CHAPTER 4

Ethernet (IEEE 802™.3)

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

- Technology Description, page 4-1
- Inventory and Information Model Objects (IMOs), page 4-3
- Vendor Specific Inventory and Information Model Objects, page 4-10
- QinQ (IEEE802.1ad), page 4-11
- Network Topology, page 4-13
- Service Alarms, page 4-13

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 (ILinkAggregationGroup802dot3ad)
- Link Aggregation Group Port Entry (ILagPortEntry)
- Ethernet Interface (IEthernet)
- Ethernet Physical (IPhysicalLayer)
- Virtual LAN Interface (IVlanInterface)
- Virtual LAN Entry (IVlanEntry)
- Virtual LAN Multiplexer (IVlanEncapMux)
- Virtual LAN Encapsulation (IIEEE802)
- Data Link Aggregation Container (IDataLinkAggregationContainer)
- Spanning Tree Protocol Service (IStpService)
- Multiple Spanning Tree Protocol Service (IMstService)
- Multiple Spanning Tree Protocol Properties (IMstProperties)
- Spanning Tree Protocol Instance Information (IStpInstanceInfo)
- Multi Spanning Tree Protocol Instance Information (IMstInstanceInfo)
- Per Virtual LAN Spanning Tree Protocol Instance Information (IPvstpInstanceInfo)
- Rapid Spanning Tree Protocol Instance Information (IRstpInstanceInfo)
- Spanning Tree Protocol Port Information (IStpPortInfo)
- Multi Spanning Tree Protocol Port Information (IMstPortInfo)Cisco's Ethernet Channel (IEthernetChannel)

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 • 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.*