Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Releases 15.2(2)Ex

Current release

IOS 15.2(2)E10—May 31, 2019
Prior releases
IOS 15.2(2)E9—September 12, 2018, IOS 15.2(2)E8—January 31, 2018, IOS 15.2(2)E7—July 10, 2017, IOS 15.2(2)E5a—October 14, 2016, IOS 15.2(2)E5—June 07, 2016, IOS 15.2(2)E4, IOS 15.2(2)E3, IOS 15.2(2)E2, IOS 15.2(2)E1, IOS 15.2(2)E0—June 27, 2016

These release notes describe the features, modifications, and caveats for Cisco IOS Release 15.2(2)Ex on the Catalyst 4500 series switch.

Support for Cisco IOS Software Release 15.2(2)Ex follows the standard Cisco Systems® support policy, available at

http://www.cisco.com/en/US/products/products_end-of-life_policy.html

For more information on the Catalyst 4500 Series Switches, visit:

http://www.cisco.com//en/US/products/hw/switches/ps4324/index.html

Note Although their Release Notes are unique, the platforms Catalyst 4900M/Catalyst 4948E/Catalyst 4948E-F and Catalyst 4500 leverage the same *Software Configuration Guide*, *Command Reference Guide*, and *System Message Guide.*

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

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.

The IP Base image supports Open Shortest Path First (OSPF) for Routed Access, Enhanced Interior Gateway Routing Protocol (EIGRP) "limited" Stub Routing, Nonstop Forwarding/Stateful Switchover (NSF/SSO), and RIPv1/v2. The IP Base image does not support enhanced routing features such as BGP, Intermediate System-to-Intermediate System (IS-IS), Full OSPF, Full Enhanced Interior Gateway Routing Protocol (EIGRP) & Virtual Routing Forwarding (VRF-lite).

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 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.

Starting with Cisco IOS Release 15.0(2)SG, on the Catalyst 4500 Series Switch, support for NEAT feature has been extended from IP Base to LAN Base and support for HSRP v2 IPV6 has been extended from Enterprise Services to IP Base.

Starting with Cisco IOS Release 15.2(1)E, OSPF Routed Access in IP Base support rose to 1000 routes.

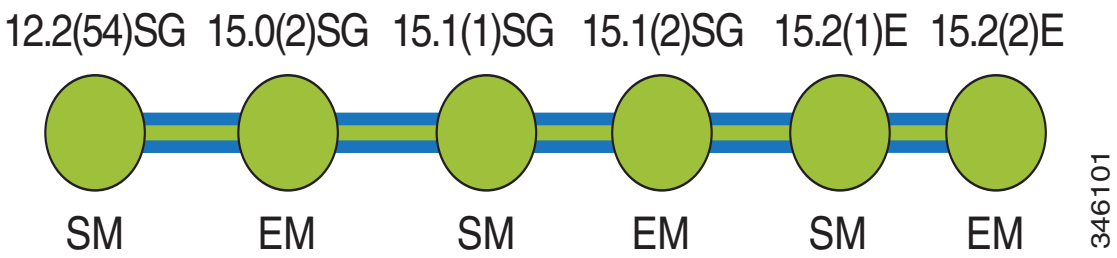
Cisco Classic IOS Release Strategy

Customers using Supervisor Engine 6-E or 6L-E with Catalyst 4500 Series Switches who need the latest hardware and software features should migrate to Cisco IOS Release 15.2(2)E.

The Catalyst 4500 Series Switch has three extended maintenance (EM) trains: 15.2(2)Ex, 15.1(2)SGx, and 15.0(2)SGx. Cisco IOS Release 12.2(54)SG, 15.1(1)SG, and 15.2(1)E are standard maintenance releases.

Figure 1 displays the maintenance trains for the Catalyst 4500 series switch.

Figure 1 Software Release Strategy for the Catalyst 4500 Series Switch



Support

Support for Cisco IOS Software Release 15.2(2)E 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

Table 1 lists the hardware supported on the Catalyst 4500 Series Switch.

Table 1 Supported Hardware

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
Supervisor Engines		
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

Table 1 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**	**Software Release Minimum**
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
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-X4640-CSFP-E	80 ports with Gigabit compact SFP (4:1 oversubscribed); 40 modules of Gigabit SFP line card (1000BaseX), providing 24 gigabits per-slot capacity (SFP optional) (2:1 oversubscribed)	15.1(1)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

Table 1 Supported Hardware (continued)

Product Number (append with "=" for spares)	**Product Description**	**Software Release**
		Minimum
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
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
PWR-C45-9000ACV	Catalyst 4500 Series Switch 9000 W AC power supply	XE 3.4(0)SG, 15.1(2)SG

Table 1 briefly describes the four chassis in the Catalyst 4500 Series Switch. For the chassis listed in the table, refer to Table 4 on page 8 for software release information.

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
WS-C4506	Catalyst 4506 chassis includes these components: • 6 slots • Fan tray
WS-C4507R	Catalyst 4507R chassis includes these components: • 7 slots • Fan tray
WS-C4510R	Catalyst 4510R chassis includes these components: • 10 slots; slot 10 accepts only the Catalyst 4500 series 2-port Gigabit Ethernet line card • Fan tray

Table 2 DOM Support on the Catalyst 4500 Series Switch applies to these module

Transceiver Module
CWDM- SFP-*xx*
DWDM-GBIC-*xx*
DWDM-SFP
DWDM-X2-*xx*
GLC-BX-D
GLC-BX-U
GLC-EX-SMD
SFP-10G-SR
SFP-10G-LR
SFP-10G-LRM
SFP-10G-ER
SFP-10G-ZR

For details on transceiver module compatibility information, please refer to the URL:

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

Supported Hardware on Catalyst 4500 E-Series Switch

In addition to the classic line cards and supervisor engines, Cisco IOS Software Release 15.2(2)E 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 3).

Table 3 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
WS-C4510R-E	Cisco Catalyst 4500 E-Series 10-Slot Chassis • Fan tray • No Power Supply • Redundant supervisor engine capability • Slots 8, 9, and 10 are limited to 6Gbps when used with a Supervisor Engine 6-E or a Supervisor Engine 6L-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 or a Supervisor Engine 6L-E.
WS-X45-Sup6-E	Cisco Catalyst 4500 E-Series Sup 6-E, 2x10GE(X2) w/ TwinGig

Table 3 Supported E-Series Hardware

Product Number	Description
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 4 outlines the chassis and supervisor engine compatibility.
(M=Minimum release, R=Recommended release)

Table 4 Chassis and Supervisor Compatibility

Chassis	Sup 6-E	Sup 6L-E
WS-C4503-E	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4506-E	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4507R-E	M: 12.2(40)SG	M: 12.2(52)XO
WS-C4507R+E	M: 12.2(54)SG	M: 12.2(54)SG
WS-C4510R-E	M: 12.2(40)SG	
WS-C4510R+E	M: 12.2(54)SG	

Feature Support by Image Type

Table 5 is a detailed list of features supported on Catalyst 4500 Series Switch running Cisco IOS Software Release 15.2(2)E. For the full list of supported features, check the Feature Navigator application:

http://tools.cisco.com/ITDIT/CFN/

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
2-way Community Private VLANs	No	Yes	Yes
8-Way CEF Load Balancing	No	Yes	Yes
10G Uplink Use	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
AAA Server Group	Yes	Yes	Yes
ACL Logging	Yes	Yes	Yes
ANCP Client	No	Yes	Yes
ANSI TIA-1057 LLDP - MED Location Extension	Yes	Yes	Yes
ANSI TIA-1057 LLDP - MED Support	Yes	Yes	Yes
AppleTalk 1 and 2 (not supported on Sup 6-E and 6L-E)	No	No	Yes
Auto Security	Yes	Yes	Yes
Auto SmartPorts	Yes	Yes	Yes
AutoQoS	Yes	Yes	Yes
Auto-MDIX	Yes	Yes	Yes
Auto-Voice VLAN (part of Auto QoS)	No	Yes	Yes
Bidirectional Forwarding Detection (BFD) Hardware Offload Support	No	Yes	Yes
BFD - EIGRP Support	No	Yes	Yes
BFD - Static Route Support over IPv4	No	Yes	Yes
BFD IPv6 Encapsulation Support	No	Yes	Yes
BGP Support for BFD	No	No	Yes
BGP	No	No	Yes
BGP 4	No	No	Yes
BGP 4 4Byte ASN (CnH)	No	No	Yes
BGP 4 Multipath Support	No	No	Yes
BGP 4 Prefix Filter and In-bound Route Maps	No	No	Yes
BGP Conditional Route Injection	No	No	Yes
BGP Link Bandwidth	No	No	Yes
BGP Neighbor Policy	No	No	Yes
BGP Prefix-Based Outbound Route Filtering	No	No	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
BGP Route-Map Continue	No	No	Yes
BGP Route-Map Continue Support for Outbound Policy	No	No	Yes
BGP Route-Map Policy List Support	No	No	Yes
BGP Soft Reset	No	No	Yes
BGP Wildcard	No	No	Yes
Bidirectional PIM (IPv4 only)	No	Yes	Yes
BOOTP	Yes	Yes	Yes
Bootup GOLD	No	Yes	Yes
Broadcast/Multicast Suppression	Yes	Yes	Yes
Call Home	No	Yes	Yes
CDP/CDPv2	Yes	Yes	Yes
CFM	Yes	Yes	Yes
CGMP - Cisco Group Management Protocol	Yes	Yes	Yes
Cisco IOS Scripting w/Tcl	Yes	Yes	Yes
CiscoView Autonomous Device Manager (ADP)	Yes	Yes	Yes
CNS	Yes	Yes	Yes
Command Scheduler (Kron)	Yes	Yes	Yes
Community PVLAN support	No	Yes	Yes
Config File	Yes	Yes	Yes
Configuration Replace and Configuration Rollback	Yes	Yes	Yes
Configuration Rollback Confirmed Change	Yes	Yes	Yes
Copy Command	Yes	Yes	Yes
Console Access	Yes	Yes	Yes
Control Plane Policing (CoPP)	Yes	Yes	Yes
CoS to DSCP Map	Yes	Yes	Yes
CPU Optimization for Layer 3 Multicast Control Packets	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Crashdump Enhancement[1]	Yes	Yes	Yes
DAI (Dynamic ARP Inspection)	Yes	Yes	Yes
DBL (Dynamic Buffer Limiting) - Active Queue Management	Yes	Yes	Yes
Debug Commands	Yes	Yes	Yes
Device Management	Yes	Yes	Yes
DHCPv6 Relay Agent notification for Prefix Delegation	No	Yes	Yes
DHCP Client	Yes	Yes	Yes
DHCP Gleaning	No	Yes	Yes
DHCP Server	Yes	Yes	Yes
DHCP Snooping	Yes	Yes	Yes
DHCPv6 Ethernet Remote ID option	No	Yes	Yes
Diagnostics Tools	Yes	Yes	Yes
Diffserv MIB	Yes	Yes	Yes
Digital Optical Monitoring (DOM)	Yes	Yes	Yes
DSCP to CoS Map	Yes	Yes	Yes
DSCP to egress queue mapping	Yes	Yes	Yes
DSCP/CoS via LLDP	Yes	Yes	Yes
Duplication Location Reporting Issue	No	Yes	Yes
Easy Virtual Network (EVN)	No	No	Yes
EIGRP	No	No	Yes
EIGRP Service Advertisement Framework	Yes	Yes	Yes
EIGRP Stub Routing	No	Yes	Yes
Embedded Event Manager (EEM) 4.0	Yes	Yes	Yes
Embedded Event Manager and EOT integration	No	Yes	Yes
Energywise Agentless SNMP support	Yes	Yes	Yes
Energywise Wake-On-Lan Support	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
EPoE	Yes	Yes	Yes
EtherChannel	Yes	Yes	Yes
Ethernet Management Port (Fa1 interface)[2]	Yes	Yes	Yes
Ethernet Operations, Administration, and Maintenance (OAM)	Yes	Yes	Yes
Event Log	Yes	Yes	Yes
FHRP - Enhanced Object Tracking of IP SLAs	Yes	No	Yes
FHRP - GLBP - IP Redundancy API	No	Yes	Yes
FHRP - HSRP - Hot Standby Router Protocol V2	No	Yes	Yes
FHRP - Object Tracking List	No	Yes	Yes
FIPS 140-2/3 Level 2 Certification	Yes	Yes	Yes
File Management	Yes	Yes	Yes
Flex Links+ (VLAN Load balancing)	Yes	Yes	Yes
Gateway Load Balancing Protocol (GLBP)	No	Yes	Yes
GOLD Online Diagnostics	Yes	Yes	Yes
HSRP: Global IPv6 Address	No	Yes	Yes
HSRP - Hot Standby Router Protocol	No	Yes	Yes
HSRPv2 for IPv6 Global Address Support	No	Yes	Yes
HTTP TACAC+ Accounting support	Yes	Yes	Yes
Identity 4.1 ACL Policy Enhancements	Yes	Yes	Yes
Identity 4.2: MAB with Configurable User Name/Password	Yes	Yes	Yes
Identity 4.1 Network Edge Access Topology	Yes	Yes	Yes
ID 4.0 Voice Vlan assignment	Yes	Yes	Yes
ID 4.1 Filter ID and per use ACL	Yes	Yes	Yes
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)	Yes	Yes	Yes
IEEE 802.1ab LLDP/LLDP-MED	Yes	Yes	Yes
IEEE 802.1ab LLDP enhancements (PoE+Layer 2 COS)	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.1ag D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet	Yes	Yes	Yes
IEEE 802.1p Support	Yes	Yes	Yes
IEEE 802.1p Prioritization	Yes	Yes	Yes
IEEE 802.1p/802.1q	Yes	Yes	Yes
IEEE 802.1Q Tunneling	Yes	Yes	Yes
IEEE 802.1Q VLAN Trunking	Yes	Yes	Yes
IEEE 802.1s Multiple Spanning Tree (MST) Standard Compliance	Yes	Yes	Yes
IEEE 802.1w Spanning Tree Rapid Reconfiguration	Yes	Yes	Yes
IEEE 802.1x (Auth-Fail VLAN, Accounting)	Yes	Yes	Yes
IEEE 802.1x Critical Authorization for Voice and Data	Yes	Yes	Yes
IEEE 802.1x Flexible Authentication	Yes	Yes	Yes
IEEE 802.1x with Multiple authenticated, multi-host	Yes	Yes	Yes
IEEE 802.1x Open Authentication	Yes	Yes	Yes
IEEE 802.1x with User Distribution	Yes	Yes	Yes
IEEE 802.1x User Port Description	Yes	Yes	Yes
IEEE 802.1x VLAN Assignment)	Yes	Yes	Yes
IEEE 802.1x VLAN User Group Distribution	Yes	Yes	Yes
IEEE 802.1x Wake on LAN	Yes	Yes	Yes
IEEE 802.1x Agentless Audit Support	Yes	Yes	Yes
IEEE 802.1x Authenticator	Yes	Yes	Yes
IEEE 802.1x Fallback support	Yes	Yes	Yes
IEEE 802.1x Guest VLAN	Yes	Yes	Yes
IEEE 802.1x MIB Support	Yes	Yes	Yes
IEEE 802.1x Multi-Domain Auth with Voice VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x Multi-Domain Authentication	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IEEE 802.1x Private Guest VLAN	Yes	Yes	Yes
IEEE 802.1x Private VLAN Assignment	Yes	Yes	Yes
IEEE 802.1x RADIUS Accounting	Yes	Yes	Yes
IEEE 802.1x Radius-Supplied Session Timeout	Yes	Yes	Yes
IEEE 802.1x and MAB with ACL assignment	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP)	Yes	Yes	Yes
IEEE 802.3ad Link Aggregation (LACP) Port-Channel Standalone Disable	Yes	Yes	Yes
IEEE 802.3ah and CFM Interworking	No	Yes	Yes
IEEE 802.3x Flow Control	Yes	Yes	Yes
IEEE 802.1x Web-Auth	Yes	Yes	Yes
IGMP Filtering	Yes	Yes	Yes
IGMP Querier	Yes	Yes	Yes
IGMP Snooping	Yes	Yes	Yes
IGMP Version 1	Yes	Yes	Yes
IGMP Version 2	Yes	Yes	Yes
IGMP Version 3	Yes	Yes	Yes
IGMPv3 Host Stack	Yes	Yes	Yes
Ingress Policing	Yes	Yes	Yes
Interface Access (Telnet, Console/Serial, Web)	Yes	Yes	Yes
IOS Based Device Profiling	No	Yes	Yes
IP Enhanced IGRP Route Authentication	No	No	Yes
IP Event Dampening	Yes	Yes	Yes
IP Multicast Load Splitting across Equal-Cost Paths	No	Yes	Yes
IP Named Access Control List	Yes	Yes	Yes
IPv6 Tunnels (in software)	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IP Routing	Yes	Yes	Yes
IP SLAs DHCP Operation	No	Yes	Yes
IP SLAs Distribution of Statistics	No	Yes	Yes
IP SLAs DNS Operation	No	Yes	Yes
IP SLAs FTP Operation	No	Yes	Yes
IP SLAs History Statistics	No	Yes	Yes
IP SLAs HTTP Operation	No	Yes	Yes
IP SLAs ICMP Echo Operation	No	Yes	Yes
IP SLAs ICMP Path Echo Operation	No	Yes	Yes
IP SLAs Multi Operation Scheduler	No	Yes	Yes
IP SLAs One Way Measurement	No	Yes	Yes
IP SLAs Path Jitter Operation	No	Yes	Yes
IP SLAs Random Scheduler	No	Yes	Yes
IP SLAs Reaction Threshold	No	Yes	Yes
IP SLAs Responder	Yes	Yes	Yes
IP SLAs Scheduler	No	Yes	Yes
IP SLAs SNMP Support	No	Yes	Yes
IP SLAs Sub-millisecond Accuracy Improvements	No	Yes	Yes
IP SLAs TCP Connect Operation	No	Yes	Yes
IP SLAs UDP Based VoIP Operation	No	Yes	Yes
IP SLAs UDP Echo Operation	No	Yes	Yes
IP SLAs UDP Jitter Operation	No	Yes	Yes
IP SLAs Video Operations	No	Yes	Yes
IP SLAs VoIP Threshold Traps	No	Yes	Yes
IP Unnumbered for VLAN-SVI interfaces	No	Yes	Yes
IPsecv3/IKEv2 (for management traffic only)	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IPSG (IP Source Guard) v4	Yes	Yes	Yes
IPSG (IP Source Guard) v4 for Static Hosts	Yes	Yes	Yes
IPv4 Policy Based Routing	No	No	Yes
IPv4 Policy Based Routing with recursive next hop	No	No	Yes
IPv6 / v4 BFD with OSPF/ BGP/ EIGRP and Static	No	Yes	Yes
IPv6 Bootstrap Router (BSR) Scoped Zone Support	No	No	Yes
IPv6 First Hop Security (FHS): DHCPv6 Guard Lightweight DHCPv6 Relay Agent IPv6 Destination Guard IPv6 Snooping IPv6 Neighbor Discovery Multicast Suppression IPv6 Router Advertisement (RA) Guard	Yes	Yes	Yes
IPv6 First Hop Security (FHS) Phase 2: Binding table recovery Bulk Lease Query support from Lightweight DHCPv6 Relay Agent (LDRA) Neighbor Discovery (ND) Multicast Suppress Source & Prefix Guard[3]	Yes	Yes	Yes
