of the traffic across the service provider’s backbone.

When the configuration is properly done and correct, then the assumption would be that route advertisement from one CE device, across the MPLS L3VPN Backbone to the other CE device would be successful. This is not always the case as in some scenarios, ping or tracerouting from one CE to the other sometimes returns the unwanted result.

The role of troubleshooting is to correct the situation, for instance to make the undesired result that one gets change to the desired result that was expected in the first instance. An example of such is to make the ping failure back to a success.

In the MPLS L3VPN troubleshooting, it is wise to start at a particular end of the VPN i.e. the local CE router and to follow the routes to the remote CE device. The start in this case will be the VPNSITE1 which represents the CE number 1. The question to ask is whether the customer routes that are advertised by the VPNSITE1 are successfully advertised between the given CE device and the MPLS Backbone. The flow of traffic will be from the VPNSITE1 which runs IOS to the PE-R2 running JunOS. So much of the troubleshooting commands will be from JunOS and entered in the PE-R2 router.

The routing protocol that was configured between the VPNSITE1 and the PE-R2 router is RIPv2. In regards to this, the important component is to check that the adjacency and the peering information are all correct and fully operational. While doing this, the name of the routing instance has to be specified. To check the configured RIPv2 adjacency information, the following command, **`run show rip neighbor instance CUSTOMER1_VPN`** will display whether the adjacency is up or down. In this case, the peering and adjacency is fully operational. In a case where it is not, the routing protocol that was configured on the VPNSITE1 should be checked whether it was done correctly, and eventually the routing protocol configuration for the VPN **`CUSTOMER1_VPN`** routing instance that was configured on the PE-R2. These are the two common mistakes that will make the RIPv2 adjacency and peering to not work.

Secondly, check that the VPNSITE1 and the PE-R2 can ping each other successfully. Run the ping from the VPNSITE1 to the 172.16.12.2 which is the IP address of the PE-R2. If the ping turns out a positive result then it means that the results set out in the project have been achieved. To check that the local PE-R2 router can ping the VPNSITE1, then use the following command, **`run ping routing-instance CUSTOMER1_VPN 172.16.12.1`**. It is worth noting that the adjacency or the peering between a local PE and CE routers always has to be up before the **`ping`** command is

successful. To prove this then, delete the **interface** statement under the **[edit routing-instances CUSTOMER1_VPN]**. Then recommit the configuration. This will remove the already configured interface from the configured VPN. Trying the **ping** command again will be successful.

Thirdly, on the local PE-R2 device, the routes that were advertised by the local VPNSITE1 should be installed in the VRF table. The following command will show the routes.

```
root@PE-R2# run show route table CUSTOMER1_VPN.inet.0 detail

CUSTOMER1_VPN.inet.0: 6 destinations, 6 routes (6 active, 0
holddown, 0 hidden)
172.16.1.1/32 (1 entry, 1 announced)
        *RIP    Preference: 100
                Next hop type: Router, Next hop index: 581
                Address: 0x9334328
                Next-hop reference count: 2
                Next hop: 172.16.12.1 via em0.0, selected
                State: <Active Int>
                Age: 1:53:09  Metric: 2    Tag: 0
                Task: CUSTOMER1_VPN-RIPv2
                Announcement bits (2): 0-KRT 2-
BGP_RT_Background
                AS path: I
         Route learned from 172.16.12.1 expires in 169
seconds

172.16.12.0/24 (1 entry, 1 announced)
        *Direct Preference: 0
                Next hop type: Interface
                Address: 0x9334298
                Next-hop reference count: 1
                Next hop: via em0.0, selected
                State: <Active Int>
                Age: 1:53:23
```

Listing 7. JunOS PE-R2 VRF Table installed routes.

The above output information about the VRF table shows the RIPv2 routes that are advertised by the local VPNSITE1. In some situations, the routes from the VPNSITE1 might not be available in the VRF routing table. The way to troubleshoot this is by checking that the VPNSITE1 is actually advertising routes.

