Release Notes for Cisco IOS Release 15.2(1)SY

February 18, 2019

Note

- See this product bulletin for information about the standard maintenance and extended maintenance 15.2SY releases:

  http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-15-0sy/product_bulletin_c25-687567.html

- For general product information about the Catalyst 6500 series switches, refer to these product bulletins: Unsupported Features, page 50

  http://www.cisco.com/c/en/us/products/switches/catalyst-6500-series-switches/literature.html

The most current version of this document is available on Cisco.com at this URL:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/release_notes/release_notes.html

Caution Cisco IOS supports redundant configurations with identical supervisor engines. If they are not identical, one supervisor engine will boot first and become active and hold the other in a reset condition.

Contents

This publication consists of these sections:

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

Chronological List of Releases

Note

- See the "Images and Feature Sets" section on page 40 for information about which releases are deferred.

This is a chronological list of the 15.2SY releases:

- Release 15.2(1)SY8—18 February 2019
- Release 15.2(1)SY7—20 August 2018
- Release 15.2(1)SY6—28 February 2018
- Release 15.2(1)SY5—25 August 2017
- Release 15.2(1)SY4—21 April 2017
- Release 15.2(1)SY3—24 October 2016
- Release 15.2(1)SY2—07 April 2016
- Release 15.2(1)SY1a—06 Oct 2015
- Release 15.2(1)SY1—14 May 2015
- Release 15.2(1)SY0a—31 Mar 2015
- Release 15.2(1)SY—19 Dec 2014

FPD-Image Dependant Modules

FPD image packages update FPD images. If a discrepancy exists between an FPD image and the Cisco IOS image, the module that has the FPD discrepancy is deactivated until the discrepancy is resolved. These modules use FPD images:

- ASA services module (WS-SVC-ASA-SM1-K9)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/release/notes/asarn85.html
- Network Analysis Module 3 (WS-SVC-NAM3-6G-K9)—See these publications:

  http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-analysis-module-software/products-release-notes-list.html

Supported Hardware

These sections describe the hardware supported in Release 15.1(2)SY1 and later releases:

Note Enter the **show power** command to display current system power usage.

Supervisor Engines, PFCs, DFCs, and CFC

Supervisor Engine 2T-10GE

Note For information about DRAM requirements on all supervisor engines, see this publication:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/qa_c67_457347.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
VS-S2T-10G-XL	Supervisor Engine 2T-10GE with PFC4XL	15.0(1)SY
VS-S2T-10G	Supervisor Engine 2T-10GE with PFC4	

Features

- One of these policy feature cards:
  - Policy Feature Card 4XL (PFC4XL)
  - Policy Feature Card 4 (PFC4)

  See the "Policy Feature Cards Supported with Supervisor Engine 2T" section on page 5.
- Supports 2-Tbps switch fabric connectivity.
- 2-GB DRAM.
- Internal 1-GB bootflash (**bootdisk:**).

- One external slot:
  - **disk0:**
  - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 2T-10GE.
- Console ports:
  - EIA/TIA-232 (RS-232) port
  - USB port
- Ports 1, 2, and 3:
  - QoS architecture: **2q4t**/**1p3q4t**
  - Ports 1, 2, and 3: Gigabit Ethernet SFP (fiber SFP or 1000 Mbps RJ-45 SFP)
- Ports 4 and 5:
  - Support for 10-Gigabit Ethernet X2 tranceivers
  - QoS architecture:
    - With ports 1, 2, and 3 enabled: **2q4t**/**1p3q4t**
    - With ports 1, 2, and 3 disabled: **8q4t**/**1p7q4t**
- One port group: ports 1 through 5

Note See the *Supervisor Engine 2T-10GE Connectivity Management Processor Configuration Guide* for information about the 10/100/1000 Mbps RJ-45 port.

- Connectivity Management Processor (CMP)—See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/cmp_configuration/guide/sup2T_10GEcmp.html

Supervisor Engine 2T-10GE Restrictions

- The 1-Gigabit Ethernet ports and the 10-Gigabit Ethernet ports have the same QoS port architecture (**2q4t**/**1p3q4t**) unless you disable the 1-Gigabit Ethernet ports with the **platform qos 10g-only** global configuration command. With the 1-Gigabit Ethernet ports disabled, the QoS port architecture of the 10-Gigabit Ethernet ports is **8q4t**/**1p7q4t**.
- In RPR redundancy mode, the ports on a Supervisor Engine 2T-10GE in standby mode are disabled.

Policy Feature Cards Supported with Supervisor Engine 2T

- Policy Feature Card 4 Guidelines and Restrictions, page 5
- Policy Feature Card 4XL, page 7
- Policy Feature Card 4, page 7

Policy Feature Card 4 Guidelines and Restrictions

- The PFC4 supports a theoretical maximum of 131,072 (128K) MAC addresses with 118,000 (115.2K) MAC addresses as the recommended maximum.

- The PFC4 partitions the hardware FIB table to route IPv4 unicast, IPv4 multicast, MPLS, and IPv6 unicast and multicast traffic in hardware. Traffic for routes that do not have entries in the hardware FIB table are processed by the route processor in software.

  The defaults for XL mode are:

  – IPv4 unicast and MPLS: 512,000 routes

  – IPv4 multicast and IPv6 unicast and multicast: 256,000 routes

  The defaults for Non-XL mode are:

  – IPv4 unicast and MPLS: 192,000 routes

  – IPv4 multicast and IPv6 unicast and multicast: 32,000 routes

  Note The size of the global internet routing table plus any local routes might exceed the non-XL mode default partition sizes.

  These are the theoretical maximum numbers of routes for the supported protocols (the maximums are not supported simultaneously):

  – XL mode:

    • IPv4 and MPLS: Up to 1,007,000 routes

    • IPv4 multicast and IPv6 unicast and multicast: Up to 503,000 routes

  – Non-XL mode:

    • IPv4 and MPLS: Up to 239,000 routes

    • IPv4 multicast and IPv6 unicast and multicast: Up to 119,000 routes

  Enter the **platform cef maximum-routes** command to repartition the hardware FIB table. IPv4 unicast and MPLS require one hardware FIB table entry per route. IPv4 multicast and IPv6 unicast and multicast require two hardware FIB table entries per route. Changing the partition for one protocol makes corresponding changes in the partitions of the other protocols. You must enter the **reload** command to put configuration changes made with the **platform cef maximum-routes** command into effect.

  Note With a non-XL-mode system, if your requirements cannot be met by repartitioning the hardware FIB table, upgrade components as necessary to operate in XL mode.

- You cannot use one type of PFC on one supervisor engine and a different type on the other supervisor engine for redundancy. You must use identical policy feature cards for redundancy.
- PFC4—These restrictions apply to a configuration with a PFC4 and these DFCs:
  – PFC4 and DFC4—No restrictions (PFC4 mode).
  – PFC4 and DFC4XL—The PFC4 restricts DFC4XL functionality: the DFC4XL functions as a DFC4 (PFC4 mode).
- PFC4XL—These restrictions apply to a configuration with a PFC4XL and these DFCs:
  – PFC4XL and DFC4—PFC4XL functionality is restricted by the DFC4: after a reload with a DFC4-equipped module installed, the PFC4XL functions as a PFC4 (PFC4 mode).
  – PFC4XL and DFC4XL—No restrictions (PFC4XL mode).

- Switching modules that you install after bootup that are equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode remain powered down.
- You must reboot to use a switching module equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode.
- Enter the **show platform hardware pfc mode** command to display the PFC mode.
- FIB TCAM exception may be thrown in case of a route churn where TCAM utilization is more than 80% of the total utilization. This limitation is applicable to DFC TCAM on XL line cards. If FIB TCAM exception is thrown for a transit route for IPv4 or IPv6 or MPLS traffic, the route does not get installed in FIB and connectivity gets affected. This can result in elevated CPU usage due to software switching.

Policy Feature Card 4XL

Product ID (append "=" for spares)	Product Description	Minimum Software Version
VS-F6K-PFC4XL	Policy Feature Card 4XL (PFC4XL) **Note** Use VS-F6K-PFC4XL= to upgrade to a PFC4XL.	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Policy Feature Card 4

Product ID (append "=" for spares)	Product Description	Minimum Software Version
VS-F6K-PFC4	Policy Feature Card 4 (PFC4)	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Distributed Forwarding Cards Supported with Supervisor Engine 2T

- Distributed Forwarding Card 4XL, page 8
- Distributed Forwarding Card 4, page 8

Note

- See the "Policy Feature Cards Supported with Supervisor Engine 2T" section on page 5 for Policy Feature Cards (PFC) and Distributed Forwarding Card (DFC) restrictions.
- The DFC4 uses memory that is installed on the switching module.
- For more information about the DFCs, see these documents:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/OL_24918.html

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/catalyst-6500-series-supervisor-engine-2t/data_sheet_c78-648214.html

Distributed Forwarding Card 4XL

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6K-DFC4-EXL **WS-F6K-DFC4-AXL**	Distributed Forwarding Card 4XL (DFC4XL)	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Distributed Forwarding Card 4

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6K-DFC4-E **WS-F6K-DFC4-A**	Distributed Forwarding Card 4 (DFC4)	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Centralized Forwarding Card (WS-F6700-CFC)

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6700-CFC	Centralized Forwarding Card (CFC) for use on CEF720 modules	
	With Supervisor Engine 2T-10GE	15.0(1)SY

40-Gigabit Ethernet Switching Modules

WS-X6904-40G-2T 4-Port 40-Gigabit Ethernet Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6904-40G-2TXL (Has WS-F6K-DFC4-EXL) **WS-X6904-40G-2T** (Has WS-F6K-DFC4-E)	4-port 40-Gigabit Ethernet module	
	With Supervisor Engine 2T-10GE	15.0(1)SY1

- WS-X6904-40G-2T and WS-X6904-40G-2TXL are the orderable product IDs.
- The front panel is labeled WS-X6904-40G.

- Cisco IOS software commands display WS-X6904-40G with either WS-F6K-DFC4-E or WS-F6K-DFC4-EXL.
- Has hardware abstraction layer (HAL) support.
- QoS port architecture (Rx/Tx): **1p7q4t** or **2p6q4t/1p7q4t** or **2p6q4t**
- Dual switch-fabric connections:
  - Fabric Channel #1: Ports 1 and 2 or 5 through 12
  - Fabric Channel #2: Ports 3 and 4 or 13 through 20
- Number of ports: 4 or 16
  Number of port groups: 2
  Port per port group:
  –Ports 1 and 2 or 5 through 12
  –Ports 3 and 4 or 13 through 20
- dCEF2T.
- In a 3-slot chassis, supported only with WS-C6503-E hardware revision 1.3 or higher.
- Upgrade to Release15.0(1)SY1 or later before installing WS-X6904-40G (see the "EFSU Compatibility" section on page 41).
- Each bay can support a CFP transceiver (supports one 40 Gigabit Ethernet port) or a FourX adapter (supports four 10 Gigabit Ethernet SFP+ transceivers).
- WS-X6904-40G supported modes (default mode is oversubscribed):
  - 40 Gigabit Ethernet oversubscribed mode:
    —Four 40 Gigabit Ethernet ports
    —Ports 1 through 4
  - 10 Gigabit Ethernet oversubscribed mode:
    —Sixteen 10 Gigabit Ethernet ports
    —Ports 5 through 20
  - Mixed 10/40 Gigabit Ethernet oversubscribed mode:
    —Left bays:
      –Either two 40 Gigabit Ethernet ports (1 and 2)
      –Or eight 10 Gigabit Ethernet ports (5 through 12)
    —Right bays:
      –Either two 40 Gigabit Ethernet ports (3 and 4)
      –Or eight 10 Gigabit Ethernet ports (13 through 20)
  - Performance mode:
    —Configurable per module or per bay:

      ```
      no hw-module slot slot_number oversubscription [port-group port_group_number]
      ```

    —Supported in the top left bay and top right bay.
    —Any of these combinations:
      –40 Gigabit Ethernet port 1 (top left bay) and port 3 (top right bay)
      –10 Gigabit Ethernet ports 5 through 9 (top left bay) and ports 13 through 16 (top right bay)
      –Top left bay: 40 Gigabit Ethernet port 1 or 10 Gigabit Ethernet ports 5 through 9
      Top right bay: 40 Gigabit Ethernet port 3 or 10 Gigabit Ethernet ports 13 through 16

  - 40 Gigabit Ethernet performance mode, 10 Gigabit Ethernet oversubscribed mode:
    —Either of these combinations:
    –Top left bay: 40 Gigabit Ethernet port 1
    Right bays: eight 10 Gigabit Ethernet ports (13 through 20)
    –Left bays: eight 10 Gigabit Ethernet ports (5 through 13)
    Top right bay: 40 Gigabit Ethernet port 3
  - 40 Gigabit Ethernet oversubscribed mode, 10 Gigabit Ethernet performance mode:
    —Either of these combinations:
    –Top left bay: four 10 Gigabit Ethernet ports (5 through 9)
    Right bays: two 40 Gigabit Ethernet ports (3 and 4)
    –Left bays: two 40 Gigabit Ethernet ports (1 and 2)
    Top right bay: four 10 Gigabit Ethernet ports (13 through 16)
- For more information about WS-X6904-40G, see these publications:
  40 Gigabit Ethernet on Cisco Catalyst 6500 Series Switches: How It Works
  40 Gigabit Ethernet Interface Module for Cisco Catalyst 6500 Series Switches Data Sheet

10-Gigabit Ethernet Switching Modules

Catalyst C6800-8P10G, Catalyst C6800-8P10G-XL

- C6800-8P10G and C6800-8P10G-XL are the orderable product IDs
- Cisco IOS software commands display C6800-8P10G or C6800-8P10G-XL
- QoS Architecture
  - Receive:
    1p7q4t (default)
    2p6q4t (configurable)
  - Transmit:
    1p7q4t (default)
    2p6q4t (configurable)
- Number of ports: 8
- Port Groups: 2
  - 2 port-sets per port group

  - Port-group 1: 1, 2, 3, 4
  - Port-group 2: 5, 6, 7, 8
- Oversubscription: Not Applicable
- Upgrade to Release15.2(1)SY or later before installing either C6800-8P10G or C6800-8P10G-XL
- Supported modes
  - In C6807-XL: 8 ports: line rate 1:1
  - In Catalyst 6500-E: 8 ports: line rate 1:1
- Number of forwarding engines: 1
- Port Buffers
  - 500 MB per port (Egress)
  - 2.5 MB per port (Ingress)

Catalyst C6800-16P10G, Catalyst C6800-16P10G-XL

- C6800-16P10G and C6800-16P10G-XL are the orderable product IDs
- Cisco IOS software commands display C6800-16P10G or C6800-16P10G-XL
- QoS Architecture
  - Receive:
    1p7q4t (default)
    2p6q4t (configurable)
  - Transmit:
    1p7q4t (default)
    2p6q4t (configurable)
- Number of ports: 16
- Port Groups: 2
  - 2 port-sets per port group
  - Port-group 1:
    1, 2, 3, 4
    5, 6, 7, 8
  - Port-group 2:
    9, 10, 11, 12
    13, 14, 15, 16
- Performance Mode: Yes, per-port group
- Upgrade to Release15.2(1)SY or later before installing either C6800-16P10G or C6800-16P10G-XL
- Supported modes
  - In C6807-XL:
    16 ports: oversubscription mode 2:1
    8 ports: performance mode 1:1
  - In Catalyst 6500-E:
    16 ports: oversubscription mode 2:1
    8 ports: performance mode 1:1

- Number of forwarding engines: 1
- Port Buffers
  - Oversubscription mode:
    250 MB per port (Egress)
    1.25 MB per port (Ingress)
  - Performance mode:
    500 MB per port (Egress)
    2.5 MB per port (Ingress)

Catalyst C6800-32P10G, Catalyst C6800-32P10G-XL

- C6800-32P10G and C6800-32P10G-XL are the orderable product IDs
- Cisco IOS software commands display C6800-32P10G or C6800-32P10G-XL
- QoS Architecture
  - Receive:
    1p7q4t (default)
    2p6q4t (configurable)
  - Transmit:
    1p7q4t (default)
    2p6q4t (configurable)
- Number of ports: 32
- Port Groups: 4
  - 2 port-sets per port group
  - Port-group 1:
    1, 3, 5, 7
    9,11, 13, 15
  - Port-group 2:
    2,4,6,8
    10, 12, 14, 16
  - Port-group 3:
    17,19,21,23
    25, 27, 29, 31
  - Port-group 4:
    18,20,22,24
    26, 28, 30, 32
- Performance Mode: Yes, per-port group
- Upgrade to Release15.2(1)SY or later before installing either C6800-32P10G or C6800-32P10G-XL
- Supported modes
  - In C6807-XL:
    32 ports: oversubscription mode 2:1
    16 ports: performance mode 1:1

  - In Catalyst 6500-E:
    32 ports: oversubscription mode 4:1
    16 ports: performance mode 2:1
- Number of forwarding engines: 2
- Port Buffers
  - Oversubscription mode:
    250 MB per port (Egress)
    1.2 MB per port (Ingress)
  - Performance mode:
    500 MB per port (Egress)
    2.5 MB per port (Ingress)

WS-X6908-10GE 8-Port 10-Gigabit Ethernet X2 Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6908-10G-XL (Has WS-F6K-DFC4-EXL) **WS-X6908-10G** (Has WS-F6K-DFC4-E)	8-port 10-Gigabit Ethernet X2 module	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- WS-X6908-10G and WS-X6908-10G-XL are the orderable product IDs.
- The front panel is labeled WS-X6908-10GE.
- Cisco IOS software commands display WS-X6908-10GE with either WS-F6K-DFC4-E or WS-F6K-DFC4-EXL.
- dCEF2T
- QoS port architecture (Rx/Tx): **8q4t/1p7q4t**
- Dual switch-fabric connections
  Fabric Channel #1: Ports 2, 3, 6, 8
  Fabric Channel #2: Ports 1, 4, 5, 7
- Number of ports: 8
  Number of port groups: 8
  Port ranges per port group: 1 port in each group
- In a 3-slot chassis, supported only with WS-C6503-E hardware revision 1.3 or higher.

