ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Implementation of Hub & Spoke Topologies for the MPLS VPN Customers with Customers Using EIGRP for Their Sites

Asik Rahman. M[1], Kalaiyarasan. S[2], Kashif Ahmed.T[3], and Dr. K. A. Dattatreya[4]

UG Scholar, Department of ECE, Adhiyamaan College of Engineering, Hosur, TN, India[1,2,3]

Associate Professor, Department of ECE, Adhiyamaan College of Engineering, Hosur, TN, India[4]

ABSTRACT: MPLS technology is being widely adopted by service providers worldwide to implement VPNs to connect geographically separated customer sites. VPNs were originally introduced to enable service providers to use common physical infrastructure to implement emulated point-to-point links between customer sites. A customer network implemented with any VPN technology would contain distinct regions under the customer's control called the customer sites connected to each other via the service provider network. The cost of implementation depended on the number of customer sites to be connected with these dedicated links. Frame Relay and ATM were the first technologies widely adopted to implement VPNs. As customer can use any routing protocol to send his networks information to ISP, this project deals with customer asking to interconnect their branches using EIGRP as PE-CE routing protocol as per the diagram shown below. Now the responsibility lies with service provider to route the traffic between their branches.

KEYWORDS: MPLS, VPN, EIGRP, HUB & SPOKE

I. INTRODUCTION

In traditional router based networks, different sites belonging to the same customer were connected to each other using dedicated point-to-point links. The cost of implementation depended on the number of customer sites to be connected with these dedicated links. A full mesh of connected sites would consequently imply an exponential increase in the cost associated. Frame Relay and ATM were the first technologies widely adopted to implement VPNs. These networks consisted of various devices, belonging to either the customer or the service provider, that were components of the VPN solution. Depending on the service provider's participation in customer routing, the VPN implementations can be classified broadly into one of the following Overlay model, Peer-to-peer model. The peer-to-peer model, consequently, does not require the creation of virtual circuits. Layer 3 VPNs implemented on MPLS backbone of service providers are referred as “MPLS L3 VPNs”.

II. WORKING PRINCIPLE

Overlay VPNs were initially implemented by the Service Provider by providing either Layer 1 (physical layer) connectivity or a Layer 2 transport circuit between customer sites. In the Layer 1 implementation, the Service Provider would provide physical layer connectivity between customer sites, and the customer was responsible for all other layers. In the Layer 2 implementation the Service Provider was responsible for transportation of Layer 2 frames (or cells) between customer sites, which was traditionally implemented using either Frame Relay or ATM switches as Provider Edge devices. The peer-to-peer model was developed to overcome the drawbacks of the Overlay model and provide customers with optimal data transport via the Service Provider backbone. Hence, the service provider would actively participate in customer Layer 3 routing. In the peer-to-peer model, routing information is exchanged between the customer routers and the

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

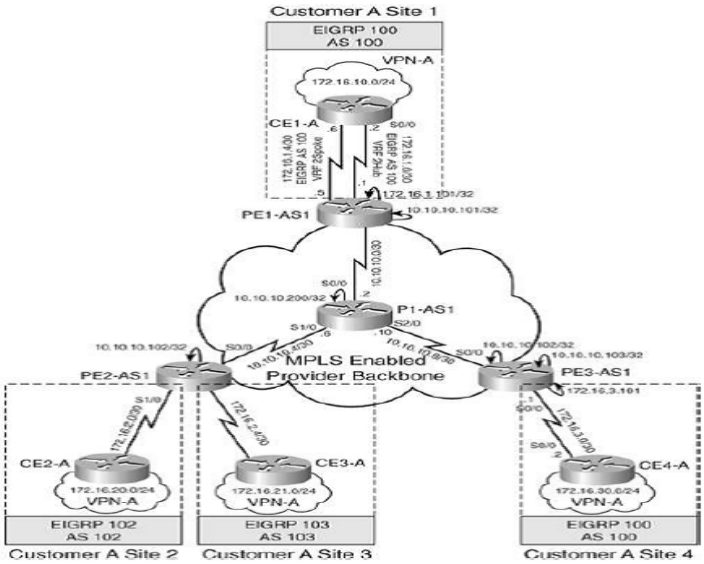
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

service provider routers, and customer data is t Customer Layer 3 routing information is carried between routers in the provider network and customer network.

III. ALGORITHM

Step1: A small ISP network and customer network with few number of routers.
Step2: Configure the Routing protocols, MPLS in that ISP network routers.
Step3: Configure VPN customer branch routing at different locations towards service provider domain.
Step4: Configure VPN customer in ISP routers and check for end to end connectivity of the branches.
Step5: Checking the Branch to Branch connectivity with Hub & Spoke topology. (Main Branch – Client branch scenario)

IV. ARCHITECTURE DIAGRAM



V. COMPONENTS

Customer network, which is usually a customer-controlled domainconsisting of devices or routers spanning multiple sites belonging to the customer. The customer network for Customer A consists of the routers CE1-A and CE2-A along with devices in the Customer A sites 1 and 2.

CE routers, which are routers in the customer network that interface withthe service provider network. The CE routers for Customer A are CE1-A and CE2-A, and the CE routers for Customer B are CE1-B and CE2-B.

Provider network, which is the provider-controlled domain consisting ofprovider edge and provider core routers that connect sites belonging to the customer on a shared infrastructure. The provider network controls the traffic routing between sites belonging to a customer along with customer traffic isolation. The provider network consists of the routers PE1, PE2, P1, P2, P3, and P4.

PE routers, which are routers in the provider network that interface orconnect to the customer edge routers in the customer network. PE1 and PE2 are the provider edge routers in the MPLS VPN domain for customers A and B.

P routers, which are routers in the core of the provider network thatinterface with either other provider core routers or provider edge routers. Routers P1, P2, P3, and P4 are the provider routers.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 1, March 2018

6th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '18)

13th-14th March 2018

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

VI. SOFTWARE DESCRIPTION

GNS3 is a Graphical Network Simulator that allows emulation of complex networks. These allow we to run operating systems such as Windows XP Professional or Ubuntu Linux in a virtual environment on our computer. GNS3 allows the same type of Emulation using Cisco Internetwork Operating Systems, a network protocol analyzer, otherwise known as a "packet sniffer", captures and decodes packets of information from a network. Wireshark can capture live network traffic or read data from a file and translate the data to be presented in a format.

VII. ADVANTAGES

- Size of label is lesser thansize of IPV4
- Speed can be said as “like a shot”
- Security can be high as possible
- Each and every data can be stored successfully

VIII. RESULT AND DISCUSSION

This paper highlights the need for implementing MPLS technology to overcome some of the limitations involved in pure IP based forwarding. So, the end result is that performance of Layer 2 MPLS VPN is much better when compared to Layer 3 MPLS VPN.

REFERENCES

[1] Engineering Analysis and Research of MPLS VPN, Ming-Song Sun, Wen-Hao Wu, Network Information Center, Harbin University of Science and Technology, Harbin, China, 150080, sunms@hrbust.edu.cn
[2] Ivan Pepelnjak and Jim Guichard, “MPLS and VPN Architectures,” Cisco Press, March 2001.
[3] Md. Arifur Rahman, AhmedulHaqueKabir, K. A. M. Lutfullah, M. Zahedul Hassan and M. R. Amin, “Performance Analysis and the Study of the behavior of MPLS Protocols,” in Proceeding of the International Conference on Computer and Communication Engineering 2008, Kuala Lumpur, Malaysia, May 13-15 2008.