Chapter 2 Literature Review

This chapter covers the review of the current networking technologies. The first section begins with an introduction to MPLS. A detail description is provided, which includes the MPLS terminology, MPLS operation as well as the strength of MPLS. This section ends with a summary of MPLS.

The following sections cover an overview of VPN. This section begins with an introduction of VPN. Then, it follows by a discussion on the various type of VPN, the attribute of VPN and the model of VPN. Besides that, different topologies for VPN are discussed followed by the strength of VPN and a summary of VPN.

The third section of this chapter discusses the MPLS VPN. This section begins with an introduction of IPSec and MPLS VPN. A comparison between IPSec and MPLS is reviewed. Then, it is followed by a detail description on MPLS VPN, which includes the MPLS VPN terminology, the characteristic of MPLS VPN, the strength of MPLS VPN and the security of MPLS VPN. The current research on MPLS VPN is also discussed in this section.

The fourth section details some of the protocol needed in the MPLS VPN backbone. It includes the discussion of MP-iBGP, OSPF and Cisco Express Forwarding technology. The final section will conclude a review on the networking technologies describe in this chapter.

2.1 MPLS

MPLS is a technology for backbone networks that can be used for Internet Protocol as well as for other network layer protocols. It is the convergence of connection-oriented techniques and the Internet routing protocols. The ability to forward packets over arbitrary non-shortest path and emulate high-speed tunnel between non-label switched domains makes MPLS the solution to IP QoS, gigabit forwarding, network scaling and traffic engineering [5].

MPLS evolved from numerous priors' technologies including Cisco's Tag Switching, IBM's ARIS and Toshiba's Cell-Switched Router [6]. MPLS was created to combine the benefits of

connectionless layer 3 routing and forwarding with connection-oriented layer 2 forwarding.

One of the most important features under the MPLS architecture is that, MPLS is split into two components, namely the control plane and forwarding plane. The forwarding component of MPLS is used to perform forwarding of data packets based on labels carried by packets. The control component of MPLS is responsible for creating and maintaining label binding among a group of interconnected label switches [5]. The separation of control and forwarding component allows each component to be developed and modified independently.

MPLS simplifies per-hop data forwarding by replacing the layer 3-lookup functions performed in traditional routers with simplified label swapping [1]. MPLS also improves scalability through label stacking and merging. Furthermore, MPLS provides traffic engineering via efficient routing.

2.1.1 MPLS Terminology

There are some new terminologies under the MPLS architecture. The following section discusses briefly each of these terminologies.

2.1.1.1 Label

A label is a short, fixed length, locally significant identifier that is used to identify a Forwarding Equivalence Class (FEC) [7]. These labels are used to identify classes of data packets, which are treated indistinguishably when forwarding under the label swapping. One key to the scalability of MPLS is that labels have local significance between two devices or switches that are communicating [3].

MPLS label is carried in a packet header and represents the packet's FEC. The header format depends upon network characteristics. In router networks, the label is a separate 32-bit header located after the layer 2 header and before the IP header or the layer 3 header. In ATM networks, the label is encoded in the virtual channel identifier/virtual path identifier (VCI/VPI) fields. Figure 2.1 shows the MPLS label in ATM and PPP/LAN.

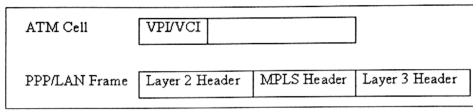

Figure 2.1 MPLS Labels in ATM and PPP/LAN

The MPLS label header is formatted as below. Figure 2.2 shows the MPLS label header.

- The label field, whose length is 20 bits, carries the actual value of the MPLS label.
- The Class of Service (CoS) field, whose length is 3 bits, affects the queuing and discard algorithms applied to the packet as it is transmitted through the network.
- The Stack (S) field, whose length is 1 bit, supports a hierarchical label stack.
- The Time-To-Live (TTL) field, whose length is 8 bits, provides conventional IP TTL functionality.

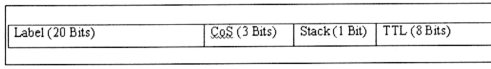

Figure 2.2 MPLS Labels Header

2.1.1.2 Forwarding Equivalency Class (FEC)

FEC can be visualized as describing a group of IP packets that are forwarded in the same manner, over the same path and with the same treatment [7]. Typically packets belonging to the same FEC will follow the same path in the MPLS domain. While assigning a packet to an FEC, the ingress LSR looks at the IP header and the interface. Then, a label is assigned to the packet, which identified the FEC.

One example of an FEC is a set of unicast packets whose network layer destination address matches a particular IP address prefix and whose Type of Service bits are the same. Besides that, a set of multicast packets with the same source and destination network layer addresses is another example of FEC [8].

2.1.1.3 Label Stack

In order to transmit a labeled packet on a particular data link, LSR must support an encoding technique. LSR will produce a labeled packet when given a label stack and a network layer packet. A packet with an empty stack is called an unlabeled packet. An LSR forwards unlabeled packets at the IP layer. It is possible for a packet to have a stack of m labels. In a given domain, the label at the top of the stack is the only one that determines the forwarding decision [9].

Label stacking has a number of usages. It is useful when two labels are used for Interior Gateway Protocol (IGP) and Border Gateway Protocol (BGP). The BGP label is used to forward packets from one BGP speaker to another BGP speaker, while the IGP label is used to forward packets within an autonomous system [9].

2.1.1.4 VC Merging

Under the merging approach, if multiple incoming streams at a given LSR are going to the same egress LSR, the incoming labels will be swapped to the same outgoing label. The merging of stream can be viewed as creating a multipoint to point connection [10].

