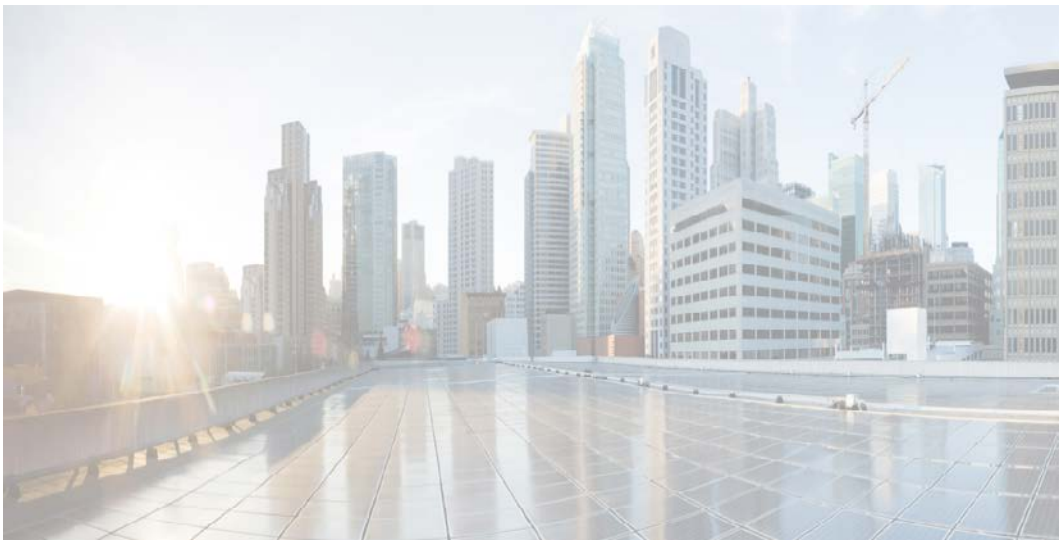

# Cisco Prime Network 4.3 Supported Technologies and Topologies

July, 2016


**Americas Headquarters**

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

http://www.cisco.com

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

**Abstract**



Cisco Prime Network 4.3 Supported Technologies and Topologies

# 1 Table of Contents

# 2 Supported Technologies in Prime Network

Table 2-1 lists the technologies supported in Prime Network 4.3, and the level of support provided for each technology. Note the fact that if a specific technology is listed in Table 11-1, it does not imply that every aspect of the relevant standard is represented and supported. In addition, the specific level of support provided for a particular technology on individual network elements can vary. For details on technology support on individual VNEs, see *Cisco Prime Network Supported Cisco VNEs*.

The supported technologies table indicates the level of support that Prime Network provides for the various technologies, such as:

- Element modeling—Device-level inventory, support for events.
- Network modeling—Support for flows (correlation, path trace).
- Topology view—Technologies for which links are auto-discovered, and technologies that can be viewed in the context of topological links in a map.

**Note**: Please refer to the Prime Network Technology Center on Cisco Developer Network (CDN) for information about technology IMOs and their attributes.

**Table 2-1 Supported Technologies**

| Technology Family | Technology Group | Technology | Element Modeling | Network Modeling | Topology View |
|---|---|---|---|---|---|
| Network (L3) | IP | IP (including IPv6) | Yes | Yes | |
| | | Address Resolution Protocol (ARP) | Yes | Yes | |
| | | Hot Standby Router Protocol (HSRP) | Yes | | |
| | | Generic Routing Encapsulation (GRE) | Yes | Yes | Yes |
| | | Carrier Grade NAT | Yes | | |
| | | IP SLA Responder | Yes | | |
| | | 6PE | Yes | Yes | |
| | | 6RD | Yes | | |
| | | X-LAT | Yes | | |
| | | Access Control Lists (ACLs), including ahp, eigrp, esp, gre, icmp, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, tcp, udp, sctp and IPv6 | Limited | | |
| | | VRRP | Yes | | |
| | | IP Address Pool | Yes | | |

| Technology Family | Technology Group | Technology | Element Modeling | Network Modeling | Topology View |
|---|---|---|---|---|---|
| Network (L3) *(cont'd)* | Routing Protocols | Border Gateway Protocol (BGP), Multiprotocol extensions (MP-BGP), external BGP (eBGP), internal BGP (iBGP) | Yes | Yes | Yes |
| | | Open Shortest Path First (OSPF) and OSPFv3 | Yes | Yes | Yes |
| | | Intermediate System to Intermediate System (IS-IS) | Yes | | |
| | Multicast Protocols | Internet Group Management Protocol (IGMP) | Yes | | |
| | | Protocol Independent Multicasting (PIM) | Yes | | |
| | VPN and VRF | Virtual Routing and Forwarding (VRF) | Yes | Yes | Yes |
| | | VRF-Lite (Multi-VRF) | Yes | Yes | |
| | | VPN | | Yes | Yes |
| | | CSCVPN | Yes | | |
| | | 6VPE | Yes | Yes | Yes |
| | | Multicast VPN (mVPN) | Yes | | |
| | BFD | Bidirectional Forwarding Detection | Yes | | Yes |
| | SBC | Session Border Controller | Yes | | |
| | BNG (Broadband Network Gateway) | Subscriber Access Points (1:1, 1:N access VLAN config) | Yes | | |
| | | BBA (Broadband Access Group) | Yes | | |
| | | Dynamic Config Templates | Yes | | |
| | | IPV4 DHCP Profiles | Yes | | |
| | RFC3107 | Carrying Label Information in BGP-4 | Yes | Yes | |
| | G.8032 | Ethernet Ring Protection Switching | Yes | Yes | |
| Hybrid Network/ Data Link (L3/2) | MPLS | Multiprotocol Label Switching (MPLS) | Yes | Yes | Yes |
| | | Label Distribution Protocol (LDP) | Yes | | Yes |
| | | Multicast Label Distribution Protocol (mLDP) | Yes | | |
| | MPLS TP | MPLS TP | Yes | Yes | Yes |
| | MPLS TE | Multiprotocol Label Switching Traffic Engineering (MPLS TE) | Yes | Yes | Yes |
| | | P2MP (Point-to-Multipoint) TE | Yes | Yes | Yes |
| | | MPLS TE Fast Reroute (MPLS TE FRR) | Yes | | |

