Release Notes for Cisco IOS Release 12.2ZY on the Supervisor Engine 32 PISA

January 12, 2011

Note This publication applies to the CAT6000-SUP32/PISA platform.

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/12.2ZY/release/notes/ol_13011.html

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

Contents

This publication consists of these sections:

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

Chronological List of Releases

Note See the "Release Hierarchy" section on page 2 for information about parent releases.

This is a chronological list of the 12.2ZY releases:

- 12 Jan 2011—Release 12.2(18)ZYA3c
- 25 Oct 2010—Release 12.2(18)ZYA3b
- 11 May 2010—Release 12.2(18)ZYA3a
- 01 Dec 2009—Release 12.2(18)ZYA3
- 24 Jun 2009—Release 12.2(18)ZYA2
- 23 Dec 2008—Release 12.2(18)ZYA1
- 07 Aug 2008—Release 12.2(18)ZYA
- 30 Nov 2007—Release 12.2(18)ZY2
- 15 Jun 2007—Release 12.2(18)ZY1
- 04 May 2007—Release 12.2(18)ZY

Release Hierarchy

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

- Release 12.2(18)ZYA3c:
  - Date of release: 12 Jan 2011
  - Based on Release 12.2(18)ZYA3b
- Release 12.2(18)ZYA3b:
  - Date of release: 25 Oct 2010
  - Based on Release 12.2(18)ZYA3a

- Release 12.2(18)ZYA3a:
  - Date of release: 11 May 2010
  - Based on Release 12.2(18)ZYA3
- Release 12.2(18)ZYA3:
  - Date of release: 01 Dec 2009
  - Based on Release 12.2(18)ZYA2 and Release 12.2(18)SXF17
- Release 12.2(18)ZYA2:
  - Date of release: 24 Jun 2009
  - Based on Release 12.2(18)ZYA1 and Release 12.2(18)SXF16
- Release 12.2(18)ZYA1:
  - Date of release: 23 Dec 2008
  - Based on Release 12.2(18)ZYA and Release 12.2(18)SXF15
- Release 12.2(18)ZYA:
  - Date of release: 07 Aug 2008
  - Based on Release 12.2(18)ZY2 and Release 12.2(18)SXF13
- Release 12.2(18)ZY2:
  - Date of release: 30 Nov 2007
  - Based on Release 12.2(18)ZY1 and Release 12.2(18)SXF10
- Release 12.2(18)ZY1:
  - Date of release: 15 Jun 2007
  - Based on Release 12.2(18)ZY and Release 12.2(18)SXF8
- Release 12.2(18)ZY:
  - Date of release: 09 May 2007
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Based on Release 12.2(18)SXF7

This publication does not describe features that are available in Release 12.2, Release 12.2 T, Release 12.2 S, or other Release 12.2 early deployment releases.

For a list of the Release 12.2 caveats that apply to Release 12.2ZY, see the "Caveats" section on page 75 and refer to this publication:

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfmulti.html

For a list of the Release 12.2 S caveats that apply to Release 12.2ZY, see the "Caveats" section on page 75 and refer to this publication:

http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html

Supported Hardware

These sections describe the hardware supported in Release 12.2ZY:

Note

- Use the values in the “Power Required” column to determine the exact power requirements for your configuration to ensure that you are within the power budget.
- Daughtercard power is shown separately.
- Enter the **show power** command to display current system power usage.

Supervisor Engine 32 PISA (CAT6000-SUP32/PISA)

These sections describe the Supervisor Engine 32 PISA:

Supervisor Engine 32 PISA Restrictions

- Supervisor Engine 32 PISA requires a high-capacity fan tray (see the "Fan Trays" section on page 25).
- In some chassis, Supervisor Engine 32 PISA requires a high-capacity power supply (see the "Power Supplies" section on page 26).

Supervisor Engine 32 PISA Features

Product ID (append "=" for spares)	**Power Required**	**Product Description**	**Minimum Software Version**
WS-S32-GE-PISA	2.96 A@42 V	WS-S32-GE-PISA features: • Eight Gigabit Ethernet SFP ports • Requires Gigabit Ethernet SFPs	12.2(18)ZY
WS-S32-10GE-PISA	2.97 A@42 V	WS-S32-10GE-PISA features: • Two 10-Gigabit Ethernet ports • Requires XENPAKs	12.2(18)ZY1
		Supervisor Engine 32 PISA common features: • One 10/100/1000 Mbps RJ-45 port • QoS port architecture (Rx/Tx): **2q8t/1p3q8t** • 512-MB DRAM or 1-GB DRAM (cannot be upgraded in the field) • 256-MB bootdisk • Policy Feature Card 3B (PFC3B; see the "Policy Feature Cards" section on page 6) • Programmable Intelligent Services Accelerator (PISA): – 1-GB DRAM – 256-MB bootdisk	

Policy Feature Cards

Policy Feature Card Guidelines and Restrictions

- The PFC3B supports a theoretical maximum of 64 K MAC addresses (32 K MAC addresses recommended maximum).
- The PFC3B 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 routed by the PISA in software.

  The defaults 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 default partition sizes.

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

  - IPv4 and MPLS—Up to 239,000 routes
  - IPv4 multicast and IPv6 unicast and multicast—Up to 119,000 routes

  Enter the **mls 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 **mls cef maximum-routes** command into effect.
- Enter the **show platform hardware pfc mode** command to display the PFC mode.
- The Supervisor Engine 32 PISA operates in PFC3B mode.

Policy Feature Card 3B

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-PFC3B	2.25 A@42 V	Policy Feature Card 3B (PFC3B)	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Note There are no memory upgrade options for WS-F6K-PFC3B.

Transceivers

XENPAKs

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(18)ZY
XENPAK-10GB-ZR	10GBASE for any SMF type	
DWDM-XENPAK	10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid	
WDM-XENPAK-REC	10GBASE receive-only wavelength division multiplexing (WDM)	
XENPAK-10GB-CX4	10GBASE for CX4 (copper) cable	
XENPAK-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	
XENPAK-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	
XENPAK-10GB-ER+	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	
XENPAK-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	
XENPAK-10GB-LR+	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	
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, as described in this external field notice (CSCee47030), are not supported: http://www.cisco.com/en/US/ts/fn/200/fn29736.html	
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 and supports transmission at a data rate of 9.6Gbps.	

Small Form-Factor Pluggable (SFP) Modules

These sections describe SFPs:

Gigabit Ethernet SFPs

Note See the "Unsupported Hardware" section on page 30 for information about unsupported DWDM-SFPs.

Product ID (append "=" for spares)	Product Description	Minimum Software Version
DWDM-SFP-6061	1000BASE-DWDM 1560.61 nm SFP (100-GHz ITU grid) SFP module	12.2(18)ZY
DWDM-SFP-5979	1000BASE-DWDM 1559.79 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-5898	1000BASE-DWDM 1558.98 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-5655	1000BASE-DWDM 1556.55 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-5575	1000BASE-DWDM 1555.75 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-5494	1000BASE-DWDM 1554.94 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-5413	1000BASE-DWDM 1554.13 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-5092	1000BASE-DWDM 1550.92 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4851	1000BASE-DWDM 1548.51 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4772	1000BASE-DWDM 1547.72 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4612	1000BASE-DWDM 1546.12 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4453	1000BASE-DWDM 1544.53 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4294	1000BASE-DWDM 1542.94 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4056	1000BASE-DWDM 1540.56 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3819	1000BASE-DWDM 1538.19 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3661	1000BASE-DWDM 1536.61 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3425	1000BASE-DWDM 1534.25 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3268	1000BASE-DWDM 1532.68 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3190	1000BASE-DWDM 1531.90 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3112	1000BASE-DWDM 1531.12 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3033	1000BASE-DWDM 1530.33 nm SFP (100-GHz ITU grid) SFP module	
GLC-BX-D	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength	
GLC-BX-U	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength	
GLC-ZX-SM	1000BASE-ZX SFP module	
CWDM-SFP	1000BASE coarse wavelength-division multiplexing (CWDM) SFP module	
GLC-T	1000BASE-T SFP module	
GLC-LH-SM	1000BASE-LX/LH SFP	
GLC-SX-MM	1000BASE-SX SFP	

Fast Ethernet SFPs

Note Only WS-X6148-FE-SFP supports these Fast Ethernet SFPs.

Product ID (append "=" for spares)	Product Description	Minimum Software Version
GLC-FE-100BX-U	100BASE-BX10-U SFP	12.2(18)ZY
GLC-FE-100BX-D	100BASE-BX10-D SFP	
GLC-FE-100EX	100BASEEX SFP	
GLC-FE-100ZX	100BASEZX SFP	
GLC-FE-100FX	100BASEFX SFP	
GLC-FE-100LX	100BASELX SFP	

Gigabit Interface Converters (GBICs)

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

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WDM-GBIC-REC	Receive-only wavelength division multiplexing (WDM) GBIC	12.2(18)ZY
DWDM-GBIC	Dense wavelength division multiplexing (DWDM) GBIC	
CWDM-GBIC	Coarse wave division multiplexing (CWDM) GBIC	
WS-G5483	1000BASET GBIC	
WS-G5484	Short wavelength, 1000BASE-SX	
WS-G5486	Long wavelength/long haul, 1000BASE-LX/LH	
WS-G5487	Extended distance, 1000BASE-ZX	

10-Gigabit Ethernet Switching Modules

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6502-10GE	3.30 A@42 V	1-port 10-Gigabit Ethernet • QoS port architecture (Rx/Tx): **1p1q8t/1p2q1t** • Number of ports: 1 Number of port groups: 1 Port ranges per port group: 1 port in 1 group	
		With Supervisor Engine 32 PISA	12.2(18)ZY
Note WS-X6502-10GE does not support ISL encapsulation.			
Optical Interface Module (OIM) for WS-X6502-10GE			
WS-G6488		10GBASE-LR serial 1310 nm long-reach OIM	12.2(18)ZY
WS-G6483		10GBASE-ER serial 1550 nm extended-reach OIM	

Gigabit Ethernet Switching Modules

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6516A-GBIC	3.62 A@42 V	16-port Gigabit Ethernet GBIC • CEF256 • 1-MB per-port packet buffers • Supports egress multicast replication • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6516-GBIC	3.40 A@42 V	16-port Gigabit Ethernet GBIC • CEF256 • 512-KB per-port packet buffers • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6416-GBIC	2.81 A@42 V	16-port Gigabit Ethernet GBIC • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6416-GE-MT	2.50 A@42 V	16-Port Gigabit Ethernet MT-RJ • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6316-GE-TX	5.15 A@42 V	16-port Gigabit Ethernet RJ-45 • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6408A-GBIC	2.00 A@42 V	8-port Gigabit Ethernet GBIC • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Number of ports: 8 Number of port groups: 1 Port ranges per port group: 1–8	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6408-GBIC	2.00 A@42 V	8-port Gigabit Ethernet GBIC • QoS port architecture (Rx/Tx): **1q4t/2q2t** • Number of ports: 8 Number of port groups: 1 Port ranges per port group: 1–8	
		With Supervisor Engine 32 PISA	12.2(18)ZY

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)	**Power Required**	**Product Description**	**Minimum Software Version**
WS-F6K-FE48X2-AF	0.42 A@42 V	IEEE 802.3af PoE daughtercard for WS-X6148X2-RJ-45 and WS-X6196-RJ-21.	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-F6K-GE48-AF **WS-F6K-48-AF**	0.18 A@42 V	IEEE 802.3af PoE daughtercard for: • WS-X6548-GE-TX • WS-X6148-GE-TX • WS-X6148A-GE-TX • WS-X6148A-RJ-45 **Note** WS-F6K-GE48-AF and WS-F6K-48-AF are not FRUs for these switching modules: • WS-X6148-RJ-45 or WS-X6148-RJ45V (replace with WS-X6148-45AF-UG=). • WS-X6148-RJ-21 or WS-X6148-RJ-21V (replace with WS-X6148-21AF-UG=).	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-F6K-VPWR-GE	0.42 A@42 V	PoE daughtercard for WS-X6548-GE-TX and WS-X6148-GE-TX	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-F6K-VPWR	None	PoE daughtercard for: • WS-X6348-RJ-45 • WS-X6348-RJ-21V • WS-X6148-RJ-45 • WS-X6148-RJ-21	
		With Supervisor Engine 32 PISA	12.2(18)ZY

10/100/1000 Ethernet Switching Modules

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6548-GE-TX	2.98 A@42 V	48-port 10/100/1000 Mbps	
WS-X6548V-GE-TX	3.40 A@42 V	• RJ-45 • CEF256 • WS-X6548-GE-TX supports: – WS-F6K-VPWR-GE – WS-F6K-GE48-AF – WS-F6K-48-AF • WS-X6548V-GE-TX has WS-F6K-VPWR-GE • WS-X6548-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF • QoS port architecture (Rx/Tx): **1q2t/1p2q2t** • Number of ports: 48 Number of port groups: 2 Port ranges per port group: 1–24, 25–48	
WS-X6548-GE-45AF	3.16 A@42 V		
		With Supervisor Engine 32 PISA	12.2(18)ZY

Note

- WS-X6548-GE-TX and WS-X6548V-GE-TX do not support these features:
  - ISL trunking
  - Jumbo frames
  - 802.1Q tunneling
  - Traffic storm control

WS-X6148A-GE-TX	2.50 A@42 V	48-port 10/100/1000 Mbps	
WS-X6148A-GE-45AF	2.68 A@42 V	• 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 • 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.	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Note WS-X6148A-GE-TX and WS-X6148A-GE-45AF do not support traffic storm control.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6148-GE-TX	2.47 A@42 V	48-port 10/100/1000 Mbps	
WS-X6148V-GE-TX	2.89 A@42 V	• RJ-45 • WS-X6148-GE-TX supports: – WS-F6K-VPWR-GE – WS-F6K-GE48-AF – WS-F6K-48-AF • WS-X6148V-GE-TX has WS-F6K-VPWR-GE • WS-X6148-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF • QoS port architecture (Rx/Tx): **1q2t/1p2q2t** • Number of ports: 48 Number of port groups: 2 Port ranges per port group: 1–24, 25–48	
WS-X6148-GE-45AF	2.65 A@42 V		
		With Supervisor Engine 32 PISA	12.2(18)ZY

Note WS-X6148-GE-TX, WS-X6148V-GE-TX, and WS-X6148-GE-45AF do not support these features:

- More than 1 Gbps of traffic per EtherChannel
- ISL trunking
- Jumbo frames
- 802.1Q tunneling
- Traffic storm control

WS-X6516-GE-TX	3.45 A@42 V	16-port 10/100/1000BASE-T • CEF256 • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Fast Ethernet Switching Modules

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6148-FE-SFP	2.30 A@42 V	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	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6524-100FX-MM	1.90 A@42 V	24-port 100FX Ethernet multimode • CEF256 • QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t** • Number of ports: 24 Number of port groups: 1 Port ranges per port group: 1–24	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6324-100FX-SM	1.52 A@42 V	24-port 100FX Ethernet • Single mode and multimode MT-RJ • 128-KB per-port packet buffers • QoS port architecture (Rx/Tx): **1q4t/2q2t** • Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24	
WS-X6324-100FX-MM	1.52 A@42 V		
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6224-100FX-MT	1.90 A@42 V	24-port 100FX Ethernet Multimode MT-RJ • QoS port architecture (Rx/Tx): **1q4t/2q2t** • Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Ethernet/Fast Ethernet (10/100) Switching Modules

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6548-RJ-45	2.90 A@42 V	48-port 10/100TX RJ-45 • CEF256 • QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t** • Number of ports: 48 Number of port groups: 1 Port ranges per port group: 1–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6548-RJ-21	2.90 A@42 V	48-port 10/100TX RJ-21 • CEF256 • QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t** • Number of ports: 48 Number of port groups: 1 Port ranges per port group: 1–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6148X2-RJ-45	2.65 A@42 V	96-port 10/100TX RJ-45	
WS-X6148X2-45AF	2.92 A@42 V	• QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t** • WS-X6148X2-RJ-45 supports WS-F6K-FE48X2-AF • WS-X6148X2-45AF has WS-F6K-FE48X2-AF	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6196-RJ-21	2.74 A@42 V	96-port 10/100TX RJ-21	
WS-X6196-21AF	3.16 A@42 V	• QoS port architecture (Rx/Tx): **1p1q0t/1p3q1t** • WS-X6196-RJ-21 supports WS-F6K-FE48X2-AF • WS-X6196-21AF has WS-F6K-FE48X2-AF	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6348-RJ-45	2.39 A@42 V	48-port 10/100TX RJ-45	
WS-X6348-RJ-45V	2.39 A@42 V	• 128-KB per-port packet buffers • QoS port architecture (Rx/Tx): **1q4t/2q2t** • WS-X6348-RJ-45 supports WS-F6K-VPWR • WS-X6348-RJ-45V has WS-F6K-VPWR • Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6348-RJ-21V	2.39 A@42 V	48-port 10/100TX RJ-21 • 128-KB per-port packet buffers • QoS port architecture (Rx/Tx): **1q4t/2q2t** • Has WS-F6K-VPWR • Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6248-RJ-45	2.69 A@42 V	48-port 10/100TX RJ-45 • QoS port architecture (Rx/Tx): **1q4t/2q2t** • Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6248A-TEL	2.69 A@42 V	48-port 10/100TX RJ-21 • 128-KB per-port packet buffers • QoS port architecture (Rx/Tx): **1q4t/2q2t** • Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6248-TEL	2.69 A@42 V	48-port 10/100TX RJ-21 • QoS port architecture (Rx/Tx): **1q4t/2q2t** • Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6148A-RJ-45 **WS-X6148A-45AF**	2.39 A@42 V 2.57 A@42 V	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	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6148-RJ-45	2.39 A@42 V	48-port 10/100TX RJ-45	
WS-X6148-RJ45V	2.39 A@42 V	• 128-KB per-port packet buffers	
WS-X6148-45AF	2.57 A@42 V	• QoS port architecture (Rx/Tx): **1q4t/2q2t**	
		• WS-X6148-RJ-45 supports WS-F6K-VPWR	
		• WS-X6148-RJ45V has WS-F6K-VPWR	
		• WS-X6148-45AF has WS-F6K-48-AF	
		• Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY
WS-X6148-RJ-21	2.39 A@42 V	48-port 10/100TX RJ-21	
WS-X6148-RJ-21V	2.39 A@42 V	• 128-KB per-port packet buffers	
WS-X6148-21AF	2.57 A@42 V	• QoS port architecture (Rx/Tx): **1q4t/2q2t**	
		• WS-X6148-RJ-21 supports WS-F6K-VPWR	
		• WS-X6148-RJ-21V has WS-F6K-VPWR	
		• WS-X6148-21AF has WS-F6K-48-AF	
		• Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Ethernet Switching Modules

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6024-10FL-MT	1.52 A@42 V	24-port 10BASE-FL MT-RJ	
		• QoS port architecture (Rx/Tx): **1q4t/2q2t**	
		• Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Shared Port Adapter (SPA) Interface Processors (SIPs)

Note See the "FPD Image Packages" section on page 32 for information about additional procedures required to support SIPs.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
7600-SIP-400	6.31 A@42 V	SPA Interface Processor-400	
		With Supervisor Engine 32 PISA	12.2(18)ZY
7600-SIP-200	5.72 A@42 V	SPA Interface Processor-200	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Shared Port Adapters (SPAs)

These sections describe SPAs:

Note PISA-accelerated features are not supported on SPA interfaces.

Gigabit Ethernet SPAs

Product ID (append "=" for spares)	SIP Support	Product Description	Minimum Software Version
SPA-2X1GE	7600-SIP-400	2-port Gigabit Ethernet SPA, SFP Optics	12.2(18)ZY
SFPs Supported in Gigabit Ethernet SPAs			
SFP-GE-S	Extended Temperature SX SFP		
SFP-GE-L	Extended Temperature LX/LH SFP		
SFP-GE-Z	Extended Temperature ZX SFP		

POS SPAs

Product ID (append "=" for spares)	SIP Support	Product Description	Minimum Software Version
SPA-1XOC48POS/RPR	7600-SIP-400	1-Port OC-48 POS/RPR SPA **Note** Requires SFPs.	12.2(18)ZY2
SPA-2XOC3-POS	7600-SIP-200 7600-SIP-400	2-port OC-3c/STM-1c POS SPA **Note** Requires SFPs.	12.2(18)ZY
SPA-4XOC3-POS	7600-SIP-200 7600-SIP-400	4-port OC-3c/STM-1c POS SPA **Note** Requires SFPs.	
SPA-1XOC12-POS	7600-SIP-400	1-port OC-12c/STM-4c POS SPA **Note** Requires an SFP.	

ATM SPAs

Product ID (append "=" for spares)	SIP Support	Product Description	Minimum Software Version
SPA-2XOC3-ATM	7600-SIP-200 7600-SIP-400	2-port OC-3c/STM-1c ATM SPA **Note** Requires SFPs.	12.2(18)ZY
SPA-4XOC3-ATM	7600-SIP-200 7600-SIP-400	4-port OC-3c/STM-1c ATM SPA **Note** Requires SFPs.	
SPA-1XOC12-ATM	7600-SIP-400	1-Port OC-12c/STM-4c ATM SPA **Note** Requires an SFP.	
SPA-1XOC48-ATM	7600-SIP-400	1 port OC-48c/STM-16 ATM SPA	

SFPs for OC3 and OC12 POS and ATM SPAs

Product ID (append "=" for spares)	Product Description
SFP-OC3-MM	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC3-SR	OC-3/STM-1 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-IR1	OC-3/STM-1 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC3-LR1	OC-3/STM-1 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector

Product ID (append "=" for spares)	Product Description
SFP-OC3-LR2	OC-3/STM-1 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector
SFP-OC12-MM	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, MMF, LC connector
SFP-OC12-SR	OC-12/STM-4 pluggable short-reach (2 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC12-IR1	OC-12/STM-4 pluggable intermediate-reach (15 km) transceiver module, 1310-nm wavelength
SFP-OC12-LR1	OC-12/STM-4 pluggable long-reach (40 km) transceiver module, 1310-nm wavelength, LC connector
SFP-OC12-LR2	OC-12/STM-4 pluggable long-reach (80 km) transceiver module, 1550-nm wavelength, LC connector

Serial SPAs

Product ID (append "=" for spares)	SIP Support	Product Description	Minimum Software Version
SPA-8XCHT1/E1	7600-SIP-200	8-Port Channelized T1/E1 SPA	12.2(18)ZY
SPA-2XT3/E3	7600-SIP-200	2-port Clear Channel T3/E3 SPA	
SPA-4XT3/E3	7600-SIP-200	4-port Clear Channel T3/E3 SPA	
SPA-2XCT3/DS0	7600-SIP-200	2-port Channelized T3 to DS0 SPA	
SPA-4XCT3/DS0	7600-SIP-200	4-port Channelized T3 to DS0 SPA	

Services SPA Carrier (SSC)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
7600-SSC-400	5.43 A@42 V	Services SPA Carrier (SSC)	
		With Supervisor Engine 32 PISA	12.2(18)ZY1

Note 7600-SSC-400 does not maintain state when an NSF with SSO redundancy mode switchover occurs.

Services SPAs

Note See the "FPD Image Packages" section on page 32 for information about additional procedures required to support SPA-IPSEC-2G.

Enhanced FlexWAN Module

Note PISA-accelerated features are not supported on FlexWAN module interfaces.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6582-2PA	2.50 A@42 V	Enhanced FlexWAN Module; CEF256	
		With Supervisor Engine 32 PISA	12.2(18)ZY

Enhanced FlexWAN Module Port Adapters

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PA-2FE	2-port Fast Ethernet Port Adapter	12.2(18)ZY
PA-1FE	1-port Fast Ethernet Port Adapter	
PA-POS-1OC3	1-port Packet over SONET OC3c/STM1 Port Adapter	
PA-POS-2OC3	2-port POS OC3c/STM1	
SFPs for PA-POS-2OC3		
SFP-OC3-MM	Short range, multimode fiber	
SFP-OC3-IR1	Intermediate range, single-mode fiber	
SFP-OC3-LR1	Long range, single-mode fiber	
PA-POS-OC3MM **PA-POS-OC3SMI** **PA-POS-OC3SML**	Packet over SONET (OC-3)	

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PA-A6-OC3MM	1-port ATM OC-3c/STM-1 multimode port adapter, enhanced	12.2(18)ZY
PA-A6-OC3SMI	1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced	
PA-A6-OC3SML	1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced	
PA-A6-T3	1-port ATM DS3 port adapter, enhanced	
PA-A6-E3	1-port ATM E3 port adapter, enhanced	
PA-A3-OC3MM **PA-A3-OC3SMI** **PA-A3-T3** **PA-A3-OC3SML** **PA-A3-E3** **PA-A3-8T1IMA** **PA-A3-8E1IMA**	ATM with traffic shaping **Note** These port adapters do not support LANE when installed in the FlexWAN module.	
PA-T3 **PA-T3+** **PA-2T3** **PA-2T3+** **PA-E3** **PA-2E3** **PA-MC-T3** **PA-MC-E3** **PA-MC-2T3+**	T3/E3 (clear-channel and channelized)	12.2(18)ZY
PA-4T+ **PA-8T-V35** **PA-8T-X21** **PA-8T-232** **PA-MC-2E1/120** **PA-MC-8T1** **PA-MC-8E1/120** **PA-MC-2T1** **PA-MC-4T1**	T1/E1	
PA-4E1G/75 **PA-4E1G/120**	T1/E1	
PA-MC-8TE1+	Multichannel T1/E1 8PRI **Note** This port adapter does not support ISDN PRI when installed in the FlexWAN module.	
PA-H **PA-2H**	HSSI	
PA-MC-STM-1	Multichannel STM-1	

Service Modules

Note

- For any service module that runs its own software, see the service module software release notes for information about the minimum required service module software version.
- PISA-accelerated features are not supported on service module switch virtual interfaces (SVIs).

Firewall Services Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-FWM-1-K9	4.09 A@42 V	Firewall Services Module; CEF256	
		With Supervisor Engine 32 PISA	12.2(18)ZY

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.

Note With Firewall Services Module Software Release 2.3(1), WS-SVC-FWM-1-K9 maintains state when an NSF with SSO redundancy mode switchover occurs.

Intrusion Detection System Modules (IDSMs)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-IDSM2-K9	2.50 A@42 V	Intrusion Detection System Module 2; CEF256	
		With Supervisor Engine 32 PISA	12.2(18)ZY1

WS-SVC-IDSM2-K9 runs its own software—See these publications:

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfmulti.html

See the WS-SVC-IDSM2-K9 software release notes for information about the minimum required WS-SVC-IDSM2-K9 software version.

Network Analysis Modules (NAMs)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-NAM-2	3.47 A@42 V	Network Analysis Module 2; CEF256	
WS-SVC-NAM-1	2.89 A@42 V	Network Analysis Module 1; CEF256	
		With Supervisor Engine 32 PISA	12.2(18)ZY

WS-SVC-NAM-2 and WS-SVC-NAM-1 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 WS-SVC-NAM-2 and WS-SVC-NAM-1 software release notes for information about the minimum required WS-SVC-NAM-2 and WS-SVC-NAM-1 software version.

Fan Trays

Note Enter the **show environment status | include fan** command or the **show environment cooling** command to display information about the installed fan trays.

These high-capacity fan trays require at least a 2,500 W power supply.