When ATM is used, incoming VCs will be merged to the same outgoing VC. However, cells belonging to different packets for the same egress LSR cannot be interleaved because the receiver will not be able to reassemble the packets. Thus, under the VC merging, the cells should first be reassembled by using the end of packet bit accommodated in ATM Adaptation layer (AAL5) before merging [10].

Since the number of labels used can be significantly reduced when implementing the merging. MPLS has offered a great degree of scalability and makes it appropriate for very large domain.

2.1.1.5 Label Switch Router (LSR)

LSR is any router or switch that implements label distribution procedures and forwards packets based on labels. There are various types of LSR, namely the normal LSR, edge-LSR, ATM-LSR and ATM edge-LSR. A normal LSR forwards labeled packet according to pre computed switching tables. When an edge LSR receives an IP packet, it will perform layer 3 lookups and impose a label stack before forwarding the packet into the LSR domain. This type of edge LSR is called ingress edge LSR. Another type of edge LSR is called egress edge LSR. When the egress edge LSR receives a labeled packet, it will remove the labels, performs layer 3 lookups and forwards the IP packet towards its next hop [7].

An ATM-LSR is an ATM switch that can act as a LSR. The ATM-LSR will perform IP routing and label assignment in the control plane and forwards the data packets using traditional ATM cell switching mechanisms on the forwarding plane. The ingress ATM edge LSR will receive a labeled or unlabeled packet and then segments it into ATM cells before forwarding the cells towards the next hop ATM-LSR. Meanwhile, the egress ATM edge LSR will receive ATM cells from an adjacent ATM-LSR and then reassembles these cells into the original packet before forwarding the packet as a labeled or unlabeled packet [7].

2.1.1.6 Label Switched Path (LSP)

LSP is a specific traffic path through an MPLS network. This path will describe the set of LSRs through which a labeled packet must traverse to reach the egress LSRs for a particular FEC. The LSP is unidirectional. A different LSP is needed to return traffic from a particular FEC [7]. A LSP is provisioned using Label Distribution Protocols (LDP). It can be either static or dynamic. Normally the creation of LSP is connection-oriented because the path is setup prior to any traffic flow.

Since MPLS allows hierarchy of labels known as label stack, it is possible to have different LSPs at different levels of labels for a packet to reach its destination. Basically, a LSP of a packet with a label of level m is a set of LSRs that a packet p has to travel at level m to reach its destination.

2.1.1.7 Label Distribution Protocol (LDP)

LDP is a protocol that enables LSR to distribute labels to its LDP peers. When a LSR assigns a label to a FEC, it needs to let its relevant peers know of this label and its meaning and LDP is used for this purpose. Label bindings between two LSR can be distributed by an upstream LSR or a downstream LSR [11].

During the LDP process, when LSR1 detects that LSR2 is its next hop for FEC. LSR1 will send a label request message to LSR2. Upon receiving the message, LSR2 will respond with a label-binding message that specifies the label-to-FEC binding. This mode is called the downstream-on-demand mode because LSR2 distribute a label binding in response to an explicit request from LSR1 [11].

LDP provides communication between edge and core devices. It assigns labels in edge and core devices to establish LSPs in conjunction with routing protocols such as OSPF, IS-IS, EIGRP or BGP.

Since a set of labels from the ingress LSR to the egress LSR in an MPLS domain defines a LSP, LDP helps in establishing a LSP by using a set of procedures to distribute the labels among the LSR peers. LDP dynamically establishes a shortest path LSP tree between all the edge LSRs for each identifiable FEC [11].

2.1.1.8 Explicit Routing

In an explicit routing, the route taken by a packet is determined by a single node usually the ingress LSR. It allows traffic to be mapped to the physical topology of a network in a more flexible way than the hop-by-hop routing. One useful application of explicit routing is to maximize resource utilization in the network.

MPLS facilitates explicit routing, since the sequence of LSRs to be followed need not be carried in the packet header as in conventional datagram networks. In the MPLS network, there may be multiple explicit routing routed LSPs setup between the ingress and egress

LSRs. Based on the state of the LSPs, the ingress LSR can perform load balancing to use the network resources efficiently [12].

2.1.2 MPLS Operation

In a MPLS network, incoming packets are assigned a label by an ingress edge LSR. This label will indicate both routes and service attributes. The core merely reads labels, applies appropriate services, and forwards packets based on the label. Processor-intensive analysis, classification and filtering happen only once at the ingress edge. At the egress edge, labels are stripped and packets are forwarded to their final destination [3]. Figure 2.3 shows an example of MPLS network.

Under the MPLS architecture, the LDP will first automatically assigned label to each LSRs. The network automatically builds routing tables through routers or IP+ATM switches throughout the ISP network using IGP such as OSPF, EIGRP, or IS-IS. The LDP uses the routing topology in the tables to establish label values between adjacent devices. This operation creates LSPs or pre configured maps between destination end points.

After the label has been setup successfully, the MPLS network will be able to perform label switching. When an ingress packet enters the ingress edge LSR, it is processed to determine which layer 3 services it requires, such as QoS and bandwidth management. Based on routing and policy requirements, the ingress edge LSR selects and applies a label to the packet header. Then, it forwards the packet to the core LSR. The LSR in the core reads the label on each packet and replaces it with a new one as listed in the table and forwards the packet to next router. This action is repeated at all hops in the core.

Finally, when the packet reaches the egress edge LSR, it strips the label, reads the packet header and forwards it to its final destination.

