Release Notes for Cisco IOS Release 15.0SY

February 12, 2016

Note

- This publication applies to the Supervisor Engine 2T-10GE (CAT6000-VS-S2T-10G/MSFC5) platform.
- See this product bulletin for information about the standard maintenance and extended maintenance 15.0SY releases:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps11821/ps11845/product_bulletin_c25-687567_ps708_Products_Bulletin.html
- For general product information about the Catalyst 6500 series switches, refer to these product bulletins:

  http://www.cisco.com/en/US/products/hw/switches/ps708/prod_literature.html

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

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/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 34 for information about which releases are deferred.
- See the "Hierarchical List of Releases" section on page 3 for information about parent releases.

This is a chronological list of the 15.0SY releases:

- Release 15.0(1)SY10—12 Feb 2016
- Release 15.0(1)SY9—11 Aug 2015
- Release 15.0(1)SY8—20 Feb 2015
- Release 15.0(1)SY7a—01 Oct 2014
- Release 15.0(1)SY7—01 Aug 2014
- Release 15.0(1)SY6—07 Feb 2014
- Release 15.0(1)SY5—23 Aug 2013
- Release 15.0(1)SY4—21 Mar 2013
- Release 15.0(1)SY3—26 Nov 2012
- Release 15.0(1)SY2—16 Jul 2012

- Release 15.0(1)SY1—24 Feb 2012
- Release 15.0(1)SY—27 Sep 2011

Hierarchical List of Releases

These releases support the hardware listed in the "Supported Hardware" section on page 4:

- Release 15.0(1)SY10—
  - Date of release: 12 Feb 2016
  - Based on Release 15.0(1)SY9
- Release 15.0(1)SY9—
  - Date of release: 11 Aug 2015
  - Based on Release 15.0(1)SY8
- Release 15.0(1)SY8—
  - Date of release: 20 Feb 2015
  - Based on Release 15.0(1)SY7a
- Release 15.0(1)SY7a—
  - Date of release: 01 Oct 2014
  - Based on Release 15.0(1)SY7
- Release 15.0(1)SY7:
  - Date of release: 01 Aug 2014
  - Based on Release 15.0(1)SY6
- Release 15.0(1)SY6:
  - Date of release: 07 Feb 2014
  - Based on Release 15.0(1)SY5
- Release 15.0(1)SY5:
  - Date of release: 23 Aug 2013
  - Based on Release 15.0(1)SY4
- Release 15.0(1)SY4:
  - Date of release: 21 Mar 2013
  - Based on Release 15.0(1)SY3
- Release 15.0(1)SY3:
  - Date of release: 26 Nov 2012
  - Based on Release 15.0(1)SY2
- Release 15.0(1)SY2:
  - Date of release: 16 Jul 2012
  - Based on Release 15.0(1)SY1
- Release 15.0(1)SY1:
  - Date of release: 24 Feb 2012

  - Based on Release 15.0(1)SY
- Release 15.0(1)SY:
  - Date of release: 27 Sep 2011
  - Based on Release 12.2(50)SY

Note Release 15.0(1)SY and rebuilds support only Ethernet ports. Release 15.0(1)SY and rebuilds do not support any WAN features or commands.

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/en/US/docs/security/asa/asa84/release/notes/asarn85.html#Upgrading_the_FPD_Image
- Network Analysis Module 3 (WS-SVC-NAM3-6G-K9)—See these publications:

  http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_notes_list.html

Supported Hardware

These sections describe the hardware supported in Release 15.0(1)SY and later releases:

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

Supervisor Engine 2T-10GE

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

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/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" section on page 6.
- 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 or 1000 Mbps RJ-45)
- 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/en/US/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

Policy Feature Card 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 and Centralized Forwarding Cards

Note

- See the "Policy Feature Cards" section on page 6 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/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/OL_24918.html

  http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps11878/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/1p7q4t**
- 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 34).
- 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
  Note: Some features described in the whitepaper will be supported in future releases.

  40 Gigabit Ethernet Interface Module for Cisco Catalyst 6500 Series Switches Data Sheet

10-Gigabit Ethernet Switching Modules

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 either WS-F6K-DFC4-E or WS-F6K-DFC4-EXL.
- dCEF720
- 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-X6716-10GE 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 either WS-F6K-DFC4-E or WS-F6K-DFC4-EXL.
- dCEF720
- 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

- Unless equipped with a WS-F6700-CFC, must be upgraded with WS-F6K-DFC4-AXL or WS-F6K-DFC4-A.
- dCEF720 with a DFC or CEF720 with a WS-F6700-CFC.
- Requires 512-MB DRAM with a WS-F6700-CFC (CSCtk82279). See this publication:

  http://www.cisco.com/en/US/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 either WS-F6K-DFC4-A or WS-F6K-DFC4-AXL.
- 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)

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**	48-port Gigabit Ethernet SFP	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- dCEF720 with a DFC or CEF720 with a WS-F6700-CFC.
- Unless equipped with a WS-F6700-CFC, WS-X6748-SFP must be upgraded with WS-F6K-DFC4-AXL or WS-F6K-DFC4-A.
- 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**	24-port Gigabit Mbps Ethernet SFP	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- dCEF720 with a DFC or CEF720 with a WS-F6700-CFC.
- Unless equipped with a WS-F6700-CFC, WS-X6724-SFP must be upgraded with WS-F6K-DFC4-AXL or WS-F6K-DFC4-A.
- 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 descibe the supported 10/100/1000 Ethernet switching modules:

- WS-X6848-TX-2T, WS-X6748-GE-TX, page 16
- WS-X6148E-GE-45AT, page 17
- WS-X6148A-GE-TX, WS-X6148A-GE-45AF, page 17

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

- dCEF720 with a DFC or CEF720 with a WS-F6700-CFC.
- Unless equipped with a WS-F6700-CFC, WS-X6748-GE-TX must be upgraded with WS-F6K-DFC4-AXL or WS-F6K-DFC4-A.

- 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

- 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.
- Not supported in virtual switch mode.
- Does not support traffic storm control.

WS-X6148A-GE-TX, WS-X6148A-GE-45AF

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148A-GE-TX **WS-X6148A-GE-45AF**	48-port 10/100/1000 Mbps	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- RJ-45
- WS-X6148A-GE-TX supports WS-F6K-GE48-AF or WS-F6K-48-AF
- WS-X6148A-GE-45AF has 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.
- Not supported in virtual switch mode.
- Does not support traffic storm control.

100MB Ethernet Switching Modules

WS-X6148-FE-SFP

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148-FE-SFP	48-port 100BASE-FX	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- Requires Fast Ethernet SFPs
- QoS port architecture (Rx/Tx): **1p1q4t/1p3q8t**
- Number of ports: 48
  Number of port groups: 3
  Port ranges per port group: 1–16, 17–32, and 33–48
- Not supported in virtual switch mode.
- Does not support traffic storm control.

10/100MB Ethernet Switching Modules

- WS-X6148A-RJ-45, WS-X6148A-45AF, page 18
- WS-X6196-RJ-21, WS-X6196-21AF, page 19

WS-X6148A-RJ-45, WS-X6148A-45AF

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148A-RJ-45 **WS-X6148A-45AF**	48-port 10/100TX RJ-45	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- 5.3-MB per-port packet buffers

- QoS port architecture (Rx/Tx): **1p1q4t/1p3q8t**
- WS-X6148A-RJ-45 supports WS-F6K-GE48-AF or WS-F6K-48-AF
- WS-X6148A-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF
- 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
- Not supported in virtual switch mode.

WS-X6196-RJ-21, WS-X6196-21AF

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-X6196-RJ-21 **WS-X6196-21AF**	96-port 10/100TX RJ-21	
	With Supervisor Engine 2T-10GE	15.0(1)SY1

- Not supported in VSS mode.
- Upgrade to Release15.0(1)SY1 or later before installing WS-X6196-21AF (see the "EFSU Compatibility" section on page 34).
- QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t**
- WS-X6196-RJ-21 supports WS-F6K-FE48X2-AF
- WS-X6196-21AF has WS-F6K-FE48X2-AF

Power over Ethernet Daughtercards

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-F6K-GE48-AF **WS-F6K-48-AF**	IEEE 802.3af PoE daughtercard for: • WS-X6148A-GE-TX • WS-X6148A-RJ-45 **Note** With WS-X6148A-GE-TX, supports up to 45 ports of ePoE (16.8W).	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Transceivers

- XENPAKs, page 22
- Small Form-Factor Pluggable (SFP) Modules, page 24

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-X6716-10GE does 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-X6716-10GE became available provide EMI compliance with WS-X6816-10G and WS-X6716-10G.
- Some X2 modules shipped before WS-X6716-10GE 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/en/US/prod/collateral/modules/ps5455/ps6574/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
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

Product ID (append "=" for spares)	Product Description		Minimum Software Version
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-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-X6716-10GE.		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-X6716-10GE.		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/en/US/ts/fn/misc/FN62840.html • X2-10GB-LX4 modules labeled with a number that ends with -01 to -03 do not provide EMI compliance with WS-X6716-10GE.	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-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/en/US/prod/collateral/modules/ps5455/ps6576/product_data_sheet0900aecd801f9333.html

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

  http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a008007cd00_ps5251_Products_Data_Sheet.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/en/US/ts/fn/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

These sections describe SFPs:

- Gigabit Ethernet SFPs, page 24
- Fast Ethernet SFPs, page 26

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/en/US/prod/collateral/modules/ps5455/ps6575/product_data_sheet09186a00801a557c_ps4999_Products_Data_Sheet.html

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

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6576/product_data_sheet0900aecd80582763.html

- See the "Unsupported Hardware" section on page 33 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/en/US/prod/collateral/modules/ps5455/ps6577/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	15.0(1)SY
GLC-SX-MMD **GLC-SX-MM**	1000BASE-SX SFP	15.0(1)SY
GLC-T	1000BASE-T 10/100/1000 SFP module **Note** Supported only at 1000 Mbps.	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

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

- The WS-X6148-FE-SFP supports Fast Ethernet SFPs.
- For information about Fast Ethernet SFPs, see the *Cisco 100BASE-X SFP For Fast Ethernet SFP Ports* data sheet:

  http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6578/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	

Note GLC-GE-100FX Fast Ethernet SFPs are not supported.

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/en/US/ts/fn/610/fn61935.html

- Application Control Engine (ACE) Module, page 27
- ASA Services Module, page 27
- Firewall Services Module (FWSM), page 27
- Network Analysis Modules (NAMs), page 28
- Wireless Services Modules (WiSMs), page 28

Application Control Engine (ACE) Module

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
ACE30-MOD-K9 **ACE20-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/en/US/products/ps6906/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-K9	ASA Services Module	
	With Supervisor Engine 2T-10GE	15.0(1)SY1

Note Upgrade to Release15.0(1)SY1 or later before installing WS-SVC-ASA-SM1-K9 (see the "EFSU Compatibility" section on page 34).

Firewall Services Module (FWSM)

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-SVC-FWM-1-K9	Firewall Services Module	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- With Firewall Services Module Software Release 2.3(1) and later releases, WS-SVC-FWM-1-K9 maintains state when an NSF with SSO redundancy mode switchover occurs.
- WS-SVC-FWM-1-K9 runs its own software—See these publications:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

  See the WS-SVC-FWM-1-K9 software release notes for information about the minimum required WS-SVC-FWM-1-K9 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
WS-SVC-NAM-2 **WS-SVC-NAM-1**	Network Analysis Module 2 Network Analysis Module 1	
	With Supervisor Engine 2T-10GE	15.0(1)SY

- Upgrade to Release15.0(1)SY1 or later before installing WS-SVC-NAM3-6G-K9 (see the "EFSU Compatibility" section on page 34).
- NAM modules run their own software—See these publications for more information:
  - http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_notes_list.html
  - http://www.cisco.com/en/US/products/sw/cscowork/ps5401/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
WS-SVC-WISM-1-K9	Wireless Services Module (WiSM)	
	With Supervisor Engine 2T-10GE	15.0(1)SY

Wireless services modules run their own software—See these publications:

http://www.cisco.com/en/US/products/ps6526/tsd_products_support_eol_model_home.html

See the wireless services modules software release notes for information about the minimum required wireless services module software version.

Power Supplies

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

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-AC	950 W AC power supply	15.0(1)SY
PWR-950-DC	950 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/en/US/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-CAC-2500W	2,500 W AC power supply	
WS-CDC-2500W	2,500 W DC power supply	

Chassis

- 13-Slot Chassis, page 31
- 9-Slot Chassis, page 31
- 6-Slot Chassis, page 32
- 4-Slot Chassis, page 33
- 3-Slot Chassis, page 33

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

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6513-E	Catalyst 6513-E chassis: • 13 slots • Slot 7 and slot 8 are reserved for supervisor engines. • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.0(1)SY

9-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6509-V-E	Catalyst 6509-V-E chassis: • 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
CISCO7609-S	Cisco 7609-S chassis: • 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

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6509-E	Catalyst 6509-E chassis: • 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

6-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6506-E	Catalyst 6506 chassis: • 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

4-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6504-E	Catalyst 6504-E chassis: • 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	15.0(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 15.0SY supports only the hardware listed in the "Supported Hardware" section on page 4. Unsupported modules remain powered down if detected and do not affect system behavior.

Release 12.2SX supported these modules, which are not supported in Release 15.0SY:

- Supervisor Engine 720-10GE (CAT6000-VS-S720-10G/MSFC3)
- Supervisor Engine 720 (CAT6000-SUP720/MSFC3)
- Supervisor Engine 32 (CAT6000-SUP32/MSFC2A)
- ME 6500 Series Ethernet Switches (ME6524)
- Policy Feature Card 3A and Distributed Forwarding Card 3A
- 76-ES+XT-4TG3CXL, 76-ES+XT-4TG3C
- 76-ES+XT-2TG3CXL, 76-ES+XT-2TG3C
- 7600-ES+4TG3CXL, 7600-ES+4TG3C
- 7600-ES+2TG3CXL, 7600-ES+2TG3C
- Shared Port Adapter (SPA) Interface Processors (SIPs) and Shared Port Adapters (SPAs)
- Services SPA Carrier (SSC) and Services SPAs
- Enhanced FlexWAN Module
- Anomaly Guard Module(AGM)

- Traffic Anomaly Detector Module (ADM)
- Communication Media Module (CMM)
- Content Switching Module (CSM)
- Content Switching Module with SSL (CSM-S)
- Secure Sockets Layer (SSL) Services Module

Images and Feature Sets

Use Cisco Feature Navigator to display information about the images and feature sets in Release 15.0(1)SY.

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 (XLSX - Opens with Microsoft Excel)

Release 15.0(1)SY1 provides initial Release 15.0SY support for these modules:

- WS-X6904-40G
- WS-X6196-RJ-21, WS-X6196-21AF
- WS-SVC-ASA-SM1-K9
- WS-SVC-NAM3-6G-K9

Do not install these modules before an EFSU upgrade to Release 15.0(1)SY1. These modules should not be installed if EFSU downgrade to Release 15.0(1)SY is required.

If any of the listed modules were installed in a non-VSS system prior to an EFSU upgrade to Release 15.0(1)SY1, perform these steps:

1. Remove the modules.
2. Perform the EFSU upgrade.
3. Insert the modules.

If any of the listed modules were installed in (or were installed and then removed from) a VSS system prior to an EFSU upgrade to Release 15.0(1)SY1, perform these steps:

1. Remove the modules.
2. For each chassis where the modules were, enter the **no module provision switch** [**1**|**2**] global configuration mode command (provision information for the modules will be lost).
3. Save the configuration.
4. Perform the EFSU upgrade.
5. Insert the modules.

