Release Notes for Cisco IOS Release 12.2SY

February 28, 2013

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 12.2SY releases:

  http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd804f0694.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/12.2SY/release/notes/ol_20679.html

Caution

Cisco IOS running on the switch processor and the route processor supports redundant configurations where the switch processor and the route processor are identical. If they are not identical, one switch processor and the route processor 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

This is a chronological list of the 12.2SY releases:

- Release 12.2(50)SY4—28 Feb 2013
- Release 12.2(50)SY3—14 Sep 2012
- Release 12.2(50)SY2—23 May 2012
- Release 12.2(50)SY1—30 Nov 2011
- Release 12.2(50)SY—29 Jun 2011

Hierarchical List of Releases

These releases support the hardware listed in the "Supported Hardware" section on page 3:

- Release 12.2(50)SY4:
  - Date of release: 28 Feb 2013
  - Based on Release 12.2(50)SY3
- Release 12.2(50)SY3:
  - Date of release: 14 Sep 2012
  - Based on Release 12.2(50)SY2
- Release 12.2(50)SY2:
  - Date of release: 23 May 2012
  - Based on Release 12.2(50)SY1

- Release 12.2(50)SY1:
  - Date of release: 30 Nov 2011
  - Based on Release 12.2(50)SY
- Release 12.2(50)SY:
  - Date of release: 29 Jun 2011
  - Based on Release 12.2(33)SXI3

Note Release 12.2(50)SY supports only Ethernet ports. Release 12.2(50)SY does not support any WAN features or commands.

Supported Hardware

These sections describe the hardware supported in Release 12.2(50)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	12.2(50)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 5.
- Supports 2-Tbps switch fabric connectivity.
- 2-GB DRAM.
- Internal 1-GB bootflash (**bootdisk:**).
- One external slot:
  - **disk0:**
  - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 2T-10GE.
- Console ports:
  - EIA/TIA-232 (RS-232) port
  - USB port
- Ports 1, 2, and 3:
  - QoS architecture: **2q4t/1p3q4t**
  - Ports 1, 2, and 3: Gigabit Ethernet SFP (fiber 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.

Policy Feature Card 4XL

Product ID (append "=" for spares)	Product Description	Minimum Software Version
VS-F6K-PFC4XL	Policy Feature Card 4XL (PFC4XL)	
	With Supervisor Engine 2T-10GE	12.2(50)SY
Note Use VS-F6K-PFC4XL= to upgrade to a PFC4XL.		

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	12.2(50)SY

Distributed and Centralized Forwarding Cards

Note

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

  http://www.cisco.com/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	12.2(50)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	12.2(50)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	12.2(50)SY

10-Gigabit Ethernet Switching Modules

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

Note

- 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.
- To configure WS-X6908-10GE port oversubscription, use the **hw-module oversubscription** command.
- In a 3-slot chassis, supported only with WS-C6503-E hardware revision 1.3 or higher.

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 • dCEF2T • Supports egress multicast replication • 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	
	With Supervisor Engine 2T-10GE	12.2(50)SY

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

Note

- 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.
- When not configured in oversubscription mode, supported in virtual switch links.
- To configure port oversubscription, use the **hw-module slot** command.

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 • dCEF720 • Supports egress multicast replication • 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	
	With Supervisor Engine 2T-10GE	12.2(50)SY

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

Note

- 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.
- To configure port oversubscription, use the **hw-module slot** command.

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 • dCEF720 • Supports egress multicast replication • 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.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

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 • 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 • Supports egress multicast replication • 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)	
	With Supervisor Engine 2T-10GE	12.2(50)SY

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 • 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. • Supports egress multicast replication • 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.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

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 • 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. • Supports egress multicast replication • 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.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

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

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 • 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. • Supports egress multicast replication • 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.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

WS-X6148E-GE-45AT

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148E-GE-45AT	48-port 10/100/1000 Mbps • 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.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

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 • 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. • Do not support traffic storm control.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

WS-X6148-FE-SFP Fast Ethernet Switching Module

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148-FE-SFP	48-port 100BASE-FX • 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.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

WS-X6148A-RJ-45, WS-X6148A-45AF 10/100 Ethernet Switching Modules

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-X6148A-RJ-45 **WS-X6148A-45AF**	48-port 10/100TX RJ-45 • 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.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

Power over Ethernet Daughtercards

Note The power over Ethernet (PoE) daughtercard "Power Required" values do not include the power drawn by phones.

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	12.2(50)SY

Transceivers

- X2 Modules, page 17
- XENPAKs, page 19
- Small Form-Factor Pluggable (SFP) Modules, page 21

X2 Modules

Note

- WS-X6716-10GE do not support X2 modules that are labeled with a number that ends with -01. (This restriction does not apply to X2-10GB-LRM.)
- All X2 modules shipped since WS-X6716-10GE 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	12.2(50)SY
	10 Gbps Ethernet SFP+ Modules	
	SFP-10G-LRM—10GBASE-LRM 1310 nm MMF and SMF	12.2(50)SY
	SFP-10G-SR—10GBASE-SR 850 nm MMF	12.2(50)SY
	SFP-H10GB-CU1M—1m Twinax cable, passive, 30AWG cable assembly	12.2(50)SY
	SFP-H10GB-CU3M—3m Twinax cable, passive, 30AWG cable assembly	
	SFP-H10GB-CU5M—5m Twinax cable, passive, 24AWG cable assembly	

Product ID (append "=" for spares)	Product Description		Minimum Software Version
DWDM-X2-60.61=	10GBASE-DWDM 1560.61 nm X2 (100-GHz ITU grid)	ITU 21	12.2(50)SY
DWDM-X2-59.79=	10GBASE-DWDM 1559.79 nm X2 (100-GHz ITU grid)	ITU 22	
DWDM-X2-58.98=	10GBASE-DWDM 1558.98 nm X2 (100-GHz ITU grid)	ITU 23	
DWDM-X2-58.17=	10GBASE-DWDM 1558.17 nm X2 (100-GHz ITU grid)	ITU 24	
DWDM-X2-56.55=	10GBASE-DWDM 1556.55 nm X2 (100-GHz ITU grid)	ITU 26	
DWDM-X2-55.75=	10GBASE-DWDM 1555.75 nm X2 (100-GHz ITU grid)	ITU 27	
DWDM-X2-54.94=	10GBASE-DWDM 1554.94 nm X2 (100-GHz ITU grid)	ITU 28	
DWDM-X2-54.13=	10GBASE-DWDM 1554.13 nm X2 (100-GHz ITU grid)	ITU 29	
DWDM-X2-52.52=	10GBASE-DWDM 1552.52 nm X2 (100-GHz ITU grid)	ITU 31	
DWDM-X2-51.72=	10GBASE-DWDM 1551.72 nm X2 (100-GHz ITU grid)	ITU 32	
DWDM-X2-50.92=	10GBASE-DWDM 1550.92 nm X2 (100-GHz ITU grid)	ITU 33	
DWDM-X2-50.12=	10GBASE-DWDM 1550.12 nm X2 (100-GHz ITU grid)	ITU 34	
DWDM-X2-48.51=	10GBASE-DWDM 1548.51 nm X2 (100-GHz ITU grid)	ITU 36	
DWDM-X2-47.72=	10GBASE-DWDM 1547.72 nm X2 (100-GHz ITU grid)	ITU 37	
DWDM-X2-46.92=	10GBASE-DWDM 1546.92 nm X2 (100-GHz ITU grid)	ITU 38	
DWDM-X2-46.12=	10GBASE-DWDM 1546.12 nm X2 (100-GHz ITU grid)	ITU 39	
DWDM-X2-44.53=	10GBASE-DWDM 1544.53 nm X2 (100-GHz ITU grid)	ITU 41	
DWDM-X2-43.73=	10GBASE-DWDM 1543.73 nm X2 (100-GHz ITU grid)	ITU 42	
DWDM-X2-42.94=	10GBASE-DWDM 1542.94 nm X2 (100-GHz ITU grid)	ITU 43	
DWDM-X2-42.14=	10GBASE-DWDM 1542.14 nm X2 (100-GHz ITU grid)	ITU 44	
DWDM-X2-40.56=	10GBASE-DWDM 1540.56 nm X2 (100-GHz ITU grid)	ITU 46	
DWDM-X2-39.77=	10GBASE-DWDM 1539.77 nm X2 (100-GHz ITU grid)	ITU 47	
DWDM-X2-38.98=	10GBASE-DWDM 1538.98 nm X2 (100-GHz ITU grid)	ITU 48	
DWDM-X2-38.19=	10GBASE-DWDM 1538.19 nm X2 (100-GHz ITU grid)	ITU 49	
DWDM-X2-36.61=	10GBASE-DWDM 1536.61 nm X2 (100-GHz ITU grid)	ITU 51	
DWDM-X2-35.82=	10GBASE-DWDM 1535.82 nm X2 (100-GHz ITU grid)	ITU 52	
DWDM-X2-35.04=	10GBASE-DWDM 1535.04 nm X2 (100-GHz ITU grid)	ITU 53	
DWDM-X2-34.25=	10GBASE-DWDM 1534.25 nm X2 (100-GHz ITU grid)	ITU 54	
DWDM-X2-32.68=	10GBASE-DWDM 1532.68 nm X2 (100-GHz ITU grid)	ITU 56	
DWDM-X2-31.90=	10GBASE-DWDM 1531.90 nm X2 (100-GHz ITU grid)	ITU 57	
DWDM-X2-31.12=	10GBASE-DWDM 1531.12 nm X2 (100-GHz ITU grid)	ITU 58	
DWDM-X2-30.33=	10GBASE-DWDM 1530.33 nm X2 (100-GHz ITU grid)	ITU 59	
X2-10GB-ZR	10GBASE-ZR X2 Module for SMF		12.2(50)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
X2-10GB-CX4	10GBASE for CX4 (copper) cable	12.2(50)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.	12.2(50)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.	12.2(50)SY
X2-10GB-LRM	10GBASE-LRM for FDDI-grade multimode fiber (MMF) **Note** Not supported by the **show idprom** command. (CSCsj35671)	12.2(50)SY
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.	12.2(50)SY
X2-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	12.2(50)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)	12.2(50)SY
DWDM-XENPAK	10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid	12.2(50)SY
WDM-XENPAK-REC	10GBASE receive-only wavelength division multiplexing (WDM)	12.2(50)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
XENPAK-10GB-CX4	10GBASE for CX4 (copper) cable; uses Infiniband connectors	12.2(50)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	12.2(50)SY
XENPAK-10GB-ER+	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(50)SY
XENPAK-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(50)SY
XENPAK-10GB-LR+	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(50)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)	12.2(50)SY
XENPAK-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	12.2(50)SY
XENPAK-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	12.2(50)SY
XENPAK-10GB-ZR	10GBASE for any SMF type	12.2(50)SY

