International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 3 Issue 2 ǁ February 2014 ǁ PP.38-42

Effective Tunneling of Traffic and Data in a Network with L2TP Based ON L2F

Pushpa Yadav[1] and Rohit Singhal [2]
[1] *Computer Science,Gurgaon College of Engg ,Gurgaon, India*
[2] *Computer Science,Institute of Engineering & Technology, Alwar, India*

ABSTRACT: *Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force(IETF) standard that combines the best features of two existing tunneling protocols: Microsoft's Point-to-Point Tunneling Protocol(PPTP) and Cisco's Layer 2 Forwarding(L2F) and ensures confidentiality, interoperability and security among vendors, increase service availability and customer flexibility. In this paper, we will study how tunneling enables remote access to users in order to connect to a variety of network resources (an Internet Service Provider) through a public data network and traffic is managed by shaping or queuing traffic on a per-session basis that helps to avoid traffic congestion and provides a higher degree of granularity on the network.*

KEYWORDS: *GRE, L2F, L2TP, PPTP, Tunneling.*

I. INTRODUCTION

In today's connected business environment, straightforward and effective traffic management from the network core to the network edge is very essential. Enterprises need a network infrastructure that scales to meet new business needs and manages added complexity in a cost-effective manner. Many companies today are looking for a dial-in solution where the employees can access the corporate network from a remote location. Since security is a major concern in such networks, the only available setup has involved long-distance telephone calls to corporate Network Access Servers (NAS).

II. TUNNELING

A tunnel is just a special type of connection across a network. It is very much like the connections your browser makes to web servers, except tunnel connections are long term and are done in a way to make the tunnel resemble a direct wire connecting two computers. Tunneling is a technique that enables remote access users to connect to a variety of network resources (Corporate Home Gateways or an Internet Service Provider) through a public data network. However, we mostly use them for other purposes, such as providing static IP service to users on other physical networks.

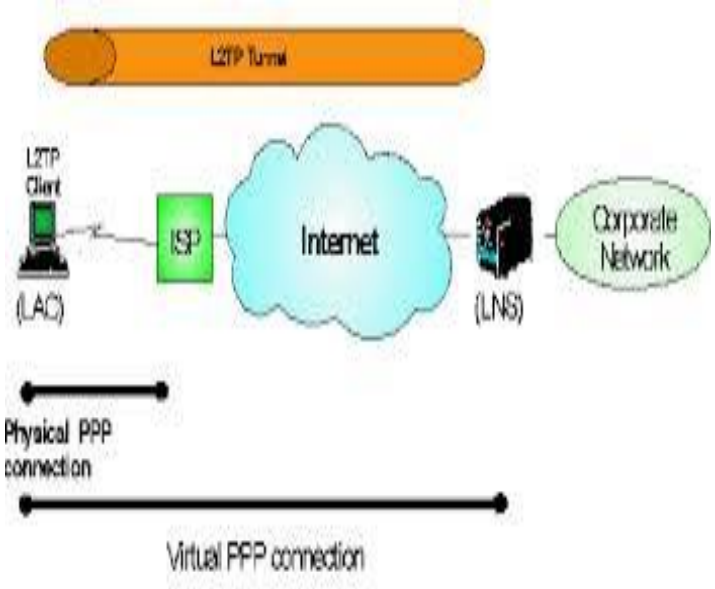

Figure 1: Tunneling Technique

A computer connected to our network with a tunnel has *two* IP addresses. One is on the network of the ISP being used for access, usually a broadband ISP (cable modem, DSL, or wireless). This IP address is used by the packets forming the tunnel and is the *carrier* IP address. The second IP address is one on our network and is the tunnel *payload* IP address, often called the *virtual* address. In normal operation the carrier address is used for nothing except carrying the tunnel. Otherwise the computer operates as if it had only the one address on our network. Other modes of operation are possible but require some understanding of IP routing and network operation. For such users we provide a small subnet, not just a single IP a ddress. However, for most users running a tunnel is no more complicated than establishing a dialup connection. In fact, the on-screen action for the most common type of tunnel is almost identical to dialling in. No modem or phone lines are involved though. Example Tunnel User - Mail Server, Web Server.

2.1 GRE Tunnel

It is possible to tunnel layer 2 over GRE by bridging the physical interface with a GRE tunnel interface. Assuming similar hardware the configuration of both tunnel endpoints will be almost identical except for the IP addressing and the routing statements, if they are used.