If any of the listed modules were installed in (or were installed and then removed from) a non-VSS system prior to an EFSU downgrade to Release 15.0(1)SY, perform these steps:

1. Ensure that the modules are present (or reinstalled, if necessary).
2. Enter the **module clear-config** global configuration mode command.
3. Remove the modules from the chassis.
4. Verify that no configuration information remains for any of the modules.
5. Save the configuration.
6. Perform the EFSU downgrade.

If any of the listed modules were installed in (or were installed and then removed from) a VSS system prior to an EFSU downgrade to Release 15.0(1)SY, perform these steps:

1. Remove any remaining modules.
2. Enter the **show running-config | begin provision** command to display the module provisioning information. For example:

```
Router# show running-config | begin provision
module provision switch 1
slot 3 slot-type 95 port-type 30 number 8  virtual-slot 19
slot 4 slot-type 322 port-type 112 number 16  virtual-slot 20
slot 7 slot-type 318 port-type 31 number 3 port-type 60 number 2  virtual-slot 23
slot 8 slot-type 318 port-type 31 number 3 port-type 60 number 2  virtual-slot 24
slot 12 slot-type 147 port-type 61 number 48  virtual-slot 28
slot 13 slot-type 333 port-type 113 number 4 port-type 60 number 16  virtual-slot 29
!
module provision switch 2
slot 1 slot-type 333 port-type 113 number 4 port-type 60 number 16  virtual-slot 33
slot 3 slot-type 328 port-type 60 number 8  virtual-slot 35
slot 7 slot-type 318 port-type 31 number 3 port-type 60 number 2  virtual-slot 39
slot 8 slot-type 318 port-type 31 number 3 port-type 60 number 2  virtual-slot 40
slot 9 slot-type 156 port-type 31 number 24  virtual-slot 41
slot 11 slot-type 156 port-type 31 number 24  virtual-slot 43
```

3. Enter the **module provision switch** [**1**|**2**] global configuration mode command to remove the provisioning information for the modules. For example:

```
Router# configure terminal
Router(config)# module provision switch 1
Router(config-prov-switch)# no slot 13 slot-type 333 port-type 113 number 4
port-type 60 number 16  virtual-slot 29
Router(config-prov-switch)# exit
Router(config)# module provision switch 2
Router(config-prov-switch)# no slot 1 slot-type 333 port-type 113 number 4
port-type 60 number 16  virtual-slot 33
Router(config-prov-switch)# end
```

4. Verify that no configuration information remains for any of the modules.
5. Save the configuration.
6. Perform the EFSU downgrade.

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.

Release 15.0(1)SY10

None.

Release 15.0(1)SY9

None.

Release 15.0(1)SY8

None.

Release 15.0(1)SY7a

None.

Release 15.0(1)SY7

None.

Release 15.0(1)SY6

None.

Release 15.0(1)SY5

None.

Release 15.0(1)SY4

- CLI associated with the Services SPA Carrier (SSC) and IPsec SPA (CSCty04467)

  Old Behavior: Release 12.2(50)SY and rebuilds, Release 15.0(1)SY and rebuilds, and Release 15.1(1)SY and later releases do not support the Services SPA Carrier (SSC) and IPsec SPA, but the associated CLI is present and can cause problems if entered.

  New Behavior: The CLI associated with the Services SPA Carrier (SSC) and IPsec SPA is not present.

Release 15.0(1)SY3

- BGP Processing of the Removal of Private AS Numbers from AS Path

  Old Behavior: When the **neighbor remove-private-as** command is configured and a route-map without a **continue** clause is configured, the processing order is:

  1. **neighbor remove-private-as processing**

  2. **set as-path prepend** or **set as-path prepend last-as**

  If the route-map contains a continue clause, the processing order is reversed.

  New Behavior: When the **neighbor remove-private-as** command is configured and a route-map is configured (whether it has a **continue** clause or not), the processing order is always:

  1. **neighbor remove-private-as processing**

  2. **set as-path prepend** or **set as-path prepend last-as**

- Switching mode restrictions for 1-Gigabit Ethernet ports are changed.

  Old Behavior: You must shut down 1-Gigabit Ethernet ports before you enter the **platform qos 10g-only** command.

  New Behavior: You must shut down 1-Gigabit Ethernet ports and ensure that no trust state and the default class of service (CoS) are configured before you enter the **platform qos 10g-only** command.

Release 15.0(1)SY2

- Changes to the **no** form of the **exec-timeout** command

  Old Behavior: When using the **no** form of the **exec-timeout** command, the EXEC command interpreter is reconfigured to wait for user input for the configuration default period of 10 min 0 sec.

  New Behavior: The **no** form of the exec-timeout command configures a wait period of 0 min 0 sec before timeout.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-76805E6F-9E89-4457-A9DC-5944C8FE5419

- Output changes for the show module command

  Old Behavior: For WS-SVC-NAM3-6G-K9, the **show module** command displays “Trifecta NAM Module”. For WS-SVC-WISM2, the show module command displays “WiSM Jian Service Module”.

  New Behavior: For WS-SVC-NAM3-6G-K9, the **show module** command displays “Network Analysis Module 3”. For WS-SVC-WISM2, the **show module** command displays “WiSM 2 WLAN Service Module”.

- WS-X6904-40G-2T requirement for the bandwidth command

  Old Behavior: On WS-X6904-40G-2T ports, the **bandwidth** command is required if you configure any nondefault values for any other queueing commands on the port, but the CLI does not enforce the requirnment.

  New Behavior: On WS-X6904-40G-2T ports, the CLI enforces the requirement for the **bandwidth** command if you configure any nondefault values for any other queueing commands on the port.

- Unsupported energywise management configuration mode command

  Old Behavior: The unsupported **energywise management** configuration mode command was present in the CLI.

  New Behavior: The unsupported **energywise management** configuration mode command is not present in the CLI.

New Features in Release 15.0(1)SY10

These sections describe the new features in Release 15.0(1)SY10, 12 Feb 2016:

- New Hardware Features in Release 15.0(1)SY10, page 38
- New Software Features in Release 15.0(1)SY10, page 38

New Hardware Features in Release 15.0(1)SY10

None.

New Software Features in Release 15.0(1)SY10

None.

New Features in Release 15.0(1)SY9

These sections describe the new features in Release 15.0(1)SY9, 11 Aug 2015:

New Hardware Features in Release 15.0(1)SY9

None.

New Software Features in Release 15.0(1)SY9

None.

New Features in Release 15.0(1)SY8

These sections describe the new features in Release 15.0(1)SY8, 20 Feb 2015:

New Hardware Features in Release 15.0(1)SY8

None.

New Software Features in Release 15.0(1)SY8

None.

New Features in Release 15.0(1)SY7a

These sections describe the new features in Release 15.0(1)SY7a, 01 Oct 2014:

New Hardware Features in Release 15.0(1)SY7a

None.

New Software Features in Release 15.0(1)SY7a

None.

New Features in Release 15.0(1)SY7

These sections describe the new features in Release 15.0(1)SY7, 01 Aug 2013:

New Hardware Features in Release 15.0(1)SY7

None.

New Software Features in Release 15.0(1)SY7

None.

New Features in Release 15.0(1)SY6

These sections describe the new features in Release 15.0(1)SY6, 07 Feb 2013:

New Hardware Features in Release 15.0(1)SY6

None.

New Software Features in Release 15.0(1)SY6

None.

New Features in Release 15.0(1)SY5

These sections describe the new features in Release 15.0(1)SY5, 23 Aug 2013:

New Hardware Features in Release 15.0(1)SY5

None.

New Software Features in Release 15.0(1)SY5

- IP Access List Entry - Persistent Sequence Numbering Across Reloads—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_acl/configuration/12-2sx/sec-acl-seq-num-persistent.html

New Features in Release 15.0(1)SY4

These sections describe the new features in Release 15.0(1)SY4, 21 Mar 2013:

New Hardware Features in Release 15.0(1)SY4

None.

New Software Features in Release 15.0(1)SY4

None.

New Features in Release 15.0(1)SY3

These sections describe the new features in Release 15.0(1)SY3, 26 Nov2012:

New Hardware Features in Release 15.0(1)SY3

None.

New Software Features in Release 15.0(1)SY3

- DHCPv6 - Relay chaining for Prefix Delegation—See this publication:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-relay-agent.html

New Features in Release 15.0(1)SY2

These sections describe the new features in Release 15.0(1)SY2, 16 Jul 2012:

New Hardware Features in Release 15.0(1)SY2

None.

New Software Features in Release 15.0(1)SY2

None.

New Features in Release 15.0(1)SY1

These sections describe the new features in Release 15.0(1)SY1, 24 Feb 2012:

New Hardware Features in Release 15.0(1)SY1

- 4-Port 40-Gigabit Ethernet Switching Module (WS-X6904-40G-2T; Cisco SFP-10G-LR)
- 96-port 10/100TX RJ-21 Ethernet Switching Module (WS-X6196-RJ-21, WS-X6196-21AF)
- ASA services module (WS-SVC-ASA-SM1-K9)
- Network Analysis Module 3 (WS-SVC-NAM3-6G-K9)
- Cisco 7609-S chassis (CISCO7609-S)

Note Upgrade to Release15.0(1)SY1 or later before installing any of these modules (see the "EFSU Compatibility" section on page 34).

New Software Features in Release 15.0(1)SY1

- BFD - Static Route Support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bfd/configuration/15-sy/irb-bi-fwd-det.html
- BFD - VRF Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd.html
- Cisco TrustSec L3 Identity Port Mapping—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html#Manually_Configuring_IP-Address-to-SGT_Mapping
- Cisco TrustSec Subnet to SGT Mapping—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html#Manually_Configuring_IP-Address-to-SGT_Mapping
- Cisco TrustSec VLAN to SGT Mapping—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html#Manually_Configuring_IP-Address-to-SGT_Mapping
- Classification TCAM banks allocation—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/qos_restrictions.html#General_Guidelines
- EIGRP IPv6 VRF-Lite—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_eigrp/configuration/guide/ire_cfg_eigrp.html
- Energywise Phase - 2—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/energywise/phase2/ios/configuration/guide/ew_v2.html

- Enhanced IPv6 Neighbor Discovery Cache Management—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-addrg-bsc-con.html

- EVN EIGRP—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-confg.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-overview.html

- EVN OSPF—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-confg.html
  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-overview.html

- EVN - Route Replication—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-shared-svcs.html

- EVN Traceroute—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-shared-svcs.html

- EVN VNET trunk—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-15-sy-book.html

- Fast UDLD—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/udld.html#Fast_UDLD

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/udld.html#Configuring_Fast_UDLD

- Flexible NetFlow: 32 bit AS Number Support—With Release 15.0(1)SY1 and later releases, Flexible NetFlow supports 32-bit autonomous system (AS) numbers. Flexible NetFlow can capture and export 32-bit numbers as well as 16-bit numbers. If you specify the 4-octet keyword in the collect routing or match routing command, you configure the 32-bit autonomous system number as a nonkey or key field; otherwise, you configure the 16-bit version. If you configure both a 32-bit version and a 16-bit version within a record, only the 32-bit version applies. The 32-bit AS numbers have a different v9 export type than that used for 16-bit AS numbers. Your collector and analysis infrastructure should be able to process values for 32-bit AS numbers.

  The following commands have been added in this release to support this feature:

  ```
  [match | collect] routing destination as [4-octet]
  [match | collect] routing destination as peer [4-octet]
  [match | collect] routing source as [4-octet]
  [match | collect] routing source as peer [4-octet]
  ```

  For more information on export types, see the NetFlow Layer 2 and Security Monitoring Exports document:

  http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/nf_lay2_sec_mon_exp.html

  Note With Release 15.0(1)SY1 and later releases, Flexible Netflow is supported in the IP base image.

- IPv6 Route Health Injection (IPv6 RHI) on ACE-30—Release 15.0(1)SY1 and later releases provide support on the switch for the IPv6 RHI feature implemented on the ACE30-MOD-K9.
- IPv6 Routing: OSPF for IPv6 (OSPFv3) Authentication Support with IPsec—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-ospf.html

- IPV6 VACL (Vlan Access Control List)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/vlan_acls.html#IPV6_VACL_(Vlan_Access_Control_List)
- mVPN with L3VPN over mGRE—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/ipv4_multicast_vpn.html#Information_About_mVPN_with_L3VPN_over_mGRE
- OSPF SNMP ifIndex Value for Interface ID—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_snmp_ifindex.html
- OSPFv3 IPSec ESP Encryption and Authentication—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-ospf.html
- Static Route Support for BFD over IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-bfd.html
- Sup2T NVRAM Battery Monitor GOLD test—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/diagnostic_tests.html#TestNVRAMBatteryMonitor
- TrustSec SGACL Feature Support on IP Base k9 Images—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/release/notes/rn_cts_crossplat.html
- Virtual Network trunk—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-overview.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-confg.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-shared-svcs.html
- vrf-aware traceroute with vrf name—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/15-sy/evn-mgt-ts.html
- VRF-lite aware NAT for non-overlapping ip addresses:

Note NAT VRF-lite is supported **only** with nonoverlapping IP addresses.

The following is an example of the supported configuration:

```
ip nat outside source static real_ip_address nat_ip_address

interface vlan vlan_ID_X
  ip nat inside
  ip vrf forwarding vrf_name
  ip address vrf_ip_add mask_value

interface vlan vlan_ID_Y
  ip nat outside
  ip vrf forwarding vrf_name
  ip address vrf_ip_add mask_value
! Configuration of up to 248 interfaces supported.
!
ip nat inside source static local_ip1 global_ip1 vrf vrf_name
ip nat inside source static local_ip2 global_ip2 vrf vrf_name
!
! Up to 124 of these statements
```

Note

- This feature is not supported if there are overlaping IP address ranges among the VRF-lite domains. Support for this feature is limited to VRF-lite configurations with non-overlapping IP addresses.
- This feature has limited support based on the provided sample configuration.

- VSS VSL Multicast Fast Redirect—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/virtual_switching_systems.html#VSS_VSL_Multicast_Fast_Redirect

New Features in Release 15.0(1)SY

These sections describe the new features in Release 15.0(1)SY, 27 Sep 2011:

- New Hardware Features in Release 15.0(1)SY, page 45
- New Software Features in Release 15.0(1)SY, page 46

New Hardware Features in Release 15.0(1)SY

- Application Control Engine (ACE) module (ACE30-MOD-K9)
- Wireless Services Module 2 (WiSM2):
  - WS-SVC-WISM2-1-K9—Wireless Services Module 2 with 100 AP Support License
  - WS-SVC-WISM2-3-K9—Wireless Services Module 2 with 300 AP Support License
  - WS-SVC-WISM2-5-K9—Wireless Services Module 2 with 500 AP Support License

These hardware products are also supported in Release 12.2SY:

- Supervisor Engine 2T-10GE with PFC4XL (VS-S2T-10G-XL)
- Supervisor Engine 2T-10GE with PFC4 (VS-S2T-10G)
- Policy Feature Card 4XL (PFC4XL; VS-F6K-PFC4XL)
- Policy Feature Card 4 (PFC4; VS-F6K-PFC4)
- Distributed Forwarding Card 4XL (DFC4XL: WS-F6K-DFC4-EXL and WS-F6K-DFC4-AXL)
- Distributed Forwarding Card 4 (DFC4: WS-F6K-DFC4-E and WS-F6K-DFC4-A)
- 8-port 10-Gigabit Ethernet X2 module:
  - WS-X6908-10G-XL (has WS-F6K-DFC4-EXL)
  - WS-X6908-10G (has WS-F6K-DFC4-E)

Note

- Release 15.0(1)SY supports the hardware listed in the "Supported Hardware" section on page 4.
- Some switching modules previously supported with a DFC3 can be ordered with a DFC4:
  - WS-X6816-10T-2T, WS-X6716-10T 16-Port 10-Gigabit Ethernet Copper Switching Module, page 12
  - WS-X6816-10G-2T, WS-X6716-10GE 16-Port 10-Gigabit Ethernet X2 Switching Module, page 13
  - WS-X6848-SFP-2T, WS-X6748-SFP 48-Port Gigabit Ethernet SFP Switching Module, page 15
  - WS-X6848-TX-2T, WS-X6748-GE-TX, page 16

New Software Features in Release 15.0(1)SY

Note Release 15.0(1)SY and later releases Advanced Enterprise images support FIPS encryption.

