# Cisco Active Network Abstraction Technology Support and Information Model Reference Manual, Version 3.6



**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-12516-01

*Cisco Active Network Abstraction Technology Support and Information Model Reference Manual, Version 3.6*

# CONTENTS

# Preface

This document outlines the level of functionality that Cisco ANA provides for each supported technology.

For a detailed description of the supported technologies see the following chapters:

# Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

# Introduction

This document outlines the level of functionality that the system provides for each supported technology.

**Note** This guide describes the system capabilities. The level of support provided for the VNEs for each technology may vary and the user should refer to the individual VNE guide for details.

## Supported Technologies

The table below lists the technologies supported in this version of the document:

**Note** Cisco ANA provides different level of support for each technology, the fact that a specific technology is listed in the table below does not imply that all the specification of the relevant standard/s are represented and supported. For example, the system supports PWE3 (Pseudo Wire Edge to Edge) by modeling of the Cisco AToM implementation, but this support does not include TDM encapsulation in Pseudo Wire over MPLS.
For the details of the level of support provided for each technology please refer to the description in the specific technology chapter.

*Table 1-1 Supported Technologies*

| Family | Technology | Chapter Reference |
|---|---|---|
| Virtual Private Networks (**VPN**) | BGP-MPLS VPN Routing and Forwarding (**VRF**) | Chapter 14, "Virtual Private Networks "VPNs"" |
| | Pseudo Wire Emulation Edge to Edge (**PWE3**) | Chapter 15, "Pseudo Wire Emulation Edge to Edge (PWE3)" |

*Table 1-1 Supported Technologies (continued)*

| Family | Technology | Chapter Reference |
|---|---|---|
| Network Layer | Internet Protocol (**IP**) | Chapter 2, "Internet Protocol "IP"" |
| | Internet Protocol (**IP**) and **ARP** | Chapter 2, "Internet Protocol "IP"" |
| | Generic Routing Encapsulation (**GRE**) | Chapter 2, "Generic Routing Encapsulation (GRE) Tunnel Interface" |
| | Border Gateway Protocol and its Extensions for Multi-Protocol (**BGP/MP-BGP**) | Chapter 3, "Routing Protocols "BGP/OSPF""<br>Chapter 14, "Virtual Private Networks "VPNs"" |
| | Open Shortest Path First (**OSPF**) | Chapter 3, "Routing Protocols "BGP/OSPF"" |
| | Hot Standby Router Protocol (**HSRP**) | Chapter 2, "Hot Standby Router Protocol (HSRP) Group Entry" |
| Hybrid Network/Link Layer | Multi-Protocol Label Switching (**MPLS**) | Chapter 12, "Multiprotocol Label Switching "MPLS"" |
| | Traffic Engineering (**MPLS-TE**) | Chapter 13, "Multi Protocol Label Switching Traffic Engineering (MPLS-TE)" |
| Link/MAC Layer | Ethernet, Virtual Local Area Network (**VLAN**) and Ethernet Channel/Link Aggregation (**LAG**) | Chapter 4, "Ethernet (IEEE 802™.3)" |
| | Token Ring (**TR**) | Chapter 5, "Token Ring "TR" (IEEE 802™.5)" |
| | Asynchronous Transfer Mode (**ATM**) | Chapter 6, "Asynchronous Transfer Mode "ATM"" |
| | Inverse Multiplexing for ATM (**IMA**) | Chapter 6, "Asynchronous Transfer Mode "ATM"" |
| | Frame Relay (**FR**) | Chapter 7, "Frame Relay "FR"" |
| | Point To Point Protocol (**PPP**) | Chapter 8, "Point-to-Point Protocol "PPP" and High Level Data Link Control "HDLC"" |
| | High Level Data Link Control (**HDLC**) | Chapter 8, "Point-to-Point Protocol "PPP" and High Level Data Link Control "HDLC"" |
| | Layer 2 Tunnel Protocol (**L2TP**) | Chapter 9, "Layer 2 Tunnel Protocol "L2TP"" |
| | Packet Over SONET/SDH (**POS**)<br>**Note** This is not treated as a single technology; it is supported by a combination of IP, PPP/HDLC and Sonet. | Chapter 11, "Physical Technologies" |

*Table 1-1 Supported Technologies (continued)*

| Family | Technology | Chapter Reference |
|---|---|---|
| Physical Layer | Digital Subscriber Line (**xDSL**) | Chapter 10, "Digital Subscriber Line "DSL" and Integrated Services Digital Network "ISDN"" |
| | Integrated Services Digital Network (**ISDN**) | Chapter 10, "Digital Subscriber Line "DSL" and Integrated Services Digital Network "ISDN"" |

# Networking Related IMOs

Networking related IMOs represent the networking aspects of a Network Element (NE). The two major categories of IMOs are Termination Points and Forwarding Components.

## Termination Points

Termination Points represent an end point of a connection. Termination Points may represent a physical end point, for example, a port connector or a connection end point also referred to as a network interface, for example, an ATM layer of a port.

The relationships between Termination Points is of containment nature, and these relationships are expressed by the following attributes:

- Contained Connection Termination Point—Points to all upper layer Termination Point bound to that Termination Point.
- Containing Termination Points—Points to all lower layer Termination Point on which this Termination Point is bound to.

The relation between Termination Points may represent one of the following:

- Type of Hardware - for example:

  A SONET/SDH port with a Fiber Optic connector will be represented by two IMOs:

  - Port Connector IMO—Representing the Fiber Optic connector.
  - SonetSdh IMO—Representing the SONET/SDH port.

  The Port Connector IMO is containing the SonetSdh IMO. This containment relationship will be represented as follows:

  - The Port Connector IMO will point to the SonetSdh IMO with the Contained Connection Termination Point attribute.
  - The SonetSdh IMO will point to the Port Connector IMO with the Containing Termination Point attribute.

- Configuration - for example:

  Ethernet port configured with an IP Address (and optionally other network layer attributes) will be represented by two IMOs:

  - Ethernet Interface IMO—Representing the Ethernet layer of the port.
  - IP Interface IMO—Representing the network layer aspect including the IP address configured on the port.

  The Ethernet Interface IMO is containing the IP Interface IMO. This containment relationship will be represented as follows:

  - The Ethernet Interface IMO will point to the IP Interface IMO with the Contained Connection Termination Point attribute.
  - The IP Interface IMO will point to the Ethernet Interface IMO with the Containing Termination Point attribute.

- State - for example:

  An active PPP connection running on top of ATM VC will be represented by two IMOs:

  - Atm Vc IMO—Representing the ATM VC.
  - Vc Based Encapsulation IMO—Representing the PPPoA encapsulation.

  The Atm Vc IMO is containing the Vc Based Encapsulation IMO. This containment relationship will be represented as follows:

  - The Atm Vc IMO will point to the IP Vc Based Encapsulation IMO with the Contained Connection Termination Point attribute.
  - The Vc Based Encapsulation IMO will point to the Atm Vc IMO with the Containing Termination Point attribute.

**Note** The relationship between Termination Points may be restricted to specific Termination Point types, based on how the technology is implemented. For example, a physical layer IMO may not contain an IP interface IMO, which represents the network layer interface.

# Forwarding Components

Forwarding Components represent components that perform some kind of forwarding process between the Termination Points, for example, Forwarding Components are used to represent routing, bridging and switching components in the NE.

The relationship between the Forwarding Components and the Termination Points with which it does the forwarding, is of a logical association nature. This relationship is expressed by the logical sons attribute of the Forwarding Component IMO.

An example of such a relationship is between the IVcSwitchingEntity IMO representing the ATM/FR switching fabric and the IAtm/IFrameRelay IMOs representing the ATM/FR ports.

**Note** The support level of each network technology can be varied and is totally reflected by its related IMOs with their attributes, network topology as well as faults and alarms correlation, as described in each Technology section and Common section.

# Conventions Used in this Guide

This document uses the following conventions:

*Table 1-2 Document Conventions*

| Convention | Description |
|---|---|
| *Italic text* | Indicates references to enumeration values |
| Blue text | Indicates references to defined objects/tables |

**Note** Each object that the interface uses in the IMO is written in parenthesis.

CHAPTER 2

# Internet Protocol "IP"

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



## Technology Description

### IP

The Internet Protocol (IP) is a network layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP is documented in RFC 791 and is the primary network layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an inter-network; and providing fragmentation and reassembly of data-grams to support data links with different Maximum Transmission Unit (MTU) sizes.

### ARP

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, known as a Media Access Control or MAC address that is recognized in the local network. For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

## HSRP

Hot Standby Router Protocol (HSRP) is a routing protocol that provides automatic router backup by allowing host computers on the Internet to use multiple routers that act as a single virtual router, maintaining connectivity even if the first hop router fails, because other routers are on hot standby and ready to go. The protocol is fully compatible with Novell's Internetwork Packet Exchange (IPX), AppleTalk, and Banyan VINES, and (in some configurations) with Xerox Network Systems (XNS) and DECnet.

Developed by Cisco and specified in RFC 2281, HSRP ensures that only a single router (called the active router) is forwarding packets on behalf of the virtual router at any given time. A standby router is chosen to be ready to become the active router, in the event that the current active router fails. HSRP defines a mechanism used to determine active and standby routers by referring to their IP addresses. Once these are determined, the failure of an active router will not cause any significant interruption of connectivity.

On any given LAN, there may be multiple, possibly overlapping, hot standby groups, each with a single Media Access Control (MAC) address and IP address; the IP address should belong to the primary subnet, but must be different from any actual or virtual addresses allocated to any routers or hosts on the network.

## GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol, originated by Cisco Systems and standardized in RFC 2784. It was designed to encapsulate a wide variety of network layer packets inside IP tunneling packets. The original packet is the payload for the final packet. The protocol is used on the Internet to secure virtual private networks.

# Inventory and Information Model Objects (IMOs)

This section includes the following tables:

# IP Interface

The following network layer IP Interface object, which represents the IP level functionality of an interface configuration in a network element, is primarily bound by its Containing Termination Points attribute to a Data Link Layer Interface object, and is primarily accessed by a Routing Entity.

*Table 2-1 IP Interface (IIPInterface)*

| Attribute Name | Attribute Description |
|---|---|
| IP Address | Primary IP address |
| Subnetwork Mask | Primary IP subnetwork mask |
| IP Interface Addresses | Array of all IP Interface Addresses |
| Interface Name | Interface name |
| Interface Description | Interface description |
| IP Interface State | IP interface state (*Unknown, Up, Down*) |
| OSPF Interface Cost | 2x10^9/<interface speed in BPS> |
| MTU | Maximum transmit units |
| Lookup Method | Lookup method (*Route Table First*, *Host Table First*) |
| Address Resolution Type | Address resolution type/s |
| ARP Timeout | ARP table entry aging timeout |
| Secured ARP | Secured ARP settings (*Enable*, *Disable*) |
| ICMP Mask Reply | Control message mask reply |
| IGMP Proxy | Group management proxy |
| HSRP Groups | Arrays of Hot Standby Router Protocol (HSRP) Group Entry (valid only for Cisco routers that implement HSRP) |
| IP Multiplexing Table | Array of IP Multiplexing Entries |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# IP Multiplexer Entry

The following IP Multiplexer Entry object, of the IP Multiplexing Table of an IP Interface object, is used when an IP Interface is bound to multiple Virtual Connection based Data Link layer interfaces such as ATM Interface and Frame Relay Interface in order to map a Destination IP Subnet with a specific Virtual Connection.

*Table 2-2 IP Multiplexer Entry (IIPMuxEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Termination Point | Virtual data link layer encapsulation |
| Destination IP Subnet | Destination IP subnet |

# IP Interface Address

The following IP Interface Address object describes one of possible multiple IP Addresses along with their Subnetwork Masks assigned to an IP Interface, using an IP Subnetwork object, and whether it is the Primary or a Secondary one.

*Table 2-3 IP Interface Address (IIPInterfaceAddress)*

| Attribute Name | Attribute Description |
|---|---|
| Type | IP address type (*Primary*, *Secondary*) |
| IP Subnet | IP subnetwork |

# IP Subnetwork

The following IP Subnetwork type (not an IMO object) describes an IP Subnetwork Address (with the host part being zeroed) or alternatively a Host IP Address along with the IP Subnetwork Mask.

*Table 2-4 IP Subnetwork (IPSubnet)*

| Attribute Name | Attribute Description |
|---|---|
| IP Address | IP address |
| Subnetwork Mask | IP subnetwork mask |

# Routing Entity

The following Routing Entity object describes the routing and address resolution protocols independent forwarding component of an IP router, which is bound by its Logical Sons attribute to all Network layer IP Interface objects, which IP Packets are being routed between, by this Routing Entity.

*Table 2-5 Routing Entity (IRoutingEntity)*

| Attribute Name | Attribute Description |
|---|---|
| Routing Table | Array of Equivalent (Shared Destination) Routing Entries |
| ARP Entity | Address resolution entity (ARP Entity) |
| Routing Table Changes | Routing table changes count |
| Name | Routing entity name |
| Logical Sons | Array of all IP Interfaces which IP packets are being routed between, by this Routing Entity |

# Equivalent Routing Entry

The following Equivalent Routing Entry and Routing Entry objects describe a routing table's entries, each as an array of routing entries sharing a single IP Subnetwork destination. Based on their protocol type some of the device's routing table's entries, which are not relevant to the IMO model, may not be presented in this table structure.

*Table 2-6 Equivalent Routing Entry (IRoutingEntries)*

| Attribute Name | Attribute Description |
|---|---|
| Routing Entries | Array of Routing Entries (sharing a single destination) |

# Routing Entry

*Table 2-7 Routing Entry (IRoutingEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Destination IP Subnet | Final destination IP subnet |
| Next Hop IP Address | Next hop IP address |
| Type | Route entry type (*Null*, *Other*, *Invalid*, *Direct*, *Indirect*, *Static*) |
| Routing Protocol Type | Routing protocol type (*Null, Other, "Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN SPF IGP, OSPF, BGP, EIGRP*) |
| Outgoing Interface Name | Outgoing IP interface name |

# ARP Entity

The following ARP Entity object describes a routing domain wide Internet Protocol (IP) address to Media Access Control (MAC) Address Resolution Protocol Entity.

*Table 2-8 ARP Entity (IARPEntity)*

| Attribute Name | Attribute Description |
|---|---|
| ARP Table | Array of ARP Entries |

# ARP Entry

The following ARP Entry object describes a routing domain wide Internet Protocol (IP) address to Media Access Control (MAC) Address Resolution Protocol Table's Entry.

*Table 2-9 ARP Entry (IARPEntry)*

| Attribute Name | Attribute Description |
|---|---|
| IP Address | Internet Protocol (IP) address |
| MAC Address | Media Access Control (MAC) address |

*Table 2-9 ARP Entry (IARPEntry) (continued)*

| Attribute Name | Attribute Description |
|---|---|
| Port | Data link layer (MAC) interface |
| Entry Type | ARP entry type (*Null, Other, Invalid, Dynamic, Static*) |

# IP Address Pool

The following IP Address Pool with its IP Range Based Address Pool Entry and IP Subnet Based Address Pool Entry objects describe an IP Address Pool of a Gateway/Router device for distribution to local and remote parties by protocols such as DHCP and IPCP.

*Table 2-10 IP Address Pool (IIPPool)*

| Attribute Name | Attribute Description |
|---|---|
| IP Address Pool Entries | Array of IP Range Based Address Pool Entries or IP Subnet Based Address Pool Entries |
| Name | IP addresses pool name |
| Index | IP addresses pool index |

# IP Range Based Address Pool Entry

*Table 2-11 IP Range Based Address Pool Entry (IIPRangeBasedIPPoolEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Start IP Address | Start IP address of the IP address pool |
| End IP Address | End IP address of the IP address pool |
| Unused Addresses | Unused addresses count |
| Used Addresses | Used addresses count |
| Reserved Addresses | Reserved addresses count |

# IP Subnet Based Address Pool Entry

*Table 2-12 IP Subnet Based Address Pool Entry (IIPSubnetBasedIPPoolEntry)*

| Attribute Name | Attribute Description |
|---|---|
| IP Subnet | IP Subnetwork of the IP address pool |
| Unused Addresses | Unused addresses count |
| Used Addresses | Used addresses count |
| Reserved Addresses | Reserved addresses count |

# Hot Standby Router Protocol (HSRP) Group Entry

The following Cisco Specific Hot Standby Router Protocol (HSRP) Group Entry object, describes both the configuration and the outcome information of running this protocol within a group (two) of routers, connected to the same segment of Ethernet networks for providing backup to a router in the event of failure, by presenting an appearance of a single **virtual router** with a single set of IP and MAC addresses on that **Local Area Network (LAN)**.