IPv6 HSRP	No	Yes	Yes
IPv6 Interface Statistics	Yes	Yes	Yes
IPv6 IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)	No	Yes	Yes
IPv6 (Internet Protocol Version 6)	Yes	Yes	Yes
IPV6 MLD snooping V1 and V2	Yes	Yes	Yes
IPv6 Multicast	No	Yes	Yes
IPv6 Multicast: Bootstrap Router (BSR)	No	Yes	Yes
IPv6 Multicast: Multicast Listener Discovery (MLD) Protocol, Versions 1 and 2	No	Yes	Yes
IPv6 Multicast: PIM Accept Register	No	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
IPv6 Multicast: PIM Source-Specific Multicast (PIM-SSM)	No	Yes	Yes
IPv6 Multicast: PIM Sparse Mode (PIM-SM)	No	Yes	Yes
IPv6 Multicast: Routable Address Hello Option	No	Yes	Yes
IPv6 Neighbor Discovery	No	Yes	Yes
IPv6 OSPFv3 Fast Convergence	No	Yes[4]	Yes
IPv6 OSPFv3 NSF/SSO	No	Yes[4]	Yes
IPv6 Policy Based Routing	No	No	Yes
Identity 4.1 Network Edge Access Topology	Yes	Yes	Yes
IPv6 RA Guard (Host Mode)	Yes	Yes	Yes
IPv6 Reformation	NA	Yes	Yes
IPv6 Routing - EIGRP Support	No	No	Yes
IPv6 Routing: OSPF for IPv6 (OSPFv3)	No	Yes[4]	Yes
IPv6 Routing: RIP for IPv6 (RIPng)	No	Yes	Yes
IPv6 Static Route support for Object Tracking	Yes	Yes	Yes
IPv6 Switching: CEFv6 Switched Automatic IPv4-compatible Tunnels (in software)	No	Yes	Yes
IPv6 Switching: CEFv6 Switched Configured IPv6 over IPv4 Tunnels (in software)	No	Yes	Yes
IPv6 Switching: CEFv6 Switched ISATAP Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: Automatic 6to4 Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: Automatic IPv4-compatible Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: IPv6 over IPv4 GRE Tunnels (in software)	No	Yes	Yes
IPv6 Tunneling: ISATAP Tunnel Support (in software)	No	Yes	Yes
IPv6 Tunneling: Manually Configured IPv6 over IPv4 Tunnels (in software)	No	Yes	Yes
IPv6 Virtual LAN Access Control List	Yes	Yes	Yes
ISIS for IPv4 and IPv6	No	No	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
ISL Trunk	Yes	Yes	Yes
ISSU (IOS In-Service Software Upgrade)	No	Yes	Yes
Jumbo Frames	Yes	Yes	Yes
Layer 2 Control Packet	Yes	Yes	Yes
Layer 2 Protocol Tunneling (L2PT)	No	Yes	Yes
Layer 2 Traceroute	Yes	Yes	Yes
Layer 3 Multicast Routing (PIM SM, SSM, Bidir)	No	Yes	Yes
Link State Tracking	Yes	Yes	Yes
Local Web Auth	Yes	Yes	Yes
MAB (MAC Authentication Bypass) for Voice VLAN	Yes	Yes	Yes
MAC Address Filtering	Yes	Yes	Yes
MAC Based Access List	Yes	Yes	Yes
MAC Move and Replace	Yes	Yes	Yes
Medianet 2.0: AutoQoS SRND4 Macro	No	Yes	Yes
Medianet 2.0: Integrated Video Traffic Simulator (hardware-assisted IP SLA); IPSLA responder only	No	Yes	Yes
Medianet 2.0: Flow Metadata	No	Yes	Yes
Medianet 2.0: Media Service Proxy	No	Yes	Yes
Medianet 2.0: Media Monitoring (Performance Monitoring and Mediatrace)	No	Yes	Yes
Medianet 2.0: MSP and Metadata	No	No	Yes
MediaTrace 1.0	Yes	Yes	Yes
Multicast BGP (MBGP)	No	No	Yes
Multicast HA (NSF/SSO) for IPv4&IPv6	No	Yes	Yes
Multicast Routing Monitor (MRM)	No	Yes	Yes
Multicast Source Discovery Protocol (MSDP)	Yes	Yes	Yes
Multicast VLAN Registration (MVR)	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Multi-authentication and VLAN Assignment	Yes	Yes	Yes
Multi-VRF Support (VRF lite)	No	No	Yes
NAC - L2 IEEE 802.1x	Yes	Yes	Yes
NAC - L2 IP	Yes	Yes	Yes
ND Cache Limit/Interface	No	Yes	Yes
NEAT Enhancement: Re-Enabling BPDU Guard Based on User Configuration	Yes	Yes	Yes
Network Edge Access Topology (NEAT)	Yes	Yes	Yes
Network Time Protocol (NTP)	Yes	Yes	Yes
NMSP Enhancements • GPS support for location • Location at switch level • Local timezone change • Name value pair • Priority settings for MIBs	No	Yes	Yes
Time Protocols (SNTP, TimeP) primary (formerly known as Time Protocols (SNTP, TimeP) master)	Yes	Yes	Yes
No. of QoS Filters No. of Security ACE	Yes (4K entries)	Yes	Yes
No Service Password Recovery	Yes	Yes	Yes
No. of VLAN Support	2048	4096	4096
NSF - BGP	No	No	Yes
NSF - EIGRP	No	Yes	Yes
NSF - OSPF (version 2 only)	No	Yes	Yes
NSF/SSO (Nonstop Forwarding with Stateful Switchover)	No	No	Yes
NTP for IPv6	Yes	Yes	Yes
NTP for VRF aware	No	No	Yes
On Demand Routing (ODR)	No	No	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
OSPF	No	Yes[4]	Yes
OSPF v3 Authentication	No	Yes[4]	Yes
OSPFv3 Authentication Trailer	Yes	Yes	Yes
OSPF Flooding Reduction	No	Yes[4]	Yes
OSPF for Routed Access[5]	No	Yes	Yes
OSPF Incremental Shortest Path First (i-SPF) Support	No	Yes[4]	Yes
OSPF Link State Database Overload Protection	No	Yes[4]	Yes
OSPF Not-So-Stubby Areas (NSSA)	No	Yes[4]	Yes
OSPF Packet Pacing	No	Yes[4]	Yes
OSPF Shortest Paths First Throttling	No	Yes[4]	Yes
OSPF Stub Router Advertisement	No	Yes[4]	Yes
OSPF Support for Fast Hellos	No	Yes[4]	Yes
OSPF Support for Link State Advertisement (LSA) Throttling	No	Yes[4]	Yes
OSPF Support for Multi-VRF on CE Routers	No	Yes[4]	Yes
OSPF Update Packet-Pacing Configurable Timers	No	Yes[4]	Yes
Out-of-band Management Port	Yes	Yes	Yes
Out-of-band Management Port - IPv6	Yes	Yes	Yes
PAgP	Yes	Yes	Yes
Passwords Password clear protection	Yes	Yes	Yes
PBR Support for Multiple Tracking Options	Yes	Yes	Yes
Per Intf IGMP State Limit	Yes	Yes	Yes
Per Intf MrouteState Limit	Yes	Yes	Yes
Per-User ACL Support for 802.1X/MAB/Webauth users	Yes	Yes	Yes
Per-VLAN Learning	Yes	Yes	Yes
PIM Sparse Mode Version4	No	No	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
PIM Version 1	No	Yes	Yes
PM Version 2	No	Yes	Yes
PoE (up to 15.4W only)	Yes	Yes	Yes
PoE+ Ready	Yes	Yes	Yes
PoEP via LLDP	Yes	Yes	Yes
Port Access Control List (PACL)	Yes	Yes	Yes
Port Monitoring (interface Stats)	Yes	Yes	Yes
Port Security	Yes (supports 1024 MACs)	Yes (supports 3072 MACs)	Yes (supports 3072 MACs)s
Post Status	Yes	Yes	Yes
Pragmatic General Multicast (PGM)	Yes	Yes	Yes
Private VLANs	Yes	Yes	Yes
Propagation of Location Info over CDP	Yes	Yes	Yes
PVLAN over EtherChannel	Yes	Yes	Yes
PVST+ (Per Vlan Spanning Tree Plus)	Yes	Yes	Yes
Q-in-Q	Yes	Yes	Yes
RACL	Yes	Yes	Yes
RADIUS/TACACS+ (AAA)	Yes	Yes	Yes
RADIUS Attribute 44 (Accounting Session ID) in Access Requests	Yes	Yes	Yes
RADIUS Change of Authorization	Yes	Yes	Yes
Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)	Yes	Yes	Yes
Remote SPAN (RSPAN)	Yes	Yes	Yes
REP (Resilient Ethernet Protocol)	Yes	Yes	Yes
REP - No Edge Neighbor Enhancement	Yes	Yes	Yes
RIP v1	No	Yes	Yes
RMON	Yes	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Role-Based Access Control CLI commands (RBAC)	Yes	Yes	Yes
Role-Based CLI Inclusive Views	Yes	Yes	Yes
RPR	Yes	Yes	Yes
RPVST+	Yes	Yes	Yes
RSPAN	Yes	Yes	Yes
Secure CDP	Yes	Yes	Yes
Secure Copy (SCP)	Yes	Yes	Yes
Secure Shell SSH Version 1, 2 Server Support	Yes	Yes	Yes
Secure Shell SSH Version 1, 2 Client Support	Yes	Yes	Yes
Service Advertisement Framework (SAF)	No	No	Yes
Smart Install Director—Configuration-only Deployment and Smooth Upgrade	Yes	Yes	Yes
SmartPorts (Role based MACRO)	Yes	Yes	Yes
SMI Catalyst 4K Client	Yes	Yes	Yes
SNMP (Simple Network Management Protocol)	Yes	Yes	Yes
SNMPv3 (SNMP Version 3)	Yes	Yes	Yes
Source Port Filtering (Private VLAN)	Yes	Yes	Yes
Source Specific Multicast (SSM)	No	Yes	Yes
Source Specific Multicast (SSM) - IGMPv3,IGMP v3lite, and URD	Yes	Yes	Yes
Source Specific Multicast (SSM) Mapping	Yes	Yes	Yes
SPAN (# of sessions) – Port Mirroring	Yes (2 bidirectional sessions)	Yes (8 bidirectional sessions)	Yes (8 bidirectional sessions)
SPAN ACL Filtering for IPv6	Yes	Yes	Yes
SSHv2/Secure Copy, FTP, SSL, Syslog, Sys Information	Yes	Yes	Yes
SSO (Stateful SwitchOver)	No	Yes	Yes
Static Route Support for BFD over IPv6	No	No	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
Static Routing (IPv4/IPv6)	Yes	Yes	Yes
Storm Control - Per-Port Multicast Suppression	Yes	Yes	Yes
Stub IP Multicast Routing	No	Yes	No
Sub-second UDLD	Yes	Yes	Yes
SVI (Switch Virtual Interface) Autostate Exclude	Yes	Yes	Yes
TACACS+	Yes	Yes	Yes
TACACS+ and Radius for IPv6-	Yes	Yes	Yes
Time-Based Access Lists	Yes	Yes	Yes
Time Domain Reflectometry (TDR)[6]	No	Yes	Yes
Time Protocols (SNTP, TimeP)	Yes	Yes	Yes
Traffic Mirroring (SPAN)	Yes	Yes	Yes
Trusted Boundary (LLDP & CDP Based)	Yes	Yes	Yes
TrustSec SGT/ SGA TrustSec	No	Yes	Yes
Unicast Reverse Path Forwarding (uRPF)	Yes	Yes	Yes
UniDirectional Link Detection (UDLD)	Yes	Yes	Yes
Virtual Router Redundancy Protocol (VRRP) for IPv4	No	Yes	Yes
VLAN Access Control List (VACL)	Yes	Yes	Yes
VLAN Mapping (VLAN Translation)	No	Yes	Yes
Voice VLAN	Yes	Yes	Yes
VRF-aware TACACS+	No	No	Yes
VRF-lite for IPv6 on OSPF/ BGP/ EIGRP	No	No	Yes
VTP (Virtual Trunking Protocol) Version 2	Yes	Yes	Yes
VTP version 3	Yes	Yes	Yes
WCCP Redirection on Inbound Interfaces	No	Yes	Yes
WCCP Version 2	No	Yes	Yes