Small Form-Factor Pluggable (SFP) Modules

These sections describe SFPs:

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 Dense Wavelength-Division Multiplexing Small Form-Factor Pluggable Module* data sheet:

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

- See the "Unsupported Hardware" section on page 29 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	12.2(50)SY
GLC-BX-U	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength	12.2(50)SY
GLC-LH-SMD **GLC-LH-SM**	1000BASE-LX/LH SFP	12.2(50)SY
GLC-SX-MMD **GLC-SX-MM**	1000BASE-SX SFP	12.2(50)SY
GLC-T	1000BASE-T 10/100/1000 SFP module **Note** Supported only at 1000 Mbps.	12.2(50)SY
GLC-ZX-SM	1000BASE-ZX SFP module	12.2(50)SY
CWDM-SFP-1470	CWDM 1470-nm (Gray) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	12.2(50)SY
CWDM-SFP-1490	CWDM 1490-nm (Violet) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	12.2(50)SY
CWDM-SFP-1510	CWDM 1510-nm (Blue) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	12.2(50)SY
CWDM-SFP-1530	CWDM 1530-nm (Green) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	12.2(50)SY

Product ID (append "=" for spares)	Product Description	Minimum Software Version
CWDM-SFP-1550	CWDM 1550-nm (Yellow) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	12.2(50)SY
CWDM-SFP-1570	CWDM 1570-nm (Orange) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	12.2(50)SY
CWDM-SFP-1590	CWDM 1590-nm (Red) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	12.2(50)SY
CWDM-SFP-1610	CWDM 1610-nm (Brown) Gigabit Ethernet, 1 and 2 Gb Fibre Channel SFP module	12.2(50)SY
DWDM-SFP-5817	1000BASE-DWDM 1558.17 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5252	1000BASE-DWDM 1552.52 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5172	1000BASE-DWDM 1551.72 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5012	1000BASE-DWDM 1550.12 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4692	1000BASE-DWDM 1546.92 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4373	1000BASE-DWDM 1543.73 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4214	1000BASE-DWDM 1542.14 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3977	1000BASE-DWDM 1539.77 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3898	1000BASE-DWDM 1538.98 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3582	1000BASE-DWDM 1535.82 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3504	1000BASE-DWDM 1535.04 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-6061	1000BASE-DWDM 1560.61 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5979	1000BASE-DWDM 1559.79 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5898	1000BASE-DWDM 1558.98 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5655	1000BASE-DWDM 1556.55 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5575	1000BASE-DWDM 1555.75 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5494	1000BASE-DWDM 1554.94 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5413	1000BASE-DWDM 1554.13 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-5092	1000BASE-DWDM 1550.92 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4851	1000BASE-DWDM 1548.51 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4772	1000BASE-DWDM 1547.72 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4612	1000BASE-DWDM 1546.12 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4453	1000BASE-DWDM 1544.53 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4294	1000BASE-DWDM 1542.94 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-4056	1000BASE-DWDM 1540.56 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3819	1000BASE-DWDM 1538.19 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3661	1000BASE-DWDM 1536.61 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3425	1000BASE-DWDM 1534.25 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3268	1000BASE-DWDM 1532.68 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3190	1000BASE-DWDM 1531.90 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3112	1000BASE-DWDM 1531.12 nm SFP (100-GHz ITU grid) SFP module	12.2(50)SY
DWDM-SFP-3033	1000BASE-DWDM 1530.33 nm SFP (100-GHz ITU grid) SFP module	12.2(50)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	12.2(50)SY
GLC-FE-100BX-D	100BASE-BX10-D SFP	12.2(50)SY
GLC-FE-100EX	100BASEEX SFP	12.2(50)SY
GLC-FE-100ZX	100BASEZX SFP	12.2(50)SY
GLC-FE-100FX	100BASEFX SFP	12.2(50)SY
GLC-FE-100LX	100BASELX SFP	12.2(50)SY

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.
- How you have EtherChannels configured 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 24
- Firewall Services Module (FWSM), page 24
- Network Analysis Modules (NAMs), page 24
- Wireless Services Module (WiSM), page 25

Application Control Engine (ACE) Module

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
ACE20-MOD-K9	Application Control Engine (ACE) module	
	With Supervisor Engine 2T-10GE	12.2(50)SY

ACE20-MOD-K9 run their own software—See these publications:

http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

See the ACE20-MOD-K9 software release notes for information about the minimum required service module software version.

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	12.2(50)SY

Note

- 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-NAM-2 **WS-SVC-NAM-1**	Network Analysis Module 2 Network Analysis Module 1	
	With Supervisor Engine 2T-10GE	12.2(50)SY

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 Module (WiSM)

Product ID (append "=" for spares)	Product Description	Minimum Software Versions
WS-SVC-WISM-1-K9	Wireless Services Module (WiSM)	
	With Supervisor Engine 2T-10GE	12.2(50)SY
WS-SVC-WISM-1-K9 runs its own software—See these publications: http://www.cisco.com/en/US/products/ps6526/tsd_products_support_eol_model_home.html See the WS-SVC-WISM-1-K9 software release notes for information about the minimum required WS-SVC-WISM-1-K9 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	12.2(50)SY
PWR-2700-DC/4	2700 W DC power supply	12.2(50)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	12.2(50)SY
PWR-950-AC	950 W AC power supply	12.2(50)SY
PWR-950-DC	950 W DC power supply	12.2(50)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	12.2(50)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	12.2(50)SY
WS-CAC-6000W	6,000 W AC power supply	12.2(50)SY
PWR-4000-DC	4,000 W DC power supply	12.2(50)SY
WS-CAC-4000W	4,000 W AC power supply	12.2(50)SY
+WS-CAC-3000W	3,000 W AC power supply	12.2(50)SY
WS-CAC-3000W	3,000 W AC power supply	12.2(50)SY
WS-CAC-2500W	2,500 W AC power supply	12.2(50)SY
WS-CDC-2500W	2,500 W DC power supply	12.2(50)SY

Chassis

13-Slot Chassis

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-C6513-E	Catalyst 6513-E chassis: • 13 slots **Note:** When a Supervisor Engine 2T is installed, slot 7 and slot 8 are reserved for supervisor engines. • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	12.2(50)SY

9-Slot Chassis

Product ID (append "=" for spares)	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	12.2(50)SY

Product ID (append "=" for spares)	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	12.2(50)SY

6-Slot Chassis

Product ID (append "=" for spares)	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	12.2(50)SY

4-Slot Chassis

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-C6504-E	Catalyst 6504-E chassis: • 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 2T-10GE	12.2(50)SY

3-Slot Chassis

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-C6503-E	• 3 slots • 64 chassis MAC addresses • WS-X6908-10GE is supported only with WS-C6503-E hardware revision 1.3 or higher.	
	With Supervisor Engine 2T-10GE	12.2(50)SY

Unsupported Hardware

Release 12.2SY supports only the hardware listed in the "Supported Hardware" section on page 3. Unsupported modules remain powered down if detected and do not affect system behavior.

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

- 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 12.2(50)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.

ISSU Compatibility

SX SY ISSU Compatibility Matrix (also known as the EFSU compatibility matrix)

Cisco IOS Behavior Changes

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

- Release 12.2(50)SY4, page 30
- Release 12.2(50)SY3, page 31
- Release 12.2(50)SY2, page 31
- Release 12.2(50)SY1, page 31

Release 12.2(50)SY4

No behavior changes are introduced in Release 12.2(50)SY4.

Release 12.2(50)SY3

No behavior changes are introduced in Release 12.2(50)SY3.

Release 12.2(50)SY2

No behavior changes are introduced in Release 12.2(50)SY2.

Release 12.2(50)SY1

No behavior changes are introduced in Release 12.2(50)SY1.

New Features in Release 12.2(50)SY4

These sections describe the new features in Release 12.2(50)SY4, 28 Feb 2013:

- New Hardware Features in Release 12.2(50)SY4, page 31
- New Software Features in Release 12.2(50)SY4, page 31

New Hardware Features in Release 12.2(50)SY4

None.

New Software Features in Release 12.2(50)SY4

None.

New Features in Release 12.2(50)SY3

These sections describe the new features in Release 12.2(50)SY3, 14 Sep 2012:

- New Hardware Features in Release 12.2(50)SY3, page 31
- New Software Features in Release 12.2(50)SY3, page 31

New Hardware Features in Release 12.2(50)SY3

None.

New Software Features in Release 12.2(50)SY3

None.

New Features in Release 12.2(50)SY2

These sections describe the new features in Release 12.2(50)SY2, 23 May 2012:

New Hardware Features in Release 12.2(50)SY2

None.

New Software Features in Release 12.2(50)SY2

None.

New Features in Release 12.2(50)SY1

These sections describe the new features in Release 12.2(50)SY1, 30 Nov 2011:

New Hardware Features in Release 12.2(50)SY1

None.

New Software Features in Release 12.2(50)SY1

None.

New Features in Release 12.2(50)SY

These sections describe the new features in Release 12.2(50)SY, 29 Jun 2011:

New Hardware Features in Release 12.2(50)SY

Release 12.2(50)SY supports the hardware listed in the "Supported Hardware" section on page 3. The following hardware is supported for the first time in Release 12.2(50)SY:

- 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 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 9
- WS-X6816-10G-2T, WS-X6716-10G 16-Port 10-Gigabit Ethernet X2 Switching Module, page 10
- WS-X6848-SFP-2T, WS-X6748-SFP 48-Port Gigabit Ethernet SFP Switching Module, page 12
- WS-X6848-TX-2T, WS-X6748-GE-TX, page 14

New Software Features in Release 12.2(50)SY

Note On Sup2T (EARL8) new MAC learns for routed frames may not immediately be synced across all DFCs. When New MAC learns for routed frames, no FF is created. As a result, the MAC table between DFCs in the system may be out of sync until software synchronization performs an update (approximately 160 seconds). As a workaround, "platform mac address-table synchronize learn layer3" was added to enable Supervisor2T to learn new MACs (and MAC moves) on routed traffic. This command is disabled by default.