*Table 2-13 Hot Standby Router Protocol (HSRP) Group Entry (IHSRPGroupEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Group Number | Group number |
| Port Description | Port description |
| Priority | Priority from *0* (*Lowest*) to *255* (*Highest*) used for active router selection |
| Coupled Router | Coupled active or standby router IP address (as the group is implemented by only two routers) |
| State | Protocol state (*Disabled, Initial, Learn, Listen, Speak, Standby, Active*) |
| Virtual IP Address | Virtual IP address used by this group |
| Virtual MAC Address | Virtual MAC address used by this group |

# Generic Routing Encapsulation (GRE) Tunnel Interface

The following network layer Generic Routing Encapsulation (GRE) Tunnel Interface object, which represents a GRE Tunnel interface configuration in a network element, is primarily accessed by an IP Interface bound by its Contained Connection Termination Points attribute.

*Table 2-14 Generic Routing Encapsulation (GRE) Tunnel Interface (ITunnelGRE)*

| Attribute Name | Attribute Description |
|---|---|
| Name | Tunnel name |
| Tunnel Destination and Source | Tunnel destination and source IP addresses |
| IP Address | Primary IP address |
| IP Interface State | IP interface state (*Unknown, Up, Down*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Network Topology

The discovery of the Internet Protocol (IP) network layer is unsupported.

However, IP addresses and subnets are used for signature/test for the underlying **MPLS** and **PPP** layers topology discovery by searching for the existence of the local IP Address in any one hop away remote side's routing table. For more information see Chapter 12, "Multiprotocol Label Switching "MPLS"" and Chapter 8, "Point-to-Point Protocol "PPP" and High Level Data Link Control "HDLC"".

In particular, a comparison is made between the local and remote IP Addresses of IP Interfaces found under the same subnet.

# Service Alarms

The following alarms are supported for this technology:

- All IP Interfaces Down/IP Interface Up
- GRE Tunnel Down/GRE Tunnel Up
- IP Interface Down/IP Interface Up
- HSRP Group Member Not Active/HSRP Group Member Active

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 3

# Routing Protocols "BGP/OSPF"

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



## Technology Description

### BGP

The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet Service Providers (ISP). Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as RIP or OSPF for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between Autonomous Systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

BGP is a very robust and scalable routing protocol, as evidenced by the fact that BGP is the routing protocol employed on the Internet. To achieve scalability at this level, BGP uses many route parameters, called attributes, to define routing policies and maintain a stable routing environment. BGP neighbors exchange full routing information when the TCP connection between neighbors is first established. When changes to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and BGP routing updates advertise only the optimal path to a destination network.

## MP-BGP

The Multi-Protocol BGP feature adds capabilities to BGP to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems. That is, multi-protocol BGP is an enhanced BGP that carries IP multicast routes. BGP carries two sets of routes, one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by the Protocol Independent Multi-cast (PIM) to build data distribution trees.

## OSPF

Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks by the Interior Gateway Protocol (IGP) working group of the Internet Engineering Task Force (IETF). It was derived from several research efforts, which among other includes the early version of OSI's Intermediate System to Intermediate System (IS-IS) routing protocol.

OSPF has two primary characteristics. The first is that the protocol is open, which means that its specification is in the public domain (RFC 1247). The second principal characteristic is that OSPF is based on the Shortest Path First (SPF) algorithm, which sometimes is referred to as the Dijkstra algorithm, named for the person credited with its creation.

OSPF is a link-state routing protocol that calls for the sending of Link-State Advertisements (LSAs) to all other routers within the same hierarchical area. Information on attached interfaces, metrics used, and other variables are included in OSPF LSAs. As OSPF routers accumulate link-state information, they use the SPF algorithm to calculate the shortest path to each node.

# Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- BGP Neighbor Entry (IBgpNeighbourEntry)
- OSPF Entry (IOspfEntry)

## BGP Neighbor Entry

The following BGP Neighbor Entry object describes both the configuration and the outcome information of running the Border Gateway Protocol (BGP) within a group of participating routers within a BGP Neighborhood. It contains information about the connection with a remote BGP peer. It is the entry of the BGP Neighbors Table attribute of the Multi Protocol BGP Entity object (see Virtual Private Networks "VPNs"), representing the BGP routing service concept in the IMO.

***Table 3-1 BGP Neighbor Entry (IBgpNeighbourEntry)***

| Attribute Name | Attribute Description |
|---|---|
| Remote Identifier | Identifier of the remote peer (*IP Address*) |
| Neighbor Type | Neighbor type (*Null, Client, Non Client)* |
| Distributing Interface | Distributing IP interface |
| Remote Address | Remote peer IP address |
| Remote Autonomous System | Remote peer autonomous system |

*Table 3-1 BGP Neighbor Entry (IBgpNeighbourEntry) (continued)*

| Attribute Name | Attribute Description |
|---|---|
| Status | Status (*Null, Idle, Connect, Active, Open Sent, Open Confirm, Established*) |
| Hold Time | Established hold time in seconds |
| Keep Alive Time | Established keep alive time in seconds |

## OSPF Entry

The following OSPF Entry object describes both the configuration and the outcome information of running a single Open Shortest Path First (OSPF) protocol interface within a group of participating OSPF routers and it is aggregated by a Traffic Descriptor Container object (see Common (Shared by Several)).

*Table 3-2 OSPF Entry (IOspfEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Area Identifier | Area identification (*IP Address*) |
| IP Address | IP address |
| Type | OSPF type (*Null, Broadcast, NBMA, Point-to-Point, Point-to-Multipoint*) |
| Administrative Status | Administrative status (*Null, Enabled, Disabled*) |
| Operational Status | Operational status (*Null, Down, Loop Back, Waiting, Point-to-Point, Designated Router, Backup Designated Router, Other Designated Router*) |

# Network Topology

The discovery of Border Gateway Protocol (BGP) Neighborhood topology is done by comparing BGP router parameters on either side of potential BGP neighbors. In particular a comparison is made between the local and remote BGP router identification and autonomous system as well as the connection states on both sides.

# Service Alarms

The following alarms are supported for this technology:

- BGP Neighbor Loss/BGP Neighbor Found
- BGP Process Down/BGP Process Up

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 4

# Ethernet (IEEE 802™.3)

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



## Technology Description

### Ethernet

Ethernet refers to the family of Local Area Network (LAN) products covered by the IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol. Three data rates are currently defined for operation over optical fiber and twisted-pair cables: 10Base-T Ethernet (10Mbps), Fast Ethernet (100Mbps), Gigabit Ethernet (1000Mbps) and 10-Gigabit Ethernet (10Gbps).

The IEEE 802.3 standard provides both Media Access Control (MAC) (Layer 2), with Addressing, Duplexing, Differential Services and Flow Control attributes, and various Physicals (Layer 1) definitions, with Media, Clocking and Speed attributes. In addition, it provides a Link Aggregation (LAG) (aka Ethernet Channel) for providing both higher link capacity and availability.

### LAG

A Link Aggregation (LAG) is a group of two or more network links bundled together to appear as a single link based on IEEE 802.3ad standard. For instance, bundling two 100Mbps network interfaces into a single link creates one 200Mbps link. A LAG may include two or more network cards and two or more cables, but the software sees the link as one logical link.

A LAG provides capacity increase, load balancing and higher link availability, which prevents the failure of any single component link leading to a disruption of the communications between the interconnected devices.

# Carrier Ethernet

A Carrier Ethernet is a computer network based on the Ethernet standards covering a metropolitan area. It is commonly used as a metropolitan access network to connect subscribers and businesses to a Wide Area Network, such as the Internet. Large businesses can also use Carrier Ethernet to connect branch offices to their Intranets.

A typical service provider Carrier Ethernet network is a collection of Layer 2 or 3 switches or routers connected through optical fiber. The topology could be a ring, hub-and-spoke (star), full mesh or partial mesh. The network will also have a hierarchy; core, distribution and access. The core in most cases is an existing IP/MPLS backbone.

Ethernet on the MAN can be used as pure Ethernet, Ethernet over SDH, Ethernet over MPLS or Ethernet over DWDM. Pure Ethernet-based deployments are cheap but less reliable and scalable, and thus are usually limited to small scale or experimental deployments. SDH-based deployments are useful when there is an existing SDH infrastructure already in place, its main shortcoming being the loss of flexibility in bandwidth management due to the rigid hierarchy imposed by the SDH network. MPLS based deployments are costly but highly reliable and scalable, and are typically used by large service providers.

See also:

- Spanning Tree Protocol “STP”
- QinQ (IEEE802.1ad)

## Spanning Tree Protocol “STP”

STP is a Layer 2 link management protocol that provides path redundancy while preventing undesirable loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two devices.

STP defines a tree with a root bridge and a loop-free path from the root to all network devices in the Layer 2 network. STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the STP algorithm recalculates the spanning tree topology and activates the standby path.

STP modeling in Cisco ANA 3.6 supports devices that use the following STP variants:

- STP as defined in the 802.1D standard
- RSTP as defined in the 802.1w standard
- PvSTP and PvSTP+ which are Cisco proprietary protocols, or any per VLAN spanning tree protocol
- MST as defined in the 802.1s standard

## QinQ (IEEE802.1ad)

QinQ (IEEE802.1) tagging (namely, dot1q tunneling) is a technology that allows the nesting of an additional VLAN tag on a packet, in addition to an existing one. Either VLAN tag is an 802.1Q header by standard.

QinQ allows service providers to use a single VLAN to support customers who have multiple VLANs. The core service-provider network carries traffic with double-tagged, stacked VLAN (802.1Q-in-Q) headers of multiple customers while maintaining the VLAN and Layer 2 protocol configurations of each customer and without impacting the traffic of other customers.

For more information about QinQ in Cisco ANA 3.6 see QinQ (IEEE802.1ad).

# Inventory and Information Model Objects (IMOs)

This section includes the following tables:



## Link Aggregation Group

The following Data Link layer Link Aggregation Group object aggregates multiple Ethernet Interfaces, which it is bound to by its Containing Termination Points attribute, and is primarily accessed by the Virtual LAN Multiplexer bound by its Contained Connection Termination Points attribute. It is also being accessed by Bridging Entity.

***Table 4-1 Link Aggregation Group (ILinkAggregationGroup802dot3ad)***

| Attribute Name | Attribute Description |
|---|---|
| Group Number | Group identification of the aggregated ethernet interfaces |
| Bandwidth | Accumulated bandwidth of all aggregated ethernet interfaces in Mbps |
| Aggregation Protocol | Aggregation protocol (*None, LACP, PAGP*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (Ethernet Interface) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Link Aggregation Group Port Entry

The following Link Aggregation Group Port Entry object describes the Link Aggregation Control configuration parameters for each Aggregation Port of a Link Aggregation Group.

*Table 4-2 Link Aggregation Group Port Entry (ILagPortEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Actor and Partner Administrative Keys | Actor and partner administrative keys |
| Actor and Partner Operational Keys | Actor and partner operational keys |
| Selected and Attached Aggregation Identification | Selected and attached aggregation identification |
| Actor Port | Actor port |
| Actor Port Priority | Actor port priority |
| Partner Administrative and Operational Port | Partner administrative and operational port |
| Partner Administrative and Operational Port Priority | Partner administrative and operational port priority |
| Actor and Partner Administrative States | Actor and partner administrative states () |
| Actor and Partner Operational States | Actor and partner operational states () |

# Ethernet Interface

The following Data Link layer Ethernet Interface object, is bound by its Containing Termination Points attribute to a Physical Layer Interface (Ethernet Physical) object, and is primarily being accessed by Virtual LAN Multiplexer/Interface, Link Aggregation Group, Cisco's Ethernet Channel and/or IP Interface, bound by its Contained Connection Termination Points attribute. It is also being accessed by Bridging Entity.

*Table 4-3 Ethernet Interface (IEthernet)*

| Attribute Name | Attribute Description |
|---|---|
| MAC Address | Media Access Control (MAC) address |
| Duplex Mode | Duplex mode (*Unknown, Full, Half*) |
| Output Flow Control | Output flow control (*Enable, Disable*) |
| Input Flow Control | Input flow control (*Enable, Disable*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Point |

# Ethernet Physical

The following Physical layer Ethernet Physical object, is bound by its Containing Termination Points attribute to a Port Connector object, and is being accessed by Data Link layer Ethernet Interface bound by its Con-tained Connection Termination Points attribute.

*Table 4-4 Ethernet Physical (IPhysicalLayer)*

| Attribute Name | Attribute Description |
|---|---|
| Same as **Physical Layer** (*IPhysicalLayer*) | |

# Virtual LAN Interface

The following Data Link layer Virtual LAN Interface object, which used in a Switched LAN environ-ment, is bound by its Containing Termination Points at-tribute to an Ethernet Interface object, and is primarily being accessed by Network layer such IP Interface, bound by its Contained Connection Termination Points attribute. It is also being accessed by Bridging Entity.

*Table 4-5 Virtual LAN Interface (IVlanInterface)*

| Attribute Name | Attribute Description |
|---|---|
| Mode | Virtual LAN mode (*Access, Trunk, 802.1Q Tunnel*) |
| Native VLAN Identification | Virtual LAN identification, used for untagged received and transmitted frames |
| Virtual LAN Table | Array of Virtual LAN Entries |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Virtual LAN Entry

The following Virtual LAN Entry object describes association of a Virtual LAN Interface, which operate in Trunk mode, to one of the bridged Virtual LANs configured in the device.

*Table 4-6 Virtual LAN Entry (IVlanEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Identification | Virtual LAN identification of received and transmitted frames |
| Encapsulation Type | Virtual LAN encapsulation (*Unknown, ISL, IEEE 802.10, IEEE 802.1Q*) |
| Upper Layer | Upper layer Object Identification (OID) |

# Virtual LAN Multiplexer

The following Virtual LAN Multiplexer object, which used in a routed LAN environment, is bounded by its Containing Termination Points attribute to an Ethernet Interface object, and is primarily being accessed by Data Link layer Virtual LAN Encapsulations, bound by its Contained Connection Termination Points attribute.

*Table 4-7 Virtual LAN Multiplexer (IVlanEncapMux)*

| Attribute Name | Attribute Description |
|---|---|
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (Ethernet Interface) |
| Contained Connection Termination Points | Bound Connection Termination Points (Virtual LAN Encapsulations) |

# Virtual LAN Encapsulation

The following Data Link layer Virtual LAN Encapsulation object, which used in a routed LAN environment, is bound by its Containing Termination Points at-tribute to a Virtual LAN Multiplexer object, and is primarily being accessed by Network layer such IP Interface, bound by its Contained Connection Termination Points attribute. It is also being accessed by Bridging Entity.

*Table 4-8 Virtual LAN Encapsulation (IIEEE802)*

| Attribute Name | Attribute Description |
|---|---|
| VLAN Identification | Virtual LAN identification |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Point |

# Data Link Aggregation Container

The following Data Link Aggregation Container object aggregates or contains a single type of Data Link Aggregations such as Link Aggregation Group and Cisco's Ethernet Channel.

*Table 4-9 Data Link Aggregation Container (IDataLinkAggregationContainer)*

| Attribute Name | Attribute Description |
|---|---|
| Data Link Aggregations | Array of a single type data link aggregations (Link Aggregation Group/Cisco's Ethernet Channel) |
| Type | Aggregation type (*Null, Ethernet Link Aggregator*) |

# Spanning Tree Protocol Service

The following Spanning Tree Protocol Service object, which is used in a switched LAN environment, describes the Spanning Tree Protocol service and is accessed only by the Logical Root's Services List attribute.

