TRAFFIC POLICING OF IN-CONTRACT TRAFFIC IN A L2TP BASED L2F

Pushpa yadav

Abstract: L2TP (Layer 2 Tunneling Protocol) allows multiprotocol traffic to be encrypted and then sent over any medium that supports point-to-point datagram delivery, such as IP or asynchronous transfer mode. This paper represents the best features of PPTP and L2F. In this paper, we are mainly focusing on topic that how can shape the traffic for a smooth Traffic Management purpose so that we can easily confirm the amount of traffic travelled through the setup. This also ensures that the amount of traffic passed is same or varying to the amount of traffic we want to pass .At time of Congestion, this feature provides an additional benefit and helps in fighting congestion at the real time applications. Also this adds to the existing PPP authentication process and ensures a level of check from our side.

Keywords: Authentication, VFN, Tunnelling, VPN, l2F, LAC, PPP

1 Introduction

Tunneling, also known as "port forwarding," is the transmission of data intended for use only within a private, usually corporate network through a public network in such a way that the routing nodes in the public network are unaware that the transmission is part of a private network.L2TP requires two levels of authentication: Computer level Authentication and User level Authentication. L2TP is a tunneling protocol has the following major benefit like Supporting Multi-hop, Operate like a client initiated Virtual Private Network (VPN) solution and L2F offered value-added traits, as load sharing plus backup support. L2TP has all the security benefits of PPP, including multiple per user authentication options (CHAP, PAP and MS-CHAP). It also can authenticate the tunnel end points, which prevents potential intruders from building a tunnel and accessing precious corporate data. L2TP can be used in conjunction with secure ID cards on the client side and it works with firewalls on the corporate server side. To ensure further data confidentiality, it is recommended adding IPSec to any L2TP implementation. Depending on the corporation's specific network security requirements, L2TP can be used in conjunction with tunnel encryption, end-to-end data encryption or end-to-end application encryption [5].

2 Problem Statements

In this paper, we are going to mainly concentrate on following issues:

a) How to setup the connection?

b) How could we authenticate to ensure a secure session?

c) What could be the major possibilities with authenticating using PPP,PAP and CHAP and what would be the best way to do that?

d) How to ensure tunneling is initiated and enabled successfully?

e) How to find out tunnelling has been terminated?

f) How to be choosy regarding traffic over the setup?

g) How to observe the pros and cons of a peer-session basis of managing traffic between LAC and LNS?

h) What would happen from one state of connection to another and how to resume it back?

i) What are major management strategies for traffic to ensure secure and a congestion free traffic over tunnels? How to achieve it?

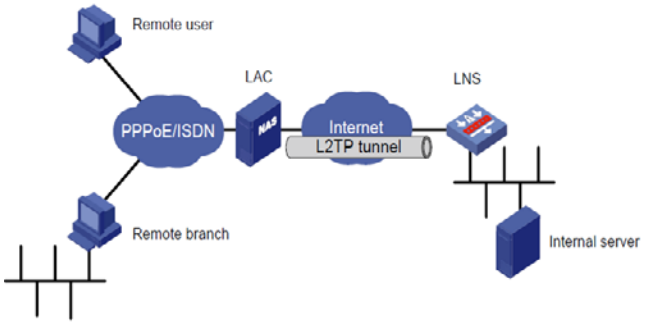

Figure 1: L2TP Tunneling

The four use cases discussed below illustrate how L2TP works in a variety of scenarios, from simple point-to-point links to large networks. Whether you're running a single-site corporate LAN or a complicated multi-site network, L2TP has the scalability to fit into our architecture [8].

The traffic Classification, Policing and Marking on a LAC feature allows service providers to classify packets based upon the IP Type Of Service (ToS) bits in an embedded IP packet. The classification is used to police the incoming traffic according to the Differentiated Services Code Point (DSCP) value. The purpose of classifying the packet by examining its encapsulation is to simplify the implementation and configuration needed for a large number of PPP sessions. The policy: Per-Session Shaping and Queuing on LNS feature provides the ability to shape (for example, transmit or drop) or queue (for transmission later) the traffic going from an Internet service provider (ISP) to an ISP subscriber over Layer 2 Tunneling Protocol (L2TP) Network Server (LNS). With this feature, the outgoing traffic is shaped or queued on a per-session basis.

3 Restrictions for traffic Classification, Policing and Marking on a LAC

Service-policy on PPP over X.25 (PPPoX) interfaces is not supported.

a) Class-based queuing and class-based shaping are not supported.

b) Layer 2 marking is not supported.

c) The clear counters command does not clear the counters of the service policy map.

d) Multi hop Virtual Private Dialup Networks (VPDNs) are not supported [9].

