CHAPTER 17

Ethernet (IEEE 802.3)

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

Technology Description

Ethernet (IEEE 802.3)

Ethernet refers to the family of LAN products covered by the IEEE 802.3 standard that defines the carrier sense multiple access collision detect (CSMA/CD) protocol. Four data rates are currently defined for operation over optical fiber and twisted-pair cables: 10Base-T Ethernet (10 Mb/s), Fast Ethernet (100 Mb/s), Gigabit Ethernet (1000 Mb/s) and 10-Gigabit Ethernet (10 Gb/s).

The IEEE 802.3 standard provides MAC (Layer 2) addressing, duplexing, differential services, and flow control attributes, and various physical (Layer 1) definitions, with media, clocking, and speed attributes. It also provides a LAG (similar to EtherChannel) definition for providing both higher link capacity and availability.

VLAN (IEEE 802.1Q)

A virtual LAN (VLAN), is a logical group of hosts that communicate as if they were attached to the same network broadcast domain, even though they do not share the same physical location or network switch. Although much like a physical LAN, VLAN hosts can be grouped together even if they are not located on the same network switch. Because a VLAN is a logical entity, its creation and reconfiguration is done through software, rather than by physically locating devices.

IEEE 802.1Q, or VLAN Tagging, is an IEEE standard allowing multiple bridged networks to transparently share the same physical network link without leakage. IEEE 802.1Q (and its shortened form, dot1q) is used to refer to the encapsulation protocol used to implement this mechanism over Ethernet networks.

QinQ (IEEE802.1ad)

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

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 affecting the traffic of other customers.

LAG

A Link Aggregation Group (LAG) is a group of two or more network links bundled together to appear as a single link based on the IEEE 802.3ad standard. For instance, bundling two 100-Mb/s network interfaces into a single link creates one 200-Mb/s 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.

EtherChannel

EtherChannel is Cisco’s link aggregation port trunking technology. Like LAG, it unifies physical Ethernet links into one link to provide high-speed links between switches, routers, and servers. An EtherChannel can be formed from two to eight active Fast Ethernet, Gigabit Ethernet, or 10 Gigabit Ethernet ports. It also provides fault tolerance in the form of from one to eight inactive failover ports, which can also be aggregated and which become active if the other active ports fail. EtherChannel is primarily a backbone network technology, providing up to 800 Mbps, 8 Gbps, or 80 Gbps of aggregate bandwidth depending on the speeds of the underlying links (100 Mbps, 1 Gbps, or 10 Gbps). Cisco's Virtual Switching System also provides Multichassis EtherChannel (MEC), in which ports can be aggregated toward different physical chassis, forming a single virtual switch.

Metro Ethernet

A Metro Ethernet is a computer network based on Ethernet standards covering a metropolitan area. It is commonly used as a metropolitan access network (MAN) to connect subscribers and businesses to a WAN, such as the Internet. Large businesses can also use Metro Ethernet to connect branch offices to their intranets.

A typical service-provider Metro Ethernet network is a collection of Layer 2 or Layer 3 switches or routers, connected through optical fiber, with a ring, hub-and-spoke (star), full mesh, or partial mesh topology. 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 dense wavelength-division multiplexing (DWDM). Pure Ethernet deployments are cheap but less reliable and scalable, and thus are usually limited to small-scale or experimental deployments. SDH 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 deployments are costly but highly reliable and scalable, and are typically used by large service providers.

STP

Spanning Treee Protocol (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.

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

- STP as defined in the 802.1D standard
- Rapid Spanning Tree Protocol (RSTP) as defined in the 802.1w standard
- Per-VLAN STP (PvSTP and PvSTP+), which are proprietary Cisco protocols, or any per-VLAN spanning tree protocol
- Multiple Spanning Tree protocol (MST) as defined in the 802.1s standard

Note that Cisco ANA does not support these STP modes when they are configured along with a bridge group.

SVI

A switch virtual interface (SVI) is a VLAN of switch ports, represented by one interface to a routing or bridging system. There is no physical interface for the VLAN. The SVI provides the Layer 3 processing for packets from all switch ports associated with the VLAN.

There is one-to-one mapping between a VLAN and SVI. Only a single SVI can be mapped to a VLAN, and the SVI cannot be activated unless associated with a physical port.

SVIs simplify VLAN routing by providing default gateway for the VLAN. They also provide layer 3 switch connectivity to the switch, and provide fallback bridging when required for non routable protocols.

VTP

VLAN Trunk (or Trunking) Protocol (VTP) is a Cisco proprietary Layer 2 messaging protocol that reduces administrative chores in a switched network by managing the addition, deletion, and renaming of VLANs on a network-wide basis. It permits configuration of VLANs on a single VTP server, with the VLAN distributed through all switches in the domain. To enable this, VTP carries VLAN information to all the switches in the VTP domain, using advertisements sent over Inter-Switch Link (ISL), 802.1q, IEEE 802.10 or LAN Emulation (LANE) trunks. VTP traffic is sent over the management VLAN (VLAN1), so all VLAN trunks must be configured to pass VLAN1.

VPLS

Virtual Private LAN Services (VPLS) is a class of Layer 2 VPN that provides Ethernet-based multipoint-to-multipoint communication over MPLS networks. It allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. The network then emulates the function of a LAN switch or bridge to connect the different LAN segments to create a single bridged (Ethernet) LAN.