| Technology Family | Technology Group | Technology | Element Modeling | Network Modeling | Topology View |
|---|---|---|---|---|---|
| Hybrid Network/ Data Link (L3/2) *(cont'd)* | Pseudowire | Pseudowire Emulation Edge to Edge (PWE3) | Yes | Yes | Yes |
| | | VCCV | Yes | | |
| | | Pseudowire Redundancy | Yes | | |
| | | Static Pseudowire | Yes | | |
| | | TDM Pseudowire | Yes | Yes | Yes |
| | | Multi-segment Pseudowire | Yes | Yes | Yes |
| | | ATM over Pseudowire (ATM PW) | Yes | Yes | Yes |
| | | PW-to-TP Tunnel Mapping | Yes | Yes | |
| | | PW-to-TE Tunnel Mapping | Yes | Yes | |
| | Pseudowire *(cont'd)* | Pseudowire Headend [PW-HE] | Yes | Yes | |
| | Clocking | IE1588 | Yes | | |
| | | SyncE | Yes | | |
| | | ACR | Yes | | |
| | Fiber Channel | Fiber Channel (FC) | Yes | | Yes |
| | | Fiber Channel Over Ethernet (FCoE) | Yes | | Yes |
| | | Fiber Channel Aggregation | Yes | | |
| | | VSAN (Virtual Storage Area Network) | Yes | | |
| Data Link/MAC (L2) | Ethernet | Ethernet (IEEE 802.3) | Yes | Yes | Yes |
| | | VLAN (IEEE 802.1Q) | Yes | Yes | Yes |
| | | QinQ (IEEE 802.1ad) | Yes | Yes | |
| | | LAG (IEEE 802.3ad) | Yes | Yes | Yes |
| | | Ethernet Channel | Yes | Yes | Yes |
| | | STP (IEEE 802.1D) | Yes | | Yes |
| | | RSTP (IEEE 802.1w) | Yes | | Yes |
| | | PvSTP | Yes | | Yes |
| | | MST (IEEE 802.1s) | Yes | | Yes |
| | | SVI | Limited | | |
| | | VTP | Yes | | |
| | | REP | Yes | | REP |
| | | VPLS | Yes | Yes | Yes |
| | | H-VPLS | Yes | Yes | Yes |
| | | VSI | Yes | Yes | Yes |
| | | PBB | Yes | | |
| | | EFP | Yes | Yes | Yes |
| | | Access Gateway | Yes | | |
| | | mLACP (ICCP Redundancy Group) | Yes | | |
| | | Virtual Port Channel (vPC) | Yes | | |
| | | Fabric Path | Yes | | |
| | Ethernet OAM | CFM (Cisco and Draft 8.1) | Yes | | |

| Technology Family | Technology Group | Technology | Element Modeling | Network Modeling | Topology View |
|---|---|---|---|---|---|
| | | Link OAM | Yes | | |
| | | Ethernet LMI | Yes | | |
| | | Y.1731 Probes | Yes | | |
| | ATM | ATM | Yes | Yes | |
| | | IMA | Yes | Yes | |
| | | ATM Cross-Connect | Yes | Yes | |
| | | ATM OAM | Yes | | |
| | | IP over ATM (MPoA 1483R) | Yes | Yes | |
| | | Ethernet over ATM (MPoA1483B) | Yes | Yes | |
| | Frame Relay | Frame Relay | Yes | Yes | |
| | ISDN | Integrated Services Digital Network (ISDN) | Limited | | |
| Data Link/MAC (L2) *(cont'd)* | PPP | Point To Point Protocol (PPP) | Yes | Yes | |
| | | PPPoA, PPPoE, PPPoFR | Yes | | |
| | | Multilink PPP | Yes | Yes | Yes |
| | HDLC | High-Level Data Link Control (HDLC) | Yes | Yes | |
| | L2TP | Layer 2 Tunnel Protocol (L2TP) | Limited | | |
| | Discovery Protocols | CDP, LLDP | Yes | | |
| | Local Switching | Local Switching | Yes | Yes | |
| Physical Layer (L1) | xDSL | Digital Subscriber Line (xDSL) | Yes | | |
| | IPoDWDM | Internet Protocol over Dense Wave Division Multiplexing (IPoDWDM) | Yes | | |
| | SONET/SDH | SONET/SDH | Yes | | |
| | TDM/DSx | TDM | Yes | | |
| | | DSx | Yes | | |
| | | CEM | Yes | | |
| | | T3/E3 | Yes | | |
| | | Channelized T3, OC3, DS3 interface | Yes | | |
| | Serial | Serial | Yes | | |
| | Hardware | Pluggable Transceiver | Yes | | |
| Mobility | GGSN | GGSN | Yes | | |
| | APN | APN | Yes | | |
| | GTPU | GTPU | Yes | | |
| | S-GW | S-GW | Yes | | |
| | P-GW | P-GW | Yes | | |
| | SAE-GW | SAE-GW | Yes | | |
| | EGTP | EGTP | Yes | | |
| | GTPP | GTPP | Yes | | |