Product ID (append "=" for spares)	Power Allocated at 42 V	Product Description	Minimum Software Version
WS-C6503-E-FAN	1.37 A@42 V	High-capacity fan tray for WS-C6503-E chassis	12.2(18)ZY
FAN-MOD-3HS	2.98 A@42 V	High-capacity fan tray for WS-C6503 chassis	
FAN-MOD-6HS	4.29 A@42 V	High-capacity fan tray for CISCO7606 chassis	
WS-C6506-E-FAN	2.35 A@42 V	High-capacity fan tray for WS-C6506-E chassis	
WS-C6K-6SLOT-FAN2	12 V fan	High-capacity fan tray for WS-C6506 chassis	
FAN-MOD-09	5.75 A@42 V	High-capacity fan tray for WS-C6509-NEB-A and CISCO7609 chassis	
WS-C6509-E-FAN	3.58 A@42 V	High-capacity fan tray for WS-C6509-E chassis	
WS-C6K-9SLOT-FAN2	12 V fan	High-capacity fan tray for WS-C6509 chassis	
WS-C6K-13SLT-FAN2	7.10 A@42 V	High-capacity fan tray for WS-C6513 and CISCO7613 chassis	

Power Supplies

CISCO7606 Power Supplies

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PWR-2700-AC	2700 W AC power supply	12.2(18)ZY
PWR-2700-DC	2700 W DC power supply	

WS-C6504-E and CISCO7604 Power Supplies

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PWR-2700-AC/4	2700 W AC power supply	12.2(18)ZY
PWR-2700-DC/4	2700 W DC power supply	

WS-C6503 and 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(18)ZY
PWR-950-AC	950 W AC power supply	
PWR-950-DC	950 W DC power supply	

All Other Power Supplies

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-CAC-8700W-E	8,700 W AC power supply	12.2(18)ZY1
	Note • Limited to 4,500 W in the WS-C6509-NEB-A chassis. • Limited to 4,000 W in these chassis: – WS-C6509 – WS-C6506 – WS-C6509-NEB • 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	
WS-CAC-6000W	**Note** • Limited to 4,500 W in the WS-C6509-NEB-A chassis. • Limited to 4,000 W in these chassis: – WS-C6509 – WS-C6506 – WS-C6509-NEB	12.2(18)ZY
PWR-4000-DC	4,000 W DC power supply	
WS-CAC-4000W	4,000 W AC power supply	
+WS-CAC-3000W	3,000 W AC power supply	
WS-CAC-3000W	3,000 W AC power supply	
WS-CAC-2500W	2,500 W AC power supply	
WS-CDC-2500W	2,500 W DC power supply	

Chassis

- 13-Slot Chassis, page 28
- 9-Slot Chassis, page 28
- 6-Slot Chassis, page 29
- 4-Slot Chassis, page 30
- 3-Slot Chassis, page 30

13-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6513	Catalyst 6513 chassis: • 13 slots • 64 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY
CISCO7613	Cisco 7613 chassis: • 13 slots • 64 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY

9-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6509-E	Catalyst 6509 chassis: • 9 horizontal slots • 1024 chassis MAC addresses • Requires WS-C6509-E-FAN • Requires 2,500 W or higher power supply	
	With Supervisor Engine 32 PISA	12.2(18)ZY
WS-C6509	Catalyst 6509 chassis: • 9 horizontal slots • 1024 chassis MAC addresses • Use with Supervisor Engine 720 or Supervisor Engine 32 requires WS-C6K-9SLOT-FAN2 • WS-CAC-6000W is limited to 4,000 W in WS-C6509	
	With Supervisor Engine 32 PISA	12.2(18)ZY
WS-C6509-NEB-A	Catalyst 6509-NEB chassis • 9 vertical slots • 64 chassis MAC addresses • No fan tray upgrade required for use with Supervisor Engine 720	
	With Supervisor Engine 32 PISA	12.2(18)ZY
WS-C6509-NEB	Catalyst 6509-NEB chassis: • 9 vertical slots • 1024 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY

Product ID (append "=" for spare)	Product Description	Minimum Software Version
CISCO7609	Cisco 7609 chassis • 9 vertical slots • 64 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY
OSR-7609	Cisco 7609 chassis: • 9 vertical slots • 1024 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY

6-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6506-E	Catalyst 6506 chassis: • 6 slots • 1024 chassis MAC addresses • Requires WS-C6506-E-FAN • Requires 2,500 W or higher power supply	
	With Supervisor Engine 32 PISA	12.2(18)ZY
WS-C6506	Catalyst 6506 chassis: • 6 slots • 1024 chassis MAC addresses • Use with Supervisor Engine 720 or Supervisor Engine 32 requires WS-C6K-6SLOT-FAN2 • WS-CAC-6000W is limited to 4,000 W in WS-C6506	
	With Supervisor Engine 32 PISA	12.2(18)ZY
CISCO7606	Cisco 7606 chassis: • 6 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720 or Supervisor Engine 32 requires FAN-MOD-6HS	
	With Supervisor Engine 32 PISA	12.2(18)ZY

4-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6504-E	Catalyst 6504-E chassis: • 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY
CISCO7604	Cisco 7604 chassis: • 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY

3-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6503-E	• 3 slots • 64 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY
WS-C6503	Catalyst 6503 chassis: • 3 slots • 64 chassis MAC addresses	
	With Supervisor Engine 32 PISA	12.2(18)ZY

Unsupported Hardware

Release 12.2(18)ZY does not support this hardware:

- Supervisor Engine 720
- Supervisor Engine 32
- Supervisor Engine 2
- Supervisor Engine 1
- WS-F6K-PFC3A Policy Feature Card 3A (PFC3A)
- WS-F6K-PFC3BXL Policy Feature Card 3BXL (PFC3BXL)
- DFCs (installed DFCs do not power up with a Supervisor Engine 32 PISA)
- Switch Fabric Modules

- These switching modules:
  - WS-X6704-10GE 4-port 10-Gigabit Ethernet XENPAK
  - WS-X6748-SFP 48-port Gigabit Ethernet SFP
  - WS-X6724-SFP 24-port Gigabit Ethernet SFP
  - WS-X6816-GBIC 16-port Gigabit Ethernet GBIC
  - WS-X6748-GE-TX 48-port 10/100/1000 RJ-45
- 7600-SIP-600 SPA Interface Processor-600
- Optical Services Modules (OSMs)
- WS-X6182-2PA FlexWAN Module (the WS-X6582-2PA Enhanced FlexWAN Module is supported)
- CISCO7603 3-slot chassis
- These service modules:
  - WS-SVC-SSL-1 Secure Sockets Layer (SSL) Services Module
  - WS-SVC-WEBVPN-K9 WebVPN Services Module
  - WS-SVC-WISM-1-K9 Wireless Services Module (WiSM)
  - WS-SVC-AON-1-K9 Application-Oriented Networking (AON) Module
  - WS-SVC-AGM-1-K9 Anomaly Guard Module
  - WS-SVC-ADM-1-K9 Traffic Anomaly Detector Module
  - WS-SVC-CSG-1 Content Services Gateway (CSG)
  - WS-X6066-SLB-APC Content Switching Module (CSM)
  - WS-X6066-SLB-S-K9 Content Switching Module with SSL (CSM-S)
  - WS-SVC-PSD-1 Persistent Storage Device (PSD) Module
  - WS-SVC-WLAN-1-K9 Wireless LAN service module
  - WS-SVC-IPSEC-1 IPsec VPN acceleration services module
  - WS-X6381-IDS Intrusion Detection System (IDS) Module

    Note WS-SVC-IDSM2-K9 is supported.

  - WS-X6380-NAM Network Analysis Module (NAM)

    Note WS-SVC-NAM-2 and WS-SVC-NAM-1 are supported.

- These DWDM SFPs:
  - DWDM-SFP-5817—1000BASE-DWDM 1558.17 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-5252—1000BASE-DWDM 1552.52 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-5172—1000BASE-DWDM 1551.72 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-5012—1000BASE-DWDM 1550.12 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-4692—1000BASE-DWDM 1546.92 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-4373—1000BASE-DWDM 1543.73 nm SFP (100-GHz ITU grid) SFP module

  - DWDM-SFP-4214—1000BASE-DWDM 1542.14 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-3977—1000BASE-DWDM 1539.77 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-3898—1000BASE-DWDM 1538.98 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-3582—1000BASE-DWDM 1535.82 nm SFP (100-GHz ITU grid) SFP module
  - DWDM-SFP-3504—1000BASE-DWDM 1535.04 nm SFP (100-GHz ITU grid) SFP module
- WS-X6624-FXS, WS-X6608-T1, and WS-X6608-E1 voice modules
- WS-X6101-OC12-MMF and WS-X6101-OC12-SMF ATM LANE modules
- WS-X6302-MSM Multilayer Switch Module
- Catalyst 6000 series chassis
- These power supplies cannot support high-capacity fan trays:
  - WS-CAC-1300W
  - WS-CDC-1300W
  - WS-CAC-1000W

Unsupported modules remain powered down if detected and do not affect system behavior.

FPD Image Packages

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

These sections describe FPD packages:

- FPD-Image Dependant Modules, page 32
- FPD Image Package Contents, page 33
- FPD Upgrades, page 33

FPD-Image Dependant Modules

These modules use FPD images:

- Shared Port Adapter (SPA) Interface Processors (SIPs)
- Shared Port Adapters
- Enhanced FlexWAN Module (WS-X6582-2PA)

Note You do not need to do a separate FPD image upgrade for the Enhanced FlexWAN module, because the Cisco IOS software images contain the FPD image for the Enhanced FlexWAN module. The FPD image package also includes the FPD image for the Enhanced FlexWAN module. (CSCin90971)

FPD Image Package Contents

Enter the **show upgrade fpd file** command to display the contents of the FPD package.

FPD Upgrades

Note You do not need to do a separate FPD image upgrade for the Enhanced FlexWAN module, because the Cisco IOS software images contain the FPD image for the Enhanced FlexWAN module. The FPD image package also includes the FPD image for the Enhanced FlexWAN module. (CSCin90971)

See this publication:

http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

Feature Sets

Use Cisco Feature Navigator to display information about the images and feature sets in Release 12.2ZY.

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

New Features in Release 12.2(18)ZYA3c

These sections describe the new features in Release 12.2(18)ZYA3c:

- New Hardware Features in Release 12.2(18)ZYA3c, page 33
- New Software Features in Release 12.2(18)ZYA3c, page 33

New Hardware Features in Release 12.2(18)ZYA3c

None.

New Software Features in Release 12.2(18)ZYA3c

None.

New Features in Release 12.2(18)ZYA3b

These sections describe the new features in Release 12.2(18)ZYA3b:

New Hardware Features in Release 12.2(18)ZYA3b

None.

New Software Features in Release 12.2(18)ZYA3b

None.

New Features in Release 12.2(18)ZYA3a

These sections describe the new features in Release 12.2(18)ZYA3a:

New Hardware Features in Release 12.2(18)ZYA3a

None.

New Software Features in Release 12.2(18)ZYA3a

None.

New Features in Release 12.2(18)ZYA3

These sections describe the new features in Release 12.2(18)ZYA3:

New Hardware Features in Release 12.2(18)ZYA3

None.

New Software Features in Release 12.2(18)ZYA3

None.

New Features in Release 12.2(18)ZYA2

These sections describe the new features in Release 12.2(18)ZYA2:

- New Hardware Features in Release 12.2(18)ZYA2, page 35
- New Software Features in Release 12.2(18)ZYA2, page 35

New Hardware Features in Release 12.2(18)ZYA2

None.

New Software Features in Release 12.2(18)ZYA2

- Application-aware NetFlow—See this publication:
  http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/nf_lay2_sec_mon_exp.html
- AutoQoS for the Enterprise - Suggested Policy—See this publication:
  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/autoqos_enterprise.html
- NBAR PDLM - Telepresence—See this publication:
  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_traffic_nbar.html

New Features in Release 12.2(18)ZYA1

These sections describe the new features in Release 12.2(18)ZYA1:

- New Hardware Features in Release 12.2(18)ZYA1, page 35
- New Software Features in Release 12.2(18)ZYA1, page 35

New Hardware Features in Release 12.2(18)ZYA1

None.

New Software Features in Release 12.2(18)ZYA1

- FPM - Copy and/or Redirect matched packet—See this publication:
  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_flex_pack_match.html

- Intelligent Traffic Redirect—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/P1.html#platform_ip_features_pisa
- Non-intrusive Protocol Discovery—See this publication:

  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_traffic_nbar.html

New Features in Release 12.2(18)ZYA

These sections describe the new features in Release 12.2(18)ZYA:

- New Hardware Features in Release 12.2(18)ZYA, page 36
- New Software Features in Release 12.2(18)ZYA, page 36

New Hardware Features in Release 12.2(18)ZYA

None.

New Software Features in Release 12.2(18)ZYA

- Enhance FPM Search Window Size To 128 bytes—See this publication:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_flex_pack_match.html
- Enhanced PoE Support (Additional Wattage Range)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/voip.html#wpCisco_Enhanced_PoE_Support
- Firewall Websense URL Filtering—See this publication:

  http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_fwall_websense.html
- NBAR and FPM activation on Layer 2 interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_trfc_nbar_map.html
- PISA - FWSM integration—See this publication:

  http://www.cisco.com/en/US/docs/security/fwsm/fwsm40/configuration/guide/protct_f.html#Permitting_or_Denying_Application_Types_with_PISA_Integration

Note Application-aware NetFlow is being developed for release in a future rebuild of Release 12.2(18)ZYA.

New Features in Release 12.2(18)ZY2

These sections describe the new features in Release 12.2(18)ZY2:

- New Hardware Features in Release 12.2(18)ZY2, page 37
- New Software Features in Release 12.2(18)ZY2, page 37

New Hardware Features in Release 12.2(18)ZY2

1-Port OC-48 POS/RPR SPA (SPA-1XOC48POS/RPR):

- Supported only with 7600-SIP-400
- See these publications:
  - http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/6500series/sipspahw.html
  - http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

New Software Features in Release 12.2(18)ZY2

NBAR URL Classification Scalable to 56 URLs—See this publication:

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_traffic_nbar.html

New Features in Release 12.2(18)ZY1

These sections describe the new features in Release 12.2(18)ZY1:

- New Hardware Features in Release 12.2(18)ZY1, page 37
- New Software Features in Release 12.2(18)ZY1, page 38

New Hardware Features in Release 12.2(18)ZY1

- Supervisor Engine 32 PISA with two 10-Gigabit Ethernet ports (WS-S32-10GE-PISA)
- Services SPA Carrier (SSC; 7600-SSC-400)

Note 7600-SSC-400 does not maintain state when an NSF with SSO redundancy mode switchover occurs.

- IPsec SPA (SPA-IPSEC-2G):
  - See these publications:

    http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/6500series/sipspahw.html

    http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- 8700 W AC power supply (WS-CAC-8700W-E)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Chassis_Installation/Cat6500/6500_ins.html

New Software Features in Release 12.2(18)ZY1

- Certificate Security Attribute-Based Access Control (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html

- Crypto Conditional Debug Support (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/12-2sx/sec-crypto-debug-sup.html

- Certificate Autoenrollment (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html

- Distinguished Name-Based Crypto Maps (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/12-2sx/sec-dist-nm-cyrpto.html

- Dynamic Multipoint VPN (DMVPN) Phase 2 on SPA-IPSEC-2G—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-s/sec-conn-dmvpn.html

- Easy VPN Server features (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_esyvpn/configuration/12-2sx/sec-easy-vpn-12-2sx-book.html

- Encrypted Multicast over GRE (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- Encrypted Preshared Key (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/12-2sx/sec-encrypt-preshare.html

- IDSM-2 EtherChannel load balancing—See this publication:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/tsd_products_support_model_home.html

- IKE: Initiate Aggressive Mode (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/12-2sx/sec-aggr-mde-ike.html

- IPsec VPN Accounting (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_imgmt/configuration/12-2sx/sec-ipsec-vpn-acctg.html

- IPsec VPN Monitoring (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_imgmt/configuration/12-2sx/sec-ip-security-vpn.html

- Manual Certificate Enrollment (TFTP and Cut-and-Paste; supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html

- Multiple RSA Key Pair Support (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-deploy-rsa-pki.html

- Protected private key storage (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-deploy-rsa-pki.html

- Real-Time Resolution for IPsec Tunnel Peer (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnav/configuration/12-2sx/sec-realtime-ipsec.html

- Re-enroll using existing certificate (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html

- Source Interface Selection for Outgoing Traffic with Certificate Authority (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-sis-with-ca.html

- Trusted Root Certification Authority (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_cert_auth_io_OBS.html

- Trustpoint CLI (supported on SPA-IPSEC-2G)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html

- VRF Aware IPsec with SPA-IPSEC-2G—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76ovwvpn.html

Features in Release 12.2(18)ZY

These sections describe the features in Release 12.2(18)ZY:

Note

- See the following site for information about MIBs:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- Features in the Cisco IOS 12.2ZY releases that are also supported in the Cisco IOS 12.2 mainline, 12.2T and 12.2S releases are documented in the publications for these releases. When applicable, this section refers to these publications for platform-independent features supported in the Cisco IOS 12.2ZY releases.

PISA-Accelerated Features

These features are accelerated in hardware on the PISA:

- Network-Based Application Recognition (NBAR)—See this publication:

  http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/clsfy_traffic_nbar.html
- Flexible Packet Matching (FPM)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/ht_fpm.html

Note NBAR and FPM are features that can only be configured on Layer 3 interfaces and are applied only to Layer 3 traffic. You cannot apply NBAR and FPM to Layer 2 traffic.

Other Features

These features are accelerated on the PFC3B or run in software on the PISA:

- 4096 Layer 2 VLANs—See this publication:

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

Note We recommend that you configure a combined total of no more than 2,000 Layer 3 VLAN interfaces and Layer 3 ports.

- Any Transport over MPLS (AToM) Features (supported on WAN ports):
  - Supported on WAN ports
  - Ethernet over MPLS (EoMPLS)
  - Frame Relay over MPLS (FRoMPLS)
  - ATM Single Cell Relay over MPLS-VC Mode (CRoMPLS)
  - ATM AAL5 over MPLS (AAL5oMPLS)

  See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE
- Any Transport over MPLS (AToM): HDLC over MPLS (HDLCoMPLS):
  - Supported on WAN ports.
  - See this publication:

    http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Configuring_Strict_Priority_Low_Latency_Queuing_(LLQ)_Support_on_the_OSM-24GE-WAN
- Any Transport over MPLS (AToM): PPP over MPLS (PPPoMPLS):
  - Supported on WAN ports.
  - See this publication:

    http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Configuring_Strict_Priority_Low_Latency_Queuing_(LLQ)_Support_on_the_OSM-24GE-WAN
- ARP ACLs for QoS Filtering—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/qos.html
- ATM Cell Loss Priority (CLP) Setting on FlexWAN module ATM interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html
- ATM OAM ping—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12satmpng.html
- ATM VC access trunk emulation—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12satmpng.html
- ATM Virtual Circuit (VC) Bundling—See these publications:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfipaov_ps1835_TSD_Products_Configuration_Guide_Chapter.html

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsmu26s.html
- Autostate - Firewall Capability for the Firewall service module—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsmu26s.html
- Bandwidth Command for HQoS Parent Class Support—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Configuring_Strict_Priority_Low_Latency_Queuing_(LLQ)_Support_on_the_OSM-24GE-WAN
- BGP Configuration Using Peer Templates—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpct.html

- BGP Cost Community—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpcc.html
- BGP Dynamic Update Peer-Groups—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpcc.html
- BGP Increased Support of Numbered AS-path Access Lists to 500—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_bgpcc.html
- BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/fsxeibmp.html

  Note With the BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN feature configured, do not attach output service policies to VRF interfaces. (CSCsb25509)

  For nonMPLS environments, see the Interior Border Gateway Protocol (iBGP) Multipath Load Sharing feature.
- BGP Policy Accounting—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgppa.html
- BGP Restart Session After Max-Prefix Limit—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgppa.html
- BGP Route Map Continue—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgppa.html
- BGP Route-Map Policy List Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgppa.html
- BGP support for TTL security check—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgppa.html
- Bidirectional Forwarding Detection (BFD) standard implementation—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  Note Catalyst 6500 switches support BFD only on Ethernet, Fast Ethernet (except PA-2FE and PA-1FE), Gigabit Ethernet, and 10-Gigabit Ethernet ports, including Ethernet SPAs. The Catalyst 6500 switches and Cisco 7600 routers do not support BFD on PA-2FE or PA-1FE Ethernet LAN ports, or on POS, ATM, or serial WAN ports.

  Also see "Integrated IS-IS support for BFD over IPv4" and "OSPF support for BFD over IPv4."
- Bidirectional Protocol Independent Multicast (PIM)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/mcastv4.html
- Boot Protocol (BOOTP) relay—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfdhcp.html
- Bridge Control Protocol (BCP)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- Bridging using RFC1483 Routed Encapsulation (BRE)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- Cisco Discovery Protocol (CDP)—See this publication:

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

- Cisco IOS IP Event Dampening—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_pi/configuration/12-2sx/iri-ip-event-damp.html

- Cisco IP Phone support and enhancements:
  - Support for a high-powered phone to negotiate a low-power mode (dimmed screen) when powered by a pre-standard Cisco PoE daughtercard.
  - Support for a high-powered phone to negotiate a high-power mode (full screen brightness) when powered by a IEEE 802.3af Cisco PoE daughtercard.
  - See this publication:

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

- Cisco Nonstop Forwarding (NSF) with stateful switchover (SSO) supervisor engine redundancy—See this publication:

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

Note

- NSF with SSO supports multicast traffic.
- NSF with SSO redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, IPX, or MPLS.
- These protocols can coexist with NSF with SSO redundancy mode, but there is no stateful support for them:
  - MPLS and LDP
  - GLBP
  - HSRP
  - VRRP
- Following an NSF with SSO switchover, traffic loss occurs on the links where the protocols are configured until the protocols converge.
- With Firewall Services Module Software Release 2.3(1), WS-SVC-FWM-1-K9 maintains state when an NSF with SSO redundancy mode switchover occurs.

- Clear hardware interface counters—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.html

- CNS Interactive CLI—Network management applications can use the Cisco Networking Services (CNS) agents to manage network routers. The CNS agent provides the capability to send commands to a router from a programmable source. The CNS Interactive CLI feature introduces a new XML interface that allows you to send interactive commands to a router, such as commands that generate

prompts for user input. A benefit of this feature is that interactive commands can be terminated before they have been fully processed. For example, for commands that generate a significant amount of output, the XML interface can be customized to limit the size of the output or the length of time allowed for the output to accumulate. The capability to use a programmable interface to terminate a command before its normal termination (similar to manually terminating a command) can greatly increase the efficiency of diagnostic applications that might use this functionality. The new XML interface also allows for multiple commands to be processed in a single session. The response for each command is packaged together and sent in a single response event.

- Configurable Per VLAN MAC Learning (PVL)—See the **mac-address-table learning** command in this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.html

- Control Plane DSCP Support for RSVP—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/15-mt/rsvp-dscp-spt-for-rsvp.html

- Custom IEEE 802.1Q Ethertypes:
  - Supported on these modules:

    —Supervisor Engine 32 PISA
    —WS-X6516-GE-TX
    —WS-X6516A-GBIC
    —WS-X6516-GBIC

    Note The WS-X6516A-GBIC and WS-X6516-GBIC modules apply a configured custom EtherType field value to all ports supported by each port ASIC (1 through 8 and 9 through 16).

  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/layer2.html

- Data-link switching plus (DLSw+)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcfdlsw_support_TSD_Island_of_Content_Chapter.html

- DE/CLP and EXP mapping on FR/ATMoMPLS VC—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE

- DHCP Option 82 on Untrusted Port—See this publication:

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

- DHCP Snooping—See this publication:

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

- Digital Optical Monitoring (DOM)—See the **show interfaces transceiver** command in this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.html

  Note See this publication for additional information about DOM:

  http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/compatibility/matrix/OL_8031.html

- Distributed LFI (dLFI) and distributed QoS (dQoS) over Leased Lines on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_latjit/configuration/15-mt/qos-mlppp-fr.html

- Distributed MLPPP (dMLPPP) on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

  Note cRTP is not supported on dMLPPP bundled links.

- Distributed Multilink Frame Relay (FRF.16)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/dmfr.html

- Distributed network-based application recognition (dNBAR) on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/dmfr.html

- Directed broadcast hardware support with the **mls ip directed-broadcast** command—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/M1.html

- Dot1q Transparency for EoMPLS on WAN ports—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE

- DSCP transparency (also called “Preserving the Received ToS Byte”)—See the procedures in this publication:

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

- Dynamic ARP Inspection (DAI)—See this publication:

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

- Dynamic Host Configuration Protocol (DHCP)— See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfdhcp.html

- Egress ACL support for remarked DSCP—See this publication:

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

- Egress DSCP mutation—See this publication:

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

- Egress policing for LAN ports configured as Layer 3 interfaces and for VLAN interfaces—See the procedures in this publication for information about configuring the **service-policy output** command:

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

- EIGRP MPLS VPN PE-CE site of origin (SoO)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_mvesoo.html

- Embedded CiscoView—See this publication:

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

- Embedded network management improvements—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/s_mvesoo.html

- Encapsulated Remote SPAN (ERSPAN)—See this publication:

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

- Enhanced support for interface link status messages (CSCeb06765). See the following publication for more information:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/I1.html

- EtherChannel Enhancement - 128 EtherChannels Support—See this publication:

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

- EtherChannel Min-Links—See this publication:

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

- EtherChannel—See this publication:

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

- Ethernet over MPLS (EoMPLS) per VLAN QoS—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE

- Field-programmable device upgrade tool—The Cisco SPA field-programmable device (FPD) upgrade tool provides customers and field engineers a consistent way across platforms to upgrade firmware or images for the programmable devices (for example, FPGAs, PLDs, ROMMON). The customer can get proper images from Cisco.com, and use this tool to automatically download (with a flash card or TFTP) to the FPD tool, or manually if needed. The FPD tool provides a convenient and safe way for customer to upgrade an FPD for related bug fixes and feature enhancement with minimum system impact. The FPD tool significantly improves customer satisfaction and product reliability.

- Flex Links—See this publication:

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

- FlexWAN interface support for 4000 ATM VCs per port adapter on the following ATM port adapters:
  - PA-A3-OC3MM
  - PA-A3-OC3SMI
  - PA-A3-OC3SML
  - PA-A3-T3
  - PA-A3-E3
  - PA-A6-OC3MM
  - PA-A6-OC3SMI
  - PA-A6-OC3SML
  - PA-A6-T3
  - PA-A6-E3
- Frame Relay virtual circuit (VC) bundling—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE
- Gateway Load Balancing Protocol—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_glbp2.html
- Generic Online Diagnostics (GOLD)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/diags.html
- Half-Bridging on FlexWAN ATM interfaces (CSCin27157)
- Hardware Capacity Monitoring—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/pwr_envr.html
- Hardware Control Plane Interface for Control Plane Policing (CoPP):
  - With Cisco IOS 12.2ZY releases, the PFC3B supports CoPP.
  - The PFC3B does not support CoPP output rate limiting (policing).
  - The PFC3B does not support the CoPP silent operation mode.
  - The PFC3B does not support the **match protocol arp** command.
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/dos.html
- Hardware-supported counters for hardware-supported ACLs, displayed by the **show tcam interface** command. See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/show4.html
- HQoS support for Ethernet over MPLS (EoMPLS) VC—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/show4.html

- H-VPLS with MPLS Edge—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE
- ICMP traffic hardware switching when Cisco IOS reflexive ACLs are configured. (CSCeb20666)
- IEEE 802.1Q protocol tunneling—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/dot1qtnl.html
- IEEE 802.1Q tunneling—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/dot1qtnl.html
- IEEE 802.1s - Multiple Spanning Tree (MST) Standard Compliance—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/spantree.html
- IEEE 802.1w rapid reconfiguration of spanning tree—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/spantree.html
- IEEE 802.1X Port-Based Authentication—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/dot1x.html
- IEEE 802.3ad link aggregation control protocol (LACP)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/channel.html
- IGMP snooping and IGMP snooping querier—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/snooigmp.html
- IGMP Static Group Range Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/stgrpsxf.html
- Ingress CoS mutation on IEEE 802.1Q tunnel ports—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/qos.html
- Integrated IS-IS global default metric—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-mt/irs-netd.html
- Integrated IS-IS protocol shutdown support maintaining configuration parameters—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_isis/configuration/guide/irs_initcf.html
- Integrated IS-IS support for BFD over IPv4—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

Note Also see "Bidirectional Forwarding Detection (BFD) standard implementation."

- Interior Border Gateway Protocol (iBGP) Multipath Load Sharing—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgpls.html

  Note For MPLS support, see BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN.

- Internet Group Management Protocol Version 3 (IGMPv3) snooping—See this publication:

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

- Invalid Special Parameter Index (SPI) Recovery—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dplane/configuration/12-2sx/sec-invald-index-rec.html

- Inverse Multiplexing over ATM (IMA) on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- IP-in-IP tunneling and generic routing encapsulation (GRE) tunneling supported in hardware—The PFC3B supports the following tunnel commands:
  - **tunnel destination**
  - **tunnel mode gre**
  - **tunnel mode ipip**
  - **tunnel source**
  - **tunnel ttl**
  - **tunnel tos**

  Other supported types of tunneling run in software on the PISA. The PFC3B does not provide hardware acceleration for tunnels configured with the **tunnel key** command.

  The **tunnel ttl** command (default 255) sets the TTL of encapsulated packets.

  The **tunnel tos** command, if present, sets the ToS byte of a packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is not enabled, the ToS byte of a packet sets the ToS byte of the packet when it is encapsulated. If the **tunnel tos** command is not present and QoS is enabled, the ToS byte of a packet as modified by PFC QoS sets the ToS byte of the packet when it is encapsulated.

  To configure GRE Tunneling and IP in IP Tunneling, refer to these publications:

  http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html

  http://www.cisco.com/en/US/docs/ios/12_2/interface/command/reference/irfshoip.html

  To configure the **tunnel tos** and **tunnel ttl** commands, refer to this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html

  Note the following information about tunnels:
  - Each hardware-assisted tunnel must have a unique source. Hardware-assisted tunnels cannot share a source even if the destinations are different. Use secondary addresses on loopback interfaces or create multiple loopback interfaces. (CSCdy72539)
  - Each tunnel interface uses one internal VLAN.
  - Each tunnel interface uses one additional router MAC address entry per router MAC address.

