Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Releases 12.2(37)SG to 12.2(25)SG

Current Release
12.2(54)SG1—February 7, 2011

Previous Releases
12.2(37)SG1, 12.2(37)SG, 12.2(31)SGA11, 12.2(31)SGA10, 12.2(31)SGA9, 12.2(31)SGA8, 12.2(31)SGA7, 12.2(31)SGA6, 12.2(31)SGA5, 12.2(31)SGA4, 12.2(31)SGA3, 12.2(31)SGA2, 12.2(31)SGA1, 12.2(31)SGA, 12.2(31)SG3, 12.2(31)SG2, 12.2(31)SG1, 12.2(31)SG, 12.2(25)SG4, 12.2(25)SG3, 12.2(25)SG2, 12.2(25)SG1, 12.2(25)SG

These release notes describe the features, modifications, and caveats for the Cisco IOS software on the Catalyst 4500 series switch. The most current software release is Cisco IOS Release 12.2(54)SG.

Support for Cisco IOS Software Release 12.2(54SG, the default image, follows the standard Cisco Systems® support policy, available at
http://www.cisco.com/en/US/products/products_end-of-life_policy.html

Note Although their *Release Notes* are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst ME 4900, and Catalyst 4900M/4948E) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*.

For more information on the Catalyst 4500 series switches, visit the following URL:

http://www.cisco.com/go/cat4500/docs

Contents

This publication consists of these sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco IOS Software Packaging for the Cisco Catalyst 4500 Series

A new Cisco IOS Software package for Cisco Catalyst 4500 Series Switches was introduced in Cisco IOS Software Release 12.2(25)SG. It is a new foundation for features and functionality and provides consistency across all Cisco Catalyst switches. The new Cisco IOS Software release train is designated as 12.2SG.

Prior Cisco Catalyst 4500 Series IOS Software images for the Cisco Catalyst 4500 Series Switches, formerly known as Basic Layer 3 and Enhanced Layer 3, now map to IP Base and Enterprise Services, respectively. All currently shipping Cisco Catalyst 4500 software features based on Cisco IOS Software are supported in the IP Base image of Release 12.2(54)SG, with a few exceptions.

The IP Base image does not support enhanced routing features such as NSF/SSO, BGP, EIGRP, EIGRPv6, OSPF, OSPFv3, IS-IS, Internetwork Packet Exchange (IPX), AppleTalk, VRF-lite, and Policy-Based Routing (PBR). The IP Base image supports EIGRP-Stub for limited routing on Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, V-10GE, and 6-E.

The Enterprise Services image supports all Cisco Catalyst 4500 Series software features based on Cisco IOS Software, including enhanced routing. Customers planning to enable BGP for Supervisor Engine IV, V, or V-10GE will no longer need to purchase a separate BGP license (FR-IRC4) because BGP is included in the Enterprise Services package. Beginning with 12.2(53)SG2, we support the Enterprise Services image on Supervisor Engine 6L-E.

Cisco IOS Release 12.2(46)SG1 introduced a new LAN Base software and an IP upgrade image. These complement the existing IP Base and Enterprise Services images. The LAN base image is supported on the Supervisor Engine II-Plus-10GE and Supervisor Engine 6L-E starting with
Cisco IOS Release 12.2(52)XO. LAN Base image is primarily focused on customer access and Layer 2 requirements and therefore many of the IP Base features are not required. The IP upgrade image is available if at a later date you require some of those features.

Figure 1 illustrates feature support within the 3 packages: LAN Base, IP Base, and Enterprise Services. This is not a detailed list. Please visit Feature Navigator for full package details:
http://tools.cisco.com/ITDIT/CFN/

Figure 1 Feature Support by Packages

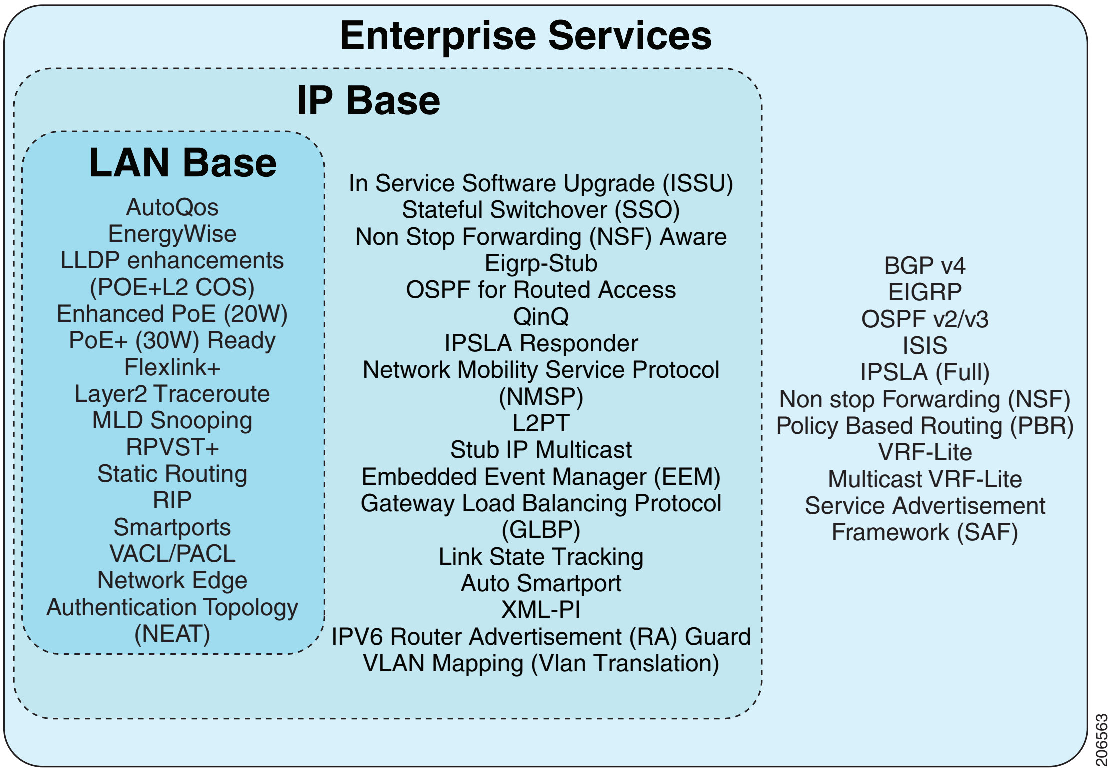


Table 1 contrasts feature support on the LAN Base vs IP Base images.

Note By default all the Features are supported on Enterprise Services image.

For information on MiBs support, pls refer to this URL:

http://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base
10G Uplink Use	12.2(46)SG1	Yes
802.1p prioritization	12.2(46)SG1	Yes
802.1p/802.1q	12.2(46)SG1	Yes
802.1w/802.1s	12.2(46)SG1	Yes
802.1X (w/ Guest VLAN and VLAN Assignment)	12.2(50)SG	Yes
802.1X and MAB with ACL assignment	12.2(50)SG	Yes
802.1X (Auth-Fail VLAN, Critical Auth, Accounting)	12.2(50)SG	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base
802.1X Wake on LAN	12.2(50)SG	Yes
802.1X Web-Auth	12.2(50)SG	Yes
802.1X with Multiple authenticated, multi-host	12.2(50)SG	Yes
802.1X w/ MDA	12.2(50)SG	Yes
802.1X w/ Open Access	12.2(50)SG	Yes
802.3ad LACP	12.2(46)SG1	Yes
802.3x – Flow Control	12.2(46)SG1	Yes
ACL Logging	12.2(46)SG1	Yes
All Mibs	12.2(52)SG	Yes
Auto QoS	12.2(53)SG	Yes
Auto SmartPort	12.2(54)SG	Yes
Auto-MDIX	12.2(46)SG1	Yes
Auto-Voice VLAN (part of Auto QoS)	No support	Yes
BOOTP	12.2(46)SG1	Yes
Bootup GOLD	No support	Yes
Broadcast Suppression	12.2(46)SG1	Yes
CDP/CDPv2	12.2(46)SG1	Yes
Community PVLAN support	No support	Yes
Config File	12.2(46)SG1	Yes
Console Access	12.2(46)SG1	Yes
Control Plane Policing	12.2(46)SG1	Yes
Copy Command	12.2(46)SG1	Yes
CoS to DSCP Map	Yes	Yes
Debug Commands	12.2(46)SG1	Yes
Device Management	12.2(46)SG1	Yes
DHCP Server	12.2(46)SG1	Yes
DHCP Snooping	12.2(46)SG1	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base
Diagnostics Tools	12.2(46)SG1	Yes
Downloading Software	12.2(46)SG1	Yes
DSCP to CoS Map	12.2(46)SG1	Yes
DSCP to egress queue mapping	12.2(46)SG1	Yes
Dynamic ARP inspection	12.2(46)SG1	Yes
EEM and EOT integration	12.2(46)SG1	No
EIGRP Stub	No support	Yes
EnergyWise 1.0	12.2(53)SG	Yes
EPoE	12.2(53)SG	Yes
Event Log	12.2(46)SG1	Yes
Factory Default Settings	12.2(46)SG1	Yes
File Management	12.2(46)SG1	Yes
Flex Link	12.2(53)SG	Yes
GLBP	No support	Yes
HSRP v1/VRRP	No support	Yes
HSRP v2 IPV4[1]	No support	Yes
HSRP v2 IPV6[2]	No support	No
ID 4.0 Voice Vlan assignment	12.2(46)SG1	Yes
ID4.1 Filter ID and per use ACL	12.2(46)SG1	Yes
IGMP	12.2(46)SG1	Yes
IGMP Snooping	12.2(46)SG1	Yes
Ingress Policing	12.2(46)SG1	Yes
Interface Access (Telnet, Console/Serial, Web)	12.2(46)SG1	Yes
IP Source Guard	12.2(46)SG1	Yes
IP Multicast	No support	Yes
IPV6 reformation	NA	Yes
IPV6 MLD snooping V1 and V2	Future	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base
IPV6 Router Advertisement (RA) Guard	12.2(54)SG	Yes
ISL Trunk	12.2(46)SG1	Yes
ISSU	No support	Yes
Jumbo Frames	12.2(46)SG1	Yes
Layer 2 Debug	12.2(46)SG1	Yes
Layer 2 PT and QinQ	No support	Yes
Layer 2 Traceroute	12.2(46)SG1	Yes
Link State Tracking	12.2(54)SG	Yes
LLDP/LLDP-MED	12.2(52)SG	Yes
LLDP enhancements (PoE+Layer 2 COS)	12.2(54)SG	No
Local Web Auth	12.2(52)SG	Yes
MAB (MAC Authentication Bypass)	12.2(50)SG	Yes
MAC Address Filtering	12.2(50)SG	Yes
MAC Based Access List	12.2(50)SG	Yes
Management IPV6 port	12.2(52)SG	Yes
MLD Snooping	12.2(53)SG	Yes
Multicast Filtering	12.2(46)SG1	Yes
Multihop SXP (CTS)	No support	12.2(52SG
Network Edge Access Topology (NEAT)	No support	Yes
No. of QoS Filters No. of Security ACE	Yes (4K entries)	Yes
No. of VLAN Support	2048	4096
OSPF for Routed Access[3]	No support	Yes
PAgP	12.2(46)SG1	Yes
Passwords Password clear protection	12.2(46)SG1	Yes
PIM SM/DM	No support	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base
PoE (up to 15.4W only)	12.2(46)SG1	Yes
PoE+ Ready	Yes	Yes
Port Monitoring (interface Stats)	12.2(46)SG1	Yes
Port Security	12.2(46)SG1	Yes; only 1024 MACs
Post Status	12.2(46)SG1	Yes
PVST+	12.2(53)SG	Yes
Q-in-Q	No support	Yes
RACL (DSCP based)	12.2(46)SG1	Yes
RADIUS/TACACS+ (AAA)	12.2(46)SG1	Yes
RMON	12.2(46)SG1	Yes
Routing – RIP, Static	12.2(46)SG1	Yes
RPR	12.2(46)SG1	Yes
RPVST+	12.2(53)SG	Yes
RSPAN	12.2(46)SG1	Yes
Service Advertisement Framework (SAF)	No support	No
Smart Call Home	No support	Yes
SmartPorts (Role based MACRO)	12/2(53)SG	Yes
SNMP (including SNMv3)	12.2(46)SG1	Yes
Source port Filtering (Private VLAN)	12.2(46)SG1	Yes
SPAN (# of sessions) – Port Mirroring	12.2(46)SG1 (2 sessions)	Yes (8 bidirectional sessions)
SSHv2/Secure Copy, FTP, SSL, Syslog, Sys Information	12.2(46)SG1	Yes
Storm Control	12.2(46)SG1	Yes
TDR	No support	Yes
Time Protocols (SNTP, TimeP)	12.2(46)SG1	Yes
Time-based ACL	12.2(46)SG1	Yes
Traffic Mirroring (SPAN)	12.2(46)SG1	Yes
Trusted Boundary (LLDP & CDP Based)	12.2(46)SG1	Yes

Table 1 LAN Base/IP Base Image Support

Feature	LAN Base	IP Base
UDLD	12.2(46)SG1	Yes
VACL and PACL	12.2(46)SG1	Yes
VLAN Mapping (VLAN Translation)	12.2(54)SG	Yes
Voice VLAN	12.2(46)SG1	Yes
VRRP	No support	Yes
VTP	12.2(46)SG1	Yes
WCCP	No support	Yes
XML-PI	12.2(54)SG	Yes

[1] Supported on all supervisor engines.

[2] Supported only for Catalyst 4900M and Supervisor Engines 6-E/6L-E.

[3] Supported on WS-X45-SUP6-E and WS-X45-SUP6L-E

Orderable Product Numbers:

- S45IPB-12237SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image) (cat4500-ipbase-mz)
- S45IPBK9-12237SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12237SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support) (cat4500-entservices-mz)
- S45ESK9-12237SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S45IPB-12231SGA—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image) (cat4500-ipbase-mz)
- S45IPBK9-12231SGA—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12231SGA—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support) (cat4500-entservices-mz)
- S45ESK9-12231SGA—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S45IPB-12231SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image) (cat4500-ipbase-mz)
- S45IPBK9-12231SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II-Plus-10GE, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12231SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support) (cat4500-entservices-mz)

- S45ESK9-12231SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)
- S45IPB-12225SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, II+10GE, IV, V, and V-10GE (IP Base image) (cat4500-ipbase-mz)
- S45IPBK9-12225SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines II-Plus, II-Plus-TS, IV, V, and V-10GE (IP Base image with Triple Data Encryption Standard (3DES)) (cat4500-ipbasek9-mz)
- S45ES-12225SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with BGP support) (cat4500-entservices-mz)
- S45ESK9-12225SG—Cisco IOS software for the Catalyst 4500 Series Supervisor Engines IV, V, and V-10GE (Enterprise Services image with 3DES and BGP support) (cat4500-entservicesk9-mz)

Catalyst 4500 Series Switch Cisco IOS Release Strategy

Cisco IOS Release 12.2SG train offers the latest features for the Catalyst 4500 Series supervisor engines. Customers with Catalyst 4500 Series supervisor engines who need the latest hardware support and software features should migrate to Cisco IOS Release 12.2(54)SG.

Note As part of the Cisco IOS Reformation effort, Cisco IOS Releases 12.2EW and 12.2SG are the same release train with a name change.

Catalyst 4500 Series has three maintenance trains. The Cisco IOS Release 12.2(31)SGA train is the longest living train. Currently, the Cisco IOS Release 12.2(31)SGA8 is the recommended release for customers who require a release with a maintenance train.The Cisco IOS Release 12.2(53)SG is the latest maintenance train and includes the most recent features including support for the WS-X45-Sup6L-E supervisor engine and OSPF for routed Access.

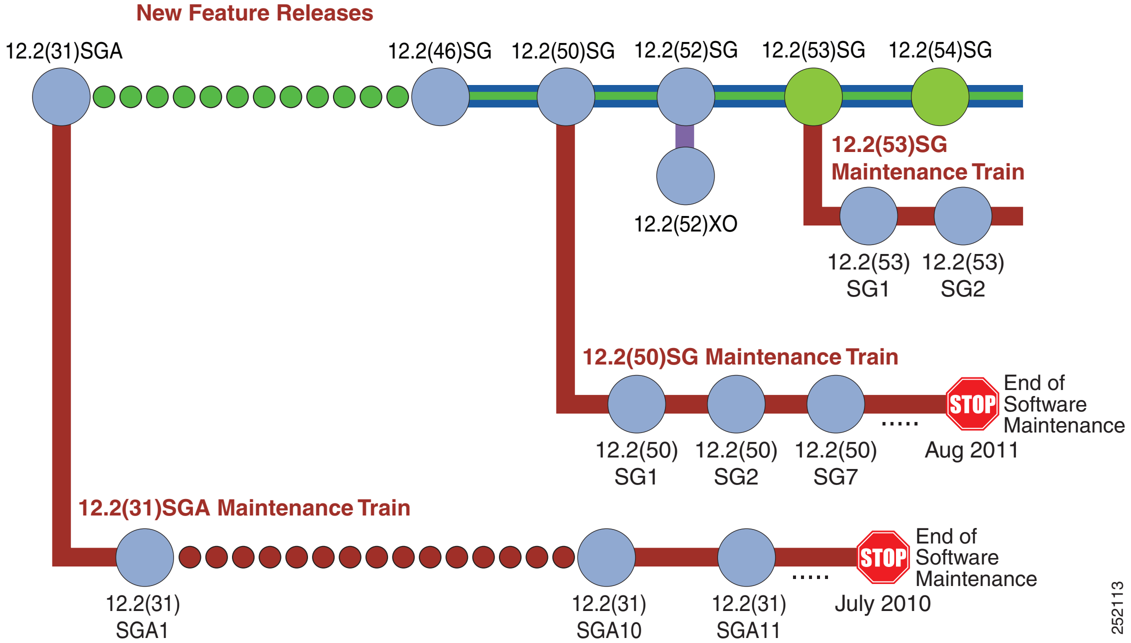
For more information on the Catalyst 4500 series switches, visit the following URL:

http://www.cisco.com/go/cat4500/docs

Cisco IOS Software Migration Guide

Figure 2 displays the two active, 12.2(31)SGA and 12.2(50)SG, and newly introduced 12.2(53)SG extended maintenance trains.

Figure 2 Software Release Strategy for the Catalyst 4500 Series Switch



Summary of Migration Plan

- Customers requiring the latest Cisco Catalyst 4500 Series hardware and software features should migrate to Cisco IOS Software Release 12.2(54)SG.
- Cisco IOS Software Release 12.2(31)SGA and 12.2(50)SG will continue offering maintenance releases. The latest release from the 12.2(31)SGA maintenance train is 12.2(31)SGA10. The latest release from the 12.2(50)SG maintenance train is 12.2(50)SG4

Support

Support for Cisco IOS Software Release 12.2(54)SG follows the standard Cisco Systems® support policy, available at
http://www.cisco.com/en/US/products/products_end-of-life_policy.html

System Requirements

This section describes the system requirements:

- Supported Hardware on Catalyst 4500 Series Switch, page 11
- Supported Features on the Catalyst 4500 Series Switch, page 19
- Unsupported Features, page 29

Supported Hardware on Catalyst 4500 Series Switch

Table 2 lists the hardware supported on the Catalyst 4500 Series Switch.

Table 2 Supported Hardware

Product Number (append with “=” for spares)	**Product Description**	**Software Release**
		Minimum
Supervisor Engines		
WS-X4013+=	Catalyst 4500 series switch Supervisor Engine II-Plus **Note** This engine is supported only on 3, 6, and 7 slot chassis (not on 10-slot chassis).	12.1(19)EW
WS-X4013+TS	Catalyst 4500 series switch Supervisor Engine II-Plus-TS **Note** This engine is supported only on 3 slot chassis.	12.2(20)EWA
WS-X4013+10GE	Catalyst 4500 series switch Supervisor Engine II-Plus-10GE **Note** This engine is supported only on 3, 6, and 7 slot chassis (not on 10-slot chassis).	12.2(25)SG
WS-X4515=	Catalyst 4500 series switch Supervisor Engine IV	12.1(12c)EW
WS-X4515/2=	Catalyst 4507R series switch Redundant Supervisor Engine IV	12.1(12c)EW
WS-X4516=	Catalyst 4500 series switch Supervisor Engine V	12.2(18)EW
WS-X4516/2=	Catalyst 4507R series switch Redundant Supervisor Engine V	12.2(18)EW
WS-X4516-10GE=	Catalyst 4500 series switch Supervisor Engine V-10GE	12.2(25)EW
WS-X45-Sup6-E	Catalyst 4500 E-series switch Supervisor Engine 6-E **Note** This engine is supported on legacy and E-series chassis.	12.2(40)SG
WS-X45-Sup6L-E	Catalyst 4500 E-series switch Supervisor Engine 6L-E **Note** This engine is supported on legacy and E-series 3,6, and 7 slot chassis.	12.2(52)XO
Gigabit Ethernet Switching Modules		
WS-X4302-GB	2-port 1000BASE-X (GBIC) Gigabit Ethernet module	12.1(19)EW
WS-X4306-GB	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4418-GB	18-port 1000BASE-X (GBIC) Gigabit Ethernet server switching module	12.1(8a)EW
WS-X4412-2GB-T	12-port 1000BASE-T Gigabit Ethernet and 2-GBIC ports switching module	12.1(8a)EW
WS-X4424-GB-RJ45	24-port 10/100/1000BASE-T Gigabit Ethernet RJ-45 switching module	12.1(8a)EW
WS-X4448-GB-LX	48-port 1000BASE-LX (small form-factor pluggable) Gigabit Ethernet fiber optic interface switching module	12.1(8a)EW
WS-X4448-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet switching module	12.1(8a)EW
WS-X4448-GB-SFP	48-port 1000BASE-X (small form-factor pluggable) module	12.2(20)EW

Table 2 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
WS-X4506-GB-T	6-port Alternately-Wired 10/100/1000BASE-T Catalyst 4500 series Power over Ethernet (PoE) 802.3af or 1000BASE-X SFP	12.2(20)EWA
WS-X4524-GB-RJ45V	24-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4548-GB-RJ45	48-port 10/100/1000BASE-T Gigabit Ethernet module	12.1(19)EW
WS-X4548-GB-RJ45V	48-port 10/100/1000BASE-T RJ-45 Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4548-RJ45V+	48-port 10/100/1000 Premium PoE line card	12.2(50)SG
WS-X4624-SFP-E	Non-blocking 24-port 1000BASEX (small form factor pluggable) module	12.2(44)SG
WS-X4648-RJ45V-E	48 port 10/100/1000 Mb with 2 to 1 oversubscription	12.2(40)SG
WS-X4648-RJ45V+E	48 port 10/100/1000 Mb with 2 to 1 oversubscription	12.2(40)SG
Fast Ethernet Switching Modules		
WS-X4124-FX-MT	24-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module	12.1(8a)EW
WS-X4148-FX-MT	48-port 100BASE-FX Fast Ethernet MT-RJ multimode fiber switching module	12.1(8a)EW
WS-X4148-FE-LX-MT	48-port 100BASE-LX10 Fast Ethernet MT-RJ single-mode fiber switching module	12.1(13)EW
WS-X4148-FE-BD-LC	48-port 100BASE-BX10-D module	12.2(18)EW
WS-X4248-FE-SFP	48-port 100BASE-X SFP switching module	12.2(25)SG
WS-U4504-FX-MT	4-port 100BASE-FX (MT-RF) uplink daughter card	12.1(8a)EW
Ethernet/Fast Ethernet (10/100) Switching Modules		
WS-X4124-RJ45	24-port 10/100 RJ-45 module	12.2(20)EW
WS-X4148-RJ	48-port 10/100 RJ-45 switching module	12.1(8a)EW
WS-X4148-RJ21	48-port 10/100 4xRJ-21 (telco connector) switching module	12.1(8a)EW
WS-X4148-RJ45V	48-port Pre-standard PoE 10/100BASE-T switching module	12.1(8a)EW for data support 12.1(11b)EW for data and inline power support
WS-X4224-RJ45V	24-port 10/100BASE-TX RJ-45 Cisco Catalyst 4500 series PoE 802.3af	12.2(20)EW
WS-X4232-GB-RJ	32-port 10/100 Fast Ethernet RJ-45, plus 2-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	12.1(8a)EW
WS-X4248-RJ45V	48-port 10/100BASE-T RJ-45 Cisco Catalyst 4500 series PoE 802.3af	12.2(18)EW
WS-X4248-RJ21V	48-port 10/100 Fast Ethernet RJ-21 Cisco Catalyst 4500 series PoE 802.3af telco	12.2(18)EW

Table 2 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
WS-X4232-RJ-XX	32-port 10/100 Fast Ethernet RJ-45 modular uplink switching module	12.1(8a)EW
Other Modules		
MEM-C4K-FLD64M	Catalyst 4500 series switch CompactFlash, 64 MB Option	12.1(8a)EW
MEM-C4K-FLD128M	Catalyst 4500 series switch CompactFlash, 128 MB Option	12.1(8a)EW
WS-F4531	Catalyst 4500 series switch NetFlow Services Card on Catalyst 4500 series switch Supervisor Engines IV and V	12.1(13)EW
WS-X4590=	Catalyst 4500 series switch Fabric Redundancy Modules	12.2(18)EW
PWR-C45-1000AC	Catalyst 4500 series switch 1000 Watt AC power supply for chassis 4503, 4506, and 4507R (data only)	12.1(12c)EW
PWR-C45-1400DC	Catalyst 4500 series switch 1400 Watt DC triple input power supply (data-only)	12.2(25)EW
PWR-C45-1400DC-P	Catalyst 4500 series switch 1400 Watt DC power supply with integrated PEM	12.1(19)EW
PWR-C45-1400AC	Catalyst 4500 series switch 1400 Watt AC power supply (data-only)	12.1(12c)EW
PWR-C45-1300ACV	Catalyst 4500 series switch 1300 Watt AC power supply with integrated voice for chassis 4503, 4506, and 4507R	12.1(12c)EW
PWR-C45-2800ACV	Catalyst 4500 series switch 2800 Watt AC power supply with integrated voice (data and PoE) for chassis 4503, 4506, and 4507R	12.1(12c)EW
PWR-C45-4200ACV	Catalyst 4500 series switch 4200 Watt AC dual input power supply with integrated voice (data and PoE)	12.2(25)EWA5
WS-P4502-1PSU	Catalyst 4500 series switch auxiliary power shelf (25-slot), including one PWR-4502	12.1(19)EW
PWR-4502	Catalyst 4500 series switch auxiliary power shelf redundant power supply	12.1(19)EW
PWR-C45-6000ACV	Catalyst 4500 Series Switch 6000 W AC power supply	12.2(53)SG

For Catalyst 4500 transciever module compatibility information, see the url:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Table 3 briefly describes the supported CWDM wavelengths in the Catalyst 4500 Classic Series Switch.