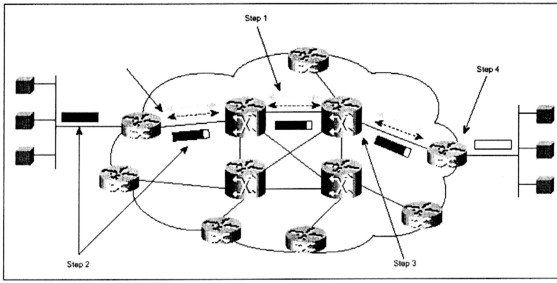

Figure 2.3 MPLS Network

2.1.3 Strength of MPLS

MPLS is an innovative approach that uses a label-based forwarding paradigm. One key to the scalability of MPLS is that labels have only local significance between two devices that are communicating. This characteristic is essential to implementing advanced IP services such as QoS, mega scale VPNs and traffic engineering.

MPLS provides traffic engineering during explicit routing. Routing with Resource Reservation (RRR) lets ISPs maximize the utilization of network resources and operate their IP networks as efficiently as possible. RRR allows the network operator to apply and enforce explicit routing, which overrides the traditional IP forwarding techniques and provides fast restoration and protection mechanisms. [13]

MPLS has a number of advantages over the conventional IP routing. In conventional IP forwarding, a particular router will typically consider two packets to be in the same FEC if there is some address prefix X in that router's routing tables such that X is the longest match for each packet's destination address. As the packet traverses the network, each hop in turn reexamines the packet and assigns it to a FEC.

In MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network. The FEC to which the packet is assigned is encoded as a short fixed length value known as a label. When a packet is forwarded to its next hop, the label is sent along with it. At subsequent hops, there is no further analysis of the packet's network layer header. Rather, the label is used as an index into a table, which specifies the next hop and a new label. The old label is replaced with the new label and the packet is forwarded to its next hop [13].

In the MPLS forwarding paradigm, once a packet is assigned to a FEC, no further header analysis is done by subsequent routers. All forwarding is driven by the labels. This has a number of advantages over conventional network layer forwarding.

2.1.4 MPLS Summary

As a summary, MPLS was created to combine the benefits of connectionless layer 3 routing and forwarding with connection-oriented layer 2 forwarding. One of the key features of MPLS is the separation of the control component and forwarding component.

By using the label swapping forwarding paradigm, MPLS provides scalability. Besides that, MPLS architecture has support a lot of applications besides IP routing such as IP multicast routing, QoS, traffic engineering as well as VPN.

2.2 VPN

Businesses today are faced with supporting a variety of communications among a wide range of sites even as the business seek to reduce cost of their communications infrastructure. Employees are looking to access their corporate Intranet when telecommute or dial in from the customer sites. Furthermore, business partners are joining together in Extranet to share business information.

Due to the issue above, VPNs have been created to virtualize some portion of an organization communications. VPN is defined loosely as a network in which customer connectivity amongst multiple sites is deployed on a share infrastructure with the same access or security

policies as a private network [1]. In addition, VPNs are not limited to corporate sites and branch offices. It provides secure connectivity to the mobile users.

VPNs naturally fit the desire for low-cost WAN services over shared public infrastructures. It embodies the promise of delivering Intranet and Extranet services at a much lower cost than a private network. With the cost reduction and enhanced scalability and flexibility associated with the VPN technologies, VPN service has become the major driver for MPLS deployment in service provider and enterprise network [1].

2.2.1 Type of VPN

There are three common types of VPNs, which are aligned with how businesses and organizations use VPNs. Each of these VPNs type has its own unique usage and requirement.

2.2.1.1 Access VPNs

Access VPN provides remote access to a corporate Intranet or Extranet over a shared infrastructure with the same policies as a private network. It connects telecommuters and mobile users securely and cost-effectively to corporate network resources from anywhere in the world over any access technology. Access VPNs encompass analog, dial, ISDN, Digital Subscriber Line (DSL), mobile IP and cable technologies to securely connect mobile users, telecommuters or branch offices. Since this traffic may run on untrusted segments outside the ISP's network, it must be encrypted to ensure privacy and security.

Access VPNs use different architectures and technologies compared to Intranet and Extranet VPNs. Access VPNs today use a variety of access technologies that provide tunneling and overlay on top of an existing network, along with encryption for privacy. [3]

2.2.1.2 Intranet VPNs

Intranet VPNs link corporate headquarters, remote offices and branch offices over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, quality of service (QoS), manageability and reliability. It offers

an extremely cost-effective alternative to dedicated WANs. It needs to scale easily as the organization grows.

2.2.1.3 Extranet VPNs

Extranet VPNs link network resources with third party vendors and business partners, extending elements of the corporate Intranet beyond the organization. Extranet VPN access needs to be turned on and off on the fly to keep pace with rapidly changing business climates.

2.2.2 Attribute of VPN

This section describes the attribute of VPN. The essential attributes of a VPN can be segmented into six broad categories as follows:

Scalability - Must be scalable across various VPN platforms ranging from a small office configuration through the largest enterprise implementations ubiquitously on a global scale. Additionally, it must be highly scalable in order to accommodate unplanned growth and the ability to provision tens of thousands of VPNs. [14]

Security - Must offer different levels and methods of security to support wide variety of customers, including tunneling, encryption, traffic separation, packet authentication, user authentication and access control. [15]

Quality of Service - Must be able to assign priority to mission-critical or delay-sensitive traffic and manage congestion across varying bandwidth rates. Quality of service (QoS) functions like queuing, network congestion avoidance, traffic shaping and packet classification as well as VPN routing services utilizing an optimal routing protocol. [16].