VPLS uses the provider core to join multiple attachment circuits together to simulate a virtual bridge that connects the multiple attachment circuits together. From a customer point of view, there is no topology for VPLS. All of the CE devices appear to connect to a logical bridge emulated by the provider core. The logical bridge performs MAC address learning, just like a physical bridge.

The Virtual Switching Instance (VSI), also known as the Virtual Forwarding Instance (VFI), is the main component in the PE router which construct the logical bridge. All VSIs which construct a provider logical bridge are connected with MPLS PWs.

Learning is done based on the customer Ethernet frame arriving at the VSI. A Forwarding Information Base (FIB) keeps track of the mapping of customer Ethernet frame addressing and the appropriate pseudowire to use.

H-VPLS

Hierarchical VPLS (H-VPLS) improves the scalability characteristics of VPLS by reducing signaling overhead and packet replication requirements for the provider edge. Two types of provider edge devices are defined in this model:

- User-facing provider edge (u-PE)
- Network provider edge (n-PE)

Customer edge devices connect to u-PEs directly and aggregate VPLS traffic before it reaches the n-PE, where the VPLS forwarding takes place based on the VSI. In this hierarchical model, u-PEs are expected to support Layer 2 switching and to perform normal bridging functions. Cisco VPLS uses 802.1Q Tunneling, a double 802.1Q or QinQ encapsulation, to aggregate traffic between the u-PE and n-PE. The QinQ trunk becomes an access port to a VPLS instance on an n-PE.

Carrier Ethernet

Cisco Carrier Ethernet uses high-bandwidth Ethernet technology to provide Internet access and WAN communications to business and consumer LANs. It enables users to connect their LANs to service provider networks via the same interface they use to attach other network elements. It provides a transparent service that connects LANs in distant locations together as if they were one network. Users can manage these connected networks using VLAN tools that group computers together logically, no matter where they physically reside.

Carrier Ethernet is commonly deployed in three ways:

- Conventional Ethernet—The least expensive type of system, but difficult to modify or expand.
- Ethernet over Synchronous Digital Hierarchy (SDH)—An ideal solution where an SDH infrastructure already exists, but is relatively inflexible and does not always offer the desired degree of management when bandwidth usage varies greatly.
- Ethernet over MPLS—Offers scalability and bandwidth management but is the most expensive technology of the three.

To extend Ethernet to a global network that serves multiple customers, it had to be extensively upgraded to handle fault tolerance, service levels and continuous traffic changes. Carrier Ethernet standards are set via the Metro Ethernet Forum (MEF).

REP

Cisco Resilient Ethernet Protocol (REP) is a new technology implemented on Cisco Carrier Ethernet switches and intelligent service edge routers. It extends network resiliency across Cisco IP Next-Generation Network (NGN) Carrier Ethernet Design. Requiring no hardware upgrades, REP is designed to provide network and application convergence within 50 ms. In some scenarios, the network convergence times may increase to within 250 ms, but a 250-ms convergence time is still expected to have limited or no discernable effect on most network applications. REP is a segment protocol that integrates easily into existing Carrier Ethernet networks. It is not intended to replace STP, but allows network architects to limit the scope of STP domains. Since Cisco REP can also notify STP about potential topology changes, it allows for interoperability with STP. Ideally, REP can be positioned as a migration strategy from legacy spanning tree domains.

Because REP is a distributed and secure protocol, it does not rely on a master node controlling the status of the ring. Hence failures can be detected locally either through loss of signal (LOS) or loss of neighbor adjacency. Any REP port can initiate a switchover as long as it has acquired the secure key to unblock the alternate port. By default, REP elects an alternate port unless the administrator defines a preferred port. For optimal bandwidth usage and for traffic engineering, REP supports load balancing per group of VLANs.

CFM

Ethernet Connectivity Fault Management (CFM) is an end-to-end, per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet MANs and WANs. “End-to-end” can mean PE-to-PE or CE-to-CE. A service can be identified as a service provider VLAN (S-VLAN) or an Ethernet Virtual Connection (EVC) service.

Information Model Objects (IMOs)

This section describes the following IMOs:

- 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)
- Virtual LAN Mapping (IVlanMapping)
- 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)
- Multiple Spanning Tree Protocol Instance Information (IMstInstanceInfo)
- Per-VLAN Spanning Tree Protocol Service (IPvstpService)
- Per-VLAN Spanning Tree Protocol Instance Information (IPvstpInstanceInfo)
- Per-VLAN Spanning Tree Protocol Port Information (IPvstPortInfo)
- Rapid Spanning Tree Protocol Instance Information (IRstpInstanceInfo)
- Spanning Tree Protocol Port Information (IStpPortInfo)
- Multiple Spanning Tree Protocol Port Information (IMstPortInfo)
- Virtual Switch Interface (IVsi)
- Pseudowire Properties (IPseudowireProperties)
- VLAN Tagged Interface (IVLANTaggedInterface)
- Ethernet Flow Point (IEfp)
- VLAN Trunking Protocol Service (IVtpService)
- CFM Service (ICfmService)
- CFM Maintenance Domain (IMaintenanceDomain) (continued)
- CFM Maintenance Point (IMaintenancePoint)
- CFM Maintenance Endpoints (IMaintenanceEndPoints)
- CFM Maintenance Association (IMaintenanceAssociation)
- CFM Maintenance Intermediate Point (IMaintenanceIntermediatePoint)

Link Aggregation Group

The data link layer Link Aggregation Group object aggregates multiple Ethernet Interfaces, which it is bound to by its Containing Termination Points attribute. It is accessed primarily by the Virtual LAN Multiplexer bound by its Contained Connection Termination Points attribute. It is also accessed by the Common Components.