| Technology Family | Technology Group | Technology | Element Modeling | Network Modeling | Topology View |
|---|---|---|---|---|---|
| | QCI-QoS Mapping | QCI-QoS Mapping | Yes | | |
| | APN Profile | APN Profile | Yes | | |
| | APN Remap | APN Remap | Yes | | |
| | Operator Policy | Operator Policy | Yes | | |
| | SaMOG | SaMOG | Yes | | |
| | CGW | CGW | Yes | | |
| | MRME | MRME | Yes | | |
| | Active Charging Services | Active Charging Services | Yes | | |
| AAA | Radius | Radius | Yes | | |
| | Diameter | Diameter | Yes | | |
| QoS | QoS | QoS | Yes | | |
| | Access control & Service Policy | Access control & Service Policy | Yes | | |
| VSM | VSM | VSM | Yes | | Yes |
| Security GW | WSG Service | WSG Service | Yes | | |
| | Crypto Map | Crypto Map | Yes | | |
| | IKE SA | IKE SA | Yes | | |
| | IPSec SA | IPSec SA | Yes | | |
| | CA Certificate | CA Certificate | Yes | | |
| | WSG Lookup | WSG Lookup | Yes | | |
| | Connected Apps | Connected Apps | Yes | | |
| Virtualization | Compute Virtualization | Hypervisor, Virtual Machines, Virtual Data Stores, Virtual Clusters, Compute Resource Pools, Virtual Interfaces on Host/VM | Yes | | Yes (Entity Association across devices) |
| | Network Virtualization | Satellite/Cluster | Yes | | Yes (enhanced to support Ring Topology) |
| Cable | MAC Domain | MAC Domain | Yes | | |
| | DTI Client | DTI Client | Yes | | |
| | NarrowBand Channels | NarrowBand Channels | Yes | | |
| | WideBand Channels | WideBand Channels | Yes | | |
| | Fiber Node | Fiber Node | Yes | | |
| | QAM Domain | QAM Domain | Yes | | |
| | Redundancy System | Redundancy System | Yes | | |

# 3 Technology Support Based on Schemes

| Technology | Scheme | |
|---|---|---|
| | Product | IpCore |
| 6PE and 6VPE-based IPv6 Connectivity | No | Yes |
| 6RD | Yes | Yes |
| AAA | Yes | No |
| Access Gateway | Yes | Yes |
| ACL | Yes | Yes |
| ACR | Yes | Yes |
| ACS | Yes | No |
| APN Profile | Yes | No |
| APN Remap | Yes | No |
| ATM | Yes | Yes |
| ATM Cross-Connect | Yes | Yes |
| ATM OAM | Yes | Yes |
| ATM over Pseudowire (ATM PW) | No | Yes |
| ATM PW | No | Yes |
| Backup Pseudowire | No | Yes |
| BFD | Yes | Yes |
| BGP | Yes | Yes |
| BNG | No | Yes |
| Carrier Supporting Carrier (CSC) | No | Yes |
| CDP | Yes | Yes |
| CEM Group | Yes | Yes |
| CFM | Yes | Yes |
| CGN | Yes | Yes |
| Class of Service | Yes | No |
| Crypto Template | Yes | No |
| DHCP | Yes | No |
| Digital Subscriber Line (xDSL) | Yes | Yes |
| DTI Client | Yes | No |

| | | |
|---|---|---|
| EAP Profile | Yes | No |
| EFP | Yes | Yes |
| EGTP (Evolved GPRS Tunnel Protocol) | Yes | No |
| EOAM Probes | Yes | No |
| EPDG | Yes | No |
| Ethernet (IEEE 802.3) | Yes | Yes |
| Ethernet LMI | Yes | Yes |
| Ethernet OAM | Yes | Yes |
| Ethernet over ATM(MPoA1483B) | Yes | Yes |
| EVC SVI Services | Yes | Yes |
| FA | Yes | No |
| Fiber Channel  Aggregation | Yes | No |
| Fiber Channel (FC) | Yes | No |
| Fiber Channel Over Ethernet (FCoE) | Yes | No |
| Fiber Node | Yes | No |
| Frame Relay | Yes | Yes |
| GGSN | Yes | No |
| GRE | Yes | Yes |
| GTPP (GPRS Tunnel Protocol Prime) | Yes | No |
| GTPU | Yes | No |
| HA | Yes | No |
| HDLC | Yes | Yes |
| HeNB | Yes | No |
| Hierarchical VPLS | No | Yes |
| HNB | Yes | No |
| HSGW | Yes | No |
| HSRP | Yes | Yes |
| IE1588 | Yes | Yes |
| IMA | Yes | Yes |
| Integrated Services Digital Network (ISDN) | Yes | Yes |
| Internet Group Management Protocol (IGMP) | No | Yes |
| IP Address Pool * | No | Yes |
| IP and ARP | Yes | Yes |
| IP Multicast | No | Yes |

