IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004099

Inter Autonomous System MPLS VPN

Anjitha KB[1]

Assistant Professor, Department of Electronics & Communication Engineering, Akshaya College of Engineering, Kinathu Kadavu, Coimbatore, Tamilnadu, India[1]

ABSTRACT: One of the major difficulties associated with communication is that problems in interconnecting the branches of any corporate office which are the part of diffffferent autonomous system.
The objective of this project is to design an INTER AUTONOMOUS SYSTEM MPLS VPN along with dedicated traffic tunneling for each Virtual Private Network VPN) with the help of Open Shortest Path First(OSPF) and Multiprotocol Border Gateway Protocol(MP-BGP). It helps in keeping the customers isolated, network manageable and reliable. . Also the Virtual Routing and Forwarding (VRF) feature in Virtual Private Network allows the customers to even use the same Internet Protocol(IP) addresses. Proposed system extends the Multi Protocol Label Switching Virtual Private Network services across the geographical boundaries. It enable the communication between networks under different Autonomous System(AS)

KEYWORDS: Autonomous system, BGP, Internet Protocol, MPLS, OSPF, Routing, Virtual Private Network,

I. INTRODUCTION

There has been an exponential growth in the telecommunication sector throughout the world in the past few years, which has led to an incredibly huge amount of traffic being sent from one location to another with different requirements and choices of services. MPLS has proved to be a promising solution that provides different features in the same network of the service provider, thus replacing many transport technologies. The most significant of them is the concept of VPN which segregates the traffic according to the criteria set by the customers, making the connection secure and private. It can be used to establish private connections between different sites of the same customers that might be present at different locations. MPLS also has the capability of protecting its path in case of any failover. This helps the service provider to provide a guaranteed service to its customers. MPLS thus can provide
multiple services at the same instant in the same network. The proposed network connects customers from its headquarters to its various sites throughout the world, which is a part of different AS using a private connection enabled with traffic tunneling. These private communications are carried by MPLS VPN using features like RD and RT. MP-BGP is used to carry these large databases throughout the network along with Route Reflectors that will allow the IBGP neighbors to learn all the paths of the network. Every VPN is allotted a different tunnel path so that complete privacy and security can be achieved for every customer. Path protection mechanisms like FRR are used for faster recovery in case of a failure. Link and node protection is given to the links and nodes that carry higher importance in the network. All these features included in the MPLS network leads to an highly efficient network.

II. LITERATURE WORK

Branches of corporate offices are normally distributed geographically over the entire nation at least. Since it is the competitive world, they may require their own private, secured, faster and economical data network between corporate office and all branch offices. Construction of their data network is not economical and unwise,because it involves provision of individual paths in between their offices to ensure the safety and authentication. Virtual Private Network comes as the solution of the these problems. Virtual Private Network is Private Data Network, carved out from the Public Data Network. In this concept only switched paths (virtual paths) are assigned between the hosts. VPN can be constructed by using conventional IP network. But the users have to encounter with the defects in present IP backbone. Since MPLS adopts the connection oriented routing, VPN can be overlaid on MPLS architecture, by constructing Tunnels. Other users according to their FECs can share tunnels

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004099

III. BUILDING BLOCKS

A. Switching Layers

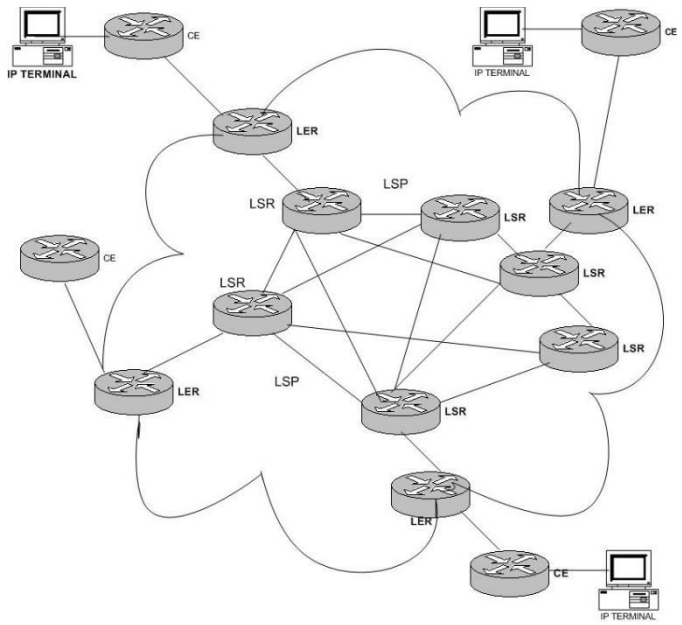
Switching is the process by which, two circuits are interconnected for exchanging information. Information is in the form of either analog or digital. In electro mechanical era, information was in the form of analog. Presently, information is in the form of digital. In order to interconnect the circuits, supporting the digitized information, suitable digital switches are designed. Digital Switches are classified as Circuit switch &Packet switch.