WS-X6816-10T-2T, WS-X6716-10T 16-Port 10-Gigabit Ethernet Copper Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6816-10T-2TXL (Has WS-F6K-DFC4-EXL) **WS-X6716-10T-3CXL** (Must be upgraded with WS-F6K-DFC4-EXL=) **WS-X6816-10T-2T** (Has WS-F6K-DFC4-E) **WS-X6716-10T-3C** (Must be upgraded with WS-F6K-DFC4-E=)	16-port 10-Gigabit Ethernet copper (RJ-45) module	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- The orderable product IDs are:
  - WS-X6816-10T-2TXL
  - WS-X6816-10T-2T
  - WS-X6716-10T-3CXL
  - WS-X6716-10T-3C
- The front panel is labeled WS-X6716-10T.
- Cisco IOS software commands display WS-X6716-10T with any DFC.
- QoS port architecture (Rx/Tx):
  - Oversubscription mode: **1p7q2t/1p7q4t**
  - Performance mode: **8q4t/1p7q4t**
- Dual switch-fabric connections
  Fabric Channel #1: ports 1–8
  Fabric Channel #2: ports 9–16
- Number of ports: 16
  Number of port groups: 4
  Port ranges per port group: 1–4, 5–8, 9–12, 13–16
- When not configured in oversubscription mode, supported in virtual switch links.
- To configure port oversubscription, use the **hw-module slot** command.

WS-X6816-10G-2T, WS-X6716-10G 16-Port 10-Gigabit Ethernet X2 Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6816-10G-2TXL (Has WS-F6K-DFC4-EXL) **WS-X6716-10G-3CXL** (Must be upgraded with WS-F6K-DFC4-EXL=) **WS-X6816-10G-2T** **(Has WS-F6K-DFC4-E)** **WS-X6716-10G-3C** (Must be upgraded with WS-F6K-DFC4-E=)	16-port 10-Gigabit Ethernet X2 module	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- The orderable product IDs are:
  - WS-X6816-10G-2TXL
  - WS-X6816-10G-2T
  - WS-X6716-10G-3CXL
  - WS-X6716-10G-3C
- The front panel is labeled WS-X6716-10GE.
- Cisco IOS software commands display WS-X6716-10GE with any DFC.
- QoS port architecture (Rx/Tx):
  - Oversubscription mode: **1p7q2t/1p7q4t**
  - Performance mode: **8q4t/1p7q4t**
- Dual switch-fabric connections
  Fabric Channel #1: ports 1–8
  Fabric Channel #2: ports 9–16
- Number of ports: 16
  Number of port groups: 4
  Port ranges per port group: 1–4, 5–8, 9–12, 13–16
- When not configured in oversubscription mode, supported in virtual switch links.
- To configure port oversubscription, use the **hw-module slot** command.

WS-X6704-10GE 4-Port 10-Gigabit Ethernet XENPAK Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6704-10G	4-port 10-Gigabit Ethernet XENPAK With Supervisor Engine 2T-10GE	15.0(1)SY

- WS-X6704-10GE requires one of the following:
  - With Supervisor Engine 2T-10GE:
    - WS-F6K-DFC4-AXL
    - WS-F6K-DFC4-A
  - With any supervisor engine, WS-F6700-CFC
- Requires 512-MB DRAM with a WS-F6700-CFC (CSCtk82279). See this publication:

  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- QoS port architecture (Rx/Tx): **8q8t/1p7q8t**
- Dual switch-fabric connections:
  Fabric Channel #1: Ports 3 and 4
  Fabric Channel #2: Ports 1 and 2
- Number of ports: 4
  Number of port groups: 4
  Port ranges per port group: 1 port in each group
- WS-X6704-10G is the orderable product ID.
- The front panel is labeled WS-X6704-10GE.
- Cisco IOS software commands display WS-X6704-10GE with any DFC.
- On WS-X6704-10GE ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6704-10GE ports that interconnect network devices. (CSCsg86315)

Cisco Catalyst 6880-X Series Extensible Fixed Aggregation Switches

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
C6880-X-LE	16 10-Gigabit (SFP+)/1-Gigabit ports (SFP), four port card slots, two power supply slots. It supports standard FIB/ACL/NetFlow tables.	15.1(2)SY1
C6880-X	16 10-Gigabit (SFP+)/1-Gigabit ports (SFP), four port card slots, two power supply slots. It supports large FIB/ACL/NetFlow tables.	
C6880-X-LE-16P10G[1]	Multi rate port card with standard tables. This module has 16 10-Gigabit or 1-Gigabit module slots which support 1-Gigabit SFPs or 10-Gigabit SFP+ modules. Supported only on the Catalyst 6880-X-LE switch model.	15.1(2)SY2
C6880-X-16P10G[1]	Multi rate port card with XL tables. This module has 16 10-Gigabit or 1-Gigabit module slots which support 1-Gigabit SFPs or 10-Gigabit SFP+s modules. Supported only on the Catalyst 6880-X switch model.	

Product ID (append "=" for spares)	Product Description	Minimum Software Version

Note See these publications for more information:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/data_sheet_c78-728228.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/white_paper_c11-728540.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6880-x-switch/white_paper_c11-728541.html

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T.html

1. These port cards are supported only on the specified switch models and are not interoperable.

Cisco Catalyst 6807-XL Modular Switch

Product ID (append "=" for spares)	Product Description	Minimum Software Version
C6807-XL	7-slot modular chassis. The switch supports redundant power supply modules (AC-input), redundant supervisor engines, fan-tray, power supply convertor modules, clock modules, and voltage termination enhanced (VTT-E) modules	15.1(2)SY3

Note See these publications for more information:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6807-xl-switch/data_sheet_c78-728229.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6807-xl-switch/white_paper_c11-728264.html

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T.html

Instant Access Catalyst 6800ia Series Switches

Product ID (append "=" for spares)	Product Description	Minimum Software Version
Catalyst C6800IA-48FPDR	48-port 10/100/1000 RJ-45 PoE-capable Ethernet (24 ports up to 30W, 48 ports up to 15.4W, 740W total; dual power supplies)	
	With Supervisor Engine 2T-10GE	15.1(2)SY3
Catalyst C6800IA-48FPD	48-port 10/100/1000 RJ-45 PoE-capable Ethernet (24 ports up to 30W, 48 ports up to 15.4W, 740W total)	
Catalyst C6800IA-48TD	48-port 10/100/1000 RJ-45 Ethernet	
	With Supervisor Engine 2T-10GE	15.1(2)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
Catalyst 3560CX-12PD-S	12-port 10/100/1000 PoE+ ports (PoE budget of 240 W); 2 Gigabit Ethernet and 2 SFP+ 2 module uplink slots.	15.2(1)SY0a
	With Supervisor Engine 2T-10GE	
Catalyst 3560CX-8PD-S	Cisco Catalyst 3560-CX 2 x mGig, 6 x 1G PoE, 2 x 10G SFP+ uplink IP Base	15.2(1)SY1
	With Supervisor Engine 2T-10GE	

Note See these publications for more information:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3560-cx-series-switches/datasheet-c78-733229.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6800ia-switch/data_sheet_c78-728230.html

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6800ia-switch/white_paper_c11-728265.html

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/instant_access.html

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6800ia/hardware/installation/guide/b_c6800ia_hig.html

IA client maximum values for Catalyst 6880-X switch:

Value Description:	Maximum Value
Maximum IA client ports	2016 ports across 42 Catalyst 6800ia access switches
Maximum IA client switches	42 (defined by IA client FEX number 1–42 range.)
Maximum Catalyst 6800ia access switches per IA client stack	5 • An IA client stack acts as single switch unit. • Instant access only supports connection with stacking cables to form a stack. • With an IA client that has multiple Catalyst 6800ia access switches, the switches in the stack assign incrementing switch numbers to themselves (automatic stacking capability). • If you add Catalyst 6800ia access switches to a configured IA client, the additional switches assign incrementing switch numbers to themselves. • The IA client configuration does not persist if the access switch number changes.

IA client maximum values for a Catalyst 6500 and Catalyst 6807-XL switch with Supervisor 2T:

Value Description:	Maximum Value	Software Version
Maximum IA client ports	1500 ports	15.2(1)SY1[1]
Maximum IA client switches	32	
Maximum Catalyst 6800ia access switches per IA client stack	5 • An IA client stack acts as single switch unit. • Instant access only supports connection with stacking cables to form a stack. • With an IA client that has multiple Catalyst 6800ia access switches, the switches in the stack assign incrementing switch numbers to themselves (automatic stacking capability). • If you add Catalyst 6800ia access switches to a configured IA client, the additional switches assign incrementing switch numbers to themselves. • The IA client configuration does not persist if the access switch number changes.	

1. The scale for Cisco IOS Releases 15.2(1)SY and 15.2(1)SY0a is 1200 ports with 25 Client Switches and 5 per IA Client stack.

Gigabit Ethernet Switching Modules

WS-X6848-SFP-2T, WS-X6748-SFP 48-Port Gigabit Ethernet SFP Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6848-SFP-2TXL (has WS-F6K-DFC4-AXL) **WS-X6848-SFP-2T** (has WS-F6K-DFC4-A) **WS-X6748-SFP** (with WS-F6700-CFC, or upgraded with WS-F6K-DFC4-AXL or WS-F6K-DFC4-A)	48-port Gigabit Ethernet SFP	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- QoS architecture: **2q8t/1p3q8t**
- Dual switch-fabric connections
  Fabric Channel #1: Ports 2, 4, 6, 8, 10, 12,
  14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34,
  36, 38, 40, 42, 44, 46, 48
  Fabric Channel #2: Ports 1, 3, 5, 7, 9, 11,
  13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33,
  35, 37, 39, 41, 43, 45, 47
- Number of ports: 48
  Number of port groups: 4
  Port ranges per port group:
  1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23
  2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24
  25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47
  26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48
- On WS-X6848-SFP-2T and WS-X6748-SFP ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6848-SFP-2T or WS-X6748-SFP ports that interconnect network devices.

WS-X6824-SFP-2T, WS-X6724-SFP 24-Port Gigabit Ethernet SFP Switching Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6824-SFP-2TXL (Has WS-F6K-DFC4-AXL) **WS-X6824-SFP-2T** (Has WS-F6K-DFC4-A) **WS-X6724-SFP** (with WS-F6700-CFC, or upgraded with WS-F6K-DFC4-AXL or WS-F6K-DFC4-A)	24-port Gigabit Mbps Ethernet SFP	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- QoS architecture: **2q8t/1p3q8t**
- Number of ports: 24
  Number of port groups: 2
  Port ranges per port group: 1–12, 13–24
- On WS-X6824-SFP-2T and WS-X6724-SFP ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6824-SFP-2T or WS-X6724-SFP ports that interconnect network devices.

10/100/1000 Ethernet Switching Modules

These sections describe the supported 10/100/1000 Ethernet switching modules:

- Catalyst C6800-48P-TX, Catalyst C6800-48P-TX-XL, Catalyst C6800-48P-SFP, Catalyst C6800-48P-SFP-XL, page 21

Catalyst C6800-48P-TX, Catalyst C6800-48P-TX-XL, Catalyst C6800-48P-SFP, Catalyst C6800-48P-SFP-XL

- C6800-48P-SFP and C6800-48P-SFP-XL OR C6800-48P-TX and C6800-48P-TX-XL are the orderable product IDs
- Cisco IOS software commands display C6800-48P-SFP or C6800-48P-SFP-XL for the SFP cards, and C6800-48P-TX or C6800-48P-TX-XL for the TX based cards.
- QoS Architecture
  - Receive:
    2q8t (for TX and SFP based cards)
  - Transmit:
    1p3q8t (for TX and SFP based cards)
- Number of ports: 48
- Forwarding and Performance: DFC4-A or DFC4-AXL daughter cards delivering performance up to a sustained 60 Mpps for L2, IPv4 and MPLS forwarding and 30 Mpps for IPv6 forwarding
- Upgrade to Release15.2(1)SY or later before installing these modules
- Backplane Connection: Connect to the switch fabric using dual full-duplex 20-Gbps switch fabric channels
- The TX models support copper RJ45 connectors 100 meters over Category 5, 5E, and 6. The SFP models support SX, LX/LH, -ZX, -T; 1000BASE-CWDM with the help of LC connecter
- Number of forwarding engines: 1
- Port Buffers (for both TX and SFP based cards)
  - Receive -173KB
  - Transmit -1.22MB

See this publication for more information:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6800-series-switches/datasheet-c78-733663.html

WS-X6848-TX-2T, WS-X6748-GE-TX

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6848-TX-2TXL (has WS-F6K-DFC4-AXL) **WS-X6848-TX-2T** (has WS-F6K-DFC4-A) **WS-X6748-GE-TX**	48-port 10/100/1000 RJ-45	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- WS-X6704-10GE requires one of the following:
  - With Supervisor Engine 2T-10GE:
    - WS-F6K-DFC4-AXL
    - WS-F6K-DFC4-A
  - With any supervisor engine, WS-F6700-CFC
- QoS architecture: **2q8t/1p3q8t**
- Dual switch-fabric connections
  Fabric Channel #1: Ports 25–48
  Fabric Channel #2: Ports 1–24
- Number of ports: 48
  Number of port groups: 4
  Port ranges per port group: 1–12, 13–24, 25–36, 37–48
- On WS-X6848-TX-2T and WS-X6748-GE-TX ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6848-TX-2T or WS-X6748-GE-TX ports that interconnect network devices.

WS-X6148E-GE-45AT

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
WS-X6148E-GE-45AT	48-port 10/100/1000 Mbps	
	With Supervisor Engine 2T-10GE	15.0(1)SY
	With Supervisor Engine 2T-10GE in VSS mode	15.1(1)SY

- RJ-45
- WS-X6148E-GE-45AT with WS-F6K-48-AT supports up to 48 ports of Class 4 PoE+ (30.0W).
- QoS port architecture (Rx/Tx): **1q2t/1p3q8t**
- Number of ports: 48
  Number of port groups: 6
  Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48
- The aggregate bandwidth of each set of 8 ports (1–8, 9–16, 17–24, 25–32, 33–40, and 41–48) is 1 Gbps.
- Does not support traffic storm control

WS-X6148A-GE-TX

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148A-GE-TX	48-port 10/100/1000 Mbps	
	With Supervisor Engine 2T-10GE (not supported in VSS mode)	15.0(1)SY

- RJ-45
- WS-X6148A-GE-TX supports WS-F6K-GE48-AF or WS-F6K-48-AF
- With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W).
- QoS port architecture (Rx/Tx): **1q2t/1p3q8t**
- Number of ports: 48
  Number of port groups: 6
  Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48
- The aggregate bandwidth of each port group is 1 Gbps.
- Does not support traffic storm control.

Power over Ethernet Daughtercards

- WS-F6K-GE48-AF, WS-F6K-48-AF, page 23

WS-F6K-GE48-AF, WS-F6K-48-AF

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-F6K-GE48-AF **WS-F6K-48-AF**	IEEE 802.3af PoE daughtercard for:	
	• WS-X6148A-GE-TX With Supervisor Engine 2T-10GE	15.0(1)SY

- WS-F6K-GE48-AF and WS-F6K-48-AF are not FRUs for these switching modules:
- WS-X6148A-GE-TX, supports up to 45 ports of ePoE (16.8W).