*Table 4-10 Spanning Tree Protocol Service (IStpService)*

| Attribute Name | Attribute Description |
|---|---|
| Protocol Type | Spanning tree protocol type (*Unknown, STP, RSTP, PVSTP, MST*) |
| Current and Bridge Maximum Age | The current used value and the value that all bridges should used when this bridge is acting as the root for maximum age of learned spanning tree protocol port information (in hundredths of seconds) |
| Current and Bridge Hello Time | The current used value and the value that all bridges should used when this bridge is acting as the root for hello time messages' keep alive interval of a spanning tree protocol root (in hundredths of seconds) |
| Current and Bridge Forward Delay | The current used value and the value that all bridges should used when this bridge is acting as the root for port delay in each of the listening and learning states, preceding the forwarding one (in hundredths of seconds) |
| Instance Information Table | Array of Spanning Tree Protocol Instance Information |
| Same as **System Service** (*ISystemService*) | |

# Multiple Spanning Tree Protocol Service

The following Multi Spanning Tree Protocol Instance Information object, which is used in a switched Virtual LAN environment, describes the Spanning Tree Protocol service and is accessed only by the Logical Root's Services List attribute.

*Table 4-11 Multiple Spanning Tree Protocol Service (IMstService)*

| Attribute Name | Attribute Description |
|---|---|
| Protocol Properties | Multiple spanning tree protocol properties |
| Same as **Spanning Tree Protocol Service** (*IStpService*) | |

# Multiple Spanning Tree Protocol Properties

The following Multiple Spanning Tree Protocol Properties object, which is used in a switched Virtual LAN environment, describes the Multiple Spanning Tree Protocol properties and is accessed only by the Multiple Spanning Tree Protocol Service's Protocol Properties attribute.

*Table 4-12 Multiple Spanning Tree Protocol Properties (IMstProperties)*

| Attribute Name | Attribute Description |
|---|---|
| Force Version | Force version (*Unknown, STP, RSTP, PVSTP, MST*) |
| Configuration Format, Region Name and Revision Level | Configuration format, region name and revision level used by this device and is negotiated with other device |
| External Root Cost | External root cost of this multi spanning tree protocol |
| Maximum Instances | Maximum multi spanning tree protocol instances |

# Spanning Tree Protocol Instance Information

The following Rapid Spanning Tree Protocol Instance Information objects describes the Instance Information associated and accessed by the Multiple Spanning Tree Protocol Service's Instance Information Table attribute.

*Table 4-13 Spanning Tree Protocol Instance Information (IStpInstanceInfo)*

| Attribute Name | Attribute Description |
|---|---|
| Object Identification | Instance Object Identification (Object ID) |
| Identification | Bridge identification (MAC address) |
| Priority | Bridge priority in the spanning tree protocol |
| Designated Root and Bridge | MAC Addresses of the designated root and bridge in the spanning tree |
| Root Cost | Root cost value for this bridge |
| Is Root | Is this bridge currently the root of the spanning tree protocol (*True, False*) |

*Table 4-13 Spanning Tree Protocol Instance Information (IStpInstanceInfo) (continued)*

| | |
|---|---|
| Root Port Identification | Object Identification (OID) of the bridge's port used to reach the designated root |
| Port Information Table | Array of Spanning Tree Protocol Port Information |

# Multi Spanning Tree Protocol Instance Information

*Table 4-14 Multi Spanning Tree Protocol Instance Information (IMstInstanceInfo)*

| Attribute Name | Attribute Description |
|---|---|
| Instance Identification | Multi spanning tree protocol instance identification |
| Same as **Spanning Tree Protocol Instance Information** (*IStpInstanceInfo*) | |

# Per Virtual LAN Spanning Tree Protocol Instance Information

*Table 4-15 Per Virtual LAN Spanning Tree Protocol Instance Information (IPvstpInstanceInfo)*

| Attribute Name | Attribute Description |
|---|---|
| Protocol Type | Spanning tree protocol type (*Unknown, STP, RSTP, PVSTP, MST*) |
| Current and Bridge Maximum Age | The current used value and the value that all bridges should used when this bridge is acting as the root for maximum age of learned spanning tree protocol port information (in hundredths of seconds) |
| Current and Bridge Hello Time | The current used value and the value that all bridges should used when this bridge is acting as the root for hello time messages' keep alive interval of a spanning tree protocol root (in hundredths of seconds) |
| Current and Bridge Forward Delay | The current used value and the value that all bridges should used when this bridge is acting as the root for port delay in each of the listening and learning states, preceding the forwarding one (in hundredths of seconds) |
| Same as **Spanning Tree Protocol Instance Information** (*IStpInstanceInfo*) | |

# Rapid Spanning Tree Protocol Instance Information

*Table 4-16 Rapid Spanning Tree Protocol Instance Information (IRstpInstanceInfo)*

| Attribute Name | Attribute Description |
|---|---|
| Force Version | Force version (*Unknown, STP, RSTP, PVSTP, MST*) |
| Same as **Spanning Tree Protocol Instance Information** (*IStpInstanceInfo*) | |

## Spanning Tree Protocol Port Information

The following Spanning Tree Protocol Port Information objects describes the Port Information associated and accessed by the Spanning Tree Protocol Instance Information's Port Information Table attribute.

*Table 4-17 Spanning Tree Protocol Port Information (IStpPortInfo)*

| Attribute Name | Attribute Description |
|---|---|
| Object Identification | Port object identification (Object ID) |
| Priority | Port priority in the spanning tree protocol |
| State | Port state (*Unknown, Disable, Blocking, Listening, Learning, Forwarding, Broken, Down, LoopBack*) |
| Path Cost | Port path cost, which represents the media speed for this port |
| Is Edge | Is this an edge (connected to a nonbridging device) Port (*True, False*) |
| Is Point To Point | Is this port connected to n point to point link (*True, False*) |
| Role | Port role (*Unknown, Disable, Backup, Alternative, Designated, Root, Boundary*) |

## Multi Spanning Tree Protocol Port Information

*Table 4-18 Multi Spanning Tree Protocol Port Information (IMstPortInfo)*

| Attribute Name | Attribute Description |
|---|---|
| Hello Time | Hello time messages' keep alive interval of a spanning tree protocol root (in hundredths of seconds) |
| Same as **Spanning Tree Protocol Port Information** (*IStpPortInfo*) | |

# Vendor Specific Inventory and Information Model Objects

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

The following section describes the object of a specific vendor:

- Cisco's Ethernet Channel

## Cisco's Ethernet Channel

Cisco's Ethernet Channel Data Link layer object aggregates multiple Ethernet Interfaces, which it is bound to by its Containing Termination Points attribute, and is primarily accessed by Virtual LAN Multiplexer/Interface and/or IP Interface, bound by its Contained Connection Termination Points attribute. It is also accessed by Bridging Entity.

*Table 4-19 Cisco's Ethernet Channel (IEthernetChannel)*

| Attribute Name | Attribute Description |
|---|---|
| Group Number | Group identification of the aggregated ethernet interfaces |
| Bandwidth | Accumulated bandwidth of all aggregated ethernet interfaces in Mbps |
| Aggregation Protocol | Aggregation protocol (*None, LACP, PAGP*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (Ethernet Interface) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# QinQ (IEEE802.1ad)

For IMO information see Inventory and Information Model Objects (IMOs).

## Opening Cisco ANA PathTracer Over Networks

You can open and view PathTracer information between service endpoints (for example, the IP interface) over a network. In order to view a specific path you must specify an initial point like an IP interface and a destination IP address. When the user selects an endpoint the system extracts the relevant IP address from this point and uses it as the destination. For QinQ the path is run from any:

- Router or switch which is part of the carrier ethernet domain with Dot1q and QinQ configuration
- IP destination which can be reached from that point of the network

## PathTracer Starting Points

The user can also enter the required destination IP address after opening the Cisco ANA PathTracer from the right-click shortcut menu. The table below describes the starting points available in the shortcut menu in order to open the PathTracer:

*Table 4-20 PathTracer Starting Points*

| Element | Location | Start PathTracer Options |
|---|---|---|
| IP Interface | Inventory window | • to IP Destination<br>• Start Here |

For information on opening the Cisco ANA PathTracer from the Inventory window as a starting point, see the Cisco Active Network Abstraction NetworkVision User Guide.

# PathTracer Endpoints

If you selected the "**Start Here**" option the following endpoints can be selected as a path destination to open the PathTracer:

*Table 4-21 PathTracer Endpoints*

| Element | Location | Start PathTracer Options |
|---|---|---|
| IP Interface | Inventory window | End Here |

The Cisco ANA PathTracer Multi-Path window is displayed. From this window you can open the Cisco ANA PathTracer Single-Path window with the appropriate QinQ information displayed in the **Layer 2** tab.

# Using Cisco ANA PathTracer to View Path Information

This section describes the Cisco ANA PathTracer for Dot1q and QinQ. For detailed information about the Cisco ANA PathTracer, see the Cisco Active Network Abstraction NetworkVision User Guide.

Cisco ANA uses the VLAN tags of the Ethernet header and the port configuration to trace the path from one interface to another over the network. The Cisco ANA's PathTracer tool enables you to:

- View a Layer 2 path across a LAN domain with all the VLAN tags' information
- For each network element view the relevant parameters for each interface on all layers along the path.

Layer 2 Dot1q and QinQ information is displayed in the Cisco ANA PathTracer windows when a path is traced over Ethernet ports with Dot1q and a QinQ configuration.

## Layer 2

The following Layer 2 properties that may be displayed in the **Layer 2** tab relate specifically to QinQ and VLAN port configuration:

- VLAN Mode—The work mode for the interface, namely, Unknown, Access, Trunk, Dot1QTunnel.

  **Note** Trunk mode refers to multiple tagging too.

- Native VLAN ID—The VLAN ID that is used to tag untagged traffic received on a trunked interface. The default native VLAN ID is '1' if VLAN tagging is enabled. The native VLAN ID is '0' or 'no VLAN ID' if VLAN tagging is disabled.
- CE VLAN ID—The customer edge device's VLAN ID.
- SP VLAN ID—The service provider's VLAN ID.

## Layer 3

There are no Layer 3 properties that relate specifically to QinQ.

# Network Topology

The discovery of Ethernet Data Link layer topology is done by searching for the existence of the local MAC Address in any remote side's bridge or Address Resolution Protocol (ARP) tables related to the same type of the local Ethernet port. The basic assumption, which is not always valid, is that every Ethernet port has a unique MAC Address. This topology is also applied to the underlying physical links.

Further verification is done by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial traffic amount in order to function correctly.

There is no topology based on STP or QinQ technology in Cisco ANA 3.6.

**Note** See CSCsi65238 which describes the potential problems in topology discovery in QinQ scenarios.

# Service Alarms

The following alarms are supported for this technology:

- Cloud Problem
- Discard Input Packets/Normal Discard Input Packets
- Dropped Output Packets/Normal Dropped Output Packets
- Link Down/Link Up
- Port Down/Port Up
- Receive Utilization/Receive Utilization Normal
- Transmit Utilization/Transmit Utilization Normal

**Note** Note that these alarms, apart from the Cloud Problem, are related to the underlying Physical Interface (Common section).

There are no alarms based on STP or QinQ technology in Cisco ANA 3.6, however correlation takes into account these technologies when performing flow analysis.

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 5

# Token Ring "TR" (IEEE 802™.5)

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



## Technology Description

### Token Ring

Token Ring refers to a Local Area Network (LAN) products covered by the IEEE 802.5 standard that unlike Ethernet, uses a ring topology whereby the data is sent from one station to the next and so on around the ring until it ends up back where it started, with a control token circulating around the ring controlling access.

The IEEE 802.5 standard provide both Media Access Control (MAC) (Layer 2), with Addressing, Access and Flow Control attributes, and various Physicals (Layer 1) definitions, with Media, Clocking and Speed attributes.

## Inventory and Information Model Objects (IMOs)

This section includes the following tables:

## Token Ring Interface

The following Data Link layer Token Ring Interface object, is bound by its Containing Termination Points attribute to a Physical Layer Token Ring Physical object, and is primarily being accessed by Network layer such IP Interface, bound by its Contained Connection Termina-tion Points attribute. It is also being accessed by Bridging Entity.

*Table 5-1 Token Ring Interface (ITokenRingLayer2)*

| Attribute Name | Attribute Description |
|---|---|
| MAC Address | Media Access Control (MAC) address |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

## Token Ring Physical

The following Physical layer Token Ring Physical object, is bound by its Containing Termination Points attribute to a Port Connector object, and is accessed solely by the Data Link layer Token Ring Interface bound by its Contained Connection Termination Points attribute.

*Table 5-2 Token Ring Physical (ITokenRingLayer1)*

| Attribute Name | Attribute Description |
|---|---|
| Same as **Physical Layer** (*IPhysicalLayer*) | |

# Network Topology

The discovery of Token Ring (TR) Data Link layer topology is unsupported and is manually (statically) configured by the system administrator.

# Service Alarms

The following alarms are supported for this technology:

- Cloud Problem
- Discard Input Packets/Normal Discard Input Packets
- Dropped Output Packets/Normal Dropped Output Packets
- Link Down/Link Up
- Port Down/Port Up
- Receive Utilization/Receive Utilization Normal
- Transmit Utilization/Transmit Utilization Normal

**Note** Note that these alarms, apart from the Cloud Problem, are related to the underlying Physical Interface (Common section).

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 6

# Asynchronous Transfer Mode "ATM"

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



## Technology Description

### ATM

ATM is a cell-switching and multiplexing technology that combines the benefits of circuit switching (guaranteed capacity and constant transmission delay) with those of packet switching (flexibility and efficiency for intermittent traffic). It provides Data Link (Layer 2) services with scalable bandwidth from a few megabits per second (Mbps) to many gigabits per second (Gbps), which usually run over Synchronous Optical NETwork/Digital Hierarchy (SONET/ SDH) Physical (Layer 1) links.

ATM networks consist of ATM switches interconnected by point-to-point ATM links or Interfaces and are fundamentally connection-oriented, which means that a virtual channel (VC) must be set up across the ATM network prior to any data transfer.

### IMA

Inverse Multiplexing over ATM (IMA) involves inverse multiplexing and demultiplexing of ATM cells in a cyclical fashion among physical links grouped to form a higher bandwidth and logical link. The rate of the logical link is approximately the sum of the rate of the physical links in the IMA group. Streams of cells are distributed in a round-robin manner across the multiple T1/E1 links and reassembled at the destination to form the original cell stream. Sequencing is provided using IMA Control Protocol (ICP) cells.

The ATM cell stream received from the ATM layer is distributed on a cell by cell basis across the multiple links within the IMA group. At the far end, the receiving IMA unit reassembles the cells from each link on a cell-by-cell basis and recreates the original ATM cell stream and passed to the ATM layer.

# Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- ATM Interface (IAtm)
- ATM Virtual Connection (IAtmVc)
- Inverse Multiplexing for ATM (IMA) Group (IIMAGroup)
- ATM Traffic Descriptor (IAtmTrafficDescriptor)
- ATM Traffic Shape Descriptor (IAtmTrafficShapingDescriptor)

## ATM Interface

The following Data Link layer ATM Interface object aggregates multiple ATM Virtual Connections by its VC Table attributes. It is bound by its Containing Termination Points attribute to a Physical Layer Interface, and is primarily being accessed by the Virtual Connection Switching Entity and VC Encapsulation Multiplexer bound by its Contained Connection Termination Points attribute. It is also being accessed by Virtual Connection Switching Entity.

***Table 6-1 ATM Interface (IAtm)***

| Attribute Name | Attribute Description |
|---|---|
| ATM Address | ATM 20 byte address (*Address Prefix* \| *MAC Address* \| *Address Selector*) |
| Interface Type | ATM interface type (*N/A, Private UNI, Public UNI, Private NNI, Public NNI, NNI, UNI, STI, Unconfigured, VNNI, VUNI, EVNNI, EVUNI, VP TRUNK UNI*) |
| VP and VC Ranges | Numeric ranges of the allowed VPI/VCI values |
| VC Table | Array of ATM Virtual Connections |
| Cross Connect Table | Array of Virtual Cross Connections |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# ATM Virtual Connection

The following Data Link layer ATM Virtual Connection object, is bound by its Containing Termination Points attribute to a Data Link layer ATM Interface object, and is primarily accessed by the Virtual Cross Connection and Data Link layer VC Encapsulation, however it is not bound to any of them by any of its attributes.

