Important Notes

- Important Notes, on page 1

Important Notes

Unsupported Features: All Models

- **Security**
  - IPsec VPN
  - Virtual Routing and Forwarding-Aware (VRF-Aware) Web Authentication
  - MACsec switch-to-host connections in an overlay network.
- **System Management**
  - Performance Monitoring (PerfMon)

Unsupported Features: Cisco Catalyst 9500 Series Switches

- **Cisco TrustSec**
  - Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks
- **Interface and Hardware**
  - Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual PoE, Fast PoE)
  - Link Debounce Timer
  - M2 SATA Module
- **IP Addressing Services**
  - GRE Redirection
  - VRRPv3: Object Tracking Integration
  - GRE IPv6 Tunnels

- HSRP and Switch Stack
- HSRP Groups and Clustering

- **IP Multicast Routing**
  - Unicast over Point-to-Multipoint (P2MP)
  - Generic Routing Encapsulation (GRE)
  - Multicast over P2MP GRE

- **IP Routing**
  - PIM Bidirectional Forwarding Detection (PIM BFD), PIM Snooping
  - Border Gateway Protocol (BGP) Additional Paths
  - OSPF NSR
  - OSPFv3 NSR
  - OSPFv2 Loop-Free Alternate IP Fast Reroute

- **Layer 2**
  - Audio Engineering Society: AES67 Timing Profile
  - Q-in-Q on a Trunk Port

- **Multiprotocol Label Switching**
  - Hierarchical VPLS with MPLS Access

- **Network Management**
  - Flexible NetFlow
    - NetFlow v5 Export Protocol
    - 4-byte (32-bit) AS Number Support
    - TrustSec NetFlow IPv4 Security Group Access Control List (SGACL) Deny and Drop Export

- **Quality of Service**
  - Classification (Layer 3 Packet Length, Time-to-Live (TTL))
  - Per queue policer support
  - Sharped profile enablement for egress per port queue
  - L2 Miss
  - Ingress Packet FIFO (IPF)

- **Security**
  - Lawful Intercept

- **VLAN**
  - QinQ VLAN Mapping

Unsupported Features: Cisco Catalyst 9500 Series Switches - High Performance

- **High Availability**
  - Graceful Insertion and Removal
  - Switch Stacks
- **IP Multicast Routing**
  - IPv6 Multicast and IPv6 Multicast over Point-to-Point GRE
- **IP Routing**
  - Unicast and Multicast over Point-to-Multipoint GRE
  - BFD Multihop Support for IPv4 Static Routes
- **Layer 2**
  - Resilient Ethernet Protocol (REP)
- **Multiprotocol Label Switching**
  - MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels
  - VPLS Routed Pseudowire IRB(v4) Unicast
- **Network Management**
  - Cisco Application Visibility and Control (AVC)
- **Quality of Service**
  - QoS Options on GRE Tunnel Interfaces
- **Security**
  - Wake-on-LAN (WoL)
- **System Management**
  - Network-Based Application Recognition (NBAR) and Next-Generation NBAR (NBAR2)

Unsupported Features: Cisco Catalyst 9500X Series Switches

- **BGP EVPN VXLAN**
  - Layer 2 Broadcast, Unknown Unicast, and Multicast (BUM) Traffic Forwarding using Ingress Replication
  - BUM Traffic Rate Limiting

- Dynamic ARP inspection (DAI) and DHCP Rogue Server Protection
- EVPN VXLAN Centralized Default Gateway
- VXLAN-Aware Flexible Netflow
- MPLS Layer 3 VPN Border Leaf Handoff
- MPLS Layer 3 VPN Border Spine Handoff
- VPLS over MPLS Border Leaf Handoff
- VPLS over MPLS Border Spine Handoff
- Interworking of Layer 3 TRM with MVPN Networks for IPv4 Traffic
- Private VLANs (PVLANs)
- BGP EVPN VXLAN with IPv6 in the Underlay (VXLANv6)
- EVPN Microsegmentation
- VRF aware NAT64 EVPN Fabric
- Cisco StackWise Virtual
- L3TRM with Data MDT
- EVPN L2TRM
- Multihoming Single Active