- Enter the **fips** global configuration mode command to enable FIPS encryption.
- Enter the **no fips** global configuration mode command to disable FIPS encryption.
- Enter the **show fips** command to display the enable state of FIPS encryption.
- In VSS mode, you cannot configure the FIPS encryption mode without VSL encryption. To avoid a system shutdown, enable VSL encryption before you enable FIPS encryption mode. (CSCts96040, CSCtx58304)

You can support management connections with FIPS encryption.

- For SSH with FIPS encryption:
  - Use SSHv2
  - Use the AES or TDES encryption algorithms
- For SSL/TLS with FIPS encryption:
  - Use TLSv1.0 or SSLv3.1 or later versions
  - Use the AES or TDES encryption algorithms

- Airdam requirement message for NEBS compliance—The software displays messages if the hardware configuration of the switch is changed in a way that might impact NEBS compliance.
- BFD IPv6 Encaps Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html
- BGP Event Based VPN Import—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_event_vpn_import.html
- BGP Neighbor Policy—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_basic_net.html
- BGP Per Neighbor SOO Configuration—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor_soo.html

- BGP RT changes without PE-CE neighbor impact—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_event_vpn_import.html
- eFSU (Enhanced Fast Software Upgrade)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/issu_efsu.html
- Enabling OSPFv2 on an Interface Using the ip ospf area Command—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-imode-ospfv2.html
- Flexible NetFlow: ISSU / SSO Support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-sy/support-issu-sso-xe.html
- GOLD Support for MediaNet 2.2—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/diagnostic_tests.html#TestMediaLoopback
- HSRP: Global IPv6 Address—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ip6-fhrp.html
- IGMPv3 Host Stack—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/15-sy/imc_customizing_igmp.html
- IP Multicast Load Splitting - Equal Cost Multipath (ECMP) using S, G and Next-hop—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_optim/configuration/15-sy/imc_load_splt_ecmp.html
- IP-RIP Delay Start—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_rip/command/reference/irr_rip.html#ip_rip_initial-delay
- IPv6: NSF & Graceful Restart for MP-BGP IPv6 Address Family—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mptcl-bgp.html
- IS-IS Support for an IS-IS Instance per VRF for IP—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-sy/irs-instance-vrf.html
- ISSU - IPv4 Multicast—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_high_availability.html
- ISSU - IPv6 Multicast—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- ISSU - MPLS VPN 6VPE & 6PE ISSU support—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_6vpe_6pe_issu_sso.html
- MediaTrace 1.0—See this publication:

  http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/mm_mediatrace.html
- MPLS VPN - Inter-AS Option AB—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_ias_optab.html
- MPLS VPN InterAS AB+—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_ias_optab.html

- MPLS VPN over mGRE—See this publication:

  http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_mplsvpnomgre.html

  Note In releases earlier than Release 15.0(1)SY1, the MPLS VPN over mGRE feature does not support multicast traffic (CSCto95014).

- MVPN - Data MDT Enhancements—Multicast distribution tree (MDT) groups were selected at random when the traffic passed the threshold and there was a limit of 255 MDTs before they were reused. The MVPN - Data MDT Enhancements feature provides the ability to deterministically map the groups from inside the VPN routing and forwarding (S,G) entry to particular data MDT groups, through an access control list (ACL). The user can now map a set of VPN routing and forwarding (S,G) to a data MDT group in one of the following ways:
  - 1:1 mapping (1 permit in ACL)
  - Many to 1 mapping (many permits in ACL)
  - Many to many mapping (multiple permits in ACL and a nonzero mask data MDT)

  Because the total number of configurable data MDTs is 1024, the user can use this maximum number of mappings in any of the described combinations.
- NSF/SSO - IPv6 Multicast—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- OSPF - Demand Circuit disable—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_cfg.html
- OSPF Graceful Shutdown—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-ttl.html
- OSPF support for NSSA RFC 3101—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-cfg.html
- OSPF TTL Security Check—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-ttl.html
- OSPFv2 Local RIB—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-local-rib.html
- OSPFv3 BFD—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-bfd.html
- OSPFv3 Fast Convergence - LSA and SPF throttling—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-ospf.html
- OSPFv3 Graceful Restart—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-ospf.html
- Parser concurrency and locking Improvements—See this publication:

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-lock.html
- Performance Monitor (Phase 1)—See this publication:

  http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/mm_pasv_mon.html

- RSVP - Previous Hop Overwrite—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/15-0sy/rsvp_prvs_hop_overwrt.html
- RSVP for flexible BW interface—See this publication:

  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html
- RSVP Over DMVPN—See this publication:

  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html
- RSVP Support for Ingress Call Admission Control—See this publication:

  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/config_rsvp.html
- RSVP-VRF Lite Admission Control—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/15-0sy/rsvp_vrf_lite_adm_ctrl.html
- Service Advertisement Framework (SAF)—See this publication:

  http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/saf_cg.html
- SSO - MPLS VPN 6VPE & 6PE SSO support—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_6vpe_6pe_issu_sso.html
- VPLS integrated routing and bridging on cat6500—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/vpls.html#VPLS_Integrated_Routing_and_Bridging
- VSL Encryption—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.0SY/configuration/guide/virtual_switching_systems.html#Configuring_VSL_Encryption

Note In VSS mode, you cannot configure the FIPS encryption mode without VSL encryption. To avoid a system shutdown, enable VSL encryption before you enable FIPS encryption mode.

Software Features from Earlier Releases

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

Unsupported Commands

Release 15.0(1)SY does not support **mls** commands or **mls** as a keyword. If you are copying Sup720 running configuration to Sup2T, the packets per burst in **mls rate-limit** command overrides the current burst value and sets the burst value to 1. You need to manually configure packets per burst using the **platform rate-limit** command.

See this document for a list of some of the **mls** commands that have been replaced:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/replacement_commands.html

Note Some of the replacement commands implemented in Release 15.0(1)SY support different keyword and parameter values than those supported by the Release 12.2SX commands.

Release 15.0(1)SY does not support these commands:

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

Unsupported Features

Note The IPsec Network Security feature (configured with the crypto ipsec command) is not supported.

These features are not supported in Release 15.0(1)SY:

- WAN features
- Performance Routing (PfR)
- OER Border Router Only Functionality
- IOS Server Load Balancing (SLB)

  Note Release 15.0(1)SY supports server load balancing (SLB) as implemented on the Application Control Engine (ACE) module (ACE20-MOD-K9).

- AppleTalk
- Cisco Group Management Protocol (CGMP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Dynamic creation of L2 entries for Multicast source-only traffic
- IDS Copy

  Note Release 15.0(1)SY supports the SPAN and VACL redirect features, which have equivalent functionality.

- Inter-Switch Link (ISL) trunking

  Note Release 15.0(1)SY supports IEEE 802.1Q trunking.

- NAC - L2 IP NAC LAN Port IP
- NetWare Link-Services Protocol (NLSP)
- Network Based Application Recognition (NBAR)
- IPX Access Control List Violation Logging
- IPX Access List Plain English Filters
- IPX Control Protocol
- IPX Encapsulation for 802.10 VLAN
- IPX Multilayer Switching (IPX MLS)
- IPX Named Access Lists
- IPX SAP-after-RIP
- Per-VLAN Spanning Tree (PVST) mode (**spanning-tree mode pvst** global configuration mode command)

  Note Release 15.0(1)SY supports these spanning tree protocols:
  —Rapid Spanning Tree Protocol (RSTP):
  - **spanning-tree mode rapid-pvst** global configuration mode command
  - Enabled by default

  —Multiple Spanning Tree Protocol (MSTP):
  - **spanning-tree mode mst** global configuration mode command
  - Can be enabled

- Router-Port Group Management Protocol (RGMP)
- Stub IP Multicast Routing
- TCP Intercept

  Note Release 15.0(1)SY supports the Firewall Services Module (WS-SVC-FWM-1-K9).

- Integrated routing and bridging (IRB)
- Concurrent routing and bridging (CRB)
- Remote source-route bridging (RSRB)
- AppleTalk
- Distance Vector Multicast Routing Protocol (DVMRP)

Restrictions

Identifier	Component	Description
CSCvi28828	nat	Dynamic Nat preferred over Static Nat with Route maps, For overlapping IP addresses.
CSCtr15373	cat6000-acl	Standby crashes when copy config from tftp to running-config
CSCts70036	cat6000-acl	With mld snooping,no egress traff seen on v6 vacl vlan after reload/sso.
CSCub95435	cat6000-env	Sup2T can't deliver 100% throughput on certain 67xx/68xx line cards
CSCsh58964	cat6000-fabric	BFD node down is detected by OIR
CSCub86977	cat6000-l2-infra	c4hd1: Config sync seen with +encapsulation dot1Q 100
CSCsv98626	cat6000-l2-mcast	Ear8 MVR interaction with IGMP snooping: when IGMPSN is disabled
CSCta03980	cat6000-l2-mcast	PIMSN:No multicast data flood with IGMPSN disable & PIMSN enabled
CSCta83272	cat6000-l2-mcast	IGMP snooping not supported over VPLS ckt.
CSCth16692	cat6000-l2-mcast	IGMPSN report suppression failed to redir MIXED mode same group joins
CSCtl86457	cat6000-l2-mcast	RL for IP Multicast Control frames doesn't work properly
CSCto92033	cat6000-l2-mcast	Multicast data frames blackholed if RTR-GRD is ON and Snooping is OFF
CSCtd18777	cat6000-mcast	NAT config punt Multicast frames to Process Switching
CSCtf59230	cat6000-mcast	Earl8 performance impact on Bidir-PIM routing cases
CSCtg58715	cat6000-mcast	"show mac addr static vlan" CLI does not display mcast entries
CSCtg91060	cat6000-mcast	IPV6 PING not working on SVI when MLD Snooping is turned ON
CSCti43981	cat6000-mcast	HW BiDir mroutes not restored after temporarily losing the RP path
CSCti97217	cat6000-mcast	Traffic forwarding to incorrect fabric channel after PO shu/no shut
CSCto75104	cat6000-mcast	Mcast Traffic blkholing upon VSS DA when all VSL links are on DFC
CSCtr05033	cat6000-mpls	Caveats for MPLS VPN over mGRE
CSCtq43621	cat6000-rommon	fc2 image:Verification FAILED err seen on bootup whn cs_fips disable_dev
CSCtj16159	cat6000-svc	standby reboots twice and comes up in rpr due to config sync fail
CSCtw91029	cts	clear cts role-based counters does not give expected results
CSCth50799	pim	Multicast traffic slow convergence with 20k-30k mroute entries

Caveats in Release 15.0SY

Open Caveats in Release 15.0SY

Identifier	Component	Description
CSCui79597	cat6000-hw-fwding	Lif entry is not getting updated on minitrunk port
CSCtr29528	cat6000-hw-fwding	NO_ROUTE RL fails due to OAL
CSCts43808	cat6000-l2-infra	TB seen on config replace and subinterface po on vnet trunk down.
CSCtt33433	cat6000-l2-mcast	(S,G) MAC with missing ports blocks egress traffic with PIM snooping
CSCtu03447	cat6000-ltl	Mem leak @ ltl_set_sw_status_cb with MEC,VSL,rxvr ports on same linecard
CSCtu31096	cat6000-span	Unexpected mcast traffic copied to SPAN destination port in MVPN setup
CSCtu37676	cat6000-svc	On FWSM insertion, standby sup may crash or active report not enough mem
CSCtx93042	cat6000-svc	MA1B:ASA-SM/ACE/FWSM VLANs not getting removed on VSS setup from SUP
CSCua96981	cat6000-svc	Some module may reset after SSO in a heavy loaded chassis
CSCuq76713	os-logging	Crash is seen on adding "loggin ip " and "loggin host ip"
CSCtx92952	cat6000-svc	SUP crash when issuing show upgrade fpd file ftp/tftp cmd

Identifier	Component	Description
CSCty14223	cat6000-svc	Trifecta project name seen in show module output of NAM3
CSCtx28226	cat6k-vs-infra	"redundancy reload peer" leads to dual-active with mcast traffic
CSCtx15860	cts	Continues t/b message in id_get when ip prefixes run out of space
CSCts59702	cts	CTS dot1x link not up between CTS capable and CTS aware cards in E8
CSCts96040	cts	VSL configuration check before reloading a VSS switch with FIPS
CSCtl50549	itasca-sup	CNMA1: ACE RHI Routes are withdrawn after doing an SSO
CSCte37338	ospf	Error messages are thrown when creating virtual link.
CSCty05150	ospf	OSPF default summary route withdrawn after SSO switchover on ABR
CSCts16791	vrfinfra	cnma1b: vnet cli present when vnetcore to switchport and then to routed
CSCty37233	vrfinfra	VNET:stby crash @swidb_if_index_assign after swover with vrf vnet subif

Caveats Resolved in Release 15.0(1)SY10

- CSCuq24202—Resolved in 15.0(1)SY10

  Symptom: A vulnerability in the TCL script interpreter of Cisco IOS Software might allow an authenticated, local attacker to escalate its privileges from those of a non-privileged user to a privileged (level 15) user, allowing a non-privileged user to execute privileged commands.

  The vulnerability is caused due to an error on resetting VTY privileges after running a TCL script. An attacker could exploit this vulnerability by establishing a session to an affected device immediately after a TCL script has been run.

  Conditions: This behavior is timing dependent because the attacker needs to log-in to the device immediately after the TCL script finishes execution.

  Workaround: None

  PSIRT Evaluation:

  The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.6/5.5:

  http://tools.cisco.com/security/center/cvssCalculator.x?vector=AV:N/AC:H/Au:S/C:N/I:N/A:C/E:H/RL:U/RC:C&version=2.0

  CVE ID CVE-2015-4185 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

- CSCuv71155—Resolved in 15.0(1)SY10

  Symptom: For dynamic ACL, the l4op programmed for user1 will change if an attempt is made to program user2 without any LOU.

  Conditions: User1 has been programmed which is issuing an LOU register.

  Workaround: None

Caveats Resolved in Release 15.0(1)SY9

- CSCur70505—Resolved in 15.0(1)SY9

  Symptom: A 6500 reloads after negotiating an IPSec tunnel with ASR9000.

  Conditions: The 6500 needs to run 12.2(33)SXJ8 and the IPsec engine must be a WS-SSC-600 WS-IPSEC-3 combination.

  This crash does not happen with 7600-SSC-400 IPSEC-2 combination.