*Table 6-2 ATM Virtual Connection (IAtmVc)*

| Attribute Name | Attribute Description |
|---|---|
| Virtual Channel Identifier | Virtual Channel Identifier (VCI) |
| Virtual Path Identifier | Virtual Path Identifier (VPI) |
| Shaping Profile | Shaping profile (ATM Traffic Shape Descriptor) |
| Discarded and Received Input Data Counters | Discarded and received input octets and reassembled packets counters |
| Dropped and Forward Output Data Counters | Dropped and forward output octets and reassembled packets counters |
| Ingress Traffic Descriptor | Ingress traffic descriptor (ATM Traffic Descriptor) |
| Egress Traffic Descriptor | Egress traffic descriptor (ATM Traffic Descriptor) |
| Administrative Status | Administrative status (*Unknown, Up, Down*) |
| Operational Status | Operational status (*Unknown, Up, Down*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Inverse Multiplexing for ATM (IMA) Group

The following Inverse Multiplexing for ATM (IMA) Group object, multiplex multiple Digital Signalling 1 Physicals, which it is bound to by its Containing Termination Points attribute, into a single Data Link layer ATM Interface, by which it is accessed.

*Table 6-3 Inverse Multiplexing for ATM (IMA) Group (IIMAGroup)*

| Attribute Name | Attribute Description |
|---|---|
| Description | IMA port description |
| Speed | Group aggregated speed |
| Administrative Status | Administrative status (*Unknown, Up, Down, Testing*) |
| Operational Status | Operational status (*Unknown, Up, Down, Testing, Dormant, Not Presented*) |
| Operational Status Last Change | Date of last operational status change |

*Table 6-3 Inverse Multiplexing for ATM (IMA) Group (IIMAGroup) (continued)*

| Attribute Name | Attribute Description |
|---|---|
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (Digital Signalling 1 Physicals) |

# ATM Traffic Descriptor

The following ATM Traffic Descriptor object describes traffic of a single ATM Virtual Connection, which it is being aggregated by a Traffic Descriptor Container object (see Common (Shared by Several)).

*Table 6-4 ATM Traffic Descriptor (IAtmTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Traffic Descriptor Type | ATM traffic descriptor type (*Null, Best Effort, No CLP and no SCR, CLP with no tagging and no SCR, CLP with tagging and no SCR, No CLP with SCR, CLP with no tagging and with SCR, CLP with tagging and with SCR, CLP with no tagging and with MCR, CLP-transparent with no SCR, CLP-transparent with SCR, No CLP with tagging and no SCR, No CLP and no SCR with CDVT, No CLP with SCR and CDVT, No CLP and no SCR with CDVT, No CLP with SCR and CDVT*) |
| Service Category | ATM service category (*Unknown, UBR, UBR1, UBR2, CBR, CBR1, CBR2, CBR3, ABR, RT VBR, NRT VBR, VBR, VBR1RT, VBR2RT, VBR3RT, VBR1NRT, VBR2NRT, VBR3NRT, GFR*) |
| Cell Loss Priority | Cell loss priority (*Unknown, True, False*) |
| Cell Delay Variation | Cell delay variation |
| Cell Delay Variation Tolerance | Cell delay variation tolerance |
| Maximum High Priority and Aggregate Burst Sizes | Maximum high priority and aggregate (CLP=0 and CLP=0+1) burst sizes |
| Minimum High Priority and Aggregate Cell Rates | Minimum high priority and aggregate (CLP=0 and CLP=0+1) cell rates |
| Sustainable High Priority and Aggregate Cell Rates | Sustainable high priority and aggregate (CLP=0 and CLP=0+1) cell rates |
| Peak High Priority and Aggregate Cell Rates | Peak high priority and aggregate (CLP=0 and CLP=0+1) cell rates |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

## ATM Traffic Shape Descriptor

The following ATM Traffic Shape Descriptor object describes the traffic shape of a single ATM Virtual Connection and is being aggregated by a Traffic Descriptor Container object (see Common (Shared by Several)).

*Table 6-5 ATM Traffic Shape Descriptor (IAtmTrafficShapingDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Maximum Burst Size | Maximum burst sizes |
| Sustainable and Peak Cell Rates | Sustainable and peak cell rates |
| Cell Delay Variation | Cell delay variation |
| State | Descriptor state (*Null, Enabled, Disabled*) |
| Buffer Size | Buffer size |
| Cell Loss Priority Discarded Size | Cell loss priority discarded size |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

# 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:

- Lucent's ATM Trunk Interface
- Cisco or Lucent's ATM Logical Interface
- Cisco or Lucent's ATM Trunk Virtual Connection
- Cisco or Lucent's ATM Soft Permanent Virtual Connection
- Alcatel's ASAM ATM Interface
- ECI's HiFocus ATM Interface
- Alcatel's ASAM ATM Traffic Descriptor
- ECI's HiFocus ATM Traffic Descriptor
- Lucent's WAN Switch ATM Traffic Descriptor
- Alcatel's ATM Access Traffic Descriptor
- Alcatel's ASAM Access Traffic Descriptor

## Lucent's ATM Trunk Interface

Lucent's ATM Trunk Interface Data Link layer object aggregates multiple ATM Virtual Connections, which it is bound to by its VC Table attributes. It is bound by its Containing Termination Points attribute to a Physical Layer Interface, and is primarily accessed by a Virtual Connection Switching Entity bound by its Contained Connection Termination Points attribute.

*Table 6-6 Lucent's ATM Trunk Interface (IAtmTrunk)*

| Attribute Name | Attribute Description |
|---|---|
| Same as ATM Interface (*IAtm*) - see Table 6-1 on page 6-2. | |

# Cisco or Lucent's ATM Logical Interface

Cisco or Lucent's ATM Logical Interface Data Link layer object aggregates multiple ATM Virtual Connections, which it is bound to by its VC Table attributes. It is bound by its Containing Termination Points attribute to a Physical Layer Interface, and is primarily accessed by a Virtual Connection Switching Entity and Data Link layer VC Encapsulation bound by its Contained Connection Termination Points attribute.

*Table 6-7 Cisco or Lucent's ATM Logical Interface (IAtmLogicalPort/Trunk)*

| Attribute Name | Attribute Description |
|---|---|
| Resource Management Cell Termination | Resource management cell termination (*Unknown*, *CCRM Only*, *CCRM & BCM*) |
| Resource Management Cell Generation | Resource management cell generation (*Unknown*, *None*, *CCRM*, *BCM*) |
| Effective Check | Effective check (*Unknown*, *No*, *Yes*) |
| Input and Output Capacities | Input and output capacities |
| Administrative Status | Administrative status (*Null*, *Up*, *Down*, *Testing*) |
| Operational Status | Operational status (*Null*, *Up*, *Down*, *Testing*, *Unknown*, *Dormant*, *Not Present*) |
| Same as ATM or ATM Trunk Interface - see Table 6-1 on page 6-2. | |

# Cisco or Lucent's ATM Trunk Virtual Connection

Cisco or Lucent's ATM Trunk Virtual Connection and Cisco or Lucent's ATM Soft Permanent Virtual Connection Data Link layer objects, are bound by their Containing Termination Points attributes to an ATM Interface object, and are primarily accessed by a Virtual Cross Connection object, although they are not bound to it by any of their attributes.

*Table 6-8 Cisco or Lucent's ATM Trunk Virtual Connection (IAtmTrunkVc)*

| Attribute Name | Attribute Description |
|---|---|
| Destination Description | Destination party description |
| Same as ATM Virtual Connection (*IAtmVc*) - see Table 6-2 on page 6-3. | |

# Cisco or Lucent's ATM Soft Permanent Virtual Connection

*Table 6-9 Cisco or Lucent's ATM Soft Permanent Virtual Connection (IAtmSpVc)*

| Attribute Name | Attribute Description |
|---|---|
| Remote Virtual Channel Identifier | Remote virtual channel identifier (*VCI*) |
| Remote Virtual Path Identifier | Remote virtual path iIdentifier (*VPI*) |
| Remote Network Service Access Point | Remote network service access point (*NSAP*), which is the destination ATM address |
| Same as ATM Virtual Connection (*IAtmVc*) - see Table 6-2 on page 6-3. | |

# Alcatel's ASAM ATM Interface

Alcatel's ASAM ATM Interface and ECI's HiFocus ATM Interface Data Link layer objects aggregate multiple ATM Virtual Connections, which they are bound to by their VC Table attributes. They are bound by their Containing Termination Points attributes to a Physical Layer Interface, and are primarily accessed by Virtual Connection Switching Entity and Data Link layer VC Encapsulation objects bound by their Contained Connection Termination Points attributes.

*Table 6-10 Alcatel's ASAM ATM Interface (IAsamAtm)*

| Attribute Name | Attribute Description |
|---|---|
| CAC Traffic Descriptor | Connection Admission Control (CAC) traffic descriptor (Alcatel's ASAM ATM Traffic Descriptor) |
| Access Traffic Descriptor | Access traffic descriptor (Alcatel's ASAM Access Traffic Descriptor) |
| Same as ATM Interface (*IAtm*) - see Table 6-1 on page 6-2. | |

# ECI's HiFocus ATM Interface

*Table 6-11 ECI's HiFocus ATM Interface (IHiFocusAtm)*

| Attribute Name | Attribute Description |
|---|---|
| CAC Traffic Descriptor | Connection Admission Control (CAC) traffic descriptor (ECI's HiFocus ATM Traffic Descriptor) |
| Access Traffic Descriptor | Access traffic descriptor (Alcatel's ATM Access Traffic Descriptor) |
| Same as ATM Interface (*IAtm*) - see Table 6-1 on page 6-2. | |

# Alcatel's ASAM ATM Traffic Descriptor

The following objects—Alcatel's ASAM ATM Traffic Descriptor, ECI's HiFocus ATM Traffic Descriptor, Lucent's WAN Switch ATM Traffic Descriptor and Lucent's WAN Switch ATM Traffic Descriptor describe traffic of a single ATM Virtual Connection, and are aggregated by a Traffic Descriptor Container object.

*Table 6-12 Alcatel's ASAM ATM Traffic Descriptor (IAsamAtmTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| User VP and VC Ranges | Numeric ranges of the allowed user VPI/VCI values |
| Same as ATM Traffic Descriptor (*IAtmTrafficDescriptor*) - see Table 6-4 on page 6-4. | |

# ECI's HiFocus ATM Traffic Descriptor

*Table 6-13 ECI's HiFocus ATM Interface (IHiFocusAtm)*

| Attribute Name | Attribute Description |
|---|---|
| Service Category | ATM service category (*Unspecified*) |
| Same as ATM Traffic Descriptor (*IAtmTraffic Descriptor*) - see Table 6-4 on page 6-4. | |

# Lucent's WAN Switch ATM Traffic Descriptor

*Table 6-14 Lucent's WAN Switch ATM Traffic Descriptor (ILucentWANSwitchAtmTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Priority | Connection pPriority |
| Type | Connection type |
| Same as ATM Traffic Descriptor (*IAtmTrafficDescriptor*) - see Table 6-4 on page 6-4. | |

# Alcatel's ATM Access Traffic Descriptor

Alcatel's ATM Access Traffic Descriptor object describes access traffic of a single ATM Virtual Connection, and is aggregated by a Traffic Descriptor Container.

*Table 6-15 Alcatel's ATM Access Traffic Descriptor (IAtmAccessTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Scope | Access scope (*Null*, *Local*, *Network*) |
| Maximum Active VPCs and VCCs | Maximum active virtual path and virtual channel connections |
| Maximum Supported VPI and VCI Bits | Maximum supported virtual path and virtual channel bits |
| Generic Flow Control Mode | Generic flow control mode (*Null*, *UNI*, *NNI*) |

*Table 6-15 Alcatel's ATM Access Traffic Descriptor (IAtmAccessTrafficDescriptor)*

| | |
|---|---|
| Police Mode | Police mode (*Null*, *None*, *VC Only*, *All*) |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

## Alcatel's ASAM Access Traffic Descriptor

Alcatel's ASAM Access Traffic Descriptor object describes access traffic of a single ATM Virtual Connection, and is aggregated by a Traffic Descriptor Container.

*Table 6-16 Alcatel's ASAM Access Traffic Descriptor (IAsamAccessTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Maximum Supported VPCs and VCCs | Maximum supported virtual path and virtual channel connections |
| Maximum Active VPI and VCI Bits | Maximum active virtual path and virtual channel bits |
| Same as ATM Access Traffic Descriptor (*IAtmAccessTrafficDescriptor*) - see Table 6-15 on page 6-8. | |

# Network Topology

The discovery of Asynchronous Transfer Mode (ATM) Data Link layer topology is done by searching for the same set of active ATM Virtual Connections in any remote side's ATM port VCs table related to the same type of the local ATM port. This topology is also applied to the underlying physical links.

In particular it looks for harmony between the VCs tables of participating ports based on the lowest active VCs (registry default to 3).

Further verification is done by matching the VC traffic signature of these ports using Cisco's confidential scheme, which requires a substantial traffic amount in order to function correctly.

This mechanism support configuration that have on both sides either the same VCs or the same VPs. However it does not support a mixture of VCs on one side and VPs on the other one.

# Service Alarms

The following alarms are supported for this technology:

- Cloud Problem
- Discard Input Packets/Normal Discard Input Packets
- Dropped Output Packets/Normal Dropped Output Packets
- Link Down/Link Up
- Port Down/Port Up
- Receive Utilization/Receive Utilization Normal
- Transmit Utilization/Transmit Utilization Normal

**Note** Note that these alarms, apart from the Cloud Problem, are related to the underlying Physical Interface (see Chapter 19, "Common (Shared by Several)").

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 7

# Frame Relay "FR"

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



## Technology Description

### Frame Relay

Frame Relay (FR) is a high performance variable length packets switching with statistical multiplexing Data Link (Layer 2) WAN protocol, which Although originally designed for use across Integrated Services Digital Network (ISDN) interface, today it is used over a variety of other network interfaces as well.

FR networks consist of FR switches interconnected by point-to-point FR links or Interfaces and are fundamentally connection-oriented, which means that a virtual channel (VC) must be set up across the FR network prior to any data transfer.

## Inventory and Information Model Objects (IMOs)

This section includes the following tables:

# Frame Relay Interface

The following Data Link layer Frame Relay Interface object aggregates multiple Frame Relay Virtual Connections, which it is bound to by its VC Table attributes. It is bound by its Containing Termination Points attribute to a Physical Layer Interface, and is primarily being accessed by Data Link layer VC Multiplexer, bound by its Contained Connection Termination Points attribute. It is also being accessed by Virtual Connection Switching Entity.

*Table 7-1 Frame Relay Interface (IFrameRelay/IFrTrunk)*

| Attribute Name | Attribute Description |
|---|---|
| Address Format | Frame relay address format (*Unknown, q921, q922March90, q922November90, q922*) |
| Maximum Supported VCs | Maximum supported virtual connections |
| Protocol Type | Frame relay protocol type (*Unknown, Frame Relay, FR FUNI, Frame Forward*) |
| VC Table | Array of Frame Relay Virtual Connections |
| Cross Connect Table | Array of Virtual Cross Connections |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Frame Relay Virtual Connection

The following Data Link layer Frame Relay Virtual Connection object, is bound by its Containing Termination Points attribute to a Data Link layer Frame Relay Interface object, and is primarily accessed by the Virtual Cross Connection and Data Link layer VC Encapsulation, however it is not bound to any of them by any of its attributes.