Fourthly, on the local PE-R2, the routes that are from the remote PE-R7 should be present in the bgp.l3vpn.0 routing table. The table displays the following shown below by listing 11.

```
root@PE-R2# run show route table bgp.l3vpn.0 extensive

bgp.l3vpn.0: 2 destinations, 2 routes (2 active, 0 holddown,
0 hidden)
100:100:192.168.8.8/32 (1 entry, 0 announced)
        *BGP    Preference: 170/-101
                Route Distinguisher: 100:100
                Next hop type: Indirect
                Address: 0x9335210
                Next-hop reference count: 3
                Source: 7.7.7.7
                Next hop type: Router, Next hop index: 587
                Next hop: 10.0.21.3 via em1.0, selected
                Label operation: Push 25, Push 19(top)
                Label TTL action: prop-ttl, prop-ttl(top)
                Protocol next hop: 7.7.7.7
                Push 25
                Indirect next hop: 944ce80 131070
                State: <Active Int Ext>
                Local AS:    27 Peer AS:    27
                Age: 2:10:42  Metric: 156160   Metric2: 1
                Task: BGP_27.7.7.7.7+179
                AS path: ?
```

Listing 8. JunOS bgp.l3vpn.0 routing table.

The output shown above contains important information about the VPN. If the routes from the VPNSITE1 are not available or cannot be seen from the VRF routing table on the PE-R7 then the following will correct the problem. Firstly, check that the VRF import policy that was configured on the PE-R7 router to be sure it was done correctly and corresponds to those configured in the PE-R2 under the VRF configuration. Secondly, check that there is LDP connectivity between the PE routers. Thirdly, check that the iBGP session configured between the two PE routers is fully functional. To see whether those routes are there on the PE router, enter the following command and get the results displayed below.

```
PE-R7#sh ip bgp Vpnv4 vrf CUSTOMER1_VPN
BGP table version is 9, local router ID is 7.7.7.7
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal,r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network      Next Hop       Metric LocPrf Weight Path
Route Distinguisher: 100:100 (default for vrf CUSTOMER1_VPN)
```

```
*>i172.16.1.1/32    2.2.2.2           2    100      0 i
*>i172.16.12.0/24   2.2.2.2                100      0 i
*> 192.168.8.8/32   192.168.78.8      156160          32768 ?
*> 192.168.78.0     0.0.0.0                0         32768 ?
```

Listing 9. Different iBGP routes installed in PE-R7.

When the routes that are advertised by the VPNSITE2 can be seen in the VRF routing table at the PE-R7, then this indicates there is a way to which the VPNSITE2 can be reached. So a ping from from the PE-R7 to the VRF interface that was configured pointing to the physical and loopback addresses of the network 192.168.78.0 should be all successful. A proof of this is shown below.

```
PE-R7#ping vrf CUSTOMER1_VPN 192.168.78.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.78.8, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
20/22/24 ms
PE-R7#ping vrf CUSTOMER1_VPN 192.168.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.8.8, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
8/20/32 ms
```

Listing 10. Ping results to remote PE-R2

If this step-by-step method works and all the components achieve the desired result, then the same could be done from the VPNSITE2 through the other routers until the VPNSITE1. These are the different scenarios and the troubleshooting techniques that will be used in solving the problems.

This part of the project set to ascertain that an end-to-end reachability can be attained in the end. Different test will be conducted ranging from simple ping to traceroute in an attempt to gain a better understanding of the end result achieved. What is expected versus the reality of the achieved results will be compared. The expected result is that a traffic generated at one local CE router should be able to reach the other remote CE

router. So a ping from the VPNSITE1 to the VPNSITE2 should be successful and vice versa when it's from the VPNSITE2 to VPNSITE1. A ping however, does not serve to portray much information albeit it depicts the reachability of one site to and from the other. Traceroute on the other hand shows the different hops and routers that the traffic takes when it comes from a particular source and directed towards a given direction.

The other important component worth taking into account is that, since the customer has no control over the Backbone core, the routes that are related to the Background core should not be displayed by either of the CE routers. The CE routers will behave as if they are directly connected. What this means is that the Backbone core is assumed to be not present by both the CE routers. So a simple **`show ip route`** command on either CE router should show the directly connected routes and those that have been learned through the routing protocol that was configured on the other CE router. So a **`show ip route`** command on VPNSITE1, should show the directly connected routes from the 172.16.0.0 network and RIPv2 learned routes from the 192.168.0.0 network. The same should hold for the VPNSITE2, which should show directly connected routes from network 192.168.0.0 and EIGRP learned routes from 172.16.0.0 network. A sample output to prove these points are shown below.

```
VPNSITE1#sh ip route

     192.168.8.0/32 is subnetted, 1 subnets
R       192.168.8.8 [120/1] via 172.16.12.2, 00:00:19,
FastEthernet0/0
R    192.168.78.0/24 [120/1] via 172.16.12.2, 00:00:19,
FastEthernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.12.0/24 is directly connected,
FastEthernet0/0
C       172.16.1.1/32 is directly connected, Loopback0
```