Table 3 CWDM GBIC and SFP Supported Wavelengths for the Catalyst 4500 Classic Series Switch

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
CWDM-GBIC (or SFP) -1470	Longwave 1470 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1490	Longwave 1490 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1510	Longwave 1510 nm laser single-mode	12.1(12c)EW

Table 3 CWDM GBIC and SFP Supported Wavelengths for the Catalyst 4500 Classic Series Switch

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
CWDM-GBIC (or SFP) -1530	Longwave 1530 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1550	Longwave 1550 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1570	Longwave 1570 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1590	Longwave 1590 nm laser single-mode	12.1(12c)EW
CWDM-GBIC (or SFP) -1610	Longwave 1610 nm laser single-mode	12.1(12c)EW

Table 4 briefly describes the supported DWDM wavelengths in the Catalyst 4500 Classic Series Switch.

Table 4 DWDM SFP Supported Wavelengths for the Catalyst 4500 Classic Series Switch

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
DWDM-SFP-6061=	Cisco 1000BASE-DWDM SFP 1560.61 nm	12.2(37)SG
DWDM-SFP-5979=	Cisco 1000BASE-DWDM SFP 1559.79 nm	12.2(37)SG
DWDM-SFP-5898=	Cisco 1000BASE-DWDM SFP 1558.98 nm	12.2(37)SG
DWDM-SFP-5817=	Cisco 1000BASE-DWDM SFP 1558.17 nm	12.2(37)SG
DWDM-SFP-5655=	Cisco 1000BASE-DWDM SFP 1556.55 nm	12.2(37)SG
DWDM-SFP-5575=	Cisco 1000BASE-DWDM SFP 1555.75 nm	12.2(37)SG
DWDM-SFP-5413=	Cisco 1000BASE-DWDM SFP 1554.13 nm	12.2(37)SG
DWDM-SFP-5494=	Cisco 1000BASE-DWDM SFP 1554.94 nm	12.2(37)SG
DWDM-SFP-5252=	Cisco 1000BASE-DWDM SFP 1552.52 nm	12.2(37)SG
DWDM-SFP-5172=	Cisco 1000BASE-DWDM SFP 1551.72 nm	12.2(37)SG
DWDM-SFP-5092=	Cisco 1000BASE-DWDM SFP 1550.92 nm	12.2(37)SG
DWDM-SFP-5012=	Cisco 1000BASE-DWDM SFP 1550.12 nm	12.2(37)SG
DWDM-SFP-4851=	Cisco 1000BASE-DWDM SFP 1548.51 nm	12.2(37)SG
DWDM-SFP-4772=	Cisco 1000BASE-DWDM SFP 1547.72 nm	12.2(37)SG
DWDM-SFP-4692=	Cisco 1000BASE-DWDM SFP 1546.92 nm	12.2(37)SG
DWDM-SFP-4612=	Cisco 1000BASE-DWDM SFP 1546.12 nm	12.2(37)SG
DWDM-SFP-4453=	Cisco 1000BASE-DWDM SFP 1544.53 nm	12.2(37)SG
DWDM-SFP-4373=	Cisco 1000BASE-DWDM SFP 1543.73 nm	12.2(37)SG
DWDM-SFP-4694=	Cisco 1000BASE-DWDM SFP 1542.94 nm	12.2(37)SG
DWDM-SFP-4614=	Cisco 1000BASE-DWDM SFP 1542.14 nm	12.2(37)SG
DWDM-SFP-4056=	Cisco 1000BASE-DWDM SFP 1540.56 nm	12.2(37)SG
DWDM-SFP-3977=	Cisco 1000BASE-DWDM SFP 1539.77 nm	12.2(37)SG
DWDM-SFP-3898=	Cisco 1000BASE-DWDM SFP 1539.98 nm	12.2(37)SG
DWDM-SFP-3819=	Cisco 1000BASE-DWDM SFP 1538.19 nm	12.2(37)SG

Table 4 DWDM SFP Supported Wavelengths for the Catalyst 4500 Classic Series Switch

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
DWDM-SFP-3661=	Cisco 1000BASE-DWDM SFP 1536.61 nm	12.2(37)SG
DWDM-SFP-3582=	Cisco 1000BASE-DWDM SFP 1535.82 nm	12.2(37)SG
DWDM-SFP-3504=	Cisco 1000BASE-DWDM SFP 1535.04 nm	12.2(37)SG
DWDM-SFP-3425=	Cisco 1000BASE-DWDM SFP 1534.25 nm	12.2(37)SG
DWDM-SFP-3268=	Cisco 1000BASE-DWDM SFP 1532.68 nm	12.2(37)SG
DWDM-SFP-3190=	Cisco 1000BASE-DWDM SFP 1531.90 nm	12.2(37)SG
DWDM-SFP-3112=	Cisco 1000BASE-DWDM SFP 1531.12 nm	12.2(37)SG
DWDM-SFP-3033=	Cisco 1000BASE-DWDM SFP 1530.33 nm	12.2(37)SG
DWDM-SFP-6141=[1]	Cisco 1000BASE-DWDM SFP 1561.41 nm	12.2(53)SG3
DWDM-SFP-5736=[2]	Cisco 1000BASE-DWDM SFP 1557.36 nm	12.2(53)SG3
DWDM-SFP-5332=[3]	Cisco 1000BASE-DWDM SFP 1553.32 nm	12.2(53)SG3
DWDM-SFP-4931=[4]	Cisco 1000BASE-DWDM SFP 1540.31 nm	12.2(53)SG3
DWDM-SFP-4532=[5]	Cisco 1000BASE-DWDM SFP 1545.32 nm	12.2(53)SG3
DWDM-SFP-4134=[6]	Cisco 1000BASE-DWDM SFP 1541.34 nm	12.2(53)SG3
DWDM-SFP-3739=[7]	Cisco 1000BASE-DWDM SFP 1537.39 nm	12.2(53)SG3
DWDM-SFP-3346=[8]	Cisco 1000BASE-DWDM SFP 1533.46 nm	12.2(53)SG3

[1] Not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG.

[2] Not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG.

[3] Not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG.

[4] Not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG.

[5] Not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG.

[6] Not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG.

[7] Not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG.

[8] Not supported on Cisco IOS Release 12.2(54)SG and Cisco IOS XE Release 3.1.0 SG.

Table 5 briefly describes the four chassis in the Catalyst 4500 Series Switch. For the chassis listed in the table, refer to Table 6 on page 17 for software release information.

Table 5 Chassis Description for the Catalyst 4500 Series Switch

Product Number (append with "=" for spares)	**Description of Modular Chassis**
WS-C4503	Catalyst 4503 chassis includes these components: • 3 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine III, Supervisor Engine II-Plus-10GE, Supervisor Engine II-Plus-TS, Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4506	Catalyst 4506 chassis includes these components: • 6 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine III, Supervisor Engine II-Plus-10GE, Supervisor Engine II-Plus, and Supervisor Engine II
WS-C4507R	Catalyst 4507R chassis includes these components: • 7 slots • Fan tray • Supports Supervisor Engine 6L-E, Supervisor Engine 6-E, Supervisor Engine V-10GE, Supervisor Engine V, Supervisor Engine IV, Supervisor Engine II-Plus-10GE, and Supervisor Engine II-Plus
WS-C4510R	Catalyst 4510R chassis includes these components: • 10 slots; slot 10 accepts only the Catalyst 4500 series 2-port Gigabit Ethernet line card (WS-X4302-GB with Supervisor Engine V) **Note** The Supervisor Engine V-10GE does not have this restriction. • Fan tray • Supports Supervisor Engine 6-E, Supervisor Engine V-10GE and Supervisor Engine V

Table 6 DOM Support on the Catalyst 4500 Series Switch

Transceiver Module	Support in Software Since...
CWDM- SFP-*xx*	12.2(20)EWA
DWDM-GBIC-*xx*	12.1(19)EW
DWDM-SFP	12.2(37)SG
DWDM-X2-*xx*	12.2(50)SG
GLC-BX-D	12.2(20)EWA
GLC-BX-U	12.2(20)EWA
SFP-10G-SR	12.2(54)SG
SFP-10G-LR	12.2(54)SG
SFP-10G-LRM	12.2(54)SG

Supported Hardware on Catalyst 4500 E-Series Switch

In addition to the classic line cards and supervisor engines, Cisco IOS Software Release 12.2(54)SG supports the next-generation high-performance E-Series Supervisor Engine 6-E with CenterFlex technology and E-Series line cards and chassis. A brief list of primary E-Series hardware supported on Catalyst 4500 series switch (Table 7).

Table 7 Supported E-Series Hardware

Product Number	Description
WS-C4503-E	Cisco Catalyst 4500 E-Series 3-Slot Chassis • Fan tray • No Power Supply
WS-C4506-E	Cisco Catalyst 4500 E-Series 6-Slot Chassis • Fan tray • No Power Supply
WS-C4507R-E	Cisco Catalyst 4500 E-Series 7-Slot Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability
WS-C4507R+E	Cisco Catalyst 4500 E-Series 7-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability

Table 7 Supported E-Series Hardware

Product Number	Description
WS-C4510R-E	Cisco Catalyst 4500 E-Series 10-Slot Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • All port card slots support 6, 24, and 48Gbps when used with Supervisor Engine 7-E. Slots 8, 9, and 10 are limited to 6Gbps when used with a Supervisor Engine 6-E.
WS-C4510R+E	Cisco Catalyst 4500 E-Series 10-Slot 48 GB-ready Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • You cannot place a linecard with a backplane traffic capacity exceeding 6Gbps in slots 8, 9 and 10 of a Catalyst 4510R+E chassis when used with a Supervisor Engine 6-E.
WS-X45-Sup6-E	Cisco Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) w/ TwinGig
WS-X45-Sup6L-E	Cisco Catalyst 4500 E-Series Sup 6L-E
WS-X4624-SFP-E	Cisco Catalyst 4500 E-series 24-Port 1000BaseX (small form factor pluggable) module
WS-X4648-RJ45V-E	Cisco Catalyst 4500 E-Series 48-Port PoE 802.3af 10/100/1000(RJ45)
WS-X4648-RJ45V+E	Cisco Catalyst 4500 E-Series 48-Port Premium PoE 10/100/1000
WS-X4606-X2-E	Cisco Catalyst 4500 E-Series 6-Port 10GbE (X2) w/ TwinGig
WS-X4648-RJ45-E	Cisco Catalyst 4500 E-Series 48-Port 10/100/1000(RJ45)

Table 8 outlines the chassis and supervisor engine compatibility.
(M=Minimum release, R=Recommended release)

Table 8 Chassis and Supervisor Compatiblity

Chassis	Sup II+	Sup II+TS	Sup II+10G	Sup IV	Sup V	Sup V-10GE	Sup 6-E	Sup 6L-E
WS-C4503-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO
WS-C4506-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8		M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO
WS-C4507R-E	M: 12.2(31)SGA6 R: 12.2(31)SGA8		M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	M: 12.2(52)XO R: 12.2(52)XO

Table 8 Chassis and Supervisor Compatiblity

Chassis	Sup II+	Sup II+TS	Sup II+10G	Sup IV	Sup V	Sup V-10GE	Sup 6-E	Sup 6L-E
WS-C4507R+E	M: 12.2(54)SG R: 12.2(54)SG		M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG
WS-C4510R-E					M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(31)SGA6 R: 12.2(31)SGA8	M: 12.2(40)SG R: 12.2(44)SG	
WS-C4510R+E					M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	M: 12.2(54)SG R: 12.2(54)SG	

Supported Features on the Catalyst 4500 Series Switch

Table 9 lists the Cisco IOS software features for the Catalyst 4500 Series Switch.

Table 9 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

Layer 2 Switching Features
Storm Control
Storm Control: Per-Port Multicast Suppression (Sup 6-E only)
Multicast Storm Control[1]
IP Source Guard
IP Source Guard for Static Hosts
PVRST+
Layer 2 protocol tunneling
Layer 2 transparent bridging[2]
Layer 2 MAC[3] learning, aging, and switching by software
Unicast MAC address filtering
VMPS[4] Client
Layer 2 hardware forwarding up to 102 Mpps
Layer 2 Control Policing (Sup 6-E and Sup 6L-E only)
Layer 2 switch ports and VLAN trunks
Spanning-Tree Protocol (IEEE 802.1D) per VLAN
802.1s and 802.1w
Layer 2 traceroute
Unidirectional Ethernet port
Per-VLAN spanning tree (PVST) and PVST+
Spanning-tree root guard
Spanning-tree Loop guard and PortFast BPDU Filtering

Table 9 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

Support for 9216 byte frames
Port security on PVLANs
Private VLANs
Private VLAN DHCP snooping
Private VLAN promiscuous trunk
Private VLAN trunks[5]
Community PVLANs
ISL[6]-based VLAN encapsulation (excluding blocking ports on WS-X4418-GB and WS-X4412-2GB-T)[7]
IEEE 802.1Q-based VLAN encapsulation
Multiple VLAN access port
VLAN Trunking Protocol (VTP) and VTP domains
VTP v3
No. of VLAN support per switch: 2048 (for LAN Base), 4096 (for IP Base)
Unidirectional link detection (UDLD) and aggressive UDLD
Sub-second UDLD (Fast UDLD)
SNMP V3 support for Bridge-MIB with VLAN indexing
Resilient Ethernet Protocol
Ethernet CFM
Ethernet OAM Protocol
Layer 3 Routing, Switching, and Forwarding
802.1Q Tunneling (Q in Q)[8]
Pragmatic General Multicast
ANCP Client[9]
PIM-SSM mapping
Bidiectional PIM[10]
Auto RP Listener
IP and IP multicast routing and switching between Ethernet ports
IP Multicast Load Splitting (Equal Cost Multipath (ECMP) using S, G and Next-hop)
Static IP routing
Classless routing[11]
PBR[12]
Dynamic Buffer Limiting
Selective Dynamic Buffer Limiting
QoS-based forwarding based on IP precedence
Trusted boundary
Cisco Modular QoS Command-Line Interface (Sup 6-E and Sup 6L-E only)
Auto QoS

Table 9 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

Match CoS for non-IPV4 traffic
IPv6 Forwarding in Hardware (Sup 6-E and Sup 6L-E only)
CoS Mutation
CEF[13] load balancing
uRPF[14] (Sup 6-E and Sup 6L-E only)
Hardware-based IP CEF routing at 48 Mpps
Up to 128,000 IP routes
Up to 32,000 IP host entries (Layer 3 adjacencies)
Up to 16,000 IP multicast route entries
Multicast flooding suppression for STP changes
Software routing of IPX, AppleTalk, and IPv6.
IGMPv1, IGMPv2, and IGMPv3 (Full Support)
IGMP Querier
VRF-lite
Multicast VRF-lite[15]
VRF-aware IP services
VRF-aware TACACS+
Route Leaking[16]
IP Unnumbered
SVI Autostate Exclude
Supported Protocols
IS-IS[17]
DTP[18]
RIP[19] and RIP II
EIGRP[20]
EIGRP IPv6 (Sup 6-E and Sup 6L-E only)
OSPF[21]
OSPF for Routed Access[22]
BGP4[23]
BGP route-map Continue
BGP Neighbor Policy
MBGP[24]
MSDP[25]
ICMP[26] Router Discovery Protocol
PIM[27]—sparse and dense mode
Static routes
Classless interdomain routing (CIDR)

Table 9 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

DVMRP[28]
SSM
NTP[29]
WCCP version 2 Layer 2 Redirection
VRRP[30]
SCP[31]
GLBP[32]
EtherChannel Features
Cisco EtherChannel technology - 10/100/1000 Mbps, 10 Gbps
Load balancing for routed traffic, based on source and destination IP addresses
Load sharing for bridged traffic based on MAC addresses
ISL on all EtherChannels
IEEE 802.1Q on all EtherChannels
Bundling of up to eight Ethernet ports
Up to 64 active Ethernet port channels
Trunk Port Security over EtherChannel
Link State Tracking
Additional Protocols and Features
Link Layer Discovery Protocol (LLDP)
Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED)
PoEP via LLDP
DSCP/CoS via LLDP
Routed Jumbo Frame support
SPAN CPU port mirroring
SPAN packet-type filtering
SPAN destination in-packets option
SPAN ACL filtering
RSPAN
Enhanced VLAN statistics
Netflow version 8
NetFlow Statistics Collection
NetFlow Statistics Export Version 1 and Version 5
NetFlow Bridged IP Flow
Secondary addressing
Bootstrap protocol (BOOTP)
Authentication, authorization, and accounting using TACACS+ and RADIUS protocol
Cisco Discovery Protocol (CDP)

Table 9 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

CDP 2nd Port Status TLV
FlexLink and MAC Address-Table Move Update
802.1ab Link Layer Discovery Protocol (LLDP)
802.1ab LLDP Media Discovery (LLDP-MED)
Network Mobility Services Protocol
Selecting Mode of Capturing Control Packets (Not supported on Sup 6-E)
Sticky port security
Trunk port security
Voice VLAN Sticky port security
Cisco Group Management Protocol (CGMP) server support
HSRP[33] over Ethernet, EtherChannels - 10/100/1000Mbps, 10 Gbps
HSRP v2 for IPv4
HSRP v2 for IPv6
IGMP snooping version1, version 2, and version 3 (Full Support)
IGMP filtering
Port Aggregation Protocol (PagP)
802.3ad LACP
SSH version 1 and version 2[34]
Inline power preallocation
show interface capabilities command
IfIndex persistence
UDLR[35]
Enhanced SNMP MIB support
SNMP[36] version 1, version 2, and version 3
SNMP version 3 (with encryption)
IPv6 Multicast Listener Discovery Snooping (Sup 6-E and 6L-E only)
IPv6 PACL (Sup 6-E and 6L-E only)
IPv6 RA Guard (Sup 6-E and 6L-E only)
IPv6 Interface Statistics (Sup 6-E and 6L-E only)
DHCP server and relay-agent
DHCP snooping
DHCP client autoconfiguration
DHCP Option 82 Pass Through
DHCP Relay Agent for IPv6 [37]
802.1X Multiple Domain Authentication and Multiple Authorization
802.1X with ACL Assignment and Redirect URLs
802.1X with per-user ACL and Filter-ID ACL

Table 9 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

RADIUS-Provided Session Timeouts
RADIUS CoA
MAC Move and Replace
802.1X with Guest VLANs
802.1X port-based authentication
802.1X with port security
802.1X accounting
802.1X with voice VLAN ID
802.1X private VLAN assignment
802.1X private guest VLAN
802.1X RADIUS-supplied session timeout
802.1X authentication failure VLAN
802.1X MAC Authentication Bypass
802.1X Inaccessible Authentication Bypass
802.1X with User Distribution
802.1X Unidirectional Controlled Port
802.1X MDA with Voice Assignment
Cisco TrustSec SGT Exchange Protocol (SXP) IPv4
Flexible Authentication Sequencing
Multi-Authentication
Open Authentication
Web Authentication
Local Web Authentication (EPM syslog and Common session ID)
PPPoE Intermediate Agent[38]
Cisco NAC[39] Layer 2 802.1X
Port flood blocking
Router standard and extended ACLs [40]on all ports with no performance penalty
Identity 4.1 ACL Policy Enforcement[41]
Identity 4.1 Network Edge Access Topology
Extended IPX ACL
VLAN ACL
PACL[42]
Time-based ACL
Downloadable ACLs
Control Plane Policing
Two-Rate Three-Color Policing (Sup 6-E and Sup 6L-E only)
Local Proxy ARP

Table 9 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

Dynamic ARP Inspection on PVLANs
Dynamic ARP Inspection
Dynamic Multi-Protocol Ternary Content Addressable Memory (Sup 6-E and Sup 6L-E only)
Per-port QoS[43] rate-limiting and shaping
QoS for IPv6
Per-port Per-VLAN QoS
Per-VLAN CTI
ARP QoS (Sup 6-E and Sup 6L-E only)
Inline power support for Cisco IP phones
PoE[44]
Energy Wise
Enhanced Power over Ethernet Support (Sup 6-E and Sup 6L-E only)
Power redundancy
RPR[45]
SSO[46]
SSO Aware HSRP
SSO support for routed ports
Non-stop Forwarding Awareness
Non-stop Forwarding Awareness for EIGRP-stub in IP base for all supervisor engines
Non-stop Forwarding with Stateful Switchover
ISSU[47]
MAC Address Notification
Combined Mode Power Resiliency
SmartPort macros
AutoSmartPort macros
Forced 10/100 Auto Negotiation
802.1s standards compliance
IS-IS MIB
OSPF and EIGRP Fast Convergence[48]
Time Domain Reflectometry
CNA[49]
CLI to turn off Auto MDIX[50]
Logging redirection
Service-Aware Resource Allocation (Sup 6-E and Sup 6L-E only)
TwinGig Converter Module (Sup 6-E nd 6L-E only)
FAT File System (Sup 6-E and Sup 6L-E only)
High Availability: 2+2 10GE or 4+4 1GE active uplinks (Sup 6-E only)

Table 9 Cisco IOS Software Feature Set for the Catalyst 4500 Series and E-Series Switch

EEM[51]
EEM with ISSU
VSS client with PagP+
IP/SLA[52]
Embedded management[53]
MAC notify MIB
Eight configurable queues per port (Sup 6-E and Sup 6L-E only)
X2 Link Debounce Timer
IP SLA
Enhanced Object Tracking subfeatures: • HSRP with EOT • VRRP with EOT • GLBP with EOT • IP SLA with EOT • Reliable Backup Static Routing with EOT
Management port
Management Port Features with IPv6
Inactivity Timer
OBFL[54]
boot config command
Crashdump enhancement
Unicast MAC filtering
Smart Call Home
DHCPv6 Ethernet Remote ID option
DHCPv6 Relay - Persistent Interface ID option DHCPv6 Relay Agent notification for Prefix Delegation
PIM SSM Mapping
VRF lite NSF support with routing protocols OSPF/EIGRP/BG
PIM Accept Register - Rogue Multicast Server Protection[55]
Configuration Rollback
Archiving crashfile information
Per-VLAN Learning
XML Programmatic Interface
VLAN Mapping (VLAN Translation)
GOLD Online Diagnostics (Sup 6-E and 6L-E only)
IPSG for Static Hosts
Layer Control Packet

1. Requires the Catalyst 4500 series switch Supervisor Engine V

2. Hardware-based transparent bridging within a VLAN
3. MAC = Media Access Control
4. VMPS = VLAN Management Policy Server
5. Only Supervisr Engine 6-E
6. ISL = Inter-Switch Link
7. Ports 3 thru 18 on the WS-X4418-GB and ports 1 thru 12 on the WS-X4412-2GB
8. Requires the Catalyst 4500 series switch Supervisor Engine V
9. not supported on E-Series Supervisor Engine 6-E
10. Only Supervisr Engine 6-E
11. The **ip classless** command is not supported as classless routing is enabled by default.
12. PBR = policy-based routing
13. CEF = Cisco Express Forwarding
14. uRPF = Unicast Reverse Path Forwarding
15. Only Supervisr Engine 6-E
16. Route Leaking from a global routing table into a VRF and Route Leaking from a VRF into a global routing table
17. IS-IS = Intermediate System to Intermediate System
18. DTP = Dynamic Trunking Protocol
19. RIP = Routing Information Protocol
20. EIGRP = Enhanced Interior Gateway Routing Protocol
21. OSPF = Open Shortest Path First
22. Support for Supervisor Engine 6-E and Supervisor Engine 6L-E only
23. BGP4 = Border Gateway Protocol 4
24. MBGP = Multicast Border Gateway Protocol
25. MSDP = Multicast Source Discovery Protocol
26. ICMP = Internet Control Message Protocol
27. PIM = Protocol Independent Multicast
28. DVMRP = Distance Vector Multicast Routing Protocol
29. NTP = Network Time Protocol
30. VRRP = Virtual Router Redundancy Protocol
31. SCP = Secure Copy Protocol
32. GLBP = Gateway Load Balancing Protocol
33. HSRP = Hot Standby Router Protocol
34. SSH = Secure Shell Protocol
35. UDLR = Unidirectional Link Routing
36. SNMP = Simple Network Management Protocol
37. only Sup 6-E and 6L-E
38. not supported on E-Series Supervisor Engine 6-E
39. NAC = Network Admission Control
40. ACLs = Access Control Lists
41. filter-ID and per-user ACL
42. PACL = Port Access Control List
43. QoS = Quality of Service
44. PoE = Power over Ethernet
45. RPR = Supervisor engine redundancy
46. SSO = Stateful switchover (includes Stateful IGMP Snooping and Stateful DHCP Snooping)
47. ISSU = In Service Software Upgrade Process
48. The Catalyst 4500 series switch supports Fast Hellos, ISPF, and LSA Throttling.
49. CNA = Cisco Network Assistant; Minimum CNA release that supports Releases 12.2(25)EW is 1.0(2). Minimum CNA release that supports Release 12.2(20)EWA is 1.0(1).
50. On supported linecards: WS-X4124-RJ45, WS-X4148-RJ (and WS-X4232-GB-RJ) with hardware revision 3.0 or higher

51. EEM = Embedded Event anager
52. Includes HTTPS-HTTP with SSL 3.0, CEF-MIB, Embedded Syslog Manage, ...
53. Includes SNMP over IPv6, SYSLOG, HTTP over IPv6.
54. OBFL = On Board Failure Logging; Supverisor Engine 6-E only
55. The route-map keyword is not supported.