Transceivers

- CFP Modules, page 24
- X2 Modules, page 24
- 10 GE SFP+ Modules, page 26

- XENPAKs, page 27
- Small Form-Factor Pluggable (SFP) Modules, page 28
- Gigabit Interface Converters (GBICs), page 31

CFP Modules

Product ID (append "=" for spares)	Product Description	Minimum Software Version
CFP-40G-LR4	40GBASE-LR4	15.0(1)SY1
CFP-40G-SR4	40GBASE-SR4	15.0(1)SY1
CVR-CFP-4SFP10G	FourX coverter to convert each 40GE port into 4 10GE SFP+ ports	15.0(1)SY1

X2 Modules

Note

- WS-X6716-10G and WS-X6708-10GE do not support X2 modules that are labeled with a number that ends with -01. (This restriction does not apply to X2-10GB-LRM.)
- All X2 modules shipped since WS-X6716-10G became available provide EMI compliance with WS-X6816-10G and WS-X6716-10G.
- Some X2 modules shipped before WS-X6716-10G became available might not provide EMI compliance with WS-X6816-10G and WS-X6716-10G. See the information listed for each type of X2 module in the following table.
- For information about X2 modules, see the *Cisco 10GBASE X2 Modules* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/10-gigabit-modules/product_data_sheet0900aecd801f92aa.html

Product ID (append "=" for spares)	Product Description		Minimum Software Version
CVR-X2-SFP10G	10G X2 to SFP+ Converter		15.0(1)SY
DWDM-X2-60.61=	10GBASE-DWDM 1560.61 nm X2 (100-GHz ITU grid)	ITU 21	15.0(1)SY
DWDM-X2-59.79=	10GBASE-DWDM 1559.79 nm X2 (100-GHz ITU grid)	ITU 22	15.0(1)SY
DWDM-X2-58.98=	10GBASE-DWDM 1558.98 nm X2 (100-GHz ITU grid)	ITU 23	15.0(1)SY
DWDM-X2-58.17=	10GBASE-DWDM 1558.17 nm X2 (100-GHz ITU grid)	ITU 24	15.0(1)SY
DWDM-X2-56.55=	10GBASE-DWDM 1556.55 nm X2 (100-GHz ITU grid)	ITU 26	15.0(1)SY
DWDM-X2-55.75=	10GBASE-DWDM 1555.75 nm X2 (100-GHz ITU grid)	ITU 27	15.0(1)SY
DWDM-X2-54.94=	10GBASE-DWDM 1554.94 nm X2 (100-GHz ITU grid)	ITU 28	15.0(1)SY
DWDM-X2-54.13=	10GBASE-DWDM 1554.13 nm X2 (100-GHz ITU grid)	ITU 29	15.0(1)SY

Product ID (append "=" for spares)	Product Description		Minimum Software Version
DWDM-X2-52.52=	10GBASE-DWDM 1552.52 nm X2 (100-GHz ITU grid)	ITU 31	15.0(1)SY
DWDM-X2-51.72=	10GBASE-DWDM 1551.72 nm X2 (100-GHz ITU grid)	ITU 32	15.0(1)SY
DWDM-X2-50.92=	10GBASE-DWDM 1550.92 nm X2 (100-GHz ITU grid)	ITU 33	15.0(1)SY
DWDM-X2-50.12=	10GBASE-DWDM 1550.12 nm X2 (100-GHz ITU grid)	ITU 34	15.0(1)SY
DWDM-X2-48.51=	10GBASE-DWDM 1548.51 nm X2 (100-GHz ITU grid)	ITU 36	15.0(1)SY
DWDM-X2-47.72=	10GBASE-DWDM 1547.72 nm X2 (100-GHz ITU grid)	ITU 37	15.0(1)SY
DWDM-X2-46.92=	10GBASE-DWDM 1546.92 nm X2 (100-GHz ITU grid)	ITU 38	15.0(1)SY
DWDM-X2-46.12=	10GBASE-DWDM 1546.12 nm X2 (100-GHz ITU grid)	ITU 39	15.0(1)SY
DWDM-X2-44.53=	10GBASE-DWDM 1544.53 nm X2 (100-GHz ITU grid)	ITU 41	15.0(1)SY
DWDM-X2-43.73=	10GBASE-DWDM 1543.73 nm X2 (100-GHz ITU grid)	ITU 42	15.0(1)SY
DWDM-X2-42.94=	10GBASE-DWDM 1542.94 nm X2 (100-GHz ITU grid)	ITU 43	15.0(1)SY
DWDM-X2-42.14=	10GBASE-DWDM 1542.14 nm X2 (100-GHz ITU grid)	ITU 44	15.0(1)SY
DWDM-X2-40.56=	10GBASE-DWDM 1540.56 nm X2 (100-GHz ITU grid)	ITU 46	15.0(1)SY
DWDM-X2-39.77=	10GBASE-DWDM 1539.77 nm X2 (100-GHz ITU grid)	ITU 47	15.0(1)SY
DWDM-X2-38.98=	10GBASE-DWDM 1538.98 nm X2 (100-GHz ITU grid)	ITU 48	15.0(1)SY
DWDM-X2-38.19=	10GBASE-DWDM 1538.19 nm X2 (100-GHz ITU grid)	ITU 49	15.0(1)SY
DWDM-X2-36.61=	10GBASE-DWDM 1536.61 nm X2 (100-GHz ITU grid)	ITU 51	15.0(1)SY
DWDM-X2-35.82=	10GBASE-DWDM 1535.82 nm X2 (100-GHz ITU grid)	ITU 52	15.0(1)SY
DWDM-X2-35.04=	10GBASE-DWDM 1535.04 nm X2 (100-GHz ITU grid)	ITU 53	15.0(1)SY
DWDM-X2-34.25=	10GBASE-DWDM 1534.25 nm X2 (100-GHz ITU grid)	ITU 54	15.0(1)SY
DWDM-X2-32.68=	10GBASE-DWDM 1532.68 nm X2 (100-GHz ITU grid)	ITU 56	15.0(1)SY
DWDM-X2-31.90=	10GBASE-DWDM 1531.90 nm X2 (100-GHz ITU grid)	ITU 57	15.0(1)SY
DWDM-X2-31.12=	10GBASE-DWDM 1531.12 nm X2 (100-GHz ITU grid)	ITU 58	15.0(1)SY
DWDM-X2-30.33=	10GBASE-DWDM 1530.33 nm X2 (100-GHz ITU grid)	ITU 59	15.0(1)SY
X2-10GB-T	10GBASE-T X2 Module for CAT6A/CAT7 copper cable		15.1(1)SY
X2-10GB-ZR	10GBASE-ZR X2 Module for SMF		15.0(1)SY
X2-10GB-CX4	10GBASE for CX4 (copper) cable		15.0(1)SY
X2-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) **Note** X2-10GB-ER modules labeled with a number that ends with -02 do not provide EMI compliance with WS-X6716-10G.		15.0(1)SY
X2-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) **Note** X2-10GB-LR modules labeled with a number that ends with -02 or -03 do not provide EMI compliance with WS-X6716-10G.		15.0(1)SY
X2-10GB-LRM	10GBASE-LRM for FDDI-grade multimode fiber (MMF) **Note** Not supported by the **show idprom** command. (CSCsj35671)		15.0(1)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
X2-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF) **Note** • See field notice 62840 for information about unsupported 10GBASE-LX4 modules: http://www.cisco.com/c/en/us/support/docs/field-notices/misc/FN62840.html • X2-10GB-LX4 modules labeled with a number that ends with -01 to -03 do not provide EMI compliance with WS-X6716-10G.	15.0(1)SY
X2-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	15.0(1)SY

10 GE SFP+ Modules

Product ID (append "" for spares)	Product Description	Minimum Software Version
SFP-10G-ZR	10GBASE-ZR SFP+ for 1550 nm SMF	15.1(2)SY3
DWDM-SFP10G-61.41	10GBASE-DWDM 1561.41 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-60.61	10GBASE-DWDM 1560.61 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-59.79	10GBASE-DWDM 1559.79 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-58.98	10GBASE-DWDM 1558.98 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-58.17	10GBASE-DWDM 1558.17 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-57.36	10GBASE-DWDM 1557.36 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-56.55	10GBASE-DWDM 1556.55 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-55.75	10GBASE-DWDM 1555.75 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-54.94	10GBASE-DWDM 1554.94 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-54.13	10GBASE-DWDM 1554.13 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-53.33	10GBASE-DWDM 1553.33 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-52.52	10GBASE-DWDM 1552.52 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-51.72	10GBASE-DWDM 1551.72 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-50.92	10GBASE-DWDM 1550.92 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-50.12	10GBASE-DWDM 1550.12 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-49.32	10GBASE-DWDM 1549.32 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-48.51	10GBASE-DWDM 1548.51 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-47.72	10GBASE-DWDM 1547.72 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-46.92	10GBASE-DWDM 1546.92 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-46.12	10GBASE-DWDM 1546.12 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-45.32	10GBASE-DWDM 1545.32 nm SFP+ (100-GHz ITU grid)	15.1(2)SY

Product ID (append “” for spares)	Product Description	Minimum Software Version
DWDM-SFP10G-44.53	10GBASE-DWDM 1544.53 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-43.73	10GBASE-DWDM 1543.73 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-42.94	10GBASE-DWDM 1542.94 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-42.14	10GBASE-DWDM 1542.14 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-41.35	10GBASE-DWDM 1541.35 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-40.56	10GBASE-DWDM 1540.56 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-39.77	10GBASE-DWDM 1539.77 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-38.98	10GBASE-DWDM 1538.98 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-38.19	10GBASE-DWDM 1538.19 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-37.40	10GBASE-DWDM 1537.40 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-36.61	10GBASE-DWDM 1536.61 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-35.82	10GBASE-DWDM 1535.82 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-35.04	10GBASE-DWDM 1535.04 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-34.25	10GBASE-DWDM 1534.25 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-33.47	10GBASE-DWDM 1533.47 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-32.68	10GBASE-DWDM 1532.68 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-31.90	10GBASE-DWDM 1531.90 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-31.12	10GBASE-DWDM 1531.12 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
DWDM-SFP10G-30.33	10GBASE-DWDM 1530.33 nm SFP+ (100-GHz ITU grid)	15.1(2)SY
SFP-10G-LR	10GBASE-LR for 1310 nm SMF	15.0(1)SY1
SFP-10G-ER	10GBASE-ER for 1550 nm SMF	15.0(1)SY1
SFP-10G-LRM	10GBASE-LRM 1310 nm MMF and SMF	15.0(1)SY
SFP-10G-SR	10GBASE-SR 850 nm MMF	15.0(1)SY
SFP-H10GB-CU1M	1m Twinax cable, passive, 30AWG cable assembly	15.0(1)SY
SFP-H10GB-CU3M	3m Twinax cable, passive, 30AWG cable assembly	15.0(1)SY
SFP-H10GB-CU5M	5m Twinax cable, passive, 24AWG cable assembly	15.0(1)SY

XENPAKs

Note

- For information about DWDM XENPAKs, see the *Cisco 10GBase DWDM XENPAK Modules* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/dwdm-transceiver-modules/product_data_sheet0900aecd801f9333.html

Product ID (append "=" for spares)	Product Description	Minimum Software Version
XENPAK-10GB-LRM	10GBASE-LRM XENPAK Module for MMF **Note** Not supported by the **show idprom** command. (CSCsl21260)	15.0(1)SY
DWDM-XENPAK	10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid	15.0(1)SY
WDM-XENPAK-REC	10GBASE receive-only wavelength division multiplexing (WDM)	15.0(1)SY
XENPAK-10GB-CX4	10GBASE for CX4 (copper) cable; uses Infiniband connectors	15.0(1)SY
XENPAK-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) **Note** XENPAK-10GB-ER units with Part No. 800-24557-01 are not supported, as described in this external field notice (CSCee47030): http://www.cisco.com/c/en/us/support/docs/field-notices/200/fn29736.html	15.0(1)SY
XENPAK-10GB-ER+	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	15.0(1)SY
XENPAK-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	15.0(1)SY
XENPAK-10GB-LR+	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	15.0(1)SY
XENPAK-10GB-LW	10GBASE-LW XENPAK Module with WAN PHY for SMF **Note** XENPAK-10GB-LW operates at an interface speed compatible with SONET/SDH OC-192/STM-64. XENPAK-10GB-LW links might go up and down if the data rate exceeds 9Gbs. (CSCsi58211)	15.0(1)SY
XENPAK-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	15.0(1)SY
XENPAK-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	15.0(1)SY
XENPAK-10GB-ZR	10GBASE for any SMF type	15.0(1)SY

Small Form-Factor Pluggable (SFP) Modules

Gigabit Ethernet SFPs

Note

- For information about coarse wavelength-division multiplexing (CWDM) SFPs, see the *Cisco CWDM GBIC and SFP Solutions* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/cwdm-transceiver-modules/product_data_sheet09186a00801a557c.html

- For information about DWDM SFPs, see the *Cisco CWDM GBIC and SFP Solutions* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/dwdm-transceiver-modules/product_data_sheet0900aecd80582763.html

- See the "Unsupported Hardware" section on page 39 for information about unsupported DWDM-SFPs.
- For information about other SFPs, see the *Cisco SFP Optics For Gigabit Ethernet Applications* data sheet:

  http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/gigabit-ethernet-gbic-sfp-modules/product_data_sheet0900aecd8033f885.html

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Version**
GLC-BX-D	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength	15.0(1)SY
GLC-BX-U	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength	15.0(1)SY
GLC-LH-SMD **GLC-LH-SM**	1000BASE-LX/LH SFP **Note** Supported with WS-X6904-40G-2T in Release 15.1(1)SY1 and later releases.	15.0(1)SY
GLC-SX-MMD **GLC-SX-MM**	1000BASE-SX SFP **Note** Supported with WS-X6904-40G-2T in Release 15.1(1)SY1 and later releases.	15.0(1)SY
GLC-T	1000BASE-T 10/100/1000 SFP module **Note** • For WS-X6904-40G-2T LC, supported only at 1000 Mbps. • Supported with WS-X6904-40G-2T in Release 15.1(1)SY1 and later releases.	15.0(1)SY
GLC-ZX-SM	1000BASE-ZX SFP module	15.0(1)SY
CWDM-SFP-1470	CWDM 1470-nm (Gray) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1490	CWDM 1490-nm (Violet) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1510	CWDM 1510-nm (Blue) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1530	CWDM 1530-nm (Green) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1550	CWDM 1550-nm (Yellow) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1570	CWDM 1570-nm (Orange) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1590	CWDM 1590-nm (Red) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
CWDM-SFP-1610	CWDM 1610-nm (Brown) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	15.0(1)SY
DWDM-SFP-5817	1000BASE-DWDM 1558.17 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5252	1000BASE-DWDM 1552.52 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5172	1000BASE-DWDM 1551.72 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5012	1000BASE-DWDM 1550.12 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4692	1000BASE-DWDM 1546.92 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4373	1000BASE-DWDM 1543.73 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4214	1000BASE-DWDM 1542.14 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3977	1000BASE-DWDM 1539.77 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
DWDM-SFP-3898	1000BASE-DWDM 1538.98 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3582	1000BASE-DWDM 1535.82 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3504	1000BASE-DWDM 1535.04 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-6061	1000BASE-DWDM 1560.61 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5979	1000BASE-DWDM 1559.79 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5898	1000BASE-DWDM 1558.98 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5655	1000BASE-DWDM 1556.55 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5575	1000BASE-DWDM 1555.75 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5494	1000BASE-DWDM 1554.94 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5413	1000BASE-DWDM 1554.13 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-5092	1000BASE-DWDM 1550.92 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4851	1000BASE-DWDM 1548.51 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4772	1000BASE-DWDM 1547.72 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4612	1000BASE-DWDM 1546.12 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4453	1000BASE-DWDM 1544.53 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4294	1000BASE-DWDM 1542.94 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-4056	1000BASE-DWDM 1540.56 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3819	1000BASE-DWDM 1538.19 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3661	1000BASE-DWDM 1536.61 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3425	1000BASE-DWDM 1534.25 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3268	1000BASE-DWDM 1532.68 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3190	1000BASE-DWDM 1531.90 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3112	1000BASE-DWDM 1531.12 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY
DWDM-SFP-3033	1000BASE-DWDM 1530.33 nm SFP (100-GHz ITU grid) SFP module	15.0(1)SY

Fast Ethernet SFPs

Note

- For information about Fast Ethernet SFPs, see the *Cisco 100BASE-X SFP For Fast Ethernet SFP Ports* data sheet: http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/fast-ethernet-sfp-modules/product_data_sheet0900aecd801f931c.html

Product ID (append "=" for spares)	Product Description	Minimum Software Version
GLC-FE-100BX-U	100BASE-BX10-U SFP	15.0(1)SY
GLC-FE-100BX-D	100BASE-BX10-D SFP	
GLC-FE-100EX	100BASEEX SFP	
GLC-FE-100ZX	100BASEZX SFP	
GLC-FE-100FX	100BASEFX SFP	
GLC-FE-100LX	100BASELX SFP	
GLC-GE-100FX	100BASEEX SFP	

Gigabit Interface Converters (GBICs)

Note The support listed in this section applies to all modules that use GBICs.