Table 5 LAN Base, IP Base, and Enterprise Services Image Support on the Catalyst 4500 Series Switch

Feature	LAN Base	IP Base	Enterprise Services
WSMA Enhancements for wireless management	Yes	Yes	Yes
XML-PI	Yes	Yes	Yes

1. Supported only on Supervisor Engine 6-E and Supervisor Engine 6L-
2. Starting with Cisco IOS Release 12.2(46)SG
3. When either Source or Prefix Guard for IPv6 is enabled, ICMPv6 packets are unrestricted on all Catalyst 4500 series switch platforms running IOS Cisco Release 15.2(1)E. All other traffic types are restricted.
4. IP Base supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 200 dynamically learned routes.
5. OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 1000 dynamically learned routes.
6. TDR is not supported on 46xx linecards.

Note You can purchase a special license to enable the 10 Gigabit uplinks in the LAN Base image without moving to IP Base.

MIB Support

For information on MIB support, please refer to this URL:

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

Features Not Supported on the Cisco Catalyst 4500 Series Switch

- BFD for IPv6 EIGRP and IPv6 BGP in any 3.4.0SG images including SG4 (to be released in May-June, 2014).
- 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
- Bridge groups
- CEF Accounting
- CFM CoS
- 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
- LLDP HA
- Lock and key
- NAT-PT for IPv6
- NetFlow per-VRF
- PBR with EOT
- PBR with Multiple Tracking Options
- QoS for IPv6 traffic (only supported on Supervisor 6)
- Reflexive ACLs
- Routing IPv6 over an MPLS network
- SMI Proxy
- WCCP version 1

Orderable Product Numbers

Table 6 Orderable Product Numbers for the Catalyst 4500 Series Switch

Product Number	Description	Image
S45EES-15202E	Cisco CAT4500E IOS ENTERPRISE SERVICES W/O CRYPTO	cat4500e-entservices-mz
S45EESU-15202E	Cisco CAT4500E IOS ENTERPRISE SERVICES UPGRADE W/O CRYPTO	cat4500e-entservices-mz
S45EESK9-15202E	Cisco CAT4500E IOS ENTERPRISE SERVICES SSH	cat4500e-entservicesk9-mz
S45EESUK9-15202E	Cisco CAT4500E IOS ENTERPRISE SERVICES UPGRADE SSH	cat4500e-entservicesk9-mz
S45EIPB-15202E	Cisco CAT4500E IOS IP BASE W/O CRYPTO	cat4500e-ipbase-mz
S45EIPBU-15202E	Cisco CAT4500E IOS IP BASE UPGRADE W/O CRYPTO	cat4500e-ipbase-mz
S45EIPBK9-15202E	Cisco CAT4500E IOS IP BASE SSH	cat4500e-ipbasek9-mz
S45EIPBUK9-15202E	Cisco CAT4500E IOS IP BASE UPGRADE SSH	cat4500e-ipbasek9-mz
S45ELB-15202E	Cisco CAT4500E IOS LAN BASE W/O CRYPTO	cat4500e-lanbase-mz
S45ELBK9-15202E	Cisco CAT4500E IOS LAN BASE SSH	cat4500e-lanbasek9-mz

New and Changed Information

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

New Software Features in Release 15.2(2)E3

The following table list the new features for Release IOS 15.2(2)E3:

Feature Name	Description

CDP Bypass	Authentication sessions are established in single and multi-host modes for IP Phones. However, if voice VLAN and 802.1x on an interface port is enabled, then CDP Bypass is enabled when the host mode is set to single or multi-host mode.
	Note By default the host mode is set to single mode in legacy mode and multi-authentication in the eedge mode.
	Use the following commands to configure CDP bypass:
	`Switch> enable`
	`Switch# configure terminal`
	`Switch(config)# interface <` *interface-id* `>`
	`Switch(config-if)# switchport mode access`
	`Switch(config-if)# switchport voice vlan <` *vlan-id* `>`
	`Switch(config-if)# authentication port-control auto`
	`Switch(config-if)# authentication host-mode {single | multi-host}`
	`Switch(config-if)# dot1x pae authenticator`
	(LAN Base, IP Base, and Enterprise Services)

New Hardware Features in Release 15.2(2)E1

- New passive CX1 assemblies: SFP-H10GB-CU1-5M, SFP-H10GB-CU2M, SFP-H10GB-CU2-5M
- Support for SFP-H10GB-ACU7M, SFP-H10GB-ACU10M (active CX1 cable assemblies)
- Support of breakout cable on the 10 GbE end for: QSFP-4SFP10G-CU1M, QSFP-4SFP10G-CU3M, QSFP-4SFP10G-CU5M
- Support for Cisco SFP+ Active Optical Cables - Cisco SFP-10G-AOC1M Cisco SFP-10G-AOC2M Cisco SFP-10G-AOC3M, Cisco SFP-10G-AOC5M, Cisco SFP-10G-AOC7M, Cisco SFP-10G-AOC10M

New Software Features in IOS Release 15.2(2)E1

The following table list the new features for Release IOS 15.2(2)E1.

Feature Name	Description
Device Sensor	(LAN Base)
Policy Based Routing (PBR)	(IP Base)

New Software Features in Release IOS 15.2(2)E

The following table list the new features for Release IOS 15.2(2)E.

Feature Name	Description
Use this URL for the Cisco IOS XE Release 3E Documentation Roadmap	Provides quick and easy access to all relevant documentation for specific platforms. Look for *Quick Links to Platform Documentation* on the respective platform documentation pages. : http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3e/tsd-products-support-series-home.html
Use this URL for the Cisco IOS Release 15E Documentation Roadmap	. : http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-15-2e/tsd-products-support-series-home.html
Auto Security	Provides a single line CLI, to enable base line security features (Port Security, DHCP snooping, DAI).
DHCP Gleaning	Allows components to register and glean DHCP packets.This is a read--only DHCP functionality.
Embedded Event Manager (EEM) 4.0	Provides unique customization capabilities and event driven automation within Cisco products.
HSRP: Global IPv6 Address	Allows users to configure multiple non-link local addresses as virtual addresses. The Hot Standby Router Protocol (HSRP) ensures host-to-router resilience and failover, in case the path between a host and the first-hop router fails, or the first-hop router itself fails.
IPv6 Static Route support for Object Tracking	Allows an IPv6 Static Route to be associated with a tracked-object.
IPv6 PBR	Allows you to manually configure how the received packets should be routed. PBR allows you to identify packets by using several attributes and to specify the next hop or the output interface to which the packet should be sent. **Note** With IOS XE Release 3.6.0E and IOS 15.2(2)E, IPv6 PBR is not supported on Supervisor Engine 8-E.

Feature Name	Description
MediaTrace 1.0	Provides the capability to diagnose Media Stream on top of various instrumentations in Cisco routers/switches and endpoints. Also addresses the MediaNet Video monitoring requirement to discover the signaling path and provides end-to-end diagnostics along the media stream routes
OSPFv3 Authentication Trailer	Provides a mechanism to authenticate Open Shortest Path First version 3 (OSPFv3) protocol packets as an alternative to existing OSPFv3 IPsec authentication.
PBR Support for Multiple Tracking Options	Extends the capabilities of object tracking using Cisco Discovery Protocol (CDP) to allow the policy-based routing (PBR) process to verify object availability by using additional methods.
Role-Based CLI Inclusive Views	Enables a standard CLI view including all commands by default.
Policy Based Routing: Recursive Next Hop	Enhances route maps to enable configuration of a recursive next-hop IP address that is used by policy-based routing (PBR).
Secure CDP	Allows you to select the type, length, value (TLV) fields that are sent on a particular interface to filter information sent through Cisco Discovery Protocol packets.
SMI Catalyst 4K Client	Enables a Catalyst 4k standalone switch acting as Smart Install Client. **Note** SMI Proxy is supported.
WSMA Enhancements for wireless management	Allows you to reduce the reconnecting rates in an outage when device connections to the management server on wireless networks are disconnected unexpectedly.

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 at least ROMMON Release 12.2(44r)SG5 to run Cisco IOS Release 15.1(2)SG on the Supervisor Engine 6-E and Supervisor Engine 6L-E. 12.2(44r)SG9 is recommended.

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 7 Supervisor Engine and Recommended ROMMON Release

Supervisor Engine	Recommended ROMMON Release
6-E	12.2(44r)SG9
6L-E	12.2(44r)SG9

Table 8 ROMMON Release and Promupgrade Programs

ROMMON Release	Promupgrade Program
12.2(31r)SGA4	cat4500-e-ios-promupgrade-122_31r_SGA4
12.2(44r)SG5	cat4500-e-ios-promupgrade-122_44r_SG5
12.2(44r)SG9	cat4500-e-ios-promupgrade-122_44r_SG9
12.2(44r)SG10	cat4500-e-ios-promupgrade-122_44r_SG10

The following sections describe how to upgrade your switch software:

- Identifying an +E Chassis and ROMMON, page 29
- Upgrading the Cisco IOS Software, page 29

Identifying an +E Chassis and ROMMON

An +E chassis is identified by a FRU minor value in the chassis' idprom.

When supervisor engine 1 (sup1) is in ROMMON and supervisor engine 2 (sup2) is in IOS, only sup2 can read the idprom contents of chassis' idprom. Chassis type is displayed as "+E" in the output of the **show version** command. Conversely, sup1 can only display the chassis type as "E."

When both sup1 and sup2 are in ROMMON, both engines can read the chassis' idprom. Chassis type is displayed correctly as "+E" in the output of the **show version** command.

When both sup1 and sup2 are in IOS, both engines can read the chassis' idprom. Chassis type is displayed correctly as "+E" in the output of the **show version** command.

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 15.1(2)SG 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.

- We recommend that you configure the **access-session interface-template sticky timer** *timer-value* command at the global or interface configuration mode, and not within the template.
- The **show exception files all** command lists only crashinfo files from the active supervisor engine. You must issue the **dir slavecrashinfo:** and **dir slvecrashinfo-dc:** commands to obtain lists of crashinfo files from the standby supervisor engine.
- Starting with Release IOS 15.1(1)SG, the seven RP restriction was removed.
- 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 behavior 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.
- Although you can configure subsecond PIM query intervals on Catalyst 4500 platforms, such an action represents a compromise between convergence (reaction time) and a number of other factors (number of mroutes, base line of CPU utilization, CPU speed, processing overhead per 1 m-route, etc.). You must account for those factors when configuring subsecond PIM timers. We recommend that you set the PIM query interval to a minimum of 2 seconds. By adjusting the available parameters, you can achieve flawless operation; that is, a top number of multicast routes per given convergence time on a specific setup.
- With Cisco IOS Release XE 3.2.1SG, **memory** configuration is enabled:

```
Switch(config)# memory ?
  chunk    chunk related configuration
  free     free memory low water mark
  record   configure memory event/traceback recording options
  reserve  reserve memory
  sanity   Enable memory sanity
```

  This configuration had been removed erroneously in a prior release.

- 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.

- 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-C45-1300ACV
  - 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.
- With Cisco IOS Release 12.2(53)SG3 (and 12.2(54)SG), we changed the default behavior such that your single supervisor, RPR, or fixed configuration switch does not reload automatically. To configure automatic reload, you must enter the **diagnostic fpga soft-error recover aggressive** command. (CSCth16953)
- Energywise WOL is not “waking up” a PC in hibernate or standby mode.

Workaround: None. CSCtr51014

- The ROMMON version number column in the output of **show module** command is truncated.

  Workaround: Use the **show version** command. CSCtr30294

- IP SLA session creation fails randomly for various 4-tuples.

  Workaround: Select an alternate destination or source port. CSCty05405

- The system cannot scale to greater than 512 SIP flows with MSP and metadata enabled.

  Workaround: None. CSCty79236

- On the following linecards running IOS Release 15.0(2)SG3:
  - 48 10/100/1000BaseT Premium POE E Series WS-X4648-RJ45V+E (JAE14310RHU)
  - 6 Sup 6-E 10GE (X2), 1000BaseX (SFP) WS-X45-SUP6-E (JAE13104VVY)

  the following restrictions apply:
  - Sub-interfaces are not supported on 1 Gigabit and Ten-Gigabit interfaces.
  - Port-channel members do not support multiple classification criteria for a QoS policy.
  - CEF is disabled automatically when uRFP is enabled and TCAM is fully utilized.