  - The PFC3B supports PFC QoS features on tunnel interfaces.
  - The PFC3B supports GRE tunnel encapsulation and de-encapsulation of multicast traffic.
  - The PISA supports tunnels configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT and PAT (for inside to outside translation), TCP intercept, context-based access control (CBAC), and encryption.
- IP routing of RFC1483 ATM bridge encapsulation (RBE)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html
- IP Unnumbered for VLAN-SVI interfaces—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/layer3.html
- IPSec Anti-Replay Window: Expanding and Disabling—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_dplane/configuration/12-2sx/sec-ipsec-antireplay.html
- IPv4 multicast over point-to-point GRE tunnels (hardware supported)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html

  Note The PFC3B does not provide hardware acceleration for tunnels configured with the **tunnel key** command.
- IPv6 supported in hardware for these basic IPv6 functions:
  - IPv6 standard access control lists (ACLs)
  - IPv6 extended ACLs
  - Reflexive ACLs
  - Manually configured v6 tunnels
  - ISATAP (ISATAP with 6-to-4 prefix is not supported in hardware)
  - Automatically configured IPv4 compatible tunnels
  - 6-to-4 tunnel
  - IPv6 over IPV4 IP in IP tunnels
- IPv6 supported in software for these basic IPv6 functions:
  - IPv6 addressing architecture
  - ICMPv6
  - Neighbor Discovery
  - Static ND cache entry
  - IPv6 stateless autoconfiguration
  - ICMPv6 Redirect
  - MTU path Discovery for IPv6
  - IPv6 ICMP rate limiting
  - IPv6 over IPV4 GRE tunnels
- IPv6 supported in software for these IPv6 routing functions:

  - Static routes within IPv6
  - RIPng
  - MP-BGP4
  - OSPFv3
  - ISIS
  - Configuring an IPv6 Multiprotocol BGP Peer using a link local address
  - IPv6 MP-BGP distance command
- IPv6 switching support:
  - Process switching
  - CEFv6 switching
  - Distributed CEFv6 switching
- IPv6 supported in software for these IPv6 applications:
  - Ping
  - Traceroute
  - Telnet
  - TFTP (client only)
  - FTP
  - SSH over IPv6
  - DNS
  - HTTP server

  For configuration information, refer to this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-mt/ip6-mcast-ssm-map.html

  For command reference information, refer to this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-mt/ip6-mcast-ssm-map.html
- IPv6 access services: DHCPv6 prefix delegation—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-mt/ip6-mcast-ssm-map.html
- IPv6 hardware: multicast assist—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/mcastv6.html
- IPv6 multicast RPR support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/redund.html
- IPv6 multicast: Bootstrap Router (BSR)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ipv6-12-2sx-book.html
- IPv6 Provider Edge Router (6PE) over MPLS—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sx/ipv6-12-2sx-book.html

- IPv6 QoS: (quality of service)—See this publication:

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

- IPv6 Support on WAN Interfaces—See this publication:

  http://www.cisco.com/en/US/tech/tk872/tech_white_papers_list.html

- IS-IS caching of redistributed routes—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isredrib.html

- IS-IS Incremental SPF—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isisispf.html

- IS-IS Limit on Number of Redistributed Routes—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsiredis.html

- IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsisiadv.html

- IS-IS support for priority-driven IP prefix RIB installation—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslocrib.html

- IS-IS Support for Route Tags—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-mt/irs-isis-supp-route-tags.html

- Jumbo frames on all Ethernet ports except ports on the WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6148-GE-TX, and WS-X6148V-GE-TX switching modules.

Caution The following switching modules support a maximum ingress frame size of 8092 bytes:

- WS-X6516-GE-TX when operating at 100 Mbps
- WS-X6148-RJ-45, WS-X6148-RJ45V and WS-X6148-RJ21, WS-X6148-RJ21V
- WS-X6248-RJ-45 and WS-X6248-TEL
- WS-X6248A-RJ-45 and WS-X6248A-TEL
- WS-X6348-RJ-45, WS-X6348-RJ45V and WS-X6348-RJ21V

When jumbo frame support is configured, these modules drop ingress frames larger than 8092 bytes.

- Key rollover for certificate renewal—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html

- L3 MPLS VPN over GRE on 7600-SIP-400—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- Layer 2 protocol tunneling global threshold—See the **l2protocol-tunnel global drop-threshold** command in the command reference at this URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.html

- Layer 2 switch ports and VLAN trunks with the Dynamic Trunking Protocol (DTP), including support on Gigabit Ethernet ports for jumbo frames—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/layer2.html

- Layer 2 traceroute—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/l2trace.html

- Link Fragmentation and Interleaving (LFI) for Frame Relay and ATM Virtual Circuits (supported on FlexWAN interfaces)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_latjit/configuration/15-mt/qos-mlppp-fr.html

- Local proxy ARP—See the *Catalyst Supervisor Engine 32 PISA Cisco IOS Command Reference*, Release 12.2ZY, publication.

  Note To use the local proxy ARP feature, you must enable the IP proxy ARP feature. The IP proxy ARP feature is enabled by default. See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfipadr.html#Enabling_Proxy_ARP

- Low Latency Queueing (LLQ) and Class-based Weighted Fair Queueing (CBWFQ) on MLPPP links (supported on FlexWAN interfaces)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html

- MAC address-based traffic blocking—See this publication:

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

- Mapping a subinterface to an EoMPLS VC on 7600-SIP-400—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- 'match cos' classification on 7600-SIP-400—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- Metro Ethernet Advanced QinQ Service Mapping—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html

- MLD snooping—See this publication:

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

- Mobile IP—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfmobip_ps1835_TSD_Products_Configuration_Guide_Chapter.html

Note These redundancy modes support MultiProtocol Label Switching (MPLS):

- Route Processor Redundancy (RPR)
- MPLS can coexist with NSF with SSO redundancy, but there is no support for stateful MPLS switchover.

- MPLS Basic, including Provider (P) and Provider Edge (PE) functionality—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html
- MPLS Label Distribution Protocol (LDP)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE
- MPLS LDP - Inbound Label Binding Filtering—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsinbd4.html
- MPLS LSP ping/traceroute and AToM VCCV—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsinbd4.html
- MPLS Traffic Engineering (TE) Fast Reroute (FRR) Link and Node Protection—See these publications:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsfrr24.html

  Note Also see MPLS Traffic Engineering DiffServ Aware (DS-TE).
  MPLS TE FRR Link and Node Protection is not supported on these interface types:
  —Port channel interfaces
  —Switch virtual interfaces (SVIs)
  —Multiple link point-to-point protocol (MLPPP) interfaces
  —Multilink Frame Relay (MLFR or MFR)
- MPLS Traffic Engineering (TE) Interarea Tunnels—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiarea3.html
- MPLS Traffic Engineering DiffServ Aware (DS-TE)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsdserv3.html

  Note Also see MPLS Traffic Engineering (TE) Fast Reroute (FRR) Link and Node Protection.
  MPLS DS-TE is not supported on these interface types:
  —Port channel interfaces
  —Switch virtual interfaces (SVIs)
  —Multiple link point-to-point protocol (MLPPP) interfaces
  —Multilink Frame Relay (MLFR or MFR)
- MPLS Virtual Private Networks (MPLS VPN)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsmvpns.html

- MPLS VPN Carrier Supporting Carrier—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs2scsc.html

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fscsclbl.html

- MPLS VPN ID—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/vpnid2.html

- MPLS VPN Inter-AS IPv4 BGP Label Distribution—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiaslbl.html

- MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) —See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiaslbl.html

  Note The MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) feature also provides EIGRP support for VRF Lite.

- MPLS VPN—OSPF and Sham-Link Support—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_sham_link.html

- MQC: distribution of remaining bandwidth (supported only on WAN ports)—You configure QoS features on an interface using the modular QoS CLI (MQC). Using MQC, you create service policies for traffic classes and attach the policies to an interface. You can use MQC to specify how the remaining bandwidth is distributed among the interface or subinterface output queues. The remaining bandwidth is the available bandwidth left on an interface or subinterface after all guaranteed traffic is accounted for. The amount of remaining bandwidth available for use is determined by the excess information rate (EIR) configured for the queue.

  The **bandwidth remaining percent** command allows you to configure the remaining bandwidth for output queues. The aggregate of all user-configured EIR bandwidth percentages cannot exceed 100 percent. If the aggregate of all remaining bandwidth is less than 100 percent, the remainder is evenly split among user queues (including the default queue) that do not have a remaining bandwidth percentage configured. The minimum EIR value of each output queue is 1.

  This example shows how to use the **bandwidth remaining percent** command to distribute percentages of remaining bandwidth to various traffic classes in a policy map:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map myPolicy
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20
Router(config-pmap-c)# class prec1
Router(config-pmap-c)# bandwidth remaining percent 30
Router(config-pmap-c)# class prec2
Router(config-pmap-c)# bandwidth remaining percent 10
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# end
Router# show policy-map myPolicy
  Policy Map myPolicy
    Class prec1
         bandwidth remaining percent 30
    Class prec2
         bandwidth percent 50
         bandwidth remaining percent 10
    Class class-default
         bandwidth remaining percent 20
```