Manageability - Must have advanced monitoring and automated flow-through systems to quickly roll out new services, enforce security and QoS policies as well as support service level agreements (SLA). [15]

Reliability - Must offer predictable and extremely high service availability that business customers expect and require. [15]

Any-to-any Connectivity - IP is by nature connectionless and globally ubiquitous. [3]

The keys to successfully broadening VPN services lie in the ability to offer Intranet and Extranet VPNs that scale well and can be quickly and flexibly deployed, along with a broad portfolio of access VPN services with maximum-security protection.

2.2.3 VPN Models

There are two widespread used of VPN models, namely the overlay model and the peer-to-peer model.

2.2.3.1 Overlay VPN Model

The overlay VPN model is a model where the ISP provides the customer with a set of emulated leased lines [1]. These leased lines are called VCs that can be manually setup like a Permanent Virtual Circuit (PVC) or established on demand like a Switched Virtual Circuit (SVC). Under this model, the routing protocol data is always exchanged between the customer devices over the VC. This model provides QoS guarantee in terms of bandwidth guarantee on a certain VC or maximum bandwidth available on a certain VC [1].

Overlay VPN model networks can be implemented with a number of network technologies like X.25, frame relay and ATM. Besides that, it can be implemented with IP-over-IP tunneling using Generic Route Encryption (GRE) and IP Security encryption (IPSec) in private IP backbone and over the public Internet.

However, the overlay VPN model has a number of drawbacks. It becomes very hard to manage in a meshed configuration when the size of the user increased. Besides that, the provision of VC capacities is not readily available. This model also increases the acquisition and operational cost when implementing with layer 2 technologies that are mostly IP-based. Figure 2.4 shows the overlay VPN model.

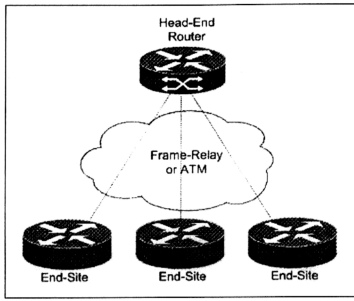

Figure 2.4 Overlay VPN Model

2.2.3.2 Peer-to-Peer VPN Model

The peer-to-peer model is a model where the ISP and the customer exchanges layer 3 routing information and the ISP relays the data between the customer sites on the optimum path between the sites and without the customer involvement [1]. This type of VPN model is introduced to alleviate the drawbacks of the overlay VPN model.

The peer-to-peer model provides a number of advantages over the overlay VPN model. In a peer-to-peer model, the routing becomes simple as the customer router exchanges routing information with only one Provider Edge (PE) router. Besides that, routing between the customer sites is always optimal because the provider routers know the customer's network topology and can thus establish inter-site routing. The bandwidth provisioning becomes simple as the customer only need to specify the outbound and inbound bandwidth. The peer-to-peer VPN model also simplified the management. All the modification is only done on one PE routers for any new site or site that need to be withdrawn.

There are two-implementation approaches under the peer-to-peer VPN model. In the share router approach, several customers can be connected to the same PE-router. Under this

approach, every PE-CE interface on the PE router need to be configured to ensure isolation between VPN customers to prevent a customer from breaking into another VPN network or performing a denial of service attack on another VPN customer. In the dedicated approach, VPN customers have their own dedicated PE router and thus have access only to the routes contained within the routing table of that PE router [17]. Figure 2.5 shows the shared router configuration of the peer-to-peer VPN model. Meanwhile, figure 2.6 shows the dedicated router configuration of the peer-to-peer VPN model [1].

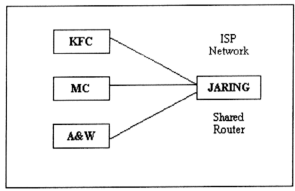

Figure 2.5 Shared Router Configuration for peer-to-peer VPN model

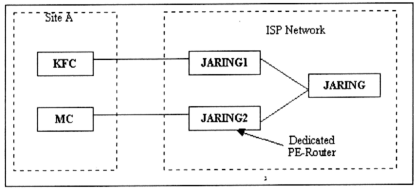

Figure 2.6 Dedicated Router Configuration for peer-to-peer VPN model

The peer-to-peer VPN model has a number of drawbacks that prevent its widespread use. The entire customer shares the same IP address space. This means that the ISP will allocate either the public IP address or private IP address to the customer. Furthermore, the peer-to-peer VPN model prevents the customers from getting Internet access from another service provider. Figure 2.7 shows the virtual networks classification based on the underlying technology.

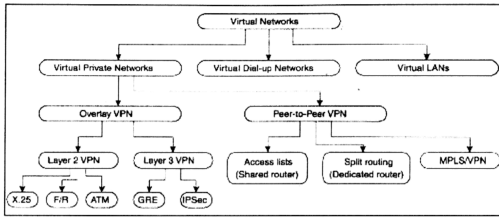

Figure 2.7 Virtual Networks Classifications

2.2.4 VPN Network Topology

A numbers of VPN network topologies are used in the industries. The type of topology chosen should be dictated by the business problems that the organization is trying to solve. This section will detail three major categories of VPN topologies:

2.2.4.1 Topologies Influence by Overlay Model

The topologies influence by the overlay model includes hub and spoke topology, partial full mesh topology and hybrid topology. The most common topology is the hub and spoke topology. Under this topology, a number of remote offices are connected to a central hub. Hub and spoke topology is used typically in organization with strict hierarchical structure. Besides that, this topology is suited to environment where the remote offices exchanged data with the central sites and not with each other. However, when implementing a redundant hub-and-spoke topology with an overlay VC-based VPN, it always poses a number of challenges. This is due to the extra VC for the additional router. When the network grows, the simple hub and spoke topology will transform into a multilevel topology [18].