- ACL - Hardware and software counters granularity for IPv4 and IPv6 ACL Statistics—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-sec-trfltr-fw.html
- Allow mixed cos/dscp threshold in a QoS LAN-queueing policy—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/qos_policy_based_queueing.html
- Blue Beacon for service indication—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/introduction.html#Blue_Beacon
- Callhome message using dedicated interface—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/callhome.html#Configuring_a_Destination_Profile_for_Email
- Cisco Express Forwarding - SNMP CEF-MIB Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipswitch/configuration/guide/cef_snmp_mib.html
- Cisco TrustSec NDAC, Network Device Admission Control—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html

- Cisco TrustSec Security Association Protocol, SAP, for MACSec Encryption—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html
- CISCO-IP-URPF-MIB Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_urpf_mib.html
- CNS Config Retrieve Enhancement with Retry and Interval—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html
- Command Scheduler (Kron) Policy for System Startup—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html
- Commands for SNMP Diagnostics—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/configuration/12-2sy/nm-snmp-cfg-snmp-support.html
- Configuring ITU-T Y.1731 Fault Management Functions—See this publication:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm_y1731.html
- CoPP for multicast on Catalyst 6500—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/control_plane_policing_copp.html#CoPP_for_multicast
- CPU Friendly Netflow export—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/12-2sy/config-cpu-fne.html
- DAI (Dynamic ARP Inspection)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/dynamic_arp_inspection.html#Configuring_DAI_Hardware_Acceleration
- Digitally Signed Cisco Software—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sys-image-mgmt/configuration/12-2sy/sysimgmgmt-12-2sy-book.html
- Distributed Aggregate Policer—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/qos_class_mark_police.html#Distributed_Aggregate_Policers
- Earl8 Online Diagnostics—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/diagnostic_tests.html
- Embedded Event Manager (EEM) 3.0—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_cli.html

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_policy_tcl.html
- Ethernet-OAM 3.0: CFM over BD, Untagged—See this publication:

  http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm.html
- EVC VLAN bundling—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ethernet_virtual_connection.html

- Flexible NetFlow—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html
- Flexible NetFlow - Ingress VRF Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon.html
- Flexible Netflow - IPv4 Multicast Statistics Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cgf-mcast.html
- Flexible NetFlow - IPv4 Unicast Flows—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon.html
- Flexible NetFlow - NetFlow v9 Export Format—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cfg_de_fnflow_exprts.html
- Flexible Netflow - NetflowV5 export protocol—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cfg_de_fnflow_exprts.html
- Flexible NetFlow - Random Sampling—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/use_fnflow_redce_cpu.html
- Flexible Netflow - Top N Talkers Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cgf-topn.html

  HA SSO and RPR support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/fast_software_upgrade.html
- Hardware Acceleration support for PIM Register packets—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ipv4_multicast.html
- Hitless ACL Update—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ios_acl_support.html#Hitless_ACL_Update
- HTTP TACAC+ Accounting support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/https/configuration/12-2sy/nm-http-web.html
- H-VPLS N-PE Redundancy for MPLS Access—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_hvpls_npe_red.html
- H-VPLS N-PE Redundancy for QinQ Access—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_hvpls_npe_red.html
- IEEE 802.1ag Compliant CFM (D8.1)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/cether/configuration/12-2sy/ce-cfm-ieee.html
- IGMP MIB Support Enhancements for SNMP—The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to neighboring multicast routers. The IGMP MIB describes objects that enable users to remotely monitor and configure IGMP using Simple Network Management Protocol (SNMP). It also allows users to remotely subscribe and unsubscribe from multicast groups. The IGMP MIB Support Enhancements for SNMP feature adds

full support of RFC 2933 (Internet Group Management Protocol MIB) in Cisco IOS software. There are no new or modified Cisco IOS commands associated with this feature. For complete details on the IGMP MIB, see this publication:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

- IGMPv3 Snooping: Full Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ipv4_igmp_snooping.html

- Interface range mac-limit configure CLI—Supports entry of the **mac-limit** command for a range of interfaces.
- IP SLAs - LSP Health Monitor with LSP Discovery—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_lsp_mon_autodisc.html

- IP SLAs Metro-Ethernet 2.0 (EVC)—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_metro_ethernet.html

- IP Source Guard—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ip_source_guard.html

- IPv6 - CNS Agents—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

- IPv6 - Config Logger—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

- IPv6 - HTTP(S)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

- IPv6 - IP SLAs (UDP Jitter, UDP Echo, ICMP Echo, TCP Connect)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_udp_echo.html

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_tcp.html

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_icmp_echo.html

  http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_udp_jitter.html

- IPv6 - Netconf—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

- IPv6 - SOAP—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

- IPv6 - TCL—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-mng-apps.html

- IPv6 ACL Scalability (Support for 4K ACL Labels)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ios_acl_support.html

- IPv6 BSR - Configure RP mapping—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html

- IPv6 Device Tracking—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- IPv6 Neighbor Discovery Inspection—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-0sy/ip6-addrg-bsc-con.html
- IPv6 PACL support—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- IPv6 Router Advertisement (RA) Guard—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security.html
- IPv6 stats and counters—With PFC4 and DFC4, the same statistics and counters are available for IPV6 and IPv4.
- Jumbo Frames—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/configuring_interfaces.html#Configuring_Jumbo_Frame_Support
- L2 over mGRE—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/L2omGRE.html
- Layer3 ACL Dry Run—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ios_acl_support.html#Dry_Run_Support_for_ACLs
- LLDP IPv6 address support—Release 12.2(50)SY and later releases support IPv6 Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (MED) addresses.
- MAC packet-classify extensions (input/output, per any interface)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ios_acl_support.html#Configuring_MAC_ACLs
- MLD Group Limits—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-multicast.html
- MPLS - Egress Netflow—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/get_start_cfg_fnflow.html
- MPLS Pseudowire Status Signaling—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_pw_status.html
- MPLS Traffic Engineering (TE) - Path Protection—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_te_path_prot.html
- MQC Queuing Policy Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/qos_policy_based_queueing.html
- Multicast Bidirectional PIM support for 8 Rendezvous Points (RP) in Hardware—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/introduction.html#Multicast_Bidirectional_PIM_support_for_8_Rendezvous_Points_(RP)_in_Hardware

- Multicast Routing Hardware Enhancements for Supervisor 2T—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ipv4_multicast.html

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ipv6_multicast.html
- MVPN Scalability Improvements—This feature provides a combination of infrastructure enhancements to improve the scalability of the MVPN feature set.
- NetFlow to Flexible NetFlow Configuration Conversion—See this publication:

  http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/ios_netflow_roadmap.html
- NSF / SSO - Any Transport over MPLS (AToM)—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_trnsprt_mlps_atom.html
- NSF/SSO - IPv4 Multicast—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_resil/configuration/12-2sy/imc-resil-12-2sy-book.html
- NSF/SSO - Virtual Private LAN Services—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpls_atom.html
- Onboard Failure Logging—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/onboard_failure_logging.html
- Optimized load-balancing for Port-Channels—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-o1.html#GUID-464753DB-036E-4225-9AF9-2580245E747E
- Packet Based CoPP—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/control_plane_policing_copp.html#Packet_Based_CoPP
- Packets dropped in hardware on source-miss for port-security violation—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/port_security.html#Packets_dropped_in_hardware_on_source-miss_for_port-security_violation
- PIM MIB Extension for IP Multicast—See this publication:

  http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_monitor_maint.html
- Policer Scalability—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/qos_class_mark_police.html#Understanding_Policing
- Port Channel Load Deferral—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/virtual_switching_systems.html#Configuring_Port_Load_Share_Deferral_on_the_Peer_Switch
- Port Security on Etherchannel Trunk Port—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/port_security.html#Port_Security_on_Etherchannel_Trunk_Port

- QoS L2 Missed Packets Policing—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/qos_class_mark_police.html#Understanding_Traffic_Classification
- QOS support for IGMP, MLD and PIM frames—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/qos_restrictions.html#QOS_support_for_IGMP_MLD_and_PIM_frames
- Ringar Online diagnostics—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/diagnostic_tests.html
- SSHv2 Enhancements—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_shell_v2.html
- Support for Other ACL per Policy Class—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/ios_acl_support.html
- TrustSec Confidentiality & Integrity with MACsec (IEEE 802.1AE)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html
- TrustSec Egress Reflector—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/sxp_config.html

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html
- TrustSec Identity Port Mapping—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html
- TrustSec Ingress Reflector—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/sxp_config.html

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html
- TrustSec L3TF Static Provisioning—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/sxp_config.html
- TrustSec Netflow IPv4 SGACL Deny and Drop Export—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon.html
- TrustSec Netflow IPv6 SGACL Deny and Drop Export—See this publication:

  http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon.html
- TrustSec SGACL L2 Bridged Forwarding—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html
- TrustSec SGACL L2 Enforcement - IPv4—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html

- TrustSec SGACL L2 Enforcement - IPv6—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/arch_over.html
- TrustSec SGT Handling: L2 SGT imposition and forwarding—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_cts/configuration/15-1s/cts-sgt-handling-imp-fwd.html
- TrustSec VRF Aware—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/sxp_config.html
- Unicast Reverse Path Forwarding for IPv6—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/denial_of_service.html#Unicast_Reverse_Path_Forwarding_for_IPv6

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-0sy/ip6-addrg-bsc-con.html
- uRPF 16 path support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/denial_of_service.html#uRPF_16_path_support

  Virtual Private LAN Services (VPLS)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/vpls.html
- VPLS MAC Address Withdrawal—See this publication:

  http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_hvpls_npe_red.html
- VPLS QoS Support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/vpls.html#VPLS_QoS_Support
- VRF aware NTP—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html
- VRF support for TFTP server, TFTP Client, and FTP client—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fundamentals_Command_Reference.html
- VSS (Virtual Switching System)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/virtual_switching_systems.html
- WCCP Version 2—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-2sy/iap-wccp.html

  WCCP: VRF Support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-2sy/iap-wccp.html
- Web Services Management Agent (WSMA)—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_wsma.html

  Web Services Management Agent with TLS—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cfg_wsma.html

- XML-PI—See this publication:

  http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_xmlpi_v1.html

Software Features from Earlier Releases

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

Unsupported Commands

Release 12.2(50)SY does not support **mls** commands or **mls** as a keyword. See this document for a list of some of the **mls** commands that have been replaced:

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

Note Some of the replacement commands implemented in Release 12.2(50)SY support different keyword and parameter values than those supported by the Release 12.2SX commands.