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WDM-GBIC-REC	Receive-only wavelength division multiplexing (WDM) GBIC	15.0(1)SY
DWDM-GBIC	Dense wavelength division multiplexing (DWDM) GBIC	15.0(1)SY
CWDM-GBIC-1470	Cisco 1000BASE-CWDM GBIC, 1470 nm (Gray)	15.0(1)SY
CWDM-GBIC-1490	Cisco 1000BASE-CWDM GBIC, 1490 nm (Violet)	15.0(1)SY
CWDM-GBIC-1510	Cisco 1000BASE-CWDM GBIC, 1510 nm (Blue)	15.0(1)SY
CWDM-GBIC-1530	Cisco 1000BASE-CWDM GBIC, 1530 nm (Green)	15.0(1)SY
CWDM-GBIC-1550	Cisco 1000BASE-CWDM GBIC, 1550 nm (Yellow)	15.0(1)SY
CWDM-GBIC-1570	Cisco 1000BASE-CWDM GBIC, 1570 nm (Orange)	15.0(1)SY
CWDM-GBIC-1590	Cisco 1000BASE-CWDM GBIC, 1590 nm (Red)	15.0(1)SY
CWDM-GBIC-1610	Cisco 1000BASE-CWDM GBIC, 1610 nm (Brown)	15.0(1)SY
WS-G5483	1000BASET GBIC	15.0(1)SY
WS-G5484	Short wavelength, 1000BASE-SX	15.0(1)SY
WS-G5486	Long wavelength/long haul, 1000BASE-LX/LH	15.0(1)SY
WS-G5487	Extended distance, 1000BASE-ZX	15.0(1)SY

Service Modules

Note

- For service modules that run their own software, see the service module software release notes for information about the minimum required service module software version.
- With SPAN configured to include a port-channel interface to support a service module, be aware of CSCth03423 and CSCsx46323.
- EtherChannel configuration can impact some service modules. In particular, distributed EtherChannels (DECs) can interfere with service module traffic. See this field notice for more information:

  http://www.cisco.com/c/en/us/support/docs/field-notices/610/fn61935.html

- Application Control Engine (ACE) Module, page 32
- ASA Services Module, page 33
- Network Analysis Modules (NAMs), page 33
- Network Analysis Modules (NAMs), page 33
- Network Analysis Modules (NAMs), page 33
- Wireless Services Modules (WiSMs), page 34

Application Control Engine (ACE) Module

Product ID (append "=" for spares)	**Product Description**	**Minimum Software Versions**
ACE30-MOD-K9	Application Control Engine (ACE) module	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- ACE modules run their own software—See these publications:

  http://www.cisco.com/c/en/us/support/interfaces-modules/ace-application-control-engine-module/tsd-products-support-model-home.html

  See the ACE module software release notes for information about the minimum required service module software version.

ASA Services Module

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-SVC-ASA-SM1-K7	ASA Services Module	
	With Supervisor Engine 2T-10GE	15.1(1)SY3
WS-SVC-ASA-SM1-K9	ASA Services Module	
	With Supervisor Engine 2T-10GE	15.0(1)SY1

- Upgrade to the minimum software version or later before installing an ASA services module (see the "EFSU Compatibility" section on page 41).
- ASA modules run their own software—See these publications:

  http://www.cisco.com/c/en/us/support/interfaces-modules/catalyst-6500-series-7600-series-asa-services-module/tsd-products-support-model-home.html

  See the module software release notes for information about the minimum required service module software version.

Network Analysis Modules (NAMs)

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-SVC-NAM3-6G-K9	Network Analysis Module 3	
	With Supervisor Engine 2T-10GE	15.0(1)SY1

- Upgrade to Release 15.0(1)SY1 or later before installing WS-SVC-NAM3-6G-K9 (see the "EFSU Compatibility" section on page 41).
- NAM modules run their own software—See these publications for more information:
  - http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-analysis-module-software/products-release-notes-list.html
  - http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-network-analysis-module-software/tsd-products-support-series-home.html

  See the software release notes for information about the minimum required NAM software version.

Wireless Services Modules (WiSMs)

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-SVC-WISM2-1-K9 **WS-SVC-WISM2-3-K9** **WS-SVC-WISM2-5-K9**	Wireless Services Module 2 (WiSM2)	
	With Supervisor Engine 2T-10GE	15.0(1)SY
Wireless services modules run their own software—See these publications: http://www.cisco.com/c/en/us/support/interfaces-modules/services-modules/products-release-notes-list.html See the wireless services modules software release notes for information about the minimum required wireless services module software version.		

Power Supplies

WS-C6503-E Power Supplies

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PWR-1400-AC	1,400 W AC power supply	15.0(1)SY
PWR-950-DC	950 W DC power supply	15.0(1)SY

WS-C6504-E Power Supplies

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PWR-2700-AC/4	2700 W AC power supply	15.0(1)SY
PWR-2700-DC/4	2700 W DC power supply	15.0(1)SY

All Other Power Supplies

Note The power supplies in this section are not supported in these chassis:

- Catalyst 6503-E
- Catalyst 6504-E

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-CAC-8700W-E	8,700 W AC power supply	15.0(1)SY
	Note • WS-CAC-8700W-E supports a remote power cycling feature. • See this publication for more information: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html	
PWR-6000-DC	6,000 W DC power supply	15.0(1)SY
WS-CAC-6000W	6,000 W AC power supply	
PWR-4000-DC	4,000 W DC power supply	
WS-CAC-4000W	4,000 W AC power supply	
+WS-CAC-3000W	3,000 W AC power supply	
WS-CAC-3000W	3,000 W AC power supply	
WS-CDC-2500W	2,500 W DC power supply	

Chassis

- 13-Slot Chassis, page 36
- 9-Slot Chassis, page 36
- 7-Slot Chassis, page 37
- 6-Slot Chassis, page 38
- 4-Slot Chassis, page 38
- 3-Slot Chassis, page 39

Note Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.**

13-Slot Chassis

Note With Supervisor Engine 2T-10GE, the slot reserved for a redundant supervisor engine can be populated with one of these modules:

- WS-X6148E-GE-45AT
- WS-X6148A-GE-TX

Product ID (append "=" for spare)	Product Description	Minimum Software Version
CISCO7613-S	• 13 slots • Slot 7 and slot 8 are reserved for supervisor engines • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.1(1)SY

9-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6509-V-E	• 9 vertical slots • 64 chassis MAC addresses • Required power supply: – 2,500 W DC or higher – 3,000 W AC or higher	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6509-E	• 9 horizontal slots • Chassis MAC addresses: – Before April 2009—1024 chassis MAC addresses – Starting in April 2009—64 chassis MAC addresses **Note** Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.** • Requires 2,500 W or higher power supply	
	With Supervisor Engine 2T-10GE	15.0(1)SY
CISCO7609-S	• 9 vertical slots • 64 chassis MAC addresses • Required power supply: – 2,500 W DC or higher – 3,000 W AC or higher	
	With Supervisor Engine 2T-10GE	15.0(1)SY1

7-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
Catalyst 6807-XL	• 7 slots • Required power supply: – 3,000 W AC or higher	
	With Supervisor Engine 2T-10GE	15.2(1)SY

6-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6506-E	• 6 slots • Chassis MAC addresses: – Before April 2009—1024 chassis MAC addresses – Starting in April 2009—64 chassis MAC addresses **Note** Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.** • Requires 2,500 W or higher power supply	
	With Supervisor Engine 2T-10GE	15.0(1)SY
CISCO7606-S	• 6 slots • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.1(1)SY1

4-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6504-E	• 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.0(1)SY
CISCO7604	• 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.1(1)SY

3-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6503-E	• 3 slots • 64 chassis MAC addresses • WS-X6904-40G-2T and WS-X6908-10GE are supported only with WS-C6503-E hardware revision 1.3 or higher.	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Unsupported Hardware

Release 15.2(1)SY supports only the hardware listed in the "Supported Hardware" section on page 3. Unsupported modules remain powered down if detected and do not affect system behavior.

Release 15.2(1)SY does not support these modules:

- Supervisor Engine 720-10GE and Supervisor Engine 720
- WS-SVC-FWM-1-K9
- WS-SVC-IDS2-BUN-K9
- WS-SVC-NAM-1
- WS-SVC-NAM-2
- WS-SVC-NAM-1-250S
- WS-SVC-NAM-2-250S
- WS-X6548-RJ-45
- WS-X6548-RJ-21
- WS-X6348-RJ45V
- WS-X6348-RJ-45
- WS-X6348-RJ21V
- WS-X6196-RJ-21
- WS-X6196-21AF
- WS-X6148X2-RJ-45
- WS-X6148X2-45AF
- WS-X6148-RJ45V
- WS-X6148-RJ-45
- WS-X6148-RJ21V
- WS-X6148-RJ-21
- WS-X6148A-RJ-45

- WS-X6148A-45AF
- WS-X6148-45AF
- WS-X6148-21AF
- WS-X6524-100FX-MM
- WS-X6324-100FX-MM
- WS-X6148-FE-SFP
- WS-X6548V-GE-TX
- WS-X6548-GE-TX
- WS-X6548-GE-45AF
- WS-X6516-GE-TX
- WS-X6148V-GE-TX
- WS-X6148A-GE-45AF
- WS-X6148-GE-TX
- WS-X6148-GE-45AF
- WS-X6816-GBIC
- WS-X6516-GBIC
- WS-X6516A-GBIC
- WS-X6416-GBIC
- WS-X6408-GBIC
- WS-X6408A-GBIC
- WS-X6502-10GE
- WS-F6K-DFC3A
- WS-F6K-DFC3B
- WS-F6K-DFC3BXL
- WS-CAC-2500W
- PWR-950-AC
- WS-C6513

Images and Feature Sets

Use Cisco Feature Navigator to display information about the images and feature sets in Release 15.1SY.

The releases includes strong encryption images. Strong encryption images are subject to U.S. and local country export, import, and use laws. The country and class of end users eligible to receive and use Cisco encryption solutions are limited. See this publication for more information:

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export/contract_compliance.html

Universal Boot Loader Image

The Universal Boot Loader (UBL) image is a minimal network-aware image that can download and install a Cisco IOS image from a running active supervisor engine in the same chassis. When newly installed as a standby supervisor engine in a redundant configuration, a supervisor engine running the UBL image automatically attempts to copy the image of the running active supervisor engine in the same chassis.

EFSU Compatibility

SX SY EFSU Compatibility Matrix

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications that are sometimes introduced in a software release. When behavior changes are introduced, existing documentation is updated.

- CSCvb40269
  Type of behavior change: Eliminating duplication of DHCP packets.
  Old behavior: Duplicate DHCP packets are created while working as DHCP Relay Agent when IP helper-address is configured either on SVI or regular L3 interface.
  New behavior: Duplicate DHCP packets are not created.
- CSCuh97087
  In the previous Cisco IOS release versions, default was the **transport input all** command and device alloed all transport protocols and accepted the incoming network connections to tty lines by default. But Based on the CSDL's Product Security Baseline Requirement (SEC-MGT-DEFT-2), transport input has been changed to NONE from ALL through CSCuh97087 and documented. Now we must configure an incoming transport {protocol | all} command before the line will accept incoming connections, Otherwise default is NONE and Cisco devices cannot accept the connections to tty lines.
- CSCuq24924, CSCuy39851
  Type of behavior change: Introduction of Cli support for optimal utilization of l4op.
  Old behavior: IPV4 uses all L4OP's although it can be expanded in TCAM. On creation of IPv6 which requires one mandatory L4OP, an error is thrown.
  New behavior: IPv4 access-list gets expanded in TCAM for lesser expandable-weight, so that few L4OP's can be available for creation of IPv6 access-list which requires mandatory l4op.
- CSCuy78465
  Type of behavior change: DHCP Snooping is not allowed on FEX control VLAN at the time of reload and during configuration.
  Old behavior: DHCP snooping was allowed on FEX control VLAN.
  New behavior: DHCP snooping is not allowed on FEX control VLAN.
  Impact on customer: Can lead to multiple FM inconsistency issues.
- CSCuz67187
  Type of behavior change: Log messages will be suppressed on standby for IA interfaces when spanning-tree portfast edge CLI is applied.
  Old behavior: This message is seen on standby for IA interfaces.
  %Warning: portfast should only be enabled on ports connected to a single host.

Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on GigabitEthernet103/1/0/4 but will only have effect when the interface is in a non-trunking mode.
New behavior: This message is not seen on standby for IA interfaces.

- CSCuz87803
  Type of behavior change: Release introduced.
  Old behavior: No CLI to match packets based on the IPv6 ND packet hoplimit.
  New behavior: New CLI option to match IPv6 ND packets with hoplimit != 255

```
Router(config)#ipv6 access-list test
Router(config-ipv6-acl)#permit
Router(config-ipv6-acl)#deny icmp any any nd-ns ?
dest-option    Destination Option header (all types)
dscp           Match packets with given dscp value
  flow-label     Flow label
  hbh            Match on hop-by-hop option
  hoplimit       Neighbor discovery packet hoplimit != 255
  log            Log matches against this entry
  log-input      Log matches against this entry, including input
  mobility       Mobility header (all types)
  mobility-type  Mobility header with type
  routing        Routing header (all types)
  routing-type   Routing header with type
  sequence       Sequence number for this entry
 time-range     Specify a time-range
<cr>
Router(config-ipv6-acl)#deny icmp any any nd-ns hoplimit
Router(config-ipv6-acl)#permit icmp any any nd-ns
Router(config-ipv6-acl)#deny icmp any any nd-na
Router(config-ipv6-acl)#permit icmp any any redirect hoplimit
Router(config-ipv6-acl)#permit icmp any any router-solicitation hoplimit
Router(config-ipv6-acl)#deny icmp any any router-advertisement
Router(config-ipv6-acl)#end
```

- CSCuz08440
  Old behavior: TE tunnel interfaces may be used to create repair paths in ISIS.
  New behavior: TE tunnel interfaces are not used to create repair paths in ISIS because ISIS does not know if the physical interface for the TE tunnel is via the protected interface or not.
  Impact on customer: Minimum.

- CSCuz88401
  Type of behavior change: Flow control send is set for copper port and the flow control send off config gets nvgen'd after reload.
  Old behavior: The flow control send off command doesn't get nvgen'd for 10G ports after reload and for copper ports the flow control send is set to wrong values.
  New behavior: The flow control send off command remains nvgen'd after reload for 10gig ports and for copper ports the flow control send is set to correct values.
  Other information: Because of incorrect flow control send off values for copper port, when an

etherchannel is formed between copper ports and 10G SR/LR ports due to mismatch in flow control send off, the ports went to suspended state in etherchannel. With the fix, the flow control send is set accordingly and the etherchannel ports dont go to suspended state.

- CSCva39982 (IPv6 neighbor discovery packet processing behavior)
  Before Fix: To rate limit the IPv6 icmp nd type 13-137 packets, there is classmap in the default policy-map, which gets programmed on control plane.
  sh policy-map policy-default-autocopp | b ndv6
  Class class-copp-match-ndv6
  police rate 1000 pps, burst 1000 packets
  conform-action set-discard-class-transmit 48
  exceed-action drop so for both valid ipv6 icmp nd type 13-137 packets (i.e with hop-limit 255) and invalid packets (with hop-limit < 255), there is single policy . So this allows attacker to send a crafted IPv6 ND packet that will cause dropping of valid CPU-bound ipv6 icmp nd traffic.
  Fix: Added a class-map above "class-copp-match-ndv6" named as "class-copp-match-ndv6hl" as follows .

```
FM-NAT#sh policy-map policy-default-autocopp  | b ndv6
    Class class-copp-match-ndv6hl
     police rate 10 pps, burst 1 packets
       conform-action drop
       exceed-action drop
    Class class-copp-match-ndv6
     police rate 1000 pps, burst 1000 packets
      conform-action set-discard-class-transmit 48
       exceed-action drop
```

- CSCva69133
  CLI changes needed for fix in CSCva39982.
- CSCun49292
  When 6500 E-chassis modules are inserted on C6807-X chassis, the power budgeting done by IOS is based on the backplane voltage of 6500 (42V) rather than C6807-X backplane voltage (52V).
- CSCuo98864
  Incorrect static mac entry created in MAC table after FEX reload.
- CSCup54165
  Crash after executing CLI "sh plat hard capacity".
- CSCun68265
  Portchannel configuration exists in interface after removing portchannel.
- CSCum20518
  L2 multicast @ DUT crash when we initiate IGMP joins.
- CSCuq39130
  RSL PO span needs to be restricted.
- CSCuq44854
  15.2SY IPv6 static route not created on dhcp server for PD client.
- CSCun30073
  15.2(1)SY: Ra-throttler not working for wired ports.

New Features in Release 15.2(1)SY8

These sections describe the new features in Release 15.2(1)SY8, 18Feb 2019:

New Hardware Features in Release 15.2(1)SY8

None.

New Software Features in Release 15.2(1)SY8

None.

New Features in Release 15.2(1)SY7

These sections describe the new features in Release 15.2(1)SY7, 20 Aug 2018:

New Hardware Features in Release 15.2(1)SY7

None.

New Software Features in Release 15.2(1)SY7

None.

New Features in Release 15.2(1)SY6

These sections describe the new features in Release 15.2(1)SY6, 28 Feb 2018:

New Hardware Features in Release 15.2(1)SY6

None.

New Software Features in Release 15.2(1)SY6

None.

New Features in Release 15.2(1)SY5

These sections describe the new features in Release 15.2(1)SY5, 25 Aug 2017:

New Hardware Features in Release 15.2(1)SY5

None.

New Software Features in Release 15.2(1)SY5

None.

-

New Features in Release 15.2(1)SY4

These sections describe the new features in Release 15.2(1)SY4, 21 April 2107:

New Hardware Features in Release 15.2(1)SY4

None.

New Software Features in Release 15.2(1)SY4

None.

New Features in Release 15.2(1)SY3

These sections describe the new features in Release 15.2(1)SY1a, 06 Oct 2015:

New Hardware Features in Release 15.2(1)SY3

None.

New Software Features in Release 15.2(1)SY3

None.

New Features in Release 15.2(1)SY2

These sections describe the new features in Release 15.2(1)SY1a, 06 Oct 2015:

New Hardware Features in Release 15.2(1)SY2

None.

New Software Features in Release 15.2(1)SY2

None.

New Features in Release 15.2(1)SY1a

These sections describe the new features in Release 15.2(1)SY1a, 06 Oct 2015:

New Hardware Features in Release 15.2(1)SY1a

None.

New Software Features in Release 15.2(1)SY1a

None.