Table 17-1 Link Aggregation Group (ILinkAggregationGroup802dot3ad)

Attribute Name	Attribute Description	Scheme	Polling Interval
Group Number	Group identifier of the aggregated Ethernet interfaces	Any	Configuration
Bandwidth	Accumulated bandwidth of all aggregated Ethernet interfaces in Mb/s	Any	Configuration
Aggregation Protocol	Aggregation protocol (*None, LACP, PAGP*)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (Ethernet Interface)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Link Aggregation Group Port Entry

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

Table 17-2 Link Aggregation Group Port Entry (ILagPortEntry)

Attribute Name	Attribute Description	Scheme	Polling Interval
Actor and Partner Administrative Keys	Actor and partner administrative keys	Any	Configuration
Actor and Partner Operational Keys	Actor and partner operational keys	Any	Configuration
Selected and Attached Aggregation Identification	Selected and attached aggregation identifier	Any	Configuration
Actor Port	Actor port	Any	Configuration
Actor Port Priority	Actor port priority	Any	Configuration
Partner Administrative and Operational Port	Partner administrative and operational port	Any	Configuration
Partner Administrative and Operational Port Priority	Partner administrative and operational port priority	Any	Configuration
Actor and Partner Administrative States	Actor and partner administrative states	Any	Configuration
Actor and Partner Operational States	Actor and partner operational states	Any	Configuration

Ethernet Interface

The data link layer Ethernet Interface object is bound by its Containing Termination Points attribute to a physical layer interface (Ethernet Physical) object. It is accessed primarily by the Virtual LAN Multiplexer/Interface, Link Aggregation Group, Cisco Ethernet Channel or IP Interface bound by its Contained Connection Termination Points attribute. It is also accessed by the Bridging Entity.

Table 17-3 Ethernet Interface (IEthernet)

Attribute Name	Attribute Description	Scheme	Polling Interval
MAC Address	MAC address	Product	Configuration
Duplex Mode	Duplex mode (*Unknown, Full, Half*)	Any	Configuration
Output Flow Control	Output flow control (*Enable, Disable*)	Any	Configuration
Input Flow Control	Input flow control (*Enable, Disable*)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound Connection Termination Point	Any	N/A
Port Type	The port type	Any	N/A

Ethernet Physical

The physical layer Ethernet Physical object is bound by its Containing Termination Points attribute to a Port Connector object. It is accessed by the data link layer Ethernet Interface bound by its Contained Connection Termination Points attribute.

Table 17-4 Ethernet Physical (IPhysicalLayer)

Attribute Name	Attribute Description	Scheme	Polling Interval
All attributes are the same as those of Physical Layer (IPhysicalLayer).			

Virtual LAN Interface

The data link layer Virtual LAN Interface object, which is used in a switched LAN environment, is bound by its Containing Termination Points attribute to an Ethernet Interface object. It is accessed primarily by the network layer object (such as IP Interface) bound by its Contained Connection Termination Points attribute. It is also accessed by the Bridging Entity.

Table 17-5 Virtual LAN Interface (IVlanInterface)

Attribute Name	Attribute Description	Scheme	Polling Interval
Mode	VLAN mode (*Access, Trunk, 802.1Q Tunnel*)	Any	Configuration
Native VLAN Identification	VLAN identifier, used for untagged received and transmitted frames	Any	Configuration
Virtual LAN Table	Array of Virtual LAN Entries (instances of IVlanEntry) configured for this VLAN interface	Any	Configuration
VlanMappings	Array of all Virtual LAN Mappings (instances of IVlanMapping) defined for this VLAN interface	Product	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Virtual LAN Entry

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

Table 17-6 Virtual LAN Entry (IVlanEntry)

Attribute Name	Attribute Description	Scheme	Polling Interval
VLAN Identification	VLAN identifier of received and transmitted frames	Any	Configuration
Encapsulation Type	VLAN encapsulation (*Unknown, ISL, IEEE 802.10, IEEE 802.1Q*)	Any	Configuration
Upper Layer	Upper layer Object Identifier (OID)	Any	Configuration

Virtual LAN Multiplexer

The Virtual LAN Multiplexer object, used in a routed LAN environment, is bound by its Containing Termination Points attribute to an Ethernet Interface object. It is accessed primarily by the data link layer Virtual LAN Encapsulations bound by its Contained Connection Termination Points attribute.

Table 17-7 Virtual LAN Multiplexer (IVlanEncapMux)

Attribute Name	Attribute Description	Scheme	Polling Interval
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Termination Points	Underlying termination points (Ethernet Interface)	Any	N/A
Contained Connection Termination Points	Bound connection termination points (Virtual LAN Encapsulations)	Any	N/A

Virtual LAN Encapsulation

The data link layer Virtual LAN Encapsulation object, used in a routed LAN environment, is bound by its Containing Termination Points attribute to a Virtual LAN Multiplexer object. It is accessed primarily by the Network layer object (such as IP Interface) bound by its Contained Connection Termination Points attribute. It is also accessed by the Bridging Entity.

Table 17-8 Virtual LAN Encapsulation (IIEEE802)

Attribute Name	Attribute Description	Scheme	Polling Interval
VLAN Identification	VLAN identifier	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
Containing Connection Termination Points	Underlying termination points (connection or physical)	Any	N/A
Contained Connection Termination Points	Bound Connection Termination Point	Any	N/A

Virtual LAN Mapping

The data link layer Virtual LAN Mapping object, used in a routed LAN environment, is bound by its Containing Termination Points attribute to a Virtual LAN Multiplexer object. It is accessed primarily by the Network layer object (such as IP Interface) bound by its Contained Connection Termination Points attribute. It is also accessed by the Bridging Entity.

