A REVIEW ON LAYER 2 TUNNELING PROTOCOL

[1]Rajeev Goyal,[2]Samta Jain Goyal

Dept. of Computer Science, Amity School of Engineering & Technology,AUMP

ABSTRACT

To implement IPV6 for carrier network IETF- Soft wire Group proposed lots of appropriate methods toward this purpose. In this paper, we will focus on L2TP (Layer 2 Tunneling Protocol) which is basically introduce to deploy the gateway and host mode. Tunneling Concept used to access remote and number of users via a public network and manage its traffic with higher degree of unprocessed data on the network.

Keywords:- IPV4,IPV6,L2TP,IETF WG, IPSec,PPP

1.INTRODUCTION

The next generation network protocol which is IPV6 presently provide the solution of the problem, occurs in IPV4.The problem of IPV4 is related with address-space, security & Complexity.Since the number of users for network access is increase, so occurring of problem in addresses, security is but obvious. There are lots of technologies proposed during the transition of IPV4 to IPV6, which are basically divided into 3 types-

1. Tunnelling
2. Dual Stack
3. Translation

These three technologies are proposed by IETF working groups.

2.IETF WORKING GROUPS (WGS)

IETF Working Groups (WGs) are the primary mechanism for development of IETF specifications and guidelines. Many of which are intended to be standards or recommendations. The goal of the IETF is “to make the Internet work better” Since its name focus on the Internet Engineering Task Force, so it make the Internet work better from an engineering point of view. This influence the way of design, use, and manage the Internet. Most participants in the IETF are engineers with knowledge of networking protocols and software. Many of them know a lot about networking hardware too. Working Groups are typically created to address a specific problem or to produce one or more specific deliverables (a guideline, standards specification, etc.). Each Working Group has a charter. WG charters state the scope of work for group, and lay out goals and milestones that show how this work will be completed. Two types of working groups are available:

- Active Working Group.
- Concluded Working Group.

3.IPV4 & IPV6

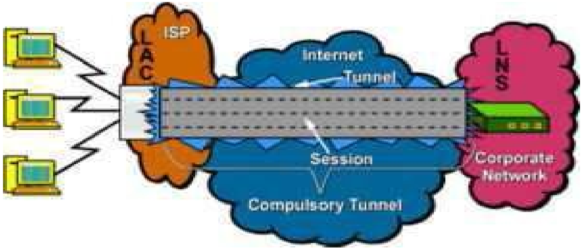
The original internal addressing system is called IPV4 which numbered the computers on network IPV4 uses 32 bits of recombined digits, has a maximum of 4.3 billion possible addresses.But the increasing numbers of users regularly exceeds this limit. Because every computer, cellphones, ipas, printers require an IP-Address.So to overcome from this limit, currently IPV6 is in role across the world. It uses 128 bits for addresses and creates 3.4*1038 possible addresses.
Three technologies are proposed by IETF:

1. Tunneling
2. Dual Stack
3. Translation

In Tunneling Technology IPV4 or IPV6 packets appended with IPV6 or IPV4 (called Encapsulation or Decapsulation) & forwarded to IPV6 or IPV4 network. In Dual Stack Technology, IPV4 & IPV6 protocol stacks are implemented in both Hosts & Routers, so host can use either IPV4 or IPV6 addresses to access other network. This serves as a foundation. In Transition Technology, it implement & perform translation between IPV4 & Ipv6 packaets.It can be used when IPV4 or IPV6 only hosts need to access the IPV6 or IPV4 network.

4.ABOUT TUNNELING

A tunnel is a Peculiar type of connection across the network.Tunne just like a direct wire which is use o connects computers. With the Tunnel Concept, connected systems has 2 IP-Addresses where one is one the network used by packet, called Carrier Address.& another is on Our network ,known as Virtual Address.



5.NEED FOR TUNNELING

It’s a technique which enables remote access users to connect variety of network resources through a public data network.