Release 12.2(50)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 12.2(50)SY:

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

  Note Release 12.2(50)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 12.2(50)SY supports the SPAN and VACL redirect features, which have equivalent functionality.

- Inter-Switch Link (ISL) trunking

  Note Release 12.2(50)SY supports IEEE 802.1Q trunking.

- NAC - L2 IP NAC LAN Port IP
- NetWare Link-Services Protocol (NLSP)
- 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
- Network Based Application Recognition (NBAR)
- Per-VLAN Spanning Tree (PVST) mode (**spanning-tree mode pvst** global configuration mode command)

  Note Release 12.2(50)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 12.2(50)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
CSCtr15373	cat6000-acl	Standby crashes when copy config from tftp to running-config
CSCub95435	cat6000-env	Sup2T can't deliver 100% throughput on certain 67xx/68xx line cards
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
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
CSCth50799	pim	Multicast traffic slow convergence with 20k-30k mroute entries

Open Caveats in Release 12.2(50)SY and Rebuilds

Identifier	Component	Description
CSCti84174	c3pl	VS2 - HA_BULK_SYNC_BEFORE_TIMEOUT: QOS-HA-BLK-SYNC-PROCESS VSS bootup
CSCtl56259	cat6000-acl	After null label pop,erspan pkts hit invalid adjacency
CSCtq47263	cat6000-env	traceback displayed when config power from redun to combine mode
CSCuc76227	cat6000-hw-fwding	SUP2T - packet forward to the wrong dest index
CSCtf63084	cat6000-hw-fwding	Traffic gets black-holed when VPLS PE redundancy failure occurs
CSCtq14603	cat6000-l2	On SSO, Ping to interfaces fails and punt adj prog. on VSS system
CSCtz92889	cat6000-mcast	DAD fails between IPv6 SVI interface
CSCub87573	config-sync	c4hd1: Config sync seen with "no platform multicast forwarding ip"
CSCtq46844	digi-sign-infra	sh auth running displays verifier as unknown

Caveats Resolved in Release 12.2(50)SY4

Resolved nat Caveats

- CSCtg47129—Resolved in 12.2(50)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

Identifier	Component	Description
CSCud95251	nat	static nat with vrf looses vrf name after nat translations expire

Caveats Resolved in Release 12.2(50)SY3

- CSCtn76183—Resolved in 12.2(50)SY3

  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

Other Caveats Resolved in Release 12.2(50)SY3

Identifier	Component	Description
CSCub45767	cat6000-firmware	Sup2T: Switch crash due to TestL3TcamMonitoring failure
CSCtc42278	isdn	%DATACORRUPTION-1-DATAINCONSISTENCY - ISDN incoming call
CSCtn76183	nat	SIP NAT Router crash when translating certain SIP packets

Caveats Resolved in Release 12.2(50)SY2

Resolved Infrastructure Caveats

- CSCtr91106—Resolved in 12.2(50)SY2

  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

- CSCtr28857—Resolved in 12.2(50)SY2

  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 Cisco IOS Caveats

- CSCts38429—Resolved in 12.2(50)SY2

  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 Caveats Resolved in Release 12.2(50)SY2

Identifier	Component	Description
CSCsd46369	aaa	IP source address on packets to TACACS server is wrong
CSCtj88224	bgp	Effect of CSCsu96698's improvement "no bgp aggregate-timer" at SRD4
CSCtw81998	bgp	BGP Global to VRF Route Leaking fails if global route is rib-failure
CSCtj46927	cat6000-dot1x	MF:Access Vlan is removed when 802.1x is enabled on port
CSCty80605	cat6000-env	nvram erase cli support needs to be implemented for peer switch LCs
CSCtz39608	cat6000-env	nvram erase cli for peer sw LCs is proceeding without user confirmation
CSCtx77503	cat6000-hw-fwding	mls config commands crash Sup2T
CSCsz72735	cat6000-l2	VSS STP state change over port channel
CSCtr36608	cat6000-l2-infra	Large TB cm_replace_req_hdlr on all DFC & RP consoles after SSO SW.
CSCtz42106	cat6000-mcast	DAD fails between IPv6 SVI interface
CSCtz87081	cat6000-mcast	Back off changes of CSCtz42106 (DAD fails between IPv6 SVI interface)
CSCto99774	cat6000-snmp	Crash in vtp mib
CSCtt46653	cts	Crash@cts_aaa_strndup when SGACL Policy is PUSHED to MA1.bubb device.
CSCtq68778	os	After ISSU complete, the reload reason line in "sh version" is missing
CSCtx68100	os	Reload reason not displayed correctly on some platforms
CSCto46716	ospf	TE tunnel is not added into RIB even its found in forwarding-ad and OSPF
CSCtn65060	snmp	Crash when applying "snmp-server community A ro ipv6 IPv6_ACL IPv4_ACL"

Caveats Resolved in Release 12.2(50)SY1

Resolved bgp Caveats

- CSCsw63003—Resolved in 12.2(50)SY1

  Symptoms: Memory increase occurs in 'BGP Router' process due to BGP path attributes. Memory used by this process increases constantly and so do the BGP path attributes while the number of routes does not increase.

  Conditions: This issue occurs with continuous churn in the network such that BGP never manages to converge and when the paths churning do not reuse the existing path attributes. This cause those paths to allocate new path attributes.

  Workaround: Reload the router if low memory conditions are reached or identify the root cause of the churn and attempt to fix that.

  Further Problem Description: Cisco IOS Software contains a vulnerability that could allow an unauthenticated, remote attacker to exhaust the memory of an affected device.

  The vulnerability is due to BGP code, when processing BGP path attributes. An attacker could exploit this vulnerability by causing path instability in the BGP environment. An exploit could allow the attacker to deplete the memory of the affected device.

  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 4.3/3.6: https://intellishield.cisco.com/security/alertmanager/cvssCalculator.do?dispatch=1&version=2&vector=AV:N/AC:M/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C

  CVE ID CVE-2012-5039 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 http Caveats

- CSCtr91106—Resolved in 12.2(50)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 igmp Caveats

- CSCtr28857—Resolved in 12.2(50)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 ipsec-isakmp Caveats

- CSCts38429—Resolved in 12.2(50)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

Resolved nat Caveats

- CSCtd10712—Resolved in 12.2(50)SY1

  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

Resolved tcl-bleeding Caveats

- CSCto72927—Resolved in 12.2(50)SY1

  Symptoms: Configuring an event manager policy may cause a cisco Router to stop responding.

  Conditions: This issue is seen when a TCL policy is configured and copied to the device.

  Workaround: There is no workaround.

Resolved ts Caveats

- CSCtn43662—Resolved in 12.2(50)SY1

  Symptom: Slow processor memory leak seen in TCP Protocols

  Conditions: This is only found in 12.2(33)SXI4 and later. A block of memory will be leaked every time a user creates an exec session to the router.

  Workaround: None

  Further Problem Description: Cisco IOS Software contains a vulnerability that could allow an authenticated, remote attacker to exhaust the memory of an affected device.

  The vulnerability is due to new code introduced into the 12.2XSH and 12.2SXI trains. An attacker could exploit this vulnerability by repeatedly making a VTY management session to the device. An exploit could allow the attacker to exhaust the available memory of the device resulting in a denial of service.

  Affected Releases: 12.2(33)SXH8 12.2(33)SXH8a 12.2(33)SXH8b 12.2(33)SXI4 12.2(33)SXI4a 12.2(33)SXI5 12.2(33)SXI5a 12.2(33)SXJ 12.2(50)SY

  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-2012-5036 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 12.2(50)SY1

Identifier	Component	Description
CSCtr94733	cat6000-acl	ping to the ipv6 host fails with ipv6 pacl config applied
CSCtt35036	cat6000-acl	Sup2T VSS: RACL Reduced and earl8 hw adj fail errors on SSO
CSCtr84253	cat6000-diag	cat6k rapidly exhausts system buffers
CSCtr10155	cat6000-env	Crash following defaulting an interface configuration in a port-channel
CSCts17084	cat6000-env	Incorrect card type information displayed for ws-x6908-10G
CSCtu50683	cat6000-env	Resetting PS on Standby VSS, reduces power from PS on Active VSS member.

Identifier	Component	Description
CSCtt37174	cat6000-qos	Sup-2T VSS: On reload, stdby continuously reloaded - XDR RRP RF timeout
CSCtt39344	cat6000-routing	Sup-2T VSS: PBR first adjacency wrongly programmed on SSO
CSCtt17210	cat6000-snmp	On setting crcSrcERSpanLoVlanMask to zero, device goes for a reset.
CSCts70696	ether-infra	TBs and crash on ip basek9 fc3 image
CSCtg44661	ip-pbr	ASR router crashes when unconfiguring route-map
CSCth74953	ipsec-core	SPI Value shown incorrectly as zero for ipsec sa with crypto profiles
CSCsh39289	pim	Crash in pim_sm_assert_rpf_nbr during the stress test
CSCee55603	snmp	SNMP ACL does not work for VRF interfaces
CSCtg48785	x25	sh x25 hunt-group %DATACORRUPTION-1-DATAINCONSISTENCY: copy err

Caveats Resolved in Release 12.2(50)SY

Resolved aaa Caveats

- CSCsh46990—Resolved in 12.2(50)SY

  Symptom: Memory leak in AAA attributes and router crashed.

  Condition: The root cause for this leak is due to the fall back method ‘enable’ configured in the EOU method list:

  ```
  aaa authentication eou default group radius enable
  ```

  Work around: Do not use **enable** or **line** as AAA fall back methods in the corresponding method lists.

