Designing a High Level Corporate Network Infrastructure with MPLS Cloud

G.V. Eswara Rao[1], Kambam Priyanka[2]

[1]Asst.Professor, Dept of Computer Science Engineering, ANITS, Andhra Pradesh, India
[2]Student, Dept of Computer Science Engineering, ANITS, Andhra Pradesh, India

---

Abstract - Network security could even be a broad set of performance enhancement towards an efficient organisation. A corporation which has its branch offices in various regions across the world got to provide a secure way for transmission of knowledge or other private information. So in these regions a cloud based solution of using MPLS results in a secure, faster and reliable transfer of data through the branch offices. This network setup is achieved by implementing OSPF protocol as interior gateway protocol and BGP because the surface gateway protocol for transferring information from branch office to headquarters and thus the opposite way around.

***Key Words*: Network security, Multi Protocol Label Switching cloud, Open Shortest Path First protocol, Border Gateway protocol[4], Redistribution mechanism[5], L3 switching[6], Redundancy protocol[7].**

INTRODUCTION

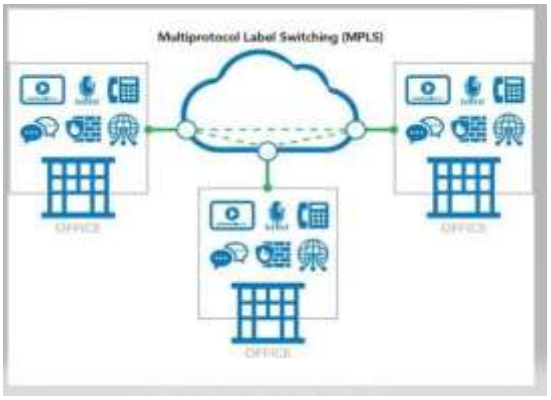
This cloud based solution is an inclusion of interior and exterior gateway protocols that connect the organization through a MPLS cloud. The variety of emerging applications cannot ensure high speed data transmission and bandwidth. In order to sustain the exponential growth of users and to deliver high volume of traffic is provided through cloud based storage solutions which have less physical devices connected and more cloud space store and transmit data to other branch officers of a main organization.

1. Related Work

The network setup of a corporation is complex and heavily susceptible to security attacks. so on safeguard the private data and tip within the branch offices of a corporation the transmission undergoes data loss and undergoes malicious activities so so on one's guard the info while transmitting from headquarters to branch offices that are located in various regions a cloud based technology could even be a much better solution for securing data integrity. Although the routing protocols are techniques like BGP, OSPF, RIP and other reliable protocols are implemented to avoid any security threat towards the organization's private information. Maintaining an outsized scale hardware devices would eventually cause a faulty occurrence so using cloud services the appliance has less hardware tools which decreases the upkeep of the general devices. During this paper we've discussed some methodologies which guarantee a secure network for a corporation. A corporation has its branch offices located at various regions across the world. The branches and thus the headquarters are becoming to be connected through the MPLS cloud and internally in each office the systems are connected through routers and implement L3 switching technique for faster means of knowledge transmission. Internal routing protocol is completed by OSPF while the external routing is completed using BGP. A redundancy routing protocol is maintained that acts as a backup router just in case of a router failure. The MPLS cloud leads to a faster, efficient and a secure network setup for the organization.

2. Overview of MPLS

MPLS stands for Multi Protocol Label Switching which plays a major role in packet forwarding switching and routing. It is a technology that enhances the capabilities of large scale IP networks and increases the Speed of forwarding routers.



2 .1 Basic Concepts of MPLS

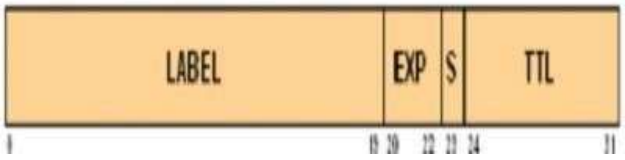
2.1.1 Forwarding Equivalence Class

The forwarding of packets is predicated on classification. The MPLS classifies the packets into categories supported their source address, destination address, protocol type ,VPN source port, destination port or any of those combinations are grouped together. The category which has an equivalent forwarding mode is named Forwarding Equivalence Class(FEC).

2.1.2 Labels

The MPLS label may be a fixed length 32 field. The label has no information about the topology.