| | | |
|---|---|---|
| IP over ATM (MPoA 1483R) | Yes | Yes |
| IP Routing | Yes | Yes |
| IPoDWDM | Yes | Yes |
| IPSec | Yes | Yes |
| IPSLA Probes (Y.1731) | Yes | Yes |
| IPSLA Responder | Yes | Yes |
| IPv6 | Yes | Yes |
| IRB/BVI | Yes | Yes |
| IServer | Yes | No |
| ISIS | No | Yes |
| L3 VPN and VRF* | No | Yes |
| LAC | Yes | No |
| LAG (IEEE 802.3ad) | Yes | Yes |
| LLDP | Yes | Yes |
| LMA | Yes | Yes |
| Local Switching | Yes | Yes |
| MAC Domain | Yes | No |
| MAG | Yes | No |
| mLACP (ICCP Redundancy Group) | Yes | Yes |
| MLPPP | Yes | Yes |
| MME | Yes | No |
| MP-BGP* | No | Yes |
| MPLS | No | Yes |
| MPLS Multicast | No | Yes |
| MPLS P2MP TE | No | Yes |
| MPLS TE-Tunnel (including FRR) | No | Yes |
| MPLS TP | No | Yes |
| MST (IEEE 802.1s) | Yes | Yes |
| MST-AG/REP-AG | Yes | Yes |
| Multi-segment Pseudowire | No | Yes |
| NarrowBand Channels | Yes | No |
| OSPF | Yes | Yes |
| OTN | Yes | Yes |
| ONU | Yes | Yes |
| PBB | Yes | Yes |

| | | |
|---|---|---|
| PDSN | Yes | No |
| P-GW | Yes | No |
| Policy | Yes | No |
| POS | Yes | Yes |
| PPP | Yes | Yes |
| Protocol Independent Multicasting (PIM) | No | Yes |
| Pseudowire Emulation Edge to Edge (PWE3) | No | Yes |
| Pseudowire Headend (PW-HE) | No | Yes |
| Pseudowire Redundancy | No | Yes |
| PTP 1588 | Yes | Yes |
| PvSTP | Yes | Yes |
| PW VCCV | No | Yes |
| PW-to-TE Tunnel Mapping | No | Yes |
| PW-to-TP Tunnel Mapping | No | Yes |
| QAM Domain | Yes | No |
| QCI | Yes | No |
| QinQ (IEEE 802.1ad) | Yes | Yes |
| QoS | Yes | Yes |
| REP | Yes | Yes |
| RFC3107 | Yes | Yes |
| G.8032 | Yes | Yes |
| RLFA | Yes | Yes |
| RSTP (IEEE 802.1w) | Yes | Yes |
| Satellite | Yes | Yes |
| SBC | No | Yes |
| SCTP | Yes | No |
| SGSN | Yes | No |
| S-GW | Yes | No |
| SONET/SDH | Yes | Yes |
| SPI | Yes | No |
| STP (IEEE 802.1D) | Yes | Yes |
| SVI | No | Yes |
| SyncE | Yes | Yes |
| TDM | Yes | Yes |

| | | |
|---|---|---|
| TDM Pseudowire | No | Yes |
| TDM PW | No | Yes |
| Transform Set | Yes | No |
| VC Switching | Yes | Yes |
| Virtual Port Channel (vPC) | Yes | Yes |
| Virtualization | Yes | No |
| VLAN (IEEE 802.1Q) | Yes | Yes |
| VPLS | No | Yes |
| VRRP | Yes | Yes |
| VSAN (Virtual Storage Area Network) | Yes | No |
| VTP (VLAN Trunk and Tunneling) | Yes | Yes |
| Wideband Channels | Yes | No |
| RedundancySystem | Yes | Yes |

***** MPBGP, IP Pool and VRF technology is supported in product scheme for ASR 5000 alone

# 4 Schemes Used by Device Type

| Device Types | Scheme | |
|---|---|---|
| | Product | IpCore |
| **Applications** | | |
| VMWare VirtualCenter | X | — |
| **Data Center** | | |
| Cisco Unified Computing System (UCS) 61xx Series Switches | X | — |
| Cisco Unified Computing System (UCS) 62xx Series Switches | X | — |
| **Optical Transport** | | |
| Cisco Carrier Packet Transport (CPT) 200 | X | X |
| Cisco Carrier Packet Transport (CPT) 600 | X | X |
| Cisco Carrier Packet Transport (CPT) 50 | X | X |
| **Security Appliances** | | |
| Cisco Adaptive Security Appliance 5550 Series | X | — |
| Cisco Adaptive Security Appliance 5580 Series | X | — |
| Cisco Adaptive Security Appliance 5585 Series | X | — |
| Cisco Adaptive Security 1000v | X | — |