New Features in Release 15.2(1)SY1

These sections describe the new features in Release 15.2(1)SY1, 14 May 2015:

New Hardware Features in Release 15.2(1)SY1

Small Form-factor Pluggable (SFP) module GLC-EX-SMD is supported on the following SFP modules:

- WS-X6724-SFP
- WS-X6748-SFP
- WS-X6824-SFP
- C6800-48P-SFP

New Software Features in Release 15.2(1)SY1

- Add or verify DOM Support for 6800—See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T.html

- Auto-Fex: FEX configuration made easy by automating FEX essential configurations—See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/instant_access.html

- Dynamic Mode Change Support for Catalyst 3560CX-12PD-S—See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/instant_access.html

- EASY FEX: Interface naming (aliasing) of FEX host port interfaces—See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/instant_access.html

- Easy VSS—See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/virtual_switching_systems.html

- Flexible MACSec Replay Protection support on Catalyst 6500 and 6800—See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/dot1x_port_based_authentication.html

- HSRP BFD Peering—See this publication: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-hsrp-bfd.html

- IPv6 ND RA Solicited Unicast Option—See this publication: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book/ipv6-i3.html#wp5031733970

- LFA FRR—See this publication: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_isis/configuration/15-sy/irs-15-sy-book/irs-ipv4-lfafrr.html.

- Manage FEX switch-id allocation from Controller after stack is booted up—See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/instant_access.html

- IPV6 ND to advertise DNS server in RA—See this publication: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/command/ipv6-cr-book/ipv6-i3.html#wp3800310030

- NEAT for IA—See this publication:

www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-sy/sec-usr-8021x-15-sy-book.html

- QoS Certification—See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T/qos_policy_based_queueing.html

New Features in Release 15.2(1)SY

These sections describe the new features in Release 15.2(1)SY, 19 Dec 2014:

- New Hardware Features in Release 15.2(1)SY, page 48
- New Software Features in Release 15.2(1)SY, page 48

New Hardware Features in Release 15.2(1)SY

- 10/100/1000 Copper Ethernet Module—Catalyst C6800-48P-TX, Catalyst C6800-48P-TX-XL
- 1-Gigabit Pluggable Ethernet Module—Catalyst C6800-48P-SFP, Catalyst C6800-48P-SFP-XL
- 10-Gigabit Pluggable Ethernet Modules:
  - Catalyst C6800-8P10G, Catalyst C6800-8P10G-XL
  - Catalyst C6800-16P10G, Catalyst C6800-16P10G-XL
  - Catalyst C6800-32P10G, Catalyst C6800-32P10G-XL

New Software Features in Release 15.2(1)SY

Note Release 15.2(1)SY Diffserv mib supports up to 256 policy maps.

- Auto configuration —See this publication: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ibns/configuration/15-sy/ibns-15-sy-book/ibns-autoconf.html
- BFD Multihop Support for IPv4 Static Routes —See this publication: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-15-sy-book/irb-bfd-mhop-ip4-static.html
- Differentiated Services Management Information Base (DS MIB)
- Earl8 FNF Full MPLS Netflow support —See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_1_sy_swcg_2T.html

- eEDGE —See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ibns/configuration/15-sy/ibns-15-sy-book.html

Note With Cisco 15.2(1)SY IOS release, on the IA parent maximum of 2016 instant access ports (across 42 Catalyst 6800IA access switches) can be enabled with 802.1x/MAB in IBNS2.0 (Identity Based Networking Services v2.0) with one client per port.

- FHS IPv6 Destination Guard —See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6f-15-sy-book/ipv6-dest-guard.html
- FHS IPv6 Source/Prefix Guard —See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6f-15-sy-book/ip6-src-guard.html
- First Hop Security (FHS) DHCPv6 Guard —See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/DHCPv6-Guard.html
- FHS IPv6 Snooping —See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6f-15-sy-book/ip6-snooping.html
- Interface template support—See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ibns/configuration/15-sy/ibns-15-sy-book/ibns-int-temp.html
- LISP Mobility Across Subnet Mode —See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_lisp/configuration/15-sy/irl-15-sy-book/irl-lisp-asm-vm-host-mobility.html
- MultiVIF and MultiVRF Service Reflect —See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_serv/configuration/15-sy/imc-serv-15-sy-book/imc_service_reflect.html
- Neighbour Discovery Multicast Suppress —See this publication:
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6f-15-sy-book/ip6-nd-mcast-supp.html

- Netflow IPFIX Support —See this publication: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-sy/fnf-15-sy-book/fnf-ipfix-export.html
- Netflow Export to IPv6 Destination address —See this publication: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-sy/fnf-15-sy-book/fnf-exp-ipv6-address.html
- Router Advertisement Throttling —See this publication: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6f-15-sy-book/ip6-ra-throttler.html
- 2000 ports scale support on Catalyst 6880-X—See this publication: http://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_2_sy_swcg_2T.pdf
- 1200 ports scale support on Sup2T —See this publication: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-2SY/config_guide/sup2T/15_1_sy_swcg_2T.html

Software Features from Earlier Releases

Use Cisco Feature Navigator to display supported features that were introduced in earlier releases.

Unsupported Commands

Cisco IOS images for the Supervisor Engine 2T do not support **mls** commands or **mls** as a keyword. See this document for a list of some of the **mls** commands that have been replaced:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/replacement_commands.html

Note Some of the replacement commands support different keyword and parameter values than those supported by the Release 12.2SX commands.

Cisco IOS images for the Supervisor Engine 2T do not support these commands:

- **ip multicast helper-map**
- **ip pim accept-register route-map**

Unsupported Features

These features are not supported in Release 15.2(1)SY8:

- Smart Install

Note Release 15.2(1)SY8 does not support Smart Install feature, but In-Service Software Upgrade (ISSU) is still supported through the dummy CLI **no vstack**. For cases where **vstack** has already been configured, it must be changed to **no vstack** in order to proceed with In-Service Software Upgrade (ISSU).

Restrictions for 15.2(1)SY8

Identifier	Component	Description
CSCvp86378	cat6000-ha	With vstack and its related CLIs enabled C6k ISSU upgrade to 15.2(1)SY8 will fail

Restrictions for 15.2(1)SY6

Identifier	Component	Description
CSCvi01427	cat6000-fabric	Diag failure seen on Switch 2 Module 1 after ISSU
CSCvi08384	cat6000-mcast	IHW entry seen on MCVPLS VC toggling

Restrictions for 15.2(1)SY4

- If you use the linecards with the hardware version, IOS, and ROMMON versions listed in the table below, you can experience the following failures as the older IOS versions do not support the required new flashes:
  - Onboard Failure Logging (OBFL) feature will not work, since IOS will not be able to save data to non-volatile memory (flash).
  - Manual Rommon upgrade using CLI will not work.

PID	Hardware version	Minimum Rommon release required	Minimum IOS release required
C6800-32P10G-XL	2.1 or later	15.2(1r)SYL3 or later	15.2(1)SY4 or later 15.4(01)SY02 or later 15.5(1)SY or later
C6800-32P10G			
C6800-16P10G-XL			
C6800-16P10G			
C6800-8P10G-XL			
C6800-8P10G			
C6880-X-16P10G	2.2 or later	15.2(02r)SYL3 or later	
C6880-X-LE-16P10G			

Restrictions for 15.2(1)SY3

Identifier	Component	Description
CSCvc21186	cat6000-lisp	LISP broken on doing ISSU from MK2.1a to MK2.3

Restrictions for 15.2(1)SY1

Identifier	Component	Description
CSCuv54588	accsw-qos	WS-C3560CX-8PD-S Mgig Port : PQ is not working as expected in Congestion
CSCuv61324	accsw-qos	IA:Drops seen on PQ after pkt size 2750 Bytes in Congestion
CSCuv78269	accsw-qos	PQ drops pkt size > 700 Bytes when policy configured
CSCur76254	cat6000-acl	IPv6 Source guard limitation for link-local addresses
CSCus13869	cat6000-diag	SA-HA: On RPR-upgrade [mk1.4to fc3], major diag-failures and crash seen.
CSCur49886	cat6000-env	"6724 , 6748" LC cards ,PID and VID values "unspec"- supported SFP's
CSCur49913	cat6000-env	6724 LC:- "1000Base-EX" SFP DOM - incorrect warning message is printed.
CSCuv03478	cat6000-firmware	Ingress 64 byte with 4 labels traffic dropped on 10G CTS link
CSCut91071	cat6000-ltl	On SSO, L2 traffic coverged after 25 to 30sec due to STP flap
CSCuv26609	cat6000-qos	IA Queue buffer difference between Catalyst 6500 Supervisor 2T and 6880
CSCup40285	cat6000-qos	Global QoS Configs are lost between 15.1SY1 and 15.2SY Images
CSCuq57919	cat6000-qos	One-Gig RSL Flaps on sending oversubscribed traffic over RSL Ports
CSCus14141	cat6000-routing	EIGRP Adjacency Flap on SSO on MEC port-channel
CSCuq84800	cat6000-vntag	mk2: active crashed while enableing ip igmp snooping with 1G adaptors
CSCun94633	medianet-metadata	metadata egress flows missing after SSO

Restrictions for 15.2(1)SY

Identifier	Component	Description
CSCvi28828	nat	Dynamic Nat preferred over Static Nat with Route maps, For overlapping IP addresses.
CSCup90839	cat6000-acl	15.2 SY data-glean + source-guard policies fail to learn entries
CSCun36071	cat6000-acl	6800-IA:Unable to convert 6800 IA host port to trunk port
CSCuo86784	cat6000-diag	C6800IA-48FPDR stack stuck up in weired state after complete diag run
CSCuo97162	cat6000-dot1x	Interface is not authorized when authentication order is mab dot1x
CSCup56935	cat6000-energy	pc entry showing in o/p sh ener ch after remove cable b/w phone & pc
CSCur06372	cat6000-fabric	Low tput for 9216FS for l2/ipv4/ipv6 unicast in oversubscription mode
CSCup33851	cat6000-firmw	64 bytes packet loss in C6800-32P10G - throughput test failed

Identifier	Component	Description
CSCuo31921	cat6000-netflow	15.2 SY Not able to apply more than 4 mpls monitor, maximum should be 16
CSCuo72924	cat6000-netflow	"show flow monitor cache" doesn't have any info
CSCun61420	cat6000-qos	QOS Queue 7 minimal bandwidth allocation is Q[7-WRR]:10 not [1]
CSCun70548	cat6000-qos	match not should not supported as match-criteria
CSCup20822	cat6000-qos	OSPF/LDP flaps on oversubscribing C6800-32P10G 1G interface
CSCup40285	cat6000-qos	Global QoS Configs are lost between 15.1SY1 and 15.2SY Images
CSCuq57919	cat6000-qos	One-Gig RSL Flaps on sending oversubscribed traffic over RSL Ports
CSCuo89837	cat6000-romm	onNetboot fails due to non-inialization of CMP intf after power cycle
CSCuo45830	cat6000-snmp	entSensorValue showing fake values when CLI shows N/A
CSCuq17088	ifs	show tech | redi bootdisk:file crash in 6880-X
CSCun41916	ipmulticast	MK2 C4 :Wrong IPV6 PIM Neighborship is seen with V6 VRF configs.
CSCup93860	l2vpn	A-VPLS: VCs stays UP though corresponding SVI and AC is down
CSCun94633	medianet-metadata	metadata egress flows missing after SSO
CSCun58576	sisf	IPDT: c4mk2: Config sync @ip device tracking after ISSU LV

Caveats in Release 15.2(1)SY8

Caveats Open in Release 15.2(1)SY8

None.

Caveats Resolved in Release 15.2(1)SY8

Caveat ID Number	Component	Description
CSCvk25074	cat6000-dot1x	cat6000 authentication violation restrict does not stop all traffic in Closed authentication
CSCve89361	sisf	Crash in SISF while processing IPv6 packet

Caveats in Release 15.2(1)SY7

Caveats Open in Release 15.2(1)SY7

None.

Caveats Resolved in Releases 15.2(1)SY7

Caveat ID Number	Component	Description
CSCvi05126	ipsec-isakmp	ISAKMP Notification messages carry unnecessary data
CSCuu76493	energywise	Cisco IOS and IOS XE Software EnergyWise Denial of Service Vulnerabilities

Caveats in Release 15.2(1)SY6

Caveats Open in Release 15.2(1)SY6

Caveat ID Number	Component	Description
CSCvi01412	cat6000-l2-mcast	MCVPLS table entries/grups disappears after ISSU

Caveats Resolved in Release 15.2(1)SY6

Caveat ID Number	Component	Description
CSCvh55201	accsw-ease-of-use	VSS with SMI enabled may experience an unexpected reboot
CSCva27392	accsw-ease-of-use	Memory leak in SMI Director DB Process on 3750
CSCvg96252	cat6000-l2-ec	SUP2T crashes when doing a failover by power off switch 2.
CSCvf56977	cat6000-acl	Duplicate ACL entries in ACL TCAM for dACLs
CSCuy60158	cat6000-acl	Hosts are not able to obtain IP address when DHCP Snooping enabled
CSCvg81219	cat6000-env	Egress traffic drop observed due to interlaken error in T1 device
CSCvg14189	cat6000-env	6880 False alarms on asic-1 temperature
CSCvh32048	cat6000-env	6880X uplink reports CRC errors for rx frames and Traffic drops
CSCvg02572	cat6000-firmware	MET flow control assertion [Fatal Error condition] on C6800-16P10G/8P10G
CSCve99670	cat6000-firmware	6880-X sends empty UDLD echo after reload causing UDLD ERR-DISABLED on the other side
CSCvg30966	cat6000-hw-fwding	NLB multicast with static MAC LTL index mapping * empty * after reload
CSCvf71215	cat6000-ltl	TrafficLoss for ~15secs on QuadSup2t while performing OIR/reset of stdby-sup
CSCux96045	cat6000-ltl	Remove/Add a FortyG as SPAN dst affects other FortyG SPAN dst TX traffic
CSCvh86177	cat6000-mcast	6500//SUP2T Multicast Streams in IHW State over VPLS Circuit
CSCvf53685	cat6000-mcast	Catalyst 6840-X crashes after removing vlans from virtual interface
CSCvf49510	cat6000-mpls	VPLS disposition not programmed properly on standby SUP [Disp: tcam / Disp_flow: tcam missing]
CSCvg03323	cat6000-netflow	Memory holding @"NF ISR Intr Task" process due to parity error

CSCvg02097	cat6000-span	VSS config-sync failure with SPAN session configured
CSCvh18854	cat6k-vs-infra	VSDA link moves to up/down state after ISSU on SSO
CSCvc18597	cat6k-vs-infra	Complete packet loss for specific flows on Sup6T using mixed 40g module
CSCve81627	eedge-epm	C6880-X VSS :: SYS-SW2_STBY-3-TIMERNEG: Cannot start timer (HEX) with negative offset
CSCvf94876	flexible-netflow	C6800-X switch may crash upon executing "show flow monitor" command
CSCvh04421	ipc	Modules reloaded after force-switchover

Caveats in Release 15.2(1)SY5

Caveats Open in Release 15.2(1)SY5

None

Caveats Resolved in Release 15.2(1)SY5

Caveat ID Number	Component	Description
CSCvd42234	cat6000-acl	NAT entries wrongly ages out and translated port changes with active flows.
CSCvb72414	cat6000-acl	RSPAN with VACL does not work if "Redirect" command is used
CSCve59700	cat6000-acl	Cat6000 memory leak due to ACLs at FM L4OP / FM VMR chunk
CSCve84115	cat6000-cm	FMCORE-4-RACL_REDUCED device reloaded with 9k ACE in single ACL.
CSCuz50240	cat6000-diag	TestTrafficStress fails while running diagnostic start switch 1 test all
CSCva27657	cat6000-diag	Diagfail(TestLoopback,TestL2/L3CTSLoopback)on dualactive fast hello link
CSCve56899	cat6000-dot1x	CAT 6K fails to process EAP response from Access Point in multi-auth/domain mode
CSCve26748	cat6000-env	QUAD sup :: Delay in port going down during CSSO crash
CSCvb20422	cat6000-firmware	Tftp server is not reachable after reload with GLC-T and speed < 1000
CSCuz97139	cat6000-firmware	Diag failure on WS-X6904-40G after boot up and ports put into err-disbld
CSCvd94928	cat6000-firmware	input queue/overrun noticed on WS-X6816-10G with service policy applied
CSCvf08983	cat6000-firmware	Generate a log and reset card when interlaken error increments on Radian
CSCur04595	cat6000-firmware	PID & VID blank for GLC-SX-MM, GLC-LH-SM & GLC-T SFPs on Nappar
CSCvf02060	cat6000-firmware	dscp-map - incoming traffic not hitting the correct rcv-queue on the interface
CSCvf39985	cat6000-firmware	6880X uplink remains down with third party switch
CSCvd76917	cat6000-firmware	Ports 7 &15 on C6800-32P10G fail to come up using 100BASEFXMM
CSCvd83170	cat6000-hw-fwding	6500sup2t VSS - MAC addresses learnt over VPLS are timed out prematurely