*Table 7-2 Frame Relay Virtual Connection (IFrVc)*

| Attribute Name | Attribute Description |
|---|---|
| Data Link Connection Identifier | Data Link Connection Identifier (DLCI) |
| Traffic Descriptor | Traffic descriptor (Frame Relay Traffic Descriptor) |
| Discarded and Received Input Data Counters | Discarded and received input octets and packets counters |
| Dropped and Forward Output Data Counters | Dropped and forward output octets and packets counters |
| Ingress Traffic Descriptor | Ingress traffic descriptor (Frame Relay Traffic Descriptor) |
| Egress Traffic Descriptor | Egress traffic descriptor (Frame Relay Traffic Descriptor) |
| Administrative Status | Administrative status (*Unknown, Up, Down*) |
| Operational Status | Operational status (*Unknown, Up, Down*) |
| IANA Type | IANA type of the sub/layer |

*Table 7-2 Frame Relay Virtual Connection (IFrVc) (continued)*

| Attribute Name | Attribute Description |
|---|---|
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Frame Relay Traffic Descriptor

The following Frame Relay Traffic Descriptor object describes the traffic of a single Frame Relay Virtual Connection is being aggregated by a Traffic Descriptor Container object (see Common (Shared by Several)).

*Table 7-3 Frame Relay Traffic Descriptor (IFRTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Committed Rate | Committed burst rate |
| Excess Burst Rate | Excess burst rate |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

# Frame Relay Logical Interface

The following Data Link layer Frame Relay Logical Interface object aggregates multiple Frame Relay Virtual Connections, which it is bound to by its VC Table attributes. It is bound by its Containing Termination Points attribute to a Physical Layer Interface, and is primarily accessed by the Virtual Connection Switching Entity and Data Link layer VC Encapsulation bound by its Contained Connection Termination Points attribute.

*Table 7-4 Frame Relay Logical Interface (IFrameRelayLogicalPort/Trunk)*

| Attribute Name | Attribute Description |
|---|---|
| Administrative Status | Administrative status (*Null, Up, Down, Testing*) |
| Operational Status | Operational status (*Null, Up, Down, Testing, Unknown, Dormant, Not Present*) |
| Same as **Frame Relay Interface** (*IFrameRelay/IFrTrunk*) | |

## Frame Relay Trunk Virtual Connection

The following Data Link layer Frame Relay Trunk Virtual Connection object, is bound by its Containing Termination Points attribute to a Frame Relay Interface object, and is primarily accessed by the Virtual Cross Connection and Data Link layer VC Encapsulation, however it is not bound to any of them by any of its attributes.

*Table 7-5 Frame Relay Trunk Virtual Connection (IFrTrunkVc)*

| Attribute Name | Attribute Description |
|---|---|
| Destination Description | Destination party description |
| Same as **Frame Relay Virtual Connection** (*IFrVc*) | |

# Network Topology

The discovery of Frame Relay (FR) Data Link layer topology is unsupported and is manually (statically) configured by the system administrator.

# Service Alarms

The following alarms are supported for this technology:

- Cloud Problem
- Discard Input Packets/Normal Discard Input Packets
- Dropped Output Packets/Normal Dropped Output Packets
- Link Down/Link Up
- Port Down/Port Up
- Receive Utilization/Receive Utilization Normal
- Transmit Utilization/Transmit Utilization Normal

**Note** Note that these alarms, apart from the Cloud Problem, are related to the underlying Physical Interface (Common section).

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 8

# Point-to-Point Protocol "PPP" and High Level Data Link Control "HDLC"

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



## Technology Description

### PPP

The Point-to-Point Protocol (PPP) (RFC 1661) originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses,  Octet Synchronous (Asynchronous) encapsulation, using HDLC like framing (RFC 1662) protocol, Bit Synchronous encapsulation, using HDLC protocol, network Protocol Multiplexing, Link Configuration, Link Quality Testing, Error Detection, and option negotiation for such capabilities as Network Layer Address and Data Compression negotiation.

PPP supports these functions by providing an extensible Link Control Protocol (LCP) and a family of Network Control Protocols (NCPs) to negotiate optional configuration parameters and facilities.

### HDLC

High-level Data Link Control (HDLC) is a Data Link Layer (Layer 2) group of protocols for transmitting synchronous data packets between point-to-point nodes. In HDLC, data is organized into an addressable frame, which its format has been used for other multipoint to multipoint protocol as well inspired the HDLC like framing protocol described in RFC 1662.

HDLC uses zero insertion/deletion process (bit stuffing) to ensure that the bit pattern of the delimiter flag does not occur in the fields between flags. The HDLC frame is synchronous and therefore relies on the Physical Layer (Layer 1) to provide method of clocking and synchronizing the transmission and reception of frames.

# Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- Point To Point Protocol Encapsulation (IVcBasedEncapsulation)
- High Level Data Link Control Encapsulation (IEncapsulation)

## Point To Point Protocol Encapsulation

The following Data Link layer Point To Point Protocol Encapsulation object, is bound by its Containing Termination Points attribute to an ATM/Frame Relay VC Multiplexer object, and is primarily accessed by a Network layer such as the IP Interface bound by its Contained Connection Termination Points attribute.

*Table 8-1 Point To Point Protocol Encapsulation (IVcBasedEncapsulation)*

| Attribute Name | Attribute Description |
|---|---|
| Virtual Connection | Virtual connection if applicable (ATM Virtual Connection, Frame Relay Virtual Connection or Virtual LAN Interface) |
| Binding Information | Binding information (*User Name*, …) |
| Binding Status | Binding status (*Not Bound, Bound*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

## High Level Data Link Control Encapsulation

The following Data Link layer High Level Data Link Control Encapsulation (HDLC) object, is bound by its Containing Termination Points attribute to an ATM/ Frame Relay VC Multiplexer object, and is primarily accessed by a Network layer such as the IP Interface bound by its Contained Connection Termination Points attribute.

*Table 8-2 High Level Data Link Control Encapsulation (IEncapsulation)*

| Attribute Name | Attribute Description |
|---|---|
| Virtual Connection | Virtual connection if applicable (ATM Virtual Connection or Frame Relay Virtual Connection) |
| Binding Information | Binding information (*User Name*, …) |
| Binding Status | Binding status (*Not Bound, Bound*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Network Topology

The discovery of Point-to-Point Protocol (PPP) Data Link layer topology is done by searching for the existence of the local IP Subnet in any one hop away remote side’s PPP interface. In particular, a comparison is made between the local and remote IP subnets gathered from the upper IP Network layers.

# Service Alarms

There are no faults and alarms related to this technology.

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

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.

CHAPTER 10

# Digital Subscriber Line "DSL" and Integrated Services Digital Network "ISDN"

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



## Technology Description

### xDSL

Digital Subscriber Line (DSL) technology is a modem technology that uses existing twisted pair telephone lines to transport high bandwidth data, such as multimedia and video, to service subscribers. The term xDSL covers a number of similar yet competing forms of DSL, including Asymmetric DSL (ADSL/ADSL2), Symmetric DSL (SDSL), High Speed DSL (HDSL), Rate Adaptive (RADSL), and Very High Bit Data Rate DSL (VDSL) for delivering up to 52 Mbps downstream.

At the customer end of the connection a DSL modem converts data from the digital signals used by computers into a voltage signal of a suitable frequency range which is then applied to the phone line. At the exchange end, a Digital Subscriber Line Access Multiplexer (DSLAM) terminates the DSL circuits and aggregates them, where they are handed off onto other networking transports. In the case of ADSL, the voice component is also separated at this step, either by a filter integrated in the DSLAM or by specialized filtering equipment installed before it.

### ISDN

Integrated Services Digital Network (ISDN) is comprised of digital telephony and data transport services offered by regional telephone carriers. ISDN involves the digitization of the telephone network, which permits voice, data, text, graphics, music, video, and other source material to be transmitted over existing telephone wires.

There are two type of channel in ISDN: A 64 Kbps Bearer (B) channel, which used for data and up to 64 Kbps Delta (D) channel used for signalling and control over the Layers 1 through 3 of the OSI reference model.

With those there are two types of services associated: The 192Kbps Basic Rate Interface (BRI) service, which offers two B channels and one D channel (2B+D) and the 1.544/2.048 Mbps Primary Rate Interfaces (PRI) service, which offers 23/31 B channels and one D channel respectively for the xDSL interface backup.

# Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- Digital Subscriber Line Interface (IDsl/IIdsl/ISdsl/IShdsl)
- Asynchronous Digital Subscriber Line Interface (IADsl)
- Asynchronous Digital Subscriber Line 2 Interface (IADsl2)
- ISDN DSL Traffic Descriptor (IIdslTrafficDescriptor)
- Asynchronous DSL Traffic Descriptor (IAdslTrafficDescriptor)
- Asynchronous DSL 2 Spectrum Traffic Descriptor (IAdsl2TrafficDescriptor)
- Synchronous DSL Traffic Descriptor (ISdslTrafficDescriptor)
- Synchronous High Bit Rate DSL Traffic Descriptor (IShdslTrafficDescriptor)
- Integrated Services Digital Network Interface (IIsdnLayer2)
- Integrated Services Digital Network Channel (IIsdnChannel)
- Integrated Services Digital Network Physical (IIsdnLayer1)

## Digital Subscriber Line Interface

The following Physical layer Digital Subscriber Line Interface, which represents any DSL interface, as well as Asynchronous Digital Subscriber Line Interface and Asynchronous Digital Subscriber Line 2 Interface objects, are bound by their Containing Termination Points attribute to a Port Connector object, and is primarily accessed by only a Data Link Layer ATM Interface bound by its Contained Connection Termination Points attribute.

***Table 10-1 Digital Subscriber Line Interface (IDsl/IIdsl/ISdsl/IShdsl)***

| Attribute Name | Attribute Description |
|---|---|
| Modulation Type | Modulation type (*Null, DMT, CAP, QAM, GLite, GDMT, 2B1Q*) |
| Customer Identification | Customer identification |
| Traffic Descriptor | Traffic descriptor (DSL Traffic Descriptor) |
| Same as **Physical Layer** (*IPhysicalLayer*) | |

# Asynchronous Digital Subscriber Line Interface

*Table 10-2 Asynchronous Digital Subscriber Line Interface (IADsl)*

| Attribute Name | Attribute Description |
|---|---|
| Maximum Reception and Transmission Bandwidth | Maximum reception and transmission bandwidth |
| Same as **Digital Subscriber Line Interface** (*IDsl*) | |

# Asynchronous Digital Subscriber Line 2 Interface

*Table 10-3 Asynchronous Digital Subscriber Line 2 Interface (IADsl2)*

| Attribute Name | Attribute Description |
|---|---|
| Spectrum Traffic Descriptor | Spectrum traffic descriptor (Asynchronous DSL 2 Spectrum Traffic Descriptor) |
| Traffic Descriptor | Traffic descriptor (Asynchronous DSL Traffic Descriptor) |
| Same as **Asynchronous Digital Subscriber Line Interface** (*IADsl*) | |

# DSL Traffic Descriptor

The following various DSL Traffic Descriptor objects describe the traffic of various standard DSL Interfaces and are being aggregated by a Traffic Descriptor Container object (see Common (Shared by Several)).

*Table 10-4 ISDN DSL Traffic Descriptor (IIdslTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Target Bit Rate | Target Bit rate |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

# Asynchronous DSL Traffic Descriptor

*Table 10-5 Asynchronous DSL Traffic Descriptor (IAdslTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Maximum, Minimum and Target Transmission and Reception Noise Margins | Maximum, minimum and target transmission and reception noise margins |
| Maximum, Minimum and Planned Transmission and Reception Bit Rates | Maximum, minimum and planned transmission and reception Bit rates |

*Table 10-5 Asynchronous DSL Traffic Descriptor (IAdslTrafficDescriptor) (continued)*

| | |
|---|---|
| Maximum Transmission Power Spectral Density | Maximum transmission Power Spectral Density (PSD) |
| Transmission and Reception Rate Adaptation | Transmission and reception rate adaptation mode (*Null, Fixed, Adapt at Startup, Adapt at Runtime*) |
| Channel Type | ADSL channel type (*Null, Fast, Interleaved, Fast or Interleaved, Fast and Interleaved*) |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

# Asynchronous DSL 2 Spectrum Traffic Descriptor

*Table 10-6 Asynchronous DSL 2 Spectrum Traffic Descriptor (IAdsl2TrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Maximum, Minimum and Target Transmission and Reception Noise Margins | Maximum, minimum and target transmission and reception noise margins |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

# Synchronous DSL Traffic Descriptor

*Table 10-7 Synchronous DSL Traffic Descriptor (ISdslTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Target and Minimum Bit Rate | Target and minimum line Bit rate |
| Target Noise Margin | Target noise margin |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

# Synchronous High Bit Rate DSL Traffic Descriptor

*Table 10-8 Synchronous High Bit Rate DSL Traffic Descriptor (IShdslTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Target Bit Rate | Target line Bit rate |
| Wire Mode | Wire mode (*Null, Two Wire, Four Wire*) |
| Spectral Mode | Spectral mode (*Null, Symmetric, Asymmetric*) |

*Table 10-8 Synchronous High Bit Rate DSL Traffic Descriptor (IShdslTrafficDescriptor) (continued)*

| | |
|---|---|
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

# Integrated Services Digital Network (ISDN) Interface

The following Data Link layer Integrated Services Digital Network (ISDN) Interface object, is bound by its Containing Termination Points attribute to a Physical Layer Integrated Services Digital Network (ISDN) Physical object, and is primarily accessed by Point To Point Protocol Encapsulation bound by its Contained Connection Termination Points attribute.

*Table 10-9 Integrated Services Digital Network Interface (IIsdnLayer2)*

| Attribute Name | Attribute Description |
|---|---|
| Control Administrative Status | Administrative status (*Unknown, Up, Down, Testing*) |
| Operational Status | Operational status (*Unknown, Up, Down, Testing, Dormant, Not Present*) |
| Channels Table | Array of Integrated Services Digital Network (ISDN) Channels |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Integrated Services Digital Network (ISDN) Channel

The following Data Link layer Integrated Services Digital Network (ISDN) Channel object describes an Integrated Services Digital Network (ISDN) Interface channels table's entry.

*Table 10-10 Integrated Services Digital Network Channel (IIsdnChannel)*

| Attribute Name | Attribute Description |
|---|---|
| Control Administrative Status | Administrative status (*Unknown, Up, Down, Testing*) |
| Operational Status | Operational status (*Unknown, Up, Down, Testing, Dormant, Not Present*) |

## Integrated Services Digital Network (ISDN) Physical

The following Physical layer Integrated Services Digital Network (ISDN) Physical object, is bound by its Containing Termination Points attribute to a Port Connector object, and is accessed by the Data Link layer Integrated Services Digital Network (ISDN) Interface bound by its Contained Connection Termination Points attribute.

*Table 10-11 Integrated Services Digital Network Physical (IIsdnLayer1)*

| Attribute Name | Attribute Description |
|---|---|
| Same as **Physical Layer** (*IPhysicalLayer*) | |

# Vendor Specific Inventory and Information Model Objects

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

The following vendors' DSL Traffic Descriptor objects describe traffic of these vendors' standard DSL interfaces, and are aggregated by a Traffic Descriptor Container object.

