CHAPTER 9

Layer 2 Tunnel Protocol "L2TP"

This chapter describes the level of support that Cisco ANA provides for L2TP, as follows:

Note L2TP technology for Cisco devices is currently not supported.

Technology Description

L2TP

L2TP acts like a Data Link layer (Layer 2) protocol for tunneling network traffic between two peers over an existing network (usually the Internet). The two endpoints of an L2TP tunnel are the initiator of the tunnel L2TP Access Concentrator (LAC) and the L2TP Network Server (LNS), which waits for new tunnels. Once a tunnel is established, the network traffic between the peers is bidirectional.

L2TP is in fact a Session Layer (Layer 5) protocol, as the entire L2TP packet is sent within a UDP datagram, while it is common to carry Point-to-Point Protocol (PPP) sessions within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity.

Inventory and Information Model Objects (IMOs)

This section includes the following tables:

Layer 2 Tunnel Protocol Interface

The following Layer 2 Tunnel Protocol Interface object represents one edge of an L2TP Tunnel. It aggregates multiple Layer 2 Tunnel Protocol Session Entries, which it is bound to by its Session Table attributes, while being aggregated by a Layer 2 Tunnel Protocol Peer, from which it is created or cloned.

Table 9-1 Layer 2 Tunnel Protocol Interface (IL2TPTunnel)

Attribute Name	Attribute Description
Local and Remote Tunnel Identifications	Local and remote tunnel identifications
Local and Remote Tunnel Names	Local and remote tunnel names
Remote Address	Remote IP address
Control Errors	Control errors count
Last Error Code	Last error code value which cause tunnel disconnection
Tunnel State	Tunnel state (*Unknown, Idle, Connecting, Established, Disconnecting*)
Sessions Count	Current sessions count
Sessions Table	Array of Layer 2 Tunnel Protocol Session Entries

Layer 2 Tunnel Protocol Session Entry

The following Layer 2 Tunnel Protocol Session Entry object represents a session within an L2TP Tunnel. It is primarily accessed by the Layer 2 Tunnel Protocol Interface in which it is contained.

Table 9-2 Layer 2 Tunnel Protocol Session Entry (IL2TPSessionEntry)

Attribute Name	Attribute Description
Local and Remote Session Identifications	Local and remote session identifications
Subscriber Name	Subscriber name
Session Type	Session type (*Unknown, LAC, LNS*)
Session State	Session state (*Unknown, Idle, Connecting, Established, Disconnecting*)
Input and Output Data Counters	Input and output data octets and packets counters

Vendor Specific Inventory and Information Model Objects

Vendor specific Information Model Objects are implemented only for specific devices of the vendor.

The following sections describe the objects of specific vendors:

- Redback's Layer 2 Tunnel Protocol Peer
- Redback's Layer 2 Tunnel Protocol Group
- Redback's Layer 2 Tunnel Protocol Domain Entry

Redback's Layer 2 Tunnel Protocol Peer

Redback's Layer 2 Tunnel Protocol Peer object describes a logical component, aggregating multiple Layer 2 Tunnel Protocol Interfaces with their configuration, which it is being bound to by its Logical Sons attribute. It is primarily used for managing the creation of L2TP Tunnels.

Table 9-3 Redback's Layer 2 Tunnel Protocol Peer (IL2TPPeer)

Attribute Name	Attribute Description
Local and Peer Addresses	Local and peer IP addresses
Local and Peer Names	Local and peer names
Tunnel Type	Tunnel type (*Unknown, LAC, LNS*)
Tunnel Mode	Tunnel mode (*Null, Static, Dynamic*)
Maximum and Current Tunnels Counts	Maximum and current tunnels counts
Maximum and Current Sessions Counts	Maximum and current sessions counts
Session Authentication Type	Session authentication type (*Null, None, Simple, Challenge*)
Tunnel Password	Tunnel password for the authentication phase of the tunnel establishment
RADIUS Identification	Remote Authentication Dial In User Service (RADIUS) identification
Hello Time Interval	Time interval in witch hello (keep alive) packets should be sent
Control Errors	Control errors count
Media Type	Underlying media type (*Null, Other, None, UDPLP, Frame Relay, ATM*)
Group Identification	Object Identification (OID) of layer 2 tunnel protocol group (*IL2TPGroup*)
Domains Table	Array of Layer 2 Tunnel Protocol Domain Entries
Logical Sons	Array of aggregated Layer 2 Tunnel Protocol Interface

Redback's Layer 2 Tunnel Protocol Group

Redback's Layer 2 Tunnel Protocol Group object describes a logical component, load balancing multiple Redback's Layer 2 Tunnel Protocol Peers, which are grouped by its Peer List attribute. It is aggregated by a Traffic Descriptor Container object.