Caveat ID Number	Component	Description
CSCva61927	cat6000-hw-fwding	mld-vpls: LC crash observed with 1000 IPv6 hosts configured
CSCuz30687	cat6000-hw-fwding	6500 Sup2T - LDB Out of Resource on ICS
CSCvd65374	cat6000-hw-fwding	CDP neighbors disappear when we change the sub-interface maximum-vlan vlan-id from default to any.
CSCve25352	cat6000-hw-fwding	Traffic via private vlan went down after delete/re-config private vlan or reload
CSCvf14948	cat6000-hw-fwding	Cat6000 crash from NULL dereference from temporary mem spike
CSCvc46259	cat6000-l2-infra	%FMCORE-4-RACL_REDUCED: with ip flow monitor input
CSCvf33742	cat6000-l2-infra	CAT6K PD part commit holder for CSCve93788
CSCvc49765	cat6000-l2-mcast	6500//SUP2T Multicast Streams get dropped when passing over VPLS Circuit
CSCvf34391	cat6000-l2-mcast	"Traceback:" MCVPLS holding memory on the Quadsup-ICS
CSCve27925	cat6000-mcast	LTL stuck in PNDG state due to missing port deletion callback
CSCve08850	cat6000-netflow	Reduce syslog messages for VRAM parity error
CSCuz01552	cat6000-l2-infra	CAPI-2-INVALID_SLOT_NUM error when polling POE Mibs
CSCve09599	cat6000-span	DHCP options not visible in mini protocol analyzer capture
CSCvc14292	cat6000-wccp	WCCP redirection ACL with multiple ports per ACE / redirection done in software
CSCva86436	bgp	no export ipv4 unicast map triggered router to crash
CSCve93788	l2vpn	Number of virtual-ethernet interfaces in Cat6k

Caveats in Release 15.2(1)SY4

Caveats Open in Release 15.2(1)SY4

Caveat ID Number	Component	Description
CSCvd42859	cat6000-diag	TestL2CTSLoopback diag fails after ISSU LV
CSCvd99900	cat6000-lisp	Traffic loss observed in ASM mobility movement at XTR2 router
CSCux06827	lisp	LISP ASM: Failed to detect all dynamic EIDs after move

Caveats Resolved in Release 15.2(1)SY4

Identifier	Component	Description
CSCut87445	snmp	SNMP ifAlias set request fails to update running config
CSCuy54914	cat6000-firmware	Mk31:After reload 2nd port group GLC interface not coming up
CSCuz52151	cat6000-qos	EARL8 - range L4Op in a QoS policy does not expand in TCAM when required
CSCva10981	cat6000-env	VSS crash at slot_online_change_notice
CSCva77668	cat6000-acl	VSS Standby stalling in progress to cold-config due to CTS Manual
CSCvb36981	cat6000-mcast	Multicast stream failures because of missing pmask in FPOE
CSCup61257	cat6000-qos	Error message not printing if unsupported QOS is applied via SSH/Telnet.
CSCuq88523	cat6000-mpls	VPLS configuration and removal causing atom mem leaks
CSCuu76720	cat6000-acl	Memory leaks after applying l4op exception (L4 acl) in phy interface
CSCux01435	cat6000-qos	DSCP values for broadcast traffic are not rewritten
CSCux11393	cat6000-hw-fwding	Mtrose:\" Failed to add MAC \" error logs are seen on fex reload
CSCux89341	cat6000-l2-ec	L3 LACP port-channel flap with sub-if on native Vlan
CSCuy46992	cat6000-eobc	ifInDiscards seen via SNMP on EOBC(EO0/2) does not match CLI counter
CSCuy96262	cat6000-acl	%SCHED-THRASHING: Process thrashing
CSCuz63959	cat6000-firmware	GLC-LH-SMD unable to link up
CSCuz82662	cat6000-hw-fwding	Unknown unicast rate-limiter impacts L2 multicast protocols
CSCuz95480	cat6000-span	6880: MPA (monitor capture) cannot export to bootdisk
CSCva29632	cat6000-firmware	6880X VSS after active reboot connected ports will experience up twice
CSCva67271	cat6000-snmp	6500 - OutMcastPkts SNMP OID returns incorrect value for a port-channel
CSCva96299	cat6000-svc	NAM 6.2(1) does not boot successfully in VSS standby chassis
CSCvb07975	cat6000-span	unexpected traffic seen on span destination ports during unicast flood
CSCvb36172	cat6000-l2-mcast	IGMP Join for groups 224.0.0.x are programmed in the IGMP snooping table
CSCvb40269	dhcp	DHCP Relay duplicates packets
CSCty47047	ip-tunnels	%TUN-STBY-3-TUN_HA: Tunnel HA: Tunnel creation on standby: mismatch seen
CSCvc28293	cat6000-lisp	LISP: MAC ACL wrong VMR Mask programming resulting traffic drop for iids in LISP decap path
CSCvb55000	cat6000-firmware	MK51:Flapping GLCT link results in VSL link going down for T1 and T2
CSCvb53731	cat6000-snmp	snmpset cpsIfVlanSecureMacAddrRowStatus deos not return MAC address for Voice VLAN
CSCva67400	cat6000-l2-mcast	mld-vpls: MCVPLS hw programming missing on ISSU LV
CSCvb16274	vpdn	PPTP Start-Control-Connection-Reply packet leaks router memory contents
CSCvb42724	cat6000-hw-fwding	FIB TCAM exception with less than Maximum routes - C6800-16P10G-XL
CSCvc50779	cat6000-fabric	%EARL-DFC13-2-EARL_RECOVERY_PATCH: EARL Recovery Patch triggered! Reason:[Data bus idle]
CSCut40437	cat6000-acl	ACL addrgroup/portgroup object-group names are missing after SSO

Identifier	Component	Description
CSCva74900	cat6000-l2-ec	Sup2t VSS Port-channel config change does not propagate to member ports
CSCux73118	cat6000-acl	Active Sup Crash when ping vrf with inside global address
CSCvc72534	cat6000-ha	C6880-X-LE-16P10G LC reloads in active chassis when VSL link fail.
CSCus68464	cat6000-l2	In RSTP/MST during conversion, port ALT BLK does not send agreement
CSCva07166	obfl	C6880x might crash after running "clear logging onboard" command
CSCvb32497	eigrp	distribute list in eigrp with source protocol doesnt block the routes
CSCux58881	crypto-engine	v6 reflex acl not install nf entry for reverse traffic
CSCvc93848	sisf	No ACL sharing for RACL for dot1x enabled interfaces
CSCvd05301	cat6000-env	Power not denied if system power available = required power
CSCvc26548	cat6000-hw-fwding	LIF access failed, leading to supervisor crash
CSCvd02533	cat6000-diag	Invalid memory action at interrupt level due to diagnostic routine
CSCut73918	cat6k-vs-infra	OVS related failure logs while doing SSO in P-T VSS setup
CSCuv85472	eigrp	EIGRP authentication not working on VNET trunk after reload
CSCva17615	cat6000-env	Faulty Sup2T in standby slot brings down all the Linecards
CSCvc93607	cat6000-span	RSPAN misprogrammed on VSS standby
CSCux91478	fex-infra	Specific FEX ID will not come online due to SDP timeout
CSCuq44349	cat6000-portsecur	Traffic from 6800IA may hit 0x7FA9 & get dropped on VSS
CSCuy64806	cat6000-cm	Cisco IOS Port ACL Bypass Vulnerability
CSCvc23375	cat6000-env	Defect to track malfra commit for issu in CSCvc08872 in MK2.x train
CSCvd07970	cat6000-l2-infra	6880 "flowcontorl send off" command disappear from show run

Caveats in Release 15.2(1)SY3

Caveats Open in Release 15.2(1)SY3

Caveat ID Number	Component	Description
CSCvb43480	accsw-fex	dot1x starting on single host ports for phone with cdp bypass
CSCuy42666	accsw-fex	Traffic Convergence takes ~30seconds on fex member up after reload
CSCuu76720	cat6000-acl	Memory leaks after applying l4op exception (L4 acl) in phy interface
CSCva77668	cat6000-acl	VSS Standby stalling in progress to cold-config due to CTS Manual
CSCvb20424	cat6000-dot1x	same access vlan part of dynamic template causing session deletion
CSCvb36050	cat6000-env	CAT6K - Removed Supervisor module not deleted from SCP MET Group

Caveat ID Number	Component	Description
CSCva57020	cat6000-env	QuadSup:CPU hog messages not printed during sw watchdog crash
CSCva10981	cat6000-env	VSS crash at slot_online_change_notice
CSCuy54914	cat6000-firmware	Mk31:After reload 2nd port group GLC interface not coming up
CSCvb20422	cat6000-firmware	Tftp server is not reachable after reload from sup6t with MK5 fc4 img
CSCux11393	cat6000-hw-fwding	Mtrose:" Failed to add MAC " error logs are seen on fex reload
CSCux89341	cat6000-l2-ec	L3 LACP port-channel flap with sub-if on native Vlan
CSCuo15657	cat6000-l2-infra	Disabled port became a-1000,a-full after doing "copy run start"
CSCuy38370	cat6000-l2-infra	VSS standby switch reload during interface configuration
CSCvb36172	cat6000-l2-mcast	IGMP Join for groups 224.0.0.x are programmed in the IGMP snooping table
CSCvb25693	cat6000-mcast	cat6k:watchdog crash with "sh plat soft multicast rout edc server cache"
CSCvb36981	cat6000-mcast	Multicast stream failures because of missing pmask in FPOE
CSCvb63054	cat6000-mcast	Multicast streams are broken as FPOE is not programmed
CSCva96299	cat6000-svc	NAM 6.2(1) does not boot successfully in VSS standby chassis
CSCvb38021	cat6k-vs-infra	Crash seen while trying to remove pre-provisioned fex module
CSCva74282	dot1x-ios	crash @ auth_mgr_pre_shim_free_event
CSCux76361	dot1x-ios	dACL removed for host with multiple IP addresses in IPDT
CSCuv85472	eigrp	EIGRP authentication not working on VNET trunk after reload
CSCux91478	fex-infra	Specific FEX ID will not come online due to SDP timeouts
CSCty47047	ip-tunnels	%TUN-STBY-3-TUN_HA: Tunnel HA: Tunnel creation on standby: mismatch seen

Caveats Resolved in Release 15.2(1)SY3

Note The fix for CSCux52863 works only with the rommon upgrade to version 15.1(02r)SYS3 (image: c6880x_rm.bin.SPA.151-02r.SYS3). Refer rommon documentation for details.

Identifier	Component	Description
CSCuw62024	cat6000-acl	Config Sync: Bulk-sync failure for ip arp inspection trust
CSCuv42980	cat6000-acl	Deny DACL with log keyword programmed as permit on 6k hardware
CSCuz43541	cat6000-acl	Duplicate ACE entry in an ACL causes standby to reload
CSCva39982	cat6000-acl	IPv6 neighbor discovery packet processing behavior
CSCuq24924	cat6000-cm	EARL8 improve L4op allocation
CSCva00330	cat6000-cm	IPv6 ACL not programming in hw
CSCuv62448	cat6000-cm	Mem leaks after adding DAI config with DHCP snooping
CSCuz50177	cat6000-diag	TestFibTcam failure running "diagnostic start switch 1 test all" command

Identifier	Component	Description
CSCux88535	cat6000-diag	VSL link goes error-disabled
CSCva01219	cat6000-env	6807XL VSS Standby console Enabled after Remote commands on Active
CSCuy96523	cat6000-env	6880 crashes when the connected FEX comes online after I2C bus jam.
CSCuz28744	cat6000-env	After reconnecting port with PoE device is in down state on 6880/IA port
CSCuz12176	cat6000-env	After reload GLC-ZX-SMD not displaying in "show inventory"
CSCux66290	cat6000-env	C6880-X-LE-16P10G LCs crash when trying to read valid IO registers.
CSCuz03015	cat6000-env	EARL Recovery Patch triggered! Reason:[Firmware Fatal Int]
CSCva51425	cat6000-env	QuadSup:save information if sup reloads due to sw watchdog timeout
CSCuz99388	cat6000-env	show inventory shows PID, VID as Unspecified for GLC-TE
CSCuy73772	cat6000-env	Sup2T :: power consumption change upon switchover
CSCut99842	cat6000-env	terminator crash but crashfile not getting generated
CSCuy78366	cat6000-env	Traffic Disruption on installation of a new line Card on 6880 Chassis
CSCuz72236	cat6000-env	Uncorrectable Read I/O timeout on C6880-X-16P10G causing crash of LC
CSCux67359	cat6000-env	VSS standby Power-Capacity Watts display is incorrect
CSCut23413	cat6000-filesys	Sup2t may crash while executing more system:running-config cmd
CSCuy31847	cat6000-firmware	Flapping GLCT link results in VSL link going down
CSCuy74862	cat6000-firmware	Shaping QoS Policy does not work with 1G GLC-T in 10 / 100 Mbps
CSCuz08070	cat6000-hw-fwding	EARL Patch Recovery logs are not sent to syslogs server
CSCva43178	cat6000-hw-fwding	ipIfStatsHCOutOctets.ipv6 calculated wrong value at port-channel I/F
CSCuz10094	cat6000-hw-fwding	Sup2T - Need CLI to modify earl patch recovery module reset threshold
CSCuz49170	cat6000-ipc	6500 - IPC duplicate frames counter continuously incrementing
CSCuz95978	cat6000-ipc	ICC class 212 unknown - messages stuck in pending state
CSCuz67187	cat6000-l2	Stdby reload due to conf sync failure after changing src template config
CSCux69697	cat6000-l2-ec	flow control inconsistency for MEC after module reload
CSCuz75545	cat6000-l2-infra	Mk51: Fex Stuck in image dnld for more than 1 hour
CSCuy45323	cat6000-lisp	LISP local EID failure after VSS swith over
CSCuy29495	cat6000-ltl	High CPU in LTL_MGR process when bringing up new FEX on RSL ports
CSCuy28942	cat6000-ltl	sup2T - UDLD err-disable on peer due to incorrect active-ICS FPOE db
CSCuz02973	cat6000-mcast	Multicast drops due to incorrect FPOE mask - EDC has duplicate entries
CSCut57054	cat6000-mcast	sup2t-ha,2-sup-vss:ltl is not synced to standby
CSCuv04476	cat6000-mcast	Terminator has ambiguous display of Titan instances
CSCuy45072	cat6000-netflow	SUP2T NetFlow filter command in console showing only 600 flows.
CSCux55921	cat6000-portsecur	PSECUR: Interface range command disables port-security on FEX ports
CSCux55270	cat6000-snmp	6880/FEX: SNMP Entity inconsistency
CSCux28695	cat6000-snmp	Mk41: SNMP CPUHOG seen and terminator crashes after deleting/adding fex
CSCuy47777	cat6000-svc	NAM 6.2(1) does not boot successfully in VSS standby chassis
CSCux11916	cat6000-sw-fwding	ARP incomplete on hosts authenticated via MAB connected to 6880

Identifier	Component	Description
CSCuz77753	cat6000-sw-fwding	Follow up of CSCuz28618
CSCuy64453	cat6000-sw-fwding	Sup2T - IBC freeze check code needs to be enhanced
CSCva88391	cat6000-vntag	Memory exhaustion by VNTAG MGR PROCES
CSCuz08233	cat6k-vs-infra	6807-X QUAD SUP2T VSS Reload of ICA because of pending ICC msgs on ICS
CSCuy90212	cat6k-vs-infra	All FEXs down with SDP timeout after a VSS switchover during high CPU
CSCuu43892	dhcp	switch crash on qpair_full after executing dhcpd_* functions
CSCuy09743	dlsw	S2T crash on removing dlsw bridge or bridge protocol vlan-group
CSCup90532	dns	Cisco IOS and IOS XE Software DNS Forwarder Denial of Service Vulnerability
CSCux64170	fex-infra	CFG_MISMATCH seen in module type with C6800IA-48FPDR SKUs
CSCuz61109	fib	Self ping to port channel sub interface dropped with LISP decap log
CSCuz63443	ios-authproxy	Memory corruption crash due to EPM redirect
CSCuw48118	ip	ASR920 - crash in bcopy called from 'addnew' during reassembly
CSCsv50590	ip	CEF drops packets due to incomplete adjacency
CSCux66005	ip	Cisco IOS XE Software IP Fragment Reassembly Denial of Service Vuln.
CSCuy03577	ip-acl	ACL configuration leads CPUHOGs followed by a WATCHDOG and a crash
CSCts95370	ip-acl	In ACL applied to vty wrongly filters out ssh session
CSCuz87803	ip-acl	IPv6 nd packet processing behavior(PI changes,CSCva39982 for PD changes)
CSCva42833	ip-acl	Object groups with a unique combination command gets rejected
CSCuz25390	ip-tunnels	IP tunnel inconsistencies cause memory corruption, crash
CSCvb29204	ipsec-isakmp	BenignCertain on IOS and IOS-XE
CSCva18067	mcast-fib	CPU HOG and Crash by MFIB_rate
CSCuz28618	mcast-fib	sup2t: sup crashed after MFIB errors
CSCut24690	mpls-te	Cat6k MPLS TE high CPU when polling SNMP mplsTunnelEntry OID
CSCux46898	ntp	NTP associations vulnerability
CSCus75471	parser	MALLOCFAIL on "Shell Pipeline Process" When Issuing "Show log | tail -x"
CSCtn75051	snmp	%SYS-3-TIMERNEG: Cannot start timer with negative offset
CSCuw36080	snmp	SNMP with Extended ACL