- **Cisco TrustSec**
  - Cisco TrustSec Meta Data Inline Tagging
  - Interface Scalable Group Tag (SGT) Tagging
  - Device SGT Tagging
  - SGT Inline Tagging
  - Cisco TrustSec Manual Configuration
  - Cisco TrustSec Security Association Protocol (SAP)
  - Cisco TrustSec Metadata Header Encapsulation
  - Cisco TrustSec VLAN to SGT Mapping
  - Local Device SGT Mapping
  - IPv6 Support for SGT and SGACL
  - Cisco TrustSec SGT Caching

- **High Availability**
  - Secure StackWise Virtual
  - Cisco Nonstop Forwarding with Stateful Switchover

- Graceful Insertion and Removal
- Switch Stacks

- **Interface and Hardware**
  - Per-port MTU
  - Link Debounce Timer

- **IP Addressing Services**
  - Next Hop Resolution Protocol (NHRP)
  - Network Address Translation (NAT)
  - Web Cache Communication Protocol (WCCP)
  - Switchport Block Unknown Unicast and Switchport Block Unknown Multicast
  - Gateway Load Balancing Protocol (GLBP)
  - Message Session Relay Protocol (MSRP)
  - TCP MSS Adjustment
  - WCCP IPv4
  - GLBP
  - GRE IPv6 Tunnels
  - IP Fast Reroute (IP FRR)
  - Non-stop Routing

- **IP Multicast Routing**
  - SDR Listener Support
  - Multicast Routing over GRE Tunnel
  - Multicast VLAN Registration (MVR) for IGMP Snooping
  - IPv6 Multicast over Point-to-Point GRE
  - IGMP Proxy
  - Bidirectional PIM
  - Multicast VPN
  - MVPNv6
  - mVPN Extranet Support
  - MLDP-Based VPN
  - PIM Snooping
  - PIM Dense Mode

- **IP Routing**
  - OSPFv2 Loop-Free Alternate IP Fast Reroute
  - EIGRP Loop-Free Alternate IP Fast Reroute
  - Policy-Based Routing (PBR)
  - PBR for IPv6
  - VRF-Aware PBR
  - Local PBR
  - Multipoint GRE
  - Web Cache Communication Protocol (WCCP)
  - Unicast Reverse Path Forwarding (uRPF)
- **Layer 2**
  - Multi-VLAN Registration Protocol (MVRP)
  - Loop Detection Guard
  - Cross-Stack UplinkFast
  - Optional Spanning Tree Protocol
  - Precision Time Protocol (PTP)
  - Audio Engineering Society: AES67 Timing Profile
  - PTPv2 on Cisco StackWise Virtual
  - Fast UniDirectional Link Detection
  - UniDirectional Link Detection (UDLD)
  - IEEE 802.1Q Tunneling
  - One-to-One VLAN Mapping
  - Selective Q-in-Q
  - Q-in-Q on a Trunk Port
  - Audio Video Bridging (AVB): IEEE 802.1BA
  - Flexlink+
  - VLAN Load Balancing for FlexLink+
  - Preemption for VLAN Load Balancing
  - FlexLink+ Dummy Multicast Packets
  - Resilient Ethernet Protocol
- **Multiprotocol Label Switching**

- BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN
- MPLS over GRE
- MPLS Layer 2 VPN over GRE
- MPLS Layer 3 VPN over GRE
- Virtual Private LAN Service (VPLS)
- VPLS Autodiscovery, BGP-based
- VPLS Layer 2 Snooping: Internet Group Management Protocol or Multicast Listener Discovery
- Hierarchical VPLS with Multiprotocol Label Switching Access
- VPLS Routed Pseudowire IRB(v4) Unicast
- MPLS VPN Inter-AS Options (options A, B, and AB)
- MPLS VPN Inter-AS IPv4 BGP Label Distribution
- Seamless Multiprotocol Label Switching