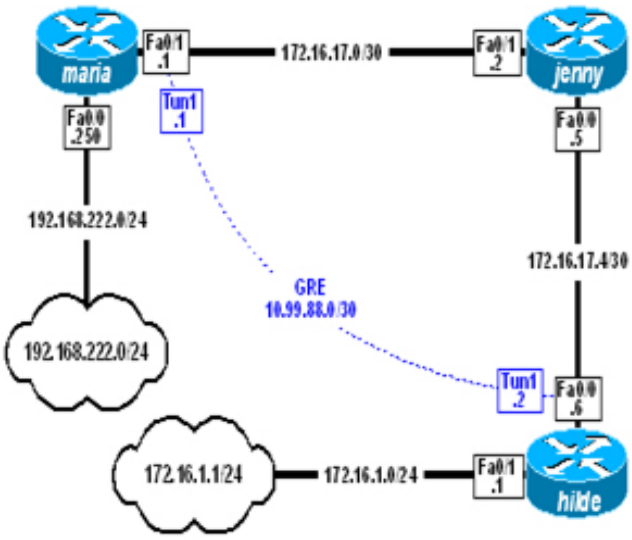

FIgure 2: GRE Tunnel

A Loopback interface will be used as the tunnel source. This Loopback interface will act as the tunnel destination for the tunnel configuration on the remote tunnel device.There are a couple of advantages to using a Loopback interface instead of a physical interface.

- As it is a logical interface it will never go down
- If the tunnel device has multiple uplinks the loopback interface will remain reachable, even if one of these links goes down.
- It allows for a somewhat more generic configuration

2.2 Tunneling Protocols

Tunneling protocols are the heart of virtual private networking. The tunnels make it possible to use a public TCP/IP network, such as the Internet, to create secure connections between remote users and a private corporate network. The secure connection is called a tunnel. The VPN 3000 Concentrator Series uses tunneling protocols to:

- Negotiate tunnel parameters
- Establish tunnels
- Authenticate users and data
- Manage security keys
- Encrypt and decrypt data
- Manage data transfer across the tunnel
- Manage data transfer inbound and outbound as a tunnel endpoint or router

The VPN Concentrator supports the most popular VPN tunneling protocols:

- **PPTP:** Point-to-Point Tunneling Protocol

- **L2F:** Layer 2 Forwarding
- **L2TP**: Layer 2 Tunneling Protocol
- **IPSec:** IP Security Protocol
- **WebVPN:** SSL VPN, which provides VPN services to remote users via an HTTPS-enabled Webbrowser, and does not require a client.

2.3 Need of Tunneling

Tunneling is a technique that enables remote access users to connect to a variety of network resources (an Internet Service Provider) through a public data network. In general, tunnels established through the public network are point-to-point (though a multipoint tunnel is possible) and link a remote user to some resource at the far end of the tunnel. The most significant benefit of Tunneling is that it allows for the creation of VPNs over public data networks to provide cost savings.A Network tunnel lets someone physically on another network be on our network also, with IP addresses of ours. The IP address and/or subnet we assign are static, so tunnel users can run Internet servers on their own computers.

III. L2TP

L2TP is a tunneling protocol that supports tunnel and user authentication. It is an important component for VPNs. Virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network.VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This not only reduces overhead costs associated with traditional remote access methods, but also improves flexibility and scalability.Traditional dial-up networking services only support registered IP addresses, which limits the types of applications that are implemented over VPNs. L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adapters (TAs), to be used. It also allows enterprise customers to outsource dial out support, thus reducing overhead for hardware maintenance cost and allows them to concentrate corporate gateway resources.Just like PPTP, L2TP provides an encrypted tunnel for VPN traffic; however, L2TP encrypts the traffic before the Point to Point (PPP) connection negotiation begins, making it much harder to conduct dictionary attacks on captured PPP packets.

3.1 L2TP Architecture

L2TP tunnels are used primarily in compulsory mode (that is, dialup LAC to LNS) access VPNs for both IP and non-IP traffic.

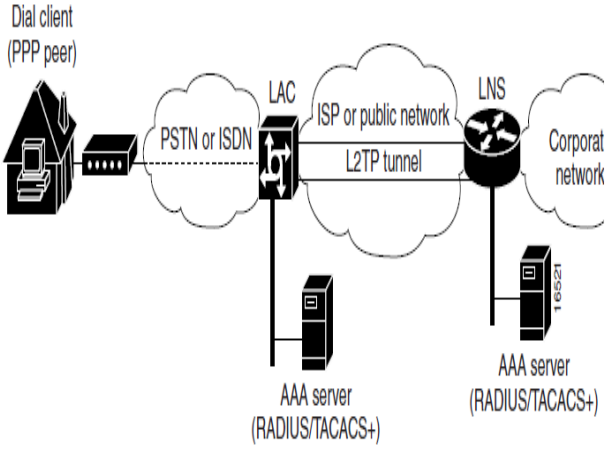

Figure 3: L2TP Architecture

A VPDN connection between a remote user, a LAC at the ISP point-of-presence (POP), and the LNS at the home LAN using an L2TP tunnel is accomplished as follows:

1) The ISP network LAC accepts the connection at the POP and the PPP link is established.
2) The remote user initiates a PPP connection to the ISP, using the analog telephone system or ISDN.
3) After the end user and LNS negotiate LCP, the LAC partially authenticates the end user with CHAP or PAP. The username, domain name, or DNIS is used to determine whether the user is a VPDN client. If the

user is not a VPDN client, authentication continues, and the client will access the Internet or other contacted service. If the username is a VPDN client, the mapping will name a specific endpoint (the LNS).

4) Once the tunnel exists, an L2TP session is created for the end user.
5) The tunnel end points, the LAC and the LNS, authenticate each other before any sessions are attempted within a tunnel. Alternatively, the LNS can accept tunnel creation without any tunnel authentication of the LAC.
6) The LAC will propagate the LCP negotiated options and the partially authenticated CHAP/PAP information to the LNS. The LNS will funnel the negotiated options and authentication information directly to the virtual access interface. If the options configured on the virtual template interface does not match the negotiated options with the LAC, the connection will fail, and a disconnect is sent to the LAC.The end result is that the exchange process appears to be between the dial-up client and the remote LNS exclusively, as if no intermediary device (the LAC) is involved. Figure 3 offers a pictorial account of the L2TP incoming call sequence with its own corresponding sequence numbers.

3.2 Features

- Ethernet packets tunnelled using BCP/PPP/L2TP
- L2TP tunnel bridges Wi-Fi clients onto carrier network
- Consistent access policies and user experience everywhere
- MAC addresses visible to broadband provider allowing device authentication
- Monitor and restrict user activity to prevent malicious use of network
- Ability to transport VLAN tags allows different policies to be applied to each SSID
- IP addresses can be allocated by centralized DHCP server
- QoS policies enforced at the edge to maximize performance and enable multimedia services
- Single L2TP tunnel simplifies operation and management overhead.

3.3 Benefits of L2TP

- Flexible, scalable remote network access environment without compromising
- Security and guaranteed priority for their most mission-critical applications
- corporate security or endangering mission-critical
- Improved connectivity, reduced costs, and freedom to refocus resources on core competencies.

IV. TRAFFIC MANAGEMENT

The ability to shape or queue traffic on a per-session basis helps to avoid traffic congestion and allows the ISP to adhere to the SLA established for handling traffic. Shaping or queuing traffic on a per-session basis provides a higher degree of granularity when managing traffic on the network.Traffic shaping allows you to control the traffic going out an interface in order to match its flow to the speed of the remote target interface. A traffic shaper typically delays excess traffic using a buffer, or a similar mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected.Traffic shaping ensures that the traffic conforms to policies contracted for it. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, eliminating bottlenecks in topologies with data-rate mismatches.

V. RESTRICTIONS

The following restrictions apply to the L2TP feature:

- Only dial in support currently exists.
- If flow control is enabled using the **l2tp flow-control receive-window** command with a value greater than zero, the switching path defaults to process level switching

VI. FUTURE SCOPES AND CONCLUSION

L2TP is a standard protocol in which all end users and service providers can enjoy a wide range of service offerings available from multiple vendors. Quality of service can be improved by using various traffic management techniques that enhances the performance factor during tunneling using L2F (Layer 2 Forwarding Protocol) which in return helps to avoid traffic congestion. L2TP combines the best features of PPTP and L2F, so that during tunneling of data can be made secure and confidential over the network.

REFERENCES

Journal Papers

[1] Secure VPN Based on Combination of L2TP and IPSec" by Ya-qinFan , Chi Li and Chao Sun
[2] Attacking Generic Routing Encapsulation " bytechrepublic associates
[3] Tunneling in VPN" by Yuan Yuan; Ji Yi ; GuGuanqun.

[4] Research and implementation of Layer Two Tunneling Protocol (L2TP) on carrier network" by Qin Zhao ; Kuramoto, M. ; Cho, F. ; Lunyong Zhang
[5] Virtual Private Networks Constructed by the Combination of IPSec& L2TP" by ZHU Changsheng, YU Dongmei.
[6] ACCESS IP-VPN SOLUTION BASED ON INTEGRATION OF L2TP & IPSEC" by Hu Jianli Wang JiazhenPengDeyun Zhang Bi
[7] PROPPING AND TUNNELING" by Eric Friedman, Simon Johnson and Todd Mitton