- ECI's HiFocus ADSL Traffic Descriptor
- Alcatel's ASAM SHDSL Traffic Descriptor

## ECI's HiFocus ADSL Traffic Descriptor

*Table 10-12 ECI's HiFocus ADSL Traffic Descriptor (IECIHiFocusAdslTrafficDescriptor)*

| Attribute Name | Attribute Description |
|---|---|
| Discrete Multi-Tone Coding Model | Discrete multi-tone coding model (*Null*, *discrtMultiTone*) |
| ATUC Downstream and ATUR Upstream Usage | ATUC downstream and ATUR upstream usage (*Null*, *Yes*, *No*) |
| ATUC Downstream Fast and Interleave Check Bytes | ATUC downstream fast and interleave check bytes |
| ATUR Upstream Fast and Interleave Check Bytes | ATUR upstream fast and interleave check bytes |
| ATUC Downstream and ATUR Upstream Interleaved Depth | ATUC downstream and ATUR interleaved depth (*Power of 2*, *0*, *Non*) |
| ATUC Downstream and ATUR Upstream Code Word Length | ATUC downstream and ATUR upstream code word length in symbols per code word |
| Trellis Coded Modulation Option Usage | Trellis coded modulation option usage (*Null*, *Enabled*, *Disabled*) |
| Echo Cancellation Option | Echo cancellation option (*Null*, *Enabled*, *Disabled*) |
| Coding Mode | Coding mode (*Null*, *Automatic*, *Manual*) |
| Same as Asynchronous DSL Traffic Descriptor (*IAdslTrafficDescriptor*) - see Table 10-5 on page 10-3. | |

## Alcatel's ASAM SHDSL Traffic Descriptor

*Table 10-13 Alcatel's ASAM SHDSL Traffic Descriptor (IAlcatelAsamShdslTrafficProfile)*

| Attribute Name | Attribute Description |
|---|---|
| Minimum and Maximum Required Bit Rate | Minimum and maximum required Bit rate |
| Same as Synchronous High Bit Rate DSL Traffic Descriptor (*IShdslTrafficDescriptor)* - see Table 10-8 on page 10-4. | |

# Network Topology

The Digital Subscriber Line (DSL) Physical layer topology is unsupported and is manually (statically) configured by the system administrator.

# Service Alarms

The following alarms are supported for this technology:

- Link Down/Link Up
- Port Down/Port Up

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 11

# Physical Technologies

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



# Technology Description

## SONET/SDH

Synchronous Optical NETwork (SONET) together with Synchronous Digital Hierarchy (SDH) were originally standardized for connecting one fiber system to another at the optical level in order to forms a single international standard for fiber interconnects between telephone networks of different countries. Today it is a widely deployed, mature enabling technology used in providing high speed, large-scale IP networks, which combines high bandwidth capacity with efficient link utilization, making it a major building block for accommodating a fast growing IP infrastructure both in the core and on the edge.

SONET/SDH is capable of accommodating a variety of transmission rates and applications by defining a technology for carrying many signals of different capacities through a synchronous, flexible, optical hierarchy. This is accomplished by means of a byte-interleaved multiplexing scheme, which simplifies multiplexing, and offers end-to-end network management. It is a layered protocol with the following four separate layers: Photonic, Section, Line and Path, all within the Physical Layer (1) of the Open System Interconnection (OSI) reference model.

SONET/SDH networks consist of Path Terminating Elements (PTE), which represent the Physical Layer (1) Interfaces as well as Add/Drop Multiplexers (ADM) or Digital Cross Connect Systems (DCS) and Regenerators interconnected by point-to-point SONET/SDH links called Sections and are fundamentally connection-oriented, which means that a Virtual Channel (VC) must be set up across the SONET/SDH network prior to any data transfer.

## POS

Packet over SONET/SDH (PoS) is a Data Link (Layer 2) technology that uses PPP (RFC 1661) in HDLC like framing (RFC 1662) encapsulation over SONET/SDH framing. POS interface supports SONET/SDH level alarm processing, performance monitoring, synchronization, and protection switching, which enables seamless interoperation with existing SONET infrastructures and provides the capability to migrate to IP+Optical networks without the need for legacy SONET infrastructures.

## DSx

Digital Signals (DSx) Hierarchy refers to the rate and format of digital telecommunication circuits, as part of the North American Digital Hierarchy. DS is related to the T designations; however DS refers to multiplexing techniques while the T designations refer to the underlying equipment and signalling.

There are various DS levels: DS0/Fractional T1 (64Kbps), which represents a single voice telephone call, DS1/T1 (1.544Mbps), which defines how to multiplex 24 DS0, DS2/T2 (6.312Mbps) and DS3/T3 (44.736Mbps), which define how to multiplex 4 and 28 DS1 respectively, onto the same circuit.

**Note** These Physical Technologies are being supported only as the underlying Physical Layer in conjunction with other Data Link technology layers such as ATM and Packet Over SONET/SDH (POS).

# Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- SONET/SDH Physical (ISonetSdh)
- Digital Signalling 0 Bundle Interface
- Digital Signalling 1 Physical
- Digital Signalling 3 Physical

## SONET/SDH Physical

The following Physical layer SONET/SDH object, is bound by its Containing Termination Points attribute to a Port Connector object, and is primarily accessed by the Data Link layer such as Asynchronous Transfer Mode “ATM” and Frame Relay “FR” interfaces as well as the Packet Over SONET/SDH (POS) interface (implemented using Point To Point Protocol Encapsulation) bound by its Contained Connection Termination Points attribute.

*Table 11-1 SONET/SDH Physical (ISonetSdh)*

| Attribute Name | Attribute Description |
|---|---|
| Specific Type | Specific type (*Null, SONET/SDH Mux, OC3, OC12, OC24, OC48, OC192, STM1, STM4, STM16, STM64*) |
| Loop Back Type | Loop back type (*Null, Cell, Payload, Diag, Line, None, Other, Path, Metalic, Non Metalic, Serial, Parallel, Local, Internal, Network, Inward, Dual, Remote, Inbound Local, No Loop, Facility Loop, Terminal Loop, Other Loop*) |
| Scrambling Mode | Scrambling mode (*Null, On, Off, Payload, Frame, Payload* and *Frame*) |
| Same as **Physical Layer** (*IPhysicalLayer*) | |

# Digital Signalling 0 Bundle Interface

The following Data Link layer Digital Signalling 0 Bundle Interface object, is bound by its Containing Termination Points attribute to either Digital Signalling 1 Physical or Digital Signalling 3 Physical Layer objects, and is primarily accessed by the Data Link layer such as the ATM Interface and the Frame Relay Interface bound by its Contained Connection Termination Points attribute.

*Table 11-2 Digital Signalling 0 Bundle Interface (IDS0Bundle)*

| Attribute Name | Attribute Description |
|---|---|
| Bundled Time Slots | Bundled time slots (DS1 channels) |
| Bundle Location | Bundle location/index |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Digital Signalling 1 Physical

The following Physical layer Digital Signalling 1 Physical and Digital Signalling 3 Physical objects, are bound by their Containing Termination Points attribute to a Port Connector object, and are primarily accessed by the Data Link layer such as the ATM Interface and the Frame Relay Interface as well as Digital Signalling 0 Bundle Interface bound by its Contained Connection Termination Points attribute.

*Table 11-3 Digital Signalling 1 Physical (IDS1Pdh)*

| Attribute Name | Attribute Description |
|---|---|
| Framing Type | Framing type (*Null, OTHER, ESF, ANSI ESFf, D4, E1, E1 CRC, E1 MF, E1 CRC MF, UNFRAMED, E1 UNFRAMED, DS2 M12, E2, E1 Q50, E1 Q50 CRC, ANSI SF, E1 CAS CRC4, E1 CAS No CRC4, E1 No CAS CRC4, E1 No CAS No CRC4, E1 Unstructured, T1 Unstructured, CLEAR CHANNEL*) |

*Table 11-3 Digital Signalling 1 Physical (IDS1Pdh) (continued)*

| | |
|---|---|
| Cell Mapping Type | Cell mapping type (*Null, PLCP, HEC, HCS, Direct, ADM*) |
| Loop Back Type | Loop back type (*Null, Cell, Payload, Diag, Line, None, Other, Path, Metalic, Non Metalic, Serial, Parallel, Local, Internal, Network, Inward, Dual, Remote, Inbound Local, No Loop*) |
| Scrambling Mode | Scrambling mode (*Null, On, Off*) |
| Same as **Physical Layer (***IPhysicalLayer***)** | |

## Digital Signalling 3 Physical

*Table 11-4 Digital Signalling 3 Physical (IDS3Pdh)*

| Attribute Name | Attribute Description |
|---|---|
| Framing Type | Framing type (*Null, Other, M23, SYNTRAN, CBIT, Clear Channel, E3 Other, E3 Framed, Unframed, E3 Unframed, ITU-T G.804, ITU-T G.832, M13*) |
| Cell Mapping Type | Cell mapping type (*Null, PLCP, HEC, HCS, Direct, ADM*) |
| Loop Back Type | Loop back type (*Null, Cell, Payload, Diag, Line, None, Other, Path, Metalic, Non Metalic, Serial, Parallel, Local, Internal, Network, Inward, Dual, Remote, Inbound Local, No Loop*) |
| Scrambling Mode | Scrambling mode (*Null, On, Off*) |
| Same as **Physical Layer (***IPhysicalLayer***)** | |

# Network Topology

The discovery of Synchronous Optical NETwork/Digital Hierarchy (SONET/SDH) as well as Digital Signals (DSx) hierarchy physical layer topology is unsupported and is manually (statically) configured by the system administrator.

However, it is used in conjunction with the Data Link layer above it, such as ATM, for discovering its physical topology, while further verifying it by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial traffic amount in order to function correctly.

# Service Alarms

The following alarms are supported for this technology:

- Discard Input Packets/Normal Discard Input Packets
- Dropped Output Packets/Normal Dropped Output Packets
- Link Down/Link Up
- Port Down/Port Up

- Receive Utilization/Receive Utilization Normal
- Transmit Utilization/Transmit Utilization Normal

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 12

# Multiprotocol Label Switching "MPLS"

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



## Technology Description

### MPLS

Multi-Protocol Label Switching (MPLS) was originally presented as a way of improving the forwarding speed of routers but is now emerging as a crucial standard technology that offers new capabilities for large scale IP networks. Traffic Engineering (TE), the ability of network operators to dictate the path that traffic takes through their network, and Virtual Private Network (VPN) support are examples of two key applications where MPLS is superior to any currently available IP technology. It integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system, or ISP, in order to simplify and improve IP packet exchange, while giving network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.

When packets enter a MPLS-based network, Label Edge Routers (LERs) give them a label (identifier). These labels not only contain information based on the routing table entry (i.e., destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service. Once this classification is complete and mapped, different packets are assigned to corresponding Labeled Switch Paths (LSPs), where Label Switch Routers (LSRs) place outgoing labels on the packets.

# Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- MPLS Interface (IMpls)
- Label Switching Entity (ILse)
- Equivalent Label Switching Entry (ILSEEntries)
- MPLS Entry (IMplsEntry)
- MPLS Aggregate Entry (IMplsAggregateEntry)

## MPLS Interface

The following Network/Data Link layer MPLS Interface object, represent an MPLS configuration in a router interface. It is bound by its Containing Termination Points attribute to a Data Link Layer Interface object, and is primarily being accessed by Network layer IP Interface, bound by its Contained Connection Termination Points attribute. It is also being accessed by Label Switching Entity.

*Table 12-1 MPLS Interface (IMpls)*

| Attribute Name | Attribute Description |
|---|---|
| Distribution Protocol | Distribution protocol (*Null, LDP, TDP, RSVP, TDP and LDP*) |
| Outer and Inner Labels | Outer and inner labels for PathTracer |
| Traffic Engineering Properties | Traffic engineering properties (MPLS TE Properties) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

## Label Switching Entity

The following Label Switching Entity object describes the label distribution protocol independent Label Switching forwarding component of a Label Switching Router (LSR), which is bound by its Logical Sons attribute to all Network or Data Link layer MPLS Interface objects, which IP Packets are being switched between by this Label Switching Entity.

*Table 12-2 Label Switching Entity (ILse)*

| Attribute Name | Attribute Description |
|---|---|
| MPLS Table | Array of Equivalent Label Switching Entries between MPLS Interfaces |
| MPLS Aggregate Table | Array of Equivalent Label Switching Entries from MPLS Interfaces into VRFs |

*Table 12-2 Label Switching Entity (ILse) (continued)*

| | |
|---|---|
| MPLS Tunnel Segments | Array of switched MPLS TE tunnel segments (GUI usage) (see Multi Protocol Label Switching Traffic Engineering (MPLS-TE)) |
| Logical Sons | Array of all MPLS Interfaces, which IP packets are being switched between, by this Label Switching Entity |

# Equivalent Label Switching Entry

The following Equivalent Label Switching Entry, MPLS Entry and MPLS Aggregate Entry objects describe an MPLS Label Switching Table's entries, each as an array of either MPLS Entries or MPLS Aggregate Entries sharing a single ingress label.

*Table 12-3 Equivalent Label Switching Entry (ILSEEntries)*

| Attribute Name | Attribute Description |
|---|---|
| Label Switching Entries | Array of either MPLS Entries or MPLS Aggregate Entries (sharing a single ingress label) |

# MPLS Entry

*Table 12-4 MPLS Entry (IMplsEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Incoming Label | Incoming label |
| Outgoing Interface and Label | Outgoing interface and label |
| Switching Action | Switching action (*Null, Pop, Swap, Aggregate, Untagged, Pop* and *Act*) |
| Next Hop IP Address | Next hop IP address |

# MPLS Aggregate Entry

*Table 12-5 MPLS Aggregate Entry (IMplsAggregateEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Virtual Routing Entity | Virtual Routing (VRF) entity |
| Incoming Label | Incoming label |
| Outgoing Interface and Label | Outgoing interface and label |
| Switching Action | Switching action (*Null, Pop, Swap, Aggregate, Untagged, Pop* and *Act*) |
| Next Hop IP Address | Next hop IP address |

# Network Topology

The discovery of Multi Protocol Label Switching (MPLS) network layer topology is done by searching for the existence of the local IP subnet in any one hop away remote side's MPLS Interface. In particular a comparison is made between the local and remote IP subnets gathered from the upper IP network layers.

# Service Alarms

The following alarms are supported for this technology:

- Broken LSP Discovered
- MPLS Black Hole Found/MPLS Black Hole Cleared
- MPLS Interface Removed/MPLS Interface Add

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction MPLS User Guide, 3.6.*

CHAPTER 13

# Multi Protocol Label Switching Traffic Engineering (MPLS-TE)

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



# Inventory and Information Model Objects (IMOs)

This section includes the following tables:



## MPLS TE Tunnel Interface

The following Network/Data Link layer MPLS TE Tunnel Interface object, is bound by its Containing Termination Points attribute to a Data Link Layer Interface object, and is primarily being accessed by Network layer IP Interface bound by its Contained Connection Termination Points attribute. It is also being accessed by Label Switching Entity.

*Table 13-1 MPLS TE Tunnel Interface (IMplsTETunnel)*

| Attribute Name | Attribute Description |
|---|---|
| Destination Address | Destination IP address |
| Outgoing Interface and Label | Outgoing interface and label |
| Path Identification | Label Switching Path (LSP) identification |
| Requested Bandwidth | Requested bandwidth |
| Measured Average, Burst and Peak Bandwidth | Measured average, burst and peak bandwidth |

*Table 13-1 MPLS TE Tunnel Interface (IMplsTETunnel) (continued)*

| Attribute Name | Attribute Description |
|---|---|
| Setup and Hold Priority | Setup and hold priority of the tunnel |
| Affinity Bits and Mask | Required traffic engineering affinity bits and mask attributes of the tunnel's links |
| Automatic Route Announcement Status | Automatic route announcement status (*Enable, Disable*) |
| Optimization Lock Down Status | Label switching path optimization lock down status (*Enable, Disable*) |
| Path Option | Label switching path option (*Explicit, Dynamic*) |
| Name | Interface name |
| Description | Interface description |
| Administrative Status | Administrative status (*Unknown, Up, Down*) |
| Operational Status | Operational status (*Unknown, Up, Down*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (MPLS Interface) |
| Contained Connection Termination Points | Bound Connection Termination Points (IP Interface or MPLS Interface) |

# MPLS TE Properties

The following MPLS TE Properties with its MPLS TE Allocation Entry objects describes the traffic engineering properties of a MPLS Interface, which is bound to by its traffic engineering properties attribute.