Features Unique to Supervisor Engines 6-E and 6L-E

With Cisco IOS Release 12.2(54)SG, the following features are available only with Supervisor Engine 6-E and Supervisor Engine 6L-E:

- IPv6
  - IPv6 Addressing Architecture
  - CDP IPv6 Address Family
  - DNS resolver for AAAA over an IPv4 transport
  - DNS resolver for AAAA over an IPv6 transport
  - Extended ACL
  - Hop-by-Hop option header
  - ICMP Rate Limiting
  - ICMPv6
  - ICMPv6 Redirect
  - IPv6 over IEEE 802.1Q
  - ISATAP (supported in software only)
  - Loopback
  - MLD Snooping (supported in software and hardware on Catalyst 4900M, Catalyst 4948E, Supervisor Engine 6-E, and Catalyst 6L-E)
  - MLDv1/v2
  - MTU Path Discovery for IPv6
  - OSPFv3
  - RIPng
  - EIGRPv6
  - PACL
  - RA Guard
  - IPv6 Interface Statistics
- FAT filesystem
- PIM (SM, DM, SDM)
- QoS
  - Two Rate three Color Policing
  - Table map support for marking
  - Class based queuing actions (shaping/bandwidth/queue-limit/dbl/strict priority)
- Voltage Margining CLI

- QoS for IPv6
- ARP QoS

Unsupported Features

For all Supervisor Engines (II-Plus thru 6-E), the following features are not supported in Cisco IOS Release 12.2(54)SG for the Catalyst 4500 series switches:

- The following ACL types:
  - Standard Xerox Network System (XNS) access list
  - Extended XNS access list
  - DECnet access list
  - Protocol type-code access list
- ADSL and Dial access for IPv6
- AppleTalk EIGRP (use native AppleTalk routing instead)
- Bridge groups
- Cisco IOS software IPX ACLs:
  - <1200-1299>   IPX summary address access list
- Cisco IOS software-based transparent bridging (also called “fallback bridging”)
- Connectionless (CLNS) routing; including IS-IS routing for CLNS. IS-IS is supported for IP routing only.
- DLSw (data-link switching)
- IGRP (use EIGRP instead)
- **isis network point-to-point** command
- Kerberos support for access control
- Lock and key
- NAT-PT for IPv6
- NetFlow per-VRF
- PBR with Multiple Tracking Options
- QoS for IPv6 traffic (only supported on Supervisor 6)
- Reflexive ACLs
- Routing IPv6 over an MPLS network
- Two-way community VLANs in private VLANs
- WCCP version 1
- CFM CoS
- PBR with EOT

New and Changed Information

These sections describe the new and changed information for the Catalyst 4500 series switch running Cisco IOS software:

New Hardware Features in Release 12.2(37)SG

Note The Catalyst 4006 chassis is no longer supported in Cisco IOS Release 12.2(37)SG.

Release 12.2(37)SG provides the following new hardware for the Catalyst 4500 series switch:

- WS-C4503-E
- WS-C4506-E

New Software Features in Release 12.2(37)SG

Release 12.2(37)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- Multi Domain Authentication (“Configuring 802.1X Port-Based Authentication” chapter)
- Selective Dynamic Buffer Limiting (“Configuring QoS” chapter)
- SVI Autostate Exclude (“Configuring Layer 3 Interface” chapter)
- IP Source Guard for Static Hosts (“Configuring DHCP Snooping, IP Source Guard, and IPSG for Static Hosts” chapter)
- BGP route-map Continue Support for Outbound Policy

  For details, locate the feature entry in the Feature Information Table located toward the end of the "Connecting to a Service Provider Using External BGP" module
- Auto RP Listener (Refer to the Cisco IOS Release 12.4 documentation)
- Logging Redirection (“Configuring Cisco NSF with SSO Supervisor Engine Redundancy” chapter and the “Catalyst 4500 Series Switch System Error Message Guide”)

Note The implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

New Hardware Features in Release 12.2(31)SGA

Note Cisco IOS Release 12.2(31)SGA is the first IOS release supporting the ME-X4924-10GE.

Following hardware was supported:

- X2-10GB-LRM

New Software Features in Release 12.2(31)SGA

Release 12.2(31)SGA provides the following Cisco IOS software features for the Catalyst 4500 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- In Service Software Upgrade ("Configuring the Cisco IOS In Service Software Upgrade" chapter)
- Trunk Port Security over EtherChannel ("Configuring Port Security and Configuring EtherChannel" chapters)
- Match CoS for Non-IPv4 Traffic ("Configuring QoS" chapter)
- CoS Mutation ("Configuring QoS" chapter)
- QinQ Tunneling and Protocol Tunneling ("Configuring 802.1Q and Layer 2 Protocol Tunneling" chapter)
- IP Unnumbered ("Configuring IP Unnunmbered Support" chapter)
- CLI to turn off Auto-MDIX CLI on supported linecards (WS-X4124-RJ45, WS-X4148-RJ (and WS-X4232-GB-RJ) with hardware revision 3.0 or higher) ("Configuring Layer 3 Interfaces" chapter)

Note The implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

New Hardware Features in Release 12.2(31)SG

Release 12.2(31)SG provides the following new hardware for the Catalyst 4500 series switch:

- None

New Software Features in Release 12.2(31)SG

Release 12.2(31)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

- Non-Stop Forwarding with Stateful Switchover (NSF/SSO) ("Configuring Cisco NSF with SSO Supervisor Engine Redundancy" chapter)
- SSO Aware HSRP ("Configuring Cisco NSF with SSO Supervisor Engine Redundancy" chapter)
- Control Plane Policing ("Configuring Control Plane Policing" chapter)
- WCCP version 2 Layer 2 Redirection ("Configuring WCCPv2 Services" chapter)
- MAC Authentication Bypass ("Configuring 802.1X Port-Based Authentication" chapter)
- 802.1X Inaccessible Authentication Bypass ("Configuring 802.1X Port-Based Authentication" chapter)
- 802.1X Unidirectional Controlled Port ("Configuring 802.1X Port-Based Authentication" chapter)
- Private VLAN Promiscuous Trunk ("Configuring Private VLANs" chapter)
- MAC Address Notification ("Administering the Switch" chapter)
- Voice VLAN Sticky Port Security ("Configuring Port Security" chapter)
- Combined Mode Power Resiliency ("Environmental Monitoring and Power Management" chapter)
- Virtual Router Redundancy Protocol (VRRP) (Refer to the Cisco IOS Release 12.3 documentation)
- Secure Copy Protocol (SCP) (Refer to the Cisco IOS Release 12.3 documentation

Note The implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

New Hardware Features in Release 12.2(25)SG

Release 12.2(25)SG provides the following new hardware for the Catalyst 4500 series switch:

- WS-X4013+10GE—Catalyst 4500 series switch Supervisor Engine II-Plus-10GE
- WS-X4248-FE-SFP—Catalyst 4500 series switch 48-port 100BASE-X SFP module
- GLC-FE-100FX—100Mbit SFP, 100BASE-FX, 1310 nm wavelength, 2 km over MMF
- GLC-FE-100LX—100Mbit SFP, 100BASE-FX, 1310 nm wavelength, 10 km over MMF
- GLC-FE-100BX-D—100Mbit SFP, 100BASE-BX-D, 1550 nm TX/1310 nm RX wavelength, 10km over single-strand SMF
- GLC-FE-100BX-U—100Mbit SFP, 100BASE-BX-U, 1310 nm TX/1550 nm RX wavelength, 10km over single-strand SMF

New Software Features in Release 12.2(25)SG

Note The following chapter references are for the *Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*.

Release 12.2(25)SG provides the following Cisco IOS software features for the Catalyst 4500 series switch:

- Cisco Catalyst 4500 Series Supervisor Engine V-10GE Uplink Enhancement for simultaneous use of 10-Gigabit Ethernet and the Gigabit Ethernet SFP interfaces. (The Catalyst 4510R requires optional configuration. See the “Configuring Interfaces” chapter.)

  Note On a Catalyst 4510R series switch, if you enable both the 10-Gigabit Ethernet and the Gigabit Ethernet SFP uplink ports, you must re-boot the switch. On the Catalyst 4503, 4506, and 4507R series switches, this capability is automatically enabled.

- Simultaneous provisioning of X2 pluggable modules and SFP uplinks on the Supervisor Engine II-Plus-10GE (WS-X4013+10GE).
- IEEE 802.1S Standards Compliance (Refer to the Cisco IOS Release 12.3 documentation)
- 802.1X Authentication Failure VLAN (“Understanding and Configuring 802.1X Port-Based Authentication” chapter)
- HTTPS (Refer to the Cisco IOS Release 12.3 documentation)
- Interface Link and Trunk Status Logging Event Enhancement (“Configuring Interfaces” chapter)
- IS-IS MIB (Refer to the Cisco IOS Release 12.3 documentation
- Microflow Policing Full Flow Match (“Configuring QoS” and Configuring Netflow” chapters)
- POST enhancement for Supervisor Engine V-10GE (“Diagnostics on the Catalyst 4500 Series Switch”)
- OSPF Fast Convergence. Catalyst 4500 series switch will support Fast Hellos, ISPF, and LSA Throttling.
- Time Domain Reflectometry (“Checking Port Status and Connectivity” chapter)

- SNMP V3 support for Bridge-MIB with VLAN indexing

Note The implementation for multiple spanning tree (MST) changed from the previous release. Multiple STP (MSTP) complies with the IEEE 802.1s standard. Previous MSTP implementations were based on a draft of the IEEE 802.1s standard.

Upgrading the System Software

In most cases, upgrading the switch to a newer release of Cisco IOS software does not require a ROMMON upgrade. However, if you are running an early release of Cisco IOS software and plan to upgrade, refer to the following tables for the minimum Cisco IOS image and the recommended ROMMON release, respectively.

Note You must upgrade to ROMMON Release 12.2(44r)SG5 to run Cisco IOS Release 12.2(54)SG on the Supervisor Engine 6-E and Supervisor Engine 6L-E.

Caution Most supervisor engines have the required ROMMON release. However, due to caveat CSCed25996, we recommend that you upgrade your ROMMON to the recommended release.

Table 10 Supervisor Engine and Minimum Cisco IOS Release

Supervisor Engine	Minimum Cisco IOS Release
IV	12.1(12c)EW or 12.1(14)E
II-Plus	12.1(19)EW
II-Plus-10GE	12.2(25)SG
V	12.2(18)EW
II-Plus-TS	12.2(20)EWA
V-10GE	12.2(25)EW
ME-X4924-10GE	12.2(31)SGA
6-E	12.2(40)SG
6L-E	12.2(52)XO

Table 11 Supervisor Engine and Recommended ROMMON Release

Supervisor Engine	Minimum ROMMON Release
IV	12.1(12r)EW
II-Plus	12.1(19r)EW
II-Plus-10GE	12.2(25r)SG
V	12.1(20r)EW1
II-Plus-TS	12.2(20r)EW

Table 11 Supervisor Engine and Recommended ROMMON Release

Supervisor Engine	Minimum ROMMON Release
V-10GE	12.2(25r)EW
ME-X4924-10GE	12.2(25r)EW
6-E	12.2(44r)SG5
6L-E	12.2(44r)SG5

Table 12 ROMMON Release and Promupgrade Programs

ROMMON Release	Promupgrade Program
12.1(11br)EW	cat4000-sup3-promupgrade-121_11br_EW
12.1(12r)EW	cat4000-sup3-promupgrade-121_12r_ew
12.1(19r)EW	cat4000-ios-promupgrade-121_19r_EW
12.1(20r)EW1	cat4000-ios-promupgrade-121_20r_EW1
12.1(20r)EW2	cat4000-ios-promupgrade-121_20r_EW2
12.2(20r)EW	cat4000-ios-promupgrade-122_20r_EW
12.2(20r)EW1	cat4000-ios-promupgrade-122_20r_EW1
12.2(31r)SG3	cat4500-ios-promupgrade-122_31r_SG3
12.2(31r)SGA1	cat4500-ios-promupgrade-122_31r_SGA1
12.2(31r)SGA	cat4500-e-ios-promupgrade-122_31r_SGA3
12.2(40r)SG	cat4500-e-ios-promupgrade-122_40r_SG
12.2(44r)SG1	cat4500-e-ios-promupgrade-122_44r_SG1
12.2(44r)SG5	cat4500-e-ios-promupgrade-122_44r_SG5

The following sections describe how to upgrade your switch software:

- Guidelines for Upgrading the ROMMON, page 35
- Upgrading the Supervisor Engine ROMMON from the Console, page 36
- Upgrading the Supervisor Engine ROMMON Remotely Using Telnet, page 38
- Upgrading the Cisco IOS Software, page 43

Guidelines for Upgrading the ROMMON

Caution If your supervisor engine is shipped with a newer version of ROMMON then do not downgrade! The new ROMMON will have board settings based on a hardware revision of components, and old settings will not work.

Upgrading the Supervisor Engine ROMMON from the Console

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Note The examples in this section use the programmable read-only memory (PROM) upgrade version 12.1(20r)EW1 and Cisco IOS Release 12.1(20)EW1. For other releases, replace the ROMMON release and Cisco IOS software release with the appropriate releases and filenames.

Follow this procedure to upgrade your supervisor engine ROMMON:

Step 1 Directly connect a serial cable to the console port of the supervisor engine.

Note This section assumes that the console baud rate is set to 9600 (default). If you want to use a different baud rate, change the configuration register value for your switch.

Step 2 Download the cat4000-ios-promupgrade-121_20r_EW1 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch that is upgraded.

The cat4000-ios-promupgrade-121_20r_EW1 programs are available on Cisco.com at the same location from which you download Catalyst 4000 system images.

Step 3 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the PROM upgrade image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

If you are using a CompactFlash card, replace **bootflash:** with **slot0:**.

Step 4 Download the cat4000-ios-promupgrade-121_20r_EW1 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image cat4000-ios-promupgrade-121_20r_EW1 from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-121_20r_EW1]?
Destination filename [cat4000-ios-promupgrade-121_20r_EW1]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-121_20r_EW1...
Loading cat4000-ios-promupgrade-121_20r_EW1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!
[OK - 455620 bytes]

455620 bytes copied in 2.644 secs (172322 bytes/sec)
Switch#
```

Step 5 Enter the **reload** command to reset the switch, press **Ctrl-C** to stop the boot process, and re-enter ROMMON.

The following example shows the output after a reset into ROMMON:

```
Switch# reload
Proceed with reload? [confirm]

03:57:16:%SYS-5-RELOAD:Reload requested
```

```
**********************************************************
 *                                                        *
 * Welcome to Rom Monitor for WS-X4515 System.            *
 * Copyright (c) 2002 by Cisco Systems, Inc.              *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Rom Monitor Program Version 12.1(12r)EW


.
.(output truncated)
.

 Established physical link 100MB Half Duplex
 Network layer connectivity may take a few seconds
rommon 1 >
```

Step 6 Run the PROM upgrade program by entering this command:
boot bootflash:cat4000-ios-promupgrade-121_20r_EW1

Caution No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process. Do not perform a reset, power cycle, or OIR of the supervisor engine until the upgrade is complete.

The following example shows the output from a successful upgrade, followed by a system reset:

```
rommon 2 > boot bootflash:cat4000-ios-promupgrade-121_20r_EW1

**********************************************************
 *                                                        *
 * Rom Monitor Upgrade Utility For WS-X4515 System       *
 * This upgrades flash Rom Monitor image to the latest    *
 *                                                        *
 * Copyright (c) 2002, 2003 by Cisco Systems, Inc.        *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


 Upgrading your PROM... DO NOT RESET the system
 unless instructed or upgrade of PROM will fail !!!

 Beginning erase of 0x80000 bytes at offset 0x3f80000...  Done!

 Beginning write of prom  (0x4e8ec bytes at offset 0x3f80000)...

 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!

 Success! The prom has been upgraded successfully.
 System will reset itself and reboot in about 15
```

Step 7 Boot the Cisco IOS software image, and enter the **show version** command to verify that ROMMON has been upgraded to 12.1(20r)EW1.

Step 8 Use the **delete** command to delete the PROM upgrade program from bootflash and the **squeeze** command to reclaim unused space.

The following example shows how to delete the **cat4000-ios-promupgrade-121_20r_EW1** image from bootflash and reclaim unused space:

```
Switch# delete bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch# squeeze bootflash:

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Switch#
```

Step 9 Use the **show version** command to verify that the ROMMON has been upgraded

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4500 L3 Switch Software (cat4500-I9S-M), Version 12.1(20)EW, E
ARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 22-Oct-03 23:42 by kellmill
Image text-base: 0x00000000, data-base: 0x00F56DDC

ROM: 12.1(20r)EW1
Dagobah Revision 86, Swamp Revision 28

Switch uptime is 0 day, 0 hour, 5 minutes
System returned to ROM by reload
System image file is "bootflash:cat4500-i9s-mz.121-20.EW1"

cisco WS-C4503 (XPC8245) processor (revision 7) with 524288K bytes of memory.
Processor board ID FOX06460YD8
Last reset from Reload
3 Ethernet/IEEE 802.3 interface(s)
51 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
403K bytes of non-volatile configuration memory.

Configuration register is 0x2102

Switch#
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 43 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Supervisor Engine ROMMON Remotely Using Telnet

Caution To avoid actions that might make your system unable to boot, read this entire section before starting the upgrade.

Follow this procedure to upgrade your supervisor engine ROMMON to Release 12.1(20r)EW1. This procedure can be used when console access is not available and when the ROMMON upgrade must be performed remotely.

Note In the following section, use the PROM upgrade version cat4000-ios-promupgrade-121_20r_EW1.

Step 1 Establish a Telnet session to the supervisor engine.

Note In the following discussion, we assume that at least one IP address has been assigned to either an SVI or a routed port.

Step 2 Download the cat4000-ios-promupgrade-121_20r_EW1 program from Cisco.com, and place it on a TFTP server in a directory that is accessible from the switch to be upgraded.

The cat4000-ios-promupgrade-121_20r_EW1 programs are available on Cisco.com at the same location from which you download Catalyst 4500 system images.

Step 3 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the PROM upgrade image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

If you are using a CompactFlash card, replace **bootflash:** with **slot0:**.

Step 4 Download the cat4000-ios-promupgrade-121_20r_EW1 program into Flash memory using the **copy tftp** command.

The following example shows how to download the PROM upgrade image cat4000-ios-promupgrade-121_20r_EW1 from the remote host 172.20.58.78 to bootflash:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-ios-promupgrade-121_20r_EW1]?
Destination filename [cat4000-ios-promupgrade-121_20r_EW1]?
Accessing tftp://172.20.58.78/cat4000-ios-promupgrade-121_20r_EW1...
Loading cat4000-ios-promupgrade-121_20r_EW1 from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
[OK - 455620 bytes]

455620 bytes copied in 2.644 secs (172322 bytes/sec)
Switch#
```

Step 5 Use the **no boot system flash bootflash:***file_name* command to clear all BOOT variable commands in the configuration file. In this example, the BOOT variable was set to boot the image cat4000-i5s-mz.121-19.EW1.bin from bootflash:

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-i5s-mz.121-19.EW1.bin
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

```
Use the boot system flash bootflash:file_name command to set the BOOT variable. You will
use two BOOT commands: one to upgrade the ROMMON and a second to load the Cisco IOS
software image after the ROMMON upgrade is complete. Notice the order of the BOOT
variables in the example below. At bootup the first BOOT variable command upgrades the
```

```
ROMMON. When the upgrade is complete the supervisor engine will autoboot, and the second
BOOT variable command will load the Cisco IOS software image specified by the second BOOT
command.
```

Note The **config-register** must be set to autoboot.

```
In this example, we assume that the console port baud rate is set to 9600 bps and that the
config-register is set to 0x0102.

Use the config-register command to autoboot using image(s) specified by the BOOT variable.
Configure the BOOT variable to upgrade the ROMMON and then autoboot the IOS image after
the ROMMON upgrade is complete. In this example, we are upgrading the ROMMON to version
12.1(20r)EW1. After the ROMMON upgrade is complete, the supervisor engine will boot Cisco
IOS software Release 12.1(20)EW1.

config-register to 0x0102.

Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch(config)# boot system flash bootflash:cat4000-i9s-mz.121-20.EW1
Switch(config)# config-register 0x0102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 6 Use the **show bootvar** command to verify the boot string. The BOOT variable in this example will first run the PROM upgrade to upgrade ROMMON. Then, the upgrade software will reload and the supervisor engine will load the Cisco IOS software image.

```
Switch# sh bootvar
BOOT variable = bootflash:cat4000-ios-promupgrade-121_20r_EW1,1;bootflash:cat400
0-i9s-mz.121-20.EW1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
```

Step 7 Run the PROM upgrade program by issuing the **reload** command. Issuing this command will terminate your Telnet session.

Caution Verify the boot string in step 6. No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process. Do not perform a reset, power cycle, or OIR of the supervisor engine until the upgrade is complete.

The following example shows the console port output from a successful ROMMON upgrade followed by a system reset. Your Telnet session is disconnected during the ROMMON upgrade, so you will not see this output. This step could take 2-3 minutes to complete. You will need to reconnect your Telnet session after 2-3 minutes when the Cisco IOS software image and the interfaces are loaded.

```
Switch#reload
Proceed with reload? [confirm]

1d05h: %SYS-5-RELOAD: Reload requested



 **********************************************************
 *                                                        *
 * Welcome to Rom Monitor for WS-X4515 System.            *
 * Copyright (c) 2002 by Cisco Systems, Inc.              *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Rom Monitor Program Version 12.1(12r)EW

 Board type 2, Board revision 7
 Swamp FPGA revision 28, Dagobah FPGA revision 86

***** The system will autoboot in 5 seconds *****


 Type control-C to prevent autobooting.
 . . . . .
 Established physical link 100MB Full Duplex
 Network layer connectivity may take a few seconds


 ******** The system will autoboot now ********


 config-register = 0x0102
 Autobooting using BOOT variable specified file.....

 Current BOOT file is --- bootflash:cat4000-ios-promupgrade-121_20r_EW1




 **********************************************************
 *                                                        *
 * Rom Monitor Upgrade Utility For  WS-X4515 System       *
 * This upgrades flash Rom Monitor image to the latest    *
 *                                                        *
 * Copyright (c) 2002, 2003 by Cisco Systems, Inc.        *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Image size = 314.236 KBytes

 Maximum allowed size = 511.75 KBytes


 Upgrading your PROM... DO NOT RESET the system
 unless instructed or upgrade of PROM will fail !!!

 Beginning erase of 0x80000 bytes at offset 0x3f80000...  Done!

 Beginning write of prom  (0x4e8ec bytes at offset 0x3f80000)...

 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!

 Success! The prom has been upgraded successfully.
 System will reset itself and reboot in about 15
.
.(output truncated)
.
******** The system will autoboot now ********
```

```
 config-register = 0x0102
 Autobooting using BOOT variable specified file.....

 Current BOOT file is --- bootflash:cat4000-i9s-mz.121-20.EW1

Rommon reg: 0x56000380

Running IOS...

Decompressing the image
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
#################################################################### [OK]
```

Step 8 Use the **no boot system flash bootflash:***file_name* command to clear the BOOT command used to upgrade the ROMMON.

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 9 Use the **show version** command to verify that the ROMMON has been upgraded.

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-I9S-M), Version 12.1(20)EW, E
ARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Wed 22-Oct-03 23:42 by kellmill
Image text-base: 0x00000000, data-base: 0x00F56DDC

ROM: 12.1(20r)EW1
Dagobah Revision 86, Swamp Revision 28

Switch uptime is 0 day, 0 hour, 5 minutes
System returned to ROM by reload
System image file is "bootflash:cat4000-i9s-mz.121-20.EW1"

cisco WS-C4503 (XPC8245) processor (revision 7) with 524288K bytes of memory.
Processor board ID FOX06460YD8
Last reset from Reload
3 Ethernet/IEEE 802.3 interface(s)
51 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
403K bytes of non-volatile configuration memory.

Configuration register is 0x0102

Switch#
```

Step 10 Use the **delete** command to delete the PROM upgrade program from bootflash and the **squeeze** command to reclaim unused space.