B. Network Layers

Network architectures define the standards and techniques for designing and building communication systems for computers and other devices. To reduce the design complexity, most of the networks are organized as a series of layers or levels, each one build upon one below it. The basic idea of a layered architecture is to divide the design into small pieces. Each layer adds to the services provided by the lower layers in such a manner that the highest layer is provided a full set of services to manage communications and run the applications. Two major classification includes ISO/OSI models & TCP/IP

IV. MPLS ARCHITECTURE

MPLS architecture is mainy consisting of CE, LER and LSR.



CE structures the customer message into IP Packets and sends to the entry node of MPLS domain. While receiving the IP Packets from the egress node of the MPLS domain, CE sends packets to Network layer of its own, after removing the IP address. Label Edge Routers are working as the gateways of MPLS Domain. Ingress LER, it receives the IP Packet from CE, assigns the appropriate Label.Label Switched Routers are basically working as transit switches in MPLS cloud. It receives Labeled IP packets through the appropriate LSP. It analyses the Label bound over the packet, consults the forwarding information table (LIB) and routes the packet through the appropriately mapped out going LSP. OSPF is the routing protocol, that multicasts the change in routing table of a host to all other hosts with in the boundary of Network. In MPLS Network, this protocol is used as Label Distribution Protocol between peers.This protocol is one among the IGP.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004099

V. VIRTUAL PRIVATE NETWORK

A virtual private network can be defined loosely as a network in which customer connectivity amongs the multiple sites is deployed on a shared infrastructure that utilizes the same security, management, and qos policies that are applied in a private network. VPN services can be offered based on two major paradigms:

A. Overlay VPNs

Whereby the service provider furnishes virtual point-to-point links between customer sites. The traditional approach for service providers has been to provide Tunnel based managed VPN service, by setting up secure, end-to-end connections, often emulating leased lines or virtual circuits, over public networks, according to the overlay model. A tunnel has two end points where the security service is both negotiated and rendered. Tunnels can exist at several protocol layers

B. Peer-to-Peer VPNs,

whereby the service provider participates in customer routing.The peer model is based on a Layer 3 connectionless architecture offffering the advantages of a highly scalable VPN solution in which some or all VPN capabilities are deployed within the service provider's network. A customer site is required to "peer" with only one router located at the service provider's POPs, as opposed to all other VPN terminators or customer routers in the same VPN. The most promising approach to peer model VPN is based on the MPLS technology that is rapidly emerging as a core technology for next generation networks, in particular optical networks. MPLS is essentially a hybrid routing and forwarding strategy, streamlining the backbone switching of IP packets between the network (Layer 3) and transport (Layer 2) mainly focused on improving Internet scalability through better Traffic Engineering practices and qos provisioning