The second type of topology is the partial mesh mode. The VPN sites are connected by VCs based on the traffic requirement. This topology is full mesh if every site has a direct connection to every other site and partial mesh if not the entire site have direct connection to each other. This topology is suitable for the organization that requiring data exchange

between various points. It also suitable for the organization that needs to handle the peer-to-peer communication among each others [18].

Provisioning a full-mesh topology is simple than the partials mesh topology because the full mesh topology needs to indicate the traffic matrix between a pair of sites. On the other hand, the partial mesh topology needs to indicate the traffic matrix as well as the traffic aggregation achieved over the VCs that the traffic between any two sites will flow [1].

2.2.4.2 Extranet Topologies

The Extranet topology links organizations that belong to the same community of interest and allowing any-to-any connectivity between the organizations. Thus, the data in the Extranet can be exchanged between any numbers of sites. This topology can be implemented as two different models. In the peer-to-peer model, each site specifies on the bandwidth requirement. Thus, the provision on the customer and service provider is very simple and effective. In the overlay model, the traffic between sites is exchanged over point-to-point VCs. One of the reasons that the Extranet is popular compared to the public Internet is that the Extranet offers QoS guarantee. Besides that, the data that exchanged over the Extranet are often sensitive and require more security protection [1].

2.2.4.3 Virtual Private Dial-up Network (VPDN) Topology

The VPDN topology is implemented by tunneling PPP frames exchanged between the dial-up user and the home gateway. The dial-up user and the home gateway establish IP connectivity over the tunneled PPP link and exchange data packets over it. Layer 2 Forwarding (L2F) and Layer 2 Transport Protocol (L2TP) are the protocols that used to implement the VPDN topology over the IP. In order to support security feature over the VPDN technology, the PPP can be encapsulated.

2.2.4.4 Manage Network VPN Topology

When ISP manages the customer premises routers in a managed network service, the managed network VPN topology is used. Under this topology, the ISP provisions a numbers

of routers in customer sites. All of this router will be connected with a Network Management Center. Normally a central services Extranet topology is implemented under this topology.

2.2.5 Strength of VPN

One of most compelling advantage of VPN is the cost reduction. While VPN offers direct cost savings over other communications methods such as leased lines and long-distance calls, it also offers other advantages, including indirect cost savings as a result of reduced training requirements and equipment, increased flexibility and scalability.

VPNs can reduce the demand for technical support resources. Outsourcing the VPN to ISP can reduce internal technical-support requirements, as the ISP will be responsible of the support tasks for the network.

Another important benefit of VPN is improved connectivity. Companies can enjoy higher levels of connectivity through a carrier-grade service offering. Businesses are connected worldwide through the enormous span of the ISP's IP, Frame Relay or ATM infrastructure, often in conjunction with the Internet. This allows access to a corporate network from a home office or small branch office no farther than a local or toll-free phone number. Besides that, VPNs enable the delivery of broadband services that are capable of delivering emerging multimedia applications [19].

VPNs include comprehensive security policies that are another valuable commodity to businesses. With VPN, organizations can be confident that their corporate data remains private and that their company transmissions are secure. The ability to prioritize traffic over a VPN ensures that the necessary bandwidth is available to mission-critical applications when required. The type of service needed is normally specified in the service level agreements (SLA).

2.2.6 VPN Summary

As a summary, VPNs deliver enterprise scale connectivity deployed on a shared infrastructure with the same policies enjoyed in a private network. However, the current VPN model namely

the overlay VPN model and the peer-to-peer VPN model still has a number of shortcomings. Due to this situation, MPLS VPN has been created in order to alleviate the drawbacks by combining the benefits of the peer-to-peer VPN technologies with the security and isolation of the overlay model.

2.3 MPLS VPN

Network vendors have scrambled to develop the technologies needed to realize the vision of fully standards-based VPNs. New world VPN services need reliable networks to support them. These networks must be scalable, cost-effective and capable of handling a wide range of customer requirements including security, QoS, and any-to-any connectivity. Besides that, this networks need to be application-aware. In order to achieve this goal, native separation and specific handling according to unique policies must be provided to each customer.

The IP-based virtual private network (VPN) is rapidly becoming the foundation for the delivery of new world services and many ISPs are offering value-added applications on top of their VPN transport networks. Two unique and complementary VPN architectures based on IP Security (IPSec) and Multiprotocol Label Switching (MPLS) technologies are emerging to form the predominant foundations for delivery of new world services.

2.3.1 Overview of MPLS VPN

In MPLS VPN, a VPN generally consists of a set of sites that are interconnected by means of an MPLS provider core network. The VPN can consist of sites that are all from the same enterprise, which is Intranet or from different enterprises, which is the Extranet. Each VPN has its own policies configured by the ISP.

MPLS VPN is created in layer 3 and it is a true peer-to-peer VPN model. MPLS enables ISP to provision complex VC meshes for each customer VPN and uses the same network infrastructure to support tens of thousands of VPNs with centralized, simplified provisioning and management [20].

MPLS VPN provides end-to-end security for subscriber transmissions. It provides security by separating traffic within the ISP's network using unique, per-customer labels or route distinguishers (RDs). RDs are assigned automatically when the VPN is provisioned and are transparent to end-users. The RDs are placed in packet headers to isolate traffic to specific VPN communities. Within the ISP network, RDs are associated with every packet, so the attempt to spoof a flow or packet cannot penetrate VPNs.

The MPLS VPN model is a true peer-to-peer VPN model that enforces traffic separations by assigning unique VPN route forwarding tables (VRFs) to each customer's VPN. Traffic separation occurs without tunneling or encryption because it is built directly into the network.