The following example shows how to delete the cat4000-ios-promupgrade-121_20r_EW1 image from bootflash and reclaim unused space:

```
Switch# delete bootflash:cat4000-ios-promupgrade-121_20r_EW1
Switch# squeeze bootflash:

All deleted files will be removed, proceed (y/n) [n]? y

Squeeze operation may take some time, proceed (y/n) [n]? y
Switch#
```

Step 11 Use the **show bootvar** command to verify that the ROMMON upgrade program has been removed from the BOOT variable.

```
Switch#sh bootvar
BOOT variable = bootflash:cat4000-i9s-mz.121-20.EW1,1
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x0102
```

The ROMMON has now been upgraded.

See the "Upgrading the Cisco IOS Software" section on page 43 for instructions on how to upgrade the Cisco IOS software on your switch.

Upgrading the Cisco IOS Software

Caution To avoid actions that might make your system unable to boot, please read this entire section before starting the upgrade.

Before you proceed, observe the following rules for hostname:

- Do not expect case to be preserved

  Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, Choosing a Name for Your Computer.
- Must start with a letter and end with a letter or digit.
- Interior characters can only be letters, digits, and hyphens; periods and underscores not allowed.
- Names must be 63 characters or fewer; hostname of fewer than 10 characters is recommended.
- On most systems, a field of 30 characters is used for the host name and the prompt in the CLI. Longer configuration mode prompts may be truncated.

To upgrade the Cisco IOS software on your Catalyst 4500 series switch, use this procedure:

Step 1 Download Cisco IOS Release 12.1(20)EW from Cisco.com, and place the image on a TFTP server in a directory that is accessible from the supervisor engine that is upgraded.

Step 2 Use the **dir bootflash:** command to ensure that there is sufficient space in Flash memory to store the **promupgrade** image. If there is insufficient space, delete one or more images, and then enter the **squeeze bootflash:** command to reclaim the space.

If you are using a CompactFlash card, use **slot0:** instead of **bootflash**.

Step 3 Download the software image into Flash memory using the **copy tftp** command.

The following example shows how to download the Cisco IOS software image cat4000-is-mz.121-12c.EW from the remote host **172.20.58.78** to **bootflash**:

```
Switch# copy tftp: bootflash:
Address or name of remote host [172.20.58.78]?
Source filename [cat4000-is-mz121_12c.EW]?
Destination filename [cat4000-is-mz.121-12c.EW]?
Accessing tftp://172.20.58.78/cat4000-is-mz.121-12c.EW...
Loading cat4000-is-mz.121-12c.EW from 172.20.58.78 (via
FastEthernet2/1):!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
|!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 6923388/13846528 bytes]

6923388 bytes copied in 72.200 secs (96158 bytes/sec)
Switch#
```

Step 4 Use the **no boot system flash bootflash:***file_name* command to clear the cat4000-is-mz.121-8a.EW file and to save the BOOT variable.

The following example shows how to clear the BOOT variable:

```
Switch# configure terminal
Switch(config)# no boot system flash bootflash:cat4000-is-mz.121-8a.EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 5 Use the **boot system flash** command to add the Cisco IOS software image to the BOOT variable.

The following example shows how to add the cat4000-is-mz.121-12c.EW image to the BOOT variable:

```
Switch# configure terminal
Switch(config)# boot system flash bootflash:cat4000-is-mz.121-12c.EW
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3641 to 1244 bytes [OK]
Switch#
```

Step 6 Use the **config-register** command to set the configuration register to 0x2102.

The following example show how to set the second least significant bit in the configuration register:

```
Switch# configure terminal
Switch(config)# config-register 0x2102
Switch(config)# exit
Switch# write
Building configuration...
Compressed configuration from 3723 to 1312 bytes [OK]
Switch#
```

Step 7 Enter the **reload** command to reset the switch and load the software.

Caution No intervention is necessary to complete the upgrade. To ensure a successful upgrade, do not interrupt the upgrade process by performing a reset, power cycle, or OIR of the supervisor, for at least five minutes.

The following example shows the output from a successful upgrade followed by a system reset:

```
Switch# reload
Rommon reg: 0x2B004180

Upgrading FPGA...

Decompressing the image
############## [OK]

 *******************************************************
 *                                                        *
 * WS-X4014 FPGA Upgrade Utility For WS-X4014 Machines *
 *                                                        *
 * Copyright (c) 2002 by Cisco Systems, Inc.              *
 * All rights reserved.                                   *
 *                                                        *
 **********************************************************

 Image size = 483.944 KBytes

 Maximum allowed size = 1023.75 KBytes


 Upgrading your FPGA image... DO NOT RESET the system
 unless instructed or upgrade of FPGA will fail !!!

 Beginning erase of 0x100000 bytes at offset 0x3d00000...  Done!

 Beginning write of fpga image  (0x78fb0 bytes at offset 0x3d00000)...

 This could take as little as 30 seconds or up to 2 minutes.
 Please DO NOT RESET!

 Success! FPGA image has been upgraded successfully.
 System will reset itself and reboot in about 15 seconds.
 0
 ***********************************************************
 *                                                         *
 * Welcome to Rom Monitor for WS-X4014 System.             *
 * Copyright (c) 2002 by Cisco Systems, Inc.               *
 * All rights reserved.                                    *
 *                                                         *
 ***********************************************************

 Rom Monitor Program Version 12.1(12r)EW

 Board type 1, Board revision 5
 Swamp FPGA revision 16, Dagobah FPGA revision 47


 MAC Address  : 00-30-85-XX-XX-XX
 IP Address   : 10.10.10.91
 Netmask      : 255.255.255.0
 Gateway      : 10.10.10.1
 TftpServer   : Not set.
 Main Memory  : 256 MBytes

 ***** The system will autoboot in 5 seconds *****


 Type control-C to prevent autobooting.
Switch#
```

Step 8 Use the **show version** command to verify that the new Cisco IOS release is operating on the switch.

Limitations and Restrictions

These sections list the limitations and restrictions for the current release of Cisco IOS software on the Catalyst 4500 series switch.

All Supervisor Engines

- When you enter the **permit any any ?** command you will observe the **octal** option, which is unsupported in Cisco IOS Release 12.2(54)SG.

  CSCsy31324
- A Span destination of fa1 is not supported.
- The "keepalive" CLI is not supported in interface mode on the switch, although it will appear in the running configuration. This behavious has no impact on functionality.
- TDR is only supported on interfaces Gi1/1 through Gi1/48, at 1000BaseT under open or shorted cable conditions. TDR length resolution is +/- 10 m. If the cable is less than 10 m or if the cable is properly terminated, the TDR result displays "0" m. If the interface speed is not 1000BaseT, an "unsupported" result status displays. TDR results will be unreliable for cables extended with the use of jack panels or patch panels.
- The following guidelines apply to Fast UDLD:
  - Fast UDLD is disabled by default.

  - Configure fast UDLD only on point-to-point links between network devices that support fast UDLD.
  - You can configure fast UDLD in either normal or aggressive mode.
  - Do not enter the link debounce command on fast UDLD ports.
  - Configure fast UDLD on at least two links between each connected network device. This reduces the likelihood of fast UDLD incorrectly error disabling a link due to false positives.
  - Fast UDLD does not report a unidirectional link if the same error occurs simultaneously on more than one link to the same neighbor device.

- A XML-PI specification file entry does not return the desired CLI output.

  The outputs of certain commands, such as **show ip route** and **show access-lists**, contain non-deterministic text. While the output is easily understood, the output text does not contain strings that are consistently output. A general purpose specification file entry is unable to parse all possible output.

  Workaround (1):

  While a general purpose specification file entry may not be possible, a specification file entry might be created that returns the desired text by searching for text that is guaranteed to be in the output. If a string is guaranteed to be in the output, it can be used for parsing.

  For example, the output of the show ip access-lists SecWiz_Gi3_17_out_ip command is this:

```
Extended IP access list SecWiz_Gi3_17_out_ip
    10 deny ip 76.0.0.0 0.255.255.255 host 65.65.66.67
    20 deny ip 76.0.0.0 0.255.255.255 host 44.45.46.47
    30 permit ip 76.0.0.0 0.255.255.255 host 55.56.57.57
```

  The first line is easily parsed because access list is guaranteed to be in the output:

```
<Property name="access list" alias="Name" distance="1.0" length="-1" type="String"
/>
```

  The remaining lines all contain the term host. As a result, the specification file may report the desired values by specifying that string. For example, this line

```
<Property name="host" alias="rule" distance="s.1" length="1" type="String" />
```

  will produce the following for the first and second rules

```
<rule>
    deny
</rule>
```

  and the following for the third statement

```
<rule>
    permit
<rule>
```

  Workaround (2):

  Request the output of the **show running-config** command using NETCONF and parse that output for the desired strings. This is useful when the desired lines contain nothing in common. For example, the rules in this access list do not contain a common string and the order (three permits, then a deny, then another permit), prevent the spec file entry from using permit as a search string, as in the following example:

```
Extended MAC access list MACCOY
    permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000 appletalk
    permit any host 65de.edfe.fefe xns-idp
```

```
        permit any any protocol-family rarp-non-ipv4
        deny   host 005e.1e5d.9f7d host 3399.e3e1.ff2c dec-spanning
        permit any any
```

The XML output of **show running-config** command includes the following, which can then be parsed programmatically, as desired:

```
<mac><access-list><extended><ACLName>MACCOY</ACLName></extended></access-list></mac>
    <X-Interface> permit 0000.0000.ffef ffff.ffff.0000 0000.00af.bcef ffff.ff00.0000
appletalk</X-Interface>
    <X-Interface> permit any host 65de.edfe.fefe xns-idp</X-Interface>
    <X-Interface> permit any any protocol-family rarp-non-ipv4</X-Interface>
    <X-Interface> deny   host 005e.1e5d.9f7d host 3399.e3e1.ff2c
dec-spanning</X-Interface>
    <X-Interface> permit any any</X-Interface>
```

- Although the Catalyst 4500 series switch still supports legacy 802.1X commands used in Cisco IOS Release 12.2(46)SG and earlier releases (that is, they are accepted on the CLI), they do not display in the CLI help menu.
- Current IOS software cannot support filenames exceeding 64 characters.
- All software releases support a maximum of 32,768 IGMP snooping group entries.

For Supervisor Engines II+Plus through V-10GE

- For the IP Unnumbered feature, the following are not supported:
  - Dynamic routing protocols
  - HSRP/VRRP
  - Static ARP
  - Unnumbered interface and numbered interface in different VRFs
- For WCCP version 2, the following are not supported:
  - GRE encapsulation forwarding method
  - Hash bucket based assignment method
  - Redirection on an egress interface (redirection out)
  - Redirect-list ACL
- For IPX software routing, the following are not supported:
  - NHRP (Next Hop Resolution Protocol)
  - NLSP
  - Jumbo Frames
- For AppleTalk software routing, the following are not supported:
  - AURP
  - AppleTalk Control Protocol for PPP
  - Jumbo Frames
  - EIGRP
- For the NetFlow feature, the following limitations apply:

  - NetFlow will not account for control packets, packets that encountered link-level errors, and ARP/RARP packets.
  - The software cache for NetFlow is fixed, users cannot change the size.
  - The statistical distribution row that displays the distribution across various packet sizes is not available.
- For the PBR feature, the following limitations apply:
  - Packet length-based matching policies are not supported.
  - IP Precedence, TOS and Qos groups are fixed.
  - ACL/Route-map statistics are not updated.
- IGRP is not supported (use EIGRP instead).
- The MAC address table is cleared when you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.
- While running NSF and IS-IS IETF mode, if you enter the **issu runversion** command within 5 minutes of entering the **issu loadversion** command, packet loss may occur during an ISSU upgrade.

  Workaround: Configure the NSF interval timer to 0 minutes, or delay entering the **issu runversion** command until the NSF interval timer expires and NSF restarts.
- Routes may not be properly redistributed from one routing protocol to another when NSF is enabled on the switch. The success of the redistribution depends on the order in which the routing protocols converge after an NSF switchover.

  Workaround: None.
- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect because only classless routing is supported. The **ip classless** command is not supported because classless routing is enabled by default.
- The Catalyst 4510R switch does not support Supervisor Engines II-Plus, III, IV, and II-Plus-10GE. Installing an unsupported supervisor engine causes unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor engine in a redundant slot might cause a supported supervisor engine in the other slot to malfunction.
- Supervisor Engine II-Plus cannot read a CompactFlash card formatted by Supervisor Engine III or Supervisor Engine IV in a prior release.
- Catalyst 4500 supervisor engines will not be properly initialized if the VLAN configuration in the startup file does not match the information stored in the VLAN database file. This situation might occur if a backup configuration file was used.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the "Troubleshooting" section on page 170 for alternatives.
- You cannot downgrade to Cisco IOS Release 12.1(8a)EW1 after running Release 12.1(13)EW (or higher). If you need to downgrade, contact your TAC representative for further instructions, and mention caveat CSCdz59058.
- Observe the following standard Cisco IOS software behavior when deploying redundant supervisor engines in a Catalyst 4507R chassis: While the startup configuration file is being parsed, the configuration file is not applied to hardware that does not exist.

For example, if the active supervisor engine is in slot 1, and you have configured interface Gi1/1, the supervisor engine in slot 2 becomes active if you remove the active supervisor engine from the chassis. In addition, while the startup configuration file is being parsed, you will receive an error message indicating that interface Gi1/1 is no longer present. This behavior is correct. When the formerly active supervisor engine is reinserted into slot 1, there is no configuration for interface Gi1/1.

This situation does not occur when both supervisor engines are present in the chassis.

Workaround: Copy the startup configuration file into the running configuration:

```
Switch# copy startup-config running-config
```

- An unsupported default CLI for mobile IP is displayed in the HSRP configuration. Although this CLI will not damage your system, you might want to remove it to avoid confusion.

  Workaround: Display the configuration with the **show standby** command, then remove the CLI. Here is an example of the **show standby GigabitEthernet1/1** command output:

```
switch(config)# interface g1/1
switch(config)# no standby 0 name (0 is hsrp group number)
```

- For HSRP preempt delay to function consistently, you must use the **standby delay minimum** command. Be sure to set the delay to more than 1 hello interval, which ensures that a hello is received before HSRP leaves the initiate state.

  Use the **standby delay reload** option if the router is rebooting after reloading the image.

- When you attempt to run OSPF between a Cisco router and a third-party router, the two interfaces might get stuck in the Exstart/Exchange state. This problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces do not match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

  Workaround: Because the problem is caused by mismatched MTUs, you should change the MTU on either router to match the other's MTU.

- You can run .1q-in-.1q packet passthrough with a Supervisor Engine III and a Supervisor Engine IV, but you can run only .1q-in-.1q encapsulation with a Supervisor Engine II+10GE, Supervisor Engine V, and Supervisor Engine V-10GE.
- For PVST and Catalyst 4500 E-Series switch VLAN, Cisco IOS Release 12.1(13)EW supports a maximum of 3000 spanning tree port instances. If you want to use more instances, use MST rather than PVST.
- Only ports 1 and 2 on the WS-X4418-GB module and ports 13 and 14 on the WS-X4412-2GB-T module can be set as ISL trunks.
- If an original packet is dropped due to transmit queue shaping or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- For all software releases, do not use over 100,000 routes.
- Use the **no ip unreachables** command on all interfaces with ACLs configured for performance reasons.
- Layer 3 path load-balancing metrics are not supported in Cisco IOS Releases 12.1(8a)EW, 12.1(11b)EW, 12.1(12c)EW, 12.1(13)EW, 12.1(19)EW, and 12.1(20)EW. (CSCdv10578)
- The threshold for the Dynamic ARP Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.

- A limited number of ACL bindings are dynamically installed by the IP source guard feature on a Catalyst 4500 series switch Supervisor Engine II-Plus. To take full advantage of the IP source guard feature, you should use Supervisor Engine IV.
- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address is lost.
- By default, IPv6 is not enabled. To route IPv6, you must enter the **IPv6 unicast-routing** command. If you plan to use IPv6 multicast routing, use the **IPv6 multicast-routing** command.
- By default, CEF is not enabled for IPv6 (after IPv6 unicast routing is enabled). To prevent IPv6 traffic from being process-switched, use the **IPv6 cef** command.
- Multicast sources in community VLANs are not supported.
- Two-way community VLANs are not supported.
- Voice VLANs are not supported on community VLAN host interfaces.
- Private VLAN trunks do not carry community VLANs.
- When you use private VLANs on the WS-4516 module, old ARP entries will not tim eout of the ARP cache if you do not manually clear the entry. This event has no affect on production.
- Compact flash formatted in Cisco IOS Release 12.2(20)EW should be reformatted in Release 12.2(25)EW on both Supervisor Engine V-10GE and non-Supervisor V-10GE systems. Compact flash formatted on any other release does not need to be reformatted on non-Supervisor Engine V-10GE systems.
- In a redundant system, do not remove and reinsert the standby supervisor engine while the active supervisor engine is booting up. Doing so may cause a failure in the online diagnostics test.

  Workaround: Remove and reinsert the standby supervisor engine after the active supervisor engine boots. (CSCsa66509)
- When used in conjunction with a 10-slot chassis, Supervisor Engine V only supports the Catalyst 4500 series two-port Gigabit Ethernet line card (WS-X4302-GB) in the 10th slot.
- The maximum number of unique private VLAN pairs supported by the **switchport private-vlan mapping trunk** command is 500. For example, one thousand secondary VLANs could map to one primary VLAN, or one thousand secondary VLANs could map one to one to one thousand primary VLANs.
- Support for PoE depends on the use of line cards and power supplies that support PoE.

  PoE switching modules:
  - WS-X4148-RJ45V
  - WS-X4224-RJ45V
  - WS-X4248-RJ45V
  - WS-X4248-RJ21V
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V
  - 'WS-X4548-GB-RJ45V+

  PoE-enabled power supplies:
  - PWR-C45-1300ACV
  - PWR-C45-1400DC

  - PWR-C4K-2800AC
  - PWR-C45-1400AC
  - PWR-C45-1300ACV
  - 'PWR-C45-6000ACV'

- The maximum number of mappings for configuring PVLAN promiscuous trunk ports is 500 primary VLANs to 500 secondary VLANs.
- The 802.1X inaccessible authentication bypass feature is not supported with the NAC LAN port IP feature.
- Changes to the console speed in line console 0 configuration mode do not affect console speed in ROMMON. To apply the same console speed in ROMMON, use the confreg ROMMON utility.
- Supervisor Engine II-Plus does not support compact flashes formatted by an Cisco IOS image prior to Cisco IOS Release 12.2(19)EW.
- If a Catalyst 4500 series switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to following appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  If this message appears, verify that the switch is connected to the ACS. You should also ensure that the switch has been properly configured as an AAA client on the ACS.

- The **bgp shutdown** command is not supported in BGP router configuration mode. Entering this command might produce unexpected results.
- A spurious error message appears when an SSH connection disconnects after an idle timeout.

  Workaround: Disable idle timeouts. (CSCec30214)

- Interfaces on the module WS-X4148-RJ45V may not establish a link with a Daiden DN-2800G media converter when both the switch and the media converter interfaces are configured to operate at 100 Mbps and full duplex. This situation occurs when the interface on the module is configured to automatically detect and power up devices inline with the **power inline auto** command. This caveat appears in all software releases.

  Workarounds:

  1. Disable inline power on the switch ports using the **power inline never** command.

  2. Configure the media converter to autonegotiate the speed and duplex instead of running them at 100 Mbps and full duplex. (CSCee62109)

- IPSG for static hosts supports the same port mode as IPSG except that it does not support trunk port:
  - It supports Layer 2 access port and PVLAN host port (isolated or community port).
  - It does not support trunk port, Layer 3 port, or EtherChannel.
- IPSG for static hosts should not be used on uplink ports.
- Selective DBL is only supported for non-tagged or single-tagged IP packets. To achieve Selective DBL-like functionality with a non-IP packet (like Q-in-Q and IPX), apply an input policy map that matches CoS values and specifies DBL in the class map.
- For Selective DBL, if the topology involves Layer 2 Q in Q tunneling, the match cos policy map will apply to the incoming port.

- If a set of DSCP values are already configured (for example, 0-30, 0-63), specifying a subset of these DSCP values with the **qos dbl dscp-based 0-7** command will not remove the unwanted DSCP values of 8 through 63. You must use the **no** form of the command to remove the extraneous values. In this case, the **no qos dbl dscp-based 8-63** command will leave 0-7 selected.
- When you use Port Security with Multi Domain Authentication (MDA) on an interface:
  - Allow for at least three MAC addresses to access the switch: two for the phone (the MAC address of a phone gets registered to the Data domain and Voice domain), and one for the PC.
  - Ensure that the data and voice VLAN IDs differ.
- For IP Port Security (IPSG) for static hosts, the following apply:
  - As IPSG learns the static hosts on each interface, the switch CPU may achieve 100 percent if there are a large number of hosts to learn. CPU usage will drop after the hosts are learned.
  - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3, 6, and 9, the violation messages are printed only for port 9.
  - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as Inactive.
  - Autostate SVI does not work on EtherChannel.
- With the resolution of CSCsg08775, a GARP ACL entry is no longer part of the Static CAM area. However, a system-defined GARP class in Control Plane Policing (CPP) still exists.
- Certain configurations on the Catalyst 4507R and Catalyst 4510R chassis exceed the available maximum data power. These configurations include a combination of the follow PIDs:
  - Seven-slot configuration
  - Chassis WS-C4507R-E, WS-C4510R-E
  - Dual supervisor WS-X45-Sup6-E
  - One or more of the models WS-X4448-GB-RJ45 or WS-X4148-FX-MT

  To maximize the 10/100/1000 port density of 7- and 10-slot chassis when using redundant Supervisor Engine 6-E, install WS-X4548-GB-RJ45 instead of WS-X4448-GB-RJ45 line cards. If you require WS-X4448-GB-RJ45 line cards, two options are available:
  - Option 1

    Only four line card slots can be used on the Catalyst 4507R and six line card slots on the Catalyst 4510R chassis.
  - Option 2

    When all slots are required, only one model WS-X4448-GB-RJ45 line card can be used.

  To maximize the 100-BASE-FX port density of 7 and 10 slot chassis when using Supervisor Engine 6-E install WS-4248-FE-SFP line cards with FX optics instead of WS-X4148-FX-MT line cards. If WS-X4148-FX-MT line cards are required, two options are available:
  - Option 1

    You can use only 4 linecard slots on the Cat4507R chassis and 6 line card slots on the Cat4510R chassis.
  - Option 2

    When all slots are required, you can only use one WS-X4448-GB-RJ45 line card.

- When IPv6 is enabled on an interface through any CLI, you might see the following message:

  ```
  % Hardware MTU table exhausted
  ```

  In such a scenario, the IPv6 MTU value programmed in hardware differs from the IPv6 interface MTU value. This will happen if no room exists in the hardware MTU table to store additional values.

  To create room in the table, unconfigure some unused MTU values. Then, either disable or reenable IPv6 on the interface, or reapply the MTU configuration.

- To stop IPSG with static hosts on an interface, use the following commands in interface configuration submode:

  ```
  Switch(config-if)# no ip verify source
  Switch(config-if)# no ip device tracking max
  ```

  To enable IPSG with static hosts on a port, enter the following commands:

  ```
  Switch(config)# ip device tracking ****enable IP device tracking globally
  Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
  Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
  ```

Caution If you configure the **ip verify source tracking** [**port-security**] interface configuration command on a port without enabling IP device tracking globally or setting an IP device tracking maximum on that interface, IPSG with static hosts reject all the IP traffic from that interface.

Note The preceding condition also applies to IPSG with static hosts on a PVLAN host port.

- You must disable hardware control plane policing by removing the **system-cpp-policy** named ACL from the controlplane before performing an ISSU upgrade between Cisco IOS Release 12.2(40)SG and a previous release. You cannot detach **system-cpp-policy** named ACL from the controlplane in previous releases. If you are running a previous release, you must first upgrade to the latest maintenance release in the Cisco IOS Release 12.2(31) SGA*x* while performing an ISSU upgrade to Cisco IOS Release 12.2(40)SG.
- On a Supervisor Engine V-10GE (WS-X4516-10GE) in a 10-slot chassis (Catalyst 4510R and 4510RE), if a startup configuration with a new uplink mode is copied into flash memory and the system is power cycled, the system will not start with the new uplink mode. After you copy the startup configuration with the new uplink mode into flash memory, you must change the uplink mode to the new uplink mode through the command interface before the system is power cycled. This ensures that the system starts in the new uplink mode.
- When you use Supervisor Engine V in a Catalyst 4510R or 4510R-E chassis, slot 10 (FlexSlot) only supports the following linecards: the two-port GBIC (WS-X4302-GB) and the Access Gateway Module (WS-X4604-GWY). Supervisor Engine V-10GE has this same restriction when you configure its uplink select mode to **all**. Supervisor Engine V-10GE supports all Catalyst 4500 Series linecards in slot 10 when its uplink select mode is configured as tengigabitethernet or gigabitethernet. Supervisor Engine 6-E supports all Catalyst 4500 series linecards in slot 10.
- Prior to Cisco IOS Release 12.2(50)SG, on switches with Supervisor Engines V, V-10GE and earlier, class-map hit statistics on a user defined class-map in system-cpp-policy are not updated properly. With Cisco IOS Release 12.2(50)SG, the hit statistics for user-defined class-map in the system-cpp-policy are updated properly. However, in per-vlan capture mode, the hit stats for system defined in system-cpp-policy are not updated. In the global capture mode, hit stats for all class-maps (user-defined and system-defined) in the system-cpp-policy are updated properly.

For Supervisor Engine 6-E and Supervisor Engine 6L-E

- The Catalyst 4510R switch does not support Supervisor Engines 6L-E. Installing an unsupported supervisor engine causes unpredictable hardware behavior that cannot be controlled by the software. Using an unsupported supervisor engine in a redundant slot might cause a supported supervisor engine in the other slot to malfunction.
- The MAC address table is cleared while you switch between supervisor engines if either the 802.1s or 802.1w Spanning Tree Protocol is configured. To minimize address clearing and subsequent packet flooding, configure the edge ports as **spanning-tree portfast** and the link type as **spanning-tree link-type point-to-point**.
- IP classful routing is not supported; do not use the **no ip classless** command; it will have no effect, because only classless routing is supported. The command **ip classless** is not supported because classless routing is enabled by default.
- A Layer 2 LACP channel cannot be configured with the spanning tree PortFast feature.
- Netbooting using a boot loader image is not supported. See the "Troubleshooting" section on page 170 for alternatives.
- When you deploy redundant supervisors in a Catalyst 4507R, for hardware that does not exist while the startup configuration file is being parsed, the configuration file for the hardware is not applied.

  For example, if the active supervisor engine is in slot 1, and you have configured interface Gi1/1, the supervisor engine in slot 2 becomes active if you remove the active supervisor engine from the chassis. In addition, while the startup configuration file is being parsed, you will receive an error message indicating that interface Gi1/1 is no longer present. This behavior is correct. When the formerly active supervisor engine is reinserted into slot 1, there is no configuration for interface Gi1/1.

  This situation will not occur when both supervisor engines are physically in the chassis.

  Workaround: Copy the startup configuration file into the running configuration:

  ```
  Switch# copy startup-config running-config
  ```

- An unsupported default CLI for mobile IP is displayed in the HSRP configuration. Although this CLI will not harm your system, you might want to remove it to avoid confusion.

  Workaround: Display the configuration with the **show standby** command, then remove the CLI. Here is an example of **show standby GigabitEthernet1/1** command output:

  ```
  switch(config)# interface g1/1
  switch(config)# no standby 0 name (0 is hsrp group number)
  ```

- For HSRP preempt delay to function consistently, you must use the **standby delay minimum** command. Be sure to set the delay to more than 1 hello interval, thereby ensuring that a hello is received before HSRP leaves the initiate state.

  Use the **standby delay reload** option if the router is rebooting after reloading the image.
- When you attempt to run OSPF between a Cisco router and a third party router, the two interfaces might get stuck in the Exstart/Exchange state. This problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces do not match. If the router with the higher MTU sends a packet larger than the MTU set on the neighboring router, the neighboring router ignores the packet.

  Workaround: Ensure that the MTUs match.
- You can run only .1q-in-.1q packet pass-through with Supervisor Engine 6-E.

- For PVST and Catalyst 4500 E-Series switch VLAN, Cisco IOS Release 12.1(13)EW support a maximum of 3000 spanning tree port instances. If you want to use more instances, use MST rather than PVST.
- Because the Supervisor Engine 6-E supports the FAT filesystem, the following restrictions apply:
  - The **verify** and **squeeze** commands are not supported.
  - The **rename** command is supported in FAT file system.

    For Supervisor Engine 6-E, the **rename** command is available for bootflash and slot0. For all other supervisor engines, the **rename** command is supported for nvram devices only.
  - The **fsck** command is supported for slot0 device. It is not supported in the file systems on supervisor engines other than 6-E.
  - In the FAT file system, the IOS **format bootflash:** command erases user files only. It does not erase system configuration.
  - The FAT file system supports a maximum of 63 characters for file/directory name. The maximum for path length is 127 characters.
  - The FAT file system does not support the following characters in file/directory names:{ }#%^ and space characters.
  - The FAT file system honors the Microsoft Windows file attribute of read-only and read-write, but it does not support the Windows file hidden attribute.
  - Supervisor Engine 6-E uses the FAT file system for compact flash (slot0). If a compact flash is not formatted in FAT file system (such as compact flash on a supervisor engine other than 6-E), the switch does not recognize it.
- If an original packet is dropped because of transmit queue shaping or sharing configurations, a SPAN packet copy can still be transmitted on the SPAN port.
- All software releases support a maximum of 16,000 IGMP snooping group entries.
- To maximize performance, use the **no ip unreachables** command on all interfaces that are configured for ACLs.
- The threshold for the Dynamic Arp Inspection err-disable function is set to 15 ARP packets per second per interface. You should adjust this threshold depending on the network configuration. The CPU should not receive DHCP packets at a sustained rate greater than 1000 pps.
- If you first configure an IP address or IPv6 address on a Layer 3 port, then change the Layer 3 port to a Layer 2 port with the **switchport** command, and finally change it back to a Layer 3 port, the original IP/IPv6 address is lost.
- In a redundant system, do not remove and reinsert the standby supervisor engine while the active supervisor engine is booting. Doing so may cause the online diagnostics test to fail.

  Workaround: Remove and reinsert the standby supervisor engine after the active supervisor engine boots. (CSCsa66509)
- The **switchport private-vlan mapping trunk** command supports a maximum of 500 unique private VLAN pairs. For example, 500 secondary VLANs could map to one primary VLAN, or 500 secondary VLANs could map to 500 primary VLANs.
- Support for PoE depends on the use of the following line cards and power supplies.

  PoE switching modules:
  - WS-X4148-RJ45V
  - WS-X4224-RJ45V

  - WS-X4248-RJ45V
  - WS-X4248-RJ21V
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V
  - WS-X4648-RJ45V-E
  - WS-X4648-RJ45V+E
  - WS-X4548-GB-RJ45V+

  PoE enabled power supplies:

  - PWR-C45-1300ACV
  - PWR-C45-1400DC
  - PWR-C4K-2800AC
  - PWR-C45-1400AC
  - PWR-C45-1300ACV
  - PWR-C45-6000ACV

- If a Catalyst 4500 series switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

```
00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
responding.
```

  If this message appears, ensure network connectivity exists between the switch and the ACS. Also check that the switch has been properly configured as an AAA client on the ACS.

- For IP Port Security (IPSG) for static hosts, the following apply:
  - As IPSG learns the static hosts on each interface, the switch CPU may achieve 100 percent if there are a large number of hosts to learn. The CPU usage will drop after the hosts are learned.
  - IPSG violations for static hosts are printed as they occur. If multiple violations occur simultaneously on different interfaces, the CLI displays the last violation. For example, if IPSG is configured for 10 ports and violations exist on ports 3,6, and 9, the violation messages are printed only for port 9.
  - Inactive host bindings will appear in the device tracking table when either a VLAN is associated with another port or a port is removed from a VLAN. So, as hosts are moved across subnets, the hosts appear in the device tracking table as inactive.
  - Autostate SVI does not work on EtherChannel.
- When IPv6 is enabled on an interface with any CLI, you might see the following message:

```
% Hardware MTU table exhausted
```

  In such a scenario, the IPv6 MTU value programmed in hardware differs from the IPv6 interface MTU value. This occurs if no room exists in the hardware MTU table to store additional values.

  To create room, unconfigure some unused MTU values. Then, either disable or re-enable IPv6 on the interface, or reapply the MTU configuration.

- To stop IPSG with static hosts on an interface, use the following commands in interface configuration submode:

```
Switch(config-if)# no ip verify source
Switch(config-if)# no ip device tracking max
```

To enable IPSG with static hosts on a port, enter the following commands:

```
Switch(config)# ip device tracking ****enable IP device tracking globally
Switch(config)# ip device tracking max <n> ***set an IP device tracking maximum on int
Switch(config-if)# ip verify source tracking [port-security] ****activate IPSG on port
```

Caution If you configure the **ip verify source tracking [port-security]** interface configuration command on a port without enabling IP device tracking globally or setting an IP device tracking maximum on that interface, IPSG with static hosts reject all the IP traffic from that interface.

Note The preceding condition also applies to IPSG with static hosts on a PVLAN host port.

- uRPF supports up to four paths. If a packet arrives at one of the valid VLANs that is not programmed as one of the RPF VLAN in hardware, it is dropped. If traffic may arrive from any other interfaces without RPF configured, it can be switched.
- Input and output ACLs cannot override or filter traffic received on an uRPF interface.
- No CLI command exists to reflect uRPF drop packets during hardware switching. The **sh ip traffic** and **show cef int** commands do not reflect uRPF drops.
- IPv6 ACL is not supported on a switchport. IPv6 packets cannot be filtered on switchports using any of the known methods: PACL, VACL, or MACLs.
- Class-map match statements using **match ip prec | dscp** match only IPv4 packets, whereas matches performed with **match prec | dscp** match both IPv4 and IPv6 packets.
- IPv6 QoS hardware switching is disabled if the policy-map contains IPv6 ACL and match CoS in the same class-map with the IPv6 access-list has any mask within the range /81 and /127. This situation causes forwarding packets to software, which efficiently disables the QoS.
- When the following data-only Catalyst 4500 linecards are used in a Catalyst 4507R-E or 4510R-E chassis with Supervisor Engine 6-Es, the capacity of the power supply may be exceeded:
  - WS-X4148-FX-MT Cisco Catalyst 4500 Fast Ethernet Switching Module, 48-port 100BASE-FX (MT-RJ)
  - WS-X4448-GB-RJ45 Cisco Catalyst 4500 48-port 10/100/1000 Module (RJ-45)

  The Catalyst 4503-E and Catalyst 4506-E have no caveats. The Catalyst 4507R-E configurations that use power supplies rated at 1400 W or above also have no caveats.

  The following replacement switching modules will not exceed the power supply capacity for any Catalyst 4500-E chassis:

	Recommended Replacement	Description
WS-X4148-FX-MT	WS-X4248-FE-SFP	Fast Ethernet, 48-port 100BASE-X (SFP)
WS-X4448-GB-RJ45	WS-X4548-GB-RJ45	Enhanced 48-port 10/100/1000 Module (RJ-45)
WS-X4448-GB-RJ45	WS-X4648-RJ45V-E	E-Series 48-port 802.3af PoE 10/100/1000 (RJ-45)

Refer to the *Catalyst 4500 Series Module Installation Guide* to determine the power requirements for all of the Catalyst 4500 linecards and the power capacities of the Catalyst 4500 power supplies.

- Supervisor Engine 6-E *only* supports Catalyst 4500 Series linecards in slots 8-10.
- If you remove a line card from a redundant switch and initiate an SSO switch-over, then reinsert the line card, all interfaces are shutdown. The remaining configuration on the original line card is preserved.

  This situation only occurs if a switch reached SSO before you removed the line card.
- On Supervisor Engine 6-E, upstream ports support flow control auto negotiation in 1G mode only, and flow control is forced in 10G mode. If the interface is configured to auto-negotiate the flow control, and the interface is operating in 10G mode, the system forces flow control to ON and does not auto-negotiate.
- Supervisor Engine 6-E supports fast UDLD on a maximum of 32 ports.

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Note All caveats in Release 12.4 also apply to the corresponding 12.1 E releases. Refer to the *Caveats for Cisco IOS Release 12.4* publication at the following URL:

http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124MCAVS.html

Note For the latest information on PSIRTS, refer to the Security Advisories on CCO at the following URL:

http://www.cisco.com/en/US/products/products_security_advisories_listing.html

Open Caveats in Cisco IOS Release 12.2(37)SG1

This section lists the open caveats in Cisco IOS Release 12.2(37)SG1:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

```
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

```
00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum (20000). Dampening is OFF
```

```
00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum 000). Dampening is OFF
```

At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

Workarounds: Enter the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- When dot1x (radius assigned vlan), port security and voice VLAN is enabled on the port with phone and PC connected to it and PC get authenticated in radius assigned VLAN, on switchover, first packet come from PC will trigger the security violation.

  Workaround: Enter **shut/no shut** on the port to authorize the PC correctly. (CSCsi31362

- IGMP Filtering feature is not available in Cisco IOS Release 12.2(37)SG. For example, the command **igmp filter ....**, used to apply IGMP filtering on an interface, is not recognized by IOS.

  This is a temporary issue and is expected to be resolved in future IOS releases

  Workaround: None. (CSCsi40783)

- The switch will stop forwarding Layer 3 packets for a few seconds during either ISSU runversion or redundancy switch-over.

  The traffic loss only occurs when the interfaces, which the traffic travel through, are configured with HSRP and currently in HSRP Active state.

  Workaround: None. (CSCsi40980)

- The following error message is seen during an ISSU upgrade from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1 to Cisco IOS Release 12.2(37)SG or later images:

  ```
  %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

Workaround: None. This message is an informational message. (CSCsi60913)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, the following message is seen in the standby supervisor engine console:

```
%XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
context:145 length:11) due to: invalid context
```

  Workaround: None. This is an informational message. (CSCsi60898)

- If you attempt to downgrade to Cisco IOS Release 12.2(37)SG from Release 12.2(37)SG1 and if the process is started with active supervisor engine in slot-2, the downgrade fails at ‘runversion.’

  Workaround: None. (CSCsj83688)

- If you attempts to upgrade to Cisco IOS Release 12.2(37)SG1 from the Release 12.2(31)SGA and its subsequent maintainance releases, the following harmless message is displayed upon 'issu commitversion':

```
At ACTIVE:
ISSU_PROCESS-3-SYSTEM: Failed to set Standby ISSU state to the local ISSU state.

At STANDBY:
ISSU_PROCESS-3-SYSTEM: STANDBY:System not in [Init (Commit Version)] or [Init (Commit
Version)] for transitioning to [*]

where "*" can be "Init", "Load Version", etc.
```

  Workaround: None. These are informative messages. (CSCsj89384)

- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as "Unknown". After booting IOS, the chassis type is listed properly.

  Workaround: None. (CSCsl72868)

Resolved Caveats in Cisco IOS Release 12.2(37)SG1

This section lists the resolved caveats in Release 12.2(37)SG1:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

```
May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

  The error message is then followed by a traceback.

  Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

- Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:
  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)

  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  (CSCeb21064)

- Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:
  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  (CSCsd81407)

- Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:
  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  (CSCsi60004)

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can cause a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

(CSCin95836)

- A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  (CSCsi01470)

Open Caveats in Cisco IOS Release 12.2(37)SG

This section lists the open caveats in Cisco IOS Release 12.2(37)SG:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  – If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.

  – If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator enters the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

```
00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum (20000). Dampening is OFF

00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
allowed maximum 000). Dampening is OFF
```

  At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

  Workarounds: Enter the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).
- When dot1x (radius assigned vlan), port security and voice VLAN is enabled on the port with phone and PC connected to it and PC get authenticated in radius assigned VLAN, on switchover, first packet come from PC will trigger the security violation.

  Workaround: Enter **shut/no shut** on the port to authorize the PC correctly. (CSCsi31362
- IGMP Filtering feature is not available in Cisco IOS Release 12.2(37)SG. For example, the command **igmp filter ....**, used to apply IGMP filtering on an interface, is not recognized by IOS.

  This is a temporary issue and is expected to be resolved in future IOS releases

  Workaround: None. (CSCsi40783)
- The switch will stop forwarding Layer 3 packets for a few seconds during either ISSU runversion or redundancy switch-over.

  The traffic loss only occurs when the interfaces, which the traffic travel through, are configured with HSRP and currently in HSRP Active state.

  Workaround: None. (CSCsi40980)
- The following error message is seen during an ISSU upgrade from Cisco IOS Release 12.2(31)SGA or 12.2(31)SGA1 to Cisco IOS Release 12.2(37)SG or later images:

  ```
      %CHKPT-4-INVALID: Invalid checkpoint client ID (189)
  ```

  Workaround: None. This message is an informational message. (CSCsi60913)
- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, the following message is seen in the standby supervisor engine console:

  ```
  %XDR-6-XDRINVALIDHDR: XDR for client (CEF push) dropped (slots:2 from slot:3
  context:145 length:11) due to: invalid context
  ```

  Workaround: None. This is an informational message. (CSCsi60898)
- Supervisor Engine II-Plus-TS in a Catalyst 4503-E chassis running ROMMON lists the chassis type as "Unknown". After booting IOS, the chassis type is listed properly.

  Workaround: None. (CSCsl72868)

Resolved Caveats in Cisco IOS Release 12.2(37)SG

This section lists the resolved caveats in Release 12.2(37)SG:

- Occassionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be “down” after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- A bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- After an ISSU is performed on a WS-X4448-GB-SFP linecard running Cisco IOS Release 12.2(31)SGA, the output of the **show inventory** command does not display some of the 1000Base SFPs.

  Workaround: None. (CSCse43697)

- PoE switch ports configured with the **switchport voice VLAN untagged** command cause ESMP communication between a supervisor engine and the PoE line card to cease. As a result, a warning message similar to the following is printed to the console:

  ```
  %C4K_LINECARDMGMTPROTOCOL-4-ONGOINGTIMEOUTWARNING: Astro 2-2(Fa2/9-16) -
  consecutive management requests timed out.
  ```

  Workaround: Remove the switchport voice VLAN untagged configuration from the switch port. (CSCsg76374)

- When trunk ports configured with VLANs associated with SVIs that are participating in a link state routing protocol come up after either a "no shutdown" or a supervisor engine switchover, log messages similar to the following may appear:

  ```
  Nov 19 05:11:02 MET: %IPC-5-WATERMARK: 1801 messages pending in rcv for
  the port CF : Standby(2020000.11) seat 2020000
  ```

  Such messages indicate that there are pending messages for active and standby supervisor engine inter-process communication. This condition does not affect switching traffic.

  Workaround: None. (CSCsg83090)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007.

(CSCsb12598)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
  - Processing Finished messages, documented as Cisco bug ID CSCsd92405

  Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. .

(CSCsb40304)

- Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  Cisco IOS is affected by the following vulnerabilities:

  - Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
  - Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. (CSCsd92405)

- A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007.

(CSCsd85587)

- A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited is affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  (CSCse56501)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

Open Caveats in Cisco IOS Release 12.2(31)SGA11

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA11:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  clearwater# sh policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

Workarounds:

- Use a different copy protocol.
- Set a longer ssh timout.

(CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA11

This section lists the resolved caveats in Cisco IOS Release 12.2(31)SGA11:

- When running Cisco IOS Release 12.2(37)SG1 or 12.2(40)SG, if you have 802.1X with voice VLAN enabled on a switchport and have a 3rd generation phone (7961/41/70/71) running firmware 8-3-3 or greater to generate LLDP frames and cause the following traceback:

  ```
  %SYS-2-NOBLOCK: idle with blocking disabled.
  -Process= "Cat4k Mgmt HiPri", ipl= 0, pid= 42
  -Traceback= 10677608 11127844 11129E2C 1109C640 103D3448 103D2008 103D3C10 1054BA14
  10056108 1005F378 11301CDC 11811E7C 11395664 113971D4
  1139B2F8 1139EBA0
  ```

  When running Cisco IOS Release 12.2(40)SG, having a 3rd generation phone (7961/41/70/71) running firmware 8-3-3 or greater to generate LLDP frames might cause the switch to crash.

  This behavior occurs because LLDP is sent out from the phone to the switch un-tagged and is flagged as a security violation.

  If you enter the **debug dot1x all** command, you see the following security violation.

  ```
  12:59:51: dot1x-ev:Potential Security Violation Packet on GigabitEthernet2/1 with MAC
  = 001b.d584.6873, Vlan = 7
  12:59:51: dot1x-ev:Passing CDP packet from IP Phone with MAC = 001b.d584.6873, VLAN =
  7 through to CDP handler
  12:59:51: dot1x-ev:Dot1x Querying CDP for 001b.d584.6873 Mac
  12:59:51: dot1x-ev:dot1x_switch_addr_add: Host access entry already exists for
  001b.d584.6873 15
  12:59:51: dot1x-ev:dot1x_switch_addr_add: Added MAC 001b.d584.6873 to vlan 15 on
  interface GigabitEthernet2/1
  12:59:51: dot1x-ev:dot1x_switch_secure_vvid_pkt:Secured Phone MAC = 001b.d584.6873 on
  Vlan = 15
  ```

  VLAN 7 is the data VLAN and VLAN 15 is the voice VLAN.

  Workaround: Disable LLDP on the IP phone.

  CSCsq34665

- Roughly 25 seconds after a link event occurs, PIM DR and HSRP status changes. At that time, IGMPSN process usage is high:

  ```
   - Chassis Type : WS-C4510R
   - SUP: WS-X4516-10GE(2ea. Redundancy)
   - 12.2(31)SGA8
   - PIM Sparse Mode / MSDP
   - The problem was happened on two C4510Rs(Active/Standby)

  #sh proc cpu | ex 0.0
  CPU utilization for five seconds: 61%/0%; one minute: 26%; five minutes:20%
   PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
    34     1150480    695383       1654  0.13%  0.15%  0.15%   0 IDB Work
    40    26451856 202703548        130  4.50%  6.97%  6.90%   0 Cat4k Mgmt HiPri
    82     2545752  54203550         46  0.62%  0.46%  0.41%   0 IP Input
   109      181684    514353        353 46.22%  3.72%  0.77%   0 IGMPSN
  ```

```
 151     4226436  64869492         65  0.96%  0.57%  0.60%   0 IP SNMP
 152      760372  23713135         32  0.20%  0.12%  0.12%   0 PDU DISPATCHER
 153     5295944  26411152        200  1.38%  0.85%  0.88%   0 SNMP ENGINE  E
```

Workaround: None.

CSCsx75612

- ARP entries learned on PVLAN SVIs are not aged out even if enter the **no ip sticky arp** command.

  This only happens to ARP entries learned on SVIs that are mapped to PVLANs. ARP entries learned on normal SVIs are not impacted.

  Workaround: Clear the ARP entries with the **clear ip arp** command.

  CSCtb37718

- When a WS-C4500-E series chassis with WS-X45-SUP6-E, two 4200W AC power supplies, and 4 identical inputs is configured for power redundant mode, and one of the inputs is lost, a 4200WAC power supply enters err-disable state and linecards may get powered down due to insufficient power. The switch detects unequal wattage power supplies and selects the lower wattage supply while err-disabling the higher one. The following messages display:

  ```
  00:33:49: %C4K_IOSMODPORTMAN-4-POWERSUPPLYOUTPUTDECREASED: Power
  supply 2 output has decreased
  00:33:49: %C4K_CHASSIS-3-MIXINPOWERDETECTED: Power supplies in the
  chassis are of different types (AC/DC) or wattage
  00:33:49: %C4K_CHASSIS-2-INSUFFICIENTPOWERDETECTED: Insufficient power
  available for the current chassis configuration
  00:33:54: %C4K_CHASSIS-2-INSUFFICIENTPOWERSHUTDOWN: Holding module in
  slot 7 in reset, due to insufficient power
  00:33:54: %C4K_CHASSIS-2-INSUFFICIENTPOWERSHUTDOWN: Holding module in
  slot 6 in reset, due to insufficient power
  ```

  Workaround: Enter **power redundancy combined max inputs 2**.

  This command selects any available inputs to provide the power equivalent of 2 inputs (1 power supply unit). Even if one or two inputs fail, the same amount of power will be supplied.

  CSCsr26624

Open Caveats in Cisco IOS Release 12.2(31)SGA10

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA10:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

```
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater# sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

  This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

  Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not affect local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA10

This section lists the resolved caveats in Release 12.2(31)SGA10:

- When SPAN is enabled and the SPAN source port is receiving malformed packet such as the error packets produced by collision, the port might stop receiving packets or might replay the packets repeatedly to cause flooding to other ports.

  This issue is observed on platforms including WS-C4948 and WS-X4548-GB, and linecards including:

  - WS-X4418-GB (Port 3-18)
  - WS-X4506-GB-T (RJ45 ports)
  - WS-X4424-GB-RJ45
  - WS-X4448-GB-RJ45
  - WS-X4548-GB-RJ45
  - WS-X4524-GB-RJ45V
  - WS-X4548-GB-RJ45V

  Workaround: Enable packet filtering so that the SPAN session passes only good packets using the command:

  ```
  monitor session 1 filter packet-type good rx
  ```

  CSCsv07168

- On a Catalyst 4948-10GE chassis running IOS Cisco Releases 12.21(31)SGA or 12.2(46)SG, the default transmit queue selection based on IP DSCP value is incorrect. For example, both CS1 and CS5 traffics are passing through transmit queue 1, instead of 1 and 3.

  Workaround: Enable and disable global QoS, as follows:

  ```
  switch# conf t
  switch(conf)# qos
  switch(conf)# no qos
  ```

  CSCsv29945

- On a Catalyst 4500, if an isolated private VLAN trunk interface flaps, the ingress and egress per-port per-vlan service policies are no longer applied on the port.

  This impacts Cisco IOS Releases 12.2(31)SGA08, 12.2(37)SG, 12.2(40)SG, 12.2(44)SG, 12.2(46)SG, 12.2(50)SG, and 12.2(50)SG1.

  Workarounds:

  For a Classic Series Supervisor Engine, disable and configure QoS on the port.

  For example, to configure Gig 2/1 as an isolated private VLAN trunk port, do the following:

  ```
  Switch# conf t
  Enter configuration commands, one per line.  End with CNTL/Z.
  Switch(config)# interface gigabitEthernet 2/1
  Switch(config-if)# no qos
  Switch(config-if)# qos
  Switch(config-if)# end
  Switch#
  ```

You can configure the following EEM script to automate this workaround. QoS will be disabled and re-enabled whenever a port flaps.