Listing 11. Routes in the VPNSITE1.

```
VPNSITE2#sh ip route

     192.168.8.0/32 is subnetted, 1 subnets
C       192.168.8.8 is directly connected, Loopback0
C    192.168.78.0/24 is directly connected, FastEthernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D EX    172.16.12.0/24
           [170/2560002816] via 192.168.78.7, 01:03:11,
FastEthernet0/0
```

```
D EX    172.16.1.1/32
                [170/2560002816] via 192.168.78.7, 01:03:11,
    FastEthernet0/0
```

Listing 12. Routes in the VPNSITE2.

The ping and traceroute are verification commands. To further get to the nitty gritty details of what is really happening, and what path a given packet takes from its source to the destination and how the labels are switched is vital. Traceroute helps in regards to this but using the packet tracer for Cisco routers and UNIX commands in the Juniper routers serve as major ways in the further understanding of what happens.

The verification process will consist of generating traffic from either CE routers and then monitoring the different activities that occur on the PE routers. A traceroute that is run on the VPNSITE1 show the path taken by a packet until it reaches the destination as shown below.

```
VPNSITE1#traceroute 192.168.8.8
Type escape sequence to abort.
Tracing the route to 192.168.8.8

  1 172.16.12.2 24 msec 12 msec 4 msec
  2 10.0.21.3 [MPLS: Labels 16/25 Exp 0] 88 msec 64 msec 68
msec
  3 10.0.27.6 [MPLS: Labels 16/25 Exp 0] 76 msec 64 msec 112
msec
  4 192.168.78.7 [MPLS: Label 25 Exp 0] 64 msec 60 msec 80
msec
  5 192.168.78.8 68 msec *  104 msec
VPNSITE1#traceroute 192.168.78.8

Type escape sequence to abort.
Tracing the route to 192.168.78.8

  1 172.16.12.2 20 msec 4 msec 20 msec
  2 10.0.21.3 [MPLS: Labels 16/26 Exp 0] 48 msec 64 msec 52
msec
  3 10.0.27.6 [MPLS: Labels 16/26 Exp 0] 68 msec 68 msec 60
msec
  4 192.168.78.7 [MPLS: Label 26 Exp 0] 68 msec 60 msec 44
msec
  5 192.168.78.8 88 msec *  60 msec
```

Listing 13. Traceroute to 192.168.0.0 network.

A traceroute from VPNSITE1 to VPNSITE2 follows the following path, **VPNSITE1→PE-R2→P-R3→P-R6→PE-R7→VPNSITE2**. The traceroute from a given CE site to the other denotes end-to-end reachability of packets from one CE site to the other [16;17, pg. 887-889]

The results of the project that were achieved and their discussions are laid out in the following chapter.

6 Results and Discussions

The goal of the project was to design, implement and verify a MPLS Layer 3 Virtual Private Network. Merely presenting the results and implementing the topological structure of the project and verifying all the configurations is not enough. Explaining what really happens behind that seems to be a key part of the project.

In as much as the end-to-end connectivity has been achieved, discussing the results and explaining why certain facts are as they seem is paramount. A simple ping or traceroute to a given CE router from another CE router seems successful. The question is not whether the pings are successful, but about what happens when a packet leaves one CE site and traverses the provider's core and reaches the other CE site successfully.

At customer site, the network can be further divided into several departments according to organizational needs. These different departments can generate traffic (inform of packets) of varying quantities. Proper mechanism has to be put in place to handle the traffic that might be going out or coming into the customer's premises/networks. The mechanisms will not be discussed, but rather, how the traffic move from one customer site to the other across and MPLS L3VPN Backbone that is run and operated by a third party: the service provider. The traffic generated by a particular site depends on the addressing scheme that the customer uses. That can be either IPv4 or IPv6. In this project the customer uses IPv4. What this means is that the customer advertised routes towards the edge PE routers are IPv4 based packets.

The traffic moves and finally gets to the PE router (VPNSITE1, assuming in the first scenario that the traffic moves from the VPNSITE1 to VPNSITE2). When it gets to the PE router, there are mechanism that are involved in the configuration at the PE-R2 to handle that traffic. The different MPLS L3VPN components that was configured on both the PE routers are VRF, import and export policies, IGP routing between the PE routers, VPNv4 and MBGP. The MP-BGP is a BGP extension that allows for unicast and multicast topological support by a router. MP-BGP can carry different types of routed protocols such as IPv4 or IPv6. These routes from VPNSITE1 are not supposed to be destined at the PE-R2. The BGP configurations in the topology was configured for unicast and carrying IPv4 and VPNv4 routes.