*Table 13-2 MPLS TE Properties (IMplsTEProperties)*

| Attribute Name | Attribute Description |
|---|---|
| Administrative Weight | Administrative weight |
| Attributes Identifier | Attributes list identifier |
| Signalling Protocol | Signalling protocol (*None, RSVP, CR-LDP, Other*) |
| Available, Physical and Reserveable Bandwidth | Available, physical and reserveable bandwidth |
| Reserved Bandwidth | Arrays of MPLS TE Allocation Entry |

## MPLS TE Allocation Entry

*Table 13-3 MPLS TE Allocation Entry (IMplsTEPropertiesAllocationEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Priority Level | Allocation priority level (*0-7*) |
| Allocated and Cumulative Bandwidth | Allocated and cumulative bandwidth at and up this priority level |

## MPLS TE Tunnel Segment

The following MPLS TE Tunnel Segment object describes, as the name implies, the properties of a single segment of an MPLS TE Tunnel, which is being used by the Graphical User Interface [GUI] of the management application for visualizing the MPLS TE Tunnels network and has no effect on the Virtual Network Element [VNE] logic implementation. The segments are aggregated in MPLS TE Tunnel Segments table of the Label Switching Entity.

*Table 13-4 MPLS TE Tunnel Segment (IMplsTESegment)*

| Attribute Name | Attribute Description |
|---|---|
| Source and Destination Addresses | Source and destination IP addresses of the tunnel |
| Incoming Interface and Label | Incoming interface and label (if not head segment) |
| Outgoing Interface and Label | Outgoing interface and label (if not tail segment) |
| Segment Type | Segment type (*Head, Intermediate, Tail*) |
| Measured Average, Burst and Peak Bandwidth | Measured average, burst and peak bandwidth |
| Path Identification | Label Switching Path (LSP) identification |
| Name | Segment name |

# Network Topology

The discovery of Multi Protocol Label Switching Traffic Engineering [MPLS-TE] Network layer topology is unsupported.

# Service Alarms

The following alarms are supported for this technology:

- MPLS TE Tunnel Down/MPLS TE Tunnel Up
- MPLS TE Tunnel Flapping/MPLS TE Tunnel Up or Down

These alarms are disabled by default.

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction MPLS User Guide, 3.6.*

CHAPTER 14

# Virtual Private Networks "VPNs"

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



## Technology Description

### VPN

BGP/MPLS VPNs, as defined in RFC 2547 and related drafts and standards, provide a Layer 3 VPN. With Layer 3 VPNs, each Provider Edge (PE) device acts like a set of virtual routers, one per VPN. The network provider configures the VPN membership of each PE router interface. In most cases, one port is used for multiple interfaces where each is associated with different VPNs. The port's view of the network is restricted to the VPNs of which it is a member, and it cannot address devices outside that environment. Either static routes are provisioned on both the Customer Edge (CE) and PE, or, for more complex scenarios, a routing protocol (such as RIP, OSPF or BGP) is run between CE and PE. So the interface between the CE and PE devices is conventional IP routing.

The network provider also establishes a suitable mesh of MPLS Label Switched Paths (LSPs) between all the PE routers that need to communicate. The PE devices qualify each external IP address that they learn with a per VPN identifier, and broadcast them to all other PE routers using an extended form of BGP depending on BGP connectivity. They also include an MPLS label that is specific to the destination route (or, in some implementations, the destination port). Through this process, the PE devices build up a complete map of the VPNs and destination labels.

The PE routers then use this information to route the packets across the backbone network to the correct destination within the relevant VPN.

## Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- Equivalent Routing Entry (IRoutingEntries)
- Virtual Routing Entry (IVrfEntry)
- Multi Protocol BGP Entity (IMpBgp)
- Equivalent Cross Virtual Routing Entry (ICrossVrf)
- Cross Virtual Routing Entry (ICrossVrfRoutingEntry)

# Virtual Routing Forwarding (VRF) Entity

The following Virtual Routing Forwarding (VRF) Entity object describes the routing and address resolution protocols independent forwarding component of a MPLS-BGP based VPN router, which is bound by its Logical Sons attribute to all Network layer IP Interface objects, which IP Packets are being routed between, by this Virtual Routing Forwarding Entity.

*Table 14-1 Virtual Routing Forwarding (VRF) Entity (IVrf)*

| Attribute Name | Attribute Description |
|---|---|
| Virtual Routing Table | Array of Equivalent Routing Entries |
| Exported Route Targets | Array of route target identifiers |
| Imported Route Targets | Array of route target identifiers |
| Route Distinguisher | Route distinguisher |
| ARP Entity | Address Resolution Entity (ARP Entity) (see Internet Protocol "IP") |
| Name | VRF name |
| Logical Sons | Array of all IP Interfaces, which IP packets are being routed between, by this Virtual Routing Forwarding (VRF) Entity |

# Equivalent Routing Entry

The following Equivalent Routing Entry and Virtual Routing Entry objects describe a routing table's entries, each as an array of Virtual Routing Entries sharing a single IP Subnetwork destination.

*Table 14-2 Equivalent Routing Entry (IRoutingEntries)*

| Attribute Name | Attribute Description |
|---|---|
| Routing Entries | Array of Virtual Routing Entries (sharing a single destination) |

# Virtual Routing Entry

*Table 14-3 Virtual Routing Entry (IVrfEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Next Hop BGP Address | Next hop BGP IP address |
| Incoming and Outgoing Inner Label | Incoming and outgoing inner MPLS label |

*Table 14-3 Virtual Routing Entry (IVrfEntry) (continued)*

| Attribute Name | Attribute Description |
|---|---|
| Outer Label | Outer MPLS label |
| Destination IP Subnet | Final destination IP subnet |
| Next Hop IP Address | Next hop IP address |
| Type | Route entry type (*Null, Other, Invalid, Direct, Indirect, Static*) |
| Routing Protocol Type | Routing protocol type (*Null, Other, "Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN SPF IGP, OSPF, BGP, EIGRP*) |
| Outgoing Interface Name | Outgoing IP interface name |

# Multi Protocol BGP Entity

The following Multi Protocol BGP Entity object describes the BGP component of a MPLS-BGP based VPN router, which is bound by its Logical Sons attribute to all Virtual Routing Forwarding (VRF) Entity objects, which IP Packets are being routed between by this Multi Protocol BGP Entity.

*Table 14-4 Multi Protocol BGP Entity (IMpBgp)*

| Attribute Name | Attribute Description |
|---|---|
| BGP Identifier | Border Gateway Protocol (BGP) identifier |
| Local Autonomous System | Local peer autonomous system |
| Cross Virtual Routing Table | Array of Equivalent Cross Virtual Routing Entry |
| BGP Neighbors | Array of BGP neighbor entries (see Routing Protocols "BGP/OSPF") |
| Logical Sons | Array of all Virtual Routing Entries, which IP packets are being routed between, by this Multi Protocol BGP Entity |

# Equivalent Cross Virtual Routing Entry

The following Equivalent Cross Virtual Routing Entry and Cross Virtual Routing Entry objects describe the first dimension of a cross virtual routing table, as an array of Cross Virtual Routing Entries sharing a single Virtual Routing Forwarding (VRF) Entity destination.

*Table 14-5 Equivalent Cross Virtual Routing Entry (ICrossVrf)*

| Attribute Name | Attribute Description |
|---|---|
| Virtual Routing Entries | Array of Cross Virtual Routing Entries (sharing a single destination) |
| Virtual Routing Entity Name | Virtual Routing Entity (VRF) name |

## Cross Virtual Routing Entry

*Table 14-6 Cross Virtual Routing Entry (ICrossVrfRoutingEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Outgoing Virtual Routing Entity Identifier | Outgoing virtual routing entity Object Identifier (OID) |
| Incoming and Outgoing Virtual Routing Tags | Incoming and outgoing virtual routing tags |
| Destination IP Subnet | Final destination IP subnet |
| Next Hop IP Address | Next hop IP address |
| Type | Route entry type (*Null, Other, Invalid, Direct, Indirect, Static*) |
| Routing Protocol Type | Routing protocol type (*Null, Other, "Local, Network Managed, ICMP, EGP, GGP, Hello, RIP, IS-IS, ES-IS, Cisco IGRP, BBN SPF IGP, OSPF, BGP, EIGRP*) |
| Outgoing Interface Name | Outgoing IP interface name |

# Network Topology

The discovery of MPLS-BGP based Virtual Private (VPN) network topology is done by searching for the existence of the local Virtual Routing Forwarding (VRF) Entity's imported route targets in any remote side's VRF entity exported route targets.

# Service Alarms

The following alarm is supported for this technology:

- Duplicate IP on VPN Found/Duplicate IP on VPN Fixed

**Note** This alarm is disabled by default.

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 15

# Pseudo Wire Emulation Edge to Edge (PWE3)

This chapter describes the level of support that Cisco ANA provides for PWE3, as follows:



## Technology Description

### PWE3

Pseudo Wire Emulation Edge-to-Edge (PWE3) provides methods for carrying networking services such as ATM, Ethernet, TDM and SONET/SDH over a Packet Switched Network (PSN) as outlined in RFC 3985. It is a point-to-point connection between pairs of Provider Edge (PE) routers, which emulates services like Ethernet over an underlying core MPLS network through encapsulation into a common MPLS format, hence allowing carriers to converge their services with an MPLS network.

## Inventory and Information Model Objects (IMOs)

This section includes the following tables:

# PTP Layer 2 MPLS Tunnel Interface

The following Network/Data Link layer PTP Layer 2 MPLS Tunnel Interface PTP Layer 2 MPLS Tunnel Interface object, is bound by its Containing Termination Points attribute to a Data Link Layer Interface object, and is primarily being accessed by Label Switching Entity.

*Table 15-1 PTP Layer 2 MPLS Tunnel Interface (IPTPLayer2MplsTunnel)*

| Attribute Name | Attribute Description |
|---|---|
| Local and Remote Router Addresses | Local and remote router IP addresses |
| Local and Remote Virtual Connection Labels | Local and remote virtual connection labels |
| Tunnel Identification | Tunnel identification |
| Tunnel Status | Tunnel status (*Unknown, Up, Down*) |
| Local and Remote Tunnel Interface | Local and remote tunnel interface object identifier |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points (Tunnel Container) |

# Network Topology

The discovery of Pseudo Wire Emulation Edge to Edge [PWE3] Network layer topology is done by searching for a match of the Local and Remote Router IP Addresses in any one hop away remote side's PTP Layer 2 MPLS Tunnel Interface. In particular a comparison is made between the Local and Remote Router IP Addresses as well as Tunnel Identification.

# Service Alarms

The following alarms are supported for this technology:

- Layer 2 Tunnel Down/Layer 2 Tunnel Up

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 16

# Quality of Service "QoS"

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



# Technology Description

## Quality of Service (QoS)

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail. Integrated and Differentiated Service (IS/DS) are the two model currently being use for providing QoS.

Integrated Service (IS) is a multiple service model that can accommodate multiple QoS requirements. In this model the application requests a specific kind of service from the network before it sends data. The request is made by explicit signalling; the application informs the network of its traffic profile and requests a particular kind of service that can encompass its bandwidth and delay requirements. The application is expected to send data only after it gets a confirmation from the network. It is also expected to send data that lies within its described traffic profile.

The network performs admission control, based on information from the application and available network resources. It also commits to meeting the QoS requirements of the application as long as the traffic remains within the profile specifications. The network fulfills its commitment by maintaining per flow state and then performing packet classification, policing, and intelligent queuing based on that state.

Differentiated Service (DS) is a multiple service model that can satisfy differing QoS requirements. However, unlike in the integrated service model, an application using differentiated service does not explicitly signal the router before sending data. For differentiated service, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the IP Precedence bit settings in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queuing.

# Inventory and Information Model Objects (IMOs)

This section currently describes Cisco's Quality of Service (QoS) objects, although they may appear to be generic QoS objects that may be used by other vendors.

This section includes the following tables:

- Access List Traffic Descriptor (IAccessList)
- Access List Entry (IAccessListEntry)

## Access List Traffic Descriptor

The following Access List Traffic Descriptor with its Access List Entry objects describes the access list of a single type (*Unknown, Standard, Extended* and *Rate Limit*), and is being aggregated by a Traffic Descriptor Container object (see Common (Shared by Several)).

***Table 16-1 Access List Traffic Descriptor (IAccessList)***

| Attribute Name | Attribute Description |
|---|---|
| Type | Access list type (*Unknown, Standard, Extended, Rate Limit*) |
| Access List Entries Table | Array of Access List Entries |
| Name | Traffic descriptor name |
| Index | Traffic descriptor index |

## Access List Entry

***Table 16-2 Access List Entry (IAccessListEntry)***

| Attribute Name | Attribute Description |
|---|---|
| Entry Identification | Entry identification |
| Action Logic | Action logic (*Unknown, Permit, Deny*) |
| Source and Destination Address | Source and destination IP address |
| Source and Destination Wildcard | Source and destination IP wildcard |
| Protocol Type | IANA type of the protocol (*HOPORT, ICMP, IGMP, GGP, IP in IP, ST, TCP, CBT, EGP, IGP, …*) |
| Source and Destination Ports Ranges | Source and destination TCP/UDP ports ranges |

*Table 16-2 Access List Entry (IAccessListEntry) (continued)*

| Attribute Name | Attribute Description |
|---|---|
| Source and Destination Port Action | Source and destination port action (*Null, Equal, Not Equal, Greater Than, Less Than, Range*) |
| Protocol Specific Info | Protocol specific information |
| Differential Services Code Points | Differential Services Code Points (DSCP) |
| Type of Service | Type of Service (ToS) (*Normal (0), Min Cost (1), Max Reliability (2), 3, Max Throughput (4), 5, 6, 7, Min Delay (8), 9, 10, 11, 12, 13, 14, 15*) |
| Precedence | Precedence (*Routine (0), Priority (1), Immediate (2), Flash (3), Flash Override (4), Critical (5), Internet (6), Network (7)*) |
| Matches | Matches count |

# Network Topology

There is no network topology related to this technology.

# Service Alarms

There are no faults and alarms related to this technology.

CHAPTER 17

# Physical Equipment

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



## Inventory and Information Model Objects (IMOs)

This section includes the following tables:



### Chassis

The following Chassis object describes a chassis equipment holder, which is bound by its Contained Equipment Holders attribute to other equipment holders such as shelves and slots.

***Table 17-1 Chassis (IChassis)***

| Attribute Name | Attribute Description |
|---|---|
| Description | Chassis description |
| Equipment Holder Type | Equipment holder type (*Chassis*) |
| Contained Equipment Holders | Contained equipment holders |
| Contained Equipments | Contained equipment |

# Shelf

The following Shelf object describes a shelf equipment holder, which is bound by its Contained Equipment Holders and Contained Equipments attributes to other equipment holders and equipments objects it contains respectively.

***Table 17-2 Shelf (IShelf)***

| Attribute Name | Attribute Description |
|---|---|
| Description | Chassis description |
| Status | Shelf status |
| Equipment Holder Type | Equipment holder type (*Shelf*) |
| Contained Equipment Holders | Contained equipment holders |
| Contained Equipments | Contained equipment |

# Module

The following Module object describes a module/board equipment, which is bound by its Contained Equipment Holders and supported Physical Termination Points attributes to other equipment holders (sub slots) and supported physical Termination Points (Port Connectors) objects it contains respectively.

***Table 17-3 Module/Board (IModule)***

| Attribute Name | Attribute Description |
|---|---|
| Module Name | Module name |
| Module Description | Module description |
| Software Version | Software version |
| Operational Status | Operational status (*Unknown, OK, Warning, Minor, Major, Critical, UnManaged, Enabled, Disabled, Information, Cleaning, Standby*) |
| Hardware Type and Version | Hardware type and version |
| Management IP Address | Management IP address |
| Redundant Equipment | Redundant equipment number |
| Configured Redundancy | Configured redundancy (*Null, Working, Protecting, None*) |
| Redundancy Status | Redundancy status (*Null, Active, Standby, None*) |
| Operational Status Last Change | Date of last operational status change |
| Contained Equipment Holders | Contained equipment holders |
| Supported Physical Termination Points | Supported physical termination points |

# Power Supply

The following Power Supply object describes a power supply equipment, which is bound by its Contained Equipment Holders attributes to other equipment holders objects that it contains.