  Workaround: None

  More Info: A vulnerability in the IKE subsystem of Cisco WS-IPSEC-3 service module could allow an authenticated, remote attacker to cause a reload of the Catalyst switch. The vulnerability is due to insufficient bounds checks on a specific message during the establishment of an IPSEC tunnel. An attacker could exploit this vulnerability by successfully establishing an IKE session and sending the offending packet during subsequent negotiations. An exploit could allow the attacker to cause a denial of service by forcibly reloading the switch.

  PSIRT Evaluation:

  The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 4.9/4.9:

  http://tools.cisco.com/security/center/cvssCalculator.x?vector=AV:N/AC:H/Au:S/C:N/I:N/A:C/E:H/RL:U/RC:C&version=2.0

  CVE ID CVE-2015-0771 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:

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

- CSCuu18788—Resolved in 15.0(1)SY9

  Symptom: An error similar to the following may be observed in the syslogs of a Cisco IOS device:

  **May 4 13:40:46.760: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error, -PC= :200CD000+1502CF4*

  -Traceback= 1#e06f72c62c6bef347348f23bdccc4b7f :200CD000+30D51C0 :200CD000+30D5588 :200CD000+3103724 :200CD000+6F2FD4C :200CD000+1502CF4 :200CD000+15033E0 :200CD000+446FF08 :200CD000+446E0B0 :200CD000+443DA40 :200CD000+442D158 :200CD000+445C0F8

  No functional impact is observed.

  Conditions: This is currently believed to affect all released versions of IOS code which support the CISCO-ENTITY-EXT-MIB.

  This may occur when polling the ceExtSysBootImageList object in CISCO-ENTITY-EXT-MIB. This object returns a semicolon-separated list of boot statements on the device, similar to the following:

CISCO-ENTITY-EXT-MIB::ceExtSysBootImageList.5000 = STRING: "flash bootflash:cat4500e-universalk9.SPA.03.04.05.SG.151-2.SG5.bin;flash bootflash:cat4500e-universalk9.SPA.03.04.02.SG.151-2.SG2.bin"

The DATACORRUPTION error will occur under a specific corner case, where the total length of one or more complete boot variables (counted starting after the 'boot system' token) is less than 255 bytes, BUT when semicolons are added (one per boot statement) meets or exceeds this number.

Consider the following example:

boot system bootflash:this_is_a_128_character_long_boot_statement_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

boot system bootflash:this_is_a_125_character_long_boot_statement_yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy

128 + 125 + 2 semicolons = 255 characters (bytes)

If another boot statement is added after this, the DATACORRUPTION error will be seen and the SNMP query will return invalid data.

Workaround: Reduce the quantity/length of configured boot variables.

More Info: This is not known to have any functional impact outside of the (potentially alarming) error message. The error will only be printed once, but subsequent occurrences of this condition can be seen via the 'show data-corruption' command.

- CSCum94811—Resolved in 15.0(1)SY9

  Symptom: A vulnerability in the TCP input module of Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak and eventual reload of the affected device.

  Conditions: The vulnerability is due to improper handling of certain crafted packet sequences used in establishing a TCP three-way handshake. An attacker could exploit this

  vulnerability by sending a crafted sequence of TCP packets while establishing a thee-way handshake. A successful exploit could allow the attacker to cause a

  memory leak and eventual reload of the affected device.

  Workaround: None

  More Info: Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150325-tcpleak

Note The March 25, 2015, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. The advisories address vulnerabilities in Cisco IOS Software and Cisco IOS XE Software. Individual publication links are in Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication at the following link: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html

- CSCuo04400—Resolved in 15.0(1)SY9

  Symptom: Box can crash.

  Conditions: Crash on receiving a malformed packet via codenomican tool.

  Workaround: None.

More Info: None

- CSCus19794—Resolved in 15.0(1)SY9
  Symptom: Cisco IOS and IOS-XE IPv6 FHS Send Denial of Service Vulnerability.
  Workaround: None
  More Info: None

Identifier	Component	Description
CSCuo11314	cat6000-l2	6500: Memory leak @parser_get_block
CSCth26920	tcl-bleeding	TCL: ungraceful exit from tclsh can leave the Tcl Server running
CSCuf85318	cat6000-env	temperature crossed threshold #1(=0C) on a Ringar and powers down

Caveats Resolved in Release 15.0(1)SY8

Identifier	Component	Description
CSCty30788	cat6000-acl	NF record not accounting phy input intf after enabling DAI
CSCuh43325	cat6000-env	Sup 720 switchover causes incorrect show power output
CSCup90562	cat6000-firmware	ws-x6904 module sets CFI to 1 and causes drops downstream
CSCun65772	cat6000-firmware	Cat6500 VSS crash due to watchdog timeout, process = slcp process
CSCuq13843	cat6000-hw-fwding	Sup2T LIF missprogramming when port-channel is configured
CSCuj54021	cat6000-ipc	Crash seen in icc_mcast_request
CSCuo11314	cat6000-l2	6500: Memory leak @parser_get_block
CSCty01365	cat6000-netflow	Supervisor 2T or Line Card Resets due to Netflow Interrupt
CSCuh94242	cat6000-qos	Agg. policer with 'platform qos police distributed' drops all traffic
CSCuj96561	cat6000-svc	wism redundancy-vlan and wism service-vlan must reject vlans in trunk
CSCun63132	ethernet-lldp	Single LLDP frame w/bad TLV hangs switch - power cycle required
CSCuo84660	ifs	copy command yields DATACORRPUTION error
CSCup93882	ipc	Crash @ ipc_compare_seats - IPC table entry freed up when seat is alive

Identifier	Component	Description
CSCtw74339	ipc	IPC errors (RPC timeouts) were observed while polling cempMemPoolEntry.
CSCtx78552	ipc	"CR10K API Stat" causing leak in middle buffer on 5x20 LC
CSCti18397	mem	Active RP crashed by stby due to missed keepalive
CSCuq09245	os-logging	Crash is seen on adding "loggin ip " and "loggin host ip"
CSCuo24560	sea-log	I/O memory leak with active SUP due to issues with standby SUP
CSCuj23802	tcp	SUP2T crash while cleaning up a Telnet connection

Caveats Resolved in Release 15.0(1)SY7a

Identifier	Component	Description
CSCuq09245	os-logging	Crash is seen on adding "loggin ip " and "loggin host ip"

Caveats Resolved in Release 15.0(1)SY7

Identifier	Component	Description
CSCtt28573	c7600-esm-20	ES20 crash @ml_update_datastruct due to Illegal access to a low address
CSCuh05334	cat6000-acl	CPU went high and standby crashed while pushing ACLs - SUP 2T
CSCue65728	cat6000-acl	SUP-2T--VRF NAT stops working after 24-48hrs into operation
CSCun51501	cat6000-acl	Crash on active supervisor when standby is reloading
CSCuh07066	cat6000-cm	Sup2T - ACL Tcam count - Malfunction - Adds additional ACL's - TCAM Leak
CSCuo66521	cat6000-cm	Unexpected reboot on switch when removing IPv6 config in the global mode
CSCug90305	cat6000-env	Power deny of 6148-ge-tx-AF/AT interface with 2602 factory reset
CSCui25588	cat6000-env	No power enable on empty slot will not keep a new linecard powered off
CSCul39734	cat6000-env	Cat6k VSS incorrect ceDisplayState & ceDisplayColor for PS "FAN OK"

Identifier	Component	Description
CSCuj13346	cat6000-env	VSS ciscoEnvMonRedundantSupplyNotification not sent from active chassis
CSCuh75585	cat6000-env	system power total restricted to 2268w with 2700 PS in 7606-S chassis
CSCum60489	cat6000-env	System LED shows amber when power supplies are restored on sup2t VSS
CSCue58955	cat6000-filesys	sup2t: LC file systems are not destroyed in Active upon reset
CSCui17608	cat6000-firmware	VACL unable to capture the routed traffic on 6500 coming from FWSM
CSCuj32632	cat6000-firmware	sup2t:traffic not received from 6848-SFP ports due to rx datapath stuck
CSCum19472	cat6000-firmware	Sup2T console is displaying "pal_power_set() bad ps_id 2"
CSCue94578	cat6000-firmware	C4 VSS - VLAN Tag removed while crossing the VSL link
CSCuj48794	cat6000-firmware	Sup2T may give false EARL temp readings
CSCug79067	cat6000-hw-fwding	Capture TCAM state when IPV6 exception occurs
CSCuj65447	cat6000-l2-ec	sup2t: crash on cat6k seen if L2 loops exists in network
CSCun17857	cat6000-l2-infra	Standby switch joins VSS in RPR mode after switchover
CSCui86318	cat6000-ltl	unicast flooding because mac address not learnt correctly across DFCs
CSCug86296	cat6000-netflow	Sup2T: EARL8 Netflow ECC enhancement
CSCta32922	cat6000-portsecur	SP crash due to heartbeat failure.
CSCuh98603	cat6000-routing	sup2t :: uRPF dropping packets
CSCun21946	cat6000-routing	SUP2T VSS "no ip redirect" is removed on loopback interface
CSCug47095	cat6000-snmp	vlanTrunkPortDynamicStatus is wrong for members of PO
CSCuh21792	cat6000-snmp	Update implementation for function vtpmib_get_trunk_status
CSCun20430	cat6000-sw-fwding	ospfv3 control packets entered incorrect queue
CSCtl70569	eventmgr	Traceback seen under event manager applet mode
CSCsu52582	ios-authproxy	unbounded while loop in ap_ftp_read_from_client()
CSCum28609	ip	SUP2T failed to send broadcast ping packet
CSCuj08831	ipc	Crash @ ipc_compare_seats part 2

Identifier	Component	Description
CSCum95311	ip-pbr	ip next-hop recursive not forwarding traffic
CSCuj34455	nat	NAT Process Switches all TCP port 139 Traffic
CSCui94118	nat	static NAT vrf removed upon removal of "vrf definition <vrf_name>"
CSCun86871	nat	Switch crashes due to nat processing Real Audio Traffic
CSCul71047	os	RF Client Cat6k Platform First Client(1319) notification timeout
CSCud53872	os-logging	ASR1K sends syslogs with the wrong source address after a reboot.
CSCtx45583	ts	% Ambiguous command: "login authentication default " under VTY line

Caveats Resolved in Release 15.0(1)SY6

Identifier	Component	Description
CSCub04965	aaa	TCP Session hung causing Packet loss
CSCuh43252	aaa	unable to login and high cpu when authenticating with TACACS
CSCug04222	cat6000-acl	SUP2T not forwarding unicast DHCP ACK when acting as relay agent
CSCui26454	cat6000-cm	c4mk1: Line card is getting reset while large acl is applied.
CSCui68336	cat6000-env	Revisit CSCug29473
CSCtr19129	cat6000-env	VSS - need to suppress "SIBYTE-SW2_DFC2-3-SB_TX_FIFO_UNDRFL" msgs
CSCuj78044	cat6000-firmware	6716-10G (Hw ver 2.0) may report inlet temperature higher than outlet
CSCui90022	cat6000-firmware	High CPU seen when ingress pkts w/ dMAC of 0000.0000.0000 on 6904 LC
CSCui65654	cat6000-firmware	Packets are looped within chassis when WS-X6904-40G is used
CSCul77666	cat6000-firmware	Undersized frames sent with CTS static SGT
CSCug75365	cat6000-ipc	Crash in icc multicast code on sup720 from cmfi_process_feature_msgs_int
CSCuh33725	cat6000-l2	VSS may switchover when configuring vlans

Identifier	Component	Description
CSCuf36123	cat6000-l2-infra	VSS Standby crash after renaming vlan
CSCti72095	cat6000-ltl	c2wa1: Switch crashed after ISSU runversion from latest sierra to SXI2a
CSCul12004	cat6000-ltl	VSL included in L3 vlan flood index when both MEC legs are up
CSCui17732	cat6000-netflow	Sup2T: show tech-support hangs VTY session on Netflow TCAM interrupt
CSCui28066	cat6000-qos	Ant24CR4 and CR3 with AdmiralCR- distributed policing not working
CSCti01426	cat6000-qos	Switch crashes after configuring 'auto qos voip trust'
CSCug26327	cat6000-routing	sup2t : urpf incorrectly drops traffic after vrf is configured
CSCue06000	cat6000-svc	Boot device statements are lost after reload on a VSS.
CSCsu29301	cat6000-svc	C2W21: Ingress SPAN on Sup - ACE module duplicates packets
CSCsx24934	cat6000-svc	CPU Monitor not heard and ipc TBs on Active VSS switch on issuing Reload
CSCte53717	cat6000-svc	Need to change default SCP keepalive timeout on IOS to ACE module
CSCtz63467	cat6000-svc	-Process= "K+ NAM IDB config process",ipl= 0, pid= 1113 and TB on bootup
CSCth04998	cat6k-vs-proto	[VSS] DFC installs drop index for MAC-address
CSCui95880	hsrp	HSRP for IPv6 flaps when there is a loop in the network.
CSCtk00976	ifs	File descriptor leak and not getting release - readh FD limit
CSCue68124	ip-pbr	PBR not work with null0 default route
CSCta48521	loadbal	%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCua00661	tcl-bleeding	Memory leak seen while creating vlans using Tclsh
CSCtb34814	x25	Crash after %DATACORRUPTION-1-DATAINCONSISTENCY

Caveats Resolved in Release 15.0(1)SY5

Resolved gsr-boot Caveats

- CSCsv74508—Resolved in 15.0(1)SY5

  Symptom: If a linecard is reset (either due to error or a command such as **hw-module slot reload**) at the precise time an SNMP query is trying to communicate with that LC, the RP could reset due to a CPU vector 400 error.

Conditions: In order to experience these symptoms the linecard is reset (either due to error or a command such as **hw-module slot reload**) at the precise time an SNMP query is received.

Workaround: None

More Info: None.

Resolved ios-firewall Caveats

- CSCtx56174—Resolved in 15.0(1)SY5

  Symptoms: Cisco router hangs until a manual power cycle is done. If the **scheduler isr-watchdog** command is configured, the device will crash and recover instead of hanging until a power cycle is done.

  Conditions: This is seen with websense URL filtering enabled and with zone based firewalls.

  Workaround: Disable URL-based filtering.

Resolved ospf Caveats

- CSCug34485—Resolved in 15.0(1)SY5

  Summary: Multiple Cisco products are affected by a vulnerability involving the Open Shortest Path First (OSPF) Routing Protocol Link State Advertisement (LSA) database. This vulnerability could allow an unauthenticated attacker to take full control of the OSPF Autonomous System (AS) domain routing table, blackhole traffic, and intercept traffic.

  The attacker could trigger this vulnerability by injecting crafted OSPF packets. Successful exploitation could cause flushing of the routing table on a targeted router, as well as propagation of the crafted OSPF LSA type 1 update throughout the OSPF AS domain.

  To exploit this vulnerability, an attacker must accurately determine certain parameters within the LSA database on the target router. This vulnerability can only be triggered by sending crafted unicast or multicast LSA type 1 packets. No other LSA type packets can trigger this vulnerability.

  OSPFv3 is not affected by this vulnerability. Fabric Shortest Path First (FSPF) protocol is not affected by this vulnerability.

  Cisco has released free software updates that address this vulnerability.