- 20bit label(number)
- 3 bit experimental field which carries the IP precedence
- 1 bit stack field which indicated whether it is the last label or not
- 8 bit Time To Live(TTL)



2. 2 Working of MPLS

In a traditional Internet Protocol forwarding the packets are forwarded supported destination address only which needs full routing information for each hop. MPLS may be a label based packet forwarding mechanism and routing of packets is completed by their packet labels. Since every packet features a unique label attached there'll not be a requirement to see the packet details after every hop which is completed during a traditional approach. For the aim of utilizing the capabilities of an MPLs enabled IP network the sting routers must perform routing lookup and therefore the internal routers must switch packets and swap labels supported their label lookups.

2.3 System Architecture

MPLS is a combination of layer 2 and layer 3 functionalities of switching and routing. There are 2 main components in MPLS. They are - control plane and data plane.

Control Plane: This exchanges the routing information of layer 3 and labels.

Data Plane: This has a simple forwarding engine.

2.4 Lable Switching Router(LSR)

The basic element of MPLS network is LSR. it's made from a forwarding plane and an impact plane. The exchange of routing information is completed by the control field while the forwarding of packets is completed by the forwarding plane. the sting router will receive the packet, examine its FEC and add a label to the packet. The transit LSR forwards the packet consistent with its label.

2.5 Why MPLS

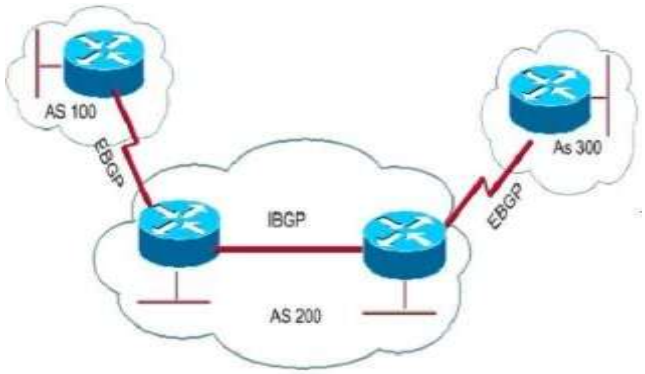
The benefits of using MPLS within the network setup is to provide- Scalability, performance, better bandwidth utilization, reduced network congestion. Since it uses a virtual private network it's considered as a secure transport mode. it's not susceptible to denial of service attacks which could affect the pure IP based networks

3. Overview of BGP

Border Gateway Protocol(BGP) could also be a typical exterior protocol designed to exchange the routing and reachability information of the destination node between multiple ISP networks called Autonomous Systems(AS) over the online. It is path vector protocol and sometimes also referred to as distance vector routing protocol. It makes the routing decisions supported paths, network policies and configured rules set by the network administrator.

3.1 How BGP Works

To transfer the routing information between the neighbouring ISP's BGP requires peering agreements which incorporates the terms and conditions for exchanging traffic. The design of BGP and its working is concentrated on security and scalability so it's harder to configure than other routing protocols. The BGP routers would have to generate a default route into the interior routing protocol to draw in the traffic for internet destinations unknown to other routers in the network.



3.2 WHY BGP

It is a standard protocol for internet routing and is required by many Internet Service Providers(ISP) to route between one another. Very large private IP uses BGP as internal routing protocol when OSPF cannot scale to the required size. Also BGP is multihoming a network for better redundancy and scalability.

3.3 Selection of a route by a router

A BGP router has several routes to succeed in a destination. Generally, the router chooses a route with minimum path length. But following attribute policies the BGP decision process consists of an ordered list of attributes. The router compares each attribute and therefore the route is chosen which has the foremost desirable attribute, otherwise it moves on to see subsequent attribute within the list.

