Important Notes

Important Notes

Unsupported Features: Cisco Catalyst 9600 Series Supervisor 2 Module

- **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 TrustSec**
  - Cisco TrustSec Security Association Protocol (SAP)
  - Cisco TrustSec SGT Caching

- **High Availability**
  - Quad-Supervisor with Route Processor Redundancy
  - Secure StackWise Virtual

- **Interface and Hardware**
  - Link Debounce Timer
  - EnergyWise

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

- **IP Multicast Routing**
  - 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) for IPv6
  - VRF-Aware PBR
  - PBR for Object-Group Access Control List (OGACL) Based Matching
  - Multipoint GRE
  - Web Cache Communication Protocol (WCCP)
  - Unicast and Multicast over Point-to-Multipoint GRE

- **Layer 2**
  - Multi-VLAN Registration Protocol (MVRP)
  - Loop Detection Guard
  - Resilient Ethernet Protocol

- **Multiprotocol Label Switching**
  - LAN MACsec over Multiprotocol Label Switching (MPLS)
  - 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 MPLS Access
  - VPLS Routed Pseudowire IRB(v4) Unicast
  - MPLS VPN Inter-AS Options (options B and AB)
  - MPLS VPN Inter-AS IPv4 BGP Label Distribution
  - Seamless Multiprotocol Label Switching

- **Network Management**
  - ERSPAN
  - Flow-Based Switch Port Analyser

- FRSPAN
- Egress Netflow
- IP Aware MPLS Netflow
- NetFlow Version 5

- **Quality of Service**
  - QoS Ingress Shaping
  - VPLS QoS
  - Microflow Policers
  - Per VLAN Policy and Per Port Policer
  - Mixed COS/DSCP Threshold in a QoS LAN-queueing Policy
  - Easy QoS: match-all Attributes
  - Classify: Packet Length
  - Class-Based Shaping for DSCP/Prec/COS/MPLS Labels
  - CoPP Microflow Policing
  - Egress Policing
  - Egress Microflow Destination-Only Policing
  - Ethertype Classification
  - Packet Classification Based on Layer3 Packet-Length
  - PACLs
  - Per IP Session QoS
  - Per Queue Policer
  - QoS Data Export
  - QoS L2 Missed Packets Policing

- **Security**
  - Lawful Intercept
  - MACsec:
    - MACsec EAP-TLS
    - Switch-to-host MACsec
    - Certificate-based MACsec
    - Cisco TrustSec SAP MACsec
  - 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.

Accessing Hidden Commands

This section provides information about hidden commands in Cisco IOS XE and the security measures that are in place, when they are accessed. These commands are only meant to assist Cisco TAC in advanced troubleshooting and are not documented.

Hidden commands are available under:

- Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the **service internal** command to access these commands.
- Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the **service internal** command.

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

- The commands have CLI help. Enter 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. For example:

Important Notes

```
*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 category 1 and 2, there remain internal commands displayed on the CLI, for which the system does NOT generate the %PARSER-5-HIDDEN syslog message.

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

If you find that you are using 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 non-hidden commands.

Default Behaviour

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).