The CE-router-received routes are converted by the PE-R2 to VPNv4 routes. VPNv4 is when the RD and the IPv4 customer prefix is combined together. The IPv4 prefixes are extracted from the customer advertised routes that come from the CE routers and are combined with the RD that is configured on the PE devices. The RD configured on both the PE routers is 100:100 and this will be combined with routes advertised by VPNSITE1 which are 172.16.1.1 and 172.16.12.1. The resultant VPNv4 routes will be 100:100:172.16.1.1/32 and 100:100:172.16.12.1/24. These routes are after that marked with VRF target. This is an extended BGP community attribute that serves in the

identification of a given VPN that a particular route belongs to. In this project there is only one VPN named `CUSTOMER1_VPN` with a RD 100 and RT value for both import and export set at 200:200.

The IGP protocol run in the core is OSPF. The concept of synchronization frequently comes up in configurations that involve BGP as the AS are required to consistently behave when IGP and IBGP are run in the provider's core. Both of them have to agree. The topology of the project consists of a scenario where the IBGP peers have several hops in between them. To reach the peers, the network in turn used an IGP which is OSPF in the communication between the peers. The purpose of this is to ensure that one of the BGP peers does not try forwarding a packet to the next peer unless the network knows what to do with the packet. The resultant VPNv4 prefixes are then passed into the MP-BGP and transported to the other PE router.

The receiving PE router (PE-R7), perform filtering of the incoming routes (VPNv4 routes). The extended community attribute is the basis of which the incoming routes are filtered. The RD is then removed from the VPNv4 routes and finally the routes are announced to the destination CE router (VPNSITE2).

For the routes that are advertised by VPNSITE2 to the PE-R7 router through EIGRP, when the route reaches the PE-R7. The received routes (192.168.78.8 and 172.16.8.8) have the RD added to them to become VPNv4 routes. The VPNv4 routes are then carried by MBGP across the P routers to the PE-R2 which then removes the RD information and then advertises such routes to the VPNSITE1.

The next chapter concludes of the project and gives the necessary important details in a summary.

7 Conclusion

The goal of the project was to design, implement and verify a Layer 3 VPN that uses MPLS and then depending on the design specification of the topology, which was to use a combination of both Cisco and Juniper routers, make the end-to-end movement of traffic from one CE device to the other successful. When conducting the project, the important things that were taken into consideration were, firstly, the routers that were from different vendors and had different design specification and IOS running inside them

that were different from each other, secondly, the way or manner in which the CLI was different and the commands between the Cisco ad Juniper quite different from each other. For Cisco, configuration-wise, it was straightforward when undertaking the configurations something that was totally different with Juniper, which was a little, complicated.

In the process of making the project, the main features of the IOSs versions that are used by Cisco and Juniper together with the benefits and drawbacks were discussed. The result was to an extent a smaller portion of what really happens in big networks that are controlled and managed by the service provider, which then offers the L3VPN as one of the many services to the customers/businesses. The project served to show that when the right/correct router versions for example those that support MPLS are used, then configuration of L3VPN is possible and can serve as an example in furthering the learning and proper understanding of how large MPLS L3VPN networks that are operated by the service providers and that involves thousands if not millions of routes are configured and made to work.

Better understanding of L3VPN, that is one of the most common service that is contracted by businesses/customers form the service provider, was understood better while conducting the project. The L3VPN service is one of the most important and highest sources of income for the service provider. Businesses too pay lots money just to contract that service. Major and important differences between Cisco and Juniper regarding the differences in their configuration, together with the benefits that one might have over the other, the drawbacks of choosing one over the other. I think that the insight gained while working on this project will not only be beneficial for me, but to the many others who may at some point like to gain insight in either the interoperability of different routers from varied vendors or in the configuration of the MPLS L3VPN.

This project did not encompass the security of the MPLS L3VPN, which in real life situations is one of the major important components in the VPNs. The project was a skeleton of a bigger MPLS L3VPN network, and what was considered here was the designing, implementation, verification and the eventual troubleshooting of the MPLS L3VPN between the specified Juniper and Cisco routers. In the end, the challenges that were to be achieved or solved in the project, which was the creation of an MPLS L3VPN and to further ensure interoperability of routers from different vendors and to ensure the eventual traversal of traffic from each side of the CE to the other. Although, the project

covers the simple details related to the L3VPNs, is can prove important to beginners who might want to better understand or expand their knowledge when it comes to understanding VPNs.