- When you enter the **ip http secure-server** command (or if the system reads it from the startup configuration), the device searches for a persistent self-signed certificate during boot up.
  - If such a certificate does not exist and the device's hostname and default_domain are 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 differs from the FQDN in the certificate, the existing persistent self-signed certificate is replaced with a new one with the updated FQDN. Be aware that the existing key pair is used in the new certificate.

  On a switch that supports redundancy, the generation of the self-signed certificate occurs independently on the active and the standby supervisor engines, and the certificates differ. After switchover, the HTTP client that holds the old certificate cannot connect to the HTTPS server.

  Workaround: Reconnect. CSCsb11964

- 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 enter the **qos account layer2 encapsulation** command.

  Workaround: None. CSCsg58526

- When hard-coded 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 appears 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)

- When performing an ISSU upgrade and the versions of the active and standby supervisor engines differ, you see the following message 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

- An IP unnumbered configuration is lost after a switch reloads.

  Workarounds: Do one of the following:

  – After a reload, copy the startup-config to the running-config.

  – Use a loopback interface as the target of the **ip unnumbered** command.

  – Change the CLI configuration so that during bootup the router port is created first.

  CSCsq63051

- In SSO mode, when a port channel is created, deleted, and recreated on an active supervisor engine with the same channel number, the standby port channel state goes out of sync. After a switch over, the following message displays:

  ```
  %PM-4-PORT_INCONSISTENT: STANDBY:Port is inconsistent:
  ```

  Workaround: When the port channel starts to flap, enter **shut** and **no shut** on the port channel. After the first switchover and after deleting the port channel, create a new channel. CSCsr00333

- When you remove a line card containing ports configured with IGMP snooping while booting a standby supervisor engine, the active supervisor engine does not synchronize this configuration to the standby supervisor engine as a part of a bulk synchronization. When you reinstall the line card, the configuration in the active and standby supervisor engines will differ.

  Workaround: Do one of the following:

  – Reload the standby switch again with the line card in place.

  – Remove and reenter the commands on the active supervisor engine. The standby supervisor engine will acquire this change. CSCsv44866

- After posture validation succeeds, the following benign traceback messages may appear after you unconfigure the **global RADIUS** and **IP device tracking** commands:

  ```
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.101   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  %SM-4-BADEVENT: Event 'eouAAAAuthor' is invalid for the current state 'eou_abort':
  eou_auth 4.1.0.102   Traceback= 101D9A88 10B76BB0 10B76FE0 10B7A114 10B7A340 1066A678
  106617F8
  ```

  This applies to classic or E-series Catalyst 4500 supervisor engines running Cisco IOS Release 12.2(50)SG

  Workaround: None. CSCsw14005

- The host's MAC address is not synchronized to the standby supervisor engine after you unconfigure 802.1X on the port and reconnect the host to a IP phone (with CDP port status TLV support) that is connected to the switch.

  If the switch were to run a supervisor switchover while in this state, the host's MAC address would not be present in the new active supervisor engine's MAC address table, causing possible connectivity interruption on the host.

  Workaround: Enter the **shutdown** command, followed by the **no shutdown** command on the interface. This triggers relearning and synchronizing of the host's MAC to the standby supervisor engine. CSCsw91661

- On a wireless control system (WCS), some device information is incorrectly displayed for PCs sitting behind an lldp-med capable phone. Specifically, WCS displays the phone's serial number, model number, and software version in the PC's device information. All other information about the PC is correctly displayed on WCS.

  This only happens when the switch is running network mobility service protocol (nmsp). It does not happen if the phone is CDP enabled.

  Workaround: Use the VLAN ID or name to differentiate the IP phone and the PC sitting behind the phone on the WCS.

  The IP phone is detected on the voice VLAN, and the displayed information of serial number, model number, and software version is correct. However, a PC sitting behind the phone is detected on a data VLAN, and the displayed device information is wrong and should be ignored.

  CSCsz34522

- If *time* is not specified in the **link debounce** command, the default value depends on the supervisor engine. The default is 10 mS for a Catalyst 4900M switch, Supervisor Engine 6-E, and Supervisor Engine 6L-E. The default is 100 mS for all other supervisor engines.

  Despite the different default value, you can configure any value in the time range.

  Workaround: None. CSCte51948

- On a peer interface on a Catalyst 4948E Ethernet Switch, if errdisabled mode flap detection is set to a very small number (such as 2 flaps in 10 sec), a 10GE link flap may cause the peer interface to enter the errdisabled state.

  Workarounds: The Cisco switch default link-flap detection value is 5 flaps in 10 seconds. Use the default value or larger numbers. CSCtg07677

- After you have enabled EPM logging and the client is authenticated via MAB or Webauth, the value of AUTHTYPE is DOT1X in EPM syslog messages irrespective of the authentication method.

  Similarly, the **show epm sessions** command always displays the authentication method as DOT1X.

  Workaround: To view the authentication method used for a client, enter the **show authentication sessions** command. CSCsx42157

- With CFM enabled globally as well as on an ingress interface, CFM packets received on the interface are not policed with hardware control plane policing.

  Workaround: None. CSCso93282

- When either the RADIUS-server test feature is enabled or RADIUS-server dead-criteria is configured, and either RADIUS-server deadtime is set to 0 or not configured, the RADIUS-server status is not properly relayed to AAA.

  Workaround: Configure both dead-criteria and deadtime.

  ```
  radius-server dead-criteria
  radius-server deadtime
  ```

  CSCtl06706

- Occasionally, if you use an X2 SR transceiver on a WS-X4706-10GE running Cisco IOS Release 12.2(40)SG, you observe CRC errors after a reload or power cycle upon inserting the card or X2.

  Workaround: Reinsert the X2. CSCsk43618

- Uplinks go down when you upgrade the ROMMON of an WS-X45-SUP6-E supervisor from version 12.2(40r)SG1 to a later version.

This behavior occurs in a redundant switch when the active supervisor engine is running Cisco IOS, the standby supervisor engine is in ROMMON, and the standby supervisor engine's ROMMON is upgraded from version 0.34 or to a later version. The upgrade process causes the uplinks on the standby supervisor engine to go down but the active supervisor engine is unaware of this.

Workarounds: To resume normal operation, do one of the following:

- Reload both supervisor engines with the **redundancy reload shelf** command.
- Power-cycle the standby supervisor engine by briefly pulling it from the chassis.

There is *no* workaround for the link flap issue. CSCsm81875

- Changing the flow control configuration with traffic and pause frames causes some traffic loss.

  This problem can happen when pause frames are sent to a switch port and the flow control receive configuration is toggled on a 10-Gigabit Ethernet port.

  Workaround: Change the flow control receive configuration when no traffic exists. CSCso71647

- When you configure **vlan dot1q tag native** globally on Supervisor Engine 6-E, MST control packets are tagged on egress on the native VLAN. This conflicts with 802.1s. The Cisco 7600 Series router drops its MST proposal agreements (because it expects the native VLAN MST control packets to be untagged), causing 30 seconds of traffic loss while spanning tree converges.

  Workaround: Disable native VLAN tagging on the trunk port of the switch by entering the **no switchport trunk native vlan tag** command. CSCsz12611

- If a large number of VLAN mappings are configured, a member port might fail to join a port channel and no warning is issued.

  Workaround: Reduce the number of VLAN mappings. CSCtn56208

- If an interface whose IP address is being used as the router ID is deleted or shuts down, and you configure a service group with a multicast group address, packet redirection to CE stops and packets are forwarded directly to the destination.

  Workaround: Unconfigure and reconfigure the service group. CSCtn88087

- Global WCCP service configuration fails to enable (WCCP global configuration is accepted but nvgen fails) on a newly deployed switch if the switch is not enabled for SVI or a Layer 3 interface.

  Workaround: Enable a Layer 3 interface in the running configuration. CSCsc88636.

- If you use the **quick** option in the **issu changeversion** command, the following might occur:
  - Links flap for various Layer 3 protocols.
  - A traffic loss of several seconds is observed during the upgrade process.

  Workaround: Do not use the **quick** option with the **issu changeversion** command. CSCto51562

- When you enter the **ip pim register-rate-limit** command, the following error message displays:

  ```
  'Failed to configure service policy on register tunnel' and 'STANDBY:Failed to
  configure service policy on register tunnel'.
  ```

  Workaround: None. The **ip pim register-rate-limit** command does not function. CSCub32679

- For packets with the same ingress and egress Layer 3 interface, ingress QoS marking policy does not work.

  Workaround: Turn off ICMP redirect through the **ip redirect** command. CSCua71929

- While configuring an IPv6 access-list, if you specify **hardware statistics** as the first statement in v6 access-list mode (i.e. before issuing any other v6 ACE statement), it will not take effect. Similarly, your hardware statistics configuration will be missing from the output of the **show running** command.

  You will not experience this behavior with IPv4 access lists.