Table 17-9 Virtual LAN Mapping (IVlanMapping)

Attribute Name	Attribute Description	Scheme	Polling Interval
Direction	Describes whether the VLAN mapping is defined in the egress or ingress direction	Product	Configuration
VLANRewriteDefinition	The rewriting actions (push tag, pop tag, and so on.) to be done over the frames which fit the match criteria.	Product	Configuration
VLANMatchCriteria	Defines the frames which undergo the VLAN mapping.	Product	Status
Drop	Defines if the frame should be dropped, instead of undergoing a rewrite definition.	Product	Status

Data Link Aggregation Container

The Data Link Aggregation Container object aggregates or contains a single type of data link aggregation, such as Link Aggregation Group or Cisco Ethernet Channel.

Table 17-10 Data Link Aggregation Container (IDataLinkAggregationContainer)

Attribute Name	Attribute Description	Scheme	Polling Interval
Data Link Aggregations	Array of single-type data link aggregations (Link Aggregation Group, Cisco Ethernet Channel)	Any	Configuration
Type	Aggregation type (*Null, Ethernet Link Aggregator*)	Any	Configuration

Spanning Tree Protocol Service

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

Table 17-11 Spanning Tree Protocol Service (IStpService)

Attribute Name	Attribute Description	Scheme	Polling Interval
Protocol Type	Spanning Tree Protocol type (*Unknown, STP, RSTP, PVSTP, MST*)	Any	Configuration
Current Maximum Age	The current used value for the maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds)	Any	Configuration
Current Hello Time	The current used value for hello time messages' keepalive interval of a Spanning Tree Protocol root (in hundredths of seconds)	Any	Configuration
Current Forward Delay	The current used value for port delay in each of the listening and learning states, preceding the forwarding one (in hundredths of seconds)	Any	Configuration

Table 17-11 Spanning Tree Protocol Service (IStpService) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
Instance Information Table	Array of Spanning Tree Protocol Instance Information	Any	Configuration
UplinkFast State	Indicates whether the UplinkFast feature is enabled *(true, false)*	Any	Configuration
BackboneFast State	Indicates whether the BackboneFast feature is enabled *(true, false)*	Any	Configuration
Bridge Maximum Age	The value that all bridges should use (when this bridge is acting as the root) for the maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds)	Any	Configuration
Bridge Hello Time	The value that all bridges should use (when this bridge is acting as the root) for hello time messages' keepalive interval of a Spanning Tree Protocol root (in hundredths of seconds)	Any	Configuration
Bridge Forward Delay	The current used value, and the value that all bridges should use (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)	Any	Configuration
All additional attributes are the same as System Service (ISystemService)			

Multiple Spanning Tree Protocol Service

The Multiple Spanning Tree Protocol Service object is used in a switched VLAN environment. It describes the Spanning Tree Protocol service. It is accessed only by the Logical Root's Services List attribute.

Table 17-12 Multiple Spanning Tree Protocol Service (IMstService)

Attribute Name	Attribute Description	Scheme	Polling Interval
Protocol Properties	Multiple Spanning Tree Protocol properties	Any	Configuration
All additional attributes are the same as Spanning Tree Protocol Service (IStpService).			

Multiple Spanning Tree Protocol Properties

The Multiple Spanning Tree Protocol Properties object, used in a switched VLAN environment. It describes the Multiple Spanning Tree Protocol properties. It is accessed only by the Multiple Spanning Tree Protocol Service's Protocol Properties attribute.

Table 17-13 Multiple Spanning Tree Protocol Properties (IMstProperties)

Attribute Name	Attribute Description	Scheme	Polling Interval
Force Version	Force version (*Unknown, STP, RSTP, PVSTP, MST*)	Any	Configuration
Configuration Format	Configuration format used by this device and negotiated with other devices	Any	Configuration
Region Name	Region name used by this device and negotiated with other devices	Any	Configuration
Revision Level	Revision level used by this device and negotiated with other devices	Any	Configuration

Table 17-13 Multiple Spanning Tree Protocol Properties (IMstProperties) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
External Root Cost	External root cost of this Multiple Spanning Tree Protocol	Any	Configuration
Maximum Instances	Maximum Multiple Spanning Tree Protocol instances	Any	Configuration

Spanning Tree Protocol Instance Information

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

Table 17-14 Spanning Tree Protocol Instance Information (IStpInstanceInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Object Identification	Instance Object Identifier (OID)	Any	Configuration
Identification	Bridge identifier (MAC address)	Any	Configuration
Priority	Bridge priority in the Spanning Tree Protocol	Any	Configuration
Designated Root and Bridge	MAC addresses of the designated root and bridge in the spanning tree	Any	Configuration
Root Cost	Root cost value for this bridge	Any	Configuration
Is Root	Is this bridge currently the root of the Spanning Tree Protocol? (*True, False*)	Any	Configuration
Root Port Identification	Object Identifier (OID) of the bridge port used to reach the designated root	Any	Configuration
Port Information Table	Array of Spanning Tree Protocol Port Information	Any	Configuration

Multiple Spanning Tree Protocol Instance Information

Table 17-15 Multiple Spanning Tree Protocol Instance Information (IMstInstanceInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Instance Identification	Multiple Spanning Tree Protocol instance identifier	Any	Configuration
All additional attributes are the same as Spanning Tree Protocol Instance Information (IStpInstanceInfo)			

Per-VLAN Spanning Tree Protocol Service

The Per-VLAN Spanning Tree Protocol Service object is used in a switched VLAN environment. It describes the Per-VLAN Spanning Tree Protocol service. It is accessed only by the Logical Root's Services List attribute.