Refences

1 Jim Duffy (2010). Cisco vs Juniper: Today's 20 Greatest Tech Battles [online]. PC World, 20 November 2010
URL:http://www.pcworld.com/article/198147/Cisco_Juniper.html
Accessed 25 January 2016.

2 Jim Duffy (2008). Cisco IOS vs Juniper JunOS: The Technical Differences [online]. Network World, 17 April 2008.
URL:http://www.networkworld.com/article/2278153/data-center/cisco-ios-vs--juniper-junos--the-technical-differences.html
Accessed 25 January 2016

3 Jim Duffy (2008). Cisco's IOS vs Juniper's JunOS: Cisco questions JUNOS purity [online]. Network World, 17 April 2008
URL:http://www.networkworld.com/article/2278150/data-center/cisco-s-ios-vs--juniper-s-junos.html Accessed 30 January 2016.

4 Margaret Roose (2013). Routing and Switching: Cisco IOS [online]. Search Networking, December 2013.
URL:http://searchnetworking.techtarget.com/definition/Cisco-IOS-Cisco-Internetwork-Operating-System Accessed 30 January 2016.

5 Cisco (2013). Cisco IOS Software Releases 12.4 Machine: Cisco IOS Software Release Guide [online]. Cisco, October 2012.
URL:http://searchnetworking.techtarget.com/definition/Cisco-IOS-Cisco-Internetwork-Operating-System
Accessed 30 January 2016.

6 Juniper Networks (2015). Network Operating System: JUNOS [online]. Juniper, 2015.
URL: http://www.juniper.net/us/en/products-services/nos/junos/
Accessed 30 January 2010.

7 Cisco (2010). Using the Cisco IOS Command-Line Interface: Cisco IOS CLI Command Modes Overview [online]. Cisco Systems, Inc., 2010.
URL:http://www.cisco.com/c/en/us/td/docs/ios/fundamentals/configuration/guide/15_1s/cf_15_1s_book/cf_cli-basics.pdf
Accessed 30 January 2016.

8 Aviva Garett (2006). JUNOS Cookbook: Time-Saving Techniques for JUNOS Software Configuration. O'Reilly Media, Inc.

9 Cisco (229). Cisco and Standards: Opening the Door to Borderless Networks [online]. Cisco Systems, Inc. 2009.

URL:http://webtorials.com/main/resource/papers/cisco/paper145/standards.pdf Accessed 30 January 2016.

10 Kevin Dooley & Ian J. Brown (2006). Cisco IOS Cookbook: Field-Tested Solutions to Cisco Router Problems. O'Reilly Media, Inc. 2006.

11 Cisco (2006). Layer 3 MPLS VPN Enterprise Consumer Guide Version 2. Cisco Systems, Inc. 2006.

12 Cisco (2009). Multiprotocol BGP MPLS VPN: Information About Multiprotocol BGP MPLS VPN. Cisco Systems, Inc. 2009. URL:http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp-bgp-mpls-vpn.pdf Accessed 30 January 2016.

13 Cisco (2013). MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T. Cisco Systems, Inc. 2013.

14 Network Working Group (2001). RFC-3031: Multiprotocol Label Switching Architecture. Cisco Systems & Juniper Networks, Inc. 2001.

15 Network Working Group (2006). RFC-4364: Multiprotocol Label Switching Architecture. Cisco Systems & Juniper Networks, Inc. 2006.

16 Mark Lewis (2006). Troubleshooting VPNs: Troubleshooting MPLS VPNs [online]. InformIT, 2006. URL:https://www.informit.com/library/content.aspx?b=Troubleshooting_VPNs&seqNum=54 Accessed 30 January 2016.

17 Juniper Networks (2016). JUNOS OS: Layer 3 VPNs Feature Guide for Routing Devices. Juniper Networks, Inc. 2016.

18 Network Lessons (2016). MPLS LDP:Label Distribution Protocol. NetworkLessons.Com, 2016. URL: https://networklessons.com/mpls/mpls-ldp-label-distribution-protocol/ Acessed 30 January 2016.

Title of the Appendix

Content of the appendix is placed here.

Title of the Appendix

Content of the appendix is placed here.