CHAPTER 38

Cisco ANA VNE Topology

This chapter describes the Cisco ANA VNE Topology, as follows:

Specifications

Table 38-1 describes the types of topologies Cisco ANA supports and how Cisco ANA discovers and displays them. Discovery takes place in two phases:

1. Discovery of existing links.
2. For discovered links, verification that the links still exist.

The Topology Type column identifies the type of technology to which each Link Type is related.

The Link Type column displays the link type as exposed by Cisco ANA.

Table 38-1 Types of Topologies Supported by Cisco ANA

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
ATM	ATM	ATM VC Counters: 1. Same Active VCs 2. VC traffic signature; see Traffic Signature.	Physical layer counters. See physical layer counters in Physical Layer.	Active VCs—Each side identifies a set of active VCs and looks for a match with the same set on another port in the network. An active VC, is a VC that has a configured level of traffic. VC Traffic Signatures—Based on the VCs counters; see Traffic Signature.
		CDP	CDP. See CDP (Cisco Discovery Protocol).	
		Static	Static	

Table 38-1 Types of Topologies Supported by Cisco ANA (continued)

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
ATM	PNNI	PNNI Information	None	PNNI Information—In this technique, each port in the ATM switch is identified with two values: 1. Node ID. 2. Port ID.
BFD	BFD	BFD session's source and destination addresses	BFD session's source and destination addresses	In this technique, the BFD session's source and destination addresses are verified by matching them against the source and destination addresses of the potential adjacent neighbors. The matching is session source to neighbor destination and session destination to neighbor source, respectively, as one side's source is the other side's destination. This method assumes that multiple BFD sessions running on the same router cannot have the same source and destination address.
BGP	BGP	BGP Info	BGP Info	BGP Info—In this technique, for each BGP Neighbor Entry the local BGP identifier is compared to the remote BGP identifier or a potential neighbor. This topology technique assume uniqueness of the BGP identifier in the network.
Business	Business	N/A	N/A	Business links are not discovered at the VNE level; they are created in the gateway. These links represent a relationship between any two objects in the model, which can be business or network related.
LAG	LAG	STP	STP. See STP (Spanning Tree Protocol).	
		MAC	MAC	In this technique, the Ethernet port MAC is checked to see if it is the only one learned on the other Ethernet port (using bridge and ARP tables). This technique discovers links between two routers and links between the router and switch, but not between two switches (includes the generic VNE).
		REP	REP	If REP is enabled between switches, the information that is provided by the 'show REP topology' command is used to connect the topology according to the REP configuration.
		LACP	LACP	If the LAG is configured as LACP, actor and partner system ID are compared between the two devices (local actor = remote partner and vice versa).

Table 38-1 Types of Topologies Supported by Cisco ANA (continued)

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
Ethernet	Ethernet	MAC	Ethernet counters and physical layer counters; see physical layer counters in Physical Layer.	In this technique, the Ethernet port MAC is checked to see if it is the only one learned on the other Ethernet port (using bridge and ARP tables). This technique discovers links between two routers and links between the router and switch, but not between two switches (includes the generic VNE). Ethernet Counters—Based on the Unicast Packets traffic signature, see Traffic Signature.
		CDP	CDP	See CDP (Cisco Discovery Protocol).
		LLDP	LLDP	See LLDP (Link Layer Discovery Protocol).
		STP	STP	See STP (Spanning Tree Protocol).
		REP	REP	If REP is enabled between switches, the information that is provided by the 'show REP topology' command is used to connect the topology according to the REP configuration.
		Static	Static	
Frame Relay	Frame Relay	Not Supported	Physical layer counters. See physical layer counters in Physical Layer.	Frame Relay links can be discovered dynamically only between Cisco devices with CDP enabled, or by using static or manual configuration (physical link discovery).
		CDP	CDP. See CDP (Cisco Discovery Protocol).	
		Static	Static	
MLPPP	MLPPP	MLPPP End Point Identifier	MLPPP End Point Identifier	In this technique, the Local and the Remote MLPPP End Point Identifier are verified by matching them against the Remote and the Local MLPPP End Point Identifier of the potential adjacent neighbors. The matching is from the Local MLPPP End Point Identifier to the neighbor Remote MLPPP End Point Identifier respectively.
MPLS	MPLS	IP Information	IP Information	IP Information—In this technique, the IP addresses of the multiple MPLS interfaces are checked to see if they are in the same subnet (includes the generic VNE). For more information, see IPv4 IP Topology Testing.