VPN-IP addresses are unique for each endpoint in the network and entries are stored in forwarding tables for each node in the VPN. As labels are used instead of IP addresses, customers can keep their private addressing schemes, within the corporate Internet, without requiring Network Address Translation (NAT) to pass traffic through the provider network [1].

To support a growing number of customers with global VPN requirements and limited bandwidth in some parts of the world, ISP requires the traffic engineering and scalability afforded by MPLS-based VPNs.

2.3.2 Overview of IPSec

IPSec is a highly secure infrastructure for transporting sensitive information over the public Internet [21]. It provides data privacy through a flexible suite of encryption and tunneling mechanisms that protect packet payloads as the data traverse the network. IPSec provides a secure infrastructure without costly changes to every computer on the network.
However, IPSec requires site-to-site peering in order to operate. Each endpoint will communicate to determine and agree upon the same authentication method. Clearly, IPSec should be used for maximum privacy when mission-critical data is involved.

For mobile users and telecommuters who require secure remote access, MPLS is simply not an option. MPLS is a network-based solution and does not go all the way out to endpoint

computing devices. MPLS stops at the edge of the service provider network. Therefore, IPSec is the only practical option at present to enable secure remote access VPNs.

2.3.3 Comparison between IPSec and MPLS VPN

The IPSec working group under the Security Area concentrates on the protection of the network layer by designing cryptographic security mechanisms that can flexibly support combinations of authentication, integrity, access control and confidentiality. The MPLS working group under the Routing Area, on the other hand, develops mechanisms to support higher layer resource reservation, QoS and definition of host behaviors. The following table shows the comparison between IPSec and MPLS VPN.

Table 2.1 Comparisons between IPSec and MPLS VPN

	IPSec	MPLS
Scalability	Large-scale deployment requires planning and coordination to address issues of policy synchronization and peering configuration.	Highly scalable since no site-to-site peering is required. Uses labels instead of predefined user relationships. A typical MPLS-based VPN deployment is capable of supporting tens of thousands of VPN groups over the same network.
Time to Market	IPSec can be deployed across any existing IP networks with no changes to applications.	Requires all participating network elements at the core and edge to be MPLS capable.
Place in Network	Best at the edge and off net where there is a higher degree of exposure to data privacy and where IPSec security mechanisms such as tunneling and encryption can best be applied.	Best within the core where QoS, traffic engineering and bandwidth utilization can be fully controlled, especially if SLA is to be offered as part of the VPN service.
Provisioning	No network level provisioning is required.	Requires just a one-time provisioning of devices at the customer edge and provider edge to enable the site to become a member of an MPLS VPN group.

Confidentiality	Provides data privacy through a flexible suite of encryption and tunneling mechanisms at the IP network layer.	Separates traffic between customers, offering security in a manner similar to a trusted frame relay or ATM network environment.
QoS and SLA	IPSec protocol does not address network reliability or QoS mechanisms.	Provides scalable, robust QoS mechanism and traffic engineering capabilities, enabling service providers to offer IP-based value-added services with guaranteed SLA compliance.
Authentication	Each IPSec session must be authenticated via digital certificate or pre shared key. Packets that do not conform to the security policy are dropped.	VPN membership is determined via a provisioning function based on logical port and unique RD. Unauthorized accesses to a VPN group is denied by device configuration.
Transparency	It resides at the network layer and transparent to the applications.	MPLS VPN operates at the IP+ATM or IP environment. It is completely transparent to the applications

ISP may choose IPSec for traffic that needs strong authentication and confidentiality and choose MPLS VPN for its broader connectivity and lower costs compared with traditional layer 2 private data networking.

2.3.4 MPLS VPN Terminology

The following section discusses briefly some of the new terminologies under the MPLS VPN architecture.

2.3.4.1 Virtual Router

A virtual router is a collection of threads, either static or dynamic in a routing device, that provides routing and forwarding services much like physical routers. A virtual router has to provide the illusion that a dedicated router is available to satisfy the needs of the networks to

which it is connected. A virtual router, like its physical counterpart, is an element in a routing domain. Normally under the MPLS VPN, the Provider Edge routers act like a virtual router [22].

A virtual router has two main functions. The first function is to construct routing tables that describing the paths between VPN sites using any routing technologies like OSPF, BGP or RIP. The second main function is to forward packets to the next hops within the VPN domain. Each virtual router participating in a single VPN domain is responsible for learning and disseminating VPN.

2.3.4.2 Virtual Routing and Forwarding (VRF)

The VPN routing and forwarding table (VRF) is a key element in the MPLS VPN technology. A VRF is a routing table instance and contains routes that should be available to a particular set of sites. The following are some of the VRF elements:

- IP routing table.
- A forwarding table that is derived from the routing table and is based on the Cisco Express Forwarding (CEF) technology.
- A set of interfaces that use to derived forwarding table.
- A set of rules that control the import and export of routes from and into the VPN routing table.
- A set of routing protocols and routing peers that inject information into the VRF.

Each PE maintains one or more VRFs. A VPN can contain one or more VRFs on a PE. When a particular packet arrived directly through an interface that is associated with that VRF, the VRF would perform a look up on the particular packet's IP destination address in the appropriate VRF [22].

2.3.4.3 Route Distinguishers (RD)

Route distinguishers (RDs) are 64 bits prefix that appended to the IP address within a VPN to make them unique. Normally a RD contains the ISP Autonomous System number and a

unique value. It is configured at the PE that connecting to a site. The purpose of the RD is to distinguish the duplicate private address and prevent overlapping. Prefixes should use the same RD when associated with the same set of route targets (RTs) and anything else that is used to select routing policy. For the RD, every CE that has the same overall role should use a VRF with the same name, same RD and same RT values. The RDs and RTs are only for route exchange between the PEs running MP-iBGP.