Table 17-16 Per-VLAN Spanning Tree Protocol Service (IPvstpService)

Attribute Name	Attribute Description	Scheme	Polling Interval
UplinkFast	Indicates whether the UplinkFast feature is enabled *(true, false)*	Any	Configuration
BackboneFast	Indicates whether the BackboneFast feature is enabled *(true, false)*	Any	Configuration

Per-VLAN Spanning Tree Protocol Instance Information

Table 17-17 Per-VLAN Spanning Tree Protocol Instance Information (IPvstpInstanceInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Protocol Type	Spanning tree protocol type (*Unknown, STP, RSTP, PVSTP, MST*)	Any	Configuration
Current and Bridge Maximum Age	The current used value, and the value that all bridges should use when this bridge is acting as the root, for the maximum age of learned Spanning Tree Protocol port information (in hundredths of seconds)	Any	Configuration
Current and Bridge Hello Time	The current used value, and the value that all bridges should use when this bridge is acting as the root, for hello time messages' keepalive interval of a Spanning Tree Protocol root (in hundredths of seconds)	Any	Configuration
Current and Bridge Forward Delay	The current used value, and the value that all bridges should use 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)	Any	Configuration
All additional attributes are the same as Spanning Tree Protocol Instance Information (IStpInstanceInfo)			

Per-VLAN Spanning Tree Protocol Port Information

Table 17-18 Per-VLAN Spanning Tree Protocol Port Information (IPvstPortInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
PortFast State	Indicates whether PortFast is enabled on the port (*true*, *false*)	Any	Configuration

Rapid Spanning Tree Protocol Instance Information

Table 17-19 Rapid Spanning Tree Protocol Instance Information (IRstpInstanceInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Force Version	Force version (*Unknown, STP, RSTP, PVSTP, MST*)	Any	Configuration
All additional attributes are the same as Spanning Tree Protocol Instance Information (IStpInstanceInfo)			

Spanning Tree Protocol Port Information

The following Spanning Tree Protocol Port Information objects describe the port information associated with and accessed by the Spanning Tree Protocol Instance Information's Port Information Table attribute.

Table 17-20 Spanning Tree Protocol Port Information (IStpPortInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Object Identification	Port Object Identifier (OID)	Any	Configuration
Priority	Port priority in the Spanning Tree Protocol	Any	Configuration
State	Port state (*Unknown, Disable, Blocking, Listening, Learning, Forwarding, Broken, Down, LoopBack*)	Any	Configuration
Path Cost	Port path cost, which represents the media speed for this port	Any	Configuration
Is Edge	Is this an edge port (connected to a nonbridging device)? (*True, False*)	Any	Configuration
Is Point To Point	Is this port connected to a point-to-point link? (*True, False*)	Any	Configuration
Role	Port role (*Unknown, Disable, Backup, Alternative, Designated, Root, Boundary*)	Any	Configuration
Port BPDU Guard State	Indicates whether the PortFast Bridge Protocol Data Unit guard is enabled on the port	Any	Configuration
Port BPDU Filter State	Indicates whether PortFast Bridge Protocol Data Unit filtering is enabled on the port	Any	Configuration

Multiple Spanning Tree Protocol Port Information

Table 17-21 Multiple Spanning Tree Protocol Port Information (IMstPortInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
Hello Time	Hello time messages' keepalive interval of a Spanning Tree Protocol root (in hundredths of a second)	Any	Configuration
All additional attributes are the same as Spanning Tree Protocol Port Information (IStpPortInfo)			

Virtual Switching Instance

The Virtual Switching Instance object represents a Virtual Switching Instance (also known as VFI, Virtual Forwarding Instance) component of a VPLS logical bridge.

Table 17-22 Virtual Switch Interface (IVsi)

Attribute Name	Attribute Description	Scheme	Polling Interval
VPLS Instance Name	The unique VPLS instance name	IPCore	Configuration
VPLS VPN ID	The unique VPN ID in the MPLS core	IPCore	Configuration
discoveryMode	The VSI discovery mode (*Manual*, *BGP*, *LDP*, *RADIUS*, *DNS*, *MSS/OSS*, *Unknown*)	IPCore	Configuration
vsiMode	The VSI mode (*point-to-point*, *multipoint*, *unknown*)	IPCore	Configuration
Operational state	The operational status of the VPLS instance (*up*, *down*)	IPCore	Configuration
Administrative state	The configured administrative status of the VPLS instance (*enabled*, *disabled*)	IPCore	Configuration
Pseudowires	An array of Pseudowire Properties (IPseudowireProperties).	IPCore	System

Pseudowire Properties

The Pseudowire Properties object represents an MPLS pseudowire connecting two or more Virtual Switching Instances.

Table 17-23 Pseudowire Properties (IPseudowireProperties)

Attribute Name	Attribute Description	Scheme	Polling Interval
Pseudowire OID	The Object Identifier of the pseudowire	IPCore	System
isSplitHorizonEnabled	Indicates whether split horizon is enabled on the pseudowire (*true*, *false*). The split horizon policy determines whether packets are returned to the MPLS core.	IPCore	System
isAutoDiscovered	Indicates how the pseudowire was discovered (*manual*, *automatic*).	IPCore	System

VLAN Tagged Interface

The VLAN Tagged Interface object represents a VLAN interface on which both dot1Q and QinQ VLAN are supported.