*Table 17-4 Power Supply (IPowerSuply)*

| Attribute Name | Attribute Description |
|---|---|
| Operational Status | Operational status (*Unknown, OK, Warning, Minor, Major, Critical, UnManaged, Enabled, Disabled, Information, Cleaning, Standby*) |
| Hardware Type and Version | Hardware type and version |
| Management IP Address | Management IP address |
| Redundant Equipment | Redundant equipment number |
| Configured Redundancy | Configured redundancy (*Null, Working, Protecting, None*) |
| Redundancy Status | Redundancy status (*Null, Active, Standby, None*) |
| Operational Status Last Change | Date of last operational status change |
| Contained Equipment Holders | Contained equipment holders |

# Port Connector

The following Port Connector object describes a port connector physical termination point, which is being accessed by the Module containing it.

*Table 17-5 Port Connector (IPortConnector)*

| Attribute Name | Attribute Description |
|---|---|
| Location | Port connector location |
| Alias | Port alias |
| Type | Port connector type (*Unknown, BNC, RJ11, RJ45, Fiber Optic, RJ48, Fiber Optic FC, Fiber Optic SC, Fiber Optic ST, Fiber Optic LC, Internal, Backplane, Fiber Optics MT RJ, DB 15 Pin, SMB, DB 60 Pin, DB 50 Pin, 34-pin Winchester, Generic, DB 9 Pin*) |
| Sub Ports | Sub connection termination points (currently being used only for Lucent SONET/ SDH equipment) |
| Supporting Equipment | Supporting equipment in which this port connector resides in |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Service Alarms

The following alarms are supported for this technology:

- Card Out/Card In
- Card Down/Card Up

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 18

# Base Logical Components

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



# Inventory and Information Model Objects (IMOs)

This section includes the following tables:



## Managed Element

The following Managed Element object describes the root object of a network element, from which all it physical (chassis, slots, modules, port connectors) and logical (routing and switching entities, communication and physical termination point) components' objects are being accessed.

***Table 18-1 Managed Element (IManagedElement)***

| Attribute Name | Attribute Description |
|---|---|
| IP Address | Management IP address |
| Communication State | Communication state with the managed device and the gateway (*Unknown, Device Unreachable, Agent Unreachable, Device Reachable, Agent Unloaded*) |
| Investigation State | Investigation state of the Virtual Network Element (VNE) (*Unknown, Initializing, Normal, Incomplete, Unsupported, Device Agent Shutting Down, Device Agent Maintenance, Device Agent Preparing for Maintenance*) |

*Table 18-1 Managed Element (IManagedElement) (continued)*

| Attribute Name | Attribute Description |
|---|---|
| Element Category | Element category (*Unknown, DSLAM, Switch, BRAS, Router, Ethernet Switch, Cloud, Metro Central, Server, EMS, Generic Device Agent, ICMP, PC, Printer, Netra, WiFi Element, Service Control Switch*) |
| Element Type and its Key | Element type and its key mapped by the registry based on the SNMP system OID |
| Logical and Physical Roots | Logical and physical roots of the VNE model |
| Device Name | Device name as configured by the user in the registry |
| System Name, Description, Location, Contact and Up Time | System name, description, location, contact and up time taken from MIB II (RFC 1213) |
| Software Version | Software version |
| Vendor Identity | Vendor identity (*Null, Copper Mountain, Alcatel, Cisco, Redback Networks, Marconi, Lucent, Nokia, ADC, TdSoft, RAD, Nortel Networks, ECI Telecom, Juniper Networks, Sheer Networks, SUN Microsystems, NEC, Huawei, Laurel, UTStarcom*) |
| Memory and CPU Usage | Memory and CPU usage |
| Agent Memory and Free Memory Sizes | Agent memory and free memory sizes |
| Number of Device Components | Number of Device Components (DCs) |
| Number of Logical Entries | Number of property holders, which are not DCs |

# Logical Root

The following Logical Root and Physical Root objects, aggregates or contains all the logical and physical components of a Managed Element, and are accessed by the later logical and physical root attributes.

*Table 18-2 Logical Root (ILogicalRoot)*

| Attribute Name | Attribute Description |
|---|---|
| Managed IPs List | Array of Managed IPs |
| Contexts List | Array of Contexts |
| Forwarding Components List | Array of Forwarding Component Containers |
| Traffic Descriptors List | Array of Traffic Descriptor Containers |
| Tunnel Containers List | Array of Tunnel Containers |
| Services List | Array of System Services |
| Data Link Aggregation Containers List | Array of data link aggregations (Link Aggregation Groups, Cisco's Ethernet Channels) |

# Physical Root

*Table 18-3 Physical Root (IPhysicalRoot)*

| Attribute Name | Attribute Description |
|---|---|
| Equipment Holders | Array of equipment holders such as Chassis and Shelf |

# Managed IP

The following Managed IP object, aggregates or contains all logical components of a Managed Element, which are being managed by one of the multiple managed IP addresses of this element. It is accessed by a Logical Root.

*Table 18-4 Managed IP (IManagedIP)*

| Attribute Name | Attribute Description |
|---|---|
| System Name, Description, Location, Contact and Up Time | System name, description, location, contact and up time taken from MIB II (RFC 1213) |
| Software Version | Software version |
| Contexts List | Array of Contexts |
| Forwarding Components List | Array of Forwarding Component Containers |
| Traffic Descriptors List | Array of Traffic Descriptor Containers |
| Tunnel Containers List | Array of Tunnel Containers |
| Services List | Array of System Services |

# Context

The following Context object, aggregates or contains all the logical components of a Managed Element with a single context, such as a virtual router, and is accessed by a Logical Root.

*Table 18-5 Context (IContext)*

| Attribute Name | Attribute Description |
|---|---|
| Name | Context name |
| IP Address Pools | Array of IP Address Pools |
| Forwarding Components List | Array of Forwarding Component Containers |
| Traffic Descriptors List | Array of Traffic Descriptor Containers |
| Tunnel Containers List | Array of Tunnel Containers |
| Data Link Aggregation Containers List | Array of data link aggregations (Link Aggregation Groups, Cisco's Ethernet Channels) |

## System Service

The following System Service objects, describe a single system service along with its status and up time, and is accessed by a Logical Root.

*Table 18-6 System Service (ISystemService)*

| Attribute Name | Attribute Description |
|---|---|
| Type | Service type (*Unknown, Radius, Network Time Protocol, Spanning Tree Protocol*) |
| Status | Service status (*Null, Running, Down, Reset, Initializing, Other*) |
| Up Time | Service up time |

# Service Alarms

The following alarms are supported for this technology:

- Component Unreachable/Component Reachable
- CPU Over Utilized/CPU Normal Use
- Device Unsupported
- Memory Over Utilized/Memory Normal Use

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*

CHAPTER 19

# Common (Shared by Several)

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



## Inventory and Information Model Objects (IMOs)

This section includes the following tables:

- Physical Layer (IPhysicalLayer)
- Bridging Entity (IBridge)
- Bridging Entry (IBridgeEntry)
- VC Multiplexer (EncapMux)
- VC Encapsulation (IVcBasedEncapsulation)
- VC Switching Entity (IVcSwitchingEntity)
- Virtual Cross Connection (IVcCrossConnect)
- Forwarding Component Container (IFWComponentContainer)
- Traffic Descriptor Container (ITrafficDescriptorContainer)
- Tunnel Container (ITunnelContainer)

### Physical Layer

The following Physical Layer object, is bound by its Containing Termination Points attribute to a Port Connector object, and is accessed by the Data Link layer bound by its Contained Connection Termination Points attribute.

**Note** The following attributes are configured in the registry and not retrieved from the device.

*Table 19-1 Physical Layer (IPhysicalLayer)*

| Attribute Name | Attribute Description |
|---|---|
| Media Type | Physical media type (*Null, Thin Coax, Thick Coax, Fiber Optic, Multi Mode Fiber Optic, Single Mode Fiber Optic, Short Single Mode Fiber Optic, Long Single Mode Fiber Optic, UTP, STP, FTP, EIA/TIA-232, EIA/TIA-449, V.35, X.21, EIA/TIA-530, EIA/TIA-530A, Generic Serial, EIA/TIA-612/613, Other*) |
| Clocking Source | Clocking source (*Unknown, Other, Network, Internal, Loop Timed, External, None, Line, Back Plane, Adaptive Timing*) |
| Maximum Speed | Maximum supported speed with units specification |
| Is Internal Port | Indicate an internal port, such as between module and backplane (*True, False*) |
| Discarded Bandwidth | Current discarded input bandwidth |
| Dropped Bandwidth | Current dropped output bandwidth |
| Input Bandwidth | Current utilized input bandwidth |
| Output Bandwidth | Current utilized output bandwidth |
| Discarded and Received Input Data Counters | Discarded and received input octets and packets counters |
| Dropped and Forward Output Data Counters | Dropped and forward output octets and packets counters |
| Administrative Status | Administrative status (*Unknown, Up, Down, Testing*) |
| Operational Status | Operational status (*Unknown, Up, Down, Testing, Dormant, Not Present*) |
| Operational Status Last Change | Date of last operational status change |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Bridging Entity

The following Bridging Entity object describes the IEEE 802™ based protocols independent forwarding component of an IEEE 802™ Bridge/Switch, which is bound by its Logical Sons attribute to all the Data Link layers such as Ethernet, Token Ring and future Wireless LAN and MAN interface objects, which IEEE 802™ based Data Link frames are being bridged or switched between, by this Bridging Entity.

*Table 19-2 Bridging Entity (IBridge)*

| Attribute Name | Attribute Description |
|---|---|
| Bridge Table | Array of Bridging Entries |
| Type | Bridge type (*Null, Automatic, Regular, Bridge Route*) |

*Table 19-2 Bridging Entity (IBridge) (continued)*

| | |
|---|---|
| MAC Address | Bridge internal MAC address used either for running Spanning Tree Protocol (STP) or for bridge's network management |
| IP Interface | OID of the IP Interface used mainly for routing traffic from that bridge |
| Name | Bridging entity name |
| Logical Sons | Array of all IEEE 802™ based data link interfaces (Ethernet Interface, Token Ring Interface ..), which IEEE 802™ based data link frames are being bridged/switched between, by this Bridging Entity |

# Bridging Entry

The following Bridging Entry object describes a bridging domain wide bridge table's entry of a Bridging Entity.

*Table 19-3 Bridging Entry (IBridgeEntry)*

| Attribute Name | Attribute Description |
|---|---|
| Destination MAC Address | Destination station MAC address |
| Outgoing Interface | Outgoing underlying interface (Cisco's Ethernet Channels, Ethernet Interfaces, Virtual LAN Interfaces or Virtual LAN Multiplexers) |

# VC Multiplexer

The following VC Multiplexer object is bounded by its Containing Termination Points attribute to either an ATM Interface or a Frame Relay Interface object, and is primarily accessed by the Data Link layer VC Encapsulations bound by its Contained Connection Termination Points attribute.

*Table 19-4 VC Multiplexer (EncapMux)*

| Attribute Name | Attribute Description |
|---|---|
| Virtual Connection Count | Bounded virtual connection count |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (ATM Interface or Frame Relay Interface) |
| Contained Connection Termination Points | Bound Connection Termination Points (VC Encapsulations) |

# VC Encapsulation

The following Data Link layer VC Encapsulation object, is bound by its Containing Termination Points attribute to an ATM or Frame Relay VC Multiplexer object, and is primarily accessed by a network layer such as an IP Interface as well as a Data Link layer such as Ethernet Interface and Point To Point Protocol Encapsulation bound by its Contained Connection Termination Points attribute.

*Table 19-5 VC Encapsulation (IVcBasedEncapsulation)*

| Attribute Name | Attribute Description |
|---|---|
| Virtual Connection | Virtual connection (ATM Virtual Connection or Frame Relay Virtual Connection) |
| Binding Information | Binding information (*User Name*, …) |
| Binding Status | Binding status (*Not Bound, Bound*) |
| IANA Type | IANA type of the sub/layer |
| Containing Termination Points | Underlying termination points (connection or physical) |
| Contained Connection Termination Points | Bound Connection Termination Points |

# Virtual Connection Switching Entity

The following Virtual Connection Switching Entity object describes the standard forwarding component of an ATM or Frame Relay Switch, which is bound by its Logical Sons attribute to all the Data Link layers such as ATM Interface or Frame Relay Interface objects, which cells or frames respectively are being switched between, by this Virtual Connection Switching Entity.

*Table 19-6 VC Switching Entity (IVcSwitchingEntity)*

| Attribute Name | Attribute Description |
|---|---|
| Cross Connect Table | Array of Virtual Cross Connections |
| Logical Sons | Array of all ATM Interfaces or Frame Relay Interfaces, which cells or frames respectively are being switched between, by this Virtual Connection Switching Entity |

# Virtual Cross Connection

The following Virtual Cross Connection object describes either a Virtual Connection Switching Entity wide or an ATM Interface specific Cross Connect table's entry.

*Table 19-7 Virtual Cross Connection (IVcCrossConnect)*

| Attribute Name | Attribute Description |
|---|---|
| Ingress and Egress Virtual Connection | Ingress and egress virtual connections (ATM Virtual Connection or Frame Relay Virtual Connection) |
| Ingress and Egress Port | Ingress and egress ports (*Port Connectors*) |

# Forwarding Component Container

The following Forwarding Component Container object aggregates a single type Forwarding Components, such as Routing Entity, Bridging Entity and Virtual Connection Switching Entity.

*Table 19-8 Forwarding Component Container (IFWComponentContainer)*

| Attribute Name | Attribute Description |
|---|---|
| Forwarding Components | Array of a single type forwarding components |
| Type | Forwarding component (*Null, Routing Entities, Bridges, VRFs, LSEs, VC Switching Entities, L2TP Peers, MPBGPs, IMA Groups*) |

# Traffic Descriptor Container

The following Traffic Descriptor Container object, which basically is a container of any table's entries, aggregates a single type Traffic Descriptors such as OSPF Entry.

*Table 19-9 Traffic Descriptor Container (ITrafficDescriptorContainer)*

| Attribute Name | Attribute Description |
|---|---|
| Traffic Descriptors | Array of a single type traffic descriptors |
| Type | Descriptor type (*Null, ATM Traffic Profiles, ADSL Traffic Descriptors, SDSL Traffic Descriptors, IDSL Traffic Descriptors, SHDSL Traffic Descriptors, MPLS Properties, CAC Profiles, ATM Access Profiles, OSPF Networks, BGP Neighbor, Access Lists, Tunnel Traffic Descriptors, QoS Policies, QoS Classes, IS-IS Database, QoS WRED, ATM Traffic Shaping Profile, Frame Relay Traffic Profiles, Rate Limit, Filter, Policer, IP Pools, ISAKMP Policies, IPsec Maps, Process List, Installed Software, L2TP Peer Group, L2TP Domain Group, QoS Object Table, QoS Class Map, QoS Policy Map, QoS Match Statments Table, QoS Queueing Config Table, QoS Service Policy Table, ADSL2 Traffic Descriptors, ADSL2 Spectrum Descriptors*) |

# Tunnel Container

The following Tunnel Container object aggregates single type tunnel interfaces, which are either MPLS TE Tunnel Interfaces or PTP Layer 2 MPLS Tunnel Interfaces.

*Table 19-10 Tunnel Container (ITunnelContainer)*

| Attribute Name | Attribute Description |
|---|---|
| Tunnel Edges | Array of either PTP Layer 2 MPLS Tunnel Interfaces or MPLS TE Tunnel Interfaces |

# Network Topology

The Cisco Discovery Protocol (CDP), although a proprietary one, plays a major role in discovery of all Cisco's network equipment. Hence it is used as part of the physical topology discovery of Cisco's equipment by searching for the existence of local CDP neighbors signature, gathered from the physical layer, in any remote side's port of the same type.

# Service Alarms

The following alarms are supported for this technology:

- Cloud Problem
- Discard Input Packets/Normal Discard Input Packets
- Dropped Output Packets/Normal Dropped Output Packets
- Link Down/Link Up
- Port Down/Port Up
- Receive Utilization/Receive Utilization Normal
- Transmit Utilization/Transmit Utilization Normal

**Note** For a detailed description of these alarms and for information about correlation see the *Cisco Active Network Abstraction Fault Management User Guide, 3.6.*