CHAPTER 38

Cisco ANA VNE Topology

This chapter describes the types of topologies Cisco ANA supports and how Cisco ANA discovers and displays them, as follows:

Supported Topology Types

The following topology types are supported by Cisco ANA 3.7.2:

- ATM
- BFD
- BGP
- Business
- Ethernet
- LAG
- Frame Relay
- MPLS
- PPP or HDLC
- Physical Layer
- Pseudowire
- 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.

Link type: ATM or PNNI

Discovery technique for ATM link:

- ATM VC Counters
- CDP (Cisco Discovery Protocol)
- Static

Verification Technique: Physical Layer Counters

Discovery technique for PNNI link:

- PNNI Information

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.

Link type: BFD

Discovery and verification technique: BFD Session Source and Destination

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.

Link type: BGP

Discovery and verification technique: BGP Information

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 business objects 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.

Cisco ANA conducts discovery of Ethernet data link layer topology by using various types of data. This includes information from, for example, OAM, 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.

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. This problem can be overcome by configuring static links on these ports. These static links will override any incorrect dynamically discovered links.

Link type: Ethernet

Discovery techniques:

- OAM
- MAC
- CDP (Cisco Discovery Protocol)
- LLDP (Link Layer Discovery Protocol)
- STP (Spanning Tree Protocol)
- REP
- Static

Verification Technique: All of the above discovery techniques and Physical Layer Counters.

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.

Link type: LAG

Discovery and verification techniques:

- MAC
- STP (Spanning Tree Protocol)
- REP
- LACP
- Static

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.

Frame Relay links between Cisco devices with CDP enabled can be discovered dynamically. For all other cases, static or manual configuration can be used.

Link type: Frame Relay

Discovery techniques:

- CDP (Cisco Discovery Protocol)
- Static

Verification Techniques: The above discovery techniques and Physical Layer Counters.

MPLS

MPLS topology represents adjacent MPLS interfaces in the network. 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.

Cisco ANA discovers MPLS network layer topology by searching for the existence of the local IP subnet in any one-hop-away remote side's MPLS Interface. In particular, it compares the local and remote IP subnets gathered from the upper IP network layers.

Link type: MPLS

Discovery and verification techniques: IP Testing

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.

Cisco ANA performs discovery of PPP or HDLC topologies by searching for the local IP subnet in any one-hop-away remote side's PPP or HDLC interface. In particular, it compares the local and remote IP subnets gathered from the upper IP Network layers.

Discovery techniques:

- IP Testing
- CDP (Cisco Discovery Protocol)
- Static

Verification Techniques: The above discovery techniques and Physical Layer Counters.

MLPPP

The Multilink PPP Interface object models a multilink PPP bundle, which is a named virtual interface with multiple member links.

Discovery and Verification Technique: MLPPP Endpoint Identifier.

VLAN

Discovery and Verification Technique: VLAN ID Matching.

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.

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.

Pseudowire

Pseudowire 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.

Cisco ANA discovers PWE3 Network layer topology by searching for matches between the local and remote router IP addresses in any one-hop-away remote side's PTP Layer 2 MPLS tunnel interface. In particular, it compares the local and remote router IP addresses and tunnel identifications.

Link type: Tunnel

Discovery and verification technique: Pseudowire Information.

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.

Link type: GRE tunnel

Discovery and verification technique: GRE Tunnel Information.

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.

Cisco ANA discovers MPLS-BGP-based VPN network topology by searching for the existence of the local VRF entity's imported route targets in any remote side's VRF entity exported route targets.

Link type: VPN or VPNv6

Discovery and verification techniques: Route Targets for either IPv4 or IPv6 address families.

Discovery Techniques

Discovery takes place in two phases:

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

This section describes the various discovery techniques used by Cisco ANA, as follows:

- ATM VC Counters
- CDP (Cisco Discovery Protocol)
- LLDP (Link Layer Discovery Protocol)
- PNNI Information
- BFD Session Source and Destination
- BGP Information
- MAC
- REP
- LACP
- OAM
- MLPPP Endpoint Identifier
- GRE Tunnel Information
- Pseudowire Information
- VLAN ID Matching
- Route Targets
- Physical Layer Counters
- IP Testing
- STP (Spanning Tree Protocol)

Note All the supported discovery techniques are enabled by default. Only MAC discovery can be disabled using the registry. See the *Cisco Active Network Abstraction 3.7.2 Administrator Guide* for more information.

ATM VC Counters

Same Active VCs

In this technique, each side identifies a set of active ATM Virtual Connections (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.

This technique supports configurations that have either the same VCs or the same VPs on both sides. It does not support a mixture of VCs on one side and VPs on the other side.

VC 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.

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.

PNNI Information

In this technique, each port in the ATM switch is identified with two values:

- Node ID.
- Port ID.

BFD Session Source and Destination

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 Information

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.

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

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

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).

OAM

If OAM is configured between two devices, local and remote OAM MACs are compared between the two devices (local OAM MAC = remote OAM MAC and vice versa).

This protocol has the highest priority and hence will be the first to be checked if it is enabled.

MLPPP Endpoint 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.

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.

Pseudowire Information

In this technique, each pseudowire is identified by the following criteria:

- Local and Remote router IP.
- Tunnel ID.

Matching between two pseudowire tunnels Pw1 and Pw2 is conducted by comparing:

- The Pw1 local IP to the Pw2 remote IP and the Pw1 remote IP to the Pw2 local IP.
- Tunnel ID.

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.

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.

Physical Layer Counters

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.

IP Testing

Cisco ANA uses IP testing (IPv4) 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.

STP (Spanning Tree Protocol)

If STP is enabled between switches, 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.

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