6.TUNNELING TECHNOLOGIES

There are so many technologies to support this concept .Some of them are:

- SNA Tunneling
- IPX Tunneling
- Point to point tunneling Protocol
- Layer 2 Tunneling Protocol
- IPSec Tunnel Mode

7.TUNNELING PROTOCOL

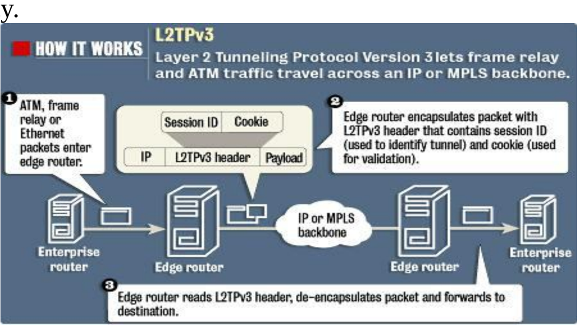
It’s a basic of VPN (Virtual Private Networking).The Tunnel provides a way to use public network like Internet which provide a secure connections in between Remote users and a private corporate network. This special and secure connection is called Tunnel.

8.VPN OVERVIEW

Historically, Layer 2 and Layer 3 VPNs referred to frame relay and best-effort IP-VPNs respectively. Frame relay allowed enterprises to cost-effectively connect multiple corporate locations together, compared to point-to-point private line services, and allowed service providers to leverage cost efficiencies from statistical multiplexing. Early IP-VPNs, based on IPSec and PPP (point-to-point tunneling protocol) allowed enterprises to more easily create multipoint data networks, and support remote locations and mobile employees, and they were cheaper than frame relay. Both of these VPN services were effective at supporting multi-site data services, but had limitations related to bandwidth scalability, provisioning simplicity and features. As service providers upgraded their networks to incorporate next-generation technologies, MPLS was used to bring networking efficiencies to their IP network and also to offer new services. These MPLS networks were initially used to deliver IP-VPNs based on the RFC 2547bis standard. More recently, service providers have started to upgrade their MPLS networks to support VPLS (Ethernet VPNs), with some service providers offering their customers a combination of both VPLS and Premium IP-VPNs based on these MPLS networks. As this research paper shows, there is some overlap with these next-generation Layer 2 and Layer 3 VPNs. These VPNs should not be considered mutually exclusive services, as many service providers are using Ethernet access circuits to connect to IP-VPN clouds, and enterprises can use both types of VPN services for their communications requirements.

Layer 2 Tunneling Protocols:

My study of this paper is based on Layer 2 Tunneling Protocol. So L2TP is a tunneling protocol used to support VPN or part of the delivery of services by ISPs, not provide any encryption or confidentiality by it. Only encryption protocol within the tunnel provides Privacy.


HOW IT WORKS

L2TPv3

Layer 2 Tunneling Protocol Version 3 lets frame relay and ATM traffic travel across an IP or MPLS backbone.

1 ATM, frame relay or Ethernet packets enter edge router.

2 Edge router encapsulates packet with L2TPv3 header that contains session ID (used to identify tunnel) and cookie (used for validation).

3 Edge router reads L2TPv3 header, de-encapsulates packet and forwards to destination.

L2TP is a standard protocol to provide wide range of services. It use various traffic management techniques to enhance the performance.L2TP is more secure due to PPTF & L2F.L2TP is the extension of Point to Point Tunneling protocol used by ISP.PPP used to transmit multi protocol packets over layer 2 point to point links.L2TP uses packet switched network connection to end point link of different network. Here two endpoints of L2TP: one is L2TP Access Concentrator (LAC) and other is L2TP Network Server (LNS).these two is proposed by IETF Software Group. In this the LAC is the initiator of the tunnel while LNS is the tunnel concentrator that waits for establishing tunnels. L2TP is one of the secure VPN which tunnels layer 2 packets since the VPN-protocols don’t have the native ability to adjust with mobility. So here to solve this problem, L2TP-tunnel has been chosen for the same purpose. Because it is very strong in security and has wide range of applications. This Protocol receives packets on Layer 2(Data Link Layer) & secures the packets on Layer 5(Session Layer).It has a problem that it provides weak authentication method.To add support for mobility to L2TP, we can keep sending packets with low delay without the thinking of cost for maintaining or reestablishing of tunnel and packets.L2TP was specially designed to provide dynamic tunneling for multiple layer 2 circuits across packet oriented data networks.L2TP focus on narrowband dialup protocols.L2tpV3 which is extended version of L2TP by letting it run on higher speed devices like Routers, also support the increase space of session and tunnel –ID from 16 to 32 bits.