```
Router#
```

- Multicast-VPN: Multicast Support for MPLS VPN—See this publication:

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

- Multi-VRF for CE Routers (VRF Lite) with IPv4 forwarding between VRFs interfaces, IPv4 ACLs, and IPv4 HSRP—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE

  Note Multi-VRF for CE Routers (VRF Lite) with the PFC3B supports multi-VRF CE functionality with EIGRP, OSPF, BGP and RIPv2 routing protocols running on a per VRF basis. Static routes are also supported. Supported on LAN and WAN ports.

- Multiple-Hot Standby Routing Protocol (mHSRP)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfip.html

- Multiple-path Unicast Reverse Path Forwarding (Unicast RPF) in hardware—See this publication:

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

- Multipoint bridging (MPB)—See these publications:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_the_VFI_in_the_PE

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/atm.html

- NAC - L2 IP; Network Admission Control (NAC) Layer 2 Layer 2 IP validation—See this publication:

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

- NetFlow Aggregation (hardware-assisted)—See this publication:

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

- NetFlow - Bridged Flow Statistics—See this publication:

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

- NetFlow Data Export (NDE)—See this publication:

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

- NetFlow Data Export (NDE) enhancement—Population of the NDE Layer 4 source port field with the ICMP type and code values.

- Netflow Multiple Export Destinations:
  - Allows entry of a second **ip flow-export destination** command
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/nde.html
- NetFlow v9 Export Format, including NetFlow Export of BGP Nexthop Information—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/12-2sx/cfg-nflow-data-expt.html
- NetFlow multicast support:
  - Supported only with NetFlow v9 export format.
  - See this publication:

    http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/12-2sx/cfg-nf-multi-acctg.html
  - The NetFlow Multicast Support document contains a prerequisite that does not apply when configuring NetFlow multicast support with Release 12.2(18)ZY and later 12.2ZY releases:

    You do not need to configure multicast fast switching or multicast distributed fast switching (MDFS); multicast CEF switching is supported with Release 12.2(18)ZY and later 12.2ZY releases.
- Network Address Translation (NAT) and Port Address Translation (PAT) for IPv4 unicast and multicast traffic (hardware-assisted)—Note the following information about hardware-assisted NAT:
  - PFC3B mode supports NAT and PAT for UDP traffic.
  - The PFC3B does not support NAT or PAT for multicast traffic.
  - The PFC3B does not support NAT or PAT configured with a route map that specifies length.
  - The PFC3B does not support NAT or PAT configured with a route map that specifies static translations.
  - When you configure NAT or PAT and NDE on an interface, the PFC3B sends all traffic in fragmented packets to the PISA to be processed in software. (CSCdz51590)

  To configure NAT or PAT, refer to the Cisco IOS IP Configuration Guide, Release 12.2, "IP Addressing and Services," "Configuring IP Addressing," "Configuring Network Address Translation," at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfipadr.html

  For information about configuring NAT or PAT with route maps, refer to this publication:

  http://www.cisco.com/en/US/tech/tk648/tk361/technologies_q_and_a_item09186a00800e523b.shtml

  To prevent a significant volume of NAT or PAT traffic from being sent to the PISA, due to either a DoS attack or a misconfiguration, enter the **mls rate-limit unicast acl** {**ingress** | **egress**} command described in this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/M1.html

  (CSCea23296)

- Optimized ACL logging—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/acl.html
- OSPF Forwarding Address Suppression in Translated Type-5 LSAs—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/12-2sx/iro-for-add-sup.html
- OSPF Inbound Filtering Using Route Maps with a Distribute List—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/routmap.html
- OSPF Incremental Shortest Path First (i-SPF)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfispf.html
- OSPF Limit on Number of Redistributed Routes—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsoredis.html
- OSPF link state database overload protection—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfopro.html
- OSPF link-local signaling (LLS) per interface basis—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospflls.html
- OSPF MIB support of RFC 1850 and latest extensions—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospflls.html
- OSPF Shortest Path First Throttling—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_spftrl.html
- OSPF support for BFD over IPv4—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  Note Also see "Bidirectional Forwarding Detection (BFD) standard implementation."
- OSPF Support for Fast Hellos—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fasthelo.html
- OSPF support for forwarding adjacencies over MPLS traffic engineered tunnels—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospffa.html
- OSPF Support for Link State Advertisement (LSA) Throttling—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsolsath.html
- OSPF support for unlimited software VRFs per provider edge (PE) router—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/12-2sx/iro-un-sw-vrfs.html
- Packet classification based on layer3 packet-length (supported on WAN ports)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_classn/configuration/12-2sx/qos-classn-ntwk-trfc.html
- Per Interface Sticky ARP—See this publication:

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

- Per port MAC limiting—See the **mac-address-table limit** command in this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.html

- Per VLAN load balancing for advanced QinQ service mapping—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Configuring_Strict_Priority_Low_Latency_Queuing_(LLQ)_Support_on_the_OSM-24GE-WAN

- PIM snooping DR flooding enhancement—See this publication:

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

- PIM Snooping—See this publication:

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

- PKI AAA authorization using the entire subject name—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html

- Policy-based routing (PBR; hardware-assisted) for route-map sequences that use the **match ip address**, **set ip next-hop**, and **set ip default next-hop** PBR keywords.

  To configure PBR, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.2, “Classification,” “Configuring Policy-Based Routing,” at this URL:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpbr_ps1835_TSD_Products_Configuration_Guide_Chapter.html

  When configuring PBR, follow these guidelines and restrictions:

  - The PFC provides hardware support for PBR configured on a tunnel interface.
  - The PFC does not provides hardware support for PBR configured with the **set ip next-hop** keywords if the next hop is a tunnel interface.
  - If the PISA address falls within the range of a PBR ACL, traffic addressed to the PISA is policy routed in hardware instead of being forwarded to the PISA. To prevent policy routing of traffic addressed to the PISA, configure PBR ACLs to deny traffic addressed to the PISA. (CSCse86399)
  - Any options in Cisco IOS ACLs that provide filtering in a PBR route map that would cause flows to be sent to the PISA to be switched in software are ignored. For example, logging is not supported in ACEs in Cisco IOS ACLs that provide filtering in PBR route maps.
  - PBR traffic through switching module ports where PBR is configured is routed in software if the switching module resets. (CSCee92191)

- —See this publication:

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

- Port Security, including:
  - Port security on 802.1Q tunnel ports
  - Port security on private VLAN ports
  - Port security on trunk ports
  - Port security with 4096 secure MAC addresses
  - Port security with sticky MAC addresses
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/port_sec.html
- PortFast BPDU filtering—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/stp_enha.html
- Private VLANs—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/pvlans.html
- Protocol-Independent MAC ACL Filtering—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/qos.html
- QoS, including:
  - Ignore Port Trust
  - Per-VLAN and CoS-based QoS filtering in MAC ACLs
  - PFC QoS features on tunnels
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/qos.html
- QoS Data Export—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/qos_sde.html
- QoS: Aggregated DSCP / Precedence Values for WRED—Aggregates multiple DSCP or IP Precedence values for a single minimum or maximum threshold and marks probability when specifying WRED parameters for 7600-SIP-400 ATM SPAs.
- QoS: ingress shaping on FlexWAN module interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpbr_ps1835_TSD_Products_Configuration_Guide_Chapter.html
- QoS: percentage based policing on WAN ports—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12spctpg.html
- Query mode definition per trustpoint—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html

- Query multiple servers during certificate revocation check—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html

- RADIUS Load Balancing (RLB) IMSI sticky—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cfg-auth-rev-cert.html

- Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)—See this publication:

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

- Received ToS byte preservation—See this publication:

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

- Remote SPAN—See this publication:

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

- RFC-1483 Spanning-Tree Interoperability Enhancements on WAN ports—See these publications:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/atm.html

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- RFC-1483 Bridging on FlexWAN—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- RFC-1490 bridging on FlexWAN interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- RFC-1889 Compressed Real-Time Protocol (cRTP; supported on FlexWAN interfaces)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcrtp.html

  Note cRTP is not supported on MLPPP bundled links.

- Router-Port Group Management Protocol (RGMP)—See this publication:

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

- RSVP Interface-based Receiver Proxy—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/rsvpprox.html

- RSVP Refresh Reduction and Reliable Messaging—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsrelmsg.html

- RSVP Scalability Enhancements—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/12-2sx/rsvp-scalability.html

- RSVP Scalability Enhancements—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/12-2sx/rsvp-scalability.html

- SafeNet IPsec VPN client support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/12-2sx/sec-safenet-supp t.html

- SCP health monitoring for enhanced-FlexWAN—The SCP health monitor feature provides improved debugging capabilities for problems that cause WAN module resets because of SCP keepalive failures.

- Secure Copy (SCP)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-secure-copy.h tml

- Secure Shell (SSH) Version 2 server support in k9 images—By default, the k9 images support both SSHv1 connections and SSHv2 connections. To restrict connections to either SSHv1 or SSHv2, enter the **ip ssh mode** [**v1** | **v2**] global configuration mode command. Except for the **v1** and **v2** keywords for the **ip ssh mode** command, you configure SSHv2 in the same way as SSHv1. See this publication for more information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-usr-ssh-12-2s x-book.html

  For information about SSHv1 client support, refer to the following publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-usr-ssh-12-2sx-bo ok.html

- Secure Shell SSH Version 2 Client Support—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-usr-ssh-12-2sx-bo ok.html

- Server load balancing (SLB), including:
  - SLB: interface-aware
  - SLB: stateful failover within single chassis
  - See this publication:

    http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_ssh/configuration/12-2sx/sec-usr-ssh-1 2-2sx-book.html

  Note Web Cache Control Protocol (WCCP) Layer 2 PFC redirection is supported with Cisco IOS SLB. Other WCCP configurations are not compatible with Cisco IOS SLB.

- Show diagnostic sanity—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/diag s.html

- Show Top-N—See this publication:

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

- SNMP ifindex persistence—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/ifind x.html

- Source Specific Multicast (SSM) Mapping—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_igmp/configuration/12-2sx/imc_ssm_mapping.html

  Note Do not configure SSM mapping in a VLAN that supports IGMPv3 multicast receivers.

- Source-Specific Multicast with IGMPv3, IGMP v3lite, and URL Rendezvous Directory (URD)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfssm.html

- SPAN destination port permit list—See this publication:

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

- Spanning tree PortFast, UplinkFast, and BackboneFast, and Root Guard Feature—See this publication:

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

- Spanning Tree Protocol—See this publication:

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

- SRR (Shaped Round Robin)—See this publication:

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

- SSM mapping for IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipmulti_pim/configuration/15-mt/ip6-mcast-ssm-map.html

- Standard Domain Naming System (DNS) support—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfipadr.html

- Strict priority low latency queueing (LLQ) on WAN ports—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Configuring_Strict_Priority_Low_Latency_Queuing_(LLQ)_Support_on_the_OSM-24GE-WAN

- Sub interface features - phase 1—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/layer3.html

- Switched Port Analyzer (SPAN)—See this publication:

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

- TCP intercept (hardware-assisted)—See this publication:

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

- TDR cable diagnostics—TDR is supported on these switching modules:
  - WS-X6148-GE-TX

  - WS-X6148V-GE-TX
  - WS-X6148-GE-45AF
  - WS-X6548-GE-TX
  - WS-X6548V-GE-TX
  - WS-X6548-GE-45AF
  - WS-X6148A-GE-TX
  - WS-X6148A-GE-45AF
  - WS-X6148A-RJ-45
  - WS-X6148A-45AF

Note TDR can test cables up to a maximum length of 115 meters.

See these publications:

  - The "Checking the Cable Status Using the TDR" section of the "Configuring Interfaces" chapter at this URL:

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

  - The **test cable-diagnostics** command in the command reference at this URL:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.html

- Traffic storm control—See this publication:

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

- UDI - Unique Device Identifier—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/12-2sx/Unique_Device_Identifier_Retrieval.html

- Unicast flood blocking (UFB)—See this publication:

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

- UniDirectional Link Detection—See this publication:

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

- Uni-Directional Link Routing (UDLR)—See this publication:

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

- User-based microflow policing—See the procedures in this publication for information about configuring microflow policing based on either source or destination addresses:

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

- VLAN Access Control Lists (VACLs), including, VACL capture—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/vacl.html
- VACL Deny Logging—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/secure.html
- Virtual Router Redundancy Protocol (VRRP)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-vrrp.html
- VLAN Trunk Protocol (VTP) and VTP domains—See this publication:
- http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/vtp.html
- VLANs over IP unnumbered sub-interfaces—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-i4.html#GUID-833D9D25-1E04-4430-84D8-1AA836DE4745
- VLANs, including VLAN translation—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/configuration/guide/vlans.html
- Voice over Frame Relay (VoFR) FRF.11 and FRF.12 (supported on FlexWAN interfaces)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/vvfvofr.html

Note Because the Catalyst 6500 series switches do not support voice modules, they can act only as a VoFR tandem switch when FRF.11 or FRF.12 is configured on the FlexWAN module.

- Web Cache Control Protocol (WCCP)—These WCCP features are supported:
  - WCCP Layer 2 PFC Redirection
  - WCCP Redirection on Inbound Interfaces
  - WCCP Version 1
  - WCCP Version 2
  - See this publication:

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

Note Release 12.2ZY does not support these WCCP features:
—WCCP L2 Return
—WCCP Layer 2 Redirection/Forwarding
—WCCP Mask Assignment
—WCCP VRF Support

Unsupported Features and Commands

- Hardware—See the "Unsupported Hardware" section on page 30.
- Egress multicast replication
- Multicast replication mode detection
- All fabric configuration commands
- Route Processor Redundancy Plus (RPR+) redundancy
- These QoS interface commands are not supported on SPA interfaces:
  - **traffic shape**
  - **priority-group**
  - **custom-queue-list**
  - **tx-queue-limit**
  - **fair-queue**
  - **random-detect**
  - **rate-limit**
  - **tx-ring-limit**
  - **max-reserved-bandwidth**
- These QoS interface commands are not supported on FlexWAN interfaces:
  - **traffic shape**
  - **priority-group**
  - **custom-queue-list**
  - **tx-queue-limit**
- Random Sampled NetFlow (**flow-sampler** commands)
- These software features are not supported:
  - Apollo Domain
  - AppleTalk EIGRP
  - Banyan Vines
  - Exterior Gateway Protocol (EGP)
  - HP Probe
  - IEEE 802.10 VLANs
  - IGRP
  - LAN Extension
  - Netware Asynchronous Services Interface (NASI)
  - Next Hop Resolution Protocol (NHRP) for IPX
  - Novell Link-State Protocol (NLSP)
  - Simple Multicast Routing Protocol (SMRP) for Appletalk
  - Xerox Network Systems (XNS)
  - Xremote

- Generic routing encapsulation (GRE) tunnel IP source and destination VRF membership (the **tunnel vrf** command). (CSCee39138)
- Warm Reload (CSCef06158)
- ARP Optimization (CSCef30539)
- Exterior Border Gateway Protocol (eBGP) multihop over CSC-PE interfaces (CSCea83165)
- Ability to accept ingress traffic on SPAN destination ports (Cisco IOS software equivalent of **set span ... inpkts enable**).
- Automatic QoS
- Unknown unicast flood protection
- Commands to globally disable EtherChannel or trunking
- **write tech-support** command
- Cisco IOS software equivalent of the **set port host** command
- Disable port startup option
- Clear counters per port or clear QoS statistics
- System warning and error counter enhancements implemented in Catalyst software release 6.1(1)
- Option for no VTP support
- Command to display the port MAC address
- Port security timer enhancement
- System warnings on port counters
- VLAN Management Policy Server (VMPS) client or server
- Cisco IOS MAC-layer access control lists (ACLs)
- Accelerated server load balancing (ASLB)
- Hot Standby Router Protocol (HSRP) between redundant supervisor engines (the redundant supervisor engine and PISA are in standby mode—HSRP to external routers is supported)
- Multi-Instance Spanning Tree Protocol (MISTP); IEEE 802.1s MST is supported
- Common Open Policy Server (COPS)
- Except to support tunnels, Resource ReSerVation Protocol (RSVP)
- GARP VLAN Registration Protocol (GVRP)
- GARP Multicast Registration Protocol (GMRP)
- Commands present in the CLI, but not supported:
  - ipv6 cef accounting
  - ip cef accounting
  - module provision

Limitations and Restrictions

These sections list limitations and restrictions for the Cisco IOS for the Catalyst 6500 series switches and Cisco 7600 series routers:

Restrictions Removed by the PFC3B

The PFC3B removes these restrictions that were present with other policy feature cards:

- You can configure features to use up to 3 different flow masks.
- You can configure more than 1 Gateway Load Balancing Protocol (GLBP) group.
- You can configure up to 255 unique HSRP group numbers.
- You can configure a separate MAC address on each interface.
- You can configure Unicast RPF check without reducing the number of available CEF entries.
- You can configure port-based and VLAN-based QoS on a per-port basis on the WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules.

General Limitations and Restrictions

This section describes general limitations and restrictions:

- When a redundant supervisor engine is in standby mode, the Ethernet ports on the redundant supervisor engine are always active.
- A supervisor engine that has one ROMMON version might boot at a different rate from a supervisor engine that has another ROMMON version. To ensure that redundant supervisor engines boot at the same rate, install the same ROMMON version on both supervisor engines. (CSCef29567)
- All Ethernet LAN ports on all modules, including those on a redundant supervisor engine, support EtherChannel (maximum of eight interfaces) with no requirement that the ports be contiguous.
- All Ethernet ports on all modules support 802.1Q VLAN trunking.
- These modules do not support Inter-Switch Link (ISL) VLAN trunking:
  - WS-X6502-10GE
  - WS-X6548-GE-TX
  - WS-X6148-GE-TX

  The ports on all other modules support ISL VLAN trunking.
- When you add a member port that does not support ISL trunking to an EtherChannel, Cisco IOS software automatically adds a **switchport trunk encapsulation dot1q** command to the port-channel interface to prevent configuration of the EtherChannel as an ISL trunk. The **switchport trunk encapsulation dot1q** command is inactive when the EtherChannel is not a trunk.

- The link state messages ("LINK-3-UPDOWN" and "LINEPROTO-5-UPDOWN") are disabled by default. See the **logging event link-status** global and interface configuration commands in this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/I1.html

  (CSCeb06765)

- RSVP Traffic Engineering (TE) tunnels might stop forwarding traffic in hardware if Label Distribution Protocol (LDP) is not enabled globally. This problem occurs when a path change requires that ternary content addressable memory (TCAM) table entries be updated for all the prefixes routed over the TE tunnel. The TCAM entries are not updated correctly.

  Workaround: If you enable LDP globally, a TE tunnel rewrite is created for each prefix. The hardware programming code receives an update for each prefix and will be able to program the TCAM entries correctly. (CSCee77417)

- The **show interface** command displays the giants field, which indicates the number of packets that are larger than 1518 octets. For Layer 2 trunk ports configured with an MTU size that supports jumbo frames on WS-X6704-10GE, WS-X6748-SFP, WS-X6724-SFP, and WS-X6748-GE-TX switching modules, the giants field always indicates zero. This is a display issue and does not impact the actual handling of jumbo frames on these ports.

  Workaround: None. (CSCek23592)

- With the BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN feature configured, do not attach output service policies to VRF interfaces. (CSCsb25509)

- To reduce CPU utilization during ACL configuration changes, use named ACLs instead of numbered ACLs whenever possible, because the ACL merge algorithm runs each time you change an ACE in a numbered ACL. With named ACLs, the ACL merge algorithm runs only when you exit the named ACL configuration mode.

- With bidirectional PIM configured, you cannot configure Bootstrap Router (BSR) rendezvous point (RP) candidates.

  Workaround: Use AutoRP or static RP. (CSCeg29898)

- Unbalanced load-sharing between the two banks of the Layer 2 forwarding engine MAC table for non-statistical distributions of data-frame MAC Layer addresses causes a fractional performance degradation. (CSCec02266)

- With a PFC3B, EoMPLS ports cannot be SPAN sources. (CSCed51245)

- IPsec in software on the PISA is supported only for administrative connections to Catalyst 6500 series switches and Cisco 7600 series routers.

- With a PFC3B, you can either set DSCP in a packet or apply an MPLS tag to the packet, but cannot do both. You cannot set DSCP in a packet and then apply an MPLS tag to that packet. (CSCef19599)

- On a Supervisor Engine 2 with several hundred Layer 3 VLAN interfaces configured and with Rapid-Per-VLAN-Spanning Tree (Rapid-PVST) configured, after a change in the Layer 2 topology (for example, a link coming up), there might be unacceptably high CPU utilization that prevents Rapid-PVST from sending BPDUs on time in all VLANs. (CSCed52310)

- There is no hardware support for fragmented multicast VPN traffic. (CSCef08631)

- When a port becomes a member port of a Layer 2 EtherChannel, any service policy on that member port is displayed by the **show mls qos ip** command as being on the port-channel interface, but the service policy is not applied to the EtherChannel. (CSCec34784)

- The time taken to execute the **show spanning-tree** interface command is proportional to the number of VLANs configured. With many VLANs configured, there might be a noticeable delay in the output of the command while Cisco IOS scans the VLANs for spanning tree ports. (CSCec65860)
- If you set the MTU size on an LACP port-channel interface, the configured MTU size propagates to the member ports. If you change the MTU size on some of the member ports of an LACP EtherChannel, the change does not propagate to the port-channel interface. The ports configured with a different MTU size than the port-channel interface form a secondary LACP EtherChannel. The port-channel interface of a secondary LACP EtherChannel is not configurable. (CSCed18149)
- See this publication for information about the supported IPv6 address formats:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/I1.html

  (CSCed30692)
- The PFC3B incorrectly apply egress IP ACLs to MPLS-tagged traffic. (CSCed29392, CSCed16560)
- With an ingress policer, the PFC3B overpolices tunnel-decapsulated packets because of the tunnel-packet length. (CSCec71389)
- ToS rewrites for bridged multicast packets do not work when TTL-failure rate limiting is configured. (CSCed07399)
- With an EIGRP default network configured, if you remove the referencing network, the default route programming might remain.

  Workaround: Use 0.0.0.0/0 as the default route or avoid entering the **ip default-network** command. Clear the EIGRP neighbors to recover. (CSCea70203)
- RPR does not synchronize configuration done through SNMP to the redundant supervisor engine. (CSCeb07866, CSCea72373)
- If the PISA address falls within the range of a PBR ACL, traffic addressed to the PISA is policy routed in hardware instead of being forwarded to the PISA. To prevent policy routing of traffic addressed to the PISA, configure PBR ACLs to deny traffic addressed to the PISA. (CSCse86399)
- SPAN and RSPAN destination ports transmit VACL-redirected traffic. (CSCea57673)
- When you apply both ingress policing and egress policing to the same traffic, both the input policy and the output policy must either mark down traffic or drop traffic. PFC QoS does not support ingress markdown with egress drop or ingress drop with egress markdown. (CSCea23571)
- PFC QoS does not rewrite the payload ToS byte in tunnel traffic.
- The PFC3B does not apply egress policing to traffic that is being bridged to the PISA.
- The PFC3B does not apply egress policing or egress DSCP mutation to multicast traffic from the PISA.
- PFC QoS does not rewrite the ToS byte in bridged multicast traffic.
- The PISA supports tunnels configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT (for inside to outside translation), TCP intercept, context-based access control (CBAC), and encryption.
- When you configure NAT and NDE on an interface, the PFC3B sends all traffic in fragmented packets to the PISA to be processed in software. (CSCdz51590)
- The PFC3B does not provide hardware switching for ICMP traffic if you configure NAT.

- If you configure Unicast RPF check to filter with an ACL, the PFC determines whether or not traffic matches the ACL. The PFC sends the traffic denied by the RPF ACL to the PISA for the Unicast RPF check. Packets permitted by the ACL are forwarded in hardware without a Unicast RPF check. (CSCdz35099)
- The PFC3B does not provide hardware supported Unicast RPF check for policy-based routing (PBR) traffic. (CSCea53554)
- If you have a network device in your network with MAC address reduction enabled, you should also enable MAC address reduction on all other Layer-2 connected network devices to avoid undesirable root bridge election and spanning tree topology issues.

  When MAC address reduction is enabled, the root bridge priority becomes a multiple of 4096 plus the VLAN ID. With MAC address reduction enabled, a switch bridge ID (used by the spanning-tree algorithm to determine the identity of the root bridge, the lowest being preferred) can only be specified as a multiple of 4096. Only the following values are possible: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440.

  If another bridge in the same spanning-tree domain does not run the MAC address reduction feature, it could win root bridge ownership because of the finer granularity in the selection of its bridge ID.
- Traffic flow and SNMP connectivity is interrupted briefly if you perform an online insertion and removal (OIR) that changes the number of fabric-enabled modules so that the switch must use a different fabric channel switching mode. (CSCdx39882)
- The Ethernet port ASICs drop frames that are invalid (for example, frames that are shorter than the minimum valid length). The Ethernet port ASICs do not keep a count of dropped frames. (CSCdx14209)
- Any options in Cisco IOS ACLs that provide filtering in a policy-map class that would cause flows to be sent to the PISA to be switched in software are ignored. For example, logging is not supported in ACEs in Cisco IOS ACLs that provide filtering in QoS policy-map classes.

  The PFC does not provide QoS for flows that match an ACE in a Cisco IOS ACL configured with options that cause the flows to be sent to the PISA to be switched in software, except when the Cisco IOS ACL provides filtering in a QoS policy-map class. For example, the PFC does not provide QoS for flows that match an ACE in a Cisco IOS ACL with logging configured. (CSCds72804)
- For multicast flows, the PFC does not provide Layer 3 switching on output interfaces with MTU sizes smaller than the flow's input interface MTU size.

  Workaround: Configure the same MTU size on both the input and output interfaces. (CSCds42685)
- Entering the **clear mls qos** command affects the policing token bucket counters and might briefly allow traffic to be forwarded, which would otherwise be policed. (CSCdt40470)
- Catalyst 6500 series switches and Cisco 7600 series routers do not support:
  - Integrated routing and bridging (IRB)
  - Concurrent routing and bridging (CRB)
  - Remote source-route bridging (RSRB)
- Use bridge groups on VLAN interfaces, sometimes called fall-back bridging, to bridge nonrouted protocols. Bridge groups on VLAN interfaces are supported in software on the PISA.
- Catalyst 6500 series switches and Cisco 7600 series routers do not support the IEEE bridging protocol for bridge groups. Configure bridge groups to use the VLAN-bridge or the DEC spanning-tree protocol.
- Ingress IP Packets with TTL=1 that are not addressed to the PISA and that match QoS filtering parameters might cause overpolicing of other ingress traffic on the same ingress interface.

- When the outgoing interface list for group G traffic transitions to null on a last-hop multicast router, the router sends a (*,G) prune message to the PIM neighbor toward the rendezvous point (RP) to stop the flow of group G traffic (if any) down the shared tree, but does not send an (S,G) prune message to stop the flow of traffic down the shortest path tree (SPT). The transition of the outgoing interface list to null does not trigger an (S,G) prune message. (S,G) prune messages are triggered by the arrival of (S,G) traffic.

  If the last-hop multicast router is a Catalyst 6500 series switch, traffic is forwarded in hardware. In most cases, RPF-MFD is installed for the (S,G) entries. The PISA does not see the multicast traffic flowing down the SPT and does not send any traffic-triggered (S,G) prunes to stop the flow of traffic down the SPT. This situation does not have any adverse effect on the PISA because the PFC processes and drops the unwanted (S,G) traffic.
- The **ip multicast rate-limit** command is not supported on LAN ports. (CSCds22281)
- Catalyst 6500 series switches and Cisco 7600 series routers do not support network booting.
- The IP HTTP server feature is disabled by default. Enter the **ip http server** command to use the feature.
- For LAN switching modules, the Cisco IOS **show controllers** command generates no output on a Catalyst 6500 series switch or Cisco 7600 series router. Enter the **show module** command instead.
- To avoid the case where all traffic is out of profile, the burst size specified in a QoS policing rule must be at least as large as the maximum packet size permissible in the traffic to which the rule is applied.
- By default, the PISA sends Internet Control Message Protocol (ICMP) unreachable messages when a packet is denied by an access group.

  With the **ip unreachables** command enabled (which is the default), the supervisor engine drops most of the denied packets in hardware and sends only a small number of packets (10 packets per second, maximum) to the PISA to be dropped, which generates ICMP-unreachable messages.

  To eliminate the load imposed on the PISA CPU by the task of dropping denied packets and generating ICMP-unreachable messages, you can enter the **no ip unreachables** interface configuration command to disable ICMP unreachable messages, which allows all access-group denied packets to be dropped in hardware.
- MAC address-based Cisco IOS ACLs are not supported for packets that are Layer 3 switched in hardware. MAC address-based Cisco IOS ACLs will be applied on software-switched packets.
- If you enable multicast routing globally, then you should also enable multicast routing (using the **ip pim** command) on all Layer 3 interfaces on which you anticipate receiving IP multicast traffic. This command causes the packets to be sent to the process switching level to create the route entry. If you disable multicast routing on the RPF interface, the entry cannot be created and the packet is dropped. If the source traffic rate exceeds what can be handled by the process level, it can have an undesirable impact on the system. For example, routing protocol packets, such as EIGRP hello packets, might get dropped.
- 24-port 100FX switching modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower only support IEEE 802.1Q VLAN trunking; they do not support ISL trunking. Do not configure ISL trunks on 24-port 100FX switching modules (WS-X6224-100FX-MT) with a hardware version of 1.1 or lower. The restriction against ISL VLAN trunking is the only known problem with hardware version 1.1 or lower of these modules. If you do not require ISL VLAN trunking, these modules are fully functional. The ISL VLAN trunking problem has been corrected in hardware version 1.2 or later. If you want to return a WS-X6224-100FX-MT module with a hardware version of 1.1 or lower, contact Cisco Systems. You can identify WS-X6224-100FX-MT hardware versions using one of these two methods:

  - Command-line interface (CLI) method—Enter the **show module** command to identify the hardware version of the WS-X6224-100FX-MT module.
  - Physical inspection method—The part number is printed on a label on the outer edge of the component side of the module. Versions 73-3245-04 or lower do not support ISL trunking.

- The RJ-21 connectors on the 48-port 10/100TX switching module (WS-X6248-TEL) do not support Category 3 RJ-21 telco connectors and cabling. Category 3 connectors and cabling cause carrier sense errors. Use Category 5 RJ-21 telco connectors and cables (the module is keyed for Category 5 telco connectors and cables).
- The in and out ports displayed in Layer 3 table entries are set by the hardware at the time the entry is created. They are not guaranteed to be accurate in case multiple flows use the same entry (for example, if the flow mask is **Dest-only** and some kind of load sharing is active) or if the source or destination of the Layer 3 entry moves in the Layer 2 topology. The port information is not always available when the Layer 3 entry is established. This is the case if the destination port of the rewritten packet is unknown when the shortcut is created.
- For EtherChannels, you can configure the QoS trust state and default CoS directly on the EtherChannel interface with the **mls qos trust** or **mls qos cos** commands, respectively. These two parameters must be the same for all physical interfaces in the channel. No other QoS queueing configuration commands can be applied to EtherChannel interfaces. Other QoS queueing configuration commands can be applied, however, to individual EtherChannel physical interfaces. After the physical interfaces are bundled into an EtherChannel, QoS classification, marking, and policing by the Policy Feature Card (PFC) for the channel packets is determined by the service-policy attached to the EtherChannel interface. The service policies attached to the individual physical interfaces of the EtherChannel do not matter. The same is true for the port-based and VLAN-based QoS state of the EtherChannel interface. You can disable the PFC QoS features using the **no mls qos** interface configuration command on the EtherChannel interface.
- The maximum recommended number of Layer 3 multicast entries is 10,000. The maximum recommended number of multicast entries supported in the Layer 2 forwarding table is 12,000.
- After enabling Protocol Independent Multicast (PIM) on an interface, you need to enter the **ip mroute-cache** command on the interface to enable multicast fast-switching. If you have “no ip mroute-cache” configured, multicast packets that are not hardware switched will go to the process level that increases the load on the router.
- The **show ibc** command misleadingly displays Inter-Switch Link (ISL) trunk status as “disabled” and the GBIC as “missing,” because the IBC in a Catalyst 6500 series switch or Cisco 7600 series router is the internal electrical interface between the switch processor and the route processor. Trunk and media types are not given for this type of interface. (CSCdp21121, CSCdp21380)
- The **show access-list** command displays statistics only for traffic that matches ACLs processed in software on the PISA. The **show access-list** command does not display statistics for traffic that matches an ACL supported in hardware on the PFC. (CSCdt14386)
- The **show interface stats** command does not display statistics for traffic that is Layer 3 switched by the PFC. The **show interface** command displays statistics (labelled **L2** and **L3**) for traffic that is Layer 3 switched by the PFC. (CSCds41388)
- To avoid subjecting routing protocol packets to policy-based routing, configure filtering in route maps so that it does not match routing protocol packets. (CSCds44369)
- Microflow policing does not support policing of identical flows arriving on different interfaces simultaneously. Attempts to do so lead to incorrectly policed flows. (CSCdt72147)
- Because the system does not boot from PISA bootflash, if the NVRAM configuration is not valid (or not present), the **service config** option defaults to “on,” and the service config feature is enabled after the **erase startup-config** command is issued. (CSCdp12598)

- In a VTP version 1 domain with some switches running Catalyst software and some switches running Cisco IOS software on both the supervisor engine and the PISA, if the VLANs were created on a switch running Catalyst software and then propagated through VTP to switches running Cisco IOS software, if you enter commands on the switches running Cisco IOS software to configure VTP version 2, you might receive messages about invalid VLAN configuration.

  Workaround: Perform VLAN configuration on a switch running Catalyst software or enter VLAN configuration commands to correct all VLAN configuration errors reported in the messages. (CSCdp47622)
- The **interface range** command is not supported by the HTTP user interface. The command will execute on only the first interface in the specified range. Do not use the **interface range** command with the HTTP interface. (CSCdm54471)
- When using the UplinkFast feature, the system does not send out the dummy multicast packets used to notify upstream users of forwarding-path changes. Normal Layer 2 aging is used to delete invalid entries. (CSCdm65881)
- Running an SNMP topology discovery application might cause high CPU utilization. (CSCef12458)
- Following power up or a reload, you might see "%ALIGN-3-TRACE: -Traceback=" messages. (CSCed76016)
- A high CPU usage might occur when ERSPAN jumbo frames exceed the frame size of the adjacency MTU of the egress interface. The ERSPAN packets are processed by the PISA, which causes the CPU usage to increase. The ERSPAN packets are dropped because the Don't Fragment (DF) bit is set.

  Workaround: The MTU failure packets are rate-limited when you enter the global configuration command **mls rate-limit all mtu-failure**. (CSCsd55182)
- When traffic with a multicast destination IP address and a broadcast destination MAC address is replicated to one or more VLANs, the destination MAC addresses in the replicated traffic are not rewritten, which preserves the broadcast destination MAC address. Systems that receive the traffic classify it as broadcast traffic instead of multicast traffic. IGMP snooping cannot constrain broadcast traffic.

  Workaround: none. (CSCse07679)

FlexWAN Limitations and Restrictions

- PISA-accelerated features are not supported on FlexWAN module interfaces.
- FlexWAN ports do not support SPAN or RSPAN.
- MPLS on the FlexWAN module does not support Virtual Private LAN Service (VPLS).
- On FlexWAN ports configured for EoMPLS, the counters displayed by the **show mpls** command for parallel links between LERs do not update. (CSCdw04208, CSCdu87648)
- On FlexWAN ports, an EoMPLS virtual circuit stays up when the VLAN interface is down. (CSCdv69982)
- Ethernet over Multiprotocol Label Switching (EoMPLS) per-VLAN traffic shaping does not work with a FlexWAN egress port. (CSCdx10583)
- On FlexWAN ports, an EoMPLS virtual circuit stays up when the VLAN interface is down. (CSCdv69982)
- To use the interfaces on the FlexWAN module, you must enable IP routing on the PISA. (CSCdp34896)

Service Module and IPsec SPA Limitations and Restrictions

- PISA-accelerated features are not supported on service module switch virtual interfaces (SVIs).
- Generating an Revisit, Shamir, and Adelman (RSA) usage key pair with modulo 360 fails.

  Workaround: Use a higher modulo value. (CSCec49861)
- When the NAM is configured as the NDE destination and the NAM is down, the NDE traffic is flooded.

  Workaround: Clear the NDE configuration for the NAM or enter the **clear arp-cache** command. (CSCdy55261)
- You cannot SPAN ingress traffic from the Firewall Services Module (WS-SVC-FWM-1-K9). (CSCec79733)
- With the tunnel MTU size configured to 9216 bytes, tunnel packets larger than 9211 bytes are corrupted.

  Workaround: None. (CSCec04627)

Additional Limitations and Restrictions

Identifier	Technology	Description
CSCso36139	Unknown	PISA-FWSM:Mix MTU on PISA NBAR Protocol-tagging behavior
CSCso83818	Unknown	Nbar: PD not working for Ip-Option pkts.
CSCso83934	Unknown	NBAR AIM ver 6 AOL protocol pdl not classifying packets
CSCsq85641	Unknown	NBAR: AOL messenger classified as http when http proxy configured.
CSCsr15153	Unknown	VACL capture on a Layer2 trunk port not working with Ingress Pisa Policy
CSCsr39414	Unknown	PTS: Netflow features are working in software with PTSacl deny traffic
CSCsy97776	Unknown	Auto discovery QoS stats get cleared on creating a custom protocol
CSCsz00970	Unknown	Unexpected behaviour on usage of AutoQoS suggested policy and class map
CSCsz15987	Unknown	Unknown flows not recognised by NBAR are not exported
CSCsz28860	Unknown	Layer-2 flows are not created when Nbar enabled on corresponding SVI
CSCsz30671	Unknown	PISA features not supported on secondary aggregator of LACP Etherchannel

Caveats

- Resolved Caveats in Release 12.2(18)ZY2, page 125
- Resolved Caveats in Release 12.2(18)ZY1, page 131
- Resolved Caveats in Release 12.2(18)ZY, page 167

Note

- All caveats in Release 12.2(18)S also apply to Release 12.2(18)ZY. See the "Caveats" section in the *Cross-Platform Release Notes for Cisco IOS Release 12.2S* publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html
- All caveats in Release 12.2(17d) also apply to Release 12.2(18)ZY.
- All caveats in Release 12.2(17b) also apply to Release 12.2(18)ZY.
- All caveats in Release 12.2(17a) also apply to Release 12.2(18)ZY.
- For information about Release 12.2(17a), Release 12.2(17b), and Release 12.2(17d), refer to this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html
- All caveats in Release 12.2(14)S also apply to Release 12.2(18)ZY. See the "Caveats" section in the *Cross-Platform Release Notes for Cisco IOS Release 12.2S* publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html
- For information about caveats in Release 12.2(18)SXF and rebuilds, see this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#Caveats_in_Release_12.2(18)SXF_and_Rebuilds
- The caveat information for Release 12.2(18)ZY and rebuilds is updated frequently.
- If you have a Cisco.com account that supports access to the Bug Toolkit, you can search for the most current Release 12.2ZY caveat information at this URL:

  http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

  Select "Catalyst 6000 Series Switches" and then select a 12.2ZY release.

Open Caveats in Release 12.2ZY

Identifier	Technology	Description
CSCsi36204	Unknown	able to configure po256 via IOS startup dialog
CSCsm09533	Unknown	MQC - switchport output policy error msg not clear
CSCsm90876	Unknown	L2PIsa:Port Manager Internal sw Error TBs, adding uplink in to pisa-chan
CSCso05141	Unknown	MQC_REMOVE_POLICY:Failed to remov policy msgs after SSO for shut/ports
CSCso41566	Unknown	URLF: Unexpected reset with a large number of UFS servers configured
CSCso41934	Unknown	NBAR: eMule: file search traffic not classified
CSCso60817	Unknown	PISA: Custom protocol with Static ID setting for NBAR tagging
CSCso81457	Unknown	NBAR: syslog PD error on intf for vlan 0 when ena/dis PD on shut intf
CSCso89069	Unknown	NBAR Unable to undo port-map change for softphone protocol
CSCsq10755	Unknown	PISA:Sup32-8GE port 8,9 and S32-10GE port 3 LED off in admin-down state

Identifier	Technology	Description
CSCsq69769	Unknown	Per-uri mode: More than one URL not filtered per packet
CSCsq90704	Unknown	PISA: NBAR incorrectly classifies remote desktop protocol as edonkey
CSCsr06455	Unknown	Escape character usage inconsistant in NBAR PDLMs
CSCsr07614	Unknown	PISA: Remove CLI command for configuring GRE key for protocol tagging
CSCsr16405	Unknown	NBAR-NAT: FTP data traffic getting classified as eDonkey and unknown.
CSCsr59046	Unknown	NBAR: Yahoo messenger connections on tcp 119 classifies as NNTP
CSCsu04441	Unknown	PTS: trf redirected to PISA w/o accel feature after reconfig switchport
CSCsv35900	Unknown	pm_mp_notify_cp_port_admin_state:Gi5/10 vl_id1025 swidb-> with reload
CSCsw37516	Unknown	bootup PISA Maj Error - test_acl failed(rc=1) for IP (input: L2 redirect
CSCsw50072	Unknown	PTS: L3 non-selected pkts seen by IXP on egress after HA swovr
CSCsz16083	Unknown	Syslog message: autoqos config not synced to the standby
CSCsz46542	Unknown	Flows not recognized by NFC after changing source interface IP
CSCsz93351	Unknown	ARP not working with gig spa
CSCsz94158	Unknown	Disabling urlf will not remove X-list entries and logging functionality
CSCta02845	Unknown	Unexpected behaviour on deleting service policy from autoqos enabled i/f
CSCta08310	Unknown	Rmon event/alarm generated by cos 5 traffic on AutoQos enabled interface
CSCta29897	Unknown	Misclassification of rtp audio & video on creating custom protocol

Resolved Caveats in Release 12.2(18)ZYA3b

Resolved Infrastructure Caveats

- CSCti25339—Resolved in 12.2(18)ZYA3c

  Symptoms: Cisco IOS device may experience a device reload.

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

  Workaround: There is no workaround.

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

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

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

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

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

Resolved IPServices Caveats

- CSCtd10712—Resolved in 12.2(18)ZYA3c

  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 LegacyProtocols Caveats

- CSCth69364—Resolved in 12.2(18)ZYA3c

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

  Cisco has released free software updates that address this vulnerability.

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

Other Caveats Resolved in Release 12.2(18)ZYA3c

Identifier	Technology	Description
CSCtl63017	Cisco IOS	Sup32 PISA - Packets to local IP address not reaching CPU
CSCtn59243	Security	Tunnel interfaces remain down after WAN recovery.

Resolved Caveats in Release 12.2(18)ZYA3b

Resolved WAN Caveats

- CSCtd75033—Resolved in 12.2(18)ZYA3b

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- NTP Access Group

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

  ```
  !--- Configure trusted peers for allowed access
  ```

```
access-list 1 permit 171.70.173.55
!--- Apply ACE to the NTP configuration
ntp access-group peer 1
```

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

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

– Infrastructure Access Control Lists

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

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

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

```
!---
!--- Feature: Network Time Protocol (NTP)
!---
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Note: If the router is acting as a NTP broadcast client
!--- via the interface command "ntp broadcast client"
!--- then broadcast and directed broadcasts must be
!--- filtered as well. The following example covers
!--- an infrastructure address space of 192.168.0.X
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 192.168.0.255 eq
ntp access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host
255.255.255.255 eq ntp
!--- Note: If the router is acting as a NTP multicast client
!--- via the interface command "ntp multicast client"
!--- then multicast IP packets to the mutlicast group must
!--- be filtered as well. The following example covers
!--- a NTP multicast group of 239.0.0.1 (Default is
!--- 224.0.1.1)
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD host 239.0.0.1 eq ntp
!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.
access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.
access-list 150 permit ip any any
!--- Apply access-list to all interfaces (only one example
!--- shown)
interface fastEthernet 2/0 ip access-group 150 in
```

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

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

– Control Plane Policing

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

– Filtering untrusted sources to the device.

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

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

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

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

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

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

```
!--- Feature: Network Time Protocol (NTP)
access-list 150 permit udp any any eq 123
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature
class-map match-all rate-udp-class match access-group 150
!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
```

