IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 3, March 2019

Implementation of Inter Provider MPLS-VPN using Back to Back VRF Method

Sakila.P[1], Rashika.R[2]

Assistant Professor, Department of Computer Science,

Ponnaiyah Ramajayam Institute of Science and Technology PRIST University, Thanjavur[1]

M.C.A., Scholar Department of Computer Science,

Ponnaiyah Ramajayam Institute of Science and Technology PRIST University, Thanjavur[2]

Abstract: MPLS technology is being widely adopted by service providers worldwide to implement VPNs to connect geographically separated customer sites i.e., Inter-provider VPN network. In this project we first briefly describe VPNs which are behind the scope of secure private MPLS connections such as several VPN deployments emerged from the sudden growth of requirements. We then discuss about the requirements of interconnections from customer end to service provider in one's perspective. We then propose and discuss the methods used for deployment options from service providers point of view. The usage of peer-to-peer model had overcome the drawbacks of the Overlay model and paved way for optimal data transport via the Service Provider backbone. Hence, the Service Providers would actively participate in customer Layer 3 routing. Customer Layer 3 routing information is carried between routers in the provider network and customer network. Layer 3 VPNs implemented on MPLS backbone of service providers are referred as "MPLS L3 VPNs" In this paper we present a novel method of communication among branches or partner branches of an organization each of them situated at distinct geographical areas with absence of the same ISP in every area. We came up with an idea of designing an Inter-provider network i.e., connecting multiple ISPs with the private network mechanism which provides global reach ability. It deals with the security issues confidently and provides the replacement of Internet in Private/Public organization

Keywords: Multi Protocol Label switching (MPLS), Digital Subscriber Line (DSL), Virtual Private Network (VPN)

I. INTRODUCTION

A Company with 1 main site and 10 remote sites could lease several different types of WAN services to connect these sites such as leased lines, frame relay or more likely today Multi Protocol Label Switching (MPLS). However, another option for connecting remote sites is simply to connect each site to the internet through some high-speed internet access technology like cable or Digital Subscriber Line (DSL). Consequently, the sites can send IP packets to each other over the Internet, using the Internet as a WAN. Unfortunately, Internet is not nearly as secure as leased lines and other WAN options As the Internet uses the public IP based communication system, it is facing more security issues though an adequate amount of security services were deployed. Our proposed Inter-AS or Inter-Provider VPN feature involves private IP based communication system. It provides seamless advantages to the customers with connection as well as the (QoS) Quality of Services with the MPLS technology in corporate So far there are many ISPs providing MPLS VPN network connections, VPN only connections, Internet based MPLS connections based on layers i.e., L2 VPNs & L3 VPNs. Also, the Inter-Provider connection (Multiple ISPs) through Internet based VPNs using MPLS in the background which are in exercise currently. This project's main theme is that we can incorporate the different ISPs to implement connection over customer sites with private IP address scheme by the agreement of each provider.

II. LITERATURE REVIEW

This paper presents the literature survey on MPLS, MPLS VPN, and Inter-AS MPLS VPN networks in the following sections. Extensive research has been done to test the performance of MPLS VPN, single AS and multi-AS, with respect to MPLS as a transport technology as well as a QOS solution for complex network design requirements. However, much less research has been done on the impact of the three- Inter-AS implementations on the end toend delay when QOS is applied to the routers in the path. Delay is the most important factor to most applications as it can have an unavoidable impact on the performance. No research has been done to evaluate the three implementations with respect to the end-to-end delay and for that an analytical model in proposed which shows the different delays that occur on every hop on the path and their impact on the end-to-end delay. The result are similar and have the least delay. The results from the test-bed show a similar result to back the proposed analytical model. Hachimietal [2] studied the