  Workaround: During IPv6 access-list configuration, configure at least one IPv6 ACE before the "hardware statistics" statement. CSCuc53234

- When an IPv6 FHS policy is applied on a VLAN and an EtherChannel port is part of that VLAN, packets received by EtherChannel (from neighbors) are not bridged across the local switch.

  Workaround: Apply FHS policies on a non EtherChannel port rather than a VLAN. CSCua53148

- Memory allocation failures can occur if more than 16K IPv6 multicast snooping entries are present.

  Workaround: None. CSCuc77376

- For any configuration where the source-interface keyword is used, if you provide an SVI that is associated with a secondary private VLAN, configuration involving the secondary VLAN may be lost when the switch is reloaded. In such scenarios, always use the primary private VLAN.

- The **show interface capabilities** command output does not show the correct linecard model.

  Workaround: Observe the **show module** command output. CSCua79513

- When performing an ISSU between any releases prior to Cisco IOS 15.1(1)SG or 3.3.0SG to release Cisco IOS 15.1(1)SG (or 3.3.0SG) or higher, a switch performing multicast routing may persistently drop traffic after the upgrade completes. You can recover multicast traffic by reloading the chassis. Alternately, you can remove all multicast configuration prior to ISSU, and add it back when ISSU completes. CSCuj42672

- When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may crash. As a workaround, disable the logging discriminator on the device (CSCur45606, CSCur28336).

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://tools.cisco.com/security/center/publicationListing

Cisco Bug Search Tool

The Bug Search Tool (BST), which is the online successor to Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat listed in this document:

1. Access the BST (use your Cisco user ID and password) at https://tools.cisco.com/bugsearch/.
2. Enter the bug ID in the **Search For:** field.

Open Caveats for Cisco IOS Release 15.2(2)Ex

Bug ID	Headline
CSCvk16783	Standby Supervisor is continuously crashing after upgrading to throttle build.

Resolved Caveats for Cisco IOS Release 15.2(2)E10

Bug ID	Headline
CSCvn72973	Device is getting crashed on the "cts role-based enforcement"
CSCvo09436	Active supervisor crashing while DFE training on Standby SUP
CSCvp19855	Crash when removing police action from policy-map

Resolved Caveats for Cisco IOS Release 15.2(2)E9

Bug ID	Headline
CSCvb59372	Double-free of VTY context causes a software-forced crash
CSCvd78456	Span config lost after reboot when using interface ranges
CSCvd96099	DOT1X %DATACORRUPTION-1-DATAINCONSISTENCY: copy error session_mgr
CSCve58352	Crash at the Ethernet Bridge Management Port
CSCvg74926	4510 Sup 8 sending invalid LACP mac-ID, generates MULTIPLE_NEIGHBORS upstream
CSCvg79459	Automate-tester does not send probes when the server is dead.
CSCvh04891	VSS Switch crash at boot time when CR (i.e. ' r') character is present in the startup-configuration
CSCvh79168	Crash on numPolicersPerBank with Invalid policerBaseIndex
CSCvh89534	4500 Sup 8E DACL applied to the incorrect interface.
CSCvh95816	crash due to access list changes
CSCvi06070	OSPF and BGP keeps flapping ever few seconds when BFD is enabled on Cat4k device
CSCvj25236	IPDT flapping after upgrade to 15.2(2)E7
CSCvj29126	RADIUS client on network fails to solicit PAC key from CTS even though the device has a valid PAC

Resolved Caveats for Cisco IOS Release 15.2(2)E8

Bug ID	Headline
CSCuz11275	4500 Switch Crash after Enabling Performance Monitoring.
CSCuz68659	unexpected packets seen while learning the mcast traffic.
CSCvc40729	Cat 4500x 3.6.2 - reloads unexpectedly on Cat4k Mgmt HiPri with Interrupt level Malloc.
CSCve37498	Switch sends duplicate accounting message, that causing ISE to generate Misconfigured NAS Alarms.
CSCve37653	4500 in RPR causing SNMP Input queue full errors and eicore timeouts.
CSCve54486	Crash when attempting to assign nonexistent/shutdown VLAN to 802.1x port.
CSCve80873	Service Policy disappears from 10G interface when neighbor port flaps, from 03.06.05.E & onwards.
CSCvf02423	C4500 - 03.06.06.E / 15.2(2)E6 - High CPU due to KxAclPathMan reprogr, KxAclPathMan update.
CSCvf18046	sticky timer stops if connected device moved from one port to other within timer expiry.
CSCvf76512	Option 82 circuit-id-tag restricted by 6 bytes.
CSCvf83057	Interface flaps once after the port change status from admin down to up.

Bug ID	Headline
CSCvf96579	2960:AAARadius authentication fails with "switchport voice vlan dot1p" command.
CSCvg70852	Unknown MAC addresses appear on port when trying to authenticate using dot1x.

Resolved Caveats for Cisco IOS Release 15.2(2)E7

Bug ID	Headline
CSCvc88353	QoS TCAM does not share labels with CTS applied .
CSCty18171	SNMP poll of CISCO-PROCESS-MIB may cause high CPU and SNMP poll timeout.
CSCuu34535	Standby reloads on removing flow monitor.
CSCuv22571	Memory corruption crash in slaJitterPacketBuild.
CSCuw15256	IOS PKI: Certificate validation fails after reload.
CSCux81234	C4500 VSS port mapped to Drop aggport when the Aggregate port id 656.
CSCuz89309	WS-X4648-RJ45V+E interface becomes unusable after INLINEPOWEROVERDRAWN.
CSCvb76862	4500VSS: Traffic Dropped on VSL due to SPTDROP.
CSCvb97901	4500X 3.8.2 TX-Queue's zero out after multiple reloads.
CSCvd01598	Tacacs+ Timeout Retransmission is done 3 times prior marking server down.
CSCvd32541	4500 :: next hop for static route mis-programmed.
CSCvd35291	Removal of "access-session template monitor" creates Drop MAC entries in CAM table.
CSCvd66637	VSS Cat4500 Standby Supervisor memory leak in EICORED process.
CSCve04704	Session blocked in Pending Deletion state due to SM Accounting Feature.

Resolved Caveats for Cisco IOS Release 15.2(2)E6

No caveats were resolved in this release.

Resolved Caveats for Cisco IOS Release 15.2(2)E5a

Bug ID	Headline
CSCvb19326	NTP leap second addition is not working during leap second event
CSCuv87976	CLI Knob for handling leap second add/delete ignore/ handle
CSCvb29204	BenignCertain on IOS and IOS-XE

Resolved Caveats for Cisco IOS Release 15.2(2)E5

Identifier	Description
CSCut93424	CAT4500 - Flexible Netflow start/end time inaccuracy
CSCur57853	4500 VSS cannot send snmp trap when active is down
CSCuy23874	4500: Auto-negotiation issue: port going to 100Mbps instead of 1Gbps
CSCuy52010	7940G phones learn mac in data vlan when EEE is disabled
CSCuw17135	Cat4k SUP7L-E CPU temperature sensor failed
CSCuy01942	wBulk dACL causes intermittent MAB Authentication with 4506 SUP_6
CSCuy19990	IOS 15.2 802.1x critical vlan feature - reinitialize is not working
CSCuw09327	Crash while config ACL- invalid mem access K5CpuEventCodeInputAclCopy
CSCuz02962	Increasing acl-ack-contexts for auth sessions causing memory exhaustion

Resolved Caveats for Cisco IOS Release 15.2(2)E4

Bug ID	Headline
CSCuv39850	Switch crashes @auth_mgr_show_method_status_list
CSCuv87875	Crash seen@Galios_newIosHeapMemoryRef on assigning DACL on reauth
CSCuw58095	AMUR MR3: SUP8E crash at dot1x_switch_handle_vlan_removal
CSCut57300	With sec ip in SVI, routed packet is not flooded back on incoming port
CSCut71405	IGMP packet not matched by ingress QoS policy if IGMP Snooping enabled
CSCuu85298	FIB/LFIB inconcistency after BGP flap
CSCuv07111	IOS and IOS-XE devices changing the next-hop on BGP route with own IP
CSCuv07620	4500X VSS won't notify about license mismatch
CSCuu21448	ISIS Metric with Multiple instances using ciiCircLevelMetric OID
CSCuu42267	vstack status shows duplicate entries for a single PID
CSCuv23475	CPUHOG and crash on "no network 0.0.0.0" with vnet configuration on intf
CSCuu68776	Multicast boundary filter-autorp broken / WS-C4500X / 15.2(1)E 15.2(3)E1
CSCuv00910	bgp afi1/safi1 and afi1/saf4 only peers in the same update-group
CSCuv07796	Truncated output of 'show platform cpu packet buffered'
CSCuv16769	ISIS: Old path not deleted in Global RIB when new path is filtered out
CSCuv19773	"nmsp attach suppress" not being added into run-config on WS-C3850-24P
CSCuv31135	Disable connected-check in one side only makes route as unreachable
CSCuv32845	no message display even unable to allocate memory for vlan mapping
CSCuw06073	EOL CRLF in startup-config breaks 4500x VSS
CSCuv46710	Segmentation Fault in Auth Manager
CSCuv50834	High CPU due to hung NMSP Session