  Workaround: Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130801-lsaospf.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.8/5.8:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:P/A:P/E:H/RL:U/RC:C CVE ID CVE-2013-0149 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Other Caveats Resolved in Release 15.0(1)SY5

Identifier	Component	Description
CSCua61330	bgp	NSF traffic loss during switchover for prefixes with BGP learnt NH
CSCua96958	bgp	BGP PIC with confederations require next hop self configuration
CSCub30577	bgp	Incorrect RTs are attached to redistributed routes

Identifier	Component	Description
CSCub48495	bgp	BGP RTC:BGP RT Filter using route-map causing crash
CSCub70336	bgp	BGP Task crash on bgp hard reset
CSCub78143	bgp	clear ip bgp vpnv4 unicast damp rd cli doesn't clear damp info in VRF
CSCub86706	bgp	XE3.7.1: router crash with BGP HA SSO while switch-over on pE
CSCue72839	bgp	BGP link-bw doesn't program traffic share cnt in RT/CEF if soft-in+r_map
CSCug82964	bgp	BGP NSF forwarding state not preserved during SSO
CSCue33266	cat6000-acl	SUP2T: DHCP relay not working after configuring secondary IP address
CSCue93721	cat6000-acl	PPTP call not getting conn. when extendable keyword used with static nat
CSCuh57776	cat6000-acl	DHCP binding entry expire
CSCuh60848	cat6000-cm	crash@cm_rbacl_replace_req_hdlr while enabling the enforcement
CSCuf85528	cat6000-diag	Multiple GOLD tests disable autoboot when HW isn't at fault post failure
CSCuh03710	cat6000-dot1x	cat6000 dot1x in MDA - IP phone losing connectivity after few minutes
CSCtl58831	cat6000-env	small buffer leak on WS-X6708-10GE
CSCue10126	cat6000-env	SW* word is not exist in syslog output under vss config
CSCue02511	cat6000-fabric	VSS FPOE incorrect on standby
CSCud15048	cat6000-ha	Add mini trunk support to LIF manager
CSCtt42531	cat6000-hw-fwding	Fib Exception only on multiple WS-X6908-10G of Sup2T system
CSCtz70317	cat6000-hw-fwding	C6K/Sup2T: On LDB mem exhaustion, report log message and err-disable int
CSCue49346	cat6000-hw-fwding	C6K/Sup2T: LDB Mgr should not preallocate 4K LIF for L3 Subinterfaces
CSCue58387	cat6000-hw-fwding	TCAM Exception State Should Capture Prefix Distribution
CSCug44811	cat6000-hw-fwding	SUP2T:Sub-interface does not stay down when LIF entries are exausted
CSCug94630	cat6000-hw-fwding	l3 svi ip address is not reachable with service-policy on mini-trunk
CSCui65190	cat6000-hw-fwding	Incorrect policing behaviour with same policer on multiple interfaces
CSCue81201	cat6000-mcast	"ip multicast boundary <ACL> in" is blocking outbound multicast
CSCue21282	cat6000-netflow	SUP2T I/O Memory Leak Due to CDP
CSCug39407	cat6000-netflow	Middle buffer leak when netflow with cdp enabled on tunnel interface
CSCuh51188	cat6000-netflow	Big buffer leak when netflow with lldp enabled on tunnel interface
CSCsq15198	cat6000-qos	EPC:SRD:RSP720:OSPF/BFD flaps when Gi5/2 (RSP gi link) is no shutted
CSCts82932	cat6000-qos	Incorrect dscp-q mapping on trusted interface
CSCue02387	cat6000-routing	removing VRF causes global default route to fail
CSCud18108	cat6000-snmp	CAT6500 SNMP timeouts polling dot1dTpFdbTable
CSCue03531	cat6000-snmp	6500-Transceiver/SFP SNMP polling interrupted when changing port config
CSCua91959	cat6000-span	monitor capture view/privilege setting causes MALLOC failures
CSCui11311	cat6000-svc	ASA(Firewall module) BW is displayed incorrectly in SUP2T
CSCug42222	cat6000-sw-fwding	VSS VPLS: Core Switch is not forwarding DHCP request received via VPLS.
CSCuf85182	cat6000-wccp	Sup2T after removing WCCP FEATURE_TUN_x interfaces are not removed
CSCug24158	cat6000-wccp	Disable LLDP on WCCP tunnel interfaces

Identifier	Component	Description
CSCub45763	cdp	crash following SYS-2-FREEFREE and SYS-6-MTRACE messages
CSCtg57657	dhcp	Router crash at dhcp function
CSCud96882	ethernet-lldp	Buffer leak seen in I/O with lldp_send_update
CSCub75883	ip-acl	Access-line numbers are NOT persistant after reload
CSCtw72952	mpls-te	Path protection not working once primary path is deleted
CSCud70205	nvram	VSS - Standby Reload when NVRAM accessed from multiple sessions
CSCtu36054	qos	cnma1b :Traceback seen @ fib_process_ipfib_xdr+144
CSCsw43080	rsr-bridging	Traceback seen @ data_inconsistency_error_with_original_ra
CSCuc82551	sla	Segmentation fault(11), Process = SNMP ENGINE on ASR1001
CSCee55603	snmp	SNMP ACL does not work for VRF interfaces
CSCtc43231	snmp	SNMP Informs Source Interface Command not working
CSCti60077	snmp	Memory leak in IP SNMP Process on cat6k

Caveats Resolved in Release 15.0(1)SY4

- CSCtg47129—Resolved in 15.0(1)SY4

  The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are not available.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130327-nat

  Note: The March 27, 2013, Cisco IOS Software Security Advisory bundled publication includes seven Cisco Security Advisories. All advisories address vulnerabilities in Cisco IOS Software. Each Cisco IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the March 2013 bundled publication.

  Individual publication links are in “Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication” at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar13.html

Other Caveats Resolved in Release 15.0(1)SY4

Identifier	Component	Description
CSCty04467	c6k-crypto	When configuring IPSEC the switch crashes.
CSCub09060	cat6000-acef	MA2.0: Crash seen while configuring xconnect encapsulation mpls
CSCuc91306	cat6000-acl	MEM LEAK seen with DHCP SNOOPING on MA1.3
CSCuc81745	cat6000-cm	TCAM error for interface with QOS policies
CSCub52879	cat6000-diag	CCP loopback test for Jian fails upon removal of service-vlan config

Identifier	Component	Description
CSCtw93788	cat6000-dot1x	MDA port during reauth goes to error disabled state on SSO.
CSCud88798	cat6000-dot1x	Build failure on V150_1_sy_throttle for sup720 based images
CSCua90130	cat6000-env	link down/up not logged even "logging event link-status default"
CSCtz23026	cat6000-firmware	VSL interface error after VSL-Encryption
CSCuc76227	cat6000-hw-fwding	SUP2T - packet forward to the wrong dest index
CSCuc43594	cat6000-ipc	VSS NTI_AGENT_STATUS_TIMED_OUT: IPC sessions not cleared on sup failover
CSCua87594	cat6000-l2	cat6k:Spanning Tree interop between MST0 & RSTP takes 6 secs to converge
CSCtu42798	cat6000-l2-ec	Metropolis RBH filtering is wrongly programmed for Met-0 ASIC in VSS
CSCtw49735	cat6000-l2-ec	load-defer config is not syncing after SSO while load-defer running
CSCty86250	cat6000-l2-infra	Sup2T Failover Changes DLY Value
CSCub50852	cat6000-l2-infra	Unable to use reserved vlan for firewall vlan-group
CSCub72971	cat6000-l2-infra	inrerface resets counter shows 4294967295 after module OIR/switchover
CSCty64855	cat6000-l2-mcast	Memory Leakage @cl2mc_l2mm_pd_pm_del_agport+58
CSCtr95194	cat6000-ltl	VSS 2T - TX SPAN fails for mcast traffic after oir/reload/shut no shut
CSCuc84396	cat6000-oir	Missing modules in CISCO-STACK-MIB
CSCua17283	cat6000-qos	Aggregate Policy-SVI not working with physical OIR of Aphrodit Line Card
CSCub81771	cat6000-qos	Revert support to allow multiple ace's in class-map
CSCty15494	cat6000-routing	Memory leak in cfib_fibsb_chunk
CSCua31785	cat6000-routing	Sup2T: Virtual MAC removed from interface after HSRP switchover
CSCud96150	cat6000-routing	6500 15.1(1)SY VRF vpn-num misprogammed causes connectivity issues
CSCtj52347	cat6000-span	Span confg removed from PO span dest causes L3 protocols to not work
CSCtt04914	cat6000-span	Span stops working and must be re-configured to continue working.
CSCtr30113	cat6000-svc	Standby reloads and never comes up after SSO in the VSS with fwsm
CSCua03386	cat6000-svc	Sup2T egress multicast replication mode fails on service modules
CSCud39765	cat6000-svc	ASASM on VSS standby unit getting PwrDown after reload
CSCua84168	cat6000-sw-fwding	[SUP2T] NLB Multicast mode packets hit CPU then are routed.
CSCud16543	cat6000-sw-fwding	IBC TX Freeze on Sup2T with CTS/MACsec
CSCuc31256	cat6k-vs-diag	Sup2T Quad Sup: Active sup crashes and does not recover
CSCtd54694	cdp	Switch crashes on Show cdp neighbor detail in some conditions
CSCts29515	cts	CTS: Peer policy is not updated after reauth.
CSCtj32137	fib	RP Crash at fib_fib_src_remove_all_repopulating_sources
CSCtz98066	fib	3750x stack fails to update ARP table after reboot causing traffic loss
CSCub54872	fib	fib missing connected interface for interface receive prefix
CSCtx74051	flexible-netflow	Unsupported subtraffic bits from XDR not ignored; ISSU downgrade breaks
CSCuc19862	flexible-netflow	Flexible Netflow on cellular int cause spurious mem access and CPU HOG
CSCtw56439	ip-tunnels	IPSEC: "IP MTU" CLI disappears after the router is reloaded
CSCua47495	ip-tunnels	tunnel event trace consumes huge memory on 3k

Identifier	Component	Description
CSCed01880	nat	Not able to configure NAT tcp timeouts beyond 4194 sec
CSCud08682	nat	NAT not translating Traceroute's ICMP Unreachables
CSCud09626	nat	NAT PPTP use_count 1 entry not removed if TCP data segment with FIN flag
CSCud95251	nat	static nat with vrf looses vrf name after nat translations expire
CSCue21223	nat	Intermitant HSRP hellos not sent w/ IP NAT redundancy configured on SVI
CSCtg82170	sla	IP SLA destination IP/port config changes over a random period of time
CSCub47374	sla	Router crashes during IP SLA probe removal/reconfiguration
CSCud11078	sla	MA1.3: Crash observed with auto IP SLA probe for ethernet cfm

Caveats Resolved in Release 15.0(1)SY3

Identifier	Technology	Description
CSCsj38112	—	High CPU due to interrupts on WS-X6704-10GE
CSCta17587	—	VRF + RHI combination does not work on FWSM
CSCtj10515	—	Exnet: Mrib and Mroute entry goes out of sync after a routing loop
CSCtl58612	—	Stby Sup resets with "boot bootldr", but file doesn't exist on stby
CSCtn96959	—	Crash @cfib_process_tunnel_delete_events in DFCs in IPv6 mcast stress
CSCtq77024	—	Route change on ATM/FR intf causes dvmc to fail
CSCts27379	—	Mem leak @ fm_cm_dynamic_policy_update+1BC upon defaulting 4k EFP intf
CSCtt26063	—	c2ma2:sdby rebooting continuously due to "mls qos trust cos" config sync
CSCtt27583	—	c4ma2:Adjacency fields is not programmed in fm interface with gre tunnel
CSCtt96152	—	VSS: corrupted Portchannel: LTL missing VSL-link
CSCtw91041	—	Convergence time for bgpv4/v6 on sup4 degrading from sierra to ma2_pi
CSCtw93140	—	On 'wr mem' command noticed "% VRF table-id 0" message
CSCtw99185	—	Ipv6 Reflexive acl not working in HW for sdby CFC
CSCtx17098	—	HSRP/Routing protocols stops working on disabling MVRP
CSCtx35465	—	RTTY client is not created in VSL enabled Estelle LC
CSCtx74258	—	6908 module may crash while reading registers
CSCtx77503	—	mls config commands crash Sup2T
CSCtx84897	—	Wrong Default interval for HM "TestEARLInternalTables " is set to 5 secs
CSCtx92054	—	On Creating monitor session device goes for a reset with traceback.
CSCtx92816	—	NDAC link with Manual Mode stops fwding packets after sometime
CSCtx98926	—	LIF expansion not requires if 'acl downloadable setup' is not configured
CSCty02902	—	cnma1b: FWSM RHI Routes are not withdrawn after SSO on VSS
CSCty54036	—	6k/SUP2T cannot do RSPAN if it is intermediate device
CSCty65189	—	First PIM Reg message gets dropped by ZBFW
CSCty70689	—	netflow entry to ignore ACL deny is not programmed for the SUP2T int Po

Identifier	Technology	Description
CSCty71564	—	VS-S720 gig ports can drop multicast traffic under certain conditions
CSCty94405	—	DCP and CCP loopback ondemand tests fail without Jian LAG configured
CSCty97033	—	Duplex not changing using snmpset
CSCtz13812	—	2960S can not receive the IP SLA control message from sender
CSCtz29869	—	Diag error on sup2T uplinks with cts dot1x enabled - ports errdisabled
CSCtz30804	—	SUP2T: crash at CM-MSG:ERR cm_icc_server error in cond
CSCtz35085	—	%SYS-2-BADBUFFER: Attempt to use contiguous buffer as scattered
CSCtz35247	—	HM_TEST_FAIL TestMgmtPortsLoopback consecutive failure for ASASM on OIR
CSCtz54207	—	After Master stack down, next hop address is duplicated on "ip next-hop"
CSCtz58941	—	Crash show_network after multiple times "show ip route x" cmd executed
CSCtz71181	—	Sup2T mem corruption crash missing corrupted memory print out
CSCtz80643	—	CEF unresolved and receive adjacency for VAI using VRF PBR selection
CSCtz87383	—	Sup2T-all LDP Packets dropped on Egress
CSCtz89775	—	cnma2:span_add_port_array_to_port_list
CSCtz94984	—	Interop issue between WS-SVC-ASA-SM1 and xconnect
CSCua02456	—	WS-X6824-SFP Minor Error during IOS boot up (TestInbandEdit failed)
CSCua06138	—	Dot1x clients are authz failed on routed ports.
CSCua19294	—	IP SLA udp-jitter operation intermittently report wrong minimum RTT
CSCua43298	—	Port loopback mode may not be cleared in corner case
CSCua61126	—	Diagnostic test fails with Wism2 on standalone
CSCua84323	—	EthChnl-MP assert failure ahwidb_primary - Traceback
CSCub01301	—	WS-X67XX 1G linecards: Changing the cos map reset the Tail Drop to WRED
CSCub01714	—	Qos -Agg-fwd Counter decrease under policy map after 15 min or so
CSCub05981	—	Interface down/down locally after WS-X6848-GE-TX boots
CSCub15825	—	SUP Crashes,if #no platform qos statistics-export delimiter is executed
CSCub45767	—	Sup2T: Switch crash due to TestL3TcamMonitoring failure
CSCub76366	—	C6K:publish (ma1bubb)1.0.30 to v150_1_sy_throttle
CSCub83606	—	"policy static sgt 7" has its effect even after it is unconfigured
CSCub93731	—	Cat6K Sup2T crash in QoS policy
CSCuc00098	—	Crash occurs with two Sup2Ts while standby Sup is initializing
CSCuc10919	—	WS-X6904-40G power on leads to control-plane traffic loss on Cat6K
CSCth83143	Infrastructure	IPv6 access list applied to SNMP community string does not work
CSCtk36938	Infrastructure	%SYS-SP-3-CPUHOG @preemption_forced_suspend
CSCtl53576	Infrastructure	Router is getting Hang up at sh run
CSCtr45030	Infrastructure	Configuration mode is locked and standby resets
CSCtr89424	Infrastructure	twamp PI18: session table is not cleared after session is completed.
CSCts67465	Infrastructure	MF:IPSLA VO: Reconfiguration of frequency value causes standby to reload