```
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates
policy-map rate-udp-traffic class rate-udp-class police 10000 1500 1500
conform-action transmit exceed-action drop violate-action drop
!--- Apply the Policy-Map to the
!--- Control-Plane of the device
control-plane service-policy input drop-udp-traffic
```

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

Further Description

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

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

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

Other Caveats Resolved in Release 12.2(18)ZYA3b

Identifier	Technology	Description
CSCtf92354	ATM	spurious memory access seen at @ atmdx_hqf_tx_poll
CSCsu67919	Unknown	SIP crashes - hqf_cwpa_pak_enqueue_local
CSCth10980	Unknown	cbQosCMPrePolicyBitRate / cbQosCMPostPolicyBitRate always return 0

Resolved Caveats in Release 12.2(18)ZYA3a

Resolved MPLS Caveats

- CSCsz45567—Resolved in 12.2(18)ZYA3a

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

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

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

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available.

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

Resolved Multicast Caveats

- CSCtc68037—Resolved in 12.2(18)ZYA3a

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

  Conditions:

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

Other Caveats Resolved in Release 12.2(18)ZYA3a

Identifier	Technology	Description
CSCsz72591	IPServices	Router configured as a DHCP client crashes with crafted DHCP packet.
CSCta64900	Unknown	PISA reload due to NBAR
CSCte69627	Unknown	After upgrading to 12.2(18)ZYA3 POE fails to work on POE modules.

Resolved Caveats in Release 12.2(18)ZYA3

Resolved Routing Caveats

- CSCsv30595—Resolved in 12.2(18)ZYA3

  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.

- CSCsx73770—Resolved in 12.2(18)ZYA3

  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.

Resolved Security Caveats

- CSCsh97579—Resolved in 12.2(18)ZYA3

  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.

- CSCsx70889—Resolved in 12.2(18)ZYA3

  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

- CSCsq31776—Resolved in 12.2(18)ZYA3

  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 Unknown Caveats

- CSCsy15227—Resolved in 12.2(18)ZYA3

  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

Other Caveats Resolved in Release 12.2(18)ZYA3

Identifier	Technology	Description
CSCei16552	Infrastructure	cannot remove snmp-server engineID from running-config
CSCin79116	Infrastructure	show memory summary could push the CPU util to 100%
CSCsa91716	Infrastructure	Command sh archive config diff hangs with a remote file in argument
CSCsc33389	Infrastructure	When snmp-server host is deleted, the trap is not sent to other hosts
CSCse09553	Infrastructure	no snmp-server sparse-table: ds1 physical layer has none 0 for HC
CSCsj06593	Infrastructure	CPU hog msgs for RFSS worker process and Async write process
CSCsk41686	Infrastructure	PARSER-3-CFGLOG_NOMEM: constanlty in log
CSCsr17897	Infrastructure	SXF : increase the buffer size for config generation
CSCsr60789	Infrastructure	W1.3: VSL crash after preemptive switchover in ifs_open_file_decrement
CSCsx05021	Infrastructure	Router crashes when filesystem becomes full
CSCsx32841	Infrastructure	ceImageDescription may exceed 255 characters
CSCta43093	Infrastructure	Add a check similar to CSCek58956
CSCef09586	IPServices	CMs stuck in init(d) if DHCP ser. ip addr. overlaps with diff VRF
CSCsa41736	IPServices	Router crash after enable NAT rate-limit feature

Identifier	Technology	Description
CSCsg00102	IPServices	SSLVPN service stops accepting any new SSLVPN connections
CSCsh49973	IPServices	NAT-ALG corrupts offset value of DNS PTR response
CSCsk23972	IPServices	Telnet failed with "No wild listener" error
CSCso42170	IPServices	CPUHOG & Traceback messages seen for IP NAT Ager process.
CSCsx15358	IPServices	Router Crashes when DNS server and DNS views are used
CSCsx33622	IPServices	Fix MSS calcuation issue in TCP
CSCsy88271	IPServices	6500 - SXF - Nat add-route does not work
CSCsz56393	IPServices	Modular IOS - SUP720 - Sends malformed syslog packet
CSCsz63733	IPServices	Traceback seen with FM Nat configuration
CSCsz89107	IPServices	high cpu due to ip_input process during SNMP trap
CSCta24043	IPServices	"%IPNAT-4-ADDR_ALLOC_FAIL" message seen when all ports are not allocated
CSCtb12332	IPServices	NAT: switch crashes at ipnat_find_map_entry with cat6k SXF16 image
CSCtc26840	IPServices	HSRP-CISCO-MIB snmpwalk results in "OID not incrementing" error
CSCsz71787	LegacyProtocols	Router crash by crafted IP packet.
CSCsw85254	MPLS	Bus error and crash at p_enqueue when modifying main:text
CSCsz19255	MPLS	LFIB: Tag rewrites are missing on LC for one of load sharable paths
CSCsz30515	MPLS	SUP720 crash due to tsptun_frr_process process hang
CSCsx15396	Multicast	Mcast IIF stays up while physical interface is down
CSCsx34506	Multicast	RPF failure with no PIM neighbor triggers PIM Hello
CSCsw43022	platform-76xx	HSRP Virtual IP Unreachable for some users
CSCsy38911	platform-76xx	MPLS TE Forwarding broken when enable LDP on TE tunnel
CSCta26106	QoS	RSVP-3-CONSISTENCY error followed by an unexpected reboot.
CSCsh15066	Routing	VRF has 2 ospf process, when one process is removed the router crashed
CSCsh23176	Routing	Router crashes @ rip_timer_process .
CSCsm57494	Routing	BGP update is not sent after reloading opposite router
CSCso07476	Routing	One way audio when RTP header compression is turned on
CSCsq49201	Routing	Password in BGP peer-session template not inherited
CSCsr11662	Routing	EIGRP active routes never go to SIA, queries not sent
CSCsr27794	Routing	BGP updates stuck during peer flap
CSCsr90248	Routing	"aggregate-address advertise-map" not updated dynamically
CSCsx06457	Routing	BGP may modify routes it does not own
CSCsx51299	Routing	Crash when remove and configure ipv6 ACL via telnet and console
CSCsx51596	Routing	TCAM ACL entry not correct after removing IP accounting
CSCsy58115	Routing	Continuous BGP mem increase with non established neighbors
CSCsy84134	Routing	ARP table is flushed when deleting secondary IP address
CSCuk55357	Routing	ALIGN-3-TRACE at ip_broadcast
CSCsb80803	Security	SSH Process: SCHED-3-UNEXPECTEDEVENT error message

Identifier	Technology	Description
CSCsd91182	Security	crypto pki export pkcs12 hangs when used with SCP
CSCsg56609	Security	Crash on talk /tmp/tbdaemon-99/../os/connect.c:1105 seen at bootup
CSCsy17893	Security	Ping to itself doesn't work on IPIP tunnels
CSCsz84055	Security	System crashed unexpected while open ssh2 session
CSCek68108	Unknown	Router crashed at ace_policyloader_util.c after remove crypto map .
CSCek74844	Unknown	sysObjectID is wrong for 7603-S and 7609-S
CSCek77996	Unknown	High CPU caused by data traffic with crypto map in crypto connect mode
CSCsb25490	Unknown	Data is not being hardware switched after OIR/SSO on WS-X6148X2-RJ45
CSCsb88996	Unknown	slb traceback spurious memory access after slb statefull switchover
CSCsb96452	Unknown	IGMPV3 TO_INC{} leave mac entry table do not expire
CSCsc85962	Unknown	Replaying Main Mode packet causing IKE SA deletion
CSCsc92676	Unknown	Rainier:Traffic captured even after vacl config is removed
CSCsd45698	Unknown	Cat6K: SLB punted to CPU if src_index is port-channel index
CSCsf05390	Unknown	CPU HOG @ hwidb_iftype_unlist followed by router crash.
CSCsf10203	Unknown	MLD gces not freed even after MLD leaves and L3 traffic stopped
CSCsf27621	Unknown	False Command-Active condition blocking execute-on on MWAM processor
CSCsg32319	Unknown	Probe connections not cleaned up when access/vrf is configured .
CSCsg37484	Unknown	Bus Error in crypto_map
CSCsi54373	Unknown	OSM maps EXP into dBus-CoS during SVI based EoMPLS disposition
CSCsj26698	Unknown	Acct-Session-Id in Accounting-Request is different from in Access-Reques
CSCsk38024	Unknown	VS2: EtherChannel state on standby is incorrect due to out of order FEC
CSCsk87604	Unknown	Device crashes on configuring LPIP with multiple hosts.
CSCsl69123	Unknown	SIP-400:QoS:Police drops MPLSCP, CDPCP negotiation packets - SRA,SRB
CSCso35659	Unknown	L3 traffic rate limited after adding and removing Xcon to a SVI
CSCso75862	Unknown	Negative counter values for input queue on layer 3 interfaces
CSCso93350	Unknown	Boot string fails to set in rommon but no error message
CSCsq69567	Unknown	SSO Switchover + unicast-routing chg cause MC traffic loss for 2 minutes
CSCsr06037	Unknown	the monitor session source is removed by deleting sub-interface
CSCsr12976	Unknown	High CPU in ION ios-base process
CSCsr39272	Unknown	%DATACORRUPTION-1 due to spa sensor temp overruning buffer
CSCsr97097	Unknown	VS: RP IPC-5-WATERMARK msgs due to CARD_RESET, after SSO
CSCsr99518	Unknown	Granikos should not init rekey after recieving new outbound SA at QM3
CSCsu29301	Unknown	C2W21: Ingress SPAN on Sup - ACE module duplicates packets
CSCsu31088	Unknown	Not able to execute any commands under intf after running SPA FPGA bert
CSCsu76360	Unknown	Memory Leak in IPSec Key Engine with HA on Sup720 RP
CSCsw17070	Unknown	18SXF: SSO switchover cause portchannel configuation lost in sup uplink
CSCsw21852	Unknown	CSM: memory leak in process "Laminar Icc Event"

Identifier	Technology	Description
CSCsw28582	Unknown	IPSec Tunnels go down after a "show run"
CSCsw43377	Unknown	add user warning for empty classes in OSM qos policy SXF7 and later
CSCsw52819	Unknown	Kernel dumper needs a few enhancements.
CSCsw53362	Unknown	c2w2b: Device crashes with NAT stress test
CSCsw68514	Unknown	SLB probes iin TESTing state while using client cmd in Vserver config
CSCsw87563	Unknown	packets with multicast mac and unicast ip are software routed by cat6500
CSCsw92171	Unknown	multiple "power-input" for new 6kW DC PS do not exist on Standby
CSCsx16206	Unknown	Traffic loss issue from SFM capable modules to other device through DEC
CSCsx21886	Unknown	ISSU switchover command sync issue
CSCsx23929	Unknown	MLPP link are not able pass traffic after SSO even when UP/UP stat on os
CSCsx39263	Unknown	TCAM entries are not installed for TCP intercept after SSO
CSCsx49889	Unknown	SPA-IPSEC-2G-3-ACEI0TCAMFAILE:SpdSpInstall:cannot install Sp TmInsertSp
CSCsx51231	Unknown	Service-policy removed from the interface, but FIE still has NBAR active
CSCsx58248	Unknown	Disable Crypto ACL in SXF
CSCsx67510	Unknown	Memory leak on SP when add/deleting channel groups on PA-MC-2T3+
CSCsx76308	Unknown	HA client crashing attempting to free unassigned memory
CSCsy06804	Unknown	DSCP not preserved during SVI based Eompls Disposition
CSCsy08838	Unknown	Zamboni allows clear packet inbound on protected interface
CSCsy24691	Unknown	entPhysicalTable has power-input 3 Sensor for 6kW DC PS1 and not PS2
CSCsy34566	Unknown	Disable VLAN mapping on ME6524, 6148A-GE-TX
CSCsy54365	Unknown	frequent datapath recovery and traffic loss on WS-X6704 with DFC
CSCsy74418	Unknown	Ping fail with bridging on interface - 6500 w/SUP2 and 6816
CSCsy78994	Unknown	Memory leak in Service Task
CSCsy82121	Unknown	IGMP Source only not working due to MC_CAP not set
CSCsy83830	Unknown	IOS-RLB crashes while deleting the username sticky
CSCsy85171	Unknown	CDL2 Read Error: Time out
CSCsy94866	Unknown	C2W2B: CSM Config sync causes memory leak
CSCsz01976	Unknown	Need a cli to dump the rommon environment and unset rommon variable
CSCsz14742	Unknown	EZVPN config not downloaded on the SPA/VPNSM
CSCsz20625	Unknown	Error message seen if SIP Is OIR'd during Standby SUP bootup
CSCsz42143	Unknown	WS-X6148A-GE-TX module fails keepalives when excessive errors on port.
CSCsz43438	Unknown	Encapsulation change on T1/E1 removes QoS Service Policy
CSCsz55834	Unknown	GLBP may provided BIA MAC instead of Virtual MAC for mobile users
CSCsz55950	Unknown	EoMPLS:DFC LTL programming is not correct for SRP as Core
CSCsz62046	Unknown	Crash at memcpy after CPUHOG in SNMP ENGINE
CSCsz67334	Unknown	ciscoEnvMonTemperatureStatus trap sent sporadically as NotFunctioning
CSCsz76015	Unknown	C2W2: Need cli to set PF_BIAS to ensure lower slot# Sup boots as active

Identifier	Technology	Description
CSCsz84544	Unknown	output drops increment on not-connected interface of 6548GE-TX module
CSCsz87648	Unknown	SP/RP and redundant system handshake broken when the kernel crashes.
CSCsz92508	Unknown	SPA module reloads when no response to keep-alive polling
CSCsz94158	Unknown	Disabling urlf will not remove X-list entries and logging functionality
CSCta12382	Unknown	Udld port config does not sync to standby in rpr-plus mode
CSCta12543	Unknown	Linecard takes MAC address from the linecard.
CSCta15614	Unknown	MQC / PD / FPM Classification fails if conf app. before acc vlan conf
CSCta21771	Unknown	%CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at 0 error on modul
CSCta26529	Unknown	Standby Reset set entPhysicalAssetID on PS1
CSCta27279	Unknown	WCCP s/w switching with Ingress redirection & interface ACL
CSCta32802	Unknown	Umbrella ddts for porting SR HA fixes+ 2T3E3 SPA fixes into SXF
CSCta34959	Unknown	ECHOREP not sent to ECHOREQ when MSFC is PISA and PPP multilink is used
CSCta42989	Unknown	"%CSM parser state" configuring CLI when configuring via XML also
CSCta47653	Unknown	Cat6k: SXF: Console hangs on reapplying running config with ACL
CSCta48521	Unknown	%DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCta48968	Unknown	Modular IOS kernel crashinfo has missing information
CSCta52689	Unknown	cat6k crash in RP due to address error with wccp configuration
CSCta53157	Unknown	SPA-4XT3/E3 int in SIP-200 admin-down on standby after fpd upgrade
CSCta55498	Unknown	[Modular IOS] MIPS CP0 registers save algorthim needs a few improvements
CSCta62394	Unknown	RP crashes @crypto_ipsec_profile_map_val on removing vlan with HA config
CSCta71873	Unknown	Mcast traffic stops flowing across fabric to required fpoes
CSCta72199	Unknown	"aggregate-address advertise-map" not updated dynamically with ION image
CSCta76808	Unknown	add CLI command for medium buffer pool
CSCtb01060	Unknown	PISA: Second ACK drop in HTTPS using wccp in cat6k with CE(ACNS)
CSCtb02774	Unknown	PI_E scanner needs to check high LTL index(0x740-0x77f) for PO interface
CSCtb23289	Unknown	Major temperature alarm has to force system shutdown
CSCtb23840	Unknown	%SYS-3-CPUHOG in Time Range Process with QoS Time based ACL
CSCtb28032	Unknown	Changing module corrupts Flex Link
CSCtb38547	Unknown	Incorrect CP0 values and empty kernel variable section in kernel crashin
CSCtb68478	Unknown	"Illegal nextSsIndex value" message should be removed
CSCsi56413	WAN	PA-POS-OC3SMI interface output stuck .

Resolved Caveats in Release 12.2(18)ZYA2

Resolved AAA Caveats

- CSCsv73509—Resolved in 12.2(18)ZYA2

  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.

Resolved Infrastructure Caveats

- CSCse85652—Resolved in 12.2(18)ZYA2

  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 implemented:

  - 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(18)ZYA2

  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(18)ZYA2

  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 IPServices Caveats

- CSCsk64158—Resolved in 12.2(18)ZYA2

  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

- CSCsm27071—Resolved in 12.2(18)ZYA2

  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

- CSCso81854—Resolved in 12.2(18)ZYA2

  Multiple Cisco products are vulnerable to DNS cache poisoning attacks due to their use of insufficiently randomized DNS transaction IDs and UDP source ports in the DNS queries that they produce, which may allow an attacker to more easily forge DNS answers that can poison DNS caches.

  To exploit this vulnerability an attacker must be able to cause a vulnerable DNS server to perform recursive DNS queries. Therefore, DNS servers that are only authoritative, or servers where recursion is not allowed, are not affected.

  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-20080708-dns

  This security advisory is being published simultaneously with announcements from other affected organizations.

- CSCsv04836—Resolved in 12.2(18)ZYA2

  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.

- CSCsw18636—Resolved in 12.2(18)ZYA2

  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.

- CSCsr29468—Resolved in 12.2(18)ZYA2

  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 LAN Caveats

- CSCsv05934—Resolved in 12.2(18)ZYA2

  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 Multicast Caveats

- CSCso90058—Resolved in 12.2(18)ZYA2

  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.

Resolved Security Caveats

- CSCsh97579—Resolved in 12.2(18)ZYA2

  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.

- CSCsx70889—Resolved in 12.2(18)ZYA2

  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

- CSCsq31776—Resolved in 12.2(18)ZYA2

  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 Unknown Caveats

- CSCsu57182—Resolved in 12.2(18)ZYA2

  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.

Resolved Voice Caveats

- CSCsi60004—Resolved in 12.2(18)ZYA2

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

Other Caveats Resolved in Release 12.2(18)ZYA2

Identifier	Technology	Description
CSCef97900	AAA	AAAA-3-DROPACCTLOWMEM warning message somewhat misleading
CSCin40015	AAA	telnet to NAS fails when user profile has access-profile
CSCsl29214	AAA	AAA server change leads to bus error crash after "show run" is issued
CSCso95210	AAA	AAA Client creates bad Message Authenticator attr for every first packet
CSCsx28646	ATM	Unable to configure atm pvp l2transport
CSCsx40747	Content	Router hangs while doing ip casa configurations
CSCsc86307	Infrastructure	c3845 crashed @ show_systat
CSCsm32392	Infrastructure	memory corruption crash at nv_ifs_open and nv_ifs_close
CSCso49598	Infrastructure	Stby reloads cont. when upto MAXINT logical int created thru int ran
CSCsq03621	Infrastructure	Timestamps in "show rmon events" wrap at 2^32-1 milliseconds (7+ weeks)
CSCsw35917	Infrastructure	SP syslog messages not sent as SNMP traps by RP's SNMP agent
CSCec72958	IPServices	Software forced crash when translating LDAP packet
CSCsg00102	IPServices	SSLVPN service stops accepting any new SSLVPN connections
CSCsk16821	IPServices	DHCP does not NAK after DHCPREQUEST from unknown client .
CSCso02053	IPServices	NAT does not add dynamic aliases after reload.
CSCso04657	IPServices	SSLVPN service stops accepting any new SSLVPN connections

Identifier	Technology	Description
CSCso42170	IPServices	CPUHOG & Traceback messages seen for IP NAT Ager process.
CSCso54027	IPServices	Spurious memory access in ttcp_rcv_stats
CSCsq60504	IPServices	Modular IOS Sup720: crashed with tcp timeout logs
CSCsr08771	IPServices	Crash seen @ dhcpd_pool_nvgen and dhcpd_copy_bootfile
CSCsx32283	IPServices	Malformed L field in LDAP crashes 6k with NAT
CSCsh33167	LegacyProtocols	Dlsw transparent cache holds MAC address for disconnected circuit
CSCsk41552	Management	T/B %SCHED-3-THRASHING of cdp2.iosproc process_wait_for_event
CSCsb52253	MPLS	IPv4 iBGP multipath in MPLS network needs to be blocked or hardcoded
CSCsc78971	MPLS	LDP:Incorrect address withdraw after IP address removal on shutdown i/f
CSCse22900	MPLS	w/mis-config'd dup vrf CEF/BGP table MPLS label mismatch may occur
CSCsk99530	MPLS	LFIB untagged entries while LIB has valid lables in CSC MPLS VPN c12000
CSCsm70668	MPLS	OIR over E3:POS impacting complete Traffic with biscuit tunnel
CSCsu45425	MPLS	FIB/LFIB not updated correctly after route-flap
CSCsw19951	MPLS	SP & DFC crash when forwarding a packet with MPLS
CSCse03637	Multicast	PIM Dense Mode - Prune sent in error after assert is won .
CSCsj88725	Multicast	Wrong (S,G) RPF after route change, no upstream join
CSCsm77608	Multicast	IP Multicast packets are Process switched.
CSCsr49316	Multicast	Crash ipv6_static_route_find after configured & executed show ipv6 rpf x
CSCsv99150	platform-76xx	status led of ge-wan module not showing proper status
CSCsg25664	PPP	dLIFoMLPPPoATM PA: Corrupted PC crash PR
CSCsr81271	PPP	Invalid VCD error messages upon PVC flap
CSCek63384	QoS	Service-Policy is Lost When the Multilink Interface is Reset .
CSCsv85791	QoS	Flexwan+/PA-MC-2T3+ introduce 5+ seconds delay on egress
CSCsy90758	QoS	NBAR doesn't reconize PASV FTP traffic based on ports in control channel
CSCee30355	Routing	Memory leak at ip_multicast_ctl
CSCeg49075	Routing	MSFC2 remark lines in ACLs duplicated in the NDR MSFC
CSCei86031	Routing	changing match command on fly does not filter route correctly .
CSCej49366	Routing	Removing default-metric under EIGRP deletes routes erroneously
CSCek75079	Routing	Problem in type7 to type5 translation if summary-addr configured
CSCsa72878	Routing	ISIS: clns route from end-system not in database
CSCsb15164	Routing	Security holes while configuring a standard ACE with host address
CSCsc01880	Routing	%FIB-4-FIBCBLK: Missing cef table for tableid 770 during routing table e
CSCse53019	Routing	redistribution not triggered when BGP as-path/community changes
CSCse68877	Routing	CEF/BGP table MPLS label mismatch YW3 Non Multi-path
CSCsg46366	Routing	OSPF NSSA LSA forwarding address set even when P bit wil be clear.
CSCsg68717	Routing	A weird behavior in maxpath configuration in ebgp+ibgp case
CSCsi01324	Routing	Modifying acl concerned with distribute-list withdraw summary route

Identifier	Technology	Description
CSCsi03434	Routing	Memory leak @ ospf_redist_work_enqueue
CSCsj09838	Routing	RR some prefix might not be sent after bgp neighbor flaps .
CSCsj13911	Routing	Cat3750:EIGRP does not receive reply for query between some Vlan
CSCsk35688	Routing	Aggregate routes not processed if child routes are deleted pre-maturely
CSCsk72259	Routing	Auto-repair not updating inconsistent cef entries
CSCsl32318	Routing	OSPF: new fix for CSCsk36324 SPF loop
CSCsl84712	Routing	Error- %OSPF-4-FLOOD_WAR: Process 123 re-originates LSA ID 10.55.122.148
CSCsm50741	Routing	Removal of DCbitless LSA causes problems
CSCsm91959	Routing	Code review: aggregation child routes can miss aggregation logic
CSCsm95129	Routing	"no ip next-hop-self eigrp" not working when redistribute from BGP
CSCsm96901	Routing	Unable to ping between vrfs through transparent bridge
CSCso08786	Routing	Standby reloads due to config sync failure on inherit peer-policy cmd.
CSCso54167	Routing	BGP peer stuck with table version 0
CSCsr88362	Routing	eigrp routes aren't updated after SSO switchover
CSCsu24087	Routing	Cisco7609 crashes after "clear ip bgp neighbor x.x.x.x soft in"
CSCsu36709	Routing	Unable to boot IOS image on PE (vrf-enabled) router - software fault
CSCsv01474	Routing	'ip rip advertise' command lost after interface flap/clear ip route
CSCsv27607	Routing	BGP: Outbound route-map updating withdraw only one member
CSCsv97472	Routing	CSCso62166_dcq_issue_rn_walktree_timed_locking is changed
CSCsw28893	Routing	Cost no longer showing with each eigrp route after IOS upgrade
CSCsw65441	Routing	ARP packets drops due to excessive ARP requests sourced from SVI
CSCsx15841	Routing	aggregate-address does not NVGEN upon switchover on cat6k
CSCsc91824	Security	SSH from router disconnects vty session if there is no matching cipher
CSCsd81870	Security	Teraterm + TTSSH2 does not work in SSH Ver.2
CSCeh00399	Unknown	RRI: refcount not inc on rekey in certain circ lead to route removal
CSCei29284	Unknown	Rockies3 SUP32 SNMP:Traceback msg when execute private vlan script
CSCek28863	Unknown	Need to change default SCP keepalive timeout on IOS to CSM module
CSCek77996	Unknown	High CPU caused by data traffic with crypto map in crypto connect mode
CSCsc73409	Unknown	IGMPv3 report suppression doesnt send out group records correctly
CSCsc98850	Unknown	ZAMBONI:Could not send pmtu information vlan 65535 pmtu 0 Error
CSCsd04937	Unknown	Crash in chunk_free called from mfib_const_rp_free after (*,G) HW enable
CSCse12518	Unknown	MET optimized update can cause blackholing and duplicates
CSCsg14926	Unknown	Standby can not boot because of insufficient memory with 32K interfaces
CSCsg53526	Unknown	Some packets to vip are denied by inbound acl after server nat
CSCsh22225	Unknown	CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR:
CSCsh98849	Unknown	SIERRA: Active and stby SP and active RP crashed@rf_proxy_fatal_error
CSCsi14145	Unknown	runt counter not implemented correctly

Identifier	Technology	Description
CSCsi36204	Unknown	able to configure po256 via IOS startup dialog
CSCsi66012	Unknown	2 garbage values in show module csm x ft details
CSCsi88920	Unknown	MLD rcvr in SVI stops receiving v6 mcast trffc if another rcvr leaves
CSCsk23521	Unknown	EARL-SPSTBY-2-SWITCH_BUS_IDLE is seen with SW switched traffic
CSCsl02190	Unknown	ICMPv6 to all node multicast address fail .
CSCsm31178	Unknown	policy-map stops working on a good int if wrongly applied on another int
CSCsm43962	Unknown	Cat6k L2TP packet looped through blocked port
CSCsm66023	Unknown	IPv6 VTI RP crashed ace_reverse_map when changing tnlsrc from v4 to v6
CSCsm75286	Unknown	bgp route-map doesn't work correctly when deleted part of sequences
CSCsm76792	Unknown	PM HA bulk sync posting RF_DONE before bulk sync has finished
CSCsm85936	Unknown	UUT cpu at 40% with bi-dir traffic across a single tunnel
CSCsm93648	Unknown	C2W2:080226 Rtr crashed when moving tunnels from VTI to GRE/TP
CSCso11822	Unknown	LACP PC switchport, on OIR, "channel group 112 active" config gets lost
CSCso29141	Unknown	DFC installs drop index for MAC-address
CSCso88042	Unknown	Wism module Allowed-Vlan statements lost on reload
CSCso88772	Unknown	sp-inband tx capture causes primary SUP to hang
CSCsq22383	Unknown	SP crash due to CPU hog by online diags
CSCsq42885	Unknown	Line card crashes with %IPC-2-ONINT error on OSM
CSCsq51378	Unknown	ATM PA Interface shows up/up after force redundancy, no cables connected
CSCsq56941	Unknown	6500 - Static MAC cleared from port-channel member ints after reload
CSCsq73122	Unknown	Proxy-ARP returns BIA instead of VMAC with LAM
CSCsq75704	Unknown	FW2 FE PA Interface stays up/down with no conn and goes up/up after sso
CSCsq80145	Unknown	VACL does not work against self initiated packet
CSCsq83789	Unknown	LTL for unknow unicast is wrongly programmed for some L3 interfaces
CSCsq84116	Unknown	Cisco 7604 with OC3, Flexwan crashes into ROMMON
CSCsq90844	Unknown	bridge-group config make packets be routed
CSCsq94136	Unknown	Burst of traffic cause anti-replay check to fail
CSCsr29559	Unknown	WCCP flap corrupts mcast CEF adjacency
CSCsr37131	Unknown	buginf calls in l2trace when 'debug l2trace' is disabled
CSCsr45495	Unknown	PBR with deny statements : TCAM running out of masks
CSCsr46399	Unknown	PISA - NO_PARTICLE:
CSCsr51799	Unknown	pa-mc-8t1 interface down after stopping BERT prematurely
CSCsr69929	Unknown	ACL based uRPF check is causing acl permit packets to be dropped
CSCsr88625	Unknown	Seeing ME_AR#0 WARNING: Cannot FLUSH Dic#0 when WS-X6708-10GE boots
CSCsr88845	Unknown	unicast BootP replies dropped by DHCP snooping
CSCsu05800	Unknown	C2W2: need to extend the wait time for bus sync after sso
CSCsu07931	Unknown	cbQosPoliceConformedByte64 counter displays aggregate instead conformed

Identifier	Technology	Description
CSCsu18231	Unknown	IKE process fails to start phase1 if in up-no-ike and DPD triggered
CSCsu33707	Unknown	Multicast traffic will not stop after PIM prune
CSCsu37481	Unknown	Netflow Incorrect Octet value with packet-based sampling
CSCsu37899	Unknown	SXF15: autostate configuration missing after SSO
CSCsu45210	Unknown	Upgrade 12.2SXF-> 12.2SXH with Port-Security causes standby boot loop
CSCsu46982	Unknown	I/O rate counter inaccurate when applying serv policy and MPLS traffic
CSCsu49002	Unknown	ciscoIpMRouteBps sometimes indicates wrongful value
CSCsu49257	Unknown	Cstn-id timer should be restarted when access-request is seen
CSCsu57958	Unknown	DHCP-Snooping not intercepting DHCP messages from the Server
CSCsu68698	Unknown	No syslogs and stack on console when SP crashes due RP boot timeout
CSCsu86524	Unknown	IKMP process leak: check_ipsec_proposal
CSCsu91725	Unknown	Bus crash problem due to cipSecGlobalStats MIB query
CSCsu99270	Unknown	CPUHOG observed when configuring more vlan interfaces
CSCsv07858	Unknown	IfIndex for unconfigured VLAN on 7613
CSCsv10229	Unknown	Failed to assert Physical Port Administrative State Down alarm
CSCsv17989	Unknown	interface in SIP200 show "admin down" when it is physical down
CSCsv18579	Unknown	'recognized & transferred a satvcl packet' observed on 6708 / module 1
CSCsv63144	Unknown	Controller remains DOWN after switchover
CSCsv64079	Unknown	SXF7: Patching fails with WiSM Card on Cat6500
CSCsv66827	Unknown	Clearing the SSH session from a different vty session crashes the box.
CSCsv85551	Unknown	SP crash due to consume all scp triggered by OIR loop when PS go off
CSCsw21852	Unknown	CSM: memory leak in process "Laminar Icc Event"
CSCsw35155	Unknown	reduce move count for SAs in SXF
CSCsw38075	Unknown	%SYS-2-GETBUF: Bad getbuffer error messages after IOS upgrade
CSCsw43953	Unknown	Card not identified SIP Is OIR'd during Standby SUP bootup
CSCsw65477	Unknown	MLD snooping broken in SXF16 engg (pre-release) images
CSCsw68032	Unknown	Serial links UP/DOWN after SSO on OSM Module
CSCsw69911	Unknown	SIP-400 POS WRED queues tail dropping without random drops
CSCsw75293	Unknown	18SXF: RP Mapping not seen in last hop router in Sup2 image
CSCsw82431	Unknown	18SXF16:Device crashes while unconfiguring PBR configs.
CSCsw96891	Unknown	CPUHOG observerd after issuing exec commands
CSCsx67510	Unknown	Memory leak on SP when add/deleting channel groups on PA-MC-2T3+
CSCsy46645	Unknown	PISA fallback bridging fail to receive some routing protocol packets
CSCsz04297	Unknown	Cat6k: False Dynamic MAC entry is installed with format 0000.<LTL>.0000
CSCta15614	Unknown	MQC / PD / FPM Classification fails if conf app. before acc vlan conf
CSCei77073	WAN	NTP client need to reset auto learnt source IP address

Resolved Caveats in Release 12.2(18)ZYA1

Resolved Infrastructure Caveats

- CSCse85652—Resolved in 12.2(18)ZYA1

  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 implemented:

  - 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

Resolved IPServices Caveats

- CSCsk64158—Resolved in 12.2(18)ZYA1

  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

- CSCsm27071—Resolved in 12.2(18)ZYA1

  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

- CSCsr29468—Resolved in 12.2(18)ZYA1

  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

- CSCsv04836—Resolved in 12.2(18)ZYA1

  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.

Resolved LAN Caveats

- CSCsv05934—Resolved in 12.2(18)ZYA1

  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 PPP Caveats

- CSCsa49019—Resolved in 12.2(18)ZYA1

  Symptoms: A memory leak may occur in the "Multilink Events" process, which can be seen in the output of the **show memory summary** command:

```
0x60BC47D0 0000000024 0000000157 0000003768    MLP bundle name
0x60BC47D0 0000000028 0000000003 0000000084    MLP bundle name
0x60BC47D0 0000000044 0000000001 0000000044    MLP bundle name
0x60BC47D0 0000000048 0000000001 0000000048    MLP bundle name
0x60BC47D0 0000000060 0000000001 0000000060    MLP bundle name
0x60BC47D0 0000000064 0000000013 0000000832    MLP bundle name
0x60BC47D0 0000000068 0000000008 0000000544    MLP bundle name
0x60BC47D0 0000000072 0000000001 0000000072    MLP bundle name
0x60BC47D0 0000000076 0000000001 0000000076    MLP bundle name
0x60BC47D0 0000000088 0000000018 0000001584    MLP bundle name
```

  Conditions: This symptom is observed when two interfaces are configured in the same multilink group or are bound to the same dialer profile.

  Workaround: There is no workaround.

Resolved Security Caveats

- CSCsj85065—Resolved in 12.2(18)ZYA1

  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 Unknown Caveats

- CSCek49649—Resolved in 12.2(18)ZYA1

  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

Other Caveats Resolved in Release 12.2(18)ZYA1

Identifier	Technology	Description
CSCdu79630	AAA	Username on vty not displayed if accounting is not configured
CSCsg18288	AAA	Enable authentication ignores Tacacs+ configuration in rare situation
CSCsl57645	AAA	tacacs-server directed-request fails for enable authentication on 6500
CSCso95426	AAA	Exposure of Radius-Keys in debugs.
CSCsj88665	Access	Bus error with PA-MC-2T3+ when deleting channel-group
CSCei33231	ATM	ATM PVC bundle protected group test failed with bumping exhausted
CSCek74474	ATM	no/default proto ip inarp cmd ineffective until ATM VC bounced.
CSCsm12247	Content	WCCP: hash assignment may be lost after service group change
CSCek58956	Infrastructure	Need process_ok_to_reschedule check in process_may_suspend
CSCsd37499	Infrastructure	%IFS-3-FSMAX: Failed to add ?, maximum filesystems 64 msg with Traceback
CSCsd62013	Infrastructure	Traceback on Standby RP@add_lpmapping_entry_private+74
CSCsk70446	Infrastructure	NRT: tracebacks @ data_inconsistency_error - 7200 for HTTP config .
CSCsl06515	Infrastructure	Sup720 Crash with 11 eFlexWan linecards
CSCsl60092	Infrastructure	Active SP crashed @ipc_fragment_cleanup with VSL shut/no shut test
CSCsm01126	Infrastructure	PRE-B crashes while in progress to standby cold-config
CSCso99219	Infrastructure	Match ip address with Named ACL not work in route-map
CSCsq19159	Infrastructure	RP crashes in chassismib_add_sub_card_entry after linecard reload

Identifier	Technology	Description
CSCec51750	IPServices	Router reloads do to bus error. and illegal access to low address
CSCsi57927	IPServices	FTP session hangs TCP in closewait after CLI times out . .
CSCsl23788	IPServices	Dlsw+ peer waits in AB_PENDING or WAIT_WR status with modular IOS
CSCsl70070	IPServices	CPUHOG when doing HSRP SNMP query
CSCsm36306	IPServices	NAT creates overlapping translation entries using the same IG address
CSCsm59037	IPServices	no service dhcp command causes switch to reload
CSCsm70580	IPServices	c2w2:ciscoFtpClientMIB: ftp_fs.proc extra processes can deadlock & crash
CSCso04657	IPServices	SSLVPN service stops accepting any new SSLVPN connections
CSCso68344	IPServices	Switch acting as DHCP server crashes on issuing no service dhcp command.
CSCsq48201	IPServices	c7300:Bridge IRB-Router crash and traffic flow issue
CSCsr08771	IPServices	Crash seen @ dhcpd_pool_nvgen and dhcpd_copy_bootfile
CSCsk32095	LAN	PA-2FE-TX port flaps on applying qos policy
CSCsk94676	LegacyProtocols	dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH
CSCsq68529	LegacyProtocols	After reload, there is no mac-address on SVI not running DECnet
CSCsl78965	MPLS	High CPU in SNMP engine, mplsVpnVrfRouteEntry
CSCsm30973	MPLS	bgp multipath with ipv4+label nexthop: label missing in cef
CSCso22730	MPLS	Prefixes get assigned imp-null local label after OIR linecard
CSCso47703	MPLS	Spurious Access error on rsvp_frr_event_lsp_down_psb
CSCek75931	Multicast	LNS: %SYS-3-CPUHOG When sessions have multicast
CSCsd14706	Multicast	PIMV2 router send PIMV1 RP-reachable messages loading recieve router CPU
CSCsk26429	Multicast	Router configured for IGMP Proxy may not send IGMP Join
CSCsl20158	Multicast	SNMP:msdpPeer counters should be able to compare with CLI counters.
CSCsl92316	Multicast	LNS: %SYS-3-CPUHOG when clear l2tp tunnel, sessions have multicast
CSCsm17426	Multicast	RP-bit not cleared on s,g; traffic outage for 4 minutes
CSCsm44620	Multicast	Shutdown interface present in PIM interface list
CSCsm48322	Multicast	IPv6 Multicast RP ignores embedded RP register messages
CSCsq14151	Multicast	RPF of (S,G) is set to NULL, When (S, G, R) entry is convered to (S, G)
CSCsq47166	platform-76xx	GE-WAN interface stays down with autonegotiation enabled
CSCsc69804	PPP	SIP1-ChOC3:Initial packets fail with SW-MLP on SIP-200
CSCse40966	PPP	MLP links down after SSO switchover if aaa new-model cfged
CSCsq37078	PPP	Input errors incrementing on Multilink 5 in admin down state
CSCsj60595	QoS	SIP-400 : offered rate in sh policy-map int is not accurate
CSCsm00570	QoS	cwpa2 crashes at hqf_cwpa_pak_enqueue_local
CSCsm29181	QoS	Crash when NBAR applied to sub-interface
CSCsm49062	QoS	cwan2: show queueing interface reports double count for wfq drops
CSCef16315	Routing	default-information originate route-map causes default route aging
CSCek47667	Routing	clear bgp ipv6 unicast * does not work .

Identifier	Technology	Description
CSCsa73179	Routing	Memory corruption/crash when 'no default-information orig' under RIP
CSCsc58258	Routing	OSPFv3: 64-bits long keys for LSDB
CSCsc72090	Routing	EIGRP doesn't honor interface IP MTU when sending packets
CSCsc96014	Routing	EIGRP neighbors from primary add space deleted when sec add removed
CSCsd92325	Routing	Config sync: no neighbor 192.168.240.34 triggers standby reset
CSCse65277	Routing	MU:default isis metric maximum returns parser error
CSCse85383	Routing	OSPFv3: Restructure link-state request list (CSCsd03021)
CSCsf06946	Routing	Removing loopback interface causes continuous standby RP reloading
CSCsh38140	Routing	CEF drops when using CEF LB paths and active link recovers from failure
CSCsi15183	Routing	change MTU value causes %DUAL-3-INTERNAL in ipigrp2_add_item_dest
CSCsi27696	Routing	oldest ebgp bestpath not retained in eibgp multpath cases
CSCsi68795	Routing	PE wrongly assigns local label to a vpnv4 confederation prefix
CSCsi98730	Routing	CEF/BGP table MPLS label mismatch in IOS 12.4(6)T5
CSCsj21785	Routing	TE tunnel does not reoptimize after mtu change
CSCsj56281	Routing	BGP inherit peer-policy not working after router reload
CSCsk35985	Routing	OSPFv3: router crashes for "show ipv6 ospf lsdb" after redist of routes
CSCsl06336	Routing	removing 'maximum-paths import 6' causes duplicate paths in VRF table
CSCsl30331	Routing	Prefixes permitted despite the deny action on route-map continue
CSCsl70287	Routing	RIP default-originate not working after a switchover
CSCsl92283	Routing	Unable to add into routing table if static route use interface + gateway
CSCsm04442	Routing	Router crash at rip_find_sum_idb
CSCsm43938	Routing	stby resets when large config/arp table to sync over to it
CSCsm45634	Routing	BGP VPNv4 route is not actived immediately after receving update
CSCsm91801	Routing	ASBR not updating metric in LSA-5 redistributing from 2-nd OSPF process
CSCso60089	Routing	7200: KBOOT image build failed
CSCso62166	Routing	Crash @ bgp_netlist_validate when ibgp established with metric
CSCso64274	Routing	0.0.0.0/0 redistributed entry not removed RIP DB after deleting command
CSCso73076	Routing	can not delete ACE enties in ACL
CSCso93535	Routing	Upon removing a VRF, BGP route timers in other VRF's get reset
CSCsq13938	Routing	reload on 'show ip bgp vpnv4' when import src delinked by BGP deconfig
CSCsq21198	Routing	PE loses VPNv4-MDTs from a RR when another RR fails (or shuts neighbor)
CSCsu03167	Routing	SXF15: IPv4/v6 BGP routes not cleared when source routes is gone
CSCsc92417	Security	Secure copy feature intreaction issues with Archive command
CSCsg03753	Security	cat6k memory leak in map->peers and peering_info_list_chunk
CSCsl34391	Security	Output of 1st page of "sh crypto ipsec sa" is blank
CSCso03917	Security	Rtr crash on "sh cry ipsec sa" @ crypto_ipsec_manipulate_ident_tree
CSCso26788	Security	Re-work CSCin91851 for SXF

Identifier	Technology	Description
CSCsr60782	Security	Fix SA warnings in ssh2_support.c
CSCsr85093	Security	SXF15: SSH session fails withRSA signature verification failed after SSO
CSCef71952	Unknown	EzVPN server disconnects all PAT users of same IP address
CSCeg35237	Unknown	Watchdog crash after sh crypto session
CSCek37984	Unknown	Inconsistent BERT behaviour observed on TE1 SPA
CSCek74347	Unknown	Router crash after ip address slarp retry
CSCek78066	Unknown	Whitney:CLI & MIB mismatch for aux-1 temperature Sensor SUP32
CSCsb56931	Unknown	The SWIDB subblock named QM was not removed, on PPP to FR encap change
CSCsb60078	Unknown	After SSO switchover, mcast ergess Vlan gets out of sync among DFCs
CSCsb81527	Unknown	sup2:Need enhanced FIB fatal error handling
CSCsb97997	Unknown	dot1dTpFdbAddress is broken
CSCsd42319	Unknown	SIP400 crashes during bootup with current pikespeak image
CSCsd58422	Unknown	%IXP_MAP-3-QOS_CONFIG: error detected: Can't download policymap
CSCsd78210	Unknown	FPD upgrade file search failed although the file is present.
CSCsd82457	Unknown	EOU Policy can't exempt Cisco 7935 Conference Station & Wireless phones
CSCse53517	Unknown	WiSM: Tracebacks seen after SSO switchover
CSCsf17163	Unknown	TCAM mask/entry resource not released after conf/unconf pacl
CSCsg00173	Unknown	v4 Sparse/SSM traffic when src is in PVLAN src port/DFC is not routed
CSCsg16964	Unknown	Sup32 crashes with 23rd image tb@_shmwin_error
CSCsg19793	Unknown	Psecure absolute aging on DFC causes MAC inconsistency w/ Central EARL
CSCsg22830	Unknown	Standby not coming up after sso switchover
CSCsg39754	Unknown	DHCP snooping redirect ACL permits more than just bootpc and bootps port
CSCsg87747	Unknown	RECV_PVID_ERR message received with bringing up etherchannel trunk
CSCsh16213	Unknown	Disabling MLDsnooping does not clean special MACs 3333.0000.0016, 3333.0
CSCsh57238	Unknown	SXF6:sh int cmd on 6148 cards display zero o/p drops even with qos drops
CSCsi00712	Unknown	Connected ipv4 routes for WAN interfaces missing on reload
CSCsi41749	Unknown	ITP-76:%SYS-2-INTSCHED: 'sleep for' at level 2 (Process- "MIP Mailbox")
CSCsi52715	Unknown	PISA:SIP200 and FW2 reboots on SSO switchover
CSCsi63649	Unknown	%SYS-3-TIMERNEG:Cannot start timer with negative offset,TTY Background
CSCsi74360	Unknown	packet loops between icpu and ocpu while sending clear mcast traffic
CSCsi76936	Unknown	Crash in GLBP if debug is enabled and it rcvs pkt from unknown group
CSCsi77983	Unknown	RP crashed ipflow_pak_pre_check on shutdown the trunk port
CSCsi97434	Unknown	A router may crash when ipsec is established
CSCsi99875	Unknown	BOOM: spa_eeprom_read_bit on BOOTUP
CSCsj25906	Unknown	Configuration changes made after scheduling a reload do not get saved
CSCsj28026	Unknown	WhitneyVS: Unable to mibwalk clcFdbVlanInfoTable . .
CSCsj43677	Unknown	Active Sup720 crash when removing Standy supervisor

Identifier	Technology	Description
CSCsj48453	Unknown	AW: CAT6k does not forward multicast traffic to WISM in L3 mode
CSCsj49293	Unknown	POS Interface Output Rate (200 mbps) > Line rate (155 Mbps)
CSCsj91738	Unknown	Non-ip packet with mcast-mac addr cause high CPU with VPN-SPA VRF mode.
CSCsk07255	Unknown	Sip-600 crash on SSO
CSCsk09552	Unknown	New varbinds showing real & virtual server info needed in SLB traps
CSCsk44233	Unknown	While raising the interrupt level, bgp_route_map_inform tries to suspend
CSCsk67578	Unknown	Flow End sysUpTime higher value than the Router sysUpTime
CSCsk80552	Unknown	Shut and no shut of interface causes the delay in forming rp mapping
CSCsk87262	Unknown	Switch crashes when polling port security MIB for SIP or Flexwan
CSCsk88760	Unknown	122SR:Routers crashes on unconfiguring vlan in the LACP mode
CSCsk93587	Unknown	TestFabricCh0Health test failure with unidir traffic via Ch1on Berytos
CSCsl02812	Unknown	TCP SYN packet lost for web applications when NAT outside IF is ATM
CSCsl04386	Unknown	%BIT-STDBY-4-OUTOFRANGE : Traceback on Bootup .
CSCsl18958	Unknown	IOS-SLB: Multicast packets are droped in SUP22 when FWLB is operational
CSCsl26998	Unknown	Switch crashes on applying PBR with next-hop verify-availability
CSCsl28371	Unknown	SPA-IPsec-2G VRF: L2 loop and broadcast storm may occur on default vlans
CSCsl39710	Unknown	cat6000 mac-address-table does not add entries for local fwsm mac . .
CSCsl52748	Unknown	SUP32 crash in tyfib_get_hw_index
CSCsl72912	Unknown	VS2: WS-X6708 DFC crash in local_cb1(Segment violation)
CSCsl74456	Unknown	VPN-SPA : TCAM not programmed on POS sub-interface after a reload
CSCsl74976	Unknown	Punted MPLS-tagged traffic causes control plane instabilities
CSCsl80682	Unknown	SPA crashes if crypto acl changed
CSCsl98238	Unknown	QoS statistics-export only exports to directly-connected destinations
CSCsm04256	Unknown	CPUHOG and crash after 'show memory detailed all statistics' issued
CSCsm11898	Unknown	IOS:SLB: Incorrect NAT Translation when Nat client is enabled
CSCsm13389	Unknown	RRI is not called be if QM rekey timer expiry forces SA deletion
CSCsm18546	Unknown	Root port is not selected with frameraly and bridge domain configs
CSCsm30858	Unknown	PIM register packets upmarked to TOS 6 by PTcam redirection
CSCsm31037	Unknown	URL maps are not properly downloaded to CSG
CSCsm32363	Unknown	Netflow SLB sw-installed entries not aging out
CSCsm37673	Unknown	Traffic from SSLM service module not going over multi-module etherchanne
CSCsm45453	Unknown	Missing 'lbusDrops' counter for WS-X6516A-GBIC in Native IOS
CSCsm48398	Unknown	mls cef adj leaking
CSCsm48410	Unknown	Vlan-based qos applied to channel when not configured after reload
CSCsm48913	Unknown	Transient SPI aging window is too long
CSCsm53873	Unknown	Module 1/0 failed in health monitoring configuration (error code 23)
CSCsm59926	Unknown	RP receives 2 copies of each PIM register with MVPN

Identifier	Technology	Description
CSCsm69112	Unknown	Multicast output drop w/ IGMP snooping @ near line rate 1Gbps
CSCsm69827	Unknown	%SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3
CSCsm70774	Unknown	Router crashes at cfg_kron_plcy_sbmd_cmd.
CSCsm73173	Unknown	Spurious memory access seen @ slb_lam_cfg_ft_track_interf
CSCsm75020	Unknown	EARL7 Additional ECC Error Handling enhancements
CSCsm78651	Unknown	malloc memory issue in standby SP supervisor
CSCsm79163	Unknown	Commit 8.6(0.306)R3V25 C2 FW libraries to the v122_18_sxf_throttle
CSCsm82382	Unknown	7600 standby RP memory leaking cause CEF disable
CSCsm82958	Unknown	radius sticky entry deleted even if the idle timer is not 0
CSCsm83948	Unknown	CISCO7609 returns sysObjectId as ciscoProducts.402 (which is cisco7606)
CSCsm84257	Unknown	crash in ipflow_periodic context due to watchdog timeout
CSCsm86027	Unknown	B2B failover,ace_tunnel_compare:Invalid address_type, router crashed
CSCsm87735	Unknown	OSM CHOC12/T1 - t1 shutdown does not disable Serial interface
CSCsm89251	Unknown	IPSec SA lifetime gets reduced during rekey
CSCsm94421	Unknown	Configuring STP cost in an etherchannel to the defaulthas no effect
CSCsm95456	Unknown	Duplicate L3 packets with 6708 and DEC
CSCsm97669	Unknown	Cat6K with NAT-T through PAT: IKE packets with src_port != 4500 dropped
CSCsm97775	Unknown	fix compile error for earl6
CSCso00793	Unknown	ITP-76: Flexwan Memory version "VI4DP647228EBK-MD" causes reload
CSCso10819	Unknown	LC not reset after 10 consecutive failures of TestMacNotification
CSCso12903	Unknown	RE MET address check missing while running MET patch on IO bus timeout
CSCso17569	Unknown	VPN-SPA: WAN interface mtu incorrectly programmed on the SPA
CSCso20519	Unknown	Cheronia: Fix SMB drive strength programming.
CSCso30038	Unknown	A OIL is not registerd properly in mroute table with static igmp group
CSCso31506	Unknown	IPv6 AH Extension Headers Punted to Software on PFC-3B & 3C
CSCso37640	Unknown	DHCP snooping ACL's are not getting programmed after switchover.
CSCso38129	Unknown	Tracebacks seen on standby & switch crash after switchover w/ct3 config
CSCso44072	Unknown	High CPU due to multicast traffic getting punted to software
CSCso53741	Unknown	VPNSPA does not handle duplicate IPSec SA correctly in nested tunnel
CSCso71355	Unknown	PVLAN - 6500 - Multicast flood broken from pvlan port to promiscuous
CSCso78097	Unknown	OSM-ct3 MFR interface is flapping
CSCso81945	Unknown	removing natpool doesn't remove from the slb-policy automatically
CSCso84567	Unknown	6500 with WCCP and CoPP punts non-TCP packets into CoPP policy.
CSCso85395	Unknown	Unable to add the 256th vlan
CSCso87348	Unknown	Corruption in subflow code
CSCso87838	Unknown	HSRP: with aggressive timers HSRP peer flaps when "wr mem"
CSCso89069	Unknown	NBAR Unable to undo port-map change for softphone protocol

Identifier	Technology	Description
CSCso89550	Unknown	cat6k crash due to SP: Supervisor has bad local fabric channel
CSCso89823	Unknown	Pos interface "rxload" and "input bytes" counters incorrectly increment
CSCso97524	Unknown	Packet drop after TCAM exception happened
CSCsq00884	Unknown	"mls qos trust" cmd lost under port-channel interface when upgrading IOS
CSCsq04355	Unknown	Fix in CSCso81632 is not complete
CSCsq12119	Unknown	SXF13 Crash on VPNSM OIR due to chunk memory double free.
CSCsq14259	Unknown	TX Flowcontrol goes on when link negotiation is disabled
CSCsq19146	Unknown	FPD creation for new pegasus rx (1.6) FPA image for Sip-1 CR
CSCsq19476	Unknown	DMVPN over POS - wrong spa vlan in cef adj after boot, gre sent in clear
CSCsq20970	Unknown	ATM option missing, while configuring T1 controller for mode atm
CSCsq29165	Unknown	Rockies-sup3:UUT hangs during installation
CSCsq37376	Unknown	Packet Buffer Capture May Crash a 6500 in IOS
CSCsq39079	Unknown	SPA-IPSEC-2G Crash under load due to IKE session establishment
CSCsq41311	Unknown	I/O memory leak in Medium buffers
CSCsq47140	Unknown	67xx module may not come online
CSCsq48271	Unknown	adding redundant CSM causes config sync to indicate in sync when not
CSCsq50429	Unknown	OSM card unexpected reload @ cwtlc_qos_create_global_qid_info
CSCsq53822	Unknown	Monitor session removal may affect traffic through WS-X6148A-RJ-45
CSCsq59297	Unknown	port-channel IDB gets mixed up
CSCsq60553	Unknown	Create cwslc-rommon3.bin for cwpa2 to accomodate release Rommon (1.8)
CSCsq77381	Unknown	W2: Diag - TestL3Capture2 failed after LV-SSO
CSCsq77464	Unknown	mls rate-limit unicast cef receive value re-written upon TCAM exception
CSCsq79253	Unknown	Pinnacle interrupts not re-enabled after memory inconsistency detected
CSCsq85850	Unknown	Opnext GLC-LH-SM :remote port stays up when local RX cable is removed
CSCsq89415	Unknown	"no bert" indicates "abort request" instead of "stopped"
CSCsr09554	Unknown	Move SIBYTE SB_RMON_OVRFL messages under debug
CSCsr28305	Unknown	Packet drops on L2 portchannel on WS-X6708-10G
CSCsr54630	Unknown	Patch workaround and s222 build fix for CSCso53756
CSCsr99933	Unknown	FWLB: High purge rate causes CPU to increase by 15%
CSCsu03772	Unknown	Dot1q native vlan tagging is not working with "switchpot nonegotiate"
CSCsu36712	Unknown	cpu spike on "pim process" with SUP32PISA with looping PIM JOIN/PRUNE
CSCsv34544	Unknown	Unexpectedly low throughput on PISA with NBAR enabled
CSCsw45069	Unknown	tx stats incorrect imcrement for debug purpose
CSCsg32308	WAN	copy/paste of ntp-authentication-key statement is not possible
CSCsl90285	WAN	POS-APS: CWPA-3-NODISPATCH messages seen when configuring APS

Resolved Caveats in Release 12.2(18)ZYA

Resolved Caveats for Product 'all' and Component 'aaa'

- CSCsj91123—Resolved in 12.2(18)ZYA

  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.

Resolved Caveats for Product 'all' and Component 'dlsw'

- CSCsk73104—Resolved in 12.2(18)ZYA

  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://www.cisco.com/en/US/products/csa/cisco-sa-20080326-dlsw.html

Resolved Caveats for Product 'all' and Component 'ifs'

- CSCsk61790—Resolved in 12.2(18)ZYA

  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 Caveats for Product 'all' and Component 'ipsec-isakmp'

- CSCsg35077—Resolved in 12.2(18)ZYA

  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 Caveats for Product 'all' and Component 'os'

- CSCsk33054—Resolved in 12.2(18)ZYA

  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 Caveats for Product 'all' and Component 'ssh'

- CSCsi17158—Resolved in 12.2(18)ZYA

  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#Applying_the_ACL_to_an_Interface_or_Terminal_Line

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

Resolved Caveats for Product 'all' and Component 'ssl'

- CSCsj85065—Resolved in 12.2(18)ZYA

  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 Caveats for Product 'all' and Component 'ts'

- CSCsj86725—Resolved in 12.2(18)ZYA

  This DDTS addresses the issue in the Cisco Product Security Incident Response Team (PSIRT) response to an issue discovered and reported to Cisco by Andy Davis from IRM, Inc. regarding a stack overflow in the Cisco IOS Line Printer Daemon (LPD) Protocol feature.

  This security response is posted at: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20071010-lpd

Other Caveats Resolved in Release 12.2(18)ZYA

Identifier	Product	Component	Description
CSCsj83102	all	7x00-t1e1	crash upon card type configuration on WS-X6582-2PA / PA-MC-8TE1+
CSCee89849	all	aaa	Router reloaded at vtemplate_build_command_strings
CSCsc98046	all	aaa	TACACS Accounting isn't sending stop time in the stop packet.
CSCsf30451	all	aaa	radius-server attrib 32 include-in-access-req/accounting-req not sent
CSCsh23142	all	aaa	aaa local authentication not happening for authproxy .
CSCsh46990	all	aaa	Console hangs with enable/line as aaa fall-back methods
CSCsh59019	all	aaa	Avoiding AAA client hangs, if a protocol subsystem is not present.
CSCsj89305	all	aaa	RADIUS/NAS-IP address is sent out as 0.0.0.0
CSCsj97165	all	aaa	%AAA-3-BADMETHODERROR: Router crash @ aaa_get_new_acct_reg_type .
CSCsl33966	all	aaa	C6509 : attribute 32 nas-Id not sent for Auth (missed by CSCsf30451) .
CSCsm06740	all	aaa	Memory Leak in AAA accounting and Virtual Exec
CSCeb69473	all	analysis	connect '/terminal-type' command memory corruption
CSCei79855	all	ata-filesystem	IOS resilience fails to work properly with secure boot command .
CSCse20115	all	ata-filesystem	System hangs when writing to a file, when the disk space is full
CSCsg15939	all	ata-filesystem	Switches crash after remove/plug in compact flash
CSCsh48919	all	ata-filesystem	Embedded spaces in DOSFS dirs/file names cause crash in some platforms
CSCek61180	all	atmcommon	crash @ write_to_url, doprintc_core, atm_remove_vc
CSCsd84347	all	atmcommon	PVC stops sending OAM loopback if AIS/RDI received
CSCeg25475	all	bgp	Distribute-list configured in ipv4 acts in vpnv4 address-family

Identifier	Product	Component	Description
CSCei93768	all	bgp	check heaps CHUNKBADMAGIC crash at BGP Router when remove dmzlink ba .
CSCek62005	all	bgp	ip prefix list deletes lists before sending notif (causing rtr crash
CSCsc75426	all	bgp	Crash when BGP sends update with bad attribute .
CSCsc98835	all	bgp	CPUHOG when access-list is modified causes OSPF and BGP session drops .
CSCsg16778	all	bgp	router may crash at bgp_update_nbrsoo after deleting BGP neighbor .
CSCsg55591	all	bgp	MPLS VPN Local label not allocated/programmed for sourced BGP network
CSCsh88825	all	bgp	bgp: advertisement-interval not nvgened for peer-groups
CSCsj78403	all	bgp	clear ip bgp causes crash to RR client with conditional route injection
CSCsj99269	all	bgp	BGP: VPNv4 general scanner runtime close to 1 hour at boot time .
CSCsk34344	all	bgp	Wrong share-count 1:10 via confed-external BGP peers using dmzlink-bw
CSCsk70844	all	bgp	%SYS-4-REGEXP: new engine: regexp compilation had failed -BGP Router
CSCsl07297	all	bgp	SXF11: BGP "no neighbor" command caused Address Error exception .
CSCsj64230	all	bidir-pim	bidir DF election should not be restarted on a downstream interface
CSCek72777	all	c6k-wan-common	%CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR for 7600 SIP card .
CSCsi91324	all	c7600-mcast	MCAST packet drop when other interface goes down on DFC
CSCsg99914	all	c7600-sip-200	sip-200 power-cycles after BGP flap (not responding to keepalive)
CSCsi87837	all	c7600-ssc-400	IF-MIB does not support gig interfaces on SPA-IPSEC-2G
CSCsj56086	all	cat6000-acl	WCCP and VACL cause Cisco router CPU High
CSCsk41374	all	cat6000-acl	device crash seen when auth-proxy enabled on the LPIP vlan .
CSCsh99116	all	cat6000-fib	bits/sec counter is way off in show int vlan
CSCsl89176	all	cat6000-l2	Cat6k may crash when vlanTrunkPortEntry is polled via snmp
CSCsj68774	all	cat6000-mpls	SIP-600 SXF bus error in const_mpls_collect_imp_te_stats .
CSCsk20887	all	cat6000-routing	Packets are route cached on multilink bundle .
CSCsl21106	all	cat6000-sw-fwding	Tunnel destination command crashes MSFC running in hybrid mode .
CSCsg88433	all	cdp	IP Telephone issues seen with Dhcp snooping and NAC posture validation
CSCsg21418	all	clns	Bus error related to CLNS fast switching
CSCsg95101	all	clns	ALIGN-3-SPURIOUS: Spurious memory access
CSCdz55178	all	cmts-docsis	QoS profile name of more then 32 chars will crash the router .
CSCsa79984	all	comm-serv	CTRLC_ENBL should be cleared when line is reset
CSCsi10974	all	dhcp	Error configuring dhcp option 67
CSCse13882	all	dlsw	Show dlsw peer caused router to crash
CSCsh92031	all	eapoudp	Sierra: Standby RP crashed at auth_proxy_posture_clear_nacl

Identifier	Product	Component	Description