performance of single-domain MPLS VPN with QOS techniques with regard to utilizing the interface queues in routers when traffic conforms or exceeds the specified thresholds. The authors proposed a scheme of sharing the interface queue between two sub-queues for different VRFs so that these queues utilize the unused buffer space of the interface queue when one queue's buffer is getting filled. They used a two-stage scheduler, one for each VPN, before the main interface scheduler. A sub-scheduler can dynamically mark the out-of-contract traffic or bandwidth in such a way that guarantees forwarding packets and not dropping them or remarking them with the least treatment which can cause high jitter. However, the impact of proposed scheme on delay was not studied. implementation Back-to-Back VRFs. Hachimietal. [2] and Ming-hu [3] research showed that OPNET is the most suitable simulation software for MPLS VPN [3]. Several analytical models have been proposed to evaluate the performance of traditional, single-domain, MPLS VPN with regard to Differentiated Service Integrated Service QOS, Traffic Engineering (TE), and TE re-route, using network simulators e.g. NS-2, OPNET, etc. Xia et al. [4] concludes that MPLS VPN does synthesize the traditional IP and ATM VPN implementations and does offer great scalability over traditional IP or ATM VPNs. Khan et al. [6] focused on using MPLS VPN as a Wide Area Network (WAN) technology with a full support of QOS. Their analysis showed that implementing MPLS VPN with Diff Serv showed a better performance over IP and MPLS without DiffServ .Using a real test bed consisting of Cisco Routers, results showed that end-to-end delay, jitter, and packet loss in different packet transmission rates and in different traffic types had very low variations or was almost constant. The NS-2 simulations done by showed that delay and packet loss improved after applying MPLS over a traditional IP network.

III. EXISTING SYSTEM

VPN (VIRTUAL PRIVATE NETWORK)

Virtual means not real or in a different state of being. In a VPN, private communication between two or more devices is achieved through a public network, the Internet. Therefore, the communication is virtually but not physically there.

Private means to keep something a secret from the general public. Although those two devices are communicating with each other in a public environment, there is no third party who can interrupt this communication or receive any data that is exchanged between them.

Network consists of two or more devices that can freely and electronically communicate with each other via cables and wire. A VPN is a network. It can transmit information over long distances effectively and efficiently.

The term VPN has been associated in the past with such remote connectivity services as the (PSTN), Public Switched Telephone Network but VPN networks have finally started to be linked with IP-based data networking. Before IP based networking, corporations had expended considerable amounts of time and resources to set up complex private networks, now commonly called Intranets. These networks were installed using costly leased line services, Frame Relay, and ATM to incorporate remote users. For the smaller sites and mobile workers on the remote end, companies supplemented their networks with remote access servers or ISDN. Small to medium-sized companies, who could not afford dedicated leased lines, used low-speed switched services. As the Internet became more and more accessible and bandwidth capacities grew, companies began to put their Intranets onto the web and create, what are now known as Extranets to link internal and external users. However, as cost-effective and quick-to-deploy as the Internet is, there is one fundamental problem – security. Today's VPN solutions overcome the security factor using special tunneling protocols and complex encryption procedures, data integrity and privacy is achieved, and the new connection produces what seems to be a dedicated point-to point connection. And, because these operations occur over a public network, VPNs can cost significantly less to implement than privately owned or leased services. Although early VPNs required extensive expertise to implement, technology has matured to a level where deployment can be a simple and affordable solution for businesses of all sizes. Simply put, a VPN, Virtual Private Network, is defined as a network that uses public network paths but maintains the security and protection of private networks. For example, Delta Company has two locations, one in Los Angeles, CA (A) and Las Vegas, Nevada (B). In order for both locations to communicate efficiently, Delta Company has the choice to set up private lines between the two locations. Although private lines would restrict public access and extend the use of their bandwidth, it will cost Delta Company a great deal of money since they would have to purchase the communication lines per mile. The more viable option is to implement a VPN. Delta Company can hook their communication lines with a local ISP in both cities. The ISP would act as a middleman, connecting the two locations. This would create an affordable small area network for Delta Company.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 3, March 2019

IV. PROPOSED SYSTEM

Inter-Provider VPN Network

Several requirements have resulted from sudden growth in VPN deployments. One such requirement is that the VPNs need to reside on different Autonomous systems in different geographic areas or extend across multiple service providers. The MPLS-Inter AS feature plays an important role in making such a requirement as seamless as possible for the end customer. The MPLS Inter-AS feature allows an MPLS VPN to span service providers and autonomous systems.