```
logging event link-status global

event manager applet linkup-reqos
 event syslog pattern "changed state to up"
 action 1 cli command "enable"
 action 2 cli command "conf t"
 action 3 cli command "interface gigabitEthernet 2/1"
 action 4 cli command "no qos"
 action 5 cli command "qos"
```

On Supervisor Engine 6-E or a Catalyst 4900M switch, remove and reapply the QoS service policy on the impacted VLAN:

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gigabitEthernet 2/1
Switch(config-if)# vlan-range 10
Switch(config-if-vlan-range)# no service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# no service policy input secVlanInPolicy
Switch(config-if-vlan-range)# service policy output primVlanOutPolicy
Switch(config-if-vlan-range)# service policy input secVlanInPolicy
Switch(config-if-vlan-range)# end
Switch#
```

CSCsw19087

- Under certain conditions, a Catalyst 4500R chassis with two supervisor engines (Sup II+, Sup IV, or Sup V) may experience a fail over (supervisor switchover) if the keepalive messages from the peer supervisor engine are missing for 162 seconds.

  While the problem is happening, the following messages display:

```
%C4K_REDUNDANCY-4-KEEPALIVE_WARNING: STANDBY:Keepalive messages from peer Supervisor
are missing for 162 seconds
%C4K_REDUNDANCY-3-PEER_RELOAD: STANDBY:The peer Supervisor is being reset because
keepalive message(s) not received.
```

  Workaround: None. (CSCsw64001)

- Provided you enable 1000base-SX Auto-negotiation, some ports might not boot correctly after you reload or reconnect an Intel 1000Base fiber NIC.

  The following linecards are affected:

  - WS-X4302-GB
  - WS-X4306-GB
  - WS-X4418-GB
  - WS-X4448-GB-SFP
  - WS-X4506-GB-T

  E-series linecards with SFP, TenGigabit ports using HAMM modules, and WS-C4948 SFP uplinks do not exhibit this problem.

  Workarounds: Do one of the following:

  - Enter the **shut** then **no shut** commands.
  - Re-connect the cable.

CSCsx74970

- Cisco IOS Software with support for Network Time Protocol (NTP) version (v4) contains a vulnerability processing specific NTP packets that will result in a reload of the device. This results in a remote denial of service (DoS) condition on the affected device.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available and are documented in the workarounds section of the posted advisory.

  CSCsq24002

Open Caveats in Cisco IOS Release 12.2(31)SGA9

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA9:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater# sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

  This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

  Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not affect local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA9

This section lists the resolved caveats in Release 12.2(31)SGA9:

- A spoke router crashes when you shut down a connected remote interface.

  Workaround: Terminate traffic before you shut down a remote interface. (CSCsj73451)

- If your switch is running IOS releases in the SGA train prior to 12.2(50)SG and 12.2(31)SGA9 (like 12.2(46)SG or 12.2(31)SGA8), you may observe the following error messages:

  %C4K_REDUNDANCY-4-KEEPALIVE_WARNING: STANDBY:Keepalive messages from peer Supervisor are missing for 27 seconds

  %C4K_ETH-4-MACFATALRXERR: STANDBY:Supervisor EOBC port MAC was reset due to a fatal Rx error

  This issue does not impact your network.

  Workaround: None. (CSCsu10462)

  The KEEPALIVE_WARNING message is documented in the system message guide as informational.

The MACFATALRXERR message will not appear Cisco IOS Release 12.2(31)SGA9 and 12.2(50)SG onwards.

- When a port is trunking and a native VLAN is defined, LACP PDUs may be tagged in the native VLAN.

  LACP PDUs should always be transmitted untagged.

  Workaround:None. (CSCsv63758)

- A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:
  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the "workarounds" section of the advisory.

  CSCsm27071

- Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  CSCsr29468

- Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory.

  CSCsk64158

- Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  CSCsv04836

Open Caveats in Cisco IOS Release 12.2(31)SGA8

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA8:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  clearwater# sh policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:
  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

  This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

  Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not affect local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA8

This section lists the resolved caveats in Release 12.2(31)SGA8:

- A switch directly connected to the uplink ports on a Catalyst 4500 supervisor engine does not see link down when the engine reloads through the **reload** command. So, if UDLD is enabled on the neighbor switch, a link partner will enter the err-disable state.

  Workaround: Shut down supervisor uplink ports prior to reload. (CSCsl34390)

- The cpscEvent OID is defined incorrectly in the CISCO-PORT-STORM-CONTROL-MIB.

  RFC2578 indicates that the next to last sub-identifier must be zero, however, cpscEvent OID is wrongly defined as: 1.3.6.1.4.1.9.9.362.0.1.1 Because the next to last sub-identifier is 1 and not 0, cpscEventRev1 is defined as: 1.3.6.1.4.1.9.9.362.0.2 and replaces the wrong cpscEvent OID.

  Workaround: None (CSCsm23134)

- When you use 802.1X with port security and guest VLANs when migrating from Cisco IOS Release 12.2(31)SGA4 to a fixed version (a version in the *integrated-in* field), IOS installs the invalid MAC address 0042.0100.0000 in the port-security table.

  Releases 12.2(37)SG, 12.2(40)SG, and 12.2(31)SGA3 (and earlier) are not affected.

  Workarounds:

  - Avoid use of guest VLAN.
  - Either upgrade or downgrade to an non-affected version.

  (CSCsm38960)

- Link flaps occur between a WS-X4506-GB-T SFP port and the Catalyst 2960 uplink port using 1000BaseSX optical modules.

  This issue may occur between a WS-X4506-GB-T and a Catalyst 4500 configured with Supervisor Engine II-Plus-10GE.

  Workarounds: Upgrade to Cisco IOS Release 12.2(46)SG or 12.2(31)SGA8. (CSCsm09735)

- While running POST tests upon a system boot, you will see the message:

  ```
  Cpu Subsystem Tests ... seeprom: . temperature_sensor: . eobc: F
  ```

  If EOBC fails, the bootup will remain in this step for roughly two minutes.

  You can also see the EOBC test result by entering the **show diagnostic result module all detail** command after your system boots.

  Workaround: None. (CSCso23121)

- A switch crashes unexpectedly during repeated transitions of the route switch.

  Workaround: None. (CSCek25021)

- If a Catalyst 4500 switch is running MST, a brief (roughly 50 msec) Layer 2 loop can occur upon reload of the active root switch.

  Workaround: None. (CSCsm19901)

- A Catalyst 4500 switch with a redundant supervisor engine may become unresponsive due to missed keepalives. The status of the standby supervisor engine becomes unknown.

  Workarounds:

  - For systems running Cisco IOS Release 12.2(46)SG and later, or 12.2(31)SGA8 and later, enter **platform eobc reset** command from the enable prompt
  - For all other systems, power cycle the chassis or active supervisor engine.

  (CSCsl88908)

- A Host still receives traffic when an IGMP Leave has been sent.

  Workarounds:

  - Disable Host Tracking with the **no ip igmp snooping vlan 27 explicit-tracking** command.
  - Revert to IGMP v2 on the receiver.

  (CSCsm71323)

- Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  (CSCec12299)

Open Caveats in Cisco IOS Release 12.2(31)SGA7

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA7:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater# sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:
  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

  This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

  Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not affect local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA7

This section lists the resolved caveats in Release 12.2(31)SGA7:

- On a Catalyst 4500 series switch with either dual 4200W AC power supplies with one or both 220V connections, or a single 4200W AC power supply with two 220V connections, a power supply firmware glitch temporarily resets the status bits. It causes Catalyst 4500 IOS software to receive the false input voltage values (from 220V to 110V) and trigger the normal recovery routine.

  You will see one or both of the following error messages:

  ```
  *Mar 5 11:16:33.663 UTC: %C4K_CHASSIS-3-MIXINVOLTAGEDETECTED: Power supplies in the
  chassis are receiving different voltage inputs
  *Mar 5 11:16:33.663 UTC: %C4K_CHASSIS-3-MIXINPOWERDETECTED: Power supplies in the
  chassis are of different types (AC/DC) or wattage
  ```

  You may also see the following message:

  ```
  %ILPOWER-5-ILPOWER_POWER_DENY: Interface Gi2/33: inline power denied
  On ports with POE devices connected.
  ```

  This glitch temporarily shuts down the affected power supply and causes a loss of power supply redundancy. Power for the data and chassis is decremented and might cause the linecard(s) to shut down. Power for PoE also will decrement, and it could cause PDs to shut down and reset.

  Note the following:

  - Only units with serial numbers starting from with AZS12200001 and higher *do not* experience this defect.
  - If both power supplies have 110V inputs, they are *not* affected.
    The output current is lower with both 110V input connections, see
    Power Supply Calculator on cisco.com at the URL:http://tools.cisco.com/cpc/launch.jsp.

  Workaround: None. (CSCso67729)

- A group of 4 ports on a PoE linecard might *not* recognize the IEEE phone device and might *not* provide inline power. The same device(s) may work in other ports on the same module; it may work with other ports of similar linecards in other slots on the same chassis.

The group(s) of ports on which the PoE devices do not power up may differ for each instance on different systems.

The problem has been observed with the following hardware combinations:

- 4500 chassis, WS-X4013+=, WS-X4548-GB-RJ45V= (hw rev 4.0 & 4.1), 12.2(40)SG
- 4500-E chassis WS-C45-Sup6-E, WS-X4548-GB-RJ45V= (hw rev 4.0 & 4.1), 12.2(40)SG

Note Cisco IP Phone is not affected as it can be detected via CDP.

Workaround: None. (CSCso29149)

- A Catalyst 4500 switch may experience a reload if you perform two or more “write memory's via CLI” on the switch.

  This occurs with Cisco IOS Releases 12.2(25)EWA13 and earlier releases, 12.2(31)SGA6 and earlier releases, and 12.2(4x)SG releases.

  Workaround: Restrict *vty access* to one session and upgrade to Cisco IOS Release 12.2(25)EWA14 or 12.2(31)SGA7. (CSCso86459)

- On a Catalyst 4500 Supervisor Engine running Cisco IOS Releases 12.2(25)EWA13, or 12.2(31)SGA4 through 12.2(31)SGA6, you might receive the message "NVRAM Verification Failed" and the running config might not be saved to the NVRAM.

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA14 or 12.2(31)SGA7. (CSCsq27434)

Open Caveats in Cisco IOS Release 12.2(31)SGA6

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA6:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater# sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

  This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

  Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not affect local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA6

This section lists the resolved caveats in Release 12.2(31)SGA6:

- Data traffic may get dropped when Dynamic Buffer Leaking (DBL) is enabled on Catalyst 4500 switches. This problem may manifest as performance issues with TCP-based applications.

  This problem is seen either when DBL is enabled via Auto-Qos or by attaching Qos policy with DBL action. For example,

  !

  ```
  policy-map p1
       class c1
          dbl
  !
  interface Gig 3/2
     service-policy output p1
  !
  ```

  While the problem is occurring, dropped traffic is displayed under the *Dbl-Drop-Queue* counter of the **show interface counter detail** command.

  Workaround: Disable DBL globally with the **no qos dbl** command.

- Data traffic may be dropped when DBL is enabled on Catalyst 4500 switches, causing performance issues with TCP-based applications.

  While the problem occurs, drops appear under the *Dbl-Drop-Queue* counter output of the **show interface counter detail** command.

  Workaround: Disable DBL globally with the **no qos dbl** command. (CSCsk07525)

  Catalyst 4500 Supervisor Engine V-10GE (WS-X4516-10GE) running a Cisco IOS release earlier than 12.2(25)EWA13 may encounter a system reset due to NFL fatal error. When it fails, you may see the following log message:

  ```
  %C4K_SWITCHINGENGINEMAN-4-FATALERRORINTERRUPTSEEN: Fatal NFL Error !additional
  characters related to failure will be reported!
  ```

  And in the crashdump, you will see vector=600.

  Workaround: None. (CSCsl99781)

- When you run Cisco IOS Release 12.2(31)SGA5 (or earlier) on Supervisor Engine V (or below) in a 4500-E Series chassis, the following message is displayed and the switch reboots:

  ```
  "ERROR! Unsupported chassis type 52, system cannot boot. Rebooting in 10 seconds."
  ```

  This caveat is seen on bootup under either of the following conditions:

  - A 4500-E Series chassis has a Supervisor Engine V (or below) and is powered on.
  - A Supervisor Engine V (or below) is plugged into a 4500-E Series chassis that is already powered on.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA6, 12.2(37)SG or later versions of software. (CSCsm82435)

- A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Cisco has released free software updates that address this vulnerability.

Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

(CSCsj85065)

Open Caveats in Cisco IOS Release 12.2(31)SGA5

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA5:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  clearwater# sh policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

  This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

  Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not affect local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA5

This section lists the resolved caveats in Release 12.2(31)SGA5:

- After an ISSU is performed on a WS-X4448-GB-SFP linecard running Cisco IOS Release 12.2(31)SGA, the output of the **show inventory** command does not display some of the 1000Base SFPs.

  Workaround: None. (CSCse43697)

- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

  Workarounds: Enter the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- Once auto-QoS is enabled on a switch, data traffic may be dropped when Dynamic Buffer Leaking (DBL) is enabled.

  While this problem occurs, traffic drops appear under the Dbl-Drop-Queue counter on the output of the **show interface <mod/port> counter detail** command.

Workaround: Disable DBL globally by configuring the **no qos dbl** command. (CSCsk07525)

- When MSDP and OSPF are configured and you enter the **no ip routing** command, the switch reloads because of memory corruption in one of the pointers used by MSDP.

  To observe the problem, the MSDP timer must be set to 1.

  Workaround: Because this s problem does not occur if the MSDP timer is bigger, increase the timer to 5. (CSCsj61328)

- A Cisco network access server (NAS) may enter an infinite loop, produce CPUHOG error messages similar to the following, and then reload:

  ```
  %SYS-3-CPUHOG: Task is running for (112000)msecs, more than (2000)msecs
  (1/0),process = RADIUS
  ```

  If “radius-server retry method reorder” is not configured, the router may neglect to transmit RADIUS packets to servers after the “server-private” server if the “server-private” server does not respond. In addition, the reference count of a server, as shown by the output of the <CmdBold>debug aaa server-ref-count<noCmdBold> EXEC command, may improperly drop to zero. This results in no packets being transmitted to the server unless it is unconfigured and reconfigured.

  Workaround: None. (CSCin45879)

- Let us say that you have the following topology with private trunk links configure:

  Multicast Source---4500------Private VLAN Trunk----Switch-----STB

  When you change channels on the set top box, the IGMP leaves are not acknowledged and the traffic accumulates across the link (the link utilization increases by 4mb).

  Workaround: Remove the trunk configuration and configure the link as an access port. (CSCsl09521)

- A router configured with **ip summary-address rip 0.0.0.0 0.0.0.0** that is running RIP on releases later than Cisco IOS 12.3(14.8) will send out the default with a metric of 16.

- A switch running RIP on a Cisco IOS Release after 12.3(14.8) that has **ip summary-address rip 0.0.0.0 0.0.0.0** configured on an interface will send out the default with a metric of 16.

  Workaround: Instead of using **ip summary-address rip 0.0.0.0 0.0.0.0** to only send out the default, configure a distribute-list under the rip process. (CSCsd68016)

- A Catalyst 4500 supervisor engine may crash when configuring **ip flow-aggregation cache**.

  This caveats affects the following supervisor engines:

  - WS-X4516-10GE
  - WS-X4516 with the Netflow daughter card WS-F4531
  - WS-X4515 with the Netflow daughter card WS-F4531

  This problem exists in the Cisco IOS Releases 12.2(25)EWAx, 12.2(25)SG, 12.2(31)SG and 12.2(31)SGAx. It does not exist in Cisco IOS Release 12.2(37)SG.

  Workaround: Do not configure the **ip flow-aggregation cache** command until either Cisco IOS Release 12.2(25)EWA11 or 12.2(31)SGA5 IOS is available. Until then, upgrade your switch to Cisco IOS Release 12.2(37)SGx. (CSCsk21849)

Open Caveats in Cisco IOS Release 12.2(31)SGA4

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA4:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  clearwater#sh policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not affect the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occassionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

Workaround: If the SVIs associated with the physical interface are down after the switchover, enter **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only affects a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:
  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

  Workarounds: Enter the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- After an ISSU is performed on a WS-X4448-GB-SFP linecard running Cisco IOS Release 12.2(31)SGA, the output of the **show inventory** command does not display some of the 1000Base SFPs.

  Workaround: None. (CSCse43697)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)
- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not affect local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)
- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)
- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)
- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not affect performance.

  Workaround: Enter the **no shutdown** command. (CSCsg27395)
- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. Once the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).
- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA4

This section lists the resolved caveats in Release 12.2(31)SGA4:

- For Cisco IOS Releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

Workaround: None.

This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

- When trunk ports configured with VLANs associated with SVIs that are participating in a link state routing protocol come up after either a **no shutdown** or a supervisor engine switchover, log messages similar to the following may appear:

  ```
  Nov 19 05:11:02 MET: %IPC-5-WATERMARK: 1801 messages pending in rcv for
  the port CF : Standby(2020000.11) seat 2020000
  ```

  Such messages indicate that there are pending messages for active and standby supervisor engine inter-process communication. This condition does not impact switching traffic.

  Workaround: None. (CSCsg83090)

- For Cisco IOS Release 12.2(31)SG and later releases, RADIUS attribute 32 is not sent to the RADIUS server.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10. (CSCsi22041)

- An inconsistancy exists between the default signalling DSCP value used by the Catalyst 4500 series switch and CallManager 4.x, which uses DSCP 24 (by default) for the Cisco IP phone and softphone signalling. However, Auto-QoS operating on a switch requires DSCP 26. This inconsistancy causes Cisco IP phone packets to egress the switch with an incorrect DSCP. This also prevents Softphone/IP Communicator packets from obtaining the appropriate QoS.

  ```
  Switch# show qos map cos dscp
  CoS-DSCP Mapping Table
  CoS: 0 1 2 3 4 5 6 7
  --------------------------------
  DSCP: 0 8 16 26 32 46 48 56
  ```

  Workaround: None. (CSCsi52529)

- If multiple interfaces in the OSPF area have the same IP address (duplicate IP addresses are present in the network) and the IP address is used as a link-state ID of the network LSA, this network LSA might occur in the OSPF database with a high Age:

  ```
                  Net Link States (Area 100)

  Link ID         ADV Router      Age         Seq#       Checksum
  192.168.22.2     192.168.22.6      3391732      0x80000CCE 0x0053CD
  ```

  Additionally, CPU load for OSPF process might increase.

  Workaround: Avoid conflicting IP addresses. Remove duplicate IP address or shutdown the interface. (CSCsi11438)

- Lock & Key on a Catalyst 4948 switch running Cisco IOS Release 12.2(31)SGA1 does not work properly. When you open up the ACL with the **access-enable host** command, the ACL is correctly updated with an entry for the host. You can verify this with the **show access-list** command. However, the entry does not take affect and the ACL does not permit traffic from that IP address.

  Workaround: After entering the **access-enable host** command, remove, then reapply the ACL to the interface. (CSCsi20981)

- When a port on a Catalyst 4500 series switch is configured as a Private VLAN trunk port carrying normal and secondary VLANs, any ingress QoS policy applied to normal VLANs on that port in the ingress direction does not get programmed in the hardware. So, ingress traffic on normal VLANs cannot be policed using per-port per-VLAN input policers.

  Ingress service policies applied to secondary VLANs on that port work properly and are not affected.

  Workaround: None. (CSCsi48332)

- On a WS-X4418-GB line card, a bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)

Open Caveats in Cisco IOS Release 12.2(31)SGA3

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA3:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1
```

```
Class-map: c1 (match-all)
  0 packets<--------It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occassionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet

QueueID	Old QueueName	New QueueName
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- A bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

  Workarounds: Issue the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- After an ISSU is performed on a WS-X4448-GB-SFP linecard running Cisco IOS Release 12.2(31)SGA, the output of the **show inventory** command does not display some of the 1000Base SFPs.

  Workaround: None. (CSCse43697)

- A bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

  This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

  Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not impact local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When trunk ports configured with VLANs associated with SVIs that are participating in a link state routing protocol come up after either a "no shutdown" or a supervisor engine switchover, log messages similar to the following may appear:

  ```
  Nov 19 05:11:02 MET: %IPC-5-WATERMARK: 1801 messages pending in rcv for
  the port CF : Standby(2020000.11) seat 2020000
  ```

  Such messages indicate that there are pending messages for active and standby supervisor engine inter-process communication. This condition does not impact switching traffic.

  Workaround: None. (CSCsg83090)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA3

This section lists the resolved caveats in Release 12.2(31)SGA3:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

```
May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
```

The error message is then followed by a traceback.

Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can cause a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  (CSCin95836)

Open Caveats in Cisco IOS Release 12.2(31)SGA2

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA2:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
```

```
FastEthernet3/2

 Service-policy output: p1

   Class-map: c1 (match-all)
     0 packets<--------It stays at '0' despite of traffic being received
     Match: access-group name fnacl21
     police: Per-interface
       Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occassionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be “down” after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate an scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- A bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

Workarounds:

- Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
- Configure the correct default gateway on the host side. (CSCse75660)

- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

  Workarounds: Issue the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- After an ISSU is performed on a WS-X4448-GB-SFP linecard running Cisco IOS Release 12.2(31)SGA, the output of the **show inventory** command does not display some of the 1000Base SFPs.

  Workaround: None. (CSCse43697)

- A bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not impact local data switching performance because the LoPri process is of low priority with limited access to the CPU.

  Workaround: None. (CSCsg76868)

- When trunk ports configured with VLANs associated with SVIs that are participating in a link state routing protocol come up after either a "no shutdown" or a supervisor engine switchover, log messages similar to the following may appear:

  ```
  Nov 19 05:11:02 MET: %IPC-5-WATERMARK: 1801 messages pending in rcv for
  the port CF : Standby(2020000.11) seat 2020000
  ```

  Such messages indicate that there are pending messages for active and standby supervisor engine inter-process communication. This condition does not impact switching traffic.

  Workaround: None. (CSCsg83090)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- If the switch administrator unconfigures a loopback interface that is required by another configured protocol (i.e., BGP) on the primary supervisor engine, the standby supervisor engine will not reload successfully.

  Workaround: Remove all configurations that require the loopback interface before removing the loopback interface. (CSCsf06946)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA2

This section lists the resolved caveats in Release 12.2(31)SGA2:

- PoE switch ports configured with the **switchport voice vlan untagged** command cause ESMP communication between a supervisor engine and the PoE line card to cease. As a result, a warning message similar to the following is printed to the console:

  ```
  %C4K_LINECARDMGMTPROTOCOL-4-ONGOINGTIMEOUTWARNING: Astro 2-2(Fa2/9-16) -
  consecutive management requests timed out.
  ```

  Workaround: Remove the switchport voice VLAN untagged configuration from the switch port. (CSCsg76374)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

- If two next-hop router interfaces are configured on a PBR route map, CPU utilization may be high if the first next-hop router interface is reachable via interface Null0:

  ```
  route-map PBR permit 10
    match ip address <ACL>
    set ip next-hop <NEXT-HOP 1> <NEXT-HOP 2>
  ```

  Workaround: Ensure that the next-hops *do not fall* under a route pointing to Null0. Such routes may have been entered either statically or by a routing protocol configured for summarization. (CSCsd88586)

- After a PC configured for 802.1X disconnects from an IP phone port through a Catalyst 4500 series switch, the port transitions to the guest VLAN. When a PC reconnects, the switch successfully authenticates the user but the user remains on the guest VLAN.

  Workarounds:

  1) Disable the 802.1X guest-vlan supplicant. The port will not remain in the guest VLAN state. It will transition out of the unauthorized state.

  2) Use dynamic VLAN assignment through the ACS to assign the correct VLAN to the port.

  (CSCsh47641)

- The Catalyst 4500 switch does not set the router alert bit in multicast group-specific queries.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA2. (CSCsi74467)

- On PoE line cards connected to IP phones or other PoE networking devices, you might see a S2W console warning message indicating that the POE devices are either not responding to polling from the supervisor or the devices are in an an error state. When this situation exists, PoE service may not work correctly. For instance, phones will not have power or power is removed intermittently from some ports.

  This might happen for the following reasons:

  - There is a marginal or failing component(s) on the line card (requires RMA and EFA).
  - The hardware and software states are not synchronized due to a power *glitch* or to a reset of the -48V PoE.

  This situation occurs on Cisco IOS Release 12.2(31)SGA1 or lower (except for Cisco IOS Release 12.2(25)EWA10).

Note This situation does not exist on the WS-X4148-RJ45V.

Workaround: Download an image that supports PoE Health Monitoring such as Cisco IOS Release 12.2(37)SG, 12.2(31)SGA2, or 12.2(25)EWA10. These software images have code that will monitor, detect, and attempt to correct random S2W errors. Although this code does not prevent the problem, it will positively identify the issue and and reduce recovery time.

If you experience three HealthCheck warning messages within a week, RMA the line card immediately, and request an Engineer Failure Analysis (EFA) report. Perform the following debugging steps if your IP phone or PoE device fails:

Step 1 Determine if the IP phone works using other ports on the same line card.

Step 2 Determine if the same IP phone works using another line card(s) within the switch.

Step 3 Capture **show tech-support** and **show platform chassis module** *module*.

Step 4 Reset the linecard by issuing **hw-module module** *module* **reset** or by removing and reinserting the line card. Determine if the IP phone receives power from the switch.