CSCuw21115	4500/WS-X4724-SFP-E port flaps when GLC-GE-100FX is inserted
CSCuw36865	L2 switched traffic matched by L3 SVI VACL in the output direction
CSCuw39020	access-session vlan-assignment ignore-errors breaks dynamic vlan assign
CSCuv76906	"bfd" disappears after issuing "snmp-server host x.x.x.x ABC bfd"
CSCuw09006	Voice Vlan bocked with NEAT Configuration
CSCuw48407	47xx line card failing complete diagnostics after temp sensor failure
CSCuw73525	3650 DHCPv6 Guard does not block rogue DHCP server to provide IPv6 addr
CSCtz92812	"ip vrf Liin-vrf" in running-config on a VSS system
CSCub56668	Handle C4K_HWFLOWMAN-3-NFEINTERRUPTSTATUS: module: fi InterruptStatus:
CSCuj81067	memory leak in crypto_create_pkcs7_msg
CSCum41167	Importing multipath routes changes next-hop to 0.0.0.0 and traffic fails
CSCuw06202	Vstack Download-Config causes 4500 to become unresponsive
CSCuq36627	WAAS Express:Failed to create SSL session. (no available resources)
CSCuo93205	Enable SSL Server Identity Check during SSL handshake
CSCur28336	Memory leak and possible crash when using a logging discriminator
CSCtg15739	Failed sessions are not removed in multi-auth mode
CSCur45606	logging discriminator doesn't work
CSCtb44674	High CPU due to SA-MISS event caused by own mac address packets received
CSCuq46932	Crash on dhcpd_find_binding_by_hw
CSCuu55421	Error - The FRULink 10G Service Module (C3KX-SM-10G) is not responding
CSCuv19258	DACL may not work under IBNS 2.0
CSCuv47729	Packet gets flooded back to the ingress port, when a MEC port is down
CSCuv50669	Port-security blocks X/Y/38 port due to incorrect MAC address
CSCuw52729	Enabling auto qos causes "line vty 0 4" length set to 0
CSCux18867	4500 3.6.0 False port-security alarms on standby supervisor
CSCux38988	redundancy config-sync failures mcl define interface range adds fifth ,

Resolved Caveats for Cisco IOS Release 15.2(2)E3

Bug ID	Headline
CSCum56902	Device crashes when classes removed from a policy-map
CSCum65703	Inconsistency on config "privilege" commands as seen in running-config
CSCup66629	Traceback @psecure_platform_delete_all_addrs on executing neg events
CSCup81878	Line by Line Sync fails while deleting dynamic NTP peer
CSCuq31722	The show platform software flood profile command caused SUP8 to crash
CSCuq54573	Service Policy disappears from Running Configuration of the interface
CSCur58372	“snmp-server enable traps syslog” shows in "show run all" output after removal

Bug ID	Headline
CSCur59242	Device crashes due to tplus_client_stop_timer
CSCus13476	CSR handled only one MACSec interface's authentication
CSCus13924	Device crashes while configuring 'Identity' commands
CSCus23125	MAC not learnt after removal of auth config
CSCus32213	CTS manual link does not come up
CSCus47009	Switch does not increment the "Received on untrusted ports" DHCP counter
CSCus79132	Dot1x authentication legacy behavior broken
CSCut05808	UDP(1975) causes Error msg %IPC-2-INVALIDZONE
CSCut10251	Some commands are not in running-config after AUTOINSTALL finishes
CSCut11679	FFM memory leak is observed when WCCP flaps
CSCut13064	BPDU filter does not work on output port when STP is disabled
CSCut13753	ACLs not syncing to the member switches on stack reload or member reload
CSCut20271	Device responds to ARP request from management port
CSCut27272	CPUHOG and crash due to Auth Manager process
CSCut45453	ICMPv6 replies are blocked
CSCut64189	Device TELNET can enter Privileged Mode without Enable Password
CSCuu92757	4500 Sup8 MAB not triggered with"authentication control-direction in"
CSCut79680	The **ip default-gateway** command is not seen in running-config after AUTOINSTALL
CSCut87425	CPU hog in "EEM TCL Proc" after TCL script termination with long runtime
CSCuu22144	Vlan1 IP apply method inconsistencies across Static / DHCP / TFTP
CSCuu48400	HW CoPP counters are not incrementing
CSCuu50392	Auth Manager memory leak with ISE authentication
CSCuu90639	IP address is missing by end of Autoinstall
CSCuu92251	Removing auth mgr configs stops MAC learning on port (no MACs on MATM)
CSCuu92757	4500 Sup8 MAB not triggered with"authentication control-direction in"
CSCuv06451	IOSd crash in eap_auth_terminal_state calling free_internal

Resolved Caveats for Cisco IOS Release 15.2(2)E2

Bug ID	Headline
CSCus75890	Switch does not resync to NTP server after clock set command or reload
CSCur20444	I/O memory leak due to DHCPv6 packets
CSCur48634	HA fails due to bulk synch failure with encrypted password
CSCus57511	Switch detects high temp, and SNMP trap causes shutdown
CSCug90126	Switch returns incorrect ciscoEnvMonSupplyState SNMP values for 6000/4200 W PSUU.
CSCul29298	Delayed detection of LinkDown message on peer interfaces

Bug ID	Headline
CSCuq80812	Incomplete ARP reply received on an active Flex Link port
CSCsv36934	BRIDGE-MIB query does not return information for inactive ports
CSCus32292	4506-E | SUP7L-E | 03.06.00.E | Crash - ffm ACL
CSCui99162	When IP device tracking is enabled, ARP probe response floods the VLAN
CSCtf75400	Wrong output for show platform software etherchannel port-channel n map
CSCup24975	Outage due to inconsistent software and hardware RX MTU threshold
CSCur58074	Some SFPs are not recognized when inserted into random ports on a switch
CSCuq04533	Cost for secondary VLANs is lost after each reload
CSCur21848	WCCP stops redirecting traffic when eighth port added to service group
CSCur84243	WS-X4640-CSFP-E ports (Tx) are disabled on start-up

Resolved Caveats for Cisco IOS Release 15.2(2)E1

Bug ID	Headline
CSCuc03836	Switch reports SYS-2-MALLOCFAIL error for a very large amount of memory
CSCum47115	EtherType 888e unicast can not pass 2960 with new releases
CSCum80951	TCAM is not sharing when same policy is applied to multiple interfaces
CSCun80959	Desg port on the RootBridge experienced block forward for 30 sec
CSCuo51767	REP preemption is not triggered with link state change
CSCuo80260	Call-home message fails; returns "Unknown" serial number
CSCuo89407	Problem with adding new ports to a channel group.
CSCup48832	Identical IPv6 DHCP remote ID for L2 ports running source-guard/snooping
CSCup96299	IPv6 Multicast RIB entry refer to wrong distance
CSCuq02796	4500X VSS failure after adding members to port-channel
CSCuq03562	PBR: Not working in XE 3.5.0E under IPBASE license
CSCuq10827	C3560X cHsrpGrpStandbyState is incorrect
CSCuq32728	3.6.0 - IP phones reboots continuously
CSCuq39071	Mcast packet loss when other receiver leaves group in IGMPv3
CSCuq44784	Mingla2: Storm-control on EC suspended post reload
CSCur00722	Hard Reset of the Active Sup cause switch to power cycle

Resolved Caveats for Cisco IOS Release 15.2(2)E

Bug ID	Headline
CSCta61825	Blocking of unknown multicast flooding breaks ARP resolution
CSCua89658	ctrlplane policing is not working when MLD snooping is enabled

Bug ID	Headline
CSCub85948	Memory leak caused by CDP, LLDP or DHCP traffic
CSCuc65538	mcast dest mac incorrect on egress for packets ingressing a GR
CSCty67871	Baseboard links remain up on improper uplink module removal
CSCub44553	CPU spike seen while sending the multicast traffic to 10k Groups.
CSCub63571	AdjSameIfFail packets in a user defined vnet are dropped
CSCuc49150	User can attach input QoS policy to VSL ports, but cannot dettach it
CSCuf08112	Cat4k Active Sup crash with multi telnet session cli **show power module**
CSCul95289	Console / VTY / SSH session hangs on **show** command

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//en/US/products/hw/switches/ps4324/index.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

- For information about individual switching modules and supervisors, refer to the *Catalyst 4500 Series Module Installation Guide* at:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/hardware/configuration/notes/OL_25315.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

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

Software documents for the Catalyst 4500 Classic, Catalyst 4500 E-Series, Catalyst 4900 Series, and Catalyst 4500-X Series 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

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:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

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 15.2(1)Ex