CSCee04271	all	eigrp	eigrp does not send update of poisoned route to stub router
CSCsc73725	all	eigrp	EIGRP packet pacing should have lower minimum value
CSCsh82953	all	eigrp	EIGRP pece routes missing extcomm attrs after redistribution to BGP .
CSCsi14346	all	eigrp	EIGRP: neighbor command missing in VRF.
CSCsi58303	all	eigrp	eigrp resync peer graceful-restart repeatedly after reload .
CSCsj25940	all	eigrp	%SYS-2-NOTQ: unqueue didn't find 6433F698 in queue .
CSCsj53663	all	eventmgr	EEM: RP crashed at fh_fd_syslog_event_match
CSCsj77819	all	fib	After SSO traffic is punted to the CPU for 20 seconds
CSCsk27685	all	fib	FIB-DFC2-4-FIBMSG: Invalid message received On bootup .
CSCei22295	all	fr	Traceback is seen at fr_svc_teardown_calls
CSCsb87686	all	fr	Spurious Access when attempting to configure a connection on MFR bundle
CSCsc38968	all	fr	Frame-relay EEK failure does not keep subinterface down
CSCsh58099	all	ftp	ftp process should call a registry cleanup- Message Could not register..
CSCsl36293	all	hsrp	Bus Error crash at standby_arp_add_if while config-change .
CSCsk29013	all	igmp	IGMP groups in the vrf not rejoined after executing a cle ip mr vrf
CSCsh64639	all	iml	VS2: [dead threads] process takes a large chunk of CPU util
CSCsj84641	all	install	some patches failed to commit during install commit of 41 patches.
CSCsh52941	all	ios-authproxy	AUTHPROXY:CLI to increase the number of HTTP Proxy process
CSCsi10945	all	ios-authproxy	Http Auth-proxy with OTP does not display token/SNK challange
CSCsi22243	all	ios-authproxy	Memory leak in *Dead* process due to HTTP Proxy Server
CSCee19119	all	ip	IP installs route for PPP interfaces that did not complete IPCP
CSCek76776	all	ip	ip interface settings persistent after deleting/adding sub-interface
CSCsi58867	all	ip	CPUHOG After show ip route static or show ip route connected
CSCsk46195	all	ip	Arp entry does not age out with private vlans and no ip sticky-arp
CSCsm27979	all	ip	router may crash for "address error exception" doing sh ip route vrf
CSCsk26719	all	ip-acl	show ip access crash with per-user acl
CSCeg85087	all	ipmulticast	S,G expire timer set to 3:00 when no downstream pim join
CSCsg24505	all	ipmulticast	PIM-DM Assert winner does not always send prune
CSCsh78277	all	ipmulticast	Sierra: mwheel CPUhog on RPF link failure causing crash .
CSCee73221	all	ip-rip	Split Horizon is in effect on redistributed static routes .
CSCsh57509	all	ip-rip	RIPv2 does not delete redundant paths with different next hops .
CSCsi20281	all	ip-rip	Static route redistribution into RIP fails on ACL change
CSCsi80057	all	ip-rip	RIP default-information originate with route-map not working correctly .
CSCsl47915	all	ip-rip	Redistribution of ospf in rip with prefix-list not working properly
CSCsm22805	all	ipsec	hsrp crypto map config got removed after reload
CSCsm32840	all	ipsec	Router crash in dmvpn-vrf setup after cheronia reset
CSCin67370	all	ipsec-core	Changing ACL or the crypto map leaves it empty ident tree .

Identifier	Product	Component	Description
CSCsb29131	all	ipsec-core	show crypto ipsec sa identity detail causes system to reload
CSCsk26973	all	ipsec-dmvpn	Memory leak in nhrp_cache_delete for incomplete cache entries
CSCsl32122	all	ipsec-ezvpn	Remote Access for certificate users fails during mode config
CSCsm32493	all	ipsec-ezvpn	Backout of CSCsh94882
CSCin89549	all	ipsec-isakmp	Router crashes if AAA returns ipv4 address attrib with no xauth
CSCsg09423	all	ipsec-isakmp	IPSEC SAs dont recover after rekey with 3000 IKE SAs and PKI (RSA-Sig) .
CSCsh53141	all	ipsec-isakmp	IKE SA not getting deleted after clear crypto session
CSCsi52382	all	ipsec-isakmp	radius attribute 5 nas-port not sent in access-request for RA VPN users
CSCsk19590	all	ipsec-isakmp	Mem Leak in IKE NODE causes router crash . .
CSCsk41134	all	ipsec-isakmp	ISAKMP SA neg not successful for in tunnel mode w/ RSA-SIG
CSCsl27236	all	ipsec-isakmp	%SYS-3-CPUHOG: Task is running for (126000)msecs, causes RP crash .
CSCsk21328	all	ipv6	6504 crashes in IPV6
CSCee04303	all	isis	Spurius Memory access during boot while processing an isis update
CSCsf05579	all	isis	ISIS passive-interface default problem in IOS 12.2(18)SXF
CSCsg40507	all	isis	SIERRA:ISIS/BFD session doesnt come up after changing ip-addr of interf
CSCsi57971	all	isis	ISIS does not advertise prefix of passive interface
CSCsj72039	all	isis	Prefix not in ISIS database if serial interface and passive
CSCsm17391	all	isis	ISIS routes are not learned through interfaces
CSCsj03722	all	laminar	exit command is subject to authorization
CSCsj33042	all	laminar	Cat6k crashes when unconfiguring vserver (CSM)
CSCej02181	all	loadbal	SLB: cannot configure weight 0
CSCsk65482	all	loadbal	clear ip slb CLI is defined with wrong privilege level
CSCei28317	all	mcast-vpn	PIM-6-INVALID_RP_JOIN reports 0.0.0.0 for source of invalid neighbor
CSCsf13044	all	mcast-vpn	MVPN: Bidir mroute OIF missing - pim joins not received from MDT tunnel
CSCsk30146	all	mcast-vpn	Router crashed %DUMPER-3-PROCINFO: pid = 12315: (sbin/ios-base) SIGBUS
CSCsb66972	all	mem	show memory shows negative numbers with 4GB RAM
CSCsj58223	all	mem	Bus Error after 'show memory' .
CSCsl41784	all	mobileip	ION: ARP Input memory leak with "mobile ip arp"
CSCej00319	all	mpls-ldp	RP Crash for E2 E3 E4 E4P interaction
CSCsa70235	all	mpls-ldp	LDP doesnt withdraw all labels after routes gone
CSCsk05059	all	mpls-lfib	NRT: traceback tfib_post_table_change_ tfib_ipfib_ ip_fib_table_
CSCsk36276	all	mpls-lfib	SXF11: on SSO switchover tracebacks are seen at network_redist_ndb_updat
CSCsk52331	all	mpls-lfib	Xconnect configuration triggers entire fib table walk
CSCsk55768	all	mpls-lfib	TAG adj doesn't recover after flap

Identifier	Product	Component	Description
CSCdy83805	all	mpls-te	%MPLS_TE-3-CONSISTENCY: consider replacing errmsg with buginf
CSCsk09197	all	mpls-te	RSVP hello instance remains at shut-down interfaces
CSCsb67427	all	mpls-vpn	Label not allocated for imported iBGP in ASBR/PE after flap 'mpls ip'
CSCsk30567	all	mpls-vpn	local label for inter-as vpn not programmed on LC Eng 5 on an ASBR .
CSCsl72702	all	mpls-vpn	MPLS should not allocate labels on standby RP in HA setup
CSCeh56158	all	nat	NAT outside source translation fails for GRE packets .
CSCeh65511	all	nat	Connected int IP may not be reachable with a static NAT trans
CSCsg97662	all	nat	Cant disable skinny (tcp 2000) .
CSCsj29841	all	nat	Port forwarding breaks NAT-overload on a 6509
CSCek76062	all	netflow-switch	Router crashed @ validmem_complete_interrupt .
CSCsd80770	all	netflow-switch	Netflow exports UDP packets with source port 0
CSCir01217	all	neutrino	name_svr.proc[64]: Could not register interest
CSCsi24069	all	neutrino	Collect additional debug info for Modular IOS kernel crashes
CSCsj17820	all	nhrp	Hub crashes during unconfiguration due to program counter error
CSCsj68446	all	ntp	NTP will not sync - NTP packets received but ignored by NTP process .
CSCsg43466	all	os	%IPC-5-INVALID: Invalid Dest Port w/ TB @ ipc_xmt_account after SSO
CSCsk37278	all	os-boot	BFD clients flaps when boot string is removed from "show running" .
CSCsg52740	all	osm-qos	OC48 OSM replicates same packet at line rate
CSCek33384	all	ospf	Tunnels stay down after cutover at MPLS head test cases
CSCsd11019	all	ospf	Rainier:After RPR-Plus switchover standby RP crashes
CSCsf00171	all	ospf	summary route not flushed from ospf database
CSCsi11438	all	ospf	OSPF does not remove maxage LSAs and age goes to bigger than 16 bit
CSCsj06265	all	ospf	Switch crashes when doing clear ip ospf process
CSCsl14632	all	ospf	SXF12:%LDP-5-NBRCHG: LDP Neighbor is down after SSO Switchover .
CSCsi15080	all	parser	RP crash when listing files by using the context-sensitive help
CSCsk38461	all	parser	Show platform hardware command getting rejected .
CSCsj57084	all	pas-atm	Voice packets in LLQ experience latency
CSCse17175	all	pas-chstm1	Line down on some serilal interfaces for Chann STM-1 SMI PA
CSCsi00099	all	pas-ct3	Spurious Memory Access Error @ ct3sw_check_freedm_fifo
CSCsg95192	all	pim	no ip rp-address <ACL name> causes an address error
CSCsi03359	all	pim	Sending extra PIM hello if the first one does not go through
CSCef54653	all	ppp	Members inactive in a multilink bundle except the first member. .
CSCsd30719	all	ppp	A2A: Stdby sup crashes @ mlp_remove_link .
CSCse28421	all	ppp	%AAAA-3-BADSTR error when Multilink interface goes down .
CSCek78675	all	qos	SIP200 crash at hqf_cwpa_pak_enqueue_local during qos test .
CSCsd17641	all	qos	SIP-400 QOS: after changing hier. policy, the policy no longer attaches

Identifier	Product	Component	Description
CSCsi73132	all	qos	Multicast DSCP value not copied to PIM-SM RP-register packet
CSCsk63794	all	qos	FlexWAN WS-X6582-2PA + T3+ Serial PA may crash/reload
CSCsk79703	all	qos	SIP-200 crashes when moving MFR bundle from OSM to SIP-200
CSCsa65031	all	rsps-time-rptr	show rtr distriution-statistics inactive status
CSCsk53642	all	rsvp	RSVP PATH msg not forwarded to MCAST receiver .
CSCsl70734	all	rsvp	Commiting CSCsk53642 broke build.
CSCsh91974	all	security	PIM CLI causes RP crash when issued under control-plane subconfig prompt
CSCeg88630	all	snmp	E3 GE:Linkdown trap via snmp not properly raised
CSCsb95806	all	snmp	Incorrect 64bit counter on 1Gb MPLS interface via SNMP .
CSCsg39295	all	snmp	Syslog Displays Password if SCP or FTP Selected in CISCO-COPY-CONFIG-MIB
CSCsg71381	all	snmp	Disabling cisco-specific lsa and tty, removea all ospf trapa from conf
CSCsh42866	all	snmp	Static analysis on SNMP code
CSCsj83966	all	snmp	Syslog traps cause CPUHOG when lot of interface come up at same time. .
CSCsk06492	all	snmp	snmp-server drop vrf-traffic implementation in 12.2 SRB train
CSCsk10335	all	snmp	Traceback @ ipc_send_message_blocked during bootup .
CSCsk61555	all	socket	Bus Error Exception in sock_tcp_directwakeup . .
CSCsk81396	all	socket	NAM process crash in 12.2SXF .
CSCsj35776	all	spa-atm-all	Some of the VCs are INACTIVE after SPA OIR
CSCin91851	all	ssh	Support keyboard-interactive authentication method
CSCsg48392	all	ssh	Resuming SSH Session Fails After Disconnecting Another One (Not Console)
CSCsj45031	all	ssh	Cat6k unable to SCP files from Tectia ssh server
CSCsj60938	all	ssh	SCP with redirect option locks up console or VTY line .
CSCsi99234	all	tcl-bleeding	RP crash at validblock with %SYS-6-BLKINFO: Corrupted redzone blk
CSCef52888	all	tcp	PMTUD: MSS is not adjusted which causes the BGP flaping .
CSCeh35980	all	tcp	after unconfig & config of BGP, seeing a crash in TCP .
CSCek68118	all	tcp	window scale option(03030001) occurs in debug ip tcp packet output .
CSCsj89544	all	tcp	TCP retransmissions get dropped below IP layer. .
CSCeb76035	all	telnet	Spurious access or crash from snmp_trap_for_tty
CSCsl10348	all	tftp	Crash writing to or from ftp/tftp server in modular IOS
CSCsg60447	all	trans-bridging	7200: BVI stops receiving CLNS/ISIS packets
CSCsk39022	all	udp	Modular IOS: ip directed-broadcast not working
CSCsk80935	all	udp	SXF12, SNMP response being broadcast .
CSCsl27840	all	vipmlp	Router may Crash / Hang, Module Reset @ Shut ATM member + MLPOA
CSCsj18014	all	voice-sig-analog	Caller ID string received with extra characters

Identifier	Product	Component	Description
CSCsh31782	all	vpn-sm	Bus error crash - show crypto isakmp sa
CSCsl26997	all	vpn-sm	Catalyst 6500 may crash when reseting VPNSM module .
CSCsi91658	all	wccp	Wccp stops layer 2 redirection when dscp is present in the redirect acl
CSCsl04908	all	wccp	WCCP: shutdown of appliance i/f leads to c6k reload
CSCsl65335	all	wccp	WCCP: reload following ACL update
CSCsl19708	all	ws-ssc-600	Naxos : Disable Telesto Internal TERMINATION For Reference Clock, PB RAM
CSCed17607	c10000	atmcommon	Reapplying oam-pvc manage does not send oam cells until shut/no shut
CSCsi25729	c12000	isis	ISIS doesn't enable BFD except after micro reload
CSCsc57207	c2800	pas-ct1	itevent flooding: code 10 arg0 0 arg1 0 arg2 0 error messages on 7200
CSCsg52355	c6k-ace	itasca-sup	RHI Injected routes lost after SUP switchover
CSCse13374	c6msfc	pas-atmima	IMA ports on 7600 always initialized to default clocking on bootup .
CSCsi32655	c6venus-slb	csg	MOD CSG <#> config mode command applied to a running CSM clears config
CSCee13737	c6venus-slb	laminar	CSM - sho mod csm # sticky reports invalid # of connections
CSCsg72976	c6venus-slb	laminar	CSM - need to add standby state to mib object slbRealServerState
CSCef82084	c7200	7x00-t1e1	Spurious memory access in pot1e1_tx_interrupt
CSCsd88768	c7200	7x00-t1e1	%SYS-2-BADSHARE: Bad refcount in datagram_done fix for PA-MCX-8TE1
CSCsh34949	c7200	dlsw	DLSW router crash with Bus Error
CSCsh85531	c7200	pas-chstm1	E1 channels down after PE reload
CSCin67287	c7500	7x00-t1e1	NxDS0 BERT capability on PA-MC-8TE1+
CSCsj78525	c7500	atmcommon	%ALIGN-3-CORRECT, %ALIGN-3-TRACE on the 7500 with 123-22
CSCsl06110	c7600	c7600-acl	DHCP snooping agent: parse failures when importing the DB
CSCsl08912	c7600	c7600-acl	Vlan access list not working when have "xconnect vfi #" under the SVI
CSCsl52092	c7600	c7600-acl	DHCP db agent considers port-channel interface (poX) as invalid
CSCsk89335	c7600	c7600-env	After SSO switchover, see 6K DC power supplies mismatched .
CSCek68218	c7600	c7600-field-diag	sip-600 crashing with diagnostics error online_wan_diag_rp_request
CSCsi65363	c7600	c7600-ha	Not able to run to t1 loopback when using a PA-MC-T3 with flexwan
CSCsk06769	c7600	c7600-lcsw-bridge	shut on L2 int cause packets to loop back on T1 int causing traffic loss
CSCsl49734	c7600	c7600-sip-200	IF_INDEX_ILLEGAL errors and crash due to memory corruption on standby RP
CSCsl59553	c7600	c7600-sip-400-ucod	SIP-400: bursty traffic causes packet drop even in low rates
CSCse81313	c7600	c7600-sip-600-ucod	policy-map not matching classes in POS STM64 in SIP600
CSCsk19652	c7600	c7600-snmp	Failed to assert Physical Port Administrative State Down alarm
CSCsj95291	c7600	cat6000-fib	100% CPU (FIB Control Queue Process) after enabling MPLS .
CSCsj37078	c7600	cat6000-qos	permit missing for internal vlan acl - causing vrf connectivity failure
CSCsk55423	c7600	cat6000-sw-fwding	7600's SPD implementation allow COS 5 or above in Extended headroom

Identifier	Product	Component	Description
CSCsj58538	c7600	ha-idb-sync	Lots of prowler/patriot interface go down for few second during sso swov
CSCsh56720	c7600	ipmulticast	CPUHOG/Watchdog timeout when using igmp static group class-map cmd
CSCsj17950	c7600	isis	ISIS redistributed static routes might not be advertised
CSCsk66339	c7600	isis	ISIS fails remove native path from local RIB / del path from global RIB
CSCsd55004	c7600	mpls-te	FRR path gets reoptimized while in Active state
CSCse18146	c7600	nbar	SIP1-CT3: SIP1 crashed after switchover @giant_node_process .
CSCsk08765	c7600	osm-choc-ds0	Bus error when executing 'encapsulation frame-relay mfr' .
CSCsj93609	c7600	osm-choc-ds3	Missing DS3-MIB table entries for OSM-1CHOC12/T3
CSCsj93636	c7600	osm-choc-ds3	Incorrect value returned for dsx3TotalUASs
CSCsf32441	c7600	osm-ct3	ALIGN-3-CORRECT: messages from process_t1e1s
CSCsj76268	c7600	osm-ct3	Autosense LMI stops responding invalid lmi type on OSM-12CT3/T1
CSCsk17205	c7600	osm-ct3	OSM:MFR LMI packets are not send out through the MFR i/f
CSCsk19333	c7600	osm-gigwan	GE-WAN interface shows incorrect link state with ws-g5483 GBIC
CSCsl20422	c7600	osm-gigwan	PXF points incorrect adjacency
CSCsi98355	c7600	osm-pos	LOP does not bring the line protocol down on OSM-1OC48-POS
CSCsj64023	c7600	osm-ucode	MPLS: Sup2 OSM sending TTL=0 packets on MPLS VPN
CSCsd18278	c7600	spa-ser-infra	Host backpressure is not handled by SPA IPC firmware code
CSCsk82821	c7600	tcp	The UUT not able to receive the Large ICMP message.
CSCsg55315	cat6000	c6k-wan-common	Packets duplicated out of Gig1/1 when SPAN Monitor session enabled
CSCsi79991	cat6000	c7600-acl	VACL capture not supported for the GE-WAN or GigabitEthernet on SIP-400
CSCsj10744	cat6000	c7600-acl	Input queue wedged with Inband Edit Packets on SIP-400
CSCsm15350	cat6000	c7600-spa-ipsec-2g	vpnspa crashed at assert failure in l2-mcpu.c on line
CSCek66590	cat6000	c7600-ssc-400	C7600-SSC-400: Crash in show hw-m subslot x status volt
CSCsj58287	cat6000	c7600-ssc-400	7600-SSC-400 crashes on reload
CSCsm21126	cat6000	c7600-ssc-400	C7600-SSC-400: Resync fabric interface on fabric error
CSCsb62762	cat6000	cat6000-acl	Crash no vlan access-map test .
CSCsi51649	cat6000	cat6000-acl	RP crashes@fm_send_inband_install_message+21C in many cases with NAT
CSCsj11561	cat6000	cat6000-acl	Inconsistent MTU for Adj. entries used by MLS Netflow and MLS CEF
CSCsj29583	cat6000	cat6000-acl	Add warning message to 12.2SXF when configuring PACL
CSCsj60883	cat6000	cat6000-acl	Error msg. Unable to change flowmask to full-flow because Cx is configur
CSCsj72251	cat6000	cat6000-acl	BOOTP replies dropped if DHCP snooping is enabled
CSCsk21414	cat6000	cat6000-acl	NAC : Buffer leak in small buffer pool .
CSCsk34237	cat6000	cat6000-acl	Egress multicast replication broken due to wccp .
CSCsl63311	cat6000	cat6000-acl	6500 May Experience High CPU due to NAT traffic

Identifier	Product	Component	Description
CSCsj68911	cat6000	cat6000-cm	DFC mem leak in SP Logger Proces when redundancy force-switchover issued
CSCsi99991	cat6000	cat6000-cmm-voice	When CMM is rebooted, FE goes into ErrDisabled state
CSCsc98471	cat6000	cat6000-diag	show diagnostic sanity fails to check software modularity boot string .
CSCsd90173	cat6000	cat6000-diag	TestIPSecEncrypDecrypPkt HM test config init error reporting is needed
CSCsh83109	cat6000	cat6000-diag	HapiEchoTest fails on SPA-IPSEC-2G when reset.
CSCsk60874	cat6000	cat6000-diag	show tech needs 'show diagnostic results' and 'show diagnostic events' .
CSCsm01399	cat6000	cat6000-diag	Bus idle recovery may cause 10GE interface to remain down
CSCse32876	cat6000	cat6000-dot1x	dot1x:cli missing for Ten Gig Ports for dot1x initialize/ reauthenticate
CSCei76590	cat6000	cat6000-env	Different wattage WS-CAC-4000W-US caused PSREDUNDANTMISMATCH output
CSCek45036	cat6000	cat6000-env	Interuppt throttling to be implemented for Sibyte Modular IOS images.
CSCsk12525	cat6000	cat6000-env	Disabling 67xx line cards with DFC3C/DFC3CXL except WS-X6708-10GE
CSCsk27835	cat6000	cat6000-env	Disable unsupported service modules in SXF Software Modularity images
CSCsk80934	cat6000	cat6000-env	Add errmsg to clearly indicate if lc reset due to power convertor failur
CSCsk91267	cat6000	cat6000-env	Module fails to come up with (FRU-power failed)
CSCsk33661	cat6000	cat6000-fabric	show platform hardware capacity should include LTL usage .
CSCsj52192	cat6000	cat6000-firmware	FE stays up when remote 'inline powered' is shutdown w/ 100Mbps/Full
CSCsj73669	cat6000	cat6000-firmware	Disable DOM hardware periodic updates (xenpaks/x2s)
CSCsk16974	cat6000	cat6000-firmware	Sup2 - Bus Asic #0 out of sync error .
CSCsk83646	cat6000	cat6000-firmware	BX10 ports don't link-up after Centaurus resets . .
CSCsl70634	cat6000	cat6000-firmware	67xx EC tx/rx traffic dependency resulting in low throughput
CSCsl97653	cat6000	cat6000-firmware	bcm2_5421_isr bcm2_num: 1 messages seen in the log
CSCsm08419	cat6000	cat6000-firmware	debounce timer issue on sup32 10GE uplink and 6708
CSCsh34467	cat6000	cat6000-ha	Standby constanly reset due to RF request with large configuration .
CSCsk80787	cat6000	cat6000-ha	SXF12 CLI: system crash when create Po interfaces . .
CSCsk84237	cat6000	cat6000-ha	SIGSEGV, Segmentation violation in rf_proxy_fatal_error . .
CSCsl34647	cat6000	cat6000-ha	18SXF: RPR RF Keep alive swover not working
CSCsc56179	cat6000	cat6000-hw-fwding	mac-address is not purge when interface is shutdown .
CSCsi11874	cat6000	cat6000-hw-fwding	Sup720 DFC forwarding some packets to MSFC instead of hw switching
CSCsj67096	cat6000	cat6000-hw-fwding	Issue w/NATed traffic on PortChannel (WS-X6408 and WS-X6516) on Sup720
CSCsk18206	cat6000	cat6000-hw-fwding	TCAM adjacency hardware programming problem with PBR and NAT .
CSCsk40931	cat6000	cat6000-hw-fwding	Port Security Inactivity Aging is not working as expected
CSCsk70087	cat6000	cat6000-hw-fwding	Sup720 TLB exception created by fill_earl_vlan_stats_hdr .
CSCsl51380	cat6000	cat6000-hw-fwding	Sup720 and Sup32 TCAM & SSRAM Consistency Checkers refinement
CSCsl83211	cat6000	cat6000-hw-fwding	Sup32 running ION image fails to bootup after a power-cycle.

Identifier	Product	Component	Description
CSCsc75381	cat6000	cat6000-l2	Native vlan mismatch is not detected if native not allowed on trunk .
CSCse33420	cat6000	cat6000-l2	LACP: config for some other port-channel gets removed on bundling ports
CSCsf98341	cat6000	cat6000-l2	UDLD failed to receive PDU when linked to L3 port.
CSCsg27123	cat6000	cat6000-l2	Learning not disabled on SPAN dest without learning option
CSCsg50698	cat6000	cat6000-l2	18SXF: set entPhysicalAlias of XENPAK cause stdby-reset .
CSCsj10375	cat6000	cat6000-l2	802.1X: VLAN Changing on port causes link to go down
CSCsj18494	cat6000	cat6000-l2	Leak +MN to pfc to avoid flooding due to tx span .
CSCsj45951	cat6000	cat6000-l2	DOM Polling May Cause Link Flaps on Some Xenpak Transceivers .
CSCsj56703	cat6000	cat6000-l2	SSO failover causes RSTP forwarding and physical interfaces blocking .
CSCsk33724	cat6000	cat6000-l2	DOM does not work anymore for cwdm gbic/sfp
CSCsk84944	cat6000	cat6000-l2	unidirectional Ethernet UDE is broken on WS-6704 after SW upgrade
CSCsh33518	cat6000	cat6000-l2-infra	STP information is not in sync with Active .
CSCsh88532	cat6000	cat6000-l2-infra	Auto-LAG EtherChannel not configurable; doesn't trust QoS. .
CSCsh97848	cat6000	cat6000-l2-infra	Sierra: LACP pdus should be untagged .
CSCsk58040	cat6000	cat6000-l2-infra	WS-X6148A-GE-45AF retains previous modules MACs after OIR
CSCsk83524	cat6000	cat6000-l2-infra	L3 physical interface input drop counter is incorrect .
CSCsl84317	cat6000	cat6000-l2-infra	Active crashes on applying acl to EoMPLS subif on SIP-600
CSCsj66829	cat6000	cat6000-l2-mcast	Switch crash with clear ip igmp snoop stat and show ip igmp snoop st
CSCse59209	cat6000	cat6000-lacp	Seeing spurious mem trace back when change etherchannel mode to pagp
CSCek73332	cat6000	cat6000-mcast	Bidir shadow entry is missing some interfaces in oif
CSCsb36463	cat6000	cat6000-mcast	RF-bit not set in the DBUS hdr for the FS switched+RTD port snooped pkt
CSCsf17739	cat6000	cat6000-mcast	Sup720 SVI does not show multicast traffic rate
CSCsg11616	cat6000	cat6000-mcast	iprouting restart crashes Sup due to Block overrun at 5E64940 (red zone
CSCsi98587	cat6000	cat6000-mcast	Excessive MET refs and memleak after ipv4 stress, crash follows .
CSCsk02962	cat6000	cat6000-mcast	Supervisor Reload after SSO switchover on Multicast MET reconstruction .
CSCsj61101	cat6000	cat6000-mpls	FRR goes down after few mints when Explicit-null is enabled .
CSCsk77164	cat6000	cat6000-mpls	Connectivity problems to addresses switched based on aggregate label
CSCse31973	cat6000	cat6000-netflow	NF double counts packets when span is configured.
CSCsh23961	cat6000	cat6000-netflow	Multicast netflow not working for Vlan interface (SVI)
CSCsk03679	cat6000	cat6000-netflow	VS2: show mls nde intermittently causes ALIGN-3-SPURIOUS T/B's
CSCsl75136	cat6000	cat6000-oir	Cat6k with Sup32 failed to boot up after power cycle.
CSCsj42303	cat6000	cat6000-portsecur	6K installs ffff.ffff.ffff in CAM table under very specific conditions
CSCsd43185	cat6000	cat6000-qos	Tx queue cos maps for even ports of card WS-X6416-GBIC are incorrect.
CSCsd77622	cat6000	cat6000-qos	show policy-map interface doesn't show drop counters .
CSCsi90816	cat6000	cat6000-qos	show policy-map interface caused sup32 crash . .
CSCsj27352	cat6000	cat6000-qos	RX Priority q-limit is set to default after reload

Identifier	Product	Component	Description
CSCsl08952	cat6000	cat6000-qos	rapid link changes causes memory leak on sup32 int with service policy
CSCsl15604	cat6000	cat6000-qos	Uplink Port becomes untrusted after SSO and shut/no shut of egress port
CSCsl21934	cat6000	cat6000-qos	Port is untrusted after SSO & shut/noshut of any port sharing same asic
CSCsl30750	cat6000	cat6000-qos	Memory leak after create-apply-remove-delete policies on QM Process RP
CSCsj56102	cat6000	cat6000-rommon	Upgrade of DFC rommon fails in 12.2SX train IOS
CSCsi00706	cat6000	cat6000-routing	Sierra: upon fib tcam exception to use ratelimiter and not reload
CSCsk28585	cat6000	cat6000-routing	stats is wrong for TE tunnel, right for physical interface for ip2tag .
CSCsl00130	cat6000	cat6000-routing	GRE tunnel not HW accelerated after reboot when source from HSRP address
CSCsl61086	cat6000	cat6000-routing	urpf global disable even some intf with urpf
CSCsm17983	cat6000	cat6000-routing	Memory corruption by l3_mgr_e7_fmask_init_platform
CSCsd66276	cat6000	cat6000-rspan	IDSM: monitor session dest config removed after two sso switchovers .
CSCsc28731	cat6000	cat6000-snmp	chassisFanStatus is minorFault when one fan is present on WS-C6509-NEB-A
CSCsk55012	cat6000	cat6000-snmp	setting portDuplex from 'full' to 'full' may cause standby reset .
CSCsk58810	cat6000	cat6000-snmp	should NOT allow enable port-security on negotiating trunk interface .
CSCsb83142	cat6000	cat6000-span	SPAN / Monitor instances in IOS report ifOperStatus wrongly as down
CSCsi74194	cat6000	cat6000-span	18SXF: Egress SPAN may cause high CPU
CSCsl18765	cat6000	cat6000-span	6500-7600 : SPAN of EoMPLS port causes packet reflection or loop
CSCsl53494	cat6000	cat6000-ssc	C7600-SSC-400: Error message display incorrect product name
CSCsg21809	cat6000	cat6000-statistics	Add bridge asic status collection support .
CSCsj00385	cat6000	cat6000-statistics	logging event link-status default negates existing interface config
CSCsh84657	cat6000	cat6000-svc	STP Loopguard: Ability to disable loopguard for Po270 and higher for FWM