Step 5 Capture **show tech-support** and **show platform chassis module** *module*.

Step 6 RMA the line card if the problem persists with RMA. Ask the TAC engineer to create an EFA.

(CSCsf26804)

- Windows XP PCs configured for machine authentication and PEAP may not receive an updated IP address from the DHCP server based on user credentials if the PC has been machine authenticated and can ping its previously assigned default gateway.

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA10 or 12.2(31)SGA2. (CSCsi34572)

- The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device’s filesystem, including the device’s saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

  (CSCsc19259)

- Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  (CSCsd95616)

Open Caveats in Cisco IOS Release 12.2(31)SGA1

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA1:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  clearwater#sh policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be “down” after the switchover.

Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:
  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)
- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)
- A bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)
- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)
- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

  Workarounds: Issue the **no bgp dampening** command, then the **bgp dampening** command. (CSCse12485)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- After an ISSU is performed on a WS-X4448-GB-SFP linecard running Cisco IOS Release 12.2(31)SGA, the output of the **show inventory** command does not display some of the 1000Base SFPs.

  Workaround: None. (CSCse43697)

- A bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)

- Configure a LACP channel in 802.1q tunnel mode between a Catalyst 4500 series switch and a Catalyst 6000 series switch, and apply the **redundancy reload shelf** command on the Catalyst 4500 series switch. This can cause link flaps on the EtherChannel interface when the Catalyst 4500 switch reloads.

  This happens to redundant Catalyst 4500 system, regardless the number of supervisor engines on the chassis. This problem applies to Cisco IOS Releases 12.2(31)SG and the 12.2(31)SGA maintenance train.

  Workaround: Shut off the EtherChannel interface and bring it up again. (CSCsf08912)

- Gigabit IP phones cannot process IEEE 802.1Q tagged CDP packets when 802.1X is configured on a voice VLAN. This causes the phone to continually register and de-register with Call Manager. 100 Mbps IP phones are not affected.

  Workaround: Remove the IEEE 802.1X configuration from the switch port. (CSCsg10135)

- PoE switch ports configured with the **switchport voice VLAN untagged** command cause ESMP communication between a supervisor engine and the PoE line card to cease. As a result, a warning message similar to the following is printed to the console:

  ```
  %C4K_LINECARDMGMTPROTOCOL-4-ONGOINGTIMEOUTWARNING: Astro 2-2(Fa2/9-16) -
  consecutive management requests timed out.
  ```

  Workaround: Remove the switchport voice VLAN untagged configuration from the switch port. (CSCsg76374)

- When the same MAC addresses are learned and aged out on different VLANs, the Cat4k Mgmt LoPri process will cause CPU utilization to increase. This does not impact local data switching performance because the LoPri process is of low priority with limited access to the CPU.

Workaround: None. (CSCsg76868)

- When trunk ports configured with VLANs associated with SVIs that are participating in a link state routing protocol come up after either a "no shutdown" or a supervisor engine switchover, log messages similar to the following may appear:

  ```
  Nov 19 05:11:02 MET: %IPC-5-WATERMARK: 1801 messages pending in rcv for
  the port CF : Standby(2020000.11) seat 2020000
  ```

  Such messages indicate that there are pending messages for active and standby supervisor engine inter-process communication. This condition does not impact switching traffic.

  Workaround: None. (CSCsg83090)

- When policing IEEE 802.1Q tagged non-IP traffic and calculating traffic conformance, the policer excludes the four bytes that constitute the 802.1Q tag even when you configure **qos account layer2 encapsulation**.

  Workaround: None. (CSCsg58526)

- In rare instances, the Supervisor Engine V-10GE might reload with the crashdump vector 0x00000100.

  Workaround: Monitor the switch and note the number of occurrences as well as any changes on the network prior to the reload. (CSCsh13318)

- When hardcoded duplex and speed settings are deleted after an interface shuts down, an "a-" is added to the duplex and speed in the output from the **show interface status** command.

  This does not impact performance.

  Workaround: Issue the **no shutdown** command. (CSCsg27395)

- If the ACL of an SVI interface is too large for the TCAM, ARP replies for the associated VLAN may not be processed.

  Workaround: Upgrade to Cisco IOS Release 12.2(31)SG or later and resize the TCAM with the **access-list hardware region balance** command to support the ACL Verify TCAM utilization with the **show platform hardware acl statistics utilization brief** command. (CSCsh50565)

- When a transceiver is removed rapidly from one port and placed in another on the same chassis, occasionally a duplicate seeprom message is displayed and the port is not able to handle traffic.

  Workaround: Remove the transceiver from the new port and place it in the old port. After the SFP is recognized in the old port, remove it slowly and insert it in the new port. (CSCse34693).

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA1

This section lists the resolved caveats in Release 12.2(31)SGA1:

- If port security is enabled on a PVLAN isolated trunk port, Layer 3 connectivity to hosts connected via that port may be unreachable.

  Workaround: None. (CSCsg11229)

- The Catalyst 4500 switch running 12.2(31)SG and configured for 802.1X may reset after displaying the following console messages while it switches EAP packets:

```
Jul 27 08:14:36: %SYS-2-FREEFREE: Attempted to free unassigned memory at 1A35ACA8,
alloc 10355D60, dealloc 103594B4
-Traceback= 10FAC5A8 1035A150 1035A30C 105A7A7C 1059F3A8
Jul 27 08:14:36: %SYS-6-MTRACE: mallocfree: addr, pc
 1A35ACA8,1035A14C 195FECAC,103592E8 1A1A97D4,60000010 1A1A9780,10359134
 1A084698,10249D60 1A16F008,10355724 1A0FBE24,10359098 127B42B8,600000F8
Jul 27 08:14:36: %SYS-6-MTRACE: mallocfree: addr, pc
 127B3E80,103594C4 1A35AF4C,600000F2 1A35ACA8,103594B4 1A1F9F6C,1083D310
 127B16CC,6000005E 127B11A8,50000208 127B15E0,1083D300 1A17258C,1083D2E4
Jul 27 08:14:36: %SYS-6-BLKINFO: Attempt to free a block that is in use blk 1A35AC80,
 words 580, alloc 10355D60, Free, dealloc 103594B4, rfcnt 0
-Traceback= 10F96808 10FAC5B8 1035A150 1035A30C 105A7A7C 1059F3A8
Jul 27 08:14:36: %SYS-6-MEMDUMP: 0x1A35AC80: 0xAB1234CD 0x390000 0x1983C854 0x11F30330
Jul 27 08:14:36: %SYS-6-MEMDUMP: 0x1A35AC90: 0x10355D60 0x1A35B130 0x1A35AC38 0x244
```

Workaround: Upgrade to Cisco IOS Release 12.2(31)SGA1 or later. (CSCsf09339)

- When you configure portchannels and portchannel members with non-autonegotiating speed and duplex settings, configuration syncs to the standby supervisor engine might fail, causing the switch to fallback to the RPR mode.

  Workarounds: None. (CSCsg62994)

- If you configure ISIS/IPv6 with the **passive-interface default** and **no passive-interface <interface>** commands, ISIS IIH advertisements is sent from such interfaces without the local IPv6 address, preventing the formation of adjacencies.

  Workaround: Remove **passive-interface** commands from the **router isis** configuration. (CSCei21664)

- GARP-based protocol packets leak through an STP block, potentially leading to a GARP storm in a redundant topology.

  Workaround: Use Hardware Control Plane Policing (CoPP) to police GARP packets. (CSCsg08775)

- Configuring an ACL on a port configured with the **switchport access vlan dynamic** command will restart the Catalyst 4500 series switch.

  This issue impacts Catalyst 4500 series switches running IOS releases including and earlier than 12.2(31)SGA and 12.2(25)EWA6.

  Workaround: None. (CSCsg03745)

- The HSRP Active-Router does not respond to ARP requests for the virtual IP (VIP) address. Issuing **clear arp** on the HSRP standby router does not resolve the problem. This problem may occur when the same HSRP VIP address exists on different HSRP groups on different routers.

  Workaround: Issue the **no standby redirects** command. (CSCsd80754)

- While upgrading the switch using the steps described in the ISSU process, issuing the **issu runversion** command causes the active supervisor engine to report a bulk sync failure as the standby supervisor engine boots up due to the mismatch command (MCL). The MCL errors are reported for PoE interfaces configured with the **power inline static max** command. The standby automatically resets and comes back in RPR mode.

  The is error occurs only with PoE interfaces when you configure **static max allowed inline power** on WS-X4506-GB-T line cards.

  Workaround: Remove the configuration lines reported in the MCL list from the running config on the active supervisor engine, and then rebooting the standby engine. After the standby supervisor engine is up and the switch reaches the STANDBY HOT state, reconfigure the original **power inline static max** command. (CSCse57813)

- When you remove the **radius-server source-ports 1645-1646** default command, the switch sends the RADIUS requests with the wrong source port, causing failed authentication attempts.

  Reloading the switch will solve the problem. Upon boot-up, **radius-server source-ports 1645-1646** is in the running-config and communication with the RADIUS server will resume

  Workaround: Ensure the **radius-server source-ports 1645-1646** command is configured. (CSCsh22161)

- Spurious memory accesses may occur when OSPF routing is configured and UDP traffic is flooded.

  Workaround: None. (CSCsd11631)

- When a switch port is disabled and enabled, the adjacent switch port may drop up to 20 packets.

  Workaround: None. (CSCsg02099)

- In a Catalyst 4500 series switch, ports on WS-X4418-GB may come up in half-duplex after the link is reset. This symptom is accompanied by logging duplex mismatch messages.

  This problem has been seen with connections between WS-X4418-GB module and the Catalyst 3550, Catalyst 3560, and Catalyst 3500xl series switches.

  Workaround: Issue the **shut/no shut** command on the WS-X4418-GB interface. (CSCsg21514)

- Occasionally, the link between a WS-X4548-GB-RJ45 and a WS-C3560-24PS running Cisco IOS Release 12.2(25)SEE might not come up after you reload the Catalyst 4500 series switch. This does not occur when the WS-C3560-24PS is reloaded.

  Workaround: Perform a **shut/no shut** on the interface. (CSCsd90837)

- QoS markings are not retained when using per-port per-VLAN QoS and IP Source Guard.

  Workaround: Disable and enable QoS. (CSCsg75348)

- The switch may reset after a PVLAN trunk port receives a high number of IGMP report messages.

  Workaround: Disable the PVLAN trunk port. (CSCsg46891)

- A switch configured in Rapid PVST spanning tree mode will not automatically recover an interface that was placed into ROOT_Inc state by ROOT guard.

  Workaround: Bounce any interface on the 4500 switch causing a spanning tree topology change. (CSCsc95631)

- A tftp client that attempts to transfer a file from an IOS device configured as a tftp server, and which is denied by an ACL, receives a result that depends on whether the file is being offered for download. This may allow a third party to enumerate which files are available for download.

  Workaround: Apply one of the following:

  1. Interface ACL - Configure and attach an access list to every active router interface configured for IP packet processing. After enabled, the tftp server in IOS listens by default on all interfaces enabled for IP processing. So, the access list needs to deny traffic to every IP address assigned to an active router interface.

  2. Control Plane Policing - Configure and apply a CoPP policy.

Note CoPP is only available on certain platforms and IOS release trains.

  3. Infrastructure ACLs (iACL) - Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and to block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as

well as a workaround for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for iACLs

4. Receive Access Lists (rACLs) - The rACLs protect a device from harmful traffic before the traffic can impact the route processor. rACLs are considered a network security best practice, and should be considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets . (CSCse04560)

Note The suggested workarounds are an "all or nothing" solution. While the tftp-server feature in IOS allows per-file ACLs to be attached to every file being offered for download, the suggested workarounds are global. They will either prevent or allow access to all files that are being shared. You should apply a workaround in addition to the existing per-file ACLs, instead of replacing them.

- Test and debug commands are not available in cryptographic images.

  Workaround: None. (CSCse61081)

- A Catalyst 4500 series switch running Cisco IOS Release 12.2(25)EWA6 might drop an ARP request. The switch cannot resolve the MAC address of connected devices.

  This problem is not seen with Cisco IOS Releases 12.2(25)EWA4 and 12.2(25)EWA5.

  Workaround: None. (CSCsf16422)

- When your DHCP address lease time is not updated on a switch configured with IP Source Guard, you cannot renew your DHCP IP addresses. Your non-DHCP traffic is dropped and the following error message is logged:

  ```
  %IP_SOURCE_GUARD-4-IP_SOURCE_GUARD_DENY_PACKET: IP Source Guard detects and drops
  illegal traffic
  ```

  Workaround: Disable and enable the affected switch ports. (CSCsd65833)

- When you configure a switch with an IEEE 802.1X Failed Authentication VLAN and IEEE 802.1X supplicants use tunneled EAP methods such as PEAP and EAP-TLS for authentication, the switch attempts to send an EAP Success message on the third consecutive failed authentication attempt rather than an EAP Failure message. This results in erratic supplicant and network behavior.

  Workaround: Either do not use tunneled EAP methods or disable the authentication failed VLAN. (CSCse71105)

- When the VTP configuration revision is higher than 0x7FFFFFFF (2147483647), the configuration revision displays in the output of the **show vtp status** command as a negative number.

  Workaround: Reset the VTP domain name for all switches in the domain. (CSCse40078)

- While upgrading the Catalyst 4500 series switch with ISSU, issuing the **issu runversion** command as the standby supervisor engine boots causes the active supervisor engine to report a bulk sync failure due to a mismatch command (MCL). The MCL errors are reported only for PoE interfaces on WS-X4506-GB-T line cards configured for inline power with the **power inline static max** command. The standby supervisor engine automatically resets and re-boots in RPR mode.

  Workarounds: Remove the configuration lines reported in the MCL list from the running config on the active supervisor engine. Then, reboot the standby supervisor engine. After the standby supervisor engine has booted and Catalyst 4500 series switch is in a STANDBY HOT state, reconfigure the original **power inline static max** command. (CSCse57813)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  (CSCsd75273)
- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  (CSCse52951)
- A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007.

(CSCsd85587)

Open Caveats in Cisco IOS Release 12.2(31)SGA

This section lists the open caveats in Cisco IOS Release 12.2(31)SGA:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

  ```
  Switch(config)# no monitor session n source cpu queue all rx
  Switch(config)# monitor session n source cpu queue <new_Queue_Name>
  ```

  (CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- When you do not save the running configuration on the active supervisor engine before a Stateful Switchover occurs due to the failure of the active supervisor engine, the following error message is observed:

  ```
  00:00:26: %PM-4-PORT_INCONSISTENT: Port Gi3/1 is inconsistent: IDB state down (set 
  00:00:02 ago), link: up (00:00:02 ago)
  ```

  Traffic loss is observed for about 500 ms.

  Workaround: Save your changes to the running configuration to avoid the error log and the loss of traffic during a Stateful Switchover.

- A bulk sync failure upon issuing the **switchport trunk encapsulation dot1q** command causes the standby supervisor engine to reload.

  Workaround: When this happens, the mismatched command list can be displayed on the active supervisor engine by issuing the **show issu config-sync failures mcl** command. The WS-X4418-GB module only supports the default dot1q encapsulation. The command mismatch can be fixed by removing the **switchport trunk encapsulation dot1q** subinterface command from each of the interfaces associated with the WS-X4418-GB module on the active supervisor engine and then rebooting the standby supervisor engine. Please verify that the above encapsulation command is removed in the running configuration on the active supervisor engine for the above interfaces. The standby supervisor engine will now boot up into SSO mode. Save the configuration on the active supervisor engine after making the above changes. (CSCse86228)

- An IP redirect may not be sent out if the outgoing interface on a Catalyst 4500 series switch is an IP unnumbered port.

  This could occur for these reasons:

  - A packet requires an IP redirect to an IP unnumbered outgoing port within 3 minutes of booting the Catalyst 4500 series switch.
  - This is also seen if the switch administrator issues the **shutdown** and **no shutdown** commands on an outgoing interface that has IP unnumbered enabled. The switch receives packets that require redirection and the destination MAC address is already in ARP table.

  Workarounds:

  - Do not inject packets that require IP redirect sent out to an IP unnumbered port within 3 minutes of booting the Catalyst 4500 series switch.
  - Configure the correct default gateway on the host side. (CSCse75660)

- After configuring the **bgp dampening route-map bgp_damp** command on an active supervisor engine in SSO mode, the following system logs are seen on the console of the standby supervisor engine:

  ```
  00:10:34: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum (20000). Dampening is OFF

  00:10:06: %BGP-5-DAMPENING_HIGH_MAX_PENALTY: Maximum penalty (32473) is more than
  allowed maximum 000). Dampening is OFF
  ```

  At this point, if you revert back to the **bgp dampening** command on the active supervisor engine, the new command is not synchronized with the standby supervisor engine.

  Workarounds: Issue the **no bgd dampening** command, then the **bgp dampening** command. (CSCse12485)

- While upgrading the Catalyst 4500 series switch with ISSU, issuing the **issu runversion** command as the standby supervisor engine boots causes the active supervisor engine to report a bulk sync failure due to a mismatch command (MCL). The MCL errors are reported only for PoE interfaces on WS-X4506-GB-T line cards configured for inline power with the **power inline static max** command. The standby supervisor engine automatically resets and re-boots in RPR mode.

  Workarounds: Remove the configuration lines reported in the MCL list from the running config on the active supervisor engine. Then, reboot the standby supervisor engine. After the standby supervisor engine has booted and Catalyst 4500 series switch is in a STANDBY HOT state, reconfigure the original **power inline static max** command. (CSCse57813)

- On redundant systems working in SSO mode, a line-by-line (LBL) configuration sync error occurs between the active and standby supervisor engines when the administrator defaults the configuration for an interface configured with port security. The error causes the standby supervisor engine to reset if the config sync policy for the LBL errors is enforced using the **issu config-sync policy lbl prc** command.

  This problem only occurs if the interface configured with port security is in violation restrict mode (through the **switchport port-security violation restrict** command). Moreover, the interface must be in security violation state when you apply the **default interface** command.

  Workarounds: Bring the interface into shutdown mode before you apply the **default interface** command. (CSCsf30157)

- After an ISSU is performed on a WS-X4448-GB-SFP linecard running Cisco IOS Release 12.2(31)SGA, the output of the **show inventory** command does not display some of the 1000Base SFPs .

  Workarounds: None. (CSCse43697)

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SGA

This section lists the resolved caveats in Release 12.2(31)SGA:

- When running Cisco IOS Release 12.2(25)EWA6 on a Catalyst 4948 series switch, or the Catalyst 4013+TS supervisor engine and the 4306-GB-T linecard, the following problems may be seen on RJ45 ports only:

  - When sending packets of size greater than 6656 bytes, the ports cannot sustain the linerate when operating at 1Gbps. However, they can sustain the linerate for packet sizes less than or equal to 6656 bytes when operating at 1Gbps.
  - Occasionally, the TxQueue's associated with the RJ45 ports may get stuck when packets greater than 6656 bytes and the port is operating in either 10Mbps or 100Mbps or 1Gbps. You would see messages like the following:

    ```
    Aug  1 04:46:01 CDT: %C4K_HWPORTMAN-4-BLOCKEDTXQUEUE: Blocked transmit queue
    HwTxQId1 on Switch Phyport Gi1/35, count=1784
    Aug  1 04:46:12 CDT: Current Freelist count 5629. Fell below threshold 601 times
    consecutively
    Aug  1 04:46:42 CDT: Current Freelist count 5629. Fell below threshold 1202 times
    consecutively
    ```

  Workaround: Upgrade to Cisco IOS Release 12.2(25)EWA8, 12.2(31)SGA, or 12.2(37)SG. (CSCse29295)

- When the standby supervisor engine is not synced with the active supervisor engine that is configured for ISSU during an IOS upgrade of IOS, the following messages appear:

  ```
  %IDBINDEX_SYNC-3-IPC_ERR:

  ifindex_sync_standby_port : no such port.
  -Process= "rf task", ipl= 0, pid= 54

  -Traceback=
  ```

  Workaround: None. (CSCse31818)

- A Catalyst 4500 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)

- Symptoms: A router may crash if it receives a packet with a specific crafted IP option.

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved.

  (CSCek26492)

- The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  There are workarounds available to mitigate the effects of the vulnerability.

  (CSCek37177)

- Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

(CSCsd58381)

- A Cisco router may drop a TCP connection to a remote router.

  When an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than the remote router can handle, the router might advertise a zero window. So, when the router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be send to the remote router, the Cisco router may drop the TCP connection.

  Workaround: Increase the window size on both ends. On the Cisco router, enter the **ip tcp window-size** command. When you use a Telnet connection, reduce the **screen-length** argument in the **terminal length** command to 20 or 30 lines. (CSCsc39357)

Open Caveats in Cisco IOS Release 12.2(31)SG3

This section lists the open caveats in Cisco IOS Release 12.2(31)SG3:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

- A Catalyst 4500 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- When you do not save the running configuration on the active supervisor engine before a Stateful Switchover occurs due to the failure of the active supervisor engine, the following error message is observed:

  ```
  00:00:26: %PM-4-PORT_INCONSISTENT: Port Gi3/1 is inconsistent: IDB state down (set
  00:00:02 ago), link: up (00:00:02 ago)
  ```

  Traffic loss is observed for about 500 ms.

  Workaround: Save your changes to the running configuration to avoid the error log and the loss of traffic during a Stateful Switchover.

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SG3

This section lists the resolved caveats in Release 12.2(31)SG3:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

- A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited is affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  (CSCse56501)

- A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  (CSCsi01470)

- Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  (CSCsd95616)

Open Caveats in Cisco IOS Release 12.2(31)SG2

This section lists the open caveats in Cisco IOS Release 12.2(31)SG2:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

```
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)
- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

```
%HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.
- A Catalyst 4500 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)
- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

  Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

  (CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- When you do not save the running configuration on the active supervisor engine before a Stateful Switchover occurs due to the failure of the active supervisor engine, the following error message is observed:

  ```
  00:00:26: %PM-4-PORT_INCONSISTENT: Port Gi3/1 is inconsistent: IDB state down (set 
  00:00:02 ago), link: up (00:00:02 ago)
  ```

  Traffic loss is observed for about 500 ms.

  Workaround: Save your changes to the running configuration to avoid the error log and the loss of traffic during a Stateful Switchover.

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SG2

This section lists the resolved caveats in Release 12.2(31)SG2:

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can cause a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  (CSCin95836)

- A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

  (CSCsi01470)

Open Caveats in Cisco IOS Release 12.2(31)SG1

This section lists the open caveats in Cisco IOS Release 12.2(31)SG1:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be “down” after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

- A Catalyst 4500 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

  This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet

QueueID	Old QueueName	New QueueName
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  – Use a different copy protocol.

  – Set a longer ssh timout.

  (CSCsc94317)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be “down” after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- When you do not save the running configuration on the active supervisor engine before a Stateful Switchover occurs due to the failure of the active supervisor engine, the following error message is observed:

```
00:00:26: %PM-4-PORT_INCONSISTENT: Port Gi3/1 is inconsistent: IDB state down (set
00:00:02 ago), link: up (00:00:02 ago)
```

  Traffic loss is observed for about 500 ms.

  Workaround: Save your changes to the running configuration to avoid the error log and the loss of traffic during a Stateful Switchover.

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

Resolved Caveats in Cisco IOS Release 12.2(31)SG1

This section lists the resolved caveats in Release 12.2(31)SG1:

- Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Because CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

  Workaround: Disable on interfaces where CDP is not necessary. (CSCse85200)

- Some (or all) CDP neighbors are invisible.

  It only happens on releases that include the fix for CSCse85200.

  When turning on "debug cdp even," the following message appears:

  ```
  CDP-EV: Received item (type : 9) with invalid length 4
  ```

  Workaround: None. (CSCsf07847)

Open Caveats in Cisco IOS Release 12.2(31)SG

This section lists the open caveats in Cisco IOS Release 12.2(31)SG:

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  clearwater#sh policy-map int
    FastEthernet3/2

     Service-policy output: p1
  ```

```
    Class-map: c1 (match-all)
      0 packets<--------It stays at '0' despite of traffic being received
      Match: access-group name fnacl21
      police: Per-interface
        Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

- A Catalyst 4500 series switch clears the mac-add-table notif counters when the feature is disabled.

  Workaround: Re-connect. (CSCsc31540)

- After upgrading to Cisco IOS 12.2(31)SG and later releases, some CPU queues configured as SPAN sources and saved in the startup configuration file do not function as they did in the older software release.

This only impacts a switch that has any of the following queues are configured as SPAN source in releases prior to 12.2(31)SG and saved to startup-config. The SPAN destination would not get the same traffic after upgrading to 12.2(31)SG.

QueueID	Old QueueName	New QueueName
5	control-packet	control-packet
6	rpf-failure	control-packet
7	adj-same-if	control-packet
8	<unused queue>	control-packet
11	<unused queue>	adj-same-if
13	acl input log	rfp-failure
14	acl input forward	acl input log

Workaround: After upgrading to 12.2(31)SG and later releases, remove the old SPAN source configuration and reconfigure with the new queue names/IDs. For example:

```
Switch(config)# no monitor session n source cpu queue all rx
Switch(config)# monitor session n source cpu queue <new_Queue_Name>
```

(CSCsc94802)

- If you initiate a scp copy from the console and it is delayed long enough to cause a timeout, the console is disconnected.

  Workarounds:

  - Use a different copy protocol.
  - Set a longer ssh timout.