Table 38-1 Types of Topologies Supported by Cisco ANA (continued)

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
PPP or HDLC	PPP or HDLC	IP Information	IP Information and physical layer counters. See physical layer counters in Physical Layer.	IP Information—In this technique, the IP addresses of the multiple PPP or HDLC interfaces are checked to see if they are in the same subnet (includes the generic VNE). For more information, see IPv4 IP Topology Testing.
		CDP	CDP. See CDP (Cisco Discovery Protocol).	
		Static	Static	
Physical Layer	Physical Layer	A physical link is not discovered independently. Physical links are created as a result of the discovery of Layer 2 links, such as ATM and Ethernet.	Physical Layer Counters	By default, the physical layer does not have specific techniques for discovery. Special cases are: • Ports from the same device will not be connected. • Static topology may be used in the physical layer. For more information, see Physical Layer. Physical Layer Counters—Based on the port traffic signature, using octet-based, or octet- and packet-based traffic; see Traffic Signature. **Note** In the discovery phase of physical topology, use the Same Device test. In this technique, the port is checked to see if it is in separate VNEs depending on the type of managed equipment.
		Static	Static	
PWE3	Tunnel	PWE3 Information	PWE3 Information	PWE3 Information—In this technique, each pseudowire is identified by the following criteria: 1. Local and Remote router IP. 2. Tunnel ID. Matching between two pseudowire tunnels Pw1 and Pw2 is conducted by comparing: 1. The Pw1 local IP to the Pw2 remote IP and the Pw1 remote IP to the Pw2 local IP. 2. Tunnel ID.

Table 38-1 Types of Topologies Supported by Cisco ANA (continued)

Topology Type	Link Type	Discovery Technique	Verification Technique	Description
GRE Tunnel	Tunnel GRE	GRE Tunnel Information	GRE Tunnel Information	GRE Tunnel Information—In this technique, each GRE tunnel is identified by the following criteria: 1. Source IP. 2. Destination IP. Matching between two tunnels T1 and T2 is done by comparing the T1 source to the T2 destination and the T1 destination to the T2 source.
VLAN	VLAN	VLAN ID matching	VLAN ID matching	In this technique, the VLAN configuration aspects of each pair of VLAN-enabled physically connected Ethernet ports will be inspected to identify which VLAN tagged traffic crosses this link. The type of VLAN configurations that are inspected include: • Switchport in all configuration modes (Access, Trunk, Dot1q_Tunnel), including the VLAN allowed and VLAN mapping. • L2 sub-interfaces/service instances configured on the Ethernet port, specifically the VLAN tag matching criteria. • L3 sub-interfaces configured on the Ethernet port, specifically the VLAN tag matching criteria.
VPN (VRF)	VPN	Route Targets	Route Targets	Route Targets—In this technique, each VRF is identified with the set of its import and export route targets (for either IPv4 or IPv6 address families). The matching criteria between two VRF entities will be matching at least one pair of import or export route targets of the one VRF to the export or import route targets of the other VRF.
	VPNv6	Route Targets for IPv6 Address Family	Route Targets for IPv6 Address Family	

Physical Layer

In Cisco ANA's topology discovery implementation, physical layer (Layer 1) discovery is coupled with data link layer (Layer 2) discovery. By default, the physical layer does not have techniques for discovery, but rather complements the discovery of Layer 2, in the following ways:

- Ports from the same device are not connected (this validation is done in the physical layer).
- If static topology is configured, it is used in the physical layer.

In addition, the physical layer is used for topology verification (that is, if a link has already been discovered, it is tested periodically). This verification is done in the physical layer using counters. Physical layer counters are based on the port traffic signature, using octet-based or octet- and packet–based traffic.

IPv4 IP Topology Testing

Cisco ANA uses IP testing to discover the topology for PPP/HDCL and MPLS technologies. In both cases, the IP test checks the IP configuration on the relevant interface(s) and verifies that there is a match. In this context, finding a match means that the IP configuration is compared using the *primary* IP subnet configured on the local and remote interfaces, and the local IP subnet is equal to or contained in the remote IP subnet.

Note that there is an inherent limitation in using only the primary address and mask to define the IP subnet to be compared. This can cause issues if two interfaces are connected but have more than one address and, in either or both cases, the primary is from a different subnet. For example: We have two devices, Device1 and Device2. POS2/1 on Device1 is connected to POS1/1 on Device2. Device1's configuration is:

```
interface POS2/1
 description Connected to POS1/1 on Device2
 encapsulation ppp ip address 10.0.0.1 255.255.255.252
 ip address 11.0.0.1 255.255.255.252 secondary
```

Device2's configuration is:

```
interface POS1/1 description Connected to POS2/1 on Device1
 encapsulation ppp ip address 11.0.0.2 255.255.255.252
 ip address 10.0.0.2 255.255.255.252 secondary
```

In this case, the two devices will *not* be connected.

CDP (Cisco Discovery Protocol)

For Cisco devices, if CDP is enabled, its information will be used for discovery and verification. This includes any upper layer techniques, such as VC-related techniques in ATM or MAC in Ethernet. In this technique, the matching criteria is the CDP neighbor information.