| | | |
|---|---|---|
| Cisco Virtual Security Gateway (WSG) | X | — |
| **Access Servers / Gateways** | | |
| Cisco Access Server 5800 | X | — |
| Cisco Access Server 5300 | X | — |
| **Radio Frequency (RF) Gateways** | | |
| Cisco RF Gateway 10 Series | X | — |
| **Routers** | | |
| Cisco 800 Series Routers | X | — |
| Cisco 1000 Series Routers | X | — |
| Cisco 1600 Series Routers | X | — |
| Cisco 1700 Series Modular Access Routers | X | — |
| Cisco 1800 Series Integrated Services Routers | X | — |
| Cisco 2000 Series Connected Grid Routers | X | X |
| Cisco CSR 1000v Cloud Service Routers | X | X |
| Cisco 2500 Series Routers | X | — |
| Cisco 2600 Series Multiservice Platform Routers | X | — |
| Cisco 2800 Series Integrated Services Routers | X | — |
| Cisco 3600 Series Multiservice Platform Routers | X | X |
| Cisco 3700 Series Multiservice Access Routers | X | X |
| Cisco 3800 Series Integrated Services Routers | X | X |
| Cisco 7200 Series Routers | X | X |
| Cisco 7300 Series Routers | X | X |
| Cisco 7400 Series Routers | X | X |
| Cisco 7500 Series Routers | X | X |
| Cisco 7600 Series Routers | X | X |
| Cisco 10000 Series Routers | X | X |
| Cisco 12000 Series Routers | X | X |
| Cisco XR 12000 Series Routers | X | X |
| Cisco CRS Carrier Routing System (CRS-1 and CRS-3) | — | X |
| Cisco NCS Network Convergence System 6000 Series | — | X |
| Cisco ASR 9000 Series Aggregation Services Routers | X | X |
| Cisco ASR 1000 Series Aggregation Services Routers | X | X |
| Cisco MWR 2900 Series Mobile Wireless Routers | X | X |
| Cisco 1900 Series Integrated Services Routers | X | — |

| | | |
|---|---|---|
| Cisco 2900 Series Integrated Services Routers | X | — |
| Cisco 3900 Series Integrated Services Routers | X | X |
| Cisco Universal Broadband Router 7200 Series | X | X |
| Cisco Universal Broadband Router 10000 Series | X | X |
| Cisco 4700 Series Routers | X | — |
| Cisco ASR 901 Aggregation Services Series Routers | X | X |
| Cisco ASR 903 Aggregation Services Series Routers | X | X |
| Cisco ASR 5000 Aggregation Services Series Routers | X | — |
| **Switches** | | |
| Cisco Catalyst 1900 Series Switches | X | — |
| Cisco ME 2600X Ethernet Access Switches | X | X |
| Cisco 2500 Series Connected Grid Switches | X | — |
| Cisco Catalyst 2900 Series Switches | X | — |
| Cisco ME 3400 Series Ethernet Access Switches | X | — |
| Cisco Catalyst 3500 XL Series Switches | X | — |
| Cisco Catalyst 3550 Series Switches | X | — |
| Cisco Catalyst 3560 Series Switches | X | — |
| Cisco Catalyst 3750 Series Switches | X | — |
| Cisco Catalyst 3750 Metro Series Switches | — | X |
| Cisco Catalyst 4000 Series Switches | X | — |
| Cisco Catalyst 4500 Series Switches | X | — |
| Cisco Catalyst 4900 Series Switches | X | — |
| Cisco ME 4900 Series Ethernet Switch | X | — |
| Cisco Catalyst 5000 Series Switches | X | — |
| Cisco Catalyst 6500 Series (CatOS) Switches | X | X |
| Cisco Catalyst 6500 Series (IOS) Switches | X | X |
| Cisco ME 6500 Series Ethernet Switches (6524) | X | X |
| Cisco ME 3600X Series Ethernet Access Switches | X | X |
| Cisco ME 3800X Series Carrier Ethernet Switch Routers | X | X |
| Cisco Nexus 1010 Series Switches | X | — |
| Cisco Nexus 7000 Series Switches | X | — |
| Cisco Nexus 5000 Series Switches | X | — |
| Cisco Nexus 3000 Series Switches | X | — |
| Cisco Nexus 1000v Series Switches | X | — |
| Cisco ACE 4700 Series Access Control Engine | X | — |

| | | |
|---|---|---|
| Cisco Service Control Engine | X | — |
| Cisco MDS 9500 Series Multilayer Directors | X | — |
| Cisco MDS 9100 Series Multilayer Fabric switches | X | — |
| **Load Balancer** | | |
| Citrix Netscaler VPX | X | — |
| **Generic Devices** | | |
| Generic SNMP Device | X | — |
| Generic Server Device | X | — |

# 5 Reduced Polling Supported VNE's:

- Cisco 10000 Series Routers
- Cisco 1900 Series Integrated Services Routers
- Cisco 2000 Series Connected Grid Routers
- Cisco 2900 Series Integrated Services Routers
- Cisco 3900 Series Integrated Services Routers
- Cisco 7200 Series
- Cisco 7600 Series
- Cisco ASR 1000 Series
- Cisco ASR 5000 Series
- Cisco ASR 9000 Series
- Cisco ASR 901 Series
- Cisco ASR 903 Series
- Cisco CPT 50 Ring Series
- Cisco CPT Series
- Cisco CSR 1000v Series
- Cisco Carrier Routing System
- Cisco Catalyst 3750 Metro Series
- Cisco Catalyst 4500 Series
- Cisco Catalyst 4900 Series
- Cisco Connected Grid Switch 2500 Series
- Cisco MDS 9000 Series
- Cisco ME 26xx Series
- Cisco ME 3400 Series
- Cisco ME 3600X Series
- Cisco ME 3800X Series
- Cisco ME 4900 Series
- Cisco MWR 2900 Series
- Cisco Network Convergence System
- Cisco Nexus 10xx Series

- Cisco Nexus 3000 Series
- Cisco Nexus 5000 Series
- Cisco Nexus 7000 Series
- Cisco OLT ME Series
- Cisco Nexus 1000v Series
- Cisco XR 12000 Series
- Cisco uBR10000 Series

# 6 Supported Topologies in Prime Network

The following topics describe the types of topologies supported by Prime Network 4.3. It also explains how Prime Network discovers and displays these topologies.