Caveats in Release 15.2(1)SY2

Caveats Open in Release 15.2(1)SY2

Identifier	Component	Description
CSCuw62024	cat6000-acl	Config Sync: Bulk-sync failure for ip arp inspection trust
CSCux66290	cat6000-env	C6880-X-LE-16P10G LCs crash when trying to read valid IO registers.
CSCut99842	cat6000-env	terminator crash but crashfile not getting generated
CSCuv08707	cat6000-env	C6880-X - module 5 asic-1 temperature is "N/O"
CSCuy73772	cat6000-env	Sup2T :: power consumption change upon switchover
CSCus31811	cat6000-firmware	Recovery patch is triggered from Firmware seen in ISSU run version
CSCuv91162	cat6000-firmware	Management port Link display issue
CSCuq36149	cat6000-firmware	6880-X GLC-T stuck in down/down even after shut/no shut
CSCuy38370	cat6000-l2-infra	VSS standby switch reload during interface configuration
CSCuy45323	cat6000-lisp	LISP local EID failure after VSS swith over
CSCuz08114	cat6000-lisp	Traffic drop is seen when vrf with lisp is configured.
CSCux21992	cat6000-lisp	LISP Decap failing during second pass (L3 by pass in this case)
CSCuz02973	cat6000-mcast	Multicast drops due to incorrect FPOE mask - EDC has duplicate entries
CSCuy45072	cat6000-netflow	SUP2T NetFlow filter command in console showing only 600 flows.
CSCux55270	cat6000-snmp	6880/FEX: SNMP Entity inconsistency
CSCuy64453	cat6000-sw-fwding	Sup2T - IBC freeze check code needs to be enhanced
CSCuz11117	cat6k-vs-infra	Inconsistent: Fex is not coming online after mtu size change in term-fex

Caveats Resolved in Release 15.2(1)SY2

Identifier	Component	Description
CSCus73299	cat6000-acl	Route-map Configured Inside Of NAT Packet Loss Is Seen On 6500 Sup2t
CSCuw21779	cat6000-acl	Hardware TCAM entry programming failed messages seen after IA comes up
CSCuw71689	cat6000-acl	Memory leak at FM core functions leads to crash
CSCuv86525	cat6000-acl	SUP2T drops DHCP OFFER when snooping is enabled on DHCP-Server vlan
CSCuq62568	cat6000-acl	ACL applied using "copy tftp: run" is not being programed in hardware
CSCux74482	cat6000-acl	DHCP snooping gets enabled on fex-control vlan and throws FMCC logs
CSCuu58037	cat6000-cm	ISSU from 15.0(1)SY2 to 15.0(1)SY8 sees resp callback error & icc_error
CSCuv36076	cat6000-env	Cisco PoE phone put into wrong power class 15.1(2)SY5
CSCuu41930	cat6000-env	MK2.0a - Nappar moves back to oversubscription mode after VSS conversion

Identifier	Component	Description
CSCux01283	cat6000-env	sup2T - supervisors do not save info to bootdata on watchdog crash
CSCuq02273	cat6000-env	c68xx platform : GDB should not be available in release images
CSCuu55971	cat6000-env	6500 - On SSO, ports after a 'power inline never' port go down
CSCuw61322	cat6000-env	after sso Insufficient power to start HP mode, standby sup into rommon
CSCux85004	cat6000-env	C6880 crashes when executing "show nvlog"
CSCur65434	cat6000-hw-fwding	L3 IF was affected when shutdown another L3 IF in different segment
CSCuv02292	cat6000-hw-fwding	RF-KPA/CPUHOG seen against spl groom for 200K+ ipv4/v6 entry insertion
CSCuy30891	cat6000-hw-fwding	Sup2T - Router MAC learnt as dynamic with 0x380 index
CSCuu11272	cat6000-ipc	Incremental memory leak at ipc_send_local
CSCux05676	cat6000-l2	Spurious Memory & Align errors at l2vlanifmib_find_entry_by_vlanid crash
CSCuu19667	cat6000-l2-ec	Crash observed on 6880 with error-EthChnl assert failure:
CSCuu48843	cat6000-l2-infra	Traffic drop after SSO with LACP rate fast - CBL blocked
CSCur04896	cat6000-l2-infra	Sup2T unexpected reboot after FWSM went down
CSCuu15276	cat6000-l2-infra	%FMCORE-4-RACL_REDUCED error on L3 int with PBR and FNF
CSCur08470	cat6000-l2-infra	After changing a macro a Sup720 might reload/switchover
CSCuy25835	cat6000-l2-infra	6500 - hw_bd programmed as 0 for new VLANs on DFCs
CSCus77170	cat6000-l2-mcast	Sup2T-IPv6 MLD shows Incorrect Entries
CSCux01628	cat6000-l2-mcast	IPv6 ND is not working for MLD v1 hosts in SUP2T
CSCux40275	cat6000-ltl	OSPF neighborship flaps during Standby sup reload with vsl links shut
CSCut42244	cat6000-ltl	cat6k UDLD triggers err-disable on reload
CSCuu64252	cat6000-mpls	Spanning tree BPDU dropping in WS-X68XX-SFP module across xconnect
CSCuu99604	cat6000-netflow	SUP2T NetFlow / show flow monitor output shown on console instead of VTY
CSCuu99732	cat6000-netflow	SUP2T NetFlow / DFC flow issues / timeout issues
CSCuu55288	cat6000-netflow	Mechanism to throttle NDE export
CSCuu18398	cat6000-netflow	NDE interface seen in the "show cdp neighbors" output in the NBR switch
CSCuw35979	cat6000-qos	QoS counters stop working for 6800ia interfaces
CSCuv47618	cat6000-routing	HSRP & GLBP VIP is unreachable after flapping its port-channel sub-intf
CSCuu67246	cat6000-span	SPAN access-list causing traceback
CSCuy14037	cat6000-sw-fwding	Sup2T - Crash at etsec_tx_free_buffers with high IBC rate
CSCux92824	cat6000-vntag	6800 sends broadcast back on ingress port
CSCuw11991	cat6k-vs-infra	VSS init in RPR incorrectly due to wrong VSL interface count
CSCuy12424	cat6k-vs-infra	6880 reboots with ICC queue full and i/o pool depleted
CSCut42645	crypto-engine	input queue wedged on a SSLVPN enabled router
CSCuw62546	dhcp	ip dhcp snooping detect CLI not present in SY, SXJ2 onwards on S720
CSCuw88059	dhcp	Crash when issuing "show ip dhcp conflict"
CSCux51309	dhcp	MK4: fail ret: messages printed during bootup of fex
CSCuu70641	elam	ELAM capture caused device to crash

Identifier	Component	Description
CSCux43058	flexible-netflow	SUP2T NetFlow / DFC flow issues / timeout issues
CSCux45452	idb	Spike seen in SLCP process due to specific OIDs being polled by SNMP
CSCuu54392	ipsec-core	Different Tunnel Protection with shared profile cannot be used
CSCuw08236	ipsec-isakmp	Partial Denial Of Service Vulnerability in IOS IKEv1 w/ DPD enabled
CSCut10305	lisp	LISP MS default allow more specifics blocks other site config
CSCux87822	mpls-te	MPLS TE Missing label on midpoint when same Tunnel ID resignalled
CSCuw85826	ntp	Evaluation of Cisco IOS and IOS-XEl for NTP_October_2015
CSCuw26339	os-logging	CLI error for logging persistent url command invalid input on size
CSCtk83641	rsvp	RSVP authentication over DMVPN Tunnel is not working
CSCuw73525	sisf	3650 DHCPv6 Guard does not block rogue DHCP server to provide IPv6 addr

Caveats in Release 15.2(1)SY1

Caveats Open in Release 15.2(1)SY1

Identifier	Component	Description
CSCuz97414	aaa	Bulk-sync failure due to ip radius source-interface Vlan701 vrf VRF_MGMT
CSCuw14021	accsw-fex6	800 IA host ports may remain "shut" after IA module is reloaded
CSCus88917	accsw-qos	Lan-q policy on FEX host port is leading to L2 traffic drop
CSCuw21779	cat6000-acl	Hardware TCAM entry programming failed messages seen after IA comes up
CSCus88810	cat6000-dot1x	Device-classifier not working for hosts on new IA module added to stack
CSCuv29631	cat6000-dot1xl	A hostports go to err-disable state in single host mode with cdp bypass
CSCut17677	cat6000-env	day1:%C6KENV-SW1-4-FEXSENSORFAILED after renumbered IA mod comes online
CSCut18304	cat6000-env	Blue Beacon glows after the renumbered IA module of SA IA comes online
CSCut30919	cat6000-envj	unk characters seen on image copy
CSCuv36076	cat6000-env	Cisco PoE phone put into wrong power class 15.1(2)SY5
CSCuw41145	cat6000-env	Syslog showing as Hex values after ISSU runversion
CSCus05372	cat6000-firmware	CPU_MONITOR errors & TBs while Nappar boots up
CSCut88639	cat6000-hw-fwding	2t-1500: Static Mac Entries are deleted on Nappar
CSCut77695	cat6000-l2-infra	"show run fex" o/p is displayed in wrong order
CSCuw21679	cat6000-l2-infra	Traceback seen on reload with PM-SW2_STBY-3-INTERNALERROR:
CSCut26595	cat6000-lisp	LISP traffic encap is failed & dropped with FRR is not supported
CSCus86619	cat6000-mpls	LFAFRR:Hardware adj not displayed properly for backup path

Identifier	Component	Description
CSCut33253	cat6000-portsecur	VLAN info altered port security table on reload with int template
CSCus60364	cat6000-qos	Priority queue threshold programming on controller and IA is different
CSCuw26487	cat6000-qos	Lan queue policy not applied to all IA host port under certain condition
CSCus85109	cat6000-snmp	Provide association support through SNMP from standalone mode
CSCut47984	cat6000-snmp	Snmpwalk still showing peer interface after vsl peer interface is shut
CSCuu07933	cat6000-snmp'	SNMP MIB Sync Failure: dot3PauseEntry' during ISSU[RV-CV] and SSO
CSCuu30711	cat6000-snmp	Need to block dissociate option through SNMP w/h auto-fex enabled
CSCus77110	cat6k-vs-infra	Autofex database holding po info even after "no int po "
CSCuu08552	cat6k-vs-infraI	A host port alias overwritten on reload of IA
CSCuu14300	cat6k-vs-infra	fex switch id not displayed properly in sh env after renumber and 2 sso
CSCus78643	cts	Tfr-Pri-show cts role-based counters ipv4 is not showing full output
CSCuw14049	dot1x-ios	No MAB sessions created due to MAB session-handle table id exhaustion
CSCuo20852	eigrp	LFA FRR not programmed for ECMP under EIGRP process
CSCuw27841	sisf	Traceback@Process="pm scp process" during bootup and SSO

Caveats Resolved in Release 15.2(1)SY1a

Identifier	Component	Description
CSCut27272	aaa	CPUHOG and crash due to Auth Manager process
CSCut29617	accsw-fex	6800IA/FEX stop forwarding multicast traffic
CSCut84834	accsw-fex	6880IA System LED lit Amber
CSCut53599	accsw-platform	C2960X RPS is not functioning correctly, reports "RPS is not responding"
CSCuu18788	accsw-platform	DATACORRUPTION-1-DATAINCONSISTENCY when polling ceExtSysBootImageList
CSCuv66869	accsw-platform	Porter/KF : To change the offset value of the I2C mux.
CSCuu30115	accsw-qos	On Congestion, PQ doesn't work on 6800 IA if pkt size > 700 Bytes
CSCui33974	cat6000-acl	High cpu due to looping packet in Sup2t
CSCuu64279	cat6000-acl	Cisco CAT6K Malformed LISP Packet Denial of Service (DoS) Vulnerability
CSCuw28153	cat6000-acl	153-1.IE101.149_20150915 build failed - Good Code Fix for CSCur37420
CSCuv39099	cat6000-cm	Hardware LIF property programming failed - Prop Udp Error: ABORTED
CSCut78924	cat6000-dot1x	crash@dot1x_sp_platform_unrestrict_macs during critical vlan testing
CSCuu86026	cat6000-env	Internal USB Bootdisk is not initialized during bootup
CSCuv41327	cat6000-env	power supply is not correctly recognized
CSCuv44524	cat6000-env	QuadSupVSS:poe device flap causes ICC messages stuck and memory leak
CSCuv96646	cat6000-env	MK2.1a:IDPROM leak while FEX go down due to ICC channel down over SSO
CSCuv99613	cat6000-env	MK2.1a:IDPROM MAX Value should be extended to 500
CSCuw30287	cat6000-env	Alingment fix for EHCI controller data structures
CSCus80305	cat6000-firmware	TestUnusedPortLoopback fails on RSL ports upon FEX PO removal

Identifier	Component	Description
CSCut40421	cat6000-firmware	Padding is not working for less than 64 bytes packets
CSCuu57899	cat6000-firmware	c6800 may not pass small frames (< 64 Bytes) on certain linecards
CSCuu96336	cat6000-firmware	OIR of GLC-T flaps other 1G links on all Nappar family cards
CSCuv89092	cat6000-firmware	Cat6800: High CPU usage due to "slcp process" when GLC-T plugged in
CSCuv06404	cat6000-ha	Cat6800 experiences unexpected switchover with mismatched fex cabling.
CSCui91874	cat6000-hw-fwding	CPU HOG seen against spl groom for ipv4 & v6 entry insertion.
CSCuw07912	cat6000-l2	Voice vlan not advertised on pre-provisioned 6800ia ports
CSCuq47073	cat6000-l2-infra	fm_cm_set_port_mode_for_rtype: idb - mih mapping failed
CSCuv09462	cat6000-ltl	Traffic dropped due to LTL fail for IAs getting online after switchover
CSCuw44036	cat6000-span	6880x crashes when running "sh monitor session egress replication-mode"
CSCug38910	cat6000-vntag	Mem leak@vnmgr_ha_set_ucast_port_feature+AC on porter reload
CSCuu54241	cat6000-vntag	6880 crashes after a connected FEX reloads
CSCuv07426	cat6k-vs-infra	old provisions of IA removed on sub sequester bring up with diff id
CSCuv18824	cat6k-vs-infra	Stale mod provision statement prevents removal of Fex-id
CSCuv87085	cat6k-vs-infra	6800IA:correct wording of error msgs appearing in IA systems during ISSU
CSCuv76322	dhcp	ip dhcp relay source-interface broken in 15.2(1)SY1
CSCus17694	dot1x-ios	Memory Leak on Auth Manager process
CSCuu05714	ethernet-lldp	Constant high cpu due to SNMP ENGINE when pooling MIB lldpXMedMIB
CSCuv02735	ethernet-lldp	SNMP ENGINE High CPU when configuring switchport and polling lldpXMedMIB
CSCuq52496	flexible-netflow	FNF: platform runs out of big buffers
CSCus77027	flexible-netflow	linecard crashes continuously when losing connectivity to Netflow collector
CSCut20073	ipc	IPC fragmentation - stop refragmenting again if the ack received already
CSCuu28199	ipc	[Amur-MR3]IOSD crash reported@spi_iosd_ipc_process_inbound_mts_msg
CSCuv18809	ipc	Unexpected reload seen @ipc_rcv_unaccount
CSCuw09071	os	USB Enumeration fail causes MCL error due to tftp-server /exception cmd
CSCuh47712	pki	mem leak at pki_get_subaltname_from_cert
CSCus77875	pki	List Headers leak verified cert chain Held CCSIP_TLS_SOCKET & Chunk Mgr
CSCut93029	pki	RA certficate issued by a subCA gets an incorrect lifetime
CSCuu46926	pki	IOS PKI default auto-rollover 30 is not displayed in running-config
CSCur20444	sisf	I/O memory leak due to DHCPv6 packets.
CSCuu14497	sisf	TB@sisf_mac_fsm_clean upon triggering dot1x/mab authentication
CSCuu47026	sisf	sisf entry is getting into STALE after timeout
CSCus25125	snmp	ICS-Standby reloads on SSO bcoz of RF timer expiry for SNMP Client
CSCur60204	ssl	IOS evaluation for CVE-2014-3567, CVE-2014-3568 and CVE-2014-3513
CSCus61884	ssl	JANUARY 2015 OpenSSL Vulnerabilities
CSCus88868	ssl	IOS openssl leak observed with SSL Anyconnect VPN
CSCut46130	ssl	MARCH 2015 OpenSSL Vulnerabilities

Identifier	Component	Description
CSCuu10219	ssl	ssl - Leak at ios_sslvpn_cert_validate_callback when using cert auth
CSCuu82607	ssl	Evaluation of all for OpenSSL June 2015
CSCuq24202	tcl-bleeding	Cisco IOS TCL script interpreter privilege escalation vulnerability
CSCum94811	tcp	TCP Packet Memory Leak Vulnerability