2.3.4.4 Route Target (RT)

The route target is the closer approximation to a VPN identifier in the MPLS VPN architecture. It is a 64-bit quantity. Every VPN route is tagged with one or more route targets when it is exported from a VRF. There are two important attributes for route target. By using the route target extended MP-BGP communities, MPLS VPN can control the distribution of VPN routing information. The second attribute of RT is based on filtering. With the introduction of route target based control of VPN-IPV4 prefixes serviced by a route reflector, it is possible to limit the number of prefixes that the route reflector has to manage [22].

2.3.5 MPLS VPN Network Architecture

Figure 2.8 shows the MPLS VPN network architecture. At the edges of the network are CE routers. CE routers are part of the customer network and are not VPN aware. Each CE router connects to a PE router. PE routers are where most VPN-specific configuration and processing occur. PE routers receive routes from CE routers and transport them to other PE routers across a service-provider MPLS backbone.

Each PE maintains a separate routing tables which is the VRFs. The VRFs contain the routes for directly connected VPN sites only. VPN information is required only at PE routers and it can be partitioned between PE routers. PE routers need to know VPN routing information only for VPNs in which there are direct connections.

In the middle of the network are provider (P) routers or label switch routers (LSRs), which implement a pure layer 3 MPLS transport service. The P routers in the backbone are not VPN

aware. Thus, it provides much more scalability. P routers do not have to carry customer routes, preventing routing tables in P routers from becoming unmanageable.

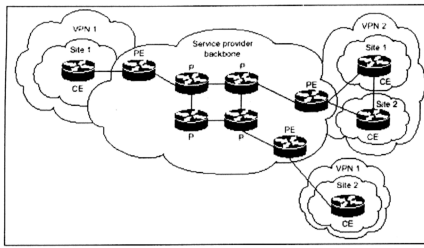

Figure 2.8 MPLS VPN Network

2.3.6 Characteristics of MPLS VPN

The following are some of the important characteristic for MPLS VPN:

- Each VPN needs a separate VPN routing and forwarding instance (VRF) in each PE router to ensure isolation and enable usage of uncoordinated private IP address.
- A route target is needed to identify the set of VPNs in which a VRF participates to support overlapping VPN topologies.
- VPN IP addresses are appended with 64-bits route distinguisher to make VPN addresses globally unique. The VPN IP addresses are exchanged between the PE routers through the MP-iBGP.
- Each PE router needs a unique router ID that is used to allocate a label and enable VPN packet forwarding across the backbone.
- Each PE-router allocates a unique label to each route in each VRF and propagates these labels together with the VPN IP addresses through MP-iBGP.
- Ingress PE-routers use a two level MPLS label stack to label the VPN packets with a VPN label assigned by the egress PE-router and an IGP label identifying the PE-router assigned

through the regular MPLS label distribution mechanisms. The label stack is appended to the VPN packet and the resulting MPLS packet is forwarded across the P-network.

2.3.7 MPLS VPN Security Consideration

ATM and frame relay have repudiation in the industry as being secure foundations for enterprise connectivity. Several key requirements need to be addressed for MPLS VPN in order to provide a secure network that equivalent to ATM and frame relay. The following sections discuss the requirement and how MPLS VPN achieved it.

2.3.7.1 Address and Routing Separation

Addressing separation implies that between two non-intersecting VPNs the address spaces between them are entirely independent [23]. This means that no two sites in the same VPN share the same address space. MPLS provides route separation by having each PE-Routers maintain a separate routing table for each connected VPN. This separation is maintained across the MPLS core to the other PE-Routers by utilizing MP-iBGP. By using the RD, MP-iBGP is able to identify different VPN routes through the core of the network. By using the features above, the routing across the MPLS network is separate per VPN. Thus, the attack inside a VPN will not affect the others VPN.

2.3.7.2 Security of Internal Structure

In order to secure an internal structure, the network topology inside the ISP must not reveal to the outside world. MPLS doesn't reveal additional unnecessary information to the customer VPNs. By using static routing, MPLS core can be kept completely hidden from the customer.

2.3.7.3 Resistance to Attacks

The network should be resistance to attacks. These attacks can be the denial of service, which cause the resources unavailable to authorized users. Besides that, the intrusions attacks is another common type of attacks that gain unauthorized access to the resources. There are

currently two possible ways to attack the MPLS core. The first attempt is to attack the PE-Router. The second method is to attack the signaling mechanism of MPLS.

The potential attack on PE-Router could be sending an extensive number of routes or to flood the PE-Router with routing updates [23]. In order to protect the PE-Router for being attack, the access control list can be implemented. This limits the point of attack to one routing protocol. Furthermore, the MD-5 authentication can be configured on the routing protocol.

The second type of attacks is to insert packets with wrong label into the MPLS network from the outside world. Thus, the PE-Router should never accept a packet with a label from a CE-Router. It should make sure that labels packet that arrives on any interface where label switching is not enabled would be dropped.

2.3.8 Strength of MPLS VPN

There are several benefits of MPLS VPN. MPLS VPN provides privacy and security equal to layer 2 VPNs by constraining the distribution of a VPN's route to only those routers that are members of that VPN and by using MPLS for forwarding.

MPLS VPN increases scalability with thousands of sites per VPN and hundreds of thousands of VPNs per ISP compared to the conventional VPNs that do not scale well. Furthermore, MPLS VPN eases the job of ISP in management of VPN membership as well as the deployment of new VPNs [20].