Overview Of Inter-Provider VPNS

Traditional MPLS VPN networks contain customer or client VPN sites traversing a single MPLS VPN backbone. However, in a geographically dispersed network, client VPN sites might connect to different MPLS VPN backbones. Figure1 shows such a network where client sites belonging to VPN-A and VPN-B are connected to different service providers. In such cases, to enable continuity of VPN services across multiple service providers, the VPN information has to be mutually redistributed. The Inter-AS or Inter-provider VPN feature allows the VPN information to be redistributed between adjacent MPLS VPN entities so that client sites belonging to VPN-A and VPN-B that are dispersed across multiple service provider backbones can communicate with each other.

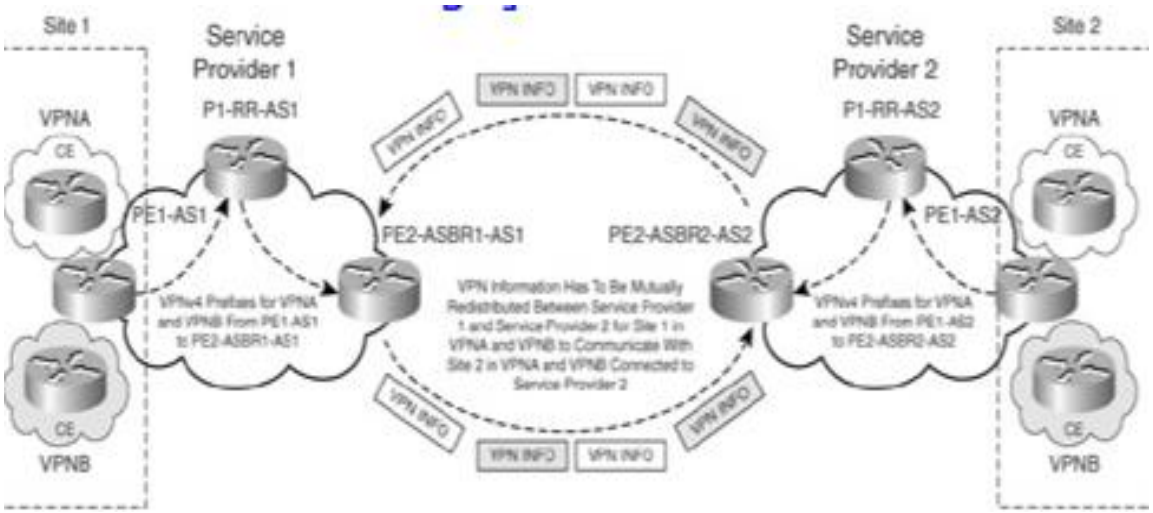


Figure2 shows the MPLS VPN network in which the edge routers PE2-ASBR1-AS1 and PE2-ASBR2-AS2 serve as Autonomous system Boundary Router (ASBR) routers. The ASBR Router PE2-AS1-AS1 is responsible for propagating Site 1 VPN information to Site 2 and PE2-ASBR2-AS2 propagates Site 2 VPN information to Site 1.