- CSCsj91123—Resolved in 12.2(50)SY

  Symptoms: Router reloads after authentication attempt fails on console.

  Conditions: Occurs while performing AAA accounting. The accounting structure was freed twice, which results in crash. Occurs when the **aaa accounting send stop-record authentication failure** command is configured, which sends a stop record for authentication failure.

  Workaround: Remove the **aaa accounting send stop-record authentication failure** command.

- CSCsv06973—Resolved in 12.2(50)SY

  Symptom: Router crashes For Authentication RESPONSE with GETUSER and when getuser-header-flags is modified and sent.

  Conditions: TACACS single-connection is configured. When authorization is configured Telnet to router and removing authorization,telnet to router again.

  Workaround: Do not use TACACS single-connection option.

- CSCsv38166—Resolved in 12.2(50)SY

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device’s file system, including the device’s saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

This vulnerability does not apply to the Cisco IOS SCP client feature.

Cisco has released free software updates that address this vulnerability.

There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

This advisory is posted at the following link:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-scp.

- CSCef52919—Resolved in 12.2(50)SY

  Symptoms: A privilege level 1 user is able to log in with a higher privilege level.

  Conditions: This symptom is observed on a Cisco platform when the **aaa new-model** command is enabled, when the **privilege level** *level* command is present under the vty lines, and when the *level* argument has any value from 2 through 15.

  Workaround: Do not configure privilege level 1 but configure any other privilege level.

- CSCsv73509—Resolved in 12.2(50)SY

  Symptoms: When **no aaa new-model** is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

  Conditions: Configure **no aaa new-model**, configure **login local** under **line vty 0 4** and configure **login tacacs** under **line vty 0 4**.

  Workaround: There is no workaround.

- CSCsa43465—Resolved in 12.2(50)SY

  Symptoms: Users may be able to access root view mode (privilege level) 15 without entering a password.

  Conditions: This symptom is observed on a Cisco router that has the Role-Based CLI Access feature enabled and occurs when the **none** keyword is enabled in the default login method list.

  For example, the symptom may occur when you enter the **aaa authentication login default group tacacs+ none**. When the TACACS+ server is down, users are allowed to enter non-privileged mode. However, users can also access the root view through the **enable view** command without having to enter a password.

  Workaround: Ensure that the **none** keyword is not part of the default login method list.

  Further Problem Description: The fix for this caveat places the authentication of the **enable view** command in the default login method list.

- CSCsg88561—Resolved in 12.2(50)SY

  Symptom: When accessing VTY lines configured for TACACS AAA authentication, the remote access session will not get access to the device.

  Conditions: If using TACACS for VTY user authentication the remote access session will stop being processed after the username and password have been entered. Operation of the device continues as per normal, just the remote VTY session can not be used.

  Limited to C7600 ONLY.

  Workaround: Local Authentication or RADIUS could be used as a workaround.

Resolved bfd Caveats

- CSCsy68923—Resolved in 12.2(50)SY

  Symptom: Cisco IOS device may reload in very rare circumstances after receiving certain packets. The BFD process may restart due to a critical software exception.

  Workarounds: None

Resolved bgp Caveats

- CSCec12299—Resolved in 12.2(50)SY

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

  Workarounds are available to help mitigate this vulnerability.

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

  This issue cannot be deterministically exploited by an attacker.

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

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-vpn

- CSCsx10140—Resolved in 12.2(50)SY

  Recent research (1) has shown that it is possible to cause BGP sessions to remotely reset by injecting invalid data, specifically AS_CONFED_SEQUENCE data, into the AS4_PATH attribute provided to store 4-byte ASN paths. Since AS4_PATH is an optional transitive attribute, the invalid data will be transited through many intermediate ASes which will not examine the content. For this bug to be triggered, an operator does not have to be actively using 4-byte AS support.

  The root cause of this problem is the Cisco implementation of RFC 4893 (4-byte ASN support) - this RFC states that AS_CONFED_SEQUENCE data in the AS4_PATH attribute is invalid. However, it does not explicitely state what to do if such invalid data is received, so the Cisco implemention of this RFC sends a BGP NOTIFICATION message to the peer and the BGP session is terminated.

  RFC 4893 is in the process of getting updated to avoid this problem, and the fix for this bug implements the proposed change. The proposed change is as follows:

  “To prevent the possible propagation of confederation path segments outside of a confederation, the path segment types AS_CONFED_SEQUENCE and AS_CONFED_SET [RFC5065] are declared invalid for the AS4_PATH attribute. A NEW BGP speaker MUST NOT send these path segment types in the AS4_PATH attribute of an UPDATE message. A NEW BGP speaker that receives these path segment types in the AS4_PATH attribute of an UPDATE message MUST discard these path segments, adjust the relevant attribute fields accordingly, and continue processing the UPDATE message.”

  The only affected version of Cisco IOS that supports RFC 4893 is 12.0(32)S12, released in December 2008.

  (1) For more information please visit:

  http://www.merit.edu/mail.archives/nanog/msg14345.html

- CSCsx73770—Resolved in 12.2(50)SY

  Symptom: A Cisco IOS device that receives a BGP update message and as a result of AS prepending needs to send an update downstream that would have over 255 AS hops will send an invalid formatted update. This update when received by a downstream BGP speaker triggers a NOTIFICATION back to the sender which results in the BGP session being reset.

  Conditions: This problem is seen when a Cisco IOS device receives a BGP update and due to a combination of either inbound, outbound, or both AS prepending it needs to send an update downstream that has more than 255 AS hops.

  Workaround: The workaround is to implement **bgp maxas-limit X** on the device that after prepending would need to send an update with over 255 AS hops. Since IOS limits the route-map prepending value to 10 the most that could be added is 21 AS hops (10 on ingress, 10 on egress, and 1 for normal eBGP AS hop addition). Therefore, a conservative value to configure would be 200 to prevent this condition.

- CSCsy86021—Resolved in 12.2(50)SY

  Recent versions of Cisco IOS Software support RFC4893 (“BGP Support for Four-octet AS Number Space”) and contain two remote denial of service (DoS) vulnerabilities when handling specific Border Gateway Protocol (BGP) updates.

  These vulnerabilities affect only devices running Cisco IOS Software with support for four-octet AS number space (here after referred to as 4-byte AS number) and BGP routing configured.

  The first vulnerability could cause an affected device to reload when processing a BGP update that contains autonomous system (AS) path segments made up of more than one thousand autonomous systems.

  The second vulnerability could cause an affected device to reload when the affected device processes a malformed BGP update that has been crafted to trigger the issue.

  Cisco has released free software updates to address these vulnerabilities.

  No workarounds are available for the first vulnerability.

  A workaround is available for the second vulnerability.

  This advisory is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090729-bgp

Resolved c7600-acl Caveats

- CSCsg53589—Resolved in 12.2(50)SY

  Symptom: On c7600 router with DHCP Relay agent configured on unnumbered Vlan interface, DHCP packets (DHCP ACK / DHCP OFFER), comming from the DHCP server, can be padded with random bits of data and packet lenght field is not updated.ng too.

  Conditions: DHCP Relay is configured on Vlan interface with “ip helper address”

  Workaround: Disable DHCP Snooping

Resolved c7600-portsecur Caveats

- CSCsl58384—Resolved in 12.2(50)SY

  Symptom: When a switchport is configured for port-security feature and line rate traffic of a highly scaled mac-addresses is sent (more than 4k). The the router crashes due to all layer2 traffic getting punted to SP (switch processor).

  Conditions: port-security feature is enabled.

Workaround: user must rate-limit the Layer 2 data using following command mls rate-limit layer2 port-security 5000

Further Problem Description:

Resolved c7600-sip-600 Caveats

- CSCsh73972—Resolved in 12.2(50)SY

  Symptom: Unicast traffic originating from a SPA card may not be encrypted

  Condition: Traffic originates from a SPA card in a SIP-600. Outbound traffic is configured for GRE with tunnel protection.

  Workaround: None

Resolved cat6000-l2-infra Caveats

- CSCsi86396—Resolved in 12.2(50)SY

  Symptoms: Two subinterfaces may have the same CEF interface index.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when the following configuration sequence occurs:

  1) Create subinterface 1, 2, and 3.

  2) Delete subinterface 1.

  3) Create subinterface 4.

  4) Enable subinterface 1.

  In this situation, subinterface 1 and 4 may have the same CEF IDB.

  Workaround: There is no workaround. You must reload the platform to clear the symptoms.

Resolved cat6000-mcast Caveats

- CSCsi99869—Resolved in 12.2(50)SY

  Symptom: Bus error crash (signal 10) seen after the following error message:

  ```
  %MCAST-SP-6-GC_LIMIT_EXCEEDED: MLD snooping was trying to allocate more Layer 2
  entries than what allowed (7744)
  ```

  Conditions: This has been observed on a Catalyst6500 running IOS version 12.2(18)SXF1.

  Workaround: A workaround exist to disable ipv6 mld snooping via the command **no ipv6 mld snooping**.

  There is no negative impact of implementing the workaround as long as there is no IPV6 multicast traffic in the network.

- CSCsj16969—Resolved in 12.2(50)SY

  Symptom: A Cisco IOS device supporting IPv6 MLD may crash with a data bus error exception and stack trace PC = 0xA0000100

  Conditions: Device is running normal production traffic. Presence of malformed MLD packet in this network caused the issue.

  Workaround: Disabling MLD snooping on the VLAN or globally on the box will stop the crash.

Resolved cat6000-mpls Caveats

- CSCsf12082—Resolved in 12.2(50)SY

  Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

  OSPF and MPLS VPNs are not enabled by default.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-queue

Resolved cat6000-snmp Caveats

- CSCsd75273—Resolved in 12.2(50)SY

  Cisco Catalyst 6500, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070228-nam

- CSCse52951—Resolved in 12.2(50)SY

  Cisco Catalyst 6500, 6500 series and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM on them are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070228-nam

Resolved cat6000-sw-fwding Caveats

- CSCek49649—Resolved in 12.2(50)SY

  Symptoms: Cisco Catalyst 6500 and Cisco 7600 modules are reachable via 127.0.0.x addresses.

  Conditions: Cisco Catalyst 6500 and Cisco 7600 series devices use addresses from the 127.0.0.0/8 (loopback) range in the Ethernet Out-of-Band Channel (EOBC) for internal communication.