Table 17-24 VLAN Tagged Interface (IVLANTaggedInterface)

Attribute Name	Attribute Description	Scheme	Polling Interval
InterfaceName	Name of the VLAN subinterface on which VLAN IDs are configured.	Product	Configuration
Inner Vlan Id	The configured customer-edge VLAN (CE-VLAN) ID.	Product	Configuration
Outer Vlan Id	The configured service-provider VLAN (SP-VLAN) ID.	Product	Configuration
Encap Type	The encapsulation type (*dot1Q*, *QinQ*).	Product	Configuration
Match Criteria	The match criteria compared against the arriving frame's first and second VLAN tags.	Product	Configuration
Operational state	The operational status of the subinterface that the QinQ resides on.	Product	System
Administrative state	The administrative status of the subinterface that the QinQ resides on.	Product	System

Ethernet Flow Point

The Ethernet Flow Point object represents a forwarding decision point in provider edge switch routers that allows Layer 2 traffic flow decisions to be made within the interface itself. Any number of EFPs can be configured on a single physical Layer 2 traffic port (usually on the User-Network Interface [UNI] port) and each can manipulate inbound frames in a different manner and make different forwarding decisions.The Ethernet Flow Point is accessed by a Virtual LAN Multiplexer.

Table 17-25 Ethernet Flow Point (IEfp)

Attribute Name	Attribute Description	Scheme	Polling Interval
EfpId	ID of the Ethernet Flow Point.	Product	Configuration
RewriteParams	The rewriting actions (*push tag*, *pop tag*, and so on.) which will be done over the frames which fit the match criteria.	IPCore	Configuration
EncapsParams	Encapsulation parameters (dot.q and dot.ad, IEEE).	Product	Configuration
AdminStatus	The administrative status of the service instance.	Product	System
OperStatus	The operational status of the service instance.	Product	System
SplitHorizonGroup	Flag indicating whether a split horizon group is configured for the EFP. If *null*, no split horizon group is defined. If split horizon is enabled on the EFP, this will always contain the default group *0*.	Product	Configuration
matchCriteria	The EFP match criteria compared against the arriving frame's first and second VLANs tags.	IPCore	Configuration

VLAN Trunking Protocol Service

The VLAN Trunking Protocol Service object represents a VTP configuration on a switch. It extends System Service.

Table 17-26 VLAN Trunking Protocol Service (IVtpService)

Attribute Name	Attribute Description	Scheme	Polling Interval
Version	The VTP version (*Version1*, *Version2*, *Version3*)	Product	Configuration
OperatingMode	The VTP mode (*Server, Client*, *Transparent*, *Primary Server*, *Secondary Server*, *Off*)	Product	Configuration
DomainName	The VTP domain name	Product	Configuration
ConfigurationRevision	The VTP's configuration revision number	Product	Configuration
isPruningEnabled	Indicates whether VTP is enabled on the switch (*True*, *False*)	Product	Configuration
isAuthenticationEnabled	Indicates whether VTP authentication is enabled on the switch (*True*, *False*)	Product	Configuration

CFM Service

The CFM Service object represents an instance of CFM enabled on a device.

Table 17-27 CFM Service (ICfmService)

Attribute Name	Attribute Description	Scheme	Polling Interval
cacheSize	The CFM traceroute cache size used by the CFM service.	IP Core	Configuration
maximumCacheSize	The CFM traceroute maximum cache size used by the CFM service.	IP Core	Configuration
holdTime	The configured hold-time value used to indicate to the receiver the validity of traceroute and loopback messages transmitted by this device. The default is 2.5 times the transmit interval.	IP Core	Configuration
version	The CFM version running on the device.	IP Core	Configuration
maintenanceIntermedatePointsTable	An array of all the CFM Maintenance Intermediate Point objects configured on the device.	IP Core	Configuration
maintenanceDomain	The CFM Maintenance Domain configured on the device.	IP Core	Configuration

CFM Maintenance Domain

The CFM Maintenance Domain object represents an instance of a CFM management space used to manage and administer a network. A CFM management domain is owned and operated by a single entity and defined by the set of ports internal to it and at its boundary.

Table 17-28 CFM Maintenance Domain (IMaintenanceDomain) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
name	The name of the management domain. This must be unique and cannot be used within a different maintenance level.	IP Core	Configuration
level	The domain level (an integer in the range *0* to *7*). Domain levels permit creation of a domain hierarchy. The larger the level value, the larger the domain. For instance, the costumer domain will have a level of 7, and the operator domain will have a level of 0.	IP Core	Configuration
Id	The domain ID. Optional and may not be defined. When undefined, the domain name is used as the default value.	IP Core	Configuration
maintenanceAssociation	A list of the domain's CFM Maintenance Associations. These are the associations represented by the service. In Cisco devices, the domain is mapped to a VLAN.	IP Core	Configuration

CFM Maintenance Point

The CFM Maintenance Point object represents an instance of a CFM maintenance point configured on one or more of a device's interfaces.