VI. MPLS VPN

When creating a VPN using connection-oriented, point-to-point overlays, such as Frame Relay, or ATM virtual connections or tunneling-on-IP techniques, the VPNs key defificiency is scalability. MPLS-based VPNs, instead, are structured according to a pure peer model-based and connectionless architecture to leverage a highly scalable solution. First, according to the peer model, a customer site is required to peer only with one PE router as opposed to all other PE or CE routers that are members of the VPN, eliminating the proliferation of point-to-point customer terminated tunnels or Virtual Circuits. Furthermore, the other great advantage of MPLS VPNs is that they are inherently connectionless. The Internet owes its success to its basic technology, TCP/IP, built on a packet-based, connectionless network paradigm. This means that no prior action is necessary to establish communication between hosts, making it easy for two parties to communicate in a very effective and flexible way. To establish privacy in a connectionless IP environment, classic tunnel-based VPN solutions impose an often complex negotiation/setup procedure on a connection oriented, point-to-point overlay created on the network. Thus, even if it runs over a connectionless network, a classic VPN cannot take advantage of the ease of connectivity and service flflexibility available in connectionless networks. MPLS VPN security is accomplished by using a data plane and control plane approach. The data plane protects against a packet from within a MPLS VPN from traveling outside of its VPN boundaries and from packets from outside a MPLS VPN traveling into the boundaries of a MPLS VPN. The service provider will ensure that routers will drop packets that do not belong to MPLS VPN by examining the label of the packet. Control plane security ensures that non trusted peers cannot inject routes into the MPLS VPN. This is accomplished by the use of the MD5 authentication feature of BGP. Control plane security will also ensure that physical security of the routers is maintained to eliminate unauthorized access

A. MPLS VPN ROUTING

PE VPN routing and forwarding tables need to be populated with the correct routing information for the attached VPNs. This routing topology data must be isolated for individual VRFs and cannot be allowed to leak into other VRFs. This separation is accomplished by adding an identififier known as a route distinguisher to traditional IP route advertisements. Route distinguishers are 8-byte blocks that are placed in front of an IPv4 network route advertisement. All VRFs must have unique route distinguishers. The route distinguisher is the mechanism that facilitates the use of overlapping customer IP address spaces; it associates each of these addresses with the correct VRF. Routing updates are accomplished via an extension of the BGP. All PE routers communicate with each other via IBPG with

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004099

Multiprotocol extensions. BGP updates are always based on the import and export routing policies confifigured within each individual router

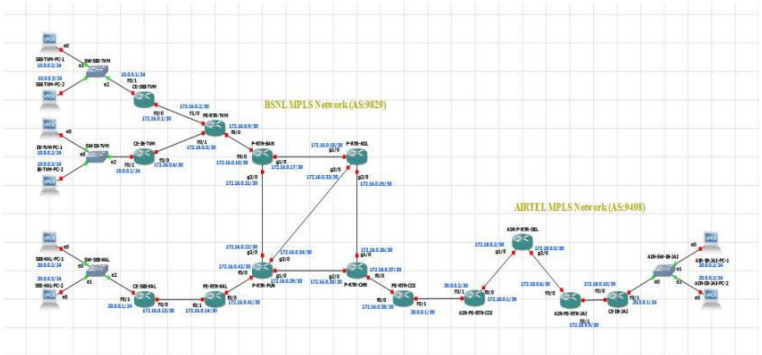
VII. INTER AUTONOMOUS SYSTEM MPLS VPN

The proposed work includes the designing of an inter as system by utilising the features of mpls VPN with mpbgp. The MPLS VPN architecture provides service providers with a peer-to-peer model that combines the best features of overlay and peer-to-peer models. Before introducing the Inter-Autonomous System MPLS VPN feature, customer sites had to be connected to a single service provider AS. This feature allows a VPN to cross more than one service provider backbone.It enables VPN sites to be connected across multiple service providers using diffffferent AS numbers and makes confederations possible within a service provider backbone.This optimizes iBGP meshing.In a normal MPLS VPN scenario, the CE routers are connected to the PE routers in the same AS. The PE routers exchange VPN routes by using multiprotocol iBGP. This carries the 96-bit VPN version 4 (VPNv4) addresses along with route targets and the associated VPN label