3.4 Use of BGP

I. Highly efficient

II. Implemented on an outsized scale

III. Suitable for ISPs

IV. Prevents loops when there are multiple physical links

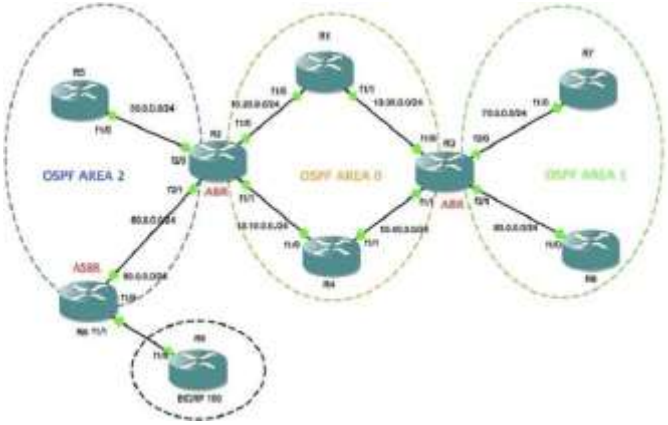
V. Load balances over redundant links

4. What is OSPF

Open Shortest Path First(OSPF) is an internal routing protocol which is link sate routing and operates on a single system within a single Autonomous System. It uses a simple hello protocol to keep the updates about the neighbouring routers by sending the hello packets for every 10 seconds. If the packet is not seen within the dead time then the source router assumes that the neighbor router is dead and status is sent to the neighbor routers OSPF uses a default distance as 110 for prioritizing the routing protocol which is implemented in the network. OSPF is mainly used to provide scalability in the network. The detailed information is kept locally by a communication mechanism called Link Area Advertisement and the summary information is sent to all the ramining routers available in the network.

4.1 OSPF Areas

Areas in OSPF are collections of routers that are grouped together. These are used as administrative boundaries in a network. The important area in OSPF is the backbone area which is known as area 0. It is the area where all the other areas must traverse to get to the other OSPF areas. While OSPF routers within an area know about the network topology ,that information is hidden at area borders.



4.2 How does OSPF work

When configured, OSPF will hear its neighbours and gathers all link state data available to make a topology map of the available paths within the network**.** Using this gathered information it will calculate the best shortest path to each reachable network or subnet using Djikstra's algorithm.This will construct three tables to store the information:

I. Neighbour table- Contains all the discovered neighbours with whom routing information are going to be interchanged.

II. Topology table- Contains the whole map of the network with all the OSPF routers and calculated best and alternative paths.

III. Routing table- Contains the present working best paths which will be wont to forward data traffic between neighbours.

4.3 Benefits of OSPF I. No hop count limitation II. Faster convergence III. Best path selection IV. Provides a loop free topology

5. Virtual LAN

VLANs are virtual local area network devices that appear to be on the same LAN. They are implemented to achieve scalability, security and ease of network management. They remove latency in the network and increases the network's efficiency. In addition VLANs are implemented to provide segmentation and clear issues related to security,

network management and scalability. Traffic within the network can also be controlled by using VLANs,It is a broadcast domain partitioned at data link layer. About 4096 VLANs can be crerated where default is th VLAN 1.

6. L3-Switching

A L3 switch also referred as multilayer switch combines the functionalities of a switch and a router. It reduces the latency as a packet are often routed without making extra network hops to a router. A layer 3 switch takes the routing decision itself, i.e. the packet is routed to a different subnet and switched to the destination network port simultaneously. Layer3 switches also can perform:

- Determining the paths using logical addressing
- Process and answer optimal information
- Update the simple network management protocol(SNMP) managers with management information base(MIB) information

Benefits

- High performance packet switching
- High speed scalability
- Low latency
- Quality of service

7. FHRP

A First Hop Redundancy Protocol is employed to protect the default gateway by allowing two or more routers to supply backup for that address. If any failure occurs in a lively router, the backup router takes over the address within a couple of seconds. This provides data security and there's no loss within the data that's being transmitted.

7.1HSRP

In this system a Hot Standby Router Protocol(HSRP) is employed as a backup mechanism protocol for the failed router address. In this protocol the first router with the very best configures priority router fails then subsequent highest priority router would take over the gateway IP address and respond with an equivalent MAC address because the primary router, thus achieving transparent default gateway failover caused by routers and switches.

Conclusion

Network security is one of the foremost important aspects to believe when working over the online LAN or other methods. It is an activity taken by any organization to prevent malicious use or accidental damage to a company's privatr data, its users or their devices. The goal of this system is to provide a security mechanism to the organization's tip or private data without getting lost or attacked by malicious activities, thus providing a stable and safer way of data transmission over a widely spread branch offices of a main centralized oraganisation.

References

[1] Optimal Performace Analysis Enabling OSPF and BGP in internal and external WAN by K.RamKumar, S.Raj Anand

[2] BGP routing policies in ISP networks by Matthew Caesar UC Berkeley Jennifier Rexford Princeton University

[3] Internet Protocol/Multi Protocol Label Switching networks by Sajid Hussain, Muhammad Tariq Javed.