Table 9-4 Redback's Layer 2 Tunnel Protocol Group (IL2TPGroup)

Attribute Name	Attribute Description
Group Name	Layer 2 tunnel protocol group name
Tunnel Algorithm	Tunnel algorithm
Dead Time	Dead time

Table 9-4 Redback's Layer 2 Tunnel Protocol Group (IL2TPGroup) (continued)

Attribute Name	Attribute Description
RADIUS Identification	Remote Authentication Dial In User Service (RADIUS) identification
Peers List	Array of Redback's Layer 2 Tunnel Protocol Peers
Domains Table	Array of Layer 2 Tunnel Protocol Domain Entries

Redback's Layer 2 Tunnel Protocol Domain Entry

Redback's Layer 2 Tunnel Protocol Domain Entry object describes an Internet Domain, in which members are allowed to open L2TP Sessions within L2TP Tunnels, aggregated by either L2TP Peers or further by L2TP Groups containing this domain. It is aggregated by a Traffic Descriptor Container object.

Table 9-5 Redback's Layer 2 Tunnel Protocol Domain Entry (IL2TPDomainEntry)

Attribute Name	Attribute Description
Domain Name	Layer 2 tunnel protocol domain name
Attached To Object	Object Identifier (OID) of either a Redback's Layer 2 Tunnel Protocol Peer or a Redback's Layer 2 Tunnel Protocol Group this domain is attached to

Network Topology

The discovery of Layer 2 Tunnelling Protocol (L2TP) Data Link layer topology is unsupported. The topology is not manually configured.

Service Alarms

A summary of the L2TP technology alarms are displayed in the alarms summary table:

Table 9-6 Alarms Summary

Alarm	Severity	Description	Up Alarm
L2TP Peer is Not Established	Major	The state of a statically configured L2TP tunnel is changed from "established" to anything else. Such a failure may be as the result of a configuration or network problem.	L2TP Peer is Established
L2TP Peer was Removed	Info	A dynamically configured L2TP Tunnel was removed from a device	None
L2TP Sessions Count Exceeded	Major	The current sessions count has exceeded its maximum threshold	L2TP Sessions Count Returned to Normal

L2TP Peer Is Not Established/Established

An L2TP peer is not established alarm is issued when the state of a statically configured L2TP tunnel is changed from "established" to anything else. Such a failure may be as the result of a configuration or network problem. The L2TP peer is established alarm is issued when this problem has been fixed.

L2TP Peer Was Removed

An L2TP peer was removed alarm is issued when a dynamically configured L2TP tunnel is removed from a device. This is not issued as a ticket; however it invokes a correlation flow and can be viewed in Cisco ANA EventVision. In addition, it also appears in the Cisco ANA NetworkVision application only if correlated to another alarm, like link or port down.

L2TP Sessions Count Exceeded/Return to Normal

An L2TP sessions count exceeded alarm is issued when the current percentage of the number of sessions in the L2TP peer has exceeded the maximum configurable threshold. A L2TP sessions count return to normal alarm is issued when the current percentage of the number of sessions has returned to below the configured threshold.

The maximum number of sessions allowed for a single peer is defined by the L2TP peer and L2TP tunnel configuration parameters.

Alarm Configuration Parameters

For more information about event and alarm configuration parameters, see the Cisco Active Network Abstraction Fault Management Guide.

Using Cisco ANA PathTracer to View L2TP Path Information

This section describes the Cisco ANA PathTracer for L2TP, including viewing tunnel information. For detailed information about the Cisco ANA PathTracer, see the Cisco Active Network Abstraction NetworkVision User Guide.

Cisco ANA uses VC ID encapsulation information to trace the path from one tunnel interface to another over the network. The Cisco ANA's PathTracer tool enables you to:

- View a path for the defined L2TP session across the network.
- For each network element view the relevant parameters for each interface on all layers along the path.

Layer 2 and Layer 3 L2TP information is displayed in the Cisco ANA PathTracer windows when a path is traced over L2TP tunnels for Redback devices.

Layer 3

The following Layer 3 property that may be displayed in the **Layer 3** tab relates specifically to L2TP tunnels:

- Name—The peer name is displayed.

Layer 2

The following Layer 2 properties that may be displayed in the **Layer 2** tab relate specifically to L2TP tunnels:

- Encapsulation Type—The encapsulation type, for example, PPPoA.
- Binding Information—The name of the subscriber.
- Binding Status—The binding status, namely, bound or unbound.
- Tunnel Session Count—The number of current sessions.
- Tunnel Remote ID—The remote tunnel identifier.
- Tunnel ID—The local tunnel identifier.
- Tunnel Name—The name of the subscriber and the tunnel ID.
- Session ID—The session identifier.
- Traffic -> L2TPSessionCounters—The number of traffic packets passing through the L2TP tunnel.
- Traffic <- L2TPSessionCounters—The number of traffic packets passing through the L2TP tunnel.
- Tunnel Ctl Errors—The number of control errors.
- Tunnel State—The tunnel state, namely, unknown, idle, connecting, established, and disconnecting.
- Session Type—The session type, namely, unknown, LAC, and LNS.
- Peer Name—The peer name.
- Tunnel Remote IP—The remote IP address of the tunnel.
- Last Error Code—The last error code value which caused the tunnel disconnection.
- Session State—The session state, namely, unknown, idle, connecting, established, and disconnecting.
- Remote Session ID—The remote session identifier.