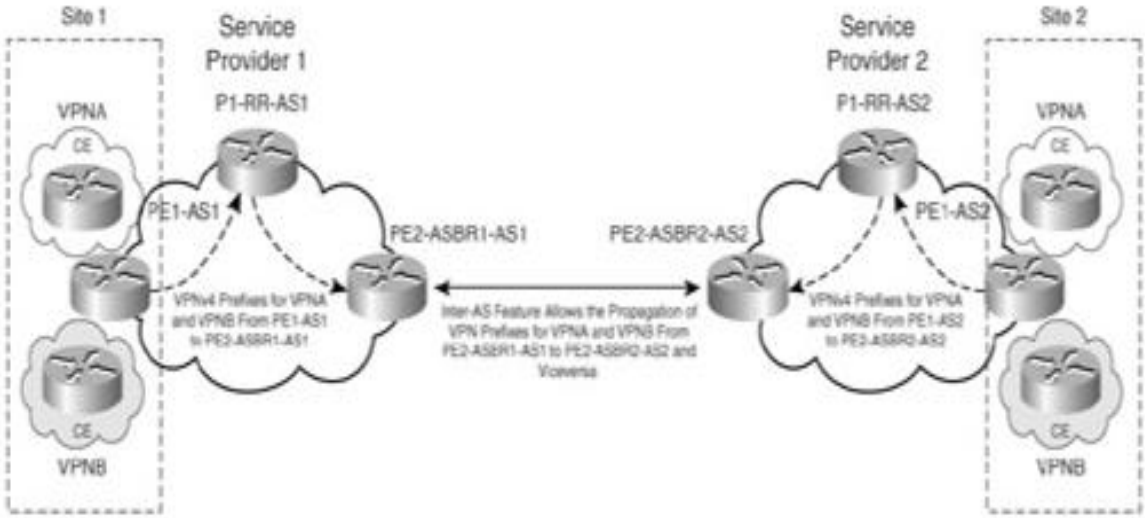


Figure2 : Inter-Provider VPN Network using Edge Routers as ASBRs

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 3, March 2019

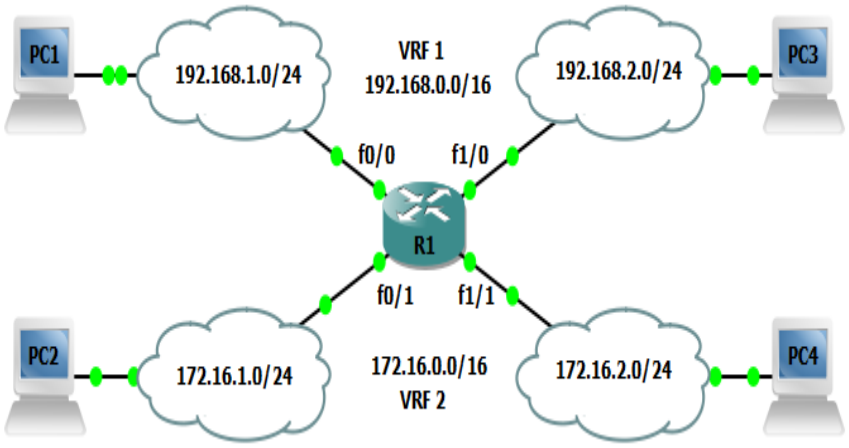
Inter-provider term itself indicates that connection is between multiple Internet Service Providers (ISPs).An Inter-provider VPN network is nothing but a network consisting multiple provider MPLS enabled VPNs. As the main aim of this project is designing a network using only private ip pool so as to make it more closed and secure resulting in no need of Internet at all. Traditional MPLS VPN networks contain customer or client VPN sites traversing a single MPLS VPN backbone. In such cases, to enable continuity of services across multiple service providers, the VPN information has to be mutually redistributed. The Inter-AS(Autonomous System) or Inter-provider VPN feature allows the VPN information to be redistributed between adjacent MPLS VPN entities so that client sites belonging to dispersed VPNs from multiple service providers can communicate to each other [4].