Identifier	Technology	Description
CSCtt21979	Infrastructure	Processor Pool Memory leak in IP SLA Responder with IPv6 Probes
CSCtw46891	Infrastructure	IP SLA probes may not respond to SNMP jitter table
CSCtw78343	Infrastructure	rttMonApplSupportedProtocols table missing on 151-4.M1
CSCtx05616	Infrastructure	cSUP2T - startup cfg is partially copied via rcp when compression is on
CSCtx19332	Infrastructure	cnma1b: Crash seen after "sh ethernet cfm maintenance-points remote"
CSCtx74931	Infrastructure	SNMP get on some OIDs fails if zero in ipv4 addr
CSCsz24818	IPServices	ASR:MCP_DEV- RP crash observed when trying to telnet using v6 address
CSCtx95334	IPServices	TCAM entries are not correctly programmed for static nat w/ interface
CSCtz85702	IPServices	NAT TCP pptp-control timing-out use_count 1 - entry not removed
CSCua43193	IPServices	Dynamic NAT'g of TCP traffic fails when redudancy VIP is used for NAT
CSCua70136	IPServices	NAT VRF with PAT - PPTP translation failure with dynamic pool
CSCub18395	IPServices	PAT not working when shut/no shut nat+hrsp config interface
CSCtc42278	ISDN	%DATACORRUPTION-1-DATAINCONSISTENCY - ISDN incoming call
CSCua40273	MPLS	ASR1K:Crash at _be_mplsvpnmib_get_vrf_interface_info
CSCtq14253	Multicast	ipv6 vrf-lite multicast joins/register not forwarded to RP
CSCsm53205	Routing	Flash updates in RIP are not filtered by output distribute-lists
CSCty96052	Routing	Extreme corner case: Crash during BGP scanner process run
CSCtz25825	Routing	Null0 route is remaining in multiple VRF even if remove aggregate-addres
CSCtz44989	Routing	Redistribution between two different EIGRPv6 VRF using BGP doesnt work
CSCtz58710	Routing	IPRT-3-INVALID_NEXTHOP for process OSPF Router
CSCtz71084	Routing	BGP PIC EDGE prefix leak after removal of prefix
CSCua06598	Routing	Router crash when polling inetCidrRouteEntry ipv6 MIB
CSCua16758	Routing	Counters fluctuating on BGP Nei. shutdown causing skewed metrics
CSCua38597	Routing	bgp remove-private -AS does not remove private asn with continue clause

Caveats Resolved in Release 15.0(1)SY2

Resolved IPServices Caveats

- CSCts12366—Resolved in 15.0(1)SY2

  Symptoms: Memory may not properly be freed when malformed SIP packets are received on the NAT interface.

  Conditions: None

  Workaround: None

  Further Problem Description: None.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5/4.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:U/RC:C CVE ID CVE-2011-2578 has been assigned to

document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Other Resolved Caveats in Release 15.0(1)SY2

Identifier	Technology	Description
CSCsu65095	—	switch crash w traceback after applying "eou rev all"
CSCta74577	—	Need to print out module number is message LTL-SP-2-LTL_PARITY_CHECK
CSCte44826	—	memory leak in cfib_alloc_sb running SXH3a
CSCth43893	—	supervisor crashes after memory allocation error
CSCti45609	—	LISP: improve map-cache build-up time
CSCti84718	—	CPUHOG @ ipnat_ipalias_check_waitlist+E8 after sh/nosh PBR po int
CSCtk64480	—	default-originate does not work w/ route-map on specific condition
CSCto56118	—	ACL: Adding a duplicate ACE via an object-group is not rejected
CSCts90103	—	Buffer leak on the RP due to IPC messages resulting in a crash
CSCtt24684	—	GOLD: Minor Errors Incorrectly Reported on a Trifecta Service Module
CSCtt96621	—	TestDCPLoopback fails on data port 2 with Jian LAG configured
CSCtu10831	—	Multiple add/remove flow monitor in single or separate sessions may fail
CSCtw61872	—	Possible crash from show flow monitor <xxx> cache on multiple sessions
CSCtw80411	—	MAB - Fails for devices already connected when enabled
CSCtw84639	—	%BIT-4-OUTOFRANGE: bit 32767 is not in the expected range of 1 to 4096
CSCtw99290	—	ASR1K:v6 mcast channel zapping and show run in a loop modifies confg
CSCtx12231	—	Config Sync: Bulk-sync failure due to PRC mismatch in ACL
CSCtx29543	—	Crash after link flap in ASR1K during BGP process
CSCtx44613	—	Tracebacks are seen after Verifying IP SLA auto probe functionality
CSCtx53272	—	CM traceback with large v6 vacl
CSCtx74756	—	w/ 10g/40g VSL comb'ns, s/w goes into dual-ACT state on toggling VSL's
CSCtx95441	—	Destination MAC 0000.0000.0000 on mapping unicast IP to multicast MAC
CSCtx99145	—	Jian project name seen in show module output..
CSCty04591	—	cnma1b: EC-5-CANNOT_BUNDLE2 error messages seen upon wism LAG config
CSCty05092	—	Eigrp doesn't remove connected route from topology after int shutdown
CSCty20876	—	Show stack does not show correct Information of Last System Crash - SP
CSCty26260	—	6500 - Stndby Sup not fluching mac when port-security is enabled
CSCty58533	—	sho int util shows same rate on tx/rx even though they are different
CSCty62457	—	traceback - %SYS-2-LINKED: Bad enqueue of x in queue y with ipv6-copy
CSCty68821	—	WS-X6908-10G is in "off (not supported)" Oper State during normal oper
CSCty80605	—	nvram erase cli support needs to be implemented for peer switch LCs
CSCty85926	—	VPLS VFI stays done if configured after LDP GR
CSCtz05347	—	Estelle bandwidth is required under all non-default classmaps

Identifier	Technology	Description
CSCtz14786	—	Update version to c6kfw@(ma1bubb)1.0.21
CSCtz15580	—	Copy files from MA1BUBB_INTEG_120406
CSCtz18103	—	publish (ma1bubb)1.0.21 to v150_1_sy_throttle
CSCtz39608	—	nvram erase cli for peer sw LCs is proceeding without user confirmation
CSCtz42106	—	DAD fails between IPv6 SVI interface
CSCtz87081	—	Back off changes of CSCtz42106 (DAD fails between IPv6 SVI interface)
CSCtz92889	—	DAD fails between IPv6 SVI interface
CSCua06082	—	Power flap may cause 'power-output-fail' alarm and high CPU (Env action)
CSCua42852	—	Redundant SUP2T's TestNonDisruptiveLoopback test causes a memory leak
CSCua51807	—	6k: TCP stale sessions not removed with EW running in MA1 image.
CSCua66829	—	Powernet Standby Crash when HA switch has MA1.2 image & connected MA2 sw
CSCth64138	AAA	CPU high@'AAA ACCT Proc' session remains after user disconnects
CSCtt70568	IPServices	PPTP timeout entries are never removed from NAT table.
CSCtx32329	Multicast	V6Mcast : Switch crashes on shutting down an RPF intf of static mroute
CSCsz45086	Routing	MF:VRF ARP table was NOT built correctly for overlapped IP space under
CSCtn02656	Routing	BGP filtering is incomplete after prefix-list reconfiguration
CSCtq24557	Routing	BGP import processing trying to free already freed chunk, causing crash.
CSCts72911	Routing	BGP RT constraint filters not advertised after SSO switchover
CSCtw98101	Routing	BGP next-hop in vrf def ignored for multipath prefix in BGP AF ipv4 vrf
CSCtx01476	Routing	Config Sync: Bulk-sync failure due to PRC mismatch in ACL
CSCtx19461	Routing	6PE router doesn't send or withdraw ::/0 if ::/X exists, X is non zero
CSCtx28597	Routing	bgp aggregate-address with send-label not being advertised to neighbors
CSCtx74342	Routing	ospfv3 route to connected prefix points to down interface until next spf
CSCty03745	Routing	BGP sending wrong next-hop while using vpls AD with default route
CSCty17538	Routing	traffic dropping with sgt-map subnet binding in egress node
CSCty41692	Routing	Standby crash if "address-family ipv4 vrf" is removed and configured
CSCty78435	Routing	MPLSomGRE: match statement ignored in route-map
CSCtz13818	Routing	IOS not sending refreshed updates to peer after change in route-map
CSCto60047	Security	Chunk corruption crash on trying to abort "show tech" over SSH

Caveats Resolved in Release 15.0(1)SY1

Resolved Infrastructure Caveats

- CSCtd72456—Resolved in 15.0(1)SY1

  Symptoms: Entering the **show snmp pending** command may cause a Cisco switch to crash.

  Conditions: None

  Applicable to all.

  Workaround:

1. Do not configure v3 informs.

2. Do not enter the **show snmp pending** if the v3 informs are pending.

- CSCtr91106—Resolved in 15.0(1)SY1

  Summary: A vulnerability exists in the Cisco IOS software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 8.5/7:
  https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:S/C:C/I:C/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0384 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved IPServices Caveats

- CSCta98734—Resolved in 15.0(1)SY1

  Symptom: DNS Memory Leak in DNS queries

  Conditions: DNS server configured: 'ip dns server'

  This bug can only possibly surface if the "ip dns-server" is configured, and then only when specific malformed datagrams are received on the DNS udp port 53. This specific datagram malfrmation is that the udp length field indicates a zero-length payload. This should never happen during normal DNS operation.

  Workaround: No Workaround at this time

- CSCtr28857—Resolved in 15.0(1)SY1

  Summary: A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0382 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved QoS Caveats

- CSCts80643—Resolved in 15.0(1)SY1

  Cisco IOS Software and Cisco IOS XE Software contain a vulnerability in the RSVP feature when used on a device configured with VPN routing and forwarding (VRF) instances. This vulnerability could allow an unauthenticated, remote attacker to cause an interface wedge, which can lead to loss of connectivity, loss of routing protocol adjacency, and other denial of service (DoS) conditions. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  A workaround is available to mitigate this vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-rsvp

Resolved Routing Caveats

- CSCef01541—Resolved in 15.0(1)SY1

  A router processes a packet that is sent to the network address of an interface, if the layer-2 frame that is encapsulating that packet is specifically crafted to target the layer-2 adress of the interface or a broadcast layer-2 address.

  This happens only in the process switching path and does not happen in Cisco Express Forwarding (CEF) path.

  Workaround is to use CEF.

Resolved Cisco IOS Caveats

- CSCts38429—Resolved in 15.0(1)SY1

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

  Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

Other Resolved Caveats in Release 15.0(1)SY1

Identifier	Technology	Description
CSCsd46369	AAA	IP source address on packets to TACACS server is wrong
CSCtr20762	AAA	L3vpn tunnel is not comming up after the router is reloaded
CSCts80209	AAA	Cat6k switch crash on "no login block-for" with login quiet-mode
CSCee38838	Infrastructure	kadis timer abort reloads router
CSCti16550	Infrastructure	Spurious memory at expressionmib_nvgen
CSCtn65116	Infrastructure	VPNv4 prefixes are not being imported
CSCtn82006	Infrastructure	cnma1: "DOSFS-5-DIBERR" displayed when issue "dir disk0:" and copy tftp
CSCto96750	Infrastructure	shutdown command is not showing up in active running-config
CSCtr29847	Infrastructure	Exit Command with Routing Context
CSCtr52740	Infrastructure	MF: IP SLA crash when history is queried via SNMP but is not configured
CSCts45378	Infrastructure	Cannot configure Ethernet Manual (echo/Jitter) probes.
CSCts69368	Infrastructure	timeout trap is not displayed in ip sla engine 3
CSCts71958	Infrastructure	Last Reload reason in the show version scenario
CSCtt26074	Infrastructure	Huge Memory leak with IPSLAs XOS Even process at slaSocketAddContext
CSCtw85356	Infrastructure	delay auto reflexed on channel interface without config
CSCtx49270	Infrastructure	memory leak @ fast udld
CSCtx68100	Infrastructure	Reload reason not displayed correctly on some platforms
CSCsb70368	IPServices	Bus error at ipnat_delete_entry with PPTP-TCP entry deletion
CSCsr03117	IPServices	UDP direct-broadcast packets get dropped despite ACL's permit config
CSCsr17315	IPServices	Autoinstall process not correct with BOOTP or DHCP server in same LAN
CSCsv02395	IPServices	Telnet hostname /vrf <name> does not work
CSCtd13999	IPServices	Bugs in the Path-mtu logic
CSCtd46206	IPServices	After Reload NAT does not create dynamic aliases and arp entry.
CSCtn07696	IPServices	6506-E/Sup720 crash related to SYS-3-URLWRITEFAIL: and TCP-2-INVALIDTCB
CSCto85802	IPServices	Incorrect Behaviour @ "(config-line)#access-class <> ".
CSCtq14817	IPServices	Traceback seen @ ipnat_pptp_client_inside
CSCtr16396	IPServices	TAC+ Code Incorrectly Implements timeout for tacacs-server timeout
CSCtr30487	IPServices	Memory Leak with static nat - NAT String Chu
CSCtt02390	IPServices	VSS: TFTP-Server fails after switchover or when one of the switches down
CSCtg48785	LegacyProtocols	sh x25 hunt-group %DATACORRUPTION-1-DATAINCONSISTENCY: copy err
CSCtq21234	MPLS	Local Label not freed from MFI after Link failure.
CSCtv97307	MPLS	MLPS LDP flaps with high Tag Control and IPRM CPU utilization
CSCsh39289	Multicast	Crash in pim_sm_assert_rpf_nbr during the stress test
CSCts27042	Multicast	Bidir DF election causes traffic duplication
CSCsz82587	QoS	Active crashed on module reset[ES20] with LSM configs
CSCtr22007	QoS	Bus Error crash in MPLS TE LM Process on 7600