  (CSCsc94317)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- To enable IP CEF if it is disabled by hardware exhaustion, use the **ip cef distributed** command.

  Workaround: None. (CSCsc11726)

- When you do not save the running configuration on the active supervisor engine before a Stateful Switchover occurs due to the failure of the active supervisor engine, the following error message is observed:

  ```
  00:00:26: %PM-4-PORT_INCONSISTENT: Port Gi3/1 is inconsistent: IDB state down (set
  00:00:02 ago), link: up (00:00:02 ago)
  ```

  Traffic loss is observed for about 500 ms.

  Workaround: Save your changes to the running configuration to avoid the error log and the loss of traffic during a Stateful Switchover.

- The RADIUS attribute 32 is not being sent to the RADIUS server for Cisco IOS Release 12.2(31)SG and beyond.

  Workaround: Downgrade to Cisco IOS Release 12.2(25)EWA10, if feasible. (CSCsi22041)

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Resolved Caveats in Cisco IOS Release 12.2(31)SG

This section lists the resolved caveats in Release 12.2(31)SG:

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- In redundant systems in SSO mode, when one or more ports belong to port-channel and you issue the sequence of commands **shut** and **no shut** quickly on a port-channel interface on the active supervisor engine, all physical ports associated with the port-channel on the standby supervisor engine remain administratively shutdown. So, the **no shut** command does not get synced correctly on the standby supervisor engine. After issuing the **shut** command, if you wait 30-60 seconds before issuing a **no shut** command, you will not see the problem.

  Workaround: Re-issue the **shut** and **no shut** commands on the ports. (CSCsb16809)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis (with dual supervisor engines operating in SSO mode) during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby.
  ```

Workaround: Reset the standby supervisor with the **redundancy reload peer** command, which synchronizes the standby supervisor engine configuration with that of the active supervisor engine

- Under rare conditions, when the active supervisor engine is running Cisco IOS 12.2(25r)EW and the standby supervisor engine is running Cisco IOS 12.2(31r)SG ROMMON, traffic may take slightly longer (less than 2 seconds) to resume switching on a WS-X4516-10GE supervisor engine after the SSO switchover.

  Workaround: Upgrade the ROMMON of both WS-4516-10GE supervisor engines with ROMMON version 12.2(31r)SG .

- Symptoms: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

  Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

  - VTP Version field DoS
  - Integer Wrap in VTP revision
  - Buffer Overflow in VTP VLAN name

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759—VTP version field DoS
  - CSCse40078/CSCse47765—Integer Wrap in VTP revision
  - CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

  (CCSCsd34759)

- Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  (CSCsd40334)

Open Caveats in Cisco IOS Release 12.2(25)SG4

This section lists the open caveats in Cisco IOS Release 12.2(25)SG4:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

  ```
  clearwater#sh policy-map int
    FastEthernet3/2

     Service-policy output: p1

       Class-map: c1 (match-all)
         0 packets<--------It stays at '0' despite of traffic being received
         Match: access-group name fnacl21
         police: Per-interface
           Conform: 9426560 bytes Exceed: 16573440 bytes
  ```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- In redundant systems in SSO mode, when one or more ports belong to port-channel and you issue the sequence of commands **shut** and **no shut** quickly on a port-channel interface on the active supervisor engine, all physical ports associated with the port-channel on the standby supervisor engine remain administratively shutdown. So, the **no shut** command does not get synced correctly on the standby supervisor engine. After issuing the **shut** command, if you wait 30-60 seconds before issuing a **no shut** command, you will not see the problem.

  Workaround: Re-issue the **shut** and **no shut** commands on the ports. (CSCsb16809)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Resolved Caveats in Cisco IOS Release 12.2(25)SG4

This section lists the resolved caveats in Release 12.2(25)SG4:

- In Cisco IOS Release 12.2(33)SXH or 12.2(18)SXF10, the output of the **show pagp neighbor** command may truncate the neighbor device name and port name fields by 1 character. This is a display issue and has no functional impact on the PAGP protocol.

  Workaround: None. If you want to determine a partner's correct information, use the **show cdp neighbor** command.

  (CSCsj81502)

Open Caveats in Cisco IOS Release 12.2(25)SG3

This section lists the open caveats in Cisco IOS Release 12.2(25)SG3:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

  ```
  000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
  config-changed command to standby
  ```

```
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- In redundant systems in SSO mode, when one or more ports belong to port-channel and you issue the sequence of commands **shut** and **no shut** quickly on a port-channel interface on the active supervisor engine, all physical ports associated with the port-channel on the standby supervisor engine remain administratively shutdown. So, the **no shut** command does not get synced correctly on the standby supervisor engine. After issuing the **shut** command, if you wait 30-60 seconds before issuing a **no shut** command, you will not see the problem.

  Workaround: Re-issue the **shut** and **no shut** commands on the ports. (CSCsb16809)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate is generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Resolved Caveats in Cisco IOS Release 12.2(25)SG3

This section lists the resolved caveats in Release 12.2(25)SG3:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

- A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited is affected.

  Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

  (CSCse56501)

Open Caveats in Cisco IOS Release 12.2(25)SG2

This section lists the open caveats in Cisco IOS Release 12.2(25)SG2:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync 
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1
```

```
Class-map: c1 (match-all)
  0 packets<--------It stays at '0' despite of traffic being received
  Match: access-group name fnacl21
  police: Per-interface
    Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- In redundant systems in SSO mode, when one or more ports belong to port-channel and you issue the sequence of commands **shut** and **no shut** quickly on a port-channel interface on the active supervisor engine, all physical ports associated with the port-channel on the standby supervisor engine remain administratively shutdown. So, the **no shut** command does not get synced correctly on the standby supervisor engine. After issuing the **shut** command, if you wait 30-60 seconds before issuing a **no shut** command, you will not see the problem.

  Workaround: Re-issue the **shut** and **no shut** commands on the ports. (CSCsb16809)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

- In software releases 12.2(25)EWA10, 12.2(31)SGA2 and 12.2(31)SGA3, PoE Health Monitoring Diagnostic software introduced via CSCsf26804 *incorrectly* reports PoE errors for module WS-X4548-GB-RJ45V, hardware revision 4.0. (Use the **show module** command to see the hardware revision of module.) The software reloads the PoE module continuously, and the module will not operate.

  WS-X4548-GB-RJ45V with hardware revision 4.0 is NOT impacted by the problem reported in CSCsf26804 hence PoE health Monitor checks are not applicable to the module.

  Workaround: None.

  This caveat is fixed in 12.2(25)EWA11 and 12.2(31)SGA4 software releases.

  Release 12.2(37)SG is other recommended software release. 12.2(37)SG does not have the fix for CSCsf26804 and hence does not run into CSCsk85158.

  A linecard replacement is *not* needed. *Do not* RMA the module. (CSCsk85158)

Resolved Caveats in Cisco IOS Release 12.2(25)SG2

This section lists the resolved caveats in Release 12.2(25)SG2:

- Cisco IOS Software has been enhanced with the introduction of additional software checks to signal improper use of data structures.

  This feature has been introduced in select Cisco IOS Software releases published after April 5, 2007.

  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp:

  ```
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

Workaround: Gather the output from the **show tech-support** command and open a service request with the Technical Assistance Center (TAC) or designated support organization. (CSCsj44081)

- Cisco IOS and Cisco IOS XR contain a vulnerability when processing specially crafted IPv6 packets with a Type 0 Routing Header present. Exploitation of this vulnerability can lead to information leakage on affected Cisco IOS and Cisco IOS XR devices, and may also cause a crash of the affected Cisco IOS device. Successful exploitation on an affected device running Cisco IOS XR will not cause a crash of the device itself, but may cause a crash of the IPv6 subsystem.

  Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  (CSCef77013)

- The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can cause a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  (CSCin95836)

- CSCsi01470

  A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

Open Caveats in Cisco IOS Release 12.2(25)SG1

This section lists the open caveats in Cisco IOS Release 12.2(25)SG1:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)

- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)

- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)

- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)

- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2
```

```
Service-policy output: p1

  Class-map: c1 (match-all)
    0 packets<--------It stays at '0' despite of traffic being received
    Match: access-group name fnacl21
    police: Per-interface
      Conform: 9426560 bytes Exceed: 16573440 bytes
```

Workaround: Verify that the MAC addresses being transmitted through the system are learned.

(CSCef01798)

- After an SSO switchover, you may receive a "PM-4-PORT_INCONSISTENT" error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

  Workaround: None. (CSCeg48586)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- Occasionally, on redundant systems in SSO mode, applying the **apply cisco-phone $AVID vlan** *$VVID vlan* macro command to an interface connected to an IP phone may render the interface in the wrong state relative to the standby supervisor engine. This causes the SVI to be "down" after the switchover.

  Workaround: If the SVIs associated with the physical interface are down after the switchover, issue **shutdown** and **no shutdown** commands on the physical interface to bring up the SVIs. (CSCsb02308)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- In redundant systems in SSO mode, when one or more ports belong to port-channel and you issue the sequence of commands **shut** and **no shut** quickly on a port-channel interface on the active supervisor engine, all physical ports associated with the port-channel on the standby supervisor engine remain administratively shutdown. So, the **no shut** command does not get synced correctly on the standby supervisor engine. After issuing the **shut** command, if you wait 30-60 seconds before issuing a **no shut** command, you will not see the problem.

  Workaround: Re-issue the **shut** and **no shut** commands on the ports. (CSCsb16809)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

  Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

Resolved Caveats in Cisco IOS Release 12.2(25)SG1

This section lists the resolved caveats in Release 12.2(25)SG1:

- Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Because CDP is a layer-2 protocol, this issue can only be triggered by systems that are residing on the same network segment.

  Workaround: Disable on interfaces where CDP is not necessary. (CSCse85200)

- Some (or all) CDP neighbors are invisible.

  It only happens on releases that include the fix for CSCse85200.

  When turning on "debug cdp even," the following message appears:

  ```
  CDP-EV: Received item (type : 9) with invalid length 4
  ```

  Workaround: None. (CSCsf07847)

- Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  (CSCsd40334)

- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  (CSCsd75273)
- Cisco Catalyst 6000, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  (CSCse52951)

Open Caveats in Cisco IOS Release 12.2(25)SG

This section lists the open caveats in Cisco IOS Release 12.2(25)SG:

- Changes to console speed are not updated in ROMMON. If a system is reloaded, you will not see a prompt until Cisco IOS software re-starts.

  Workaround: None. (CSCee65294)
- On a system reload, some of the QoS policies that had previously loaded into the hardware may fail to load due to limited space.

  Workaround: Disable QoS with the **no qos** command, and then re-enable QoS with the **qos global** command. (CSCee52449)
- Insertion of unsupported SFPs (small form-factor pluggable optics) into a WS-X4448-GB-SFP or WS-X4448-GB-LX module and can cause undetected communication failures between the supervisor engine and the corresponding module. Subsequent insertion or removal of SFPs from the module is not recognized by the system. This activity can be observed on a Catalyst 4500 series switch using Release 12.1(12c)EW1 or later releases.

  Workaround: Reset the module with the **hw-module module reset** command. (CSCee05078)
- When in SML (Smart Missing Link) mode, some converter boxes (CPE devices) send pulses on the optical side when the Ethernet cable is removed. These converter boxes should also have an LT (Link Test) mode in which the optical side stays active regardless of the connection status and an ML (Missing Link) mode in which the optical side always stays shut down if the Ethernet cable is disconnected. If a WS-X4148-FE-BD-LC port is connected to a converter box in SML mode, and the Ethernet cable on the box is removed, the port will eventually go into errdisable mode because of the continuous connecting and disconnecting (flapping) of the link.

  Workaround: Configure the convertor box (CPE device) to operate in either LT (Link Test) or ML (Missing Link) mode. (CSCed28409)
- When PBR is configured on a Supervisor Engine III or Supervisor Engine IV, hardware-switched PBR packets update the access list or route map statistics improperly.

  Workaround: None. (CSCdz10171)

- A CompactFlash module formatted on either Supervisor Engine III or Supervisor Engine IV that uses Cisco IOS Releases 12.1(14)E, 12.1(19)E, or 12.1(13)EW will not work on Supervisor Engine II-Plus. The CompactFlash module will continue to work on the other supervisor engines.

  Workaround: Format the CompactFlash module on any Catalyst 4500 series switch supervisor engine that uses Release 12.1(19)EW (or later). (CSCeb36355)

- When you enter the **access-list N permit host hostname** command on a redundant chassis operating in SSO mode, you might observe the following syslog messages. The command is not synchronized with the redundant supervisor engine, and keepalive warnings appear.

```
000099: Jul  9 01:22:36.478 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000100: Jul  9 01:22:46.534 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000101: Jul  9 01:22:56.566 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000102: Jul  9 01:23:06.598 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000103: Jul  9 01:23:16.642 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000104: Jul  9 01:23:26.682 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000105: Jul  9 01:23:36.721 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000106: Jul  9 01:23:46.777 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
000107: Jul  9 01:23:56.793 PDT: %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync
config-changed command to standby
```

  Workaround: When using the **access-list N permit host hostname** command, specify the IP address of the host rather than the hostname (CSCef67489)

- In a hierarchical policer configuration with parent as the aggregate policer and child as the microflow policer, child microflow policer-matched packets report only the packets that are in the profile (they match the policing rate). Packets that exceed the policing rate are not reported in the class-map packet match statistics.

  Workaround: None. (CSCef88634)

- In rare instances, when you are using MAC ACL-based policers, the packet match counters in **show policy-map interface fa6/1** do not show the packets being matched:

```
clearwater#sh policy-map int
  FastEthernet3/2

   Service-policy output: p1

     Class-map: c1 (match-all)
       0 packets<--------It stays at '0' despite of traffic being received
       Match: access-group name fnacl21
       police: Per-interface
         Conform: 9426560 bytes Exceed: 16573440 bytes
```

  Workaround: Verify that the MAC addresses being transmitted through the system are learned.

  (CSCef01798)

- After an SSO switchover, you may receive a “PM-4-PORT_INCONSISTENT” error message on the switch console if you enter the **shutdown** command, then the **no shutdown** command on the port that is in UDLD error-disable state. This does not impact the switch; the port remains in UDLD error-disable state. Re-entering the **shutdown** command, then the **no shutdown** command on the same port will ensure that the error message does not re-appear.

Workaround: None. (CSCeg48586)

- When changing the access VLAN ID on a sticky port configured with IPSG and voice VLAN, the secure MAC address counter on this port might become negative. This does not impact the system.

  Workaround: Avoid enabling IPSG on sticky ports that are configured with VVID. (CSCeg31712)

- QoS policing will fail if you configure more than 1000 policers on a trunk port and you remove some of the VLANs from the trunk port.

  Workaround: Use less than 1000 policers.(CSCsa57218)

- On redundant systems in SSO mode, when you issue the **cisco-phone $AVID $VVID** macro command to an interface connected to an IP phone, you might leave the interface on the standby supervisor engine in a wrong state. This would cause the data SVI or the voice SVI to be down after the switchover.

  Workaround: If the data or video SVIs associated to the physical interface (connected to the IP phone) are down after the switchover, issue the **shutdown** and **no shutdown** commands on the physical interface to restore the correct (up) state for all the SVIs. (CSCsb02308)

- When Fast Hellos is configured on an interface thru the command **ip ospf dead-interval minimal hello-multiplier**, the dead-interval can be changed to exceed 1 second with the **ip ospf dead-interval** keyword. However, the running configuration still displays the **ip ospf dead-interval minimal hello-multiplier** command instead of the **ip ospf dead-interval** command.

  Workaround: To change the dead-interval when Fast Hellos is enabled, first disable Fast Hellos and then configure the new dead-interval. (CSCsa86676)

- In redundant systems in SSO mode, when one or more ports belong to port-channel and you issue the sequence of commands **shut** and **no shut** quickly on a port-channel interface on the active supervisor engine, all physical ports associated with the port-channel on the standby supervisor engine remain administratively shutdown. So, the **no shut** command does not get synced correctly on the standby supervisor engine. After issuing the **shut** command, if you wait 30-60 seconds before issuing a **no shut** command, you will not see the problem.

  Workaround: Re-issue the **shut** and **no shut** commands on the ports. (CSCsb16809)

- When you issue the **ip http secure-server** command (or if the system reads it from the startup configuration), the device will check for the existence of a persistent self-signed certificate during boot up.

  - If such a certificate does not exist and the device's hostname and default_domain have been set, then a persistent self-signed certificate will be generated.
  - If such a certificate exists, the FQDN in the certificate is compared with the current device's hostname and default_domain. If either of these differs from the FQDN in the certificate, then the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing keypair is used in the new certificate.

  On a switch that support redundancy, the generation of the self-signed certificate is performed independently on the active and the standby supervisor engines. So, the certificates differ. After switchover, the HTTP client that holds the old certificate can not connect to the HTTPS server.

  Workaround: Re-connect. (CSCsb11964)

- If you modify policers with a large number of VLAN tags on a Catalyst 4507R or a 4510R chassis with dual supervisor engines operating in SSO mode during substantial CPU bound traffic, the following message appears:

  ```
  %HA_CONFIG_SYNC-3-LBL_CFGSYNC: Unable to sync config-changed command to standby
  ```

Workaround: Reset the standby supervisor by entering the **redundancy reload peer** command. This command synchronizes the standby supervisor configuration with the active supervisor.

Resolved Caveats in Cisco IOS Release 12.2(25)SG

This section lists the resolved caveats in Release 12.2(25)SG:

- After moving to a non-redundant chassis, a supervisor engine that was previously configured in SSO mode will not be able to configure router ports or port-channel.

  Workarounds:

  1. Before moving the supervisor engine to a non-redundancy-capable chassis, change the mode to RPR.

  2. Enter the **write memory** command and reload the switch from the non-redundancy chassis. (CSCef67677)

- If you enter the **default interface** command at the interface level, then at the interface configuration level, any command you enter after a **macro apply** command is not accepted. The Help(?) feature will show only two options: exit and help.

  Workaround: Exit, then re-enter interface configuration mode. All commands will be accepted, even after you enter the **macro apply** command. (CSCsa44632)

- Entering the **no ip flow ingress** command will not turn off the collection of switched IP flows.

  Workaround: Use the **no ip flow ingress** command in conjunction with the **no ip flow ingress layer2-switched** command. (CSCsa67042)

- Modifying a policer may not work if you configure more than 800 policers.

  Workaround: Remove, reconfigure and reinstall policers, or, use less than 800 policers. (CSCsa66422)

- When you apply smartport macros (like “cisco-switch” and “cisco-desktop”) on a WS-C457R or a WS-C4510R are using CNA, the active supervisor goes through an unexpected switchover.

  Workaround: No workarounds are available. Enter the **default interface** command and apply smartport macros such as “cisco-switch” and “cisco-desktop”. (CSCsb59783)

- When you enter the **default interface** command on a WS-C457R or a WS-C4510R are using HTTP, the active supervisor goes through an unexpected switchover.

  Workaround: No workarounds are available. Enter the **default interface** command and apply smartport macros such as “cisco-switch” and “cisco-desktop”. (CSCei76082)

- Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  (CSCei61732)

- Symptoms: The VTP feature in certain versions of Cisco IOS software is vulnerable to a locally-exploitable buffer overflow condition and potential execution of arbitrary code. If a VTP summary advertisement is received with a Type-Length-Value (TLV) containing a VLAN name greater than 100 characters, the receiving switch will reset with an Unassigned Exception error.

  Conditions: The packets must be received on a trunk enabled port, with a matching domain name and a matching VTP domain password (if configured).

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759—VTP version field DoS
- CSCse40078/CSCse47765—Integer Wrap in VTP revision
- CSCsd34855/CSCei54611—Buffer Overflow in VTP VLAN name

(CSCei54611)

Troubleshooting

These sections provide troubleshooting guidelines for the Catalyst 4000 family running IOS supervisor engines:

Netbooting from the ROMMON

Netbooting using a boot loader image is not supported. Instead, use one of the following options to boot an image:

1. Boot from a CompactFlash card by entering the following command:

```
rommon 1> boot slot0:<bootable_image>
```

2. Use ROMMON TFTP boot.

   The ROMMON TFTP boot is very similar to the BOOTLDR TFTP boot, except that:

   - the BOOTLDR variable should *not* be set
   - the TFTP server must be accessible from the Ethernet management port on the supervisor engine.

   To boot from ROMMON, perform the following tasks while in ROMMON mode:

a. Ensure that the Ethernet management port on the supervisor engine is physically connected to the network.

b. Verify that bootloader environment is not set by entering the **unset bootldr** command.

c. Set IP address of the Ethernet management port on the supervisor engine by entering the following command: **set interface fa1** *ip_address*> <*ip_mask*

   For example, to set the supervisor engine Ethernet port with an IP address 172.16.1.5 and IP mask 255.255.255.0, enter the following command:

```
rommon 2> set interface fa1 172.16.1.5 255.255.255.0
```

d. Set default gateway for the Ethernet management port on the supervisor engine by entering the following command: **set ip route default** *gateway_ip_address*. The default gateway should be directly connected to the supervisor engine Ethernet management port subnet.

e. Ping the TFTP server to ensure that there is connectivity to the server from the Ethernet management port on the supervisor engine by entering the following command: **ping** <*tftp_server_ip_address*>.

f. Once the ping is successful, boot the image from the TFTP server by entering the following command: **boot tftp://***tftp_server_ip_address*>**/**<*image_path_and_file_name*

For example, to boot the image name cat4000-is-mz.160 located on the TFTP server 172.16.1.8, enter the following command:

```
rommon 3> boot tftp://172.16.1.8/tftpboot/cat4000-is-mz
```

Troubleshooting at the System Level

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- Ensure that you do not mix the serial and Ethernet cables plugged into the supervisor engine. The Fast Ethernet port (10/100 MGT) on the supervisor engine is inoperative in all Catalyst 4500 Cisco IOS releases. An Ethernet cable plugged into the Fast Ethernet port is active only in ROMMON mode.

Troubleshooting Modules

This section contains troubleshooting guidelines for modules:

- When you hot insert a module into a chassis, always use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 4500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, ensure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the port set to autonegotiate will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

Troubleshooting MIBs

For general information on MIBs, RMON groups, and traps, refer to the Cisco public MIB directory (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml). For information on the specific MIBs supported by the Catalyst 4500 series switches, refer to the Catalyst 4000 MIB Support List located at ftp://ftp.cisco.com/pub/mibs/supportlists/cat4000/cat4000-supportlist.html.

Related Documentation

Although their Release Notes are unique, the 4 platforms (Catalyst 4500, Catalyst 4900, Catalyst ME 4900, and Catalyst 4900M) use the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide*. Refer to the following home pages for additional information:

- Catalyst 4500 Series Switch Documentation Home

  http://www.cisco.com/go/cat4500/docs

- Catalyst 4900 Series Switch Documentation Home

  http://www.cisco.com/go/cat4900/docs

- Cisco ME 4900 Series Ethernet Switches Documentation Home

  http://www.cisco.com/en/US/products/ps7009/tsd_products_support_series_home.html

Hardware Documents

Installation guides and notes including specifications and relevant safety information are available at the following URLs:

- *Catalyst 4500 Series Switches Installation Guide*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/installation/guide/78-14409-08/4500inst.html

- *Catalyst 4500 E-series Switches Installation Guide*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries.html

- For information about individual switching modules and supervisors, refer to the *Catalyst 4500 Series Module Installation Guide* at:

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html

- *Regulatory Compliance and Safety Information for the Catalyst 4500 Series Switches*

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/regulatory/compliance/78_13233.html

- Installation notes for specific supervisor engines or for accessory hardware are available at:

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_installation_guides_list.html

- Catalyst 4900 and 4900M hardware installation information is available at:

  http://www.cisco.com/en/US/products/ps6021/prod_installation_guides_list.html

- Cisco ME 4900 Series Ethernet Switches installation information is available at:

  http://www.cisco.com/en/US/products/ps7009/prod_installation_guides_list.html

Software Documentation

Software release notes, configuration guides, command references, and system message guides are available at the following URLs:

- Catalyst 4500 release notes are available at:

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_release_notes_list.html

- Catalyst 4900 release notes are available at:

  http://www.cisco.com/en/US/products/ps6021/prod_release_notes_list.html
- Cisco ME4900 4900 Series Ethernet Switch release notes are available at:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_11511.html

Software documents for the Catalyst 4500 Classic, Catalyst 4500 E-Series, Catalyst 4900, and Cisco ME 4900 Series Ethernet Switches are available at the following URLs:

- *Catalyst 4500 Series Software Configuration Guide*

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- *Catalyst 4500 Series Software Command Reference*

  http://www.cisco.com/en/US/products/hw/switches/ps4324/prod_command_reference_list.html
- *Catalyst 4500 Series Software System Message Guide*

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_system_message_guides_list.html

Cisco IOS Documentation

Platform-independent Cisco IOS documentation may also apply to the Catalyst 4500 and 4900 switches. These documents are available at the following URLs:

- Cisco IOS configuration guides, Release 12.x

  http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html
- Cisco IOS command references, Release 12.x

  http://www.cisco.com/en/US/products/ps6350/prod_command_reference_list.html

  You can also use the Command Lookup Tool at:

  http://tools.cisco.com/Support/CLILookup/cltSearchAction.do
- Cisco IOS system messages, version 12.x

  http://www.cisco.com/en/US/products/ps6350/products_system_message_guides_list.html

  You can also use the Error Message Decoder tool at:

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
- For information about MIBs, refer to:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.2(54)SG