9..PPTF & L2F

Since Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force (ISTF) standard that combines the best features of two existing tunneling protocols: Cisco’s Layer 2 Forwarding (L2F) and Microsoft’s Point-to-Point Tunneling Protocol (PPTP) and ensures interoperability among vendors, increase customer flexibility and service availability.

10.CONCLUSION

This paper presents the review of L2TP which is proposed due to IPV4.This protocol is a solution to support fast and secure network without losing packets .The current solution is use the tunnel – concentrator for communication with the server directly. The communication is more secure & protected. There is one more advantage of “No Data Loss”.

REFERENCES

[1] International Research paper “PROPPING AND TUNNELING” by Eric Friedman, Simon Johnson and Todd Mitton

[2] International Paper “Secure VPN Based on Combination of L2TP and IPSec” by Ya-qinFan, Chi Li and Chao Sun

[3] Research Paper on “Attacking Generic Routing Encapsulation “by tech republic associates

[4] International Paper on “Research and implementation of Layer Two Tunneling Protocol (L2TP) on carrier network” by Qin Zhao; Kuramoto, M.; Cho, F.; Lunyong Zhang

[5] International Paper published on “Tunneling in VPN” by Yuan Yuan; Ji Yi; GuGuanqun.

[6] International Research done on “ACCESS IP-VPN SOLUTION BASED ON INTEGRATION OF L2TP & IPSEC” by Hu Jianli Wang

[7] Microsoft: built-in client included with Windows 2000 and higher; Microsoft L2TP/IPsec VPN Client for Windows 98/Windows Me/Windows NT 4.0

[8] J. H. Carmouche, "IPsec virtual private network fundamentals", Indianapolis: Cisco Press, 2007.

[9] Ed. C. Kaufman, "Internet Key Exchange (IKEv2) Protocol", IETF RFC 4306, December 2005.

[10] N. Doraswamy and D. Harkins, "IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks", Prentice Hall PTR, 2003.

[11] B. Jim, S. Srinivasan, "Simple Mobility Support for IPSec Tunnel Mode", Vehicular Technology Conference, vol. 3, 2003

[12] M. Berioli and F. Trotta, "IP Mobility Support for IPSec-based Virtual Private Networks: an architectural solution”, Global Telecommunications Conference, Vol. 3, pp.15321536, December 2003.

[13] C. Perkins, "IP Mobility Support for IPv4", IETF RFC 3344, August 2002.

[14] D. E. Comer, "Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture", London: Prentice Hall International, 2000.

[15] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn and B. Palter, "Layer Two Tunneling Protocol (L2TP)", IETF RFC 2661, August 1999.

[16] D. Maughan, M. Schertler, M. Schneider and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", IETF RFC 2408, 1998.

[17] C. Perkins, "Minimal Encapsulation within IP", IETF RFC 2004, October 1996.

[18] W. Simpson, "The Point-to-Point Protocol (PPP)", IETF RFC1661, July 1994.

[19] P. Eronen, Ed, "IKEv2 Mobility and Multihoming Protocol
[20] (MOBIKE)", IETF RFC 4555, June 2006.

AUTHOR

Rajjv Goyal received the MCS,MCA and M.Tech degrees in Computer Science & Engineering 2001,2006 and 2011, respectively.

Samta Jain received the MCS,MCA and M.Tech degrees in Computer Science & Engineering 2001,2006 and 2011, respectively.