Identifier	Technology	Description
CSCtw48209	QoS	RSVP trap sent when MPLS-TE RSVP session state change may cause crash
CSCtn78663	Routing	Cat6k No ICMP Mask Reply
CSCto84723	Routing	Cat6K Crash when removing ACL with Object Tracking alsol ACE with OG
CSCtq49325	Routing	EIGRP graceful shutdown can cause a reload
CSCtq59923	Routing	OSPF Routes in rib point to down interface
CSCtq77801	Routing	Local route is not created for imported connected route
CSCtq81448	Routing	show ip pim int count shows incorrect counters
CSCtq86186	Routing	Switch stack shows incorrect values for output drops on show interfaces
CSCtr16802	Routing	Static routes with track configs remains un-erased after VRf removal
CSCtr27358	Routing	"setup" on ASR1000 always generates "no ip routing" config
CSCtr38563	Routing	Configuring secondary IP address crashes switch
CSCtr58140	Routing	PFR controlled EIGRP route goes into SIA and resets the neighbor
CSCtr66216	Routing	RIP sends update with incorrect hop count when apply route-map
CSCtr69144	Routing	distance change for MBGP doesn't affect
CSCtr79347	Routing	crash on BGP Task
CSCtr81102	Routing	Static route remains in config after removing interface
CSCts02777	Routing	Duplicate command attributes sent in AAA authorization and accounting
CSCts19788	Routing	crash while show ospf database
CSCts28761	Routing	Crash while isis reconfig and issuing "sh isis data" in parallel session
CSCts39535	Routing	bgp outbound route-map, [un]suppress-map fails to match sourced networks
CSCts64539	Routing	BGP Marks Next HOP inaccessible with ip vrf next-hop feature used.
CSCts68891	Routing	Reduce BGP Scan Time Lowest Value & Allow NHT to be Configured
CSCts70790	Routing	BGP default-originate for VRF neighbor does not work after link flap
CSCts72164	Routing	Router crashes due to Segmentation fault in BGP I/O
CSCts72471	Routing	Change isis default metric cause a race condition
CSCts86986	Routing	EIGRP distribute-list out route-map incorrectly checks composite metric
CSCtt17879	Routing	BGP backdoor command is not working
CSCtt55925	Routing	multicast and pim and bsr advertisements fail over unnumbered ppp link
CSCtt94986	Routing	CLNS L1 addresses are not Leaked to L2 (with only one area address)
CSCtu76678	Routing	Crash while issuing 'no neighbor' command under BGP configuration
CSCtu80224	Routing	BGP sets next-hop for redistributed recursive static routes to itself
CSCtw45055	Routing	BGP DN: Crash in BGP Scheduler due to freed bgp neighbor
CSCtw83732	Routing	Wrong TE metric advertisements after isis/ldp sync
CSCtx32628	Routing	BGP withdrawn message doesn't trigger BGP prefix removal on RR
CSCsd84640	Security	SSH2 Error message should adhere to Cisco Syslog Format
CSCsk05015	Security	USERAUTH_SUCCESS not handled correctly for "none" auth method
CSCsm27467	Security	switch crashes if kron used to copy over config via scp

Identifier	Technology	Description
CSCsv23797	Security	SSH:Crash seen on 7200 on mcp_dev
CSCth79917	Security	AAA Banner not displayed for a SSH login session
CSCtk31401	Security	Router crashes @ssh2_free_keys when exiting the SSH session from client
CSCek68936	—	6716 fabric asic causing EC performance issue
CSCsj70829	—	CPU hog caused by OBFL uptime logging
CSCsk94501	—	AUTHPROXY: info timestamp array size not the same as max-login-attempts
CSCsr82508	—	Upgrade tool sees lwapp image for AP1250s as an invalid image
CSCsr95189	—	VSS standby switch reset parser error in IDSM config command
CSCsu06967	—	auth-proxy-banner must not be displayed on result page
CSCsx65088	—	WiSM on 5.2.157.0 causes %WiSM-5-STATE: Oper-up messages on supervisor
CSCsy83266	—	Trace error and crash by snmpwalk .1.3.6.1.4.1.9.9.166.1.21.1.1.6.174482
CSCtc99947	—	Switch drops DHCP INFORM packets from DHCP client
CSCtd23028	—	LACP channel is not coming up with dot1q-all-tag configured on one side
CSCtf18308	—	RR: CTS config between RR links causes the line protocol to go down
CSCtf98621	—	Recreating a deleted vlan comes up with "act/lshut" state
CSCtg54603	—	IPC Standby port not transitioning to Active Ports after RP Switchover
CSCth04059	—	VS2 - ringar mem corr crash - VSL cfg port's peer non-VSL; link toggling
CSCth47031	—	c4hd1:Pvlan traffic is dropped on FWSM
CSCth84370	—	Standby Sup reloads when "wr mem" and "show conf" run from different VTY
CSCti08811	—	event manager cli command cause parser crash
CSCti68459	—	ISSU aborts at runversion due to BOOT var using sup-bootflash
CSCti73704	—	PfR exit links flap when a site down occures
CSCtk00056	—	Port Flow-Control Deafult changed after CSCsq14259 on Sup WS-SUP720-3B
CSCtl13134	—	"SVCLC SCP communication failed" observed on SUP during ACE reload
CSCtl48226	—	crash seen when issuing sh epm summary on ssh session
CSCtl72207	—	Cat2960: MED information missing in LLDP packets
CSCtn15098	—	MF:IDH:Local session timer does not kick in if AAA timer is disabled.
CSCtn59075	—	Router crash + __be_fnf_build_do_feat
CSCto99343	—	Neghbourship failed in eigrp in 150-1.IA273.8_110425
CSCto99774	—	Crash in vtp mib
CSCtq14603	—	On SSO, Ping to interfaces fails and punt adj prog. on VSS system
CSCtq26090	—	Static routes with next-hop shows as directly connected with RIP
CSCtq34985	—	DCI: A-VPLS VCs not synced to standby Sup
CSCtq43027	—	TB@const_dot1x_get_earl_entry upon Authfail->Guest
CSCtq48027	—	MVRP: Traffic is NOT flowing in the netwok with MVRP enabled
CSCtq90577	—	removing netflow crashes the router at ipflow_sub_adjust_free
CSCtq90744	—	SNMP trap is not sent for SVI up/down

Identifier	Technology	Description
CSCtq94581	—	voice domain cannot authc when port-security is enabled (MDA mode)
CSCtr13172	—	config replace flash0:file-name crashes the router .
CSCtr26476	—	cat6k not always putting the link going to VS sup to FWD via uplinkfast
CSCtr29831	—	ASR1000-WATCHDOG: Process = SXP CORE when adding 1k sxp connection
CSCtr42806	—	After switchover, ISSU negotiation between LC & RP fails
CSCtr43893	—	adding NAT on IRB blocks control packets for IRB interface
CSCtr46076	—	crash due to: terminated due to signal SIGBUS, Bus error: MF
CSCtr47317	—	Span replication loop after switchover on Service Module
CSCtr51517	—	SSH UNEXPECTED_MSG debugs do not display IP address
CSCtr52186	—	line console 0 doesn't session out
CSCtr67722	—	SP CPUHOG on VSS setup with span session
CSCtr84253	—	cat6k rapidly exhausts system buffers
CSCtr94733	—	ping to the ipv6 host fails with ipv6 pacl config applied
CSCts03905	—	NAM GUI access causes SNMP CPU 100%
CSCts05397	—	Layer-4 and IPv6 tag2ip load-balancing don't work
CSCts05980	—	Traffic floods upon stp root/desg link flap with known unicast
CSCts06929	—	ES+ LC does not correctly program label in disposition table
CSCts11594	—	Toggling session-params custom to default & schedule/unschdule crashes
CSCts15934	—	VSS: MALLOC failure reported by diag_display_fpoe_entries
CSCts17084	—	Incorrect card type information displayed for ws-x6908-10G
CSCts19697	—	VSS:number of inrerface resets shows 4294967295 when switchover
CSCts21059	—	Stdby DFC flows get blackholed on peer reload
CSCts22035	—	CM API crash trigger by FMCC auto-correction (e.g with 2 qos res banks)
CSCts24348	—	PBR "set vrf" causes destination ARPing for punted packets and drops
CSCts24408	—	MA1: TCAM resource not released after un config v6 ACL with cts
CSCts32884	—	HW not programed for dynamic ACL by IPV6 tunnel upon LC reset
CSCts33952	—	rsh command fails from within TclScript
CSCts41682	—	CPU hog seen at CM main thrd with ISSU test-cycle
CSCts56044	—	MF:YAP: FNF Top Talkers: crash with complex aggregate / sort
CSCts63619	—	Report REQ_MOD_RESET_ECC2 while R2D2 detect Rx/Tx memory ECC2 error
CSCts70696	—	TBs and crash on ip basek9 fc3 image
CSCts76660	—	Crash's core file not generated in ipbasek9 image
CSCts86100	—	FIPS does not work with ipservices k9 images
CSCts88817	—	ASA-SM and SVC-NAM3 lock up triggering module reload by switch
CSCts89909	—	Ping unsuccessful after reload and shutting down Uplink port from MEC
CSCts90221	—	CFM - MA1 : MEP under EFP cannot be deleted
CSCtt00490	—	snmpwalk for a N/A DOM-value is returning a bogus value

Identifier	Technology	Description
CSCtt17210	—	On setting crcSrcERSpanLoVlanMask to zero, device goes for a reset.
CSCtt26784	—	SUP32 crashes on power cycle "registration timer event"at 12.2(33)SXI6
CSCtt35036	—	Sup2T VSS: RACL Reduced and earl8 hw adj fail errors on SSO
CSCtt35853	—	Trifecta:VSS - Console Hung Indefinitely at SSO
CSCtt36279	—	NAM-3: CONST_DIAG-SW2_SPSTBY-3-HM_TEST_FAIL during OIR
CSCtt38735	—	SVIs stuck in Administratively Down state, 'no shut' takes no effect
CSCtt39344	—	Sup-2T VSS: PBR first adjacency wrongly programmed on SSO
CSCtt46982	—	WiSM-2 in switch-1 of VSS loosing native vlan config after reload
CSCtt60289	—	High delay to get linkdown notification after a module crash on VSS
CSCtu08103	—	udld error disable on peer (VSS) reload
CSCtu17483	—	MF:Switch Crashes due to LLDP process
CSCtu21067	—	Traceback is seen while configuring the WEBAUTH with bunch of cases
CSCtu28383	—	Protocol peer down and cannot ping upstream router with load-defer conf.
CSCtu33532	—	IGMPv2 Does Not Use Router Alert Option
CSCtu38265	—	MA2 : Crash seen with http auth-proxy
CSCtu50683	—	Resetting PS on Standby VSS, reduces power from PS on Active VSS member.
CSCtu80259	—	Egress Traffic drop up to 10-15s when SSO with Sup-uplink
CSCtw50679	—	Crash on "sh ipv6 mld snoop add vl <x> <grp> hosts"
CSCtw55546	—	Cat6k:sh lacp internal detail output shows wrong Timeout value
CSCtw56565	—	LC crash cmfi_eom_imp_oce_update+2B4 after SSO SW
CSCtw75035	—	Partial OSPF config missing after reload
CSCtw99132	—	Estelle: Incorrect Radian mode when configured for L3 CTS
CSCtx20506	—	Estelle: show mod shows Minor error against estelle module
CSCtx26056	—	Assertion failed: ../VIEW_ROOT/cisco.comp/cts/rbm/src/rbm_policy_api
CSCtx30857	—	hqm_cce_free_class_queue_map+48 crash on defaulting int
CSCtx39087	—	add nam/asasm sw ver to sup compatibility table in 15.0(01)SY throttle
CSCtx51935	—	c4ma2:device crash after configuring mpls te-tunnel in latest ma2_pi
CSCtx58164	—	MA1.Bubb: ddts to update Sup2T specific restriction for VNET tag.
CSCtx69623	—	Trifecta ISSU Client(6074) incompatible message during ISSU upgrade

Caveats Resolved in Release 15.0(1)SY

Resolved AAA Caveats

- CSCsg21398—Resolved in 15.0(1)SY

  Symptoms: The Cisco IOS software image may unexpectedly restart when a crafted “msg-auth-response-get-user” TACACS+ packet is received.

  Conditions: This symptom is observed after the Cisco platform had send an initial “recv-auth-start” TACACS+ packet.

Workaround: There is no workaround.

- CSCtd81458—Resolved in 15.0(1)SY

  Symptom: Spurious memory access and/or crash when configuring a TACACS/AAA server connection.

  Conditions: From internal review, this issue has been seen when a physical connection to the TACACS server isn't present or the server isn't online. If the server is connected and available, this issue may not happen.

  Workaround: Ensure that a connection to the server is present on the device in question and the server is active to try and avoid this crash.

- CSCth25634—Resolved in 15.0(1)SY

  Symptoms: Password is prompted for twice for authentication.

  Conditions: This issue occurs when login authentication has the line password as fallback and RADIUS as primary. For example: aaa authentication login default group radius line

  Workaround: Change the login authentication to fall back to the enable password that is configured on the UUT. For example: enable password <keyword> aaa authentication login default group radius enable

  Further Information: The fix for this bug also fixes an unrelated problem that may allow unauthorized users access to EXEC mode if the ''line'' authentication method is configured with fallback to the "none" authentication method. In other words, if the following is configured:

  ```
  aaa new-model aaa authentication login MYMETHOD line none
  line con 0 login authentication MYMETHOD password <some password>
  ```

  then users providing the wrong password at the password prompt will be granted access.

  This issue was originally introduced by Cisco Bug ID CSCee85053, and fixed in some Cisco IOS releases via Cisco Bug IDs CSCsb26389 ("Failover for aaa authentication method LINE is broken") and CSCsv06823 ("Authentication request doesnt failover to any method after enable"). However, the fix for this problem was not integrated into some Cisco IOS releases and this bug (CSCth25634) takes care of that.

  Note that Cisco Bug ID CSCti82605 ("AAA line password failed and access to switch still passed") is a recent bug that was filed once it was determined that the fix for CSCee85053 was still missing from some Cisco IOS releases. CSCti82605 was then made a duplicate of this bug (CSCth25634) since the fix for this bug also fixes CSCti82605.

Resolved Infrastructure Caveats

- CSCsv05154—Resolved in 15.0(1)SY

  Symptom: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20090114-http

  Conditions: See "Additional Information" section in the posted response for further details.

  Workarounds: See "Workaround" section in the posted response for further details.

- CSCti25339—Resolved in 15.0(1)SY

  Symptoms: Cisco IOS device may experience a device reload.

Conditions: This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

Workaround: There is no workaround.

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2010-3050 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCti92164—Resolved in 15.0(1)SY

  Symptom: Standby Route Processor reloads, with trace backs indicating NAT Port allocations with high availability.

  Conditions: If the device is configured for:

  a) High Availability - SSO via the configuration command **mode sso** under **redundancy**

  b) Is configured with NAT Interface Overload.

  c) Is configured with IP SLA (or SNMP -- See Cisco Bug ID CSCtj44746) and a lot of NAT traffic is flowing through the active route processor while the standby route processor is booting up.

  Workaround: None.

- CSCtk67073—Resolved in 15.0(1)SY

  The Cisco IOS IP Service Level Agreement (IP SLA) feature contains a denial of service (DoS) vulnerability. The vulnerability is triggered when malformed UDP packets are sent to a vulnerable device. The vulnerable UDP port numbers depend on the device configuration. Default ports are not used for the vulnerable UDP IP SLA operation or for the UDP responder ports.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipsla.

- CSCsl39986—Resolved in 15.0(1)SY

  Symptom: The changes introduced by Cisco bug ID CSCsi73899 introduced some performance impact.

  Conditions: Only IOS versions with CSCsi73899 integrated and not CSCsl39986 are affected. These images are only interim images and should not be available on Cisco.com for general download purposes.

  Workaround: None.

Resolved IPServices Caveats

- CSCsv87997—Resolved in 15.0(1)SY

  Symptom: DHCPv6 relay process crash on Actice RP.

  Conditions: Unknown at this time.

  Workaround: Unknown at this time.

- CSCsx16152—Resolved in 15.0(1)SY

  Symptom: Under unique circumstances erroneous routing prefixes may be added to the routing table.

  Conditions: When the DHCPv6 relay feature is enabled and a router receives a normal DHCPv6 relay reply packet, this may lead to an erroneous route being added to the routing table.

  Workaround: No workaround except turning off DHCPv6 relay.

- CSCta98734—Resolved in 15.0(1)SY

  Symptom: DNS Memory Leak in DNS queries

  Conditions: DNS server configured: 'ip dns server'

  This bug can only possibly surface if the "ip dns-server" is configured, and then only when specific malformed datagrams are received on the DNS udp port 53. This specific datagram malfrmation is that the udp length field indicates a zero-length payload. This should never happen during normal DNS operation.