- **Network Management**
  - ERSPAN and RSPAN
  - Flow-Based Switch Port Analyser
  - FRSPAN
  - IP Aware MPLS Netflow
  - NetFlow Version 5
  - VPN ID

- **Security**
  - Lawful Intercept
  - MACsec:
    - MACSec Cipher announcement
    - Switch-to-host MACsec
    - Cisco TrustSec Security Association Protocol
    - Cisco TrustSec MACsec
    - Fallback Key
    - MACsec EAP-TLS
    - MACsec Downlink
  - MAC ACLs
  - Port ACLs

- VLAN ACLs
- IP Source Guard
- IPv6 Source Guard
- Web-based Authentication
- Port Security
- Weighted Random Early Detection mechanism (WRED) Based on DSCP, PREC, or COS
- IEEE 802.1x Port-Based Authentication
- Dynamic ARP Inspection
- Dynamic ARP Inspection Snooping

- **System Management**
  - Unicast MAC Address Filtering

- **VLAN**
  - Wired Dynamic PVLAN
  - Private VLANs

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator at: https://cfnng.cisco.com.

Choose the following in the context of the Cisco Catalyst 9500 Series Switches:

- CAT9500: to see all the features supported on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models
- CAT9500 HIGH PERFORMANCE (32C, 32QC, 48Y4C, 24Y4C): to see all the features supported on the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models
- CAT9500X: to see all the features supported on the C9500X-28C8D and C9500X-60L4D models

Accessing Hidden Commands

From Cisco IOS XE Fuji 16.8.1a, as an improved security measure, the way in which hidden commands can be accessed has changed.

Hidden commands have always been present in Cisco IOS XE, but were not equipped with CLI help. That is, entering a question mark (?) at the system prompt did not display the list of available commands. Hidden commands are only meant to assist Cisco TAC in advanced troubleshooting, and are not documented either.

From Cisco IOS XE Fuji 16.8.1a, hidden commands are available under:

- Category 1: Hidden commands in Privileged or User EXEC mode. Enter the **service internal** command to access these commands.
- Category 2: Hidden commands in one of the configuration modes (global, interface, and so on).

Further, the following points apply to hidden commands under Category 1 and 2:

- The commands have CLI help. Enter a question mark (?) at the system prompt to display the list of available commands.

  Note: For Category 1, enter the **service internal** command before you enter the question mark; you do not have to do this for Category 2.

- The system generates a `%PARSER-5-HIDDEN` syslog message when a hidden command is used. The following is an example:

```
*Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header '
 is a hidden command.
Use of this command is not recommended/supported and will be removed in future.
```

Apart from categories 1 and 2, there are other internal commands displayed on the CLI, for which the system does *not* generate the `%PARSER-5-HIDDEN` syslog message.

Note We recommend that you use any hidden command only under TAC supervision.

If you find that you need to use a hidden command, open a TAC case for help with finding another way of collecting the same information as the hidden command (for a hidden EXEC mode command), or to configure the same functionality (for a hidden configuration mode command) using nonhidden commands.

Default Behaviour—All Models

Beginning from Cisco IOS XE Gibraltar 16.12.5 and later, do not fragment bit (DF bit) in the IP packet is always set to 0 for all outgoing RADIUS packets (packets that originate from the device towards the RADIUS server).

Default Interface Behaviour on Cisco Catalyst 9500 Series Switches - High Performance and Cisco Catalyst 9500X Series Switches Only

From Cisco IOS XE Gibraltar 16.11.1, the default interface for all High Performance and 9500X models in the series changes from Layer 3 to Layer 2. Use the **no switchport** command to change the Layer 2 interface into Layer 3 mode.

The startup configuration has explicit configuration of the **switchport** command for Layer 2 interfaces and the **no switchport** command for Layer 3 interfaces to address this change in behaviour and to support seamless migration.

Important Notes