Caveats Resolved in Release 15.2(1)SY1

Identifier	Component	Description
CSCum81043	aaa	Member crashed when power off master
CSCup96276	accsw-fex	"Invalid input detected at '^' marker."during WS-C3560CX-12PD-S bringup
CSCur94246	accsw-fex	No FEX Image Download mesg for migration between 15.1(2)SYx & 15.2(1)SY
CSCus51750	cat6000-acl	wccp_ipv6 and wccp_ipv6_fib missing from s2t54-ipservicesk9
CSCuq64403	cat6000-env	I/O Mem crash due to SCP queue build-up by flaps seen on FEX host ports
CSCus03417	cat6000-env	6880 Instant Access reports incorrect PoE PD Class 0
CSCus68580	cat6000-env	Cat6500 should power up mod in standby sup slot when enough power avlb
CSCut49518	cat6000-env	Enable "disable-hashing" option in MK2 - CSCus48308
CSCur49925	cat6000-env	C6800-48P-SFP:"1000Base-EX" SFP DOM (supp)-value not print.
CSCur63345	cat6000-env	Syslog for corrupted daughterboard idprom is not visible
CSCur64913	cat6000-env	Fix idprom reading for C6800-32P10G-XL
CSCut99813	cat6000-env	Crash seen after CPUHOG due to insertion & withdrawl of ipv4 & v6 routes
CSCut83493	cat6000-hw-fwding	6880X Unexpected reset due to CPU_MONITOR-2-NOT_RUNNING
CSCun23845	cat6000-hw-fwding	snmpwalk timeout for sup2T in VSS mode when polling BRIDGE-MIB
CSCus85586	cat6000-hw-fwding	Cat6880: VSS standby stuck in progress to cold-config due to snmp trap
CSCue35720	cat6000-ipv6	Sup2T crash with FNF export of IPv6 flow with wrong hw adjacency
CSCup92134	cat6000-l2	Unable to configure Speed and duplex mode on the terminator interface
CSCur17071	cat6000-l2-ec	C6880-X-LE: EC cannot bundle when sh/no sh interface on peer device
CSCup80886	cat6000-l2-ec	ASA Cluster members evicted at VSS SSO Switchover
CSCur63457	cat6000-l2-infra	retain default MTU:9216 for IA ports in 15.2(1)SY -Backout CSCur40914
CSCuq00430	cat6000-l2-infra	Flow control issue with port-channel across Ringer and Estelle cards
CSCut01624	cat6000-l2-infra	"speed nonegotiate" is displayed without configured
CSCut13971	cat6000-makefile	FPD upgrade on NAM3 and ASASM fails with 152-1.SY1
CSCus12745	cat6000-mpls	Sup2T: When xconnect goes down traffic sent to CPU causing high CPU
CSCus50539	cat6000-mpls	cat6k:mpls adj programming at LC issue
CSCus64795	cat6000-netflow	Excessive logging/Memory leak due to a parity error in the Netflow VRAM.
CSCur22975	cat6000-netflow	Switch crash in fnf_mon_process_flow

Identifier	Component	Description
CSCuq97767	cat6000-qos	trace back seen when configuring or unconfiguring dynamic VM policy
CSCur93459	cat6000-qos	Outbound service policy is not accepted on 6500
CSCur54239	cat6000-routing	EARL8 - HSRP VIP unreachable after HSRP swichover
CSCus18036	cat6000-snmp	c6500 IOS switches sending Module failure for module minor temp alarms
CSCuq58281	cat6000-snmp	Need OID in CISCO-VIRTUAL-SWITCH-MIB giving Peer Interface of VSL link
CSCus56026	cat6000-sw-fwding	Locally generated LDP packets are not queued correctly
CSCut44097	cat6000-vntag	to address CSCut09976 via retry mechanism
CSCus93563	cat6k-vs-infra	FEX host po-ch stops fwding traffic a/f SSO and then an RSL reset
CSCup54643	cat6k-vs-infra	Proposal for zero-touch replacement of Fex stack member
CSCur75737	device-sensor	Catalyst2960X device-sensor cannot send dhcp information
CSCur11484	dot1x-ios	Host behind phone not placed in critical vlan when ACS is un-reachable
CSCur43251	http	POODLE protocol-side fix: HTTPS Client
CSCus93977	idb	Changing backup interfaces causes parser error & subsequent switch crash
CSCus32786	ip-pbr	TRACK Client thread CPU hog, crash at routemap_rp_push_xdr
CSCur21093	isdn	ISDN interfaces reject load-interval configuration
CSCus74192	isis	Link down event does not flush the routes correctly with isis
CSCuo29389	ntp	NTP clients of 3900 loses sync sporadically,due to high offsetvariations
CSCup81878	ntp	standby reload - Line by Line Sync fail while deleting dynamic NTP peer
CSCuq33617l	pki	IOS RA Serever crashes in NDES and SUbCA setup
CSCus60440	sisf	C6880 crashes when dot1x device moved across a client stack
CSCuq41114	ssh	SSH configuration option to restrict cipher public key and HMAC
CSCus57661	ssh	6500 | SSH - Banner Diplays "$(hostname).$(domain)"
CSCur94774	ssh	Problem with "ip ssh source-interface" command
CSCur23656	ssl	Cisco IOS and IOSd in IOS-XE : evaluation of SSLv3 POODLE vulnerability
CSCuq52516	telnet	cat6k - 6800IA console behaviour fix
CSCul10482	tftp	TFEX: Image auto download fails due to "ip tftp source-interface" config
CSCus58908	tftp	Problem with "ip tftp source-interface" command on reload/ISSU
CSCur70505	ws-ipsec-3	Crash with IPsec Tunnel between 6500 w IPSEC-3 and ASR9000

Caveats in Release 15.2(1)SY

Caveats Open in Release 15.2(1)SY

Identifier	Component	Description
CSCup96276	accsw-fex	"Invalid input detected at '^' marker."during WS-C3560CX-12PD-S bringup
CSCur94246	accsw-fex	No FEX Image Download mesg for migration between 15.1(2)SYx & 15.2(1)SY
CSCui44899	accsw-fex	Timestamp for the Syslog & Debug msgs are different b/n 6k & 2k
CSCur49886	cat6000-env	GLC-EX-SMD insert"6724 , 6748" LC cards ,PID and VID values are "unspec"
CSCur49913	cat6000-env	6724 LC:- "1000Base-EX" SFP DOM - incorrect warning message is printed..
CSCur64913	cat6000-env	Fix idprom reading for C6800-32P10G-XL
CSCur33589	cat6000-firmware	LINK UP event without port connected on Module reset
CSCut64774	cat6000-ha	issu comp-matrix is incorrect in 15.2(1)SY0a images
CSCus21239	cat6000-l2-infra	mk2:VS_MOD_PROV-SW1-6-OPMODE_CFG_MISMATCH message on reload
CSCur32874	cat6000-mcast	MVPN traffic drop for >70sec on SSO in Quad-SUP
CSCuq85706	cat6000-oir	Improper shutting of LC's when insufficient power supply in Cat6807
CSCuq80165	cat6k-vs-infra	IA reloading continuously while upgrade from 15.1(2)SY3 to 15.2(1)SY
CSCur16755	cat6k-vs-infra	VSL link on SW2 ICS will go down while C6800-32P10G-XL in SW1
CSCuq45483	fib	Few VRF routes not programmed in DFCs in a SUP2T VSS w/C6800-32P10G-XL
CSCup73105	ios-licensing	WS-C3560CX-12PD-STB@lic_issu_recv_transform when the IA comes up
CSCuq42467	parser	Line-by-Line sync verifying failure for command "ipv4 proxy-itr"

Caveats Resolved in Release 15.2(1)SY0a

Resolved pki caveats

- CSCuo75572
  Symptom: Devices running Cisco IOS Software or IOS XE Software contain vulnerabilities within the Internet Key Exchange (IKE) version 2 subsystem that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Conditions: The vulnerabilities are due to how an affected device processes certain malformed IKEv2 packets. An attacker could exploit these vulnerabilities by sending malformed IKEv2 packets to an affected device to be processed. A successful exploit could allow the attacker to cause a reload of the affected device or excessive consumption of resources that would lead to a DoS condition. IKEv2 is automatically enabled on devices running Cisco IOS and Cisco IOS XE Software when the Internet Security Association and Key Management Protocol (ISAKMP) is enabled. these vulnerabilities can be triggered only by sending malformed IKEv2 packets.

Workaround: There are no workarounds for the vulnerabilities described in this advisory. Cisco has released free software updates that address these vulnerabilities.
This advisory is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-ikev2

Identifier	Component	Description
CSCty14415	ssh	IOS SSH version 2 to support AES Counter-mode.
CSCus53298	accsw-fex	Adding 5th member to the stack of 4 members reloads whole 6800IA stack
CSCup27045	accsw-platform	Tracebacks are continuously reported, switches inaccessible.
CSCul80136	accsw-platform	Link flap in the REP segment with edge no-neighbor configured.
CSCur94280	accsw-platform	2960x/6800IA: Link may go down randomly with GLC-T in uplink ports
CSCum02538	accsw-platform	Version id & Product id blank in \"sh int tran fex\" o/p for SFP-10-LRM
CSCur56395	accsw-platform	2960X: Link may go down randomly with GLC-T in uplinks
CSCut13971	cat6000-makefile	FPD upgrade on NAM3 and ASASM fails with MK2.1.
CSCuq64403	cat6000-env	I/O Mem crash due to SCP queue build-up by flaps on FEX i/f peers
CSCus72404	cat6000-env	SCP_POWER_DEVICE_MSG_VER2(v2) drains slowly impacting SCP_FEX_VIF_SYNC
CSCur64967	cat6000-env	MK2 throttle - Bundle latest porter images with cat6k controllers
CSCut37269	ha-issu-matrix	ISSU Generation Request for MK2.0a from Throttle v152_1_sy_throttle
CSCus60440	sisf	C6880 crashes when dot1x device moved across a client stack

Caveats Resolved in Release 15.2(1)SY

Identifier	Component	Description
CSCuq32013	accsw-ease-of-use	Wrong config send to SMI clients due to incorrect client MAC mactched.
CSCuq82491	accsw-ease-of-use	SMI: Incorrect client mac addr matched when configured first
CSCuq35209	bgp	BGP advertising incorrect Link Local ipv6 address
CSCum43798	cat6000-acl	FM_EARL8-4-ADMISSION_CONTROL_CONFLICT seen when adding IPV6 acl
CSCum02215	cat6000-diag	diag_check_snr_threshold[4/13]: Incorrect resp shows for copper links
CSCun26423	cat6000-env	WS-X6708-10G-3C Disabled Port showing up in transparent mode
CSCuo30031	cat6000-env	provide unambiguous caller_pc for scp buffers
CSCuq56417	cat6000-env	standby switch- VSS falls to rommon backplane Hardware Rev is => 1.3
CSCuq58494	cat6000-env	EARL Temperature in OBFL displaying 0 value
CSCur49925	cat6000-env	6848,6748 LC card : "1000Base-EX" SFP DOM (supp)- but value not printed
CSCun71233	cat6000-firmware	SFPs not properly seen in outputs of "show inventory"
CSCuo34488	cat6000-ha	VS-S720 may crash existing quad sup VSS on insertion

Identifier	Component	Description
CSCur08184	cat6000-l2	disable .1ad & SSO, L2 port ethertype is still 0x88A8 instead of 0x8100
CSCup52852	cat6000-l2-ec	no console messages when changing hash distribution fixed to adaptive
CSCuq04573	cat6000-l2-infra	6500 SUP2T crash during boot phase-SVIs on the Internal MET are present
CSCun20762	cat6000-ltl	LTL_PARITY_CHECK logged as Non-Critical at its first occurrence
CSCuq62648	cat6000-qos	"mls qos trust dscp" lost after add/remove subint from Port-channel
CSCuq97767	cat6000-qos	trace back seen when configuring or unconfiguring dynamic VM policy
CSCun42239	cts	CTS CA links flaps due to Sap fail - MACSEC_ERROR
CSCum90081	dhcp	Cisco IOS Software DHCPv6 Denial Of Service Vulnerability
CSCun36303	eigrp	o/p intf should not be set while talking to loopback remote neighbors
CSCur21588	ios-authproxy	Switch is not sending LOGIN page for L3-webauth client
CSCui65499	ipmulticast	PIM Null registers should match S,G expiry
CSCtz73697	ipv6	New IPv6 to MLD Notification required for resolving CSCty62014
CSCug25823	isis	Duplicate system ID configured in ip vrf <default> with router isis null
CSCug36698	mpls-mfi	%XDR-SPSTBY-6-ISSUCLIENTABSENT is printed while boot up.
CSCuj55389	ntp	ntp config removed from "sh run" when ntp broadcast done in multiple int
CSCun85168	os-logging	Device crashes and goes into boot loop with syslog cofigured
CSCue45722	parser	Last string in CLI is not counted by count
CSCtz17738	sla	IP SLA enhanced-history distribution-statistics wrong RTT values
CSCub43400	sla	Sequence error returned for some probes
CSCuj55749	snmp	VSS sup 2t : wrong snmp engine ID displayed
CSCuf48385	vrfinfra	Removing VRF AF RT import causes import issues

Troubleshooting

These sections describes troubleshooting guidelines for the Catalyst 6500 series switch configuration:

System Troubleshooting

This section contains troubleshooting guidelines for system-level problems:

- When the system is booting and running power-on diagnostics, do not reset the switch.
- After you initiate a switchover from the active supervisor engine to the redundant supervisor engine, or when you insert a redundant supervisor engine in an operating switch, always wait until the supervisor engines have synchronized and all modules are online before you remove or insert modules or supervisor engines or perform another switchover.
- If you have an interface whose speed is set to **auto** connected to another interface whose speed is set to a fixed value, configure the interface whose speed is set to a fixed value for half duplex. Alternately, you can configure both interfaces to a fixed-value speed and full duplex.
- If you apply both ACL and FnF with sampler on the SVI interface, the operational state of the Feature Manager gets reduced which causes the traffic to get software switched. In this state, if incoming traffic rate is high, CPU utilization will also go high. Therefore, apply ACL and FnF without sampler on the SVI interface. Otherwise, apply ACL and FnF with sampler on the physical interface.

Module Troubleshooting

This section contains troubleshooting guidelines for module problems:

- When you hot insert a module into a chassis, be sure to use the ejector levers on the front of the module to seat the backplane pins properly. Inserting a module without using the ejector levers might cause the supervisor engine to display incorrect messages about the module. For module installation instructions, refer to the *Catalyst 6500 Series Module Installation Guide*.
- Whenever you connect an interface that has duplex set to autonegotiate to an end station or another networking device, make sure that the other device is configured for autonegotiation as well. If the other device is not set to autonegotiate, the autonegotiating port will remain in half-duplex mode, which can cause a duplex mismatch resulting in packet loss, late collisions, and line errors on the link.

VLAN Troubleshooting

Although DTP is a point-to-point protocol, some internetworking devices might forward DTP frames. To avoid connectivity problems that might be caused by a switch acting on these forwarded DTP frames, do the following:

- For interfaces connected to devices that do not support DTP, in which trunking is not currently being used, configure interfaces with the **switchport mode access** command, which puts the interface into access mode and sends no DTP frames.
- When manually enabling trunking on a link to devices that do not support DTP, use the **switchport nonegotiate** and **switchport mode trunk** commands, which puts the interface into trunking mode without sending DTP frames.

Spanning Tree Troubleshooting

The Spanning Tree Protocol (STP) blocks certain ports to prevent physical loops in a redundant topology. On a blocked port, switches receive spanning tree bridge protocol data units (BPDUs) periodically from neighboring switches. You can configure the frequency with which BPDUs are received by entering the **spanning-tree vlan** *vlan_ID* **hello-time** command (the default frequency is set to 2 seconds). If a switch does not receive a BPDU in the time period defined by the **spanning-tree vlan** *vlan_ID* **max-age** command (20 seconds by default), the blocked port transitions to the listening state, the learning state, and to the forwarding state. As it transitions, the switch waits for the time period specified by the **spanning-tree vlan** *vlan_ID* **forward-time** command (15 seconds by default) in each of these intermediate states. If a blocked spanning tree interface does not receive BPDUs from its neighbor within 50 seconds, it moves into the forwarding state.

Note We do not recommend using the UplinkFast feature on switches with more than 20 active VLANs. The convergence time might be unacceptably long with more than 20 active VLANs.

To debug STP problems, follow these guidelines:

- The **show vlan virtual-port** command displays the number of virtual interfaces.
- These maximum numbers of virtual interfaces are supported:

	MST	RPVST+	PVST+
Stand-alone switch/VSS system limits:	100,000 total	12,000 total	15,000 total

Note Cisco IOS software displays a message if you exceed the maximum number of virtual interfaces.

- After a switchover from the active to the redundant supervisor engine, the ports on the redundant supervisor engine take longer to come up than other ports.
- Record all spanning tree-blocked ports in each switch in your network. For each of the spanning tree-blocked ports, record the output of the **show interface** command. Check to see if the port has registered many alignment, FCS, or any other type of line errors. If these errors are incrementing continuously, the port might drop input BPDUs. If the input queue counter is incrementing continuously, the port is losing input packets because of a lack of receive buffers. This problem can also cause the port to drop incoming BPDUs.
- On a blocked spanning tree port, check the duplex configuration to ensure that the port duplex is set to the same type as the port of its neighboring device.
- On trunks, make sure that the trunk configuration is set properly on both sides of the link.
- On trunks, if the neighboring device supports it, set duplex to full on both sides of the link to prevent any collisions under heavy traffic conditions.

Additional Troubleshooting Information

For additional troubleshooting information, refer to the publications at this URL:

http://www.cisco.com/c/en/us/support/switches/catalyst-6500-series-switches/tsd-products-support-troubleshoot-and-alerts.html

System Software Upgrade Instructions

See this publication:

http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/28724-161.html

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 and/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 and/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].

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

This document is to be used in conjunction with the *Catalyst 6500 Series Cisco IOS Software Configuration Guide* publication.