## 6.1 Supported Topology Types

The following topology types are supported by Prime Network 4.3:

- ATM
- BFD
- BGP
- Business
- Ethernet
- LAG
- Frame Relay
- MPLS
- PPP or HDLC
- MLPPP
- Physical Layer
- Pseudowire
- GRE Tunnel
- VPN
- VLAN Service Links
- MPLS-TE Tunnel
- MPLS-TP Tunnel

- FC and FCoE
- Entity Association
- OSPF

### 6.1.1 ATM

The ATM topology represents the link between two ATM ports that 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

**Note**: PNNI support is very limited.

### 6.1.2 BFD

The 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

### 6.1.3 BGP

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

**Link type**: BGP

**Discovery and verification technique**: BGP Information

### 6.1.4 Business

The 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 Prime Network gateway.

### 6.1.5 Ethernet

The Ethernet topology represents a link between two Ethernet ports that 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.

Prime Network conducts a discovery of the 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.
Certain data that is used for discovery might be device specific. For example, Inter Chassis Link and Inter Rack Link information that is available only for specific device type.

> **Note**: Many service providers use L2PT to configure customer access to VLAN ports. This avoids the need to process Layer 2 protocols such as CDP. In these scenarios, discovery may create links between ports that 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 (Resilient Ethernet Protocol)
- LACP
- Inter Chassis Link / Inter Rack Link
- UCS Internal Connectivity
- Static

**Verification Technique**: Physical Layer Counters and all of the above discovery techniques except MAC.

### 6.1.6 LAG

The LAG topology represents a link between two LAG or EtherChannel interfaces that 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 IMO (IDataLinkAggregationContainer), which points to the LAG or EtherChannel underline ports.

**Link type**: LAG

**Discovery and verification techniques**:

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

### 6.1.7 Frame Relay

The Frame Relay topology represents a link between two Frame Relay ports that 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.

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

**Link type**: Frame Relay

**Discovery techniques**:

- CDP (Cisco Discovery Protocol)
- Static

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

### 6.1.8 MPLS

The 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 (IMpls), which represent the MPLS interfaces.

Prime Network 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

### 6.1.9 PPP or HDLC

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

Prime Network discovers 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.

**Link type**: PPP/HDLC

**Discovery** techniques:

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

**Verification Techniques**: Physical Layer Counters.

### 6.1.10 MLPPP

The Multilink PPP topology represents a link between two Multilink PPP Interfaces. Multilink PPP is a named virtual interface with aggregate multiple PPP member interfaces.

**Link type**: MLPPP

**Discovery and Verification Technique**: MLPPP Endpoint Identifier.

### 6.1.11 Physical Layer

The 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 that inherit from the physical layer IMO (IPhysicalLayer), such as SONET/SDH Physical (ISonetSdh) and DS3 Channelized Interface (IDS3PdhChannelized), which represent physical layers of a port.

In Prime Network's topology discovery implementation, physical layer (Layer 1) discovery is coupled with data link layer (Layer 2) discovery.

**Link type**: Physical
**Discovery techniques**:

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).
- Static

**Verification Technique**: Physical Layer Counters

### 6.1.12 Pseudowire

The Pseudowire topology represents a bi-directional 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 (IPTPLayer2MplsTunnel), which represent the pseudowire tunnel endpoints.

Prime Network 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. In particular, it compares the local and remote router IP addresses and tunnel identifications.

**Link type**: Tunnel

**Discovery and verification technique**: Pseudowire Information

### 6.1.13 GRE Tunnel

The 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 GRE Tunnel IMOs (Generic Routing Encapsulation (GRE) Tunnel Interface (ITunnelGRE)), which represent the GRE tunnel endpoints.

Prime Network discovers the GRE topology by comparing the source and destination IP address on both sides accordingly.

**Link type**: GRE tunnel

**Discovery and verification technique**: GRE Tunnel Information

### 6.1.14 VPN

The VPN topology represents a link between two VRFs that are part of a VPN. In other words, 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.

Prime Network discovers MPLS-BGP-based VPN network topology by searching for the existence of a local VRF entity's imported route taget among the exported route targets of any remote side.

**Link type**: VPN or VPNv6

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

### 6.1.15 VLAN Service Links

A VLAN service link represents either an Ethernet or a LAG link in the context of a specific VLAN. It connects two Ethernet Flow Point entities, which represent Ethernet or LAG ports in the context of a specific VLAN, or with VLAN match criteria.

The two Ethernet Flow Points can reside in the same Layer 2 domain, or connect between two different Layer 2 domains when a VLAN TAG manipulation is used.