LLDP (Link Layer Discovery Protocol)

If LLDP is enabled, its information will be used for discovery and verification. In this technique, the matching criteria is the LLDP neighbor information.

STP (Spanning Tree Protocol)

If STP is enabled between switches, it has the highest priority and its information will be used for discovery and verification. In this technique the STP port information is used in the following way: bridge ID, designated bridge, and port identifier are compared with the relevant remote information. If a match is found, a link is created.

Note This STP discovery technique will work correctly only when the same STP protocol is running on both ports.

Traffic Signature

Traffic signature is based on traffic pattern analysis. The underlying assumption of traffic pattern analysis is that network traffic variety ensures that every active link or active ATM VC in the network maintains a differential traffic “fingerprint”.

Consequently, any two connected ports or VCs will have similar trend functions, which can be matched within reliable statistical significance.

Topology Types

The following topology types are described in this section:

- ATM
- BFD
- BGP
- Business
- Ethernet
- LAG
- Frame Relay
- MPLS
- PPP or HDLC
- Physical Layer
- PWE3
- GRE Tunnel
- VPN

ATM

ATM topology represents a link between two ATM ports which are connected in the network. In the VNE model, the endpoints of the link are ATM IMOs (ATM Interface (IAtm)) which represent the ATM port or interface.

BFD

BFD topology represents a BFD session, with verified BFD connectivity, between two endpoints in the network. In the VNE model, the endpoints of the link are the BFD Service IMOs (BFD Service (IBfdService)), which represent the BFD service running on the router.

BGP

BGP topology represents a TCP connection between two BGP entities which facilitate the “BGP neighborhood” in the network. In the VNE model, the endpoints of the link are the MPBgp IMOs (Multi Protocol BGP Entity), which represent the BGP service running on the router.

Business

Business topology does not represent any specific link or relationship in the network. It can represent the relationship between any two objects in the model, which can be a business object or network objects. These links are created in the Cisco ANA gateway.

Ethernet

Ethernet topology represents a link between two Ethernet ports which are connected in the network. In the VNE model the endpoints of the link are Ethernet IMOs (Ethernet Interface (IEthernet)), which represent the Ethernet ports.

LAG

LAG topology represents a link between two LAG or EtherChannel ports which are connected in the network. The underlying physical links do not have to be discovered for the LAG link to be discovered.

In the VNE model the endpoints of the link are indicated in the Data Link Aggregation Container (IDataLinkAggregationContainer) IMO, which points to the LAG or EtherChannel ports.

Frame Relay

Frame Relay topology represents a link between two Frame Relay ports which are connected in the network. In the VNE model the endpoints of the link are FrameRelay IMOs (Frame Relay Interface (IFrameRelay/IFrTrunk)), which represent the Frame Relay ports.

MPLS

MPLS topology represents adjacent MPLS interfaces in the network. This adjacency represents that these MPLS interfaces forward MPLS (labeled) traffic between them. Labels may be learned using discovery protocols, such as LDP or TDP (Cisco), or may be manually configured. In the VNE model the endpoints of the link are MPLS IMOs (MPLS Interface (IMpls)), which represent the MPLS interfaces.

PPP or HDLC

PPP or HDLC topology represents a link between two PPP or HDLC ports which are connected in the network. In the VNE model the endpoints of the link are PPP and HDLC IMOs (HDLC Encapsulation (IEncapsulation), which represent the ports.

Physical Layer

Physical Layer topology represents a link between the physical layers of two ports connected in the network. In the VNE model the endpoints are IMOs which inherit from the physical layer (Layer 1) IMOs (Serial Interface (IPhysicalLayer)), such as SONET/SDH Physical (ISonetSdh) and DS3 Channelized Interface (IDS3PdhChannelized), which represent physical layers of a port.

PWE3

PWE3 topology represents a link between the endpoints of an MPLS-based pseudowire tunnel in the network. In the VNE model the endpoints of the link are PTP Layer 2 MPLS tunnel IMOs (PTP Layer 2 MPLS Tunnel Interface (IPTPLayer2MplsTunnel)), which represent the pseudowire tunnel endpoints.

GRE Tunnel

GRE Tunnel topology represents a link between the endpoints of a GRE tunnel in the network. In the VNE model the endpoints of the link are TunnelGre IMOs (Generic Routing Encapsulation (GRE) Tunnel Interface (ITunnelGRE)), which represent the GRE tunnel endpoints.

VPN

VPN topology represents a link between two VRFs that are part of a VPN, meaning that VPN traffic can pass between customer sites connected to these VRFs. In the VNE model the endpoints of the link are VRF IMOs (Virtual Routing Forwarding (VRF) Entity (IVrf)), which represent the VRF forwarding entities in the network element.