Table 17-29 CFM Maintenance Point (IMaintenancePoint)

Attribute Name	Attribute Description	Scheme	Polling Interval
macAddress	The MAC address on the the interface on which the maintenance point is configured. In different interface modes, the MAC address may hold different values. For example, an inward facing interface uses the Bridge-Brain MAC address; an outward facing interface, such as a routed port, uses the port MAC address; and outward facing MEPs on port channels use the Bridge-Brain MAC address of the first member link. When port channel members change, the identities of outward facing MEPs do not have to change.	IP Core	Configuration
Interface	A link to the interface on which the maintenance point is configured. This property includes all interface types that can be configured with CFM maintenance points.	IP Core	Configuration

CFM Maintenance Endpoint

The CFM Maintenance Endpoint object represents an instance of a CFM Maintenance Endpoint (MEP),. Unlike MIPs, MEPs are associated by a CFM Maintenance Association (S-VLAN).

Table 17-30 CFM Maintenance Endpoints (IMaintenanceEndPoints)

Attribute Name	Attribute Description	Scheme	Polling Interval
Id	The ID of the MEP (an integer from *1* and *8191*). It identifies the MEP in CFM communications and to catalog CFM frames in the local CFM database. The MEP ID is meaningful throughout the CFM domain and through the maintenance association.	IP Core	Configuration
Continuity Check Status	Current MEP status sent to other MEPs and MIPs via multicast CCMs (*Unknown*, *MEP active*, *MEP inactive*, *MEP enabled*, *MEP disabled*). CCMs are confined to a domain and S-VLAN.	IP Core	Configuration
direction	Direction of the MEP (*inward facing*, *outward facing*). Inward facing means the MEP communicates through the Bridge Relay function and uses the Bridge-Brain MAC address. Outward facing means that the MEP communicates through the wire. Outward facing MEPs can be configured on routed ports and switch ports. A MIP configuration at a level higher than the level of the outward facing MEP is not required.	IP Core	Configuration
cfmRemoteMaintenanceEndPoints	An array listing all the remote CFM MEPs that were discovered through this MEP. Properties for each remote MEP are used to establish CFM topology between CFM MEPs.	IP Core	Configuration

CFM Maintenance Association

The CFM Maintenance Association object models a grouping of CFM Maintenance Endpoint.

Table 17-31 CFM Maintenance Association (IMaintenanceAssociation)

Attribute Name	Attribute Description	Scheme	Polling Interval
name	The Association name.	IP Core	Configuration
associationType	The Association type (*Unknown*, *Bridge Domain VLAN*, *Bridge Domain*, *Port*, *Pseudowire*).	IP Core	Configuration
maximalMeps	The maximum number of MEPs that can be configured on the Maintenance Association.	IP Core	Configuration
continuityCheckInterval	The configured time interval between continuity checks performed by the Maintenance Association's MEPs.	IP Core	Configuration

Table 17-31 CFM Maintenance Association (IMaintenanceAssociation) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
continuityCheckEnable	Indicates whether continuity checking is enabled for the Association. CFM continuity checks are periodic heartbeat messages exchanged betweenthe MEPs under the association. They allow MEPs to discover each other and CFM Maintenance Intermediate Points to discover the MEPs.	IP Core	Configuration
crossCheckEnable	Indicates whether cross-checking is enabled for the Association. CFM cross-checking verifies that all end points of a service are operational. It is timer-driven and performed once.	IP Core	Configuration
direction	The direction of the association (*up*, *down*, *unknown*).	IP Core	Configuration
bridge	Object Identifier of the bridge on which the association (VLAN) is configured.	IP Core	Configuration
maintenanceEndPoints	An array of the CFM Maintenance Endpoint configured within the bounds of the CFM Maintenance Domain.	IP Core	Configuration

CFM Maintenance Intermediate Point

The CFM Maintenance Intermediate Point object represents a single instance of a CFM Maintenance Intermediate Point (MIP). Unlike MEPs, MIPs are not grouped by CFM Maintenance Associations (S-VLAN). Instead, they are grouped by CFM Maintenance Domain (using the Level parameter) and for all S-VLANs enabled or allowed on a port.

Table 17-32 CFM Maintenance Intermediate Point (IMaintenanceIntermediatePoint)

Attribute Name	Attribute Description	Scheme	Polling Interval
level	The level defined for this MIP. This is the same as the Level parameter defined for CFM Maintenance Domains: An integer from 0 to 7, assigned to each MIP for the purpose of creating hierarchical relationships among MIPs. All CFM frames at a level lower than the level assigned to the MIP are stopped and dropped, independent of whether they originate from the wire or relay function. All CFM frames at a higher level than the MIP are forwarded, independent of whether they arrive from the wire or relay function.	IP Core	Configuration
cfmInterface	The normalized name of the interface on which the MIP is configured.	IP Core	Configuration
isAutocreated	Indicates whether this MIP was created automatically (*true*) or by entering properties manually using the command-line interface (CLI) (*false*).	IP Core	Configuration
Vlans	A list of the VLANs in which this MIP participates. A MIP configured on an interface normally functions via maintenance domain (level) and for all S-VLANs enabled or allowed on that port. To limit its functionality, however, a CFM MIP can also be configured with a list of S-VLANs or associations.	IP Core	Configuration
macAddress	The MAC address that identifies the CFM entity (for example, *bridge-brain MAC*).	IP Core	Configuration

Vendor-Specific Inventory and IMOs

Vendor-specific IMOs are implemented only for specific vendor devices. The following sections describe vendor-specific objects for this technology:

- Cisco Ethernet Channel
- Cisco REP Service
- Cisco REP Segment Information
- Cisco REP Port Information

Cisco Ethernet Channel

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

Table 17-33 Cisco Ethernet Channel (IEthernetChannel)