The VLAN service links are not discovered using the standard topology mechanism that resides in the VNE layer, but rather by the Carrier Ethernet discovery. The discovery mechanism uses Ethernet and LAG links, VNE inventory modeling information of the Ethernet/LAG interfaces, and Ethernet Flow Point entities as inputs for the VLAN service link discovery process.
**Link type**: VLAN

**Discovery and verification techniques**: VLAN ID Matching.

### 6.1.16 MPLS-TE Tunnel

The MPLS-TE Tunnel topology represents a unidirectional link between the TE tunnel interface, which is the head of the TE tunnel, and the Label Switching Entity (LSE), which is the tail of the TE tunnel. The head of the TE tunnel is represented by the MPLS-TE Tunnel IMO (IMplsTETunnel) and the tail of the TE tunnel is represented by the Label Switching Entity IMO (ILSE), which is the MPLS forwarding component on the destination VNE.

MPLS TE tunnels also have mid-points that are not represented in the MPLS-TE tunnel topology.

**Link type**: MPLS-TE, P2MP MPLS-TE
The link is unidirectional and represents a flow from the head to the tail of the TE tunnel.

Link type 'MPLS-TE' will be used when TE tunnel has a single LSP (i.e. for point to point) and 'P2MP MPLS-TE' will be used for TE tunnel with multiple LSPs (i.e. for point to multi point).

**Discovery and verification techniques**: MPLS-TE Information

### 6.1.17 MPLS-TP Tunnel

The MPLS-TP Tunnel topology represents a bidirectional link between two TP tunnel interfaces, which represent the two edges of the TP tunnel.

A TP tunnel interface is represented by the IMPLSTPTunnelEP IMO. MPLS-TP tunnels also have mid-points, which are not represented as part of the MPLS-TP tunnel topology.

**Link type**: MPLS-TP.
The link is bidirectional.

**Discovery and verification techniques**: MPLS-TP Information

### 6.1.18 FC and FCoE

The Fiber Channel (FC) and Fiber Channel over Ethernet (FCoE) topologies represent a link between two native Fiber Channel interfaces or between two Fiber Channel components of FCoE interfaces that are connected in the network. In the VNE model, the endpoints of the link are Fiber Channel IMOs (IFiberChannel), which represent the underlying native (FC) or virtual (FCoE) Fiber Channel ports.

**Note**: Fiber Channel interfaces can be connected in a point-to-point, arbitrated loop, or switched fabric topology. Prime Network supports link discovery only for the switched fabric, discovering links on extension and node ports.

**Link type**: Fiber Channel

**Discovery and verification techniques**: WWN

### 6.1.19 Entity Association

The Entity Association topology represents a link between two related entities located in two different VNEs, representing physical or virtual devices. In the VNE model, the end points of the link can be any component/IMO. In Prime Network 4.3, it is used to connect the physical and virtual entities as listed below:

- Physical server (IServer IMO) & Virtual Device running on this server (IManagedElement IMO). Virtual devices include CSR1000v, Nexus1000v, VSG, etc.
- Physical server (IServer IMO) & Host (IHost under virtualization inventory)
- Virtual Machine (IVirtualMachine IMO) & Virtual Device (IManagedElement IMO)
- VEM (Virtual Ethernet Module – modelled as IModule in Nexus1000v) & Host (Hypervsior under virtualization inventory) and Physical server (IServer IMO)

**Note**: In the above list, only item #1 & #4 will be shown as external links in the topology or device map view. Item #2 & #3 are just hyperlinks between components across VNEs and will not be visible in the topology view.

**Link type**: Entity Association

**Discovery and verification techniques**: Entity Association Information

### 6.1.20 OSPF

The links will be formed between OSPF Process DCs and not with 'OspfNeighbor', even though the link signifies the neighborship between them. This is because the 'OspfNeighbor' is a 'PropertyHolder' under the OspfProcess DC. It is a multilink topology, meaning there can be multiple links from the same OSPF process.

Single layer topology

Dynamic topology

No persistency is supported

The OSPF topological links will be shown for the neighbors which has the 'Neighbor State' as either FULL or TWOWAY.

-For neighbors with TWOWAY state, additionally the OSPF interface's network type should be either BROADCAST or NBMA.

**Link type**: OSPF

**Discovery and verification techniques**: OSPF Process information

## 6.2 Discovery Techniques

Discovery takes place in two phases:

1. Discovery of existing links.
2. Verification that the link still exists (for each discovered link).

The following discovery techniques are used by Prime Network:

- ATM VC Counters
- CDP (Cisco Discovery Protocol)
- LLDP (Link Layer Discovery Protocol)
- PNNI Information
- BFD Session Source and Destination
- BGP Information
- MAC
- REP (Resilient Ethernet Protocol)
- LACP
- OAM
- MLPPP Endpoint Identifier
- GRE Tunnel Information
- Pseudowire Information
- VLAN ID Matching

- Route Targets
- Physical Layer Counters
- IP Testing
- STP (Spanning Tree Protocol)
- MPLS-TE Information
- MPLS-TP Information
- UCS Internal Connectivity
- WWN
- Entity Association Information
- Static

**Note**: By default, all supported discovery techniques are enabled. Only MAC discovery can be disabled using the registry. See the Cisco Prime Network Administrator Guide for more information.

### 6.2.1 ATM VC Counters

#### *6.2.1.1 Same Active VCs*

In this technique, each side identifies a set of active ATM Virtual Connections (VCs) and looks for a match on another port in the network. A VC is said to be active if it 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.

#### *6.2.1.2 VC Traffic Signature*

Traffic signature is based on traffic pattern analysis. The underlying assumption of traffic pattern analysis is that network traffic variety ensures 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.