3.1 Benefits of the QoS Classification Policing and Marking on a LAC Feature

a) This feature provides policing and marking on a per-session basis for traffic forwarded into L2TP tunnels to the appropriate LNS and for traffic coming from an L2TP tunnel toward a customer edge router.

b) This feature helps recognize the IP ToS value in the Point-to-Point Protocol over Ethernet (PPPoE) encapsulated traffic in order to classify and police the traffic according to the DSCP value.

3.2 Prerequisites for Per-Session Shaping and Queuing on LNS

a) Verify that the PPPoE sessions are enabled.

b) Verify that L2TP re-sequencing is disabled.

c) This feature uses policy maps in which queuing mechanisms (such as class-based weighted fair queuing [CBWFQ]) are configured. A policy map can be configured for a session and for an outgoing interface. With this feature, a policy map (in which a queuing mechanism is configured) cannot be used for both the session and the outgoing interface simultaneously.

If a queuing mechanism is in both policy maps, one of these policy maps must be disabled.

4 Per-Session Traffic Shaping

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 [1].

4.1 Per-Session CBWFQ

WFQ offers dynamic, fair queuing that divides bandwidth across queues of traffic based on weights.WFQ ensures that all traffic is treated fairly, given its weight. CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria including protocols, Access Control Lists (ACLs) and input interfaces. Packets satisfying the match criteria for a class constitute the traffic for that class. A FIFO queue is reserved for each class, and traffic belonging to a class is directed to the queue for that class [1].

The QoS: Per-Session Shaping and Queuing on LNS feature supports CBWFQ. With this feature, CBWFQ is implemented on a per-session basis (that is, when traffic arrives at the interface).

4.2 Configuring Per-Session Shaping and Queuing on LNS

The tasks for configuring the QoS: Peer-Session Shaping and Queuing on LNS feature vary according to the configuration method we are using. We can choose to configure the feature using either a virtual template or a RADIUS server.

A policy map specifies the quality of service (QoS) feature to be applied to network traffic. Examples of features that can be specified in a policy map include class-based weighted fair queuing (CBWFQ) and traffic shaping [8].

Hierarchical Policy Maps

Policy maps can be configured in a hierarchical structure. That is, policy maps can be configured in levels subordinate to one another. The policy map at the highest level is referred to as the "parent" policy map. A subordinate policy map is referred to as the "child" policy map. A typical hierarchical policy map structure consists of a parent policy map and one child policy map. Configure the child policy map first; then configure the parent policy map. Both types of policy maps are configured in the same manner. The parent policy map typically contains one class—the class called class-default. The child policy map can contain multiple classes [9].

SUMMARY STEPS

1. Enable
2. Configure terminal
3. Policy-map policy-map-name
4. Class {class-name | class-default}
5. Shape [average | peak] mean-rate *[*burst-size*] [*excess-burst-size]
6. Bamdwidth {bandwidth-kbps | remaining percent percentage | percent percentage}
7. Service-policy {input | output} policy-map-name
8. Exit .

4.3 Configuring traffic management on a LAC

SUMMARY STEPS

1. Enable

2. Show policy-map session [uid uid-number] [input | output [class class-name]]

3. Exit

5 Testing and Experimental Results

L2TP extends the PPP model by allowing the Layer 2 and PPP endpoints to reside on different devices interconnected

by a packet-switched network. With L2TP, a user has a Layer 2 connection to an access concentrator (e.g., modem bank, ADSL DSLAM, etc.), and the concentrator then tunnels individual PPP frames to the NAS. This allows the actual processing of PPP packets to be divorced from the termination of the L2 circuit.

One obvious benefit of such a separation is that instead of requiring the L2 connections terminate at the NAS, the connection may terminate at a (local) circuit concentrator, which then extends the logical PPP session over a shared infrastructure such as frame relay circuit or the Internet. From the user's perspective, there is no functional difference between having the Layer 2 circuit terminate in a NAS directly or using L2TP.Because L2TP uses IPSec, it not only encrypts data, but also offers additional security benefits over PPTP. L2TP offers data integrity and data-origin authentication. Another advantage is its use of UDP to encapsulate data, which makes L2TP faster and easier to configure with some firewalls. With other firewalls, L2TP can have a slight disadvantage in speed because it encapsulates data twice. The main disadvantage in using L2TP is the amount of configuration needed to set it up, including PKI and computer certificates.