  Addresses from this range that are used in the EOBC on Cisco Catalyst 6500 and Cisco 7600 series devices are accessible from outside of the system. The Supervisor module, Multilayer Switch Feature Card (MSFC), or any other intelligent module may receive and process packets that are destined for the 127.0.0.0/8 network. An attacker can exploit this behavior to bypass existing access control lists; however, an exploit will not allow an attacker to bypass authentication or authorization. Valid authentication credentials are still required to access the module in question.

Per RFC 3330, a packet that is sent to an address anywhere within the 127.0.0.0/8 address range should loop back inside the host and should never reach the physical network. However, some host implementations send packets to addresses in the 127.0.0.0/8 range outside their Network Interface Card (NIC) and to the network. Certain implementations that normally do not send packets to addresses in the 127.0.0.0/8 range may also be configured to do so..

Destination addresses in the 127.0.0.0/8 range are not routed on the Internet. This factor limits the exposure of this issue.

This issue is applicable to systems that run Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the MSFC) and Native Mode (IOS Software on both the Supervisor Engine and the MSFC).

Workaround: Administrators can apply an access control list that filters packets to the 127.0.0.0/8 address range to interfaces where attacks may be launched.

```
ip access-list extended block_loopback
  deny   ip any 127.0.0.0 0.255.255.255
  permit ip any any

interface Vlan x
 ip access-group block_loopback in
```

Control Plane Policing (CoPP) can be used to block traffic with a destination IP address in the 127.0.0.0/8 address range sent 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 may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks. CoPP protects the management and control planes by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

```
!-- Permit all traffic with a destination IP
!-- addresses in the 127.0.0.0/8 address range sent to
!-- the affected device so that it will be policed and
!-- dropped by the CoPP feature
!
access-list 111 permit icmp any 127.0.0.0 0.255.255.255
access-list 111 permit udp any 127.0.0.0 0.255.255.255
access-list 111 permit tcp any 127.0.0.0 0.255.255.255
access-list 111 permit ip any 127.0.0.0 0.255.255.255
!
!-- 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-127/8-netblock-class
  match access-group 111
!
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
!
policy-map drop-127/8-netblock-traffic
  class drop-127/8-netblock-class
    police 32000 1500 1500 conform-action drop exceed-action drop
!
!-- Apply the Policy-Map to the Control-Plane of the
!-- device
!
```

```
control-plane
  service-policy input drop-127/8-netblock-traffic
!
```

Additional information on the configuration and use of the CoPP feature is available at the following links:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

Infrastructure Access Control Lists (iACLs) are also considered a network security best practice and should be considered as, long-term additions to effective network security as well as a workaround for this specific issue. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs. The white paper is available at the following link:

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

Resolved cdp Caveats

- CSCsf07847—Resolved in 12.2(50)SY

  Symptoms: Specifically crafted CDP packets can cause a router to allocate and keep extra memory. Exploitation of this behaviour by sending multiple specifically crafted CDP packets could cause memory allocation problems on the router.

  Conditions: This issue occurs in IOS images that has the fix for CSCse85200.

  Workaround: Disable CDP on interfaces where CDP is not required.

  Further Problem Description: Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

Resolved dhcp Caveats

- CSCsm45390—Resolved in 12.2(50)SY

  Symptom: An IOS software crash may occur when receiving a specific malformed DHCP packet.

  Conditions: An IOS device configured for DHCP Server and receives a DHCP-request from a DHCP relay device. A specific malformed option in the packet packet may induce a software traceback or crash. The specific packet will not occur without manual modification.

  Workaround: None.

- CSCek52673—Resolved in 12.2(50)SY

  A router that has DHCP server enabled could reload after receiving a malformed UDP packet.

  Workaround: None

Resolved dlsw Caveats

- CSCsf28840—Resolved in 12.2(50)SY

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070110-dlsw

- CSCsk73104—Resolved in 12.2(50)SY

  Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

  Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-dlsw

Resolved eigrp Caveats

- CSCsm93548—Resolved in 12.2(50)SY

  Symptom: Cisco IOS router may crash after receiving malformed EIGRP packets.

  Workaround: Only allow EIGRP packet from trusted neighbours.

- CSCso64422—Resolved in 12.2(50)SY

  Symptom: Processing of certain external routes with eigrp is not correct. The external information, i.e. originating router id, originating protocol ect is 0

  Workaround: No workaround.

Resolved fib Caveats

- CSCsk31502—Resolved in 12.2(50)SY

  Symptom: Router running IPv6 in IP tunnelling may reload upon receiving a malformed packet.

  Conditions: Router needs to be configured for IPv6 in IP tunneling.

  Workaround:

Resolved http Caveats

- CSCsc64976—Resolved in 12.2(50)SY

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

  Cisco will be making free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20051201-http

- CSCse85652—Resolved in 12.2(50)SY

  Symptom: The Cisco IOS HTTP server and the Cisco IOS HTTPS server provide web server functionality to be used by other Cisco IOS features that require it to function. For example, embedded device managers available for some Cisco IOS devices need the Cisco IOS HTTP server or the Cisco IOS HTTPS server to be enabled as a prerequisite.

  One of the functionalities provided by the Cisco IOS HTTP server and the Cisco IOS HTTPS server is the WEB_EXEC module, which is the HTTP-based IOS EXEC Server. The WEB_EXEC module allows for both “show” and “configure” commands to be executed on the device through requests sent over the HTTP protocol.

Both the Cisco IOS HTTP server and the Cisco IOS HTTPS server use the locally configured enable password (configured by using the **enable password** or **enable secret** commands) as the default authentication mechanism for any request received. Other mechanisms can also be configured to authenticate requests to the HTTP or HTTPS interface. Some of those mechanisms are the local user database, an external RADIUS server or an external TACACS+ server.

If an enable password is not present in the device configuration, and no other mechanism has been configured to authenticate requests to the HTTP interface, the Cisco IOS HTTP server and the Cisco IOS HTTPS server may execute any command received without requiring authentication. Any commands up to and including commands that require privilege level 15 might then be executed on the device. Privilege level 15 is the highest privilege level on Cisco IOS devices.

Conditions: For a Cisco IOS device to be affected by this issue all of the following conditions must be met:

- An enable password is not present in the device configuration
- Either the Cisco IOS HTTP server or the Cisco IOS HTTPS server is enabled
- No other authentication mechanism has been configured for access to the Cisco IOS HTTP server or Cisco IOS HTTPS server. Such mechanisms might include the local user database, RADIUS (Remote Authentication Dial In User Service), or TACACS+ (Terminal Access Controller Access-Control System)

The Cisco IOS HTTP server is enabled by default on some Cisco IOS releases.

Workaround: Any of the following workarounds can be implementd:

- Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an enable password

Customers requiring the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server must configure an authentication mechanism for any requests received. One option is to use the **enable password** or **enable secret** commands to configure an enable password. The enable password is the default authentication mechanism used by both the Cisco IOS HTTP server and the Cisco IOS HTTPS server if no other method has been configured.

In order to configure an enable password by using the **enable secret** command, add the following line to the device configuration:

enable secret *mypassword*

Replace *mypassword* with a strong password of your choosing. For guidance on selecting strong passwords, please refer to your site security policy. The document entitled “Cisco IOS Password Encryption Facts” explains the differences between using the **enable secret** and the **enable password** commands to configure an enable password. This document is available at the following link: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00809d38a7.shtml

- Enabling authentication of requests to the Cisco IOS HTTP Server or the Cisco IOS HTTPS server by configuring an authentication mechanism other than the default

Configure an authentication mechanism for access to the Cisco IOS HTTP server or the Cisco IOS HTTPS server other than the default. Such authentication mechanism can be the local user database, an external RADIUS server, an external TACACS+ server or a previously defined AAA (Authentication, Authorization and Accounting) method. As the procedure to enable an authentication mechanism for the Cisco IOS HTTP server and the Cisco IOS HTTPS server varies across Cisco IOS releases and considering other additional factors, no example will be provided. Customers looking for information about how to configure an authentication mechanism for the Cisco IOS HTTP server and for the Cisco IOS HTTPS server are encouraged to read the document entitled “AAA Control of the IOS HTTP Server”, which is available at the following link: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a008069bdc5.shtml

– Disabling the Cisco IOS HTTP Server and/or the Cisco IOS HTTPS server functionality

Customers who do not require the functionality provided by the Cisco IOS HTTP server or the Cisco IOS HTTPS server can disable it by adding the following commands to the device configuration:

no ip http server no ip http secure-server

The second command might return an error message if the Cisco IOS version installed and running on the device does not support the HTTPS server feature. This error message is harmless and can safely be ignored.

Please be aware that disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server may impact other features that rely on it. As an example, disabling the Cisco IOS HTTP server or the Cisco IOS HTTPS server will disable access to any embedded device manager installed on the device.

Further Problem Description: In addition to the explicit workarounds detailed above it is highly recommended that customers limit access to Cisco IOS HTTP server and the Cisco IOS HTTPS server to only trusted management hosts. Information on how to restrict access to the Cisco IOS HTTP server and the Cisco IOS HTTPS server based on IP addresses is available at the following link:
http://www.cisco.com/en/US/docs/ios-xml/ios/https/configuration/12-4/nm-http-web.html#GUID-BB57C0D5-71DB-47C5-9C11-8146773D1127

Customers are also advised to review the "Management Plane" section of the document entitled "Cisco Guide to Harden Cisco IOS Devices" for additional recommendations to secure management connections to Cisco IOS devices. This document is available at the following link:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

- CSCsi13344—Resolved in 12.2(50)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.

- CSCsr72301—Resolved in 12.2(50)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.

- CSCsx49573—Resolved in 12.2(50)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.

Resolved ifs Caveats

- CSCsk61790—Resolved in 12.2(50)SY

  Symptoms: Syslog displays password when copying the configuration via FTP.

  Conditions: This symptom occurs when copying via FTP. The Syslog message displays the password given by the user as part of syntax of FTP copy.

  Workaround: There is no workaround.

Resolved ios-authproxy Caveats

- CSCsa54608—Resolved in 12.2(50)SY

  The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

  Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

  Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

  Only devices running certain versions of Cisco IOS are affected.

  Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory will be posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050907-auth_proxy

- CSCsy15227—Resolved in 12.2(50)SY

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090923-auth-proxy

Resolved ios-firewall-aic Caveats

- CSCsg70474—Resolved in 12.2(50)SY

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

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

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

This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice.

Resolved ip-acl Caveats

- CSCsd64967—Resolved in 12.2(50)SY

  Symptom: If an ACL is edited using sequence numbers in RPR or SSO mode, any subsequent supervisor switchover or reset of the standby can cause configuration errors on the standby. As a result, if the standby ever becomes active, the running security ACL configuration may not be correct.

  Conditions: An ACL must be configured on the primary RPR, then a switchover must be made to the secondary RPR.

  Workaround: Check config after every RPR switchover to ensure corruption did not occur - reconfigure if needed.

  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 4.3/3.6:

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

  CVE ID CVE-2011-0955 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 ipmulticast Caveats

- CSCsl32142—Resolved in 12.2(50)SY

  Symptoms: A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with 'Bad getbuffer' error may also be reported.

  Condition: Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

  Workaround: Configure IP multicast boundary without the **filter-autorp** option.

- CSCso90058—Resolved in 12.2(50)SY

  Symptoms: MSFC crashes with Red Zone memory corruption.

  Conditions: This problem is seen when processing an Auto-RP packet and NAT is enabled.

  Workaround: There is no workaround.

- CSCse15770—Resolved in 12.2(50)SY

  Symptom: IOS device may reload unexpectedly

  Conditions: The Multicast Routing Monitor (MRM) feature must be enabled and corrupted traffic is received by the MRM responder.

  Workarounds: Disable the MRM feature,

Resolved ipsec-isakmp Caveats

- CSCsb29028—Resolved in 12.2(50)SY

  Symptom: Used Processor Memory increasing day by day

Conditions: IPSec connection is configured, device using VPN Service Module.

Workaround: Only reload the router.

- CSCsc06695—Resolved in 12.2(50)SY

  Symptom: When a Phase 1 SA (MM or AM) is being setup and the client does quick retransmissions within a window of one second, the server stops the restransmission timer for the SA. If the client stops retransmissions or further message afterwards, SA on server side is leaked forever (until the lifetime timer expires).

  Workaround: Clear isakmp sa manually.

- CSCsd68605—Resolved in 12.2(50)SY

  Symptoms: If a spoke cannot complete IKE phase I because of a bad certificate, the failed IKE sessions may not be deleted on an IPSec/IKE responder. Such failed sessions may accumulate, eventually causing router instability. These failed sessions can be seen in the output of the **show crypto isakmp sa | i MM** command:

```
172.18.95.21    10.253.34.80   MM_KEY_EXCH        898    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        896    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        895    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        894    0 ACTIVE
172.18.95.21    10.253.34.80   MM_KEY_EXCH        893    0 ACTIVE
...
```

  Conditions: These symptoms are observed when RSA signatures are used as the authentication method.

- CSCsu57182—Resolved in 12.2(50)SY

  Symptoms: The Cisco IOS may experience high CPU utilization.

  Conditions: ISAKMP is enabled.

  Workaround: None.

  Further Information: This issue can occur if the Cisco IOS device processes a malformed IKE message.

- CSCsy07555—Resolved in 12.2(50)SY

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

  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-20090923-ipsec

- CSCsg35077—Resolved in 12.2(50)SY

  Symptoms: A device that is running Cisco IOS software may crash during processing of an Internet Key Exchange (IKE) message.

  Conditions: The device must have a valid and complete configuration for IPsec. IPsec VPN features in Cisco IOS software that use IKE include Site-to- Site VPN tunnels, EzVPN (server and remote), DMVPN, IPsec over GRE, and GET VPN.

  Workaround: Customers that do not require IPsec functionality on their devices can use the **no crypto isakmp enable** command in global configuration mode to disable the processing of IKE messages and eliminate device exposure.

If IPsec is configured, this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.

Further Problem Description: This bug is triggered deep into the IKE negotiation, and an exchange of messages between IKE peers is necessary.

If IPsec is not configured, it is not possible to reach the point in the IKE negotiation where the bug exists.

Resolved ip-tunnels Caveats

- CSCeb47225—Resolved in 12.2(50)SY

  If a key is configured on a tunnel interface, the inbound access-list on that interface is ignored.

  This problem is seen with a configuration that is similar to the following

```
interface Tunnel0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 100 in
 tunnel source FastEthernet0/0
 tunnel destination 172.16.1.1
 tunnel key 1
end
```

  Problem does not occur if “tunnel key” is not configured.

  Workaround is to remove the “tunnel key”.

- CSCsx70889—Resolved in 12.2(50)SY

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

  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-20090923-tunnels

Resolved ipv6 Caveats

- CSCsd40334—Resolved in 12.2(50)SY

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-IOS-IPv6

- CSCti33534—Resolved in 12.2(50)SY

  Symptoms: After launching a flood of random IPv6 router advertisements when an interface is configured with “ipv6 address autoconf”, removing the IPv6 configuration on the interface with “no ipv6 address autoconf” may cause a reload. Other system instabilities are also possible during and after the flood of random IPv6 router advertisements.

Conditions: Cisco IOS is configured with “ipv6 address autoconf”.

Workarounds: Not using IPv6 auto-configuration may be used as a workaround.

Further Information: Cisco IOS checks for the hop limit field in incoming Neighbour Discovery messages and packets received with a hop limit not equal to 255 are discarded. This means that the flood of ND messages has to come from a host that is directly connected to the Cisco IOS device.

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 6.1/5.5:

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:OF/RC:C

CVE ID CVE-2010-4671 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

- CSCsd58381—Resolved in 12.2(50)SY

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070124-IOS-IPv6

Resolved mcast-vpn Caveats

- CSCsb52717—Resolved in 12.2(50)SY

  Symptom: A Cisco router configured for multicast VPN may reload after receiving a malformed MDT data group join packet.

  Conditions: Affects all IOS versions that support mVPN MDT.

  Workaround: Filter out MDT Data Join messages from the router sending the malformed packet using a Receive Access Control List (rACL) feature. Note by doing this, the offending router will not be able to participate within the mVPN data trees.

  The following example shows how to block malformed MDT Data Join messages that are sent from the device's IP addresses using a receive ACL:

  ```
  !
  ip receive access-list 111
  !
  access-list 111 deny udp host <ip address of router sending malformed join
  request> host 224.0.0.13 eq 3232
  access-list 111 permit ip any any
  !
  ```

  Note: Ensure that the rACL does not filter critical traffic such as routing protocols or interactive access to the routers. Filtering necessary traffic could result in an inability to remotely access the router, thus requiring a console connection. For this reason, lab configurations should mimic the actual deployment as closely as possible.

  As always, Cisco recommends that you test this feature in the lab prior to deployment. For more information on rACLs, refer to "Protecting Your Core: Infrastructure Protection Access Control Lists" at

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a0a5e.shtml.

- CSCsi01470—Resolved in 12.2(50)SY

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

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

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20080326-mvpn.html.

Resolved mpls-mfi Caveats

- CSCsk93241—Resolved in 12.2(50)SY

  Cisco IOS Software Multi Protocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected.

  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-20080924-mfi

Resolved nat Caveats

- CSCsx32283—Resolved in 12.2(50)SY

  Symptom: Failure to NAT certain LDAP packets

  Conditions: NAT configured, NAT of LDAP at layer 4 is enabled by default.

  Workaround Disable Layer 4 NAT of LDAP packets using the no-payload keyword in the nat rule configuration, example:

  ```
  !-- NAT rule for port TCP/389 to disable IP NAT for LDAP translation
  !-- Takes precedence over the non-port translation rule.
  ```

  ip nat outside source static tcp 192.168.0.1 389 192.168.1.2 389 no-payload

  Aditional Information: None

Resolved netconf Caveats

- CSCsv86288—Resolved in 12.2(50)SY

  Symptoms: A device configured with the NETCONF feature reloads.

  Conditions: This symptom is observed when a device configured for either NETCONF over SSH or NETCONF over BEEP receives a specially crafted packet.

  Workaround: There is no workaround.

  Further Problem Description: To be exploited, the session must first be authenticated.

  For further details on NETCONF over SSH, consult the “NETCONF over SSH” configuration guide at the following link:
  http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srnetcon.html

  For further details on NETCONF over BEEP, consult the “NETCONF over BEEP” configuration guide at the following link:
  http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htnetbe.html

Resolved os Caveats

- CSCsi02752—Resolved in 12.2(50)SY

  Symptom: IOS device crash when traffic is routed under certain conditions

  Conditions: At time of publication of this release note, this vulnerability had only been observed on a Cisco 2900 switches, however this vulnerability is in common code, so this could also been seen in other platforms running Cisco IOS Software without this fix.

  Conditions required are:

  - they are enabled for routing.
  - The next hop node must be unresponsive to ARP.

  A scenario for this issue would be to have a static route pointing to a node that is not responsive, the crash will happen when multiple ARP request are sent to the non-responsive next hop

  Workaround: None.

  Further Problem Description:

  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 5.4/5.4

  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:H/RL:U/RC:C

CVE ID CVE-2011-1615 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

- CSCsk14633—Resolved in 12.2(50)SY

  This is the Cisco Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007 regarding the crash and reload of devices running Cisco IOS after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html

  The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html

  Preliminary research pointed to a previously known issue that was documented as Cisco bug ID CSCsb08386 (registered customers only) , and entitled "PRP crash by show ip bgp regexp", which was already resolved. Further research indicates that the current issue is a different but related vulnerability.

  There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

  The full text of this response is available at

  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070912-regexp

- CSCsk33054—Resolved in 12.2(50)SY

  This is the Cisco Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007 regarding the crash and reload of devices running Cisco IOS after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html

  The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html

  Preliminary research pointed to a previously known issue that was documented as Cisco bug ID CSCsb08386 (registered customers only) , and entitled "PRP crash by show ip bgp regexp", which was already resolved. Further research indicates that the current issue is a different but related vulnerability.

  There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

  The full text of this response is available at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20070912-regexp

Resolved ospf Caveats

- CSCsv30595—Resolved in 12.2(50)SY

  Symptoms: Cisco IOS device may crash.

  Conditions: A Cisco IOS device may crash upon receiving a malformed OSPF message.