### 6.2.2 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 criterion is the CDP neighbor information.

Please note the following limitations:

- If a port has more than one CDP neighbor, no links will be created.
- Ports in a multi chassis device will not be connected by CDP if there is no entry for them in the CDP neighbors table.

### 6.2.3 LLDP (Link Layer Discovery Protocol)

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

### 6.2.4 PNNI Information

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

- Node ID.
- Port ID.

### 6.2.5 BFD Session Source and Destination

In this technique, the source and destination addresses of a BDF session are verified by matching them against the source and destination addresses of the potential adjacent neighbors. The session's source address is matched to the neighbor's destination address and the session's destination source is matched to the neighbor's source address since one side's source is the other side's destination. This method works on the assumption that multiple BFD sessions running on the same router cannot have the same source and destination address.

### 6.2.6 BGP Information

In this technique, the local BGP identifier is compared to the remote BGP identifier or a potential neighbor for each BGP Neighbor Entry. This topology technique assumes uniqueness of the BGP identifier in the network.

### 6.2.7 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 or the router and switch, but not between two switches (includes the generic VNE).

### 6.2.8 REP (Resilient Ethernet Protocol)

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.

### 6.2.9 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).

### 6.2.10 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.

### 6.2.11 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 Local MLPPP End Point Identifier is matched to the neighbor Remote MLPPP End Point Identifier.

### 6.2.12 GRE Tunnel Information

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

1. Source IP.
2. Destination IP.

Taking the example of two tunnels T1 and T2 to match, the source IP address of T1 is compared to the destination IP address of T2. Similarly, the destination IP address of T1 is compared to the source IP address of T2.

### 6.2.13 Pseudowire Information

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

- Local and Remote router IP.
- Tunnel ID.

Taking the example of two pseudowire tunnels Pw1 and Pw2 to match:

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

### 6.2.14 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.

### 6.2.15 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).

Atleast one pair of import or export route target of one VRF entity is matched to the export or import route target or the other VRF entity.

### 6.2.16 Physical Layer Counters

The physical layer is used for topology verification (that is, if a link has already been discovered, it is tested periodically), which is done using counters. Physical layer counters are based on the port traffic signature, using octet-based or octet- and packet–based traffic.
Using the port traffic signature, it is possible to disqualify a connection between two ports based on their counters.

### 6.2.17 IP Testing

Prime Network 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 when 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. The configuration of Device1 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
```

The configuration of Device 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.

### 6.2.18 STP (Spanning Tree Protocol)

If STP is enabled between switches, the STP port information is used as follows: 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 only work when compatible STP protocols are running on both ports.

### 6.2.19 MPLS-TE Information

MPLS-TE type

The MPLS-TE tunnel source IP, destination IP and the tunnel ID information from the tunnel head (taken from the MPLS TE Tunnel) are compared with destination IP, source IP and the tunnel ID on the tail (taken from the MPLS TE Tunnel Segment of the LSE).

P2MP MPLS-TE type

The MPLS-TE tunnel source IP, destination IP list and the tunnel ID information from the tunnel head (taken from the MPLS TE Tunnel) are compared with destination IP, source IP and the tunnel ID on the tail (taken from the MPLS TE Tunnel Segment of the LSE). The destination IP on the MPLS TE Tunnel Segment of the LSE is contained in destination IP list of MPLS-TE tunnel.

### 6.2.20 MPLS-TP Information

The local router ID, remote router ID and the tunnel ID of one MPLS-TP tunnel edge are compared to the remote router ID, local router ID and tunnel ID of another MPLS-TP tunnel edge.

The information is taken from the MPLS TP Tunnel EP.

### 6.2.21 UCS Internal Connectivity

For UCS devices, links between different components of a device (Fabric Interconnects, IO Modules, and Blade Servers) are created based on peer information available via HTTP management. This information is shown also in the UCS Manager application. For example, FIC ports connected to the ports of an IO Module are shown in the “Peer” column of the “Fabric Ports” table under the corresponding IO Module node, and under Fabric Port nodes in UCS Manager.

### 6.2.22 WWN

WWN (World Wide Name) is a unique identifier of a Fiber Channel port. Fiber Channel switches of a fabric store a shared database of fabric ports that contains WWNs of each connected port (extension or node) and its peer. This information is used to discover pairs of connected ports in the network. WWN of a port is compared to the peer WWN of another port found in the FCS Database Entries table under a VSAN node of the logical inventory.

### 6.2.23 Entity Association Information

Entity Association Information includes the below attributes, which are matched against the related entities in two different VNEs:

1. UUID (Universal Unique Identifier)
2. IP Address
3. MAC Address
4. Name (Name can be the component/entity name, VNE name or SysName of Device)
5. Other matching parameter (Any other matching parameter of component/entity)

The following attributes are used in Prime Network 4.3:

- Physical server to Host hyperlink → UUID or IP (whichever is available and matching).
- VM to Virtual device hyperlink → IP address or Name or Other matching parameter (whichever is available and matching).
- Physical server to Virtual device → It depends on the above hyperlink creation.
- VEM to Host/Physical Server → UUID or IP (whichever is available and matching).

### 6.2.24 Static

Static topology is simply a manual configuration of the topological links. The information on the links is persisted in the Prime Network registry under the VNE registry section.

### 6.2.25 OSPF

In this technique, the Local Area Id , Router Id and IP Interface are verified by matching them against the Remote Area Id , Router Id and IP Interface of the OSPF neighbors.

The information is taken from the OSPF Process.