Effective Tunnelling of Data and Traffic Management over Network using L2TP based on L2F

Preeti[1], Ajay Rana[2]

[1]Gurgaon College of Engg, Gurgaon

[2]Amity School of Engineering and Technology
Amity University, Noida, Uttar Pradesh, India

Abstract: ***Layer 2 Tunnel Protocol (L2TP) is an emerging Internet Engineering Task Force standard that combines the best features of two existing tunnelling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunnelling Protocol (PPTP) and ensures interoperability among vendors, increase customer flexibility and service availability. In this paper, we will study how tunnelling 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: L2TP, tunnelling, L2F, PPTP, LAC

1. 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).

2. Tunnelling

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. Tunnel technologies were originally developed for building virtual private networks (VPNs), and occasionally that's what we do with them. However, we mostly use them for other purposes, such as providing static IP service to users on other physical networks [1].

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 [4].

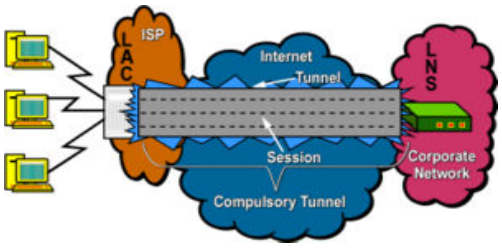

Figure 1: Tunnelling Technique

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 address. 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 line is involved though. Example is Tunnel User - Mail Server, Web Server [5].

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.

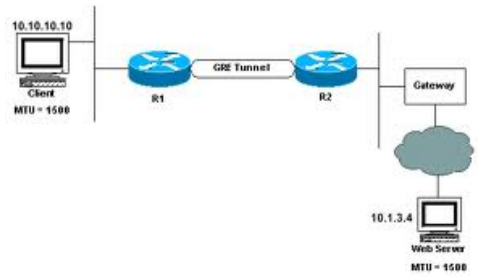

Figure 2: GRE Tunnel

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 [5].

- 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 Tunnelling Protocols

Tunnelling 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 tunnelling 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 tunnelling protocols:

- **PPTP:** Point-to-Point Tunnelling Protocol
- **L2TP**: Layer 2 Tunnelling Protocol
- **IPSec:** IP Security Protocol
- **Web VPN:** SSL VPN, which provides VPN services to remote users via an HTTPS-enabled Web browser, and does not require a client.

2.3 Need of Tunnelling

Tunnelling 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 [5].

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.

2.4 Tunnelling Technologies

Some of the mature tunnelling technologies include:

- SNA tunnelling over IP internetwork
- IPX tunnelling for Novell NetWare over IP internetwork
- Point-to-Point tunnelling protocol
- Layer 2 tunnelling protocol
- IPSec tunnel mode

3. L2TP

L2TP is a tunnelling protocol that supports tunnel and user authentication. It is an important component for VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. 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 [9].

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 Tunnels

L2TP is used in two different scenarios:

1. Compulsory Tunnelling
2. Voluntary Tunnelling

3.1.1 Compulsory Tunnelling

It refers to the scenario in which a network node- a dial or network access server, for instance acting as LAC, extends a PPP session across a backbone using L2TP to remote LNS. This. This implies that the NAS must be preconfigured to know the tunnel's terminating endpoint given a particular user's authentication information. This is done without the explicit intervention of the remote user, and the remote computer needs no special software- this operation is transparent to the user initiating the PPP session to the LAC. This allows for the decoupling of the location and/or

ownership of the modem pools used to terminate dial calls, from the site to which users are provided access.

3.1.2 Voluntary Tunnelling

Voluntary tunnelling refers to the case where an individual host/remote computer user connects to a remote site using a tunnel originating on the host, with no involvement from intermediate network nodes. There is more flexibility in how and to where they are created. This flexibility is particularly important for remote mobile users who may be dialling in from a new place each day. Because the ISP is not involved in the creation of the tunnel, the tunnel can span the networks of multiple ISPs without explicit configuration or agreement

3.2 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 [6]:

1) The remote user initiates a PPP connection to the ISP, using the analogue telephone system or ISDN.
2) The ISP network LAC accepts the connection at the POP and the PPP link is established.
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).

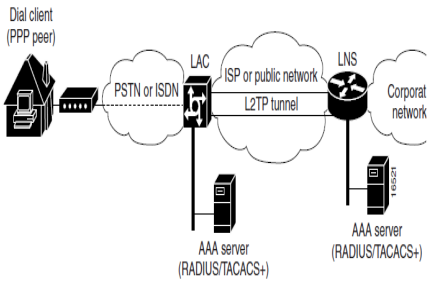

Figure 3: L2TP Architecture

4) 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.
5) Once the tunnel exists, an L2TP session is created for the end user.
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.
7) 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.

3.3 Features

Features are as follows [8]:

- L2TP tunnel bridges Wi-Fi clients onto carrier network
- Ethernet packets tunnelled using BCP/PPP/L2TP
- MAC addresses visible to broadband provider allowing device authentication
- Consistent access policies and user experience everywhere
- Monitor and restrict user activity to prevent malicious use of network
- IP addresses can be allocated by centralized DHCP server
- Ability to transport VLAN tags allows different policies to be applied to each SSID
- Single L2TP tunnel simplifies operation and management overhead
- QoS policies enforced at the edge to maximize performance and enable multimedia services [6].

3.4 Benefits of L2TP

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

4. 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 [4].

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. 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.

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

5. Restrictions

The following restrictions apply to the L2TP feature:

- 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
- Only dial in support currently exists.

6. Future Scopes and Conclusion

L2TP is a standard protocol in which all customers' service providers and corporate network managers alike—can enjoy a wide range of service offerings available from multiple vendors. L2TP utilizes more command and control messages, because of the connection-less aspect of L2TP, but will also perform better over high latency networks.

Quality of service can be improved by using various traffic management techniques that enhances the performance factor during tunnelling using L2F (Layer 2 Forwarding Protocol) which in return helps to avoid traffic congestion.

As L2TP combines the best features of PPTP and L2F so that during tunnelling of data can be made more secure over the network.

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 techrepublic 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 paper on "Virtual Private Networks Constructed by the Combination of IPSec& L2TP" by ZHU Changsheng, YU Dongmei.
[7] International Research done on "ACCESS IP-VPN SOLUTION BASED ON INTEGRATION OF L2TP & IPSEC" by Hu Jianli Wang JiazhenPengDeyun Zhang Bi
[8] http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtl2tpv3.html
[9] http://www.cisco.com/en/US/docs/ios/12_0t/12_0t1/feature/guide/l2tpT.html
[10] Microsoft: built-in client included with Windows 2000 and higher; Microsoft L2TP/IPsec VPN Client for Windows 98/Windows Me/Windows NT 4.0