  Workaround: No Workaround at this time

- CSCtd10712—Resolved in 15.0(1)SY

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  Session Initiation Protocol (Multiple vulnerabilities)
  H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-nat

- CSCte14603—Resolved in 15.0(1)SY

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20100922-igmp.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4a315.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtj57173—Resolved in 15.0(1)SY

  Symptom: Cisco IOS Software crashes when processing a specially crafted DNS reply packet.

  Conditions: Router is configured to request DNS server lookups via the command **ip name-server a.b.c.d** and has domain look up enabled (enabled by default).

  Affects all versions of Cisco IOS Software prior to first fixed software.

  Workaround: Disable the IP Name server look up functionality on Cisco IOS Software, with the command **no ip domain-lookup**.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

  CVE ID CVE-2011-0958 has been assigned to document this issue.

  Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCtr28857—Resolved in 15.0(1)SY

  Summary A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

  Note: The March 28, 2012, Cisco IOS Software Security Advisory bundled publication includes nine Cisco Security Advisories. Each advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all vulnerabilities in the March 2012 bundled publication.

  Individual publication links are in ''Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication'' at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar12.html

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2012-0382 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved LegacyProtocols Caveats

- CSCtf74999—Resolved in 15.0(1)SY

  Summary A router configured for DLSw might crash when it receives a series of certain malformed packets. This issue requires a number of conditions and a narrow timing window.

  Conditions: Cisco IOS devices configured for DLSw.

  Workaround: The only workaround in the device is to disable DLSw if not needed.

Additional mitigations can be found in the following Applied Mitigation Bulletin: http://tools.cisco.com/security/center/content/CiscoAppliedMitigationBulletin/cisco-amb-20080326-dlsw

PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 5.4/4.5:

https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:H/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

CVE ID CVE-2011-1625 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCth69364—Resolved in 15.0(1)SY

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-dlsw.

Resolved MPLS Caveats

- CSCsz45567—Resolved in 15.0(1)SY

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

  This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20100324-ldp.shtml

Resolved Multicast Caveats

- CSCtc68037—Resolved in 15.0(1)SY

  Symptom: A Cisco IOS device may experience an unexpected reload as a result of mtrace packet processing.

  Conditions:

  Workaround: None other than avoiding the use of mtrace functionality.

Resolved Routing Caveats

- CSCtc61584—Resolved in 15.0(1)SY

  Symptom: Device may experience memory leak when receiving a flood of ICMPv6 messages. The memory leak will recover (ie., memory will be released successfully in about 4 hours).

  Conditions: Device configured for IPv6 and PMTUD.

Workaround: PMTUD is enabled by default when using TCP over IPv6, and it is not possible to disable it. For this reason a possible workaround is to use an ACL to block the ICMPv6 “packet too big” message.

Please note that filtering out ICMPv6 “packet too big” messages means that the Layer 3 (IPv6) PMTUD is being shut down as well. Therefore, it is necessary to make sure that the MTU is set on the end host to the lowest possible IPv6 MTU - 1280 bytes. Otherwise, since the device is not seeing the “packet too big” message, the device will not know that an intermediate system has dropped a packet because it was too big.

ICMPv6 “packet too big” messages are the IPv6 equivalent to the ICMPv4 “fragmentation needed and DF bit set” message.

Resolved Security Caveats

- CSCsz32366—Resolved in 15.0(1)SY

  Symptoms: A Cisco router that is running Cisco IOS Release 12.4(25) may crash due to SSH.

  Conditions: This symptom occurs when SSH is enabled on the router. An attempt to access the router via SSH is made.

  Workaround: Do not use SSH. Disable SSH on the router by removing the RSA keys:

  “crypto key zeroize rsa”

  Further Problem Description: This issue has not been seen in Cisco IOS Release 12.4(23) and earlier releases. It also has not been seen in Cisco IOS Release 12.4T images.

- CSCth45540—Resolved in 15.0(1)SY

  Symptom: Device crashes in SSH Process

  Conditions: SSH process has to fail to allocate memory for the new connection. This would only occur in extremely low memory conditions.

  Workaround: None.

Resolved Cisco IOS Caveats

- CSCta57436—Resolved in 15.0(1)SY

  Symptoms: Router may experience reload after certain corrupted packets are injected into MPLS path.

  Conditions: Certain corrupted packets are injected into MPLS path.

  Workaround: None.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 7.1/5.9: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C No CVE ID has been assigned to this issue. Additional information on Cisco’s security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCtc41760—Resolved in 15.0(1)SY

  Symptom: 6500 may experience redzone crash at UDLD process. Message may appear %SYS-SP-3-OVERRUN: Block overrun at 44456570 (red zone 6D000700) -Traceback= 40291448 402938DC 40D74570 40D763A0

  Traceback will vary from code to code.

  Conditions: UDLD configured

Workaround: Disable UDLD.

- CSCth87458—Resolved in 15.0(1)SY

  Symptoms: Memory leak detected in SSH process during internal testing. Authentication is required in order for a user to cause the memory leak.

  Conditions: This was experienced during internal protocol robustness testing.

  Workaround: Allow SSH connections only from trusted hosts.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.8/5.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:L/Au:S/C:N/I:N/A:C/E:F/RL:OF/RC:C CVE ID CVE-2011-2568 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL: http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCtj22354—Resolved in 15.0(1)SY

  Symptom: System may crash when receiving LLDPDUs.

  Conditions: Incoming LLDPDUs with more than 10 LLDP MA(Management Address) TLVs

  Workaround: Disable LLDP MA TLV sending on the peers.

  Further Problem Description: Currently LLDP supports 10 MA TLVs per LLDP neighbor entry, however, it is not processed properly when more than 10 MA TLVs are received.

- CSCtj30155—Resolved in 15.0(1)SY

  Symptom: Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCtn76183—Resolved in 15.0(1)SY

  The Cisco IOS Software Network Address Translation (NAT) feature contains two denial of service (DoS) vulnerabilities in the translation of IP packets.

  The vulnerabilities are caused when packets in transit on the vulnerable device require translation.

  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-20120926-nat

  Note: The September 26, 2012, Cisco IOS Software Security Advisory bundled publication includes 9 Cisco Security Advisories. Eight of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each Cisco

IOS Software Security Advisory lists the Cisco IOS Software releases that correct the vulnerability or vulnerabilities detailed in the advisory as well as the Cisco IOS Software releases that correct all Cisco IOS Software vulnerabilities in the September 2012 bundled publication.

Individual publication links are in the "Cisco Event Response: Semi-Annual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep12.html

- CSCto07919—Resolved in 15.0(1)SY

  Symptom: Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20110928-ipv6mpls

- CSCtq36336—Resolved in 15.0(1)SY

  Symptom: An external loop between 2 dot1x enabled ports can cause a storm of unicast EAPoL pdus in the network.

  Workaround: Avoid creating a loop.

  PSIRT Evaluation: The Cisco PSIRT has assigned this bug the following CVSS version 2 score. The Base and Temporal CVSS scores as of the time of evaluation are 6.1/5.8: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:U/RC:C CVE ID CVE-2011-2058 has been assigned to document this issue. Additional information on Cisco's security vulnerability policy can be found at the following URL:
  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

- CSCtc71597—Resolved in 15.0(1)SY

  Symptom: Currently in EARL7 system, For an IPv6 packet the 96 bytes cover DBUS header (22), Ether header (14), IPv6 harder (40), IPv6 extension headers, and L4 header. That means only 20 bytes (96 - 22 - 14 - 40) are for extension header(s) and L4 header. So even packet with small extension header(s) can use up to 20 bytes that would cause l4_hdr_vld = 0. When that happens, all L4 features cannot be applied and packet would be hardware forwarded based on L3 forwarding result.

  Conditions: This issue is present from day one but would cause threat only when ipv6 access-list is configured on any interface and that access-list is containing L4 options.

  Workaround: No Workaround

- CSCtb73450—Resolved in 15.0(1)SY

  Symptom: Start-Control-Connection-Request (SCCRQ) packets may cause tunnel to reset after digest failure.

  Conditions: This issue is observed when the SCCRQ packets are sent with an incorrect hash.

  Workaround: There is no workaround.

- CSCsh61458—Resolved in 15.0(1)SY

  Symptoms: A Cat4k switch may reload after receiving a malformed packet on one specific specific port.

  Conditions: This symptom may be observed on a Cat4k switch that enables DNSIX audit trail and recieves crafted IP packets on a specific port.

  Workaround: Do not enable the DNSIX audit trail.

- CSCth27791—Resolved in 15.0(1)SY

  Symptoms: This bug has been filed to enhance the code to follow secure best practices and enhance resiliency of the product.

  Conditions: Not applicable.

  Workaround: Not applicable

  PSIRT Evaluation: The Cisco PSIRT has evaluated this issue and does not meet the criteria for PSIRT ownership or involvement. This issue will be addressed via normal resolution channels.

  If you believe that there is new information that would cause a change in the severity of this issue, please contact psirt@cisco.com for another evaluation.

  Additional information on Cisco's security vulnerability policy can be found at the following URL:

  http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html

Resolved VPDN Caveats

- CSCsw41041—Resolved in 15.0(1)SY

  Symptom: Cisco ASR1000 routers running Cisco IOS software may experience a crash when PPTP packets are sent under certain conditions to a router with VPN features configured.

  Conditions: Normal Conditions.

  Workaround: CoPP may be configured on the device to protect the management and control planes and to workaround this risk by explicitly permitting only authorized traffic sent to the route processor in accordance with existing security policies and configurations. The following example can be adapted to your network.

```
!-- Permit all TCP and UDP PPTP traffic sent to all IP addresses
!-- configured on all interfaces of the affected device so that it
!-- will be policed and dropped by the CoPP feature
access-list 100 permit tcp any any eq 1723  access-list 100 permit udp any any eq 1723
!-- Permit (Police or Drop)/Deny (Allow) all other Layer3 and Layer4
!-- traffic in accordance with existing security policies and
!-- configurations for traffic that is authorized to be sent
!-- to infrastructure devices
!
!-- Create a Class-Map for traffic to be policed by
!-- the CoPP feature
class-map match-all drop-pptp-class match access-group 100
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device
policy-map drop-pptp-traffic class drop-pptp-class  police 8000 conform-action drop
!-- Apply the Policy-Map to the Control-Plane of the
!-- device
control-plane service-policy input drop-pptp-traffic
```

Resolved WAN Caveats

- CSCtd75033—Resolved in 15.0(1)SY

  Symptom: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability. Note: The fix for this vulnerability has a behavior change affect on Cisco IOS Operations for Mode 7 packets. See the section **Further Description** of this release note enclosure.

  Conditions: Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

  This is the same as the vulnerability which is described in http://www.kb.cert.org/vuls/id/568372

  Cisco has release a public facing vulnerability alert at the following link: http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

  Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

  All other versions of Cisco IOS and Cisco IOS XE Software are affected.

  To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

  ```
  ntp master <any following commands>
  ntp peer <any following commands>
  ntp server <any following commands>
  ntp broadcast client ntp multicast client
  ```

  The following example identifies a Cisco device that is configured with NTP:

  ```
  router#show running-config | include ntp ntp peer 192.168.0.12
  ```

  The following example identifies a Cisco device that is not configured with NTP:

  ```
  router#show running-config | include ntp router#
  ```

  To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to “Cisco Internetwork Operating System Software” or “Cisco IOS Software.” The image name displays in parentheses, followed by “Version” and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

  The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

  ```
  Router#show version Cisco Internetwork Operating System Software IOS (tm) 2500
  Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE (fc2) Technical Support:
  http://www.cisco.com/techsupport Copyright ) 1986-2008 by cisco Systems, Inc. Compiled
  Mon 17-Mar-08 14:39 by dchih
  <output truncated>
  ```

  The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

  ```
  Router#show version Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M),
  Version 12.4(20)T, RELEASE SOFTWARE (fc3) Technical Support:
  http://www.cisco.com/techsupport Copyright ) 1986-2008 by Cisco Systems, Inc. Compiled
  Thu 10-Jul-08 20:25 by prod_rel_team
  <output truncated>
  ```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS and NX-OS Software Reference Guide" at the following link: http://www.cisco.com/web/about/security/intelligence/ios-ref.html

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note NTP peer authentication is not a workaround and is still a vulnerable configuration.

- NTP Access Group

  Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

  ```
  !--- Configure trusted peers for allowed access
  access-list 1 permit 171.70.173.55
  !--- Apply ACE to the NTP configuration
  ntp access-group peer 1
  ```

  For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

- Infrastructure Access Control Lists

  Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

  Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

  Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

  ```
  !---
  !--- Feature: Network Time Protocol (NTP)
  !---
  access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
  INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
  !--- Note: If the router is acting as a NTP broadcast client
  !--- via the interface command "ntp broadcast client"
  !--- then broadcast and directed broadcasts must be
  !--- filtered as well. The following example covers
  !--- an infrastructure address space of 192.168.0.X
  access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 192.168.0.255 eq
  ntp access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host
  255.255.255.255 eq ntp
  !--- Note: If the router is acting as a NTP multicast client
  ```

```
!--- via the interface command "ntp multicast client"
!--- then multicast IP packets to the mutlicast group must
!--- be filtered as well. The following example covers
!--- a NTP multicast group of 239.0.0.1 (Default is
!--- 224.0.1.1)
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 239.0.0.1 eq ntp
!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.
access-list 150 permit ip any any
!--- Apply access-list to all interfaces (only one example
!--- shown)
interface fastEthernet 2/0 ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

– Control Plane Policing

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

– Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD any eq 123
!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.
access-list 150 permit udp any any eq 123
!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all drop-udp-class match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
policy-map drop-udp-traffic class drop-udp-class drop
!--- Apply the Policy-Map to the
```

```
!--- Control-Plane of the device
control-plane service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

– Rate Limiting the traffic to the device The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning: If the rate-limits are exceeded valid NTP traffic may also be dropped.

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 permit udp any any eq 123
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all rate-udp-class match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section “4. Tuning the CoPP Policy” of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates
policy-map rate-udp-traffic class rate-udp-class police 10000 1500 1500
conform-action transmit exceed-action drop violate-action drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:
http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html

Further Description

Cisco IOS Software releases that have the fix for this Cisco bug ID, have a behavior change for mode 7 private mode packets.

Cisco IOS Software release with the fix for this Cisco bug ID, will not process NTP mode 7 packets, and will display a message “NTP: Receive: dropping message: Received NTP private mode packet. 7” if debugs for NTP are enabled.

To have Cisco IOS Software process mode 7 packets, the CLI command **ntp allow mode private** should be configured. This is disabled by default.

Other Resolved Caveats in Release 15.0(1)SY

Identifier	Technology	Description
CSCtb57180	Infrastructure	Device may crash when processing parallel "show user" commands
CSCsz71787	LegacyProtocols	Router crash by crafted IP packet.
CSCsu09697	Security	hidekeys: "key chains" doesn't hide keys in parser logs

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

Note Catalyst 6500 series switches do not support ISL-encapsulated Token Ring frames. To support trunked Token Ring traffic in your network, make trunk connections directly between switches that support ISL-encapsulated Token Ring frames. When a Catalyst 6500 series switch is configured as a VTP server, you can configure Token Ring VLANs from the switch.

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+
Per-switch 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/en/US/products/hw/switches/ps708/tsd_products_support_troubleshoot_and_alerts.html

System Software Upgrade Instructions

See this publication:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a0080116ff0.shtml

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

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:

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].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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