V. BACK-TO-BACK VRF METHOD

We considered a phenomenon in which the Inter-Provider Private (VPN) network should be built within two different ISPs, one is popular ISP from urban area and the other is local ISP from a remote area. Virtual Route Forwarding (VRF) method is the simplest method for allowing MPLS VPN providers to exchange VPN routing information for Customer End sites in different MPLS domains. In this method, the Provider Edge Border Routers present in different Autonomous systems act as ASBRs. These ASBRs are interconnected either by a single connection consisting of logical sub interfaces or multiple physical interfaces. VRFs are configured on ASBRs to collect VPN client routes. Each sub interface or interface connected between the ASBRs is dedicated to a single client VRF. The single client VRF can run EBGP RIPv2, EIGRP, OSPF or static routing to distribute the VPN routes to it's adjacent peer The use of EBGP is, however the most benefit able in Back-to-Back VRF method because EBGP scales best to this type of application, retaining the type of the route and offering better policy, scalability and security mechanisms. In this path the LSP paths in adjacent MPLS Autonomous systems are interconnected using the IP forwarding mechanism between the AS border routers [2]. This method amplifies the serviceability of MPLS VPN backbones; however it also introduces greater complexity because it requires dedicated VPN links between the adjacent ASBRs. Hence the next approach i.e., ASBR-ASBR is used to reduce complexity which works fine in this case. The VPN routing information that is passed between the two ASBR routers is in IPv4(version4) format [2].

Routers in the network with VRF configuration are configured with the following:

1) The provider edge routers on autonomous systems numbered as AS 65001 and AS 65002 are configured with MPLS using LDP protocol (Label Distribution protocol) and also designed with BGP(Border Gateway Protocol) configuration.
2) Route reflectors which are used by each ISP are updated with IP ranges using BGP protocol.
3) Border routers (ASBRs) are configured with VRF thereby using BGP protocol.



VI. CONCLUSION

As the proposed system brings the precinct of interconnection of ISP-ISP, it has the significance of private IP range. We are assigning the private IP addresses to all the cancelled routers and hosts toward the data. Although most of the companies in the countries work through Internet with their host computers access, it is formidable that their data is open to public. The risks associated with the Internet are advertised everyday by the trade and mainstream media. For corporations, the risks are even more and apparent. Stolen or deleted corporate data can adversely affect people's livelihoods, cost the company money. If it is a small company then it could put it out of business. Since the Internet is a public network you always risk having someone access any system you connect to it. So, this proposal of a private network comes with a complete non-exposure of public domain yields the ease of having no doubt about the protection

of information dealt between the inter-branches. More over this design of network also provides very low latency and thereby high speed performance since the overload caused by the exchange of overheads in the system of Internet is totally reduced and acts as a leased connection to the branches from the organization. This method also helps the providers/operators to enhance their revenue value if they form their own suitable agreements each other because of high probability of Internet services exhausts or becomes almost non-trustable in the future

REFERENCES

[1]. Wendell Odom, "Virtual Private Networks" in Cisco CCENT/CCNA ICND1 100-101, Cisco press, 2013, pp. 1130 - 1144.
[2]. Umesh Lakshman, Lancy Lobo -CCIE No. 4690, "Inter-provider VPNs" in MPLS Configuration on Cisco IOS Software, Cisco press, 2005, pp. 455 - 507.
[3]. Chris Hoffman. (2013,Jan 15). "What Is a VPN, Why would I need one?" [Online]. Available: https://www.howtogeek.com .
[4]. LuyuanFang, NabilBita et.al, "Inter provider IP MPLS services: Requirements, Implementations and Challenges", IEEE Communications Magazine, June. 2005.
[5]. Madhulika Bhandure et al., "Approach to build MPLS VPN using QOS capabilities", www.ijerd.com e-ISSN: 2278-067X, June 2013, Volume 7, Issue 8, pp. 26 - 32.
[6]. Tejender Singh Rawat et al., "A Review paper on MPLS VPN Architecture", www.ijetmas.com May 2015, Volume 3, Issue 5, ISSN 2349-4476.
[7]. Vassilis Foteinos et al., "Operator-Friendly Traffic Engineering in IP/MPLS Core networks", Vol.11 No.3, 1932-4537 © 2014 IEEE. Personal use is permitted, but redistribution requires IEEE permission,http://www.ieee.org/publications_standards/publications/rights/index.html form more information.