Besides that, MPLS VPN provides a platform for rapid development of additional value added IP services, including Extranet, Intranet, voice, multimedia and network commerce. MPLS VPN provides IP class of service, which support for multiple classes of service and priority within a VPN [20]. A well-executed MPLS-based VPN implementation will provide scalable, robust QoS mechanisms and traffic engineering capabilities, enabling ISP to offer IP-based, value-added services with guaranteed service-level agreement (SLA) compliance.

2.3.9 MPLS VPN Research

MPLS VPN is an active research topic in current situation. Basically, the two common researches on the MPLS VPN concern with the security issue on MPLS VPN and the QoS provided by the MPLS VPN. One recent research about the MPLS VPN is to study the architecture model for building VPN in a MPLS domain. The research describes the MPLS VPN scheme that must be accommodated with the existing network backbones and also provide for a full range of QoS characteristics [24].

Another research on MPLS VPN is to secure the MPLS payloads using the encryption and authentication method. It will use the IKE to establish the required security association for secure MPLS and definition of the encapsulation formats required for the encryption and authentication of MPLS payloads [25].

2.3.10 MPLS VPN Summary

As a summary, MPLS is the enabling technology that protects today's rapidly growing VPN revenue sources, while paving the way for tomorrow's value-added services portfolio. MPLS-enabled networks provide privacy on a network-by-network basis, much as Frame Relay or ATM provides it on a connection-by-connection.

2.4 Others Network Technologies

This section discusses some of the protocols related to the MPLS VPN. It includes the MP-iBGP, tag switching, OSPF and the CEF technology.

2.4.1 MP-iBGP

Border Gateway Protocol (BGP) is a protocol for exchanging routing information between routers in a network of autonomous system. BGP is often the protocol used between gateway hosts on the Internet. Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated routing table information only when one host has detected a change. The routing table contains a list of known routers, the addresses they can reach, and a cost

metric associated with the path to each router so that the best available route is chosen. BGP communicates with autonomous or local networks using internal BGP since it doesn't work well with IGP. The routers inside the autonomous network thus maintain two routing tables: one is for the interior gateway protocol and one is for internal BGP [26].

MP-iBGP is an extension of the existing BGP-4 protocol to advertise customer VPN routes between PE routers that learned from connected CE routers. All BGP sessions are internal BGP sessions because the sessions are between two routers that belong to the same autonomous system. MP-iBGP is the protocol of choice to advertise customer VPN routes across the MPLS VPN backbone due to the following advantages:

- MP-iBGP is able to carry optional parameter without extensively changing the protocol while normal IGP is unable to carry extra parameters. Under the MPLS VPN architecture, MP-iBGP update contains a VPN-IPv4 address, standard BGP communities, MPLS label information and extended BGP communities which include route target and site of origin [26]. These parameters are required to the BGP protocol so that VPN information can remain unique within the MPLS VPN backbone. Besides that, BGP speakers can identify routing updates that do not carry standard IPv4 prefix information.
- MP-iBGP is able to carry the VPN-IPv4 address that can treat the same prefix from two separate VPNs as non-comparable routes. This fulfill one of the requirements of the MPLS VPN architecture, in which, all customer routes must be unique within the backbone but not restrict the use of private IP addresses. VPN-IPv4 address is needed because MP-iBGP on its own cannot work correctly if customers use the same address space.
- MP-iBGP has the capability of handling a large number of routes. Thus, it is able to provide scalability.
- BGP communicates with autonomous or local networks using internal BGP since it doesn't work well with IGP.

A more detailed look at the configuration of MP-iBGP can be found in chapter four.

2.4.2 Tag Switching

Tag switching is aimed at resolving many of the challenges facing an evolving Internet and high-speed data communications in general. Tag-switching forwarding paradigm is based on label swapping. Basically, tag switching relies on two principal components, which are the forwarding component and the control component [27].

The forwarding component uses the tag information carried by packets and the tag-forwarding information maintained by a tag switch to perform packet forwarding. The control component is responsible for maintaining correct tag-forwarding information among a group of interconnected tag switches.

2.4.3 OSPF

Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks. As the Routing Information Protocol (RIP) was increasingly unable to serve large, heterogeneous internetworks, the design of an IGP based on the shortest path first (SPF) algorithm for use in the Internet is created.

Basically, OSPF has two primary characteristics. The first is that the protocol is open, which means that its specification is in the public domain. The second principal characteristic is that OSPF is based on the SPF algorithm, which sometimes is referred to as the Dijkstra algorithm. OSPF is a link-state routing protocol that calls for the sending of link-state advertisements (LSAs) to all other routers within the same hierarchical area. Information on attached interfaces, metrics used and other variables is included in OSPF LSAs [28].

As OSPF routers accumulate link-state information, the routers use the SPF algorithm to calculate the shortest path to each node. As a link-state routing protocol, OSPF contrasts with RIP and IGRP, which are distance-vector routing protocols. Routers running the distance-vector algorithm send all or a portion of their routing tables in routing-update messages to their neighbors.

2.4.4 CEF

Cisco Express Forwarding (CEF) is advanced layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet. CEF offers some benefits, which includes scalability and improved performance. CEF also offers unprecedented level of switching consistency and stability in large dynamic networks. CEF can switch traffic more efficiently than typical demand caching schemes because the FIB lookup table contains all known routes that exist in the routing table.

2.5 Chapter Summary

This chapter has provided a detail description of the current networking technologies such as MPLS, VPN, MPLS VPN MP-iBGP, OSPF and CEF. The review includes the basic architectures, their characteristics, and comparison with other types of technologies as well as the strength of each of the technologies.

The following chapter will discuss the network simulator. It will include the review of various types of network simulators available and the simulation models. Besides that, the next chapter also covers the programming approach that is used to develop the MPLS VPN simulator.