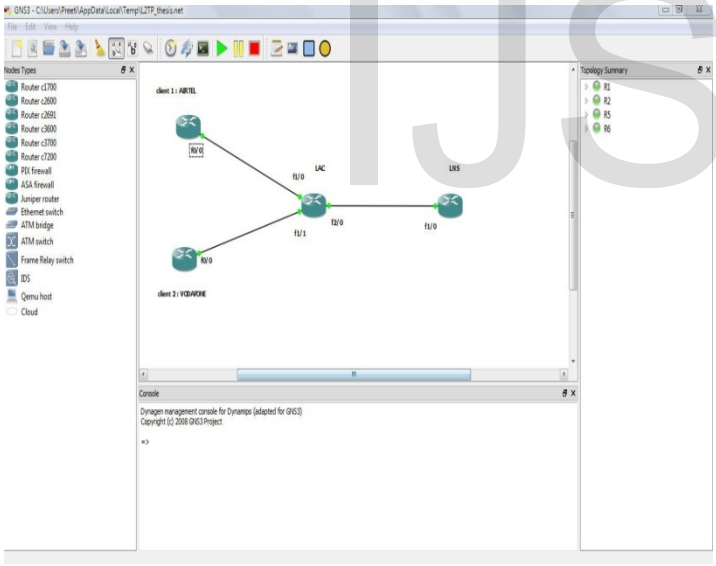

Fig2: Connection Setup

```
R2#sh l2tun

%No active L2F tunnels

L2TP Tunnel and Session Information Total tunnels 2 sessions 2

LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
                                                       VPDN Group
24276 31743 LNS           est    10.10.10.2      1701  1        100

LocID      RemID      TunID      Username, Intf/      State  Last Chg Uniq ID
                                 Vcid, Circuit
4          2          24276      cisco@cisco.com, -   est    00:03:12 3

LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
                                                       VPDN Group
32789 47536 LNS           est    10.10.10.2      1701  1        200

LocID      RemID      TunID      Username, Intf/      State  Last Chg Uniq ID
                                 Vcid, Circuit
5          3          32789      isp@isp.com, -       est    00:03:08 4

%No active PPTP tunnels

PPPoE Tunnel and Session Information Total tunnels 1 sessions 2

PPPoE Session Information
Uniq ID  PPPoE  RemMAC          Port                  VT  VA         State
         SID  LocMAC                                     VA-st
     4     4  cc03.0d44.0000  Fa1/0                  1  N/A        FWDED
              ca01.231c.001c
     3     3  cc02.0d44.0000  Fa1/1                  1  N/A        FWDED
              ca01.231c.001d
R2#
R2#
```

Fig 3: Secure Tunnel Establishment

```
R2#sh class
R2#sh pol
R2#sh policy-map
R2#sh policy-map int f2/0
 FastEthernet2/0

  Service-policy output: downstream-policy

    Class-map: customer1234 (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs1 (8) cs2 (16) cs3 (24) cs4
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        dscp af11
          Packets marked 0

    Class-map: customer56 (match-any)
      15 packets, 2006 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs5 (40) cs6 (48)
        15 packets, 2006 bytes
        5 minute rate 0 bps
      police:
          cir 20000 bps, bc 10000 bytes
          pir 40000 bps, be 10000 bytes
        conformed 15 packets, 2006 bytes; actions:
          set-dscp-transmit af21
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit af22
        violated 0 packets, 0 bytes; actions:
          set-dscp-transmit af23
        conformed 0 bps, exceed 0 bps, violate 0 b
```

Fig 4: Traffic Policing Map

6 Conclusions and Future Work

This paper results that L2TP Protocol can be used for integrating multi-protocol dial-up services into existing Internet Service Providers Point of Presence. Typically, a user obtains a L2 connection to a Network Access Server (NAS) using one of a number of techniques (e.g., dialup POTS, ISDN, ADSL, etc.) and then runs PPP over that connection.

The future work regarding L2TP would be extending research to L2TP v3. L2TPv3 can be regarded as being to MPLS (Multi-Protocol Label Switching).Another future work would be how we can use Linux as an L2TP/IPSec client. There are basically two methods of authenticating

L2TP/IPSec clients: Pre-shared Keys (PSKs) and X.509 certificates.

7 References

[1] Kent, S. and Atkinson, R., Security Architecture for the Internet Protocol", RFC 2401, November 1998.
[2] Hamzeh, K. et al, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.
[3] Oppliger, R., "Security Technologies for the World Wide Web", Artech House Computer Library, 2000.
[4] Venkateswaran, R., "Virtual Private Networks", IEEE Potentials Magazine, February/March 2001.
[5] IETF (1999), RFC 2661, Layer Two Tunneling Protocol "L2TP".
[6] Teletraffic Engineering Handbook ITU-T Study Group 2.
[7] Leonard Franken. Quality of Service Management: A Model-Based Approach. PhD thesis, Centre for Telematics and Information Technology, 1996.
[8] Fulvio Ricciardi. "QoS and Traffic Shaping in Transparent Bridge mode". Router/Bridge Linux Firewall website. Zero Shell Net Services. Retrieved October 15, 2011.
[9] http://www.cisco.com/warp/public/cc/pd/iosw/\=0prodlit/l2tun_ds.html