Before the issue can be triggered, the Cisco IOS device must be able to establish adjacency with an OSPF peer. The issue will then occur when the processing an OSPF message sent by the peer.

Workaround: There is no workaround. Using OSPF authentication can reduce/minimize the chance of hitting this issue.

Resolved pim Caveats

- CSCsm64082—Resolved in 12.2(50)SY

  Symptom: The router may report AUTORP-4-PAK_ERR.

  Conditions: PIM Auto-RP is configured and ip multicast boundary is enabled with filter-autorp option.

  Workaround: Configure ip multicast boundary without filter-autorp option.

- CSCsu79754—Resolved in 12.2(50)SY

  Symptoms: PIM packets may be processed on interfaces which PIM is not explicitly configured.

  Conditions: Unknown at this time.

  Workarounds: Create an ACL to drop PIM packets to such interfaces.

Resolved pki Caveats

- CSCsd85587—Resolved in 12.2(50)SY

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

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

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

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM) CSCsi97695

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

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto .

  Note: Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto and

can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-SSL

Resolved sgbp Caveats

- CSCsb11124—Resolved in 12.2(50)SY

  The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

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

  Cisco has published a Security Advisory on this issue; it is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20060118-sgbp

Resolved snmp Caveats

- CSCsf04754—Resolved in 12.2(50)SY

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080610-snmpv3

- CSCso85695—Resolved in 12.2(50)SY

  Symptom: System may reload upon receiving a malformed SNMP request.

  Condition: This condition occurs if a system received a specially crafted SNMP request. In order to exploit this, an attacker needs to know a valid SNMP community string.

  Workaround: None

Resolved socket Caveats

- CSCec51750—Resolved in 12.2(50)SY

  Symptoms: A router that is configured for HTTP secure-server may reload unexpectedly because of an internal memory corruption.

  Conditions: IOS HTTP Secure server enabled

  Workaround: Disable HTTPS with “no ip http secure-server”

- CSCse56501—Resolved in 12.2(50)SY

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP)

services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

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

This advisory is posted at

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080326-IPv4IPv6

- CSCsm27071—Resolved in 12.2(50)SY

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS Software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload.

  Cisco has released free software updates that address this vulnerability.

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

  The advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-ip

Resolved ssh Caveats

- CSCsc19259—Resolved in 12.2(50)SY

  The server side of the Secure Copy (SCP) implementation in Cisco Internetwork Operating System (IOS) contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device’s filesystem, including the device’s saved configuration. This configuration file may include passwords or other sensitive information.

  The IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the IOS Secure Copy Client feature.

  This advisory is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-scp.

- CSCse24889—Resolved in 12.2(50)SY

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t
ip ssh version 1 end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that is permitted access to the router, all other
access is denied
access-list 99 permit 10.1.1.0 0.0.0.255 access-list 99 deny any
line vty 0 4 access-class 99 in end
```

Further Problem Description: For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cntrl_acc_vtl.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml

- CSCse50135—Resolved in 12.2(50)SY

  Symptom: Using scripts to access a Cisco IOS device may bypass the command authorization feature.

  Conditions: AAA is configured

  Workarounds: None

- CSCsi17158—Resolved in 12.2(50)SY

  Symptoms: Devices running Cisco IOS may reload with the error message “System returned to ROM by abort at PC 0x0” when processing SSHv2 sessions. A switch crashes. We have a script running that will continuously ssh-v2 into the 3560 then close the session normally. If the vty line that is being used by SSHv2 sessions to the device is cleared while the SSH session is being processed, the next time an ssh into the device is done, the device will crash.

  Conditions: This problem is platform independent, but it has been seen on Cisco Catalyst 3560, Cisco Catalyst 3750 and Cisco Catalyst 4948 series switches. The issue is specific to SSH version 2, and its seen only when the box is under brute force attack. This crash is not seen under normal conditions.

  Workaround: There are mitigations to this vulnerability: For Cisco IOS, the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

  Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with ‘ssh’ removed from the list of permitted transports on VTY lines while in configuration mode. For example: **line vty 0 4 transport input telnet end**

  If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely using Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html

More information on configuring ACLs can be found on the Cisco public website: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

Resolved ssl Caveats

- CSCsg40567—Resolved in 12.2(50)SY

  Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

  Conditions: This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

  Workaround: Disable the **ip http secure server** command.

- CSCsj85065—Resolved in 12.2(50)SY

  A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Cisco has released free software updates that address this vulnerability. Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20080924-ssl.

Resolved tcl-bleeding Caveats

- CSCsd28570—Resolved in 12.2(50)SY

  Symptom: A vulnerability exists within the Cisco IOS Authentication, Authorization, and Accounting (AAA) command authorization feature, where command authorization checks are not performed on commands executed from the Tool Command Language (Tcl) exec shell. This may allow authenticated users to bypass command authorization checks in some configurations resulting in unauthorized privilege escalation.

  Conditions: Devices that are not running AAA command authorization feature, or do not support Tcl functionality are not affected by this vulnerability.

  This vulnerability is present in all versions of Cisco IOS that support the **tclsh** command.

  Workaround: This advisory with appropriate workarounds is posted at http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20060125-aaatcl

  Further Problem Description: This particular vulnerability only affected Cisco IOS versions 12.3(4)T trains and onwards. (12.3 Mainline is not affected)

  Please refer to the Advisories “Software Versions and Fixes” table for the first fixed release of Cisco IOS software.

Resolved tcp Caveats

- CSCsh04686—Resolved in 12.2(50)SY

  Symptoms: With X.25 over TCP (XOT) enabled on a router or Catalyst switch, malformed traffic that is sent to TCP port 1998 causes the device to reload. This symptom was first observed in Cisco IOS Release 12.2(31)SB2.

  Conditions: This symptom is observed only when X.25 routing is enabled on the device.

  Workaround: Use IPsec or other tunneling mechanisms to protect XOT traffic. Also, apply ACLs on affected devices so that traffic is accepted only from trusted tunnel endpoints.

- CSCsi39674—Resolved in 12.2(50)SY

  Symptom: Devices may reload upon receiving multiple short lived TCP sessions to the telnet port.

  Conditions: Devices that run IOS and support IOS Software Modularity are affected. Images that support IOS Software Modularity will have "-vz" in their image name.

- CSCsv04836—Resolved in 12.2(50)SY

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

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

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090908-tcp24.

- CSCee73956—Resolved in 12.2(50)SY

  Symptoms: The Generalized TTL Security Mechanism (GTSM), formerly known as BGP TTL Security Hack (BTSH), checks the time-to-live (TTL) value of the packets at the application level, which is not efficient. Also, GTSM does not stop the establishment of a TCP connection for a packet with an invalid TTL value.

  Conditions: This symptom is observed on a Cisco platform that has the **neighbor** *neighbor-address* **security ttl hops** *hop-count* command configured in a BGP environment.

  Workaround: There is no workaround.

- CSCsr29468—Resolved in 12.2(50)SY

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-tcp

Resolved telnet Caveats

- CSCtl59814—Resolved in 12.2(50)SY

  Symptoms: Kerberos/Encrypted Telnet code needs to be improved. There is a potential buffer overflow condition in the code. There is no proof of an attack vector/exploit. However, the code needs to be improved.

  Conditions: Cisco IOS device configured for Kerberos/Encrypted Telnet access.

  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 5.4/4.1: 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:U/RL:U/RC:UC 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

Resolved trans-bridging Caveats

- CSCsw18636—Resolved in 12.2(50)SY

  Symptoms: High CPU utilization occurs after device receives a ARP packet with protocol type as 0x1000.

  Conditions: This problem occurs on Supervisor 32 running Cisco IOS Release 12.2(33)SXI. This problem may also occur on Supervisor 720. The problem is only seen when you have bridge-group CLI being used, which leads to ARP packets with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

  Workaround: Filter the ARP packet. The device configuration should have bridge-group creation first, followed by interface-specific bridge-group options.

Resolved udp Caveats

- CSCsk64158—Resolved in 12.2(50)SY

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at the following link: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20090325-udp

Resolved voice-sip Caveats

- CSCsc60249—Resolved in 12.2(50)SY

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

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

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

This advisory is posted at

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice.

- CSCeb21064—Resolved in 12.2(50)SY

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

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

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

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice.

Resolved voice-xgcp Caveats

- CSCsd81407—Resolved in 12.2(50)SY

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

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

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

  This advisory is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070808-IOS-voice.

Resolved vtp Caveats

- CSCsd34759—Resolved in 12.2(50)SY

  Symptom: The VTP feature in certain versions of Cisco IOS software may be vulnerable to a crafted packet sent from the local network segment which may lead to denial of service condition.

  Conditions: The packets must be received on a trunk enabled port.

Further Information: On the 13th September 2006, Phenoelit Group posted an advisory containing three vulnerabilities:

- VTP Version field DoS
- Integer Wrap in VTP revision
- Buffer Overflow in VTP VLAN name

These vulnerabilities are addressed by Cisco IDs:

- CSCsd52629/CSCsd34759 -- VTP version field DoS
- CSCse40078/CSCse47765 -- Integer Wrap in VTP revision
- CSCsd34855/CSCei54611 -- Buffer Overflow in VTP VLAN name

Cisco's statement and further information are available on the Cisco public website at

http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20060913-vtp

- CSCsv05934—Resolved in 12.2(50)SY

  Summary: Cisco's VTP protocol implementation in some versions of Cisco IOS and CatOS may be vulnerable to a DoS attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash (and reload/hang). The crafted packet must be received on a switch interface configured to operate as a trunk port.

  Workarounds: There are no workarounds available for this vulnerability.

  This response is posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20081105-vtp

Resolved wccp Caveats

- CSCsi46028—Resolved in 12.2(50)SY

  Symptom: On routers that are configured for WCCP, interfaces that are connected to the content engine can become locked. By locked what is meant is that the interface driver is in a state where the physical interface will stop sending and receiving packets.

  Conditions: This issue has been introduced by CSCuk61396, only the images that have the fix for CSCuk61396 are affected by this issue.

  Workaround: There are no workarounds. If an interface becomes locked, the only way to recover the system is to do a reload.

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:

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

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

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

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

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. 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* and the *Catalyst 6500 Series Cisco IOS Command Reference* publications.