Attribute Name	Attribute Description	Scheme	Polling Interval
Group Number	Group identifier of the aggregated Ethernet interfaces	Any	Configuration
Bandwidth	Accumulated bandwidth of all aggregated Ethernet interfaces, in Mb/s	Any	Configuration
Aggregation Protocol	Aggregation protocol (*Manual, LACP, PAGP*)	Any	Configuration
IANA Type	Internet Assigned Numbers Authority (IANA) type of the sublayer	N/A	N/A
MAC Address	MAC address of the aggregated Ethernet interfaces	Any	Configuration
Administrative Status	Administrative status of the aggregated interfaces	Any	Configuration
Operational Status	Operational status of the aggregated interfaces	Any	Configuration
Containing Connection Termination Points	Underlying termination points (Ethernet Interface)	Any	N/A
Contained Connection Termination Points	Bound connection termination points	Any	N/A

Cisco REP Service

The Cisco REP Service object represents REP protocol configured on a device.

Table 17-34 Cisco REP Service (IREPService)

Attribute Name	Attribute Description	Scheme	Polling Interval
version	The version of REP being used.	IP Core	Configuration
administrativeVlan	The ID of the administrative VLAN used by REP to transmit its hardware flooding layer messages (an integer from *1* to *4094*).	IP Core	Configuration
notificationEnabled	Indicates whether the device will generate REP notifications.	IP Core	Configuration
segmentsTable	An array of Cisco REP Segment Information objects.	IP Core	Configuration

Cisco REP Segment Information

The Cisco REP Segment Information object represents a single REP segment.

Table 17-35 Cisco REP Segment Information (IREPSegmentInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
segmentId	The ID of the segment.	IP Core	Configuration
segmentComplete	Indicates whether the segment is complete (that is, no port in the segment is in the “failed” state).	IP Core	Configuration
portsTable	An array of Cisco REP Port Information objects.	IP Core	Configuration

Cisco REP Port Information

The Cisco REP Port Information object represents a REP port.

Table 17-36 Cisco REP Port Information (IREPPortInfo)

Attribute Name	Attribute Description	Scheme	Polling Interval
portName	The interface name.	IP Core	Configuration
portKey	The Object Identifier of the port.	IP Core	Configuration
segmentId	The segment of which the interface is a part.	IP Core	Configuration
portType	The type of port (*Primary*, *Secondary*, *Intermediate*).	IP Core	Configuration
portRole	The role the REP port is playing, determined by its link state and whether it is forwarding or blocking traffic (*Failed*, *Alternate*, *Open*).	IP Core	Configuration
operStatus	The current operational link state of the REP port (*None*, *Init Down*, *No Neighbor*, *One Way*, *Two Way*, *Flapping*, *Wait*, *Unknown*).	IP Core	Configuration
blockedVlans	The list of VLANs configured to be blocked at the alternate port. This value is only effective on the alternate port (i.e. if the portRole value is *alternate*). Formats are: *800-850,1050-1200,2900-2999,3555*.	IP Core	Configuration

Table 17-36 Cisco REP Port Information (IREPPortInfo) (continued)

Attribute Name	Attribute Description	Scheme	Polling Interval
preemptTimer	Specifies the time interval that REP waits before triggering preemption after the segment is complete (an integer from *0* to *300*, or *Disabled*) *Disabled* indicates that no time delay is configured and the preemption will happen manually. This value is only effective on the device acting as the REP primary edge.	IP Core	Configuration
lslAgeoutTimer	The link status layer age-out timer; that is, the time, in milliseconds, for which the REP interface remains up without receiving a hello from a neighbor.	IP Core	Configuration
remoteDeviceName	The name of the neighbor device on the segment to which this port is connected (may be null).	IP Core	Configuration
remoteDeviceMac	The MAC address of the neighbor bridge on the segment to which this port is connected (may be null).	IP Core	Configuration
remotePortName	The name of the neighbor port on the neighbor bridge on the segment to which this port is connected (may be null)	IP Core	Configuration

Network Topology

Cisco ANA conducts discovery of Ethernet data link layer topology by using various types of data. This includes information from CDP, LLDP, STP, and can include MAC learning information. All types of data are collected and, based on priority, used to verify the adjacency between two ports.

Connections between CDP and LLDP ports are straightforward, as they expose neighbor information.

For STP topology, the STP port information is used in the following way: The Bridge ID, Designated Bridge, and Port identifier are compared with the relevant remote information. If a match is found, a link is created.

MAC-based topology is traced by searching for the local MAC address on any remote side's bridge or in 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.

Verification is done based on STP, CDP, and LLDP. Further verification is preformed by matching the traffic signature of these ports using Cisco's confidential scheme, which requires a substantial amount of network traffic to function correctly.

Many service providers configure customer access to VLAN ports using L2PT. This avoids the need to process Layer 2 protocols such as CDP. In these scenarios, discovery may create links between ports which are not directly connected, because the Layer 2 protocol information is tunneled and does not reflect the actual physical links. Users can overcome this problem by configuring static links on these ports. These static links will override any incorrect dynamically discovered links.

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
- VSI Down/VSI Up
- EFP Down/EFP Up
- VLAN Sub Interface Down/VLAN Sub Interface Up

Note that these alarms, apart from Cloud Problem, are related to the underlying physical interface (see Common Components).

Cisco ANA does not generate service alarms specific to QinQ technology. However, correlation takes this technology into account when performing flow analysis.

For detailed information about alarms and correlation, see the *Cisco Active Network Abstraction 3.7 User Guide*.