In the Inter-AS MPLS VPN feature, the CE routers are connected to PE routers in a diffffferent AS. The PE routers exchange VPN routes with the ASBR in the same AS using multiprotocol iBGP. The ASBR of the diffffferent AS exchange VPN routes using multiprotocol eBGP. For MPLS VPN to work properly, the VPN label must be allocated by the router. This router is indicated by the next-hop attribute of a route. In BGP, the next-hop attribute of a prefifix is changed by a router when it advertises to a neighbor using eBGP. In the Inter-AS MPLS VPN feature, the next-hop address of a VPN route is changed by the AS border router. This occurs when the VPNv4 address is advertised to the border router of the neighboring AS. This is done through multiprotocol eBGP, along with a new label for the route. The ASBR binds the new label with the label received for the same route. This is done from the PE router that originally advertised the prefifix using multiprotocol iBGP and is called LSP stitching. When the ASBR receives MPLS packets with the specially assigned label, it forwards the packets into the LSP that reaches the fifinal destination. LSP stitching is used in MPLS VPN whenever the BGP next-hop attribute is changed. LSP stitching is done even when next-hop-self is configured for multiprotocol iBGP sessions. The Inter-AS MPLS VPN feature can also be used to divide an individual AS into a multiple sub-AS by using confederations to overcome iBGP full mesh requirements.

VIII. PROPOSED TOPOLOGY

The proposed system shown in fifig2.9 consists of a MPLS VPN network which are geographically seperated. There is a BSNL MPLS network and an AIRTEL MPLS network. The customers CE-SBI-TVM and CE-IB-TVM are connected to the BSNL AS(PE-RTR-TVM). Similarly the customer CE-SBI-KAL connected to the PE-RTR-KAL of BSNL AS. In the AIRTEL AS the CE-IB-JAI is connected to the AIR-PE-RTR-JAI of AIRTEL AS. Both the service provider uses the eBGP protocol at their ASBR. IBGP is used within the BSNL AS and AIRTEL AS. The VPN information that is passed between the two ASBRs(BSNL ASBR and AIRTEL ASBR). All the routers are provided with the OSPF and MPLS services. The VRF services also provided to the PE routers. The proposed system provides communication between diffffferent Autonomous Systems.



| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004099

IX. CONCLUSION

In today's economy where the most important objective for an engineer is to implement the new emerging technologies for transferring the data securely and in a cost effffective manner. Within the autonomous system of a service provider each and every router will configured by protocol OSPF. Because internally OSPF should run inside the network for transmission of the exterior gate way protocol like e-BGP. So we can say that BGP Share the information to other autonomous system with the help of OSPF only. This venture of new technology MPLS over the existing technology VPN provides benefits that service providers need urgently in their networks, such as scalability, manageability and security. By introducing this approach we can communicate with the client who are located in different geographical conditions and with the different Internet service providers.

REFERENCES

[1] Snehal Yadav and Amutha Jeyakumar "Design of Traffiffiffic Engineered MPLS VPN for Protected Traffic using GNS Simulator", Department of Electrical Engineering Veermata Jijabai Technological Institute, IEEE 2016.
[2] Francesco Palmieri, "Evaluating MPLS against traditional approaches", Eighth IEEE Symposium on Computers and Communications (ISCC'03), June 30, 2003.
[3]"COMPUTERNETWORKS"(http://www.studytonight.com/computer networks/tcp ip-reference-model).
[4] K. Hamzeh, G. Singh Pall, W. Verthein, J. Taarud, W.A. Little: Point-to-Point Tunneling Protocol PPTP, IETF draft: draft-ietf-pppext-pptp-02.txt.
[5]"MULTI PROTOCOL LABEL SWITCHING"(http://www.ietf.org/html.charters/mplscharter.html).
[6]D. Haskin, R.Krishnan A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute draft haskinmpls-fast-reroute-05.txt ,November 2000.
[7] S. Hanks, T. Li, D. Farinacci, P. Traina: Generic Routing Encapsulation over IPv4 networks, RFC1702, 1994.
[8]"TYPES OF ROUTING" (http://www.freeccnastudyguide.com/studt-guides/ccna/routing).
[9] M. P. Minei, I., Scalability considerations in bgp/mpls ip vpns, IEEE Communications Magazine, vol. 45, pp. 26 31, 2007.
[10] Dr. Hosein F. Badran, "Service Provider Networking Infrastructures with MPLS" in Sixth IEEE Symposium on Computers and Communications (ISCC'01) July 05, 2001.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details