CSCsh97395	cat6000	cat6000-svc	IDSM: Monitor config was removed after RPR switchover
CSCsk24272	cat6000	cat6000-sw-fwding	SUP720-3B RP Crash due to I/O Buffer Leak by NDE w/ NAM 127.0.0.x Addr
CSCsh80130	cat6000	cat6000-wireless	Add warning/comments to interfaces when Auto Lag is used for interface
CSCsi76115	cat6000	cat6000-wireless	r3:WiSM hw-module reset causes traceback. Cannot decode data descriptor
CSCsj85485	cat6000	eigrp	EIGRP NSF - MSFC switchover causes hello's to be sent over passive intf
CSCsg29305	cat6000	fmm	hw-module subslot reload crashes the router .
CSCso05771	cat6000	ios-urlf	PISA:URLF:Crash upon clearing Xlist
CSCsd13448	cat6000	loadbal	IOS SLB custom udp probes don't support faildetect
CSCsi93273	cat6000	netflow-switch	Leak in Big buffer pool on SIP card with NetFlow-export version 9
CSCsk88656	cat6000	osm-gigwan	Cat6k: link-flap is observed on OSM-2+4GE-WAN+ after reload .
CSCsd18296	cat6000	osm-qos	Bdwth guarantee not met in cbwfq when cfged with llq in child in MIV .
CSCsj37071	cat6000	pas-ce3	PA-MC-E3 will not recover after workload stress

Identifier	Product	Component	Description
CSCsl46678	cat6000	pisa-sw	PISA:Sup32 PISA Console inaccessible with some terminal applications
CSCso00809	cat6000	pisa-sw	%DIAG-SP-3-TEST_FAIL: Module 2: TestSPNPInbandPing{ID=31} has failed. Er
CSCsq14650	cat6000	pisa-sw	sup32-pisa: packet corrupted when reflexive ACL used
CSCsj92874	cat6000	snmp	Catalyst 6500 May Not Send linkup/linkdown SNMP Traps and may reload
CSCek39186	cat6000	spa-ipsec-2g	MAC-address for HSRPs VIP not in FVRF vlan if tunnel redirected .
CSCek67701	cat6000	spa-ipsec-2g	SPA-IPSEC-2G: Crashdump not getting saved on NMI .
CSCsd92208	cat6000	spa-ipsec-2g	vlan map ocpu is wrong in the active vpnspa after sso+b2b failover .
CSCsh27094	cat6000	spa-ipsec-2g	SSO: VPN Spa got reset twice when subslot x/1 present
CSCsh33770	cat6000	spa-ipsec-2g	contrl vlan not set; zamboni remains in initializing state .
CSCsj34552	cat6000	spa-ipsec-2g	ip address of vlan interface not programmed into spa-ipsec-2g
CSCsj82051	cat6000	spa-ipsec-2g	Cachelines not invalidated on ICPU in error case .
CSCsk33740	cat6000	spa-ipsec-2g	replay window size of 1024 causes IPSec Policy Check and Replay Failure
CSCsl12827	cat6000	spa-ipsec-2g	Handling Transit IpSec in VRF mode
CSCsl13477	cat6000	spa-ipsec-2g	SSO not working with crypto maps terminating at same peer address .
CSCsl68327	cat6000	spa-ipsec-2g	Packet loss during rekey
CSCsl70148	cat6000	spa-ipsec-2g	PIM enabled p2p Crypto GRE Tunnels not installed in Hardware
CSCsl75719	cat6000	spa-ipsec-2g	sxf13 show int tunnel with blank display
CSCsl89069	cat6000	spa-ipsec-2g	Zamboni crashed at illegal event/state combinationin CfgMonInd, clear sa
CSCsm05486	cat6000	spa-ipsec-2g	mtu mis probram in adj thru tunnel interface after b2b failover
CSCsm35364	cat6000	spa-ipsec-2g	SPA-IPSEC-2G get reload automatically by RP
CSCsm67778	cat6000	spa-ipsec-2g	To make CSCsl68327 patch friendly and restore the symbols
CSCsm54171	cat6000	tftp	Crash seen with "copy runn tftp" and large hostname in modular IOS
CSCsi09388	cat6000	vpn-sm	VPNSM SA deleted by idle timeout
CSCsj14847	cat6000	vpn-sm	crypto connect command dropped after reload on unchannelized 2CT3+ .
CSCsj30109	cat6000	vpn-sm	Cat6k with FlexWan & IPSEC AM making as unreachable BGP neighbors
CSCsl26033	cat6000	vpn-sm	Modifying the BFG doesn't re-create the SA's
CSCsf03730	rsp4	pas-chstm1	interface remains down even after E1 level local loopback on STM1
CSCsc77148	unknown	novell	Router crash while issuing show ipx cache command. Cleanup SA warnings.

Resolved Caveats in Release 12.2(18)ZY2

Resolved Caveats for Product 'all' and Component 'cat6000-l2-infra'

- CSCsi86396—Resolved in 12.2(18)ZY2

  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 Caveats for Product 'all' and Component 'dlsw'

- CSCsk73104—Resolved in 12.2(18)ZY2

  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://www.cisco.com/en/US/products/csa/cisco-sa-20080326-dlsw.html

Resolved Caveats for Product 'all' and Component 'ios-firewall-aic'

- CSCsg70474—Resolved in 12.2(18)ZY2

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

Resolved Caveats for Product 'all' and Component 'mcast-vpn'

- CSCsi01470—Resolved in 12.2(18)ZY2

  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 Caveats for Product `all' and Component `snmp'

- CSCsf04754—Resolved in Release 12.2(18)SXF6.

  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://www.cisco.com/en/US/products/csa/cisco-sa-20080610-snmpv3.html

Resolved Caveats for Product 'all' and Component 'ssl'

- CSCed67357—Resolved in 12.2(18)ZY2

  Issue has been discovered in processing SSL handshake. Fixes are integrated as advised in
  http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-SSL.html

  Workaround is to disable SSL-based services.

- CSCsg40567—Resolved in 12.2(18)ZY2

  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.

Resolved Caveats for Product 'all' and Component 'tcp'

- CSCsh04686—Resolved in 12.2(18)ZY2

  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(18)ZY2

  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.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-mcast'

- CSCsi99869—Resolved in 12.2(18)ZY2

  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(18)ZY2

  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.

Other Caveats Resolved in Release 12.2(18)ZY2

Identifier	Product	Component	Description
CSCse69002	all	aaa	Accounting of auth failure doesn't work with some switches
CSCsi99930	all	ata-filesystem	%Error opening slavedisk0:/<filename> (Cluster chain broken on file)
CSCek39364	all	atmcommon	CLI: HA Standby router reloads while unconfiguring atm bundle .
CSCsb26631	all	atmcommon	Memory leak - ATM_PVCTRAP process
CSCsb54857	all	atmcommon	ATM shaping parameters removed from ATM vc-class for IMA upon bootup
CSCef34800	all	bgp	BGP changes to accept max value for MED attribute

Identifier	Product	Component	Description
CSCeg58039	all	bgp	BGP: changing the max-paths value may cause a crash .
CSCsb63652	all	bgp	bgp aggregate-address results in high BGP Router process utilization .
CSCsb96034	all	bgp	Traffic down for too long after SSO switchover .
CSCsd41237	all	bgp	vrf import map is not working .
CSCsd52225	all	bgp	BGP soft-reconfiguration keeps the old next-hop
CSCse91962	all	bgp	prefix stays in BGP table with RD 0:0 even after vrf's RD is configured
CSCsf32449	all	bgp	Sup720 MVPN PE - Tunnel does not come back up after reload .
CSCsh80008	all	bgp	BGP: soft reconfiguration inbound and neighbor weight has no effect
CSCsd77207	all	c7600-mcast	Bidir traffic changed from HW to SW switch after add 200 sub-inf quickly
CSCsi90011	all	cat6000-dot1x	User Auth after Machine Auth causes dot1x security violation
CSCsh77220	all	cat6000-ha	SSO failover causes certain configs being removed .
CSCsj30444	all	cat6000-hw-fwding	SUP-2 Router crashes after boot UP
CSCsj16292	all	cat6000-l2	DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCei52830	all	config-sync	Banner command sync is broken by CSCin86483 .
CSCsh62565	all	crypto	SSH keys regenerated every hour cause route flaps due to high CPU load
CSCsg05873	all	dspu	Buffer leak with SNA Focalpoint PU consuming middle buffers with NMVTs
CSCsg14026	all	fib	Routers/Switches forward traffic destined to Class E Addresses
CSCsj23579	all	fib	Invalid memory action (malloc) @ SSO Switchover .
CSCsh31939	all	ftp	c2w1:ciscoFtpClientMIB:Get & Set opration cause process deadlock & crash
CSCsi45840	all	hsrp	ARP requests for HSRP virtual IP may fail after switchport cmd is used .
CSCse98795	all	ios-authproxy	bus error while printing access-list
CSCsh61119	all	ip	c10k High CPU in collection process .
CSCsi62559	all	ip	SPD classifies OSPF IP Precedence 0 as priority .
CSCeg43753	all	ip-rip	Router crashes at bgp_vpnv4_revise_route_update - corrupt PC & Sig10 .
CSCsh37957	all	ipsec	IPsec MIB entries not populated, IKE entries seem OK
CSCsh94882	all	ipsec-ezvpn	Unity client not initiating mode config should be rejected
CSCsi00173	all	ipsec-isakmp	Bus error at crypto_ipsec_unlock_peer .
CSCsi16904	all	ipsec-isakmp	VPN-SPA does not send ISAKMP packet with notification payload included
CSCsi91875	all	laminar	Cat6k crashes when unconfiguring vserver during snmp poll
CSCsj04905	all	loadbal	IOS-SLB: FWLB sticky config not get removed
CSCsi22502	all	makefile	installer imf.tar file not being zipped creates uninstallable image
CSCsh39318	all	mcast-vpn	10K / PRE-2 crashes at %MROUTE-4-ROUTELIMIT
CSCsd13491	all	mem	show memory statistics history displays wrong values in processor pool
CSCse22161	all	nbar	RP pool Memory corruption SXF4 - checkheaps_process/validblock crash
CSCeh65692	all	os	Align Spurious memory access errors .

Identifier	Product	Component	Description
CSCsd72747	all	ospf	nssa summary to null0 disappears after 'clear ip ro *'
CSCsg52336	all	ospf	Crash at ospf_flush_area_summary_lsa after 'no ip vrf' of unassigned vrf
CSCsi45422	all	ospf	iprouting.iosproc process reloads when making changes to static routes
CSCsk68269	all	pisa-sw	A router may reload when configuring 'storm-control' functions
CSCei07548	all	pki	ocsp response timestamps are mishandled
CSCei85164	all	pki	OCSP fails when timezone is configured
CSCsi05251	all	qos	bus error crash at get_rateinterval_from_service_policy at subint delete
CSCek66164	all	rcp	show command pipeline redirect into rcp crashes the router
CSCsd43344	all	redundancy-rf	isis-nsf info doesnt sync with standby in SSO mode .
CSCsi78162	all	snaswitch	SNASw %DATACORRUPTION-1-DATAINCONSISTENCY messages
CSCef66939	all	snmp	VRF aware SNMP may generate trap with incorrect address
CSCeh74715	all	snmp	SNMPv1 should not send traps with counter64
CSCse98807	all	snmp	Traceback, Process=SNMP Timers, %SCHED-3-STUCKMTMR during regression .
CSCsg39295	all	snmp	Syslog Displays Password if SCP or FTP Selected in CISCO-COPY-CONFIG-MIB
CSCsj40706	all	snmp-if	incorrect ifIndex from multi HC OID Get to various cards
CSCsi77774	all	tcp	On modular IOS,Telnet on VRF int is allowed irrespective of vrf-also key
CSCsd87810	all	tftp	IOS tftp server should not differentiate between / and backslash in path
CSCsi29875	all	udp	3/27: SP: oir_rf_reload_self: icc_req_imm failed, node not booting
CSCsi33554	all	virtual-template	Connected net for virtual-template is not created in vrf routing table
CSCsg30875	all	wccp	wccp blocking telnet to router
CSCsh98343	all	wccp	WCCP redirect-list and mask-acl merge results in wrong redirect info
CSCsi05906	all	wccp	WCCP:appliance failover does not update TCAM adjacency
CSCdv70135	c10000	atmcommon	ATM QoS classes can not be configured.
CSCsd46517	c1700	snmp	Huge Memory allocation on c1721 during snmpwalk .
CSCsi12289	c6k-fwm	other	FWSM Does Not Display Correct Timezone for DST
CSCse54191	c6venus-slb	laminar	CSM fails over when incorrect HSRP group fails
CSCsb23106	c7200	pas-t3	7206vxr with NPE-G1 bus error crash when OIR PA-2T3+
CSCsj47546	c7600	c7600-sip-400	POS: RDI-P must not be sent when the interface detects PLM-P
CSCsc83961	c7600	c7600-sip-600	Both APS protect & working ports forwarding traffic
CSCsi52209	c7600	c7600-sip-600-ucod	7600-sip-600 crash at PXF-DFC1-2-FAULT: T0 OHB Exception: SLIP FIFO full
CSCek75394	c7600	cat6000-fib	High CPU after enabling MPLS on interface .
CSCsh98909	c7600	cat6000-fib	VRRP traffic not hardware switched on Sup2/MSFC2
CSCsg92670	c7600	cat6000-mpls	7600 : MLS FIB frozen, Sanity Check of MLS FIB s/w structures failed
CSCsi42517	c7600	loadbal	SRB Crashes when upgrading from SXF to SRB with SLB stateful config
CSCek37222	c7600	osm-qos	FR-flat:classification is broken in class-default with random-detect .

Identifier	Product	Component	Description
CSCsg55237	c7600	osm-vpls	L2 flooding stops when new MAC address entries are learnt
CSCse98369	c7600	spa-atm-all	class-default bandwidth percent 100% - SPA ATM fails
CSCsi64204	c7600	spa-atm-all	SXF:SIP400:ATMSPA Noticeable delay in output of show int atm command
CSCsi98993	c7600	spa-atm-all	Block FPD for Intel SPROM based ATM SPAs
CSCek57760	c7600	spa-ipsec-2g	IP MTU of GRE tunnel not used by SPA-IPSEC
CSCsb57042	cat6000	c7600-field-diag	%SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs
CSCsj01891	cat6000	c7600-field-diag	%SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs
CSCsc11689	cat6000	cat6000-acl	Configure/Unconfigure PACL may cause memory leak.
CSCsh54951	cat6000	cat6000-acl	PBR: TCAM incorectly programmed when match statement is NOT used
CSCsi60125	cat6000	cat6000-acl	Hosts receive TCP RST due to incorrect NAT translation on cat6k .
CSCsh20211	cat6000	cat6000-diag	'Complete' diags fail TestNetflowInlineRewrite test on Service Modules
CSCsj23211	cat6000	cat6000-diag	'Complete' diags fail TestNetflowInlineRewrite test on Service Modules
CSCsj60722	cat6000	cat6000-diag	TestNetflowInlineRewrite: diag failure on bootup
CSCek68265	cat6000	cat6000-env	Major alarm on active caused syst. shutdn instead of swover to stdby
CSCsd79536	cat6000	cat6000-env	Standby RP crashes once at reload after installing set of patches .
CSCsf23115	cat6000	cat6000-env	SUP720 does not recognize FAN2 after one of fans failed. .
CSCsj29789	cat6000	cat6000-env	boot with failed fan-2, system shutdown due to insufficient cooling .
CSCsd82778	cat6000	cat6000-filesys	bootflash: bf_io_devctl: DEVCTL error 19 Error May Log During Bootup
CSCek77954	cat6000	cat6000-firmware	test platform firm get cu-sfp-phy print-reg <port> <reg-no> .
CSCsh38728	cat6000	cat6000-firmware	Show int displays half even if port is hard coded to full
CSCsc33080	cat6000	cat6000-ha	%PFINIT-SP-1-CONFIG_SYNC_FAIL_RETRY: Sync'ing the private configuration
CSCsd33992	cat6000	cat6000-ha	%PM-SP-STDBY-3-INTERNALERROR: when boot up
CSCsg07870	cat6000	cat6000-ha	crash seen on switchover at pf_redun_sync_port_asic_on_swover .
CSCsg30355	cat6000	cat6000-ha	OIR of redundant sup w/ CatOS crash the Cat6500 System running IOS
CSCej32124	cat6000	cat6000-hw-fwding	no mls verify commands doesnt take effect on standby supervisor
CSCsg06577	cat6000	cat6000-hw-fwding	'Desc ordr internal vlan allocation' brings up sup with major diag error
CSCsj27811	cat6000	cat6000-ipc	EOBC buffer leak caused by CMM module .
CSCsb14543	cat6000	cat6000-l2-infra	t/b pm_port_counters_lock on module reset of active supervisor
CSCsh33128	cat6000	cat6000-mcast	MMLS/MVPN: Partial SC internal vlan not included in (*,G)
CSCsi77720	cat6000	cat6000-mcast	PISA: TB with IPv6 multicast BSR selection
CSCsj28277	cat6000	cat6000-mcast	Sup720 ignores IGMPv3 report if first group in Exclude list is 224.0.0.x
CSCsh99351	cat6000	cat6000-mpls	Packet reflection on EoMPLS links
CSCsi97192	cat6000	cat6000-mpls	Vrf Agg label is not programmed in vpn-cam, SP thinks it as Ipv6 Agg lab
CSCsi69350	cat6000	cat6000-rommon	Newly active crashed on upgrading rp rommon @ emt_call .
CSCsi40628	cat6000	cat6000-span	Dual RSPAN session causes loop between 2 6500 chassis .
CSCsi76192	cat6000	cat6000-wireless	r3:show wism status not populated until standby up after SSO

Identifier	Product	Component	Description
CSCsi15191	cat6000	install	BOM messages observed while activation of rollback on stndby supervisor
CSCsb13358	cat6000	loadbal	failaction gtp purge doesnt delete some gtp stickies when probe fail
CSCsf18752	cat6000	loadbal	mls ip slb search wildcard rp breaks gtp slb if 2 sfarms are confgd
CSCsi42270	cat6000	loadbal	IOS-SLB Radius Server LB may not mark a real as failed
CSCsi02885	cat6000	osm-choc-ds0	OSM-1CHOC12/T1-SI incrementing abort, interface administrativel
CSCsa75285	cat6000	pas-chstm1	WS-X6582-2PA crashing cisco7600 when booting up with PA-MC-STM-1SMI
CSCsj16762	cat6000	pisa-sw	Ping failure on enabling dNBAR PD on sip200 pos sub-interface
CSCsj29344	cat6000	pisa-sw	PD stops after creating first custom protocol or loading PDLM
CSCsl38372	cat6000	pisa-sw	PISA:Trf drops for apprx 50 Sec on SSO when PISA feat appld in Ingr dir
CSCsj92874	cat6000	snmp	Catalyst 6500 May Not Send linkup/linkdown SNMP Traps and may reload
CSCsg16272	cat6000	snmp-if	Catalyst6500 LinkDown snmp trap does not generate while performing OIR .
CSCsh68976	cat6000	spa-infra	memory leak at xcvr_idprom when executing show hw-module all tranceiver
CSCek54572	cat6000	spa-ipsec-2g	crash at ace_create_cm_head_node .
CSCsg38231	cat6000	spa-ipsec-2g	'crypto eng gre vpnblade' cmd does make the tunnels to be accelerated by
CSCsh34872	cat6000	spa-ipsec-2g	With mls mpls recirc configd primary internal vlan has vpn-num .
CSCsh36377	cat6000	spa-ipsec-2g	crypto connect cmd not updated in standby RP for ATM subif .
CSCsi41791	cat6000	spa-ipsec-2g	Leak: SPA-IPSEC-2G crash-> No More Free Buffers ; SPA_IPSEC-3-PWRCYCLE .
CSCsh61061	cat6000	vpn-sm	VPM-SM:ISAKMP Lifetimes do not replicate correctly in interchassis setup

Resolved Caveats in Release 12.2(18)ZY1

Resolved Caveats for Product 'all' and Component 'mcast-vpn'

- CSCsi01470—Resolved in 12.2(18)ZY1

  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 Caveats for Product 'all' and Component 'pim'

- CSCsd95616—Resolved in Release 12.2(18)ZY1

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

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

Resolved Caveats for Product 'all' and Component 'socket'

- CSCse56501—Resolved in 12.2(18)ZY1

  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

Identifier	Product	Component	Description
CSCsh31306	all	7x00-t1e1	T1 serial o/p drops / no QOS drops - flexwan - T1 multichannel PA.
CSCsh82746	all	7x00-t1e1	Input Errors Counter not incrementing properly with Runt Errors
CSCsh74025	all	atmcommon	clns packets not being punted by an enhanced flexwan
CSCek48274	all	bgp	clear ip bgp soft in may not delete all the BGP prefix
CSCse24873	all	bgp	Default-information originate in BGP shouldnt be tied to peer group
CSCsg11830	all	bgp	12.2(18)SX Default-information originate does not generate default route
CSCsg43140	all	bgp	Switch may crash due to bgp over vpn
CSCsg46638	all	bgp	BGP does not send withdraw when distribute-list is configured
CSCsi58259	all	c7600-atom	EARL7 PFC EoMPLS: CE to CE connectivity is broken with ATM as core
CSCek55639	all	c7600-snmp	Failed to assert Physical Port Administrative State Down alarm
CSCsb19159	all	cat6000-filesys	Command copy const_nvram:vlan.dat startup-config might crash switch
CSCsg52887	all	clns	SegV at ctunnel_oqueue when 'no ctunnel destination' on one side
CSCsd25653	all	comm-serv	vrf-also in named ACL for VTY line not saved in running configuration
CSCsb27868	all	dhcp	DHCP Relay should unicast offer/ack on unnum ethernet sub- int
CSCsi34572	all	dot1x-ios	PC does not get a new DHCP address for machine authentication dot1x
CSCsa49922	all	eigrp	EIGRP internal route remains in RT but not in topology table
CSCsd98852	all	eventmgr	EEM does not allow read from stdin

Identifier	Product	Component	Description
CSCsa72748	all	fr	router crash due to watchdog timeout on frame relay broadcast
CSCsg49987	all	hsrp	HSRP learned groups appear in SNMP MIB
CSCsf04921	all	ifs	18SXF6: getnext loop condition detected on ciscoFlashFileTable
CSCsg40016	all	ifs	show tech causes various system problems
CSCsi42143	all	ifs	Image installation fails with error msg 'Failed to create output file'
CSCse65726	all	iml	command no tacacs-server admin resets router
CSCsh74322	all	install	rp fails bootup when reload installed image with 42 patch in 1 tar ball
CSCsh35311	all	ios-authproxy	Proxyacl downloaded from the ACS cause spurious memory access
CSCek39048	all	ip	Modular IOS: default distribute-list route-map crash router
CSCsg26492	all	ip-acl	Error: can not find acl. Abort - msg when removing permit entry in ACL
CSCse44079	all	ipmulticast	Multicast UDL - High CPU in IGMP Input when UDL interface down
CSCec76468	all	ip-pbr	crash in show route-map when delete route-map during concurrent conf
CSCsd50828	all	ip-pbr	AS-path based redistribution fails
CSCsh57795	all	ip-rip	Removing 1 RIP neighbor removes all neighbors
CSCsh41192	all	ipsec-core	Memory leak in IPSEC key engine process
CSCsh85355	all	ipsec-core	Address Error exception at crypto_ipsec_clear_peer_sas
CSCsf10605	all	ipsec-isakmp	crypto session count incorrect after ungraceful disconnect
CSCsg99872	all	ipsec-isakmp	VPNSM: IPSEC accounting (start/stop) not sent under some conditions
CSCsd32192	all	mcast-switching	GRE Tunnel With Checksum Enabled Does Not Transmit Multicast Packets
CSCse06752	all	mobileip	LAM /32 cef entry shows unresolved
CSCsg86806	all	mpls-lfib	Client over MPLS Traffic Engineering Tunnel unable to ping 7600 interfac
CSCsh83034	all	mpls-lfib	High CPU on Supervisor caused by FIB Control Task process
CSCsc68540	all	mpls-mib	mplsTeNotifyPrefix trap emitted instead of correct TE trap name
CSCsg44555	all	mpls-te	7600 MPLS TE mid-point stuck at up/down and Juniper headend up/up
CSCsh82993	all	mpls-vpn	Aggregate label missing if static route exists for same network
CSCsh29830	all	nat	NAT: Clear IP NAT translation * creates hardware entry for RSHELL.
CSCsc93633	all	nbar	Software bus error crash on 7206VXR w/12.3(14)T3 w/ NBAR configured
CSCse22161	all	nbar	RP pool Memory corruption SXF4 - checkheaps_process/validblock crash
CSCsd59610	all	os	%SYS-4-REGEXP: new engine: regexp compilation had failed.
CSCsg42072	all	os	Virtual Exec sessions not freeing memory
CSCsi62514	all	os	SXF9: ION image not bootable ROCKIES3_INTEG_070423
CSCse84602	all	osm-ct3	Error messages from Standby Sup when configuring OSM card channelization
CSCse60482	all	osm-qos	OSM QoS per VLAN shaping not configurable for EoMPLS with TE Tunn
CSCsc52057	all	ospf	OSPF passive-interface default bleeds to OSPF VRF subinterfaces
CSCse64565	all	ospf	OSPF passive-interface default pb when converting switchport to L3
CSCsg33571	all	ospf	Add prefix option under router xxx vrf process distribute-list options

Identifier	Product	Component	Description
CSCsg65298	all	ospf	OSPF: connected network learnt via ospf after interface shutdown #2
CSCsc04397	all	parser	Spurious memory access made at Fcheck_interface_state
CSCsg92954	all	pas-chstm1	Poor Voice Quality over congested Links
CSCeg38418	all	pki	Router crash when OCSP server use key hash as id
CSCek34117	all	qos	SIP1+ATM(OC3 SPA): Crashed at hqf_walk_and_police_inline()
CSCsd56696	all	qos	A2A: FR Adaptive shaping is not accurate
CSCsg51724	all	qos-mib	cbQosCMDropPkt stays at 0 while CLI counters shows positive values
CSCse51263	all	rcp	RP side console Exec process hangs deadly sometimes
CSCsf08419	all	remote-registry	EIGRP memory leak in registry_ion.c when neighbor flaps.
CSCek58966	all	rsps-time-rptr	Remove IPSLA Feature CLI From Modular IOS
CSCek65370	all	rsps-time-rptr	Disable IP SLA CLI/SNMP from ION image in SXF
CSCse56676	all	snmp	Some SNMP notifications go to the wrong host
CSCsh79371	all	snmp	SNMP memory leak IOM 12.2(18)SXF6
CSCsi08777	all	spa-ipsec-2g	Memory Leak seen in Chunk Manager process
CSCsi42769	all	spa-ipsec-2g	VPNSPA intermittently stop passing traffic.
CSCsf32211	all	spa-pos-oc3-12	Input bytes counter continues incrementing when a line protocol is down
CSCsd76601	all	ssh	Resuming SSH Session Fails After Other Session Has Been Disconnected
CSCse79611	all	ssh	SSH source-interface command not working
CSCsf25722	all	ssh	software forced reload after executing secure copy (scp)
CSCse53090	all	tcl-bleeding	After console timeout, access can be done to standby console.
CSCef13860	all	tcp	Invalid TCB pointer traceback on exiting from a CPU session
CSCse05736	all	tcp	A router running RCP can be reloaded with a specific packet
CSCsg00846	all	tcp	Crash of RP blob due to a missed inetd_service_mutex unlock
CSCsg19598	all	tcp	SSH session hangs intermittently
CSCsg56926	all	tcp	no logging console not working in ION for tcp debugs
CSCsi51178	all	tcp	Switch crashes due to ssh session at pak_client_set_pid
CSCsd42600	all	telnet	%SYS-3-BAD_RESET alongwith SegV exception crash
CSCsg99600	all	udp	Modular IOS : ip helper address 1.1.1.255 not work
CSCsh21505	all	udp	ip helper address on vrf interface in ION, dhcp routed with global table
CSCsi23203	all	vipmlp	Remove service policy from T1 prior to adding it to the multilink bundle
CSCea82222	as5400	os	timeout login response is broken on TTY and VTY lines with no AAA
CSCei09247	c12000	spa-ser-te1	Local serial link goes up/down when remote link is admin down
CSCsd84497	c2800	ios-authproxy	auth-proxy requests stuck in init state
CSCeg51185	c6venus-slb	laminar	New varbinds reqd in slbRealStateChange & slbVirtualStateChange trap
CSCek31610	c6venus-slb	laminar	IOS changes to support sticky replication in CSM
CSCsb84087	c6venus-slb	laminar	CSM: config-sync cmd not able to remove vlan from standby csm port-chann
CSCsd24461	c6venus-slb	laminar	Configuring CSM with SSL stickyness shows as src-ip stickyness.

Identifier	Product	Component	Description
CSCsh74881	c6venus-slb	laminar	CSM with a pair of bridged vlans can cause a variable to not function
CSCei12353	c7200	netflow-switch	Flow End sysUpTime higher value than the Router sysUpTime
CSCsa91863	c7200	pas-e3	PA-E3 may reports LOF on reload
CSCsc69076	c7600	c7600-qos	SIP1-ChOC3: Spurious access at swsb_delete on unconfig of T1 chnl group
CSCsh32199	c7600	c7600-sip-400	Input queue drop counter incrementing even when interface disconnected
CSCsi10231	c7600	c7600-sip-600-vpls	VPLS: VC types 4 and 5 can not co-exist within same VFI on 7600-SIP-600
CSCsi22379	c7600	c7600-sip-600-vpls	SIP600 vpls drops packets from VC Type 4 neigh when control word present
CSCek25660	c7600	cat6000-hw-fwding	tarceback found at l2_modify_one_entry(0x207b9614)+0x48
CSCse61387	c7600	cat6000-qos	After LC is removed, show policy-map control-plane still show LC counter
CSCse89548	c7600	cat6000-routing	SYS-DFC4-3-CPUHOG::FIB Control Queue Task
CSCsh23192	c7600	loadbal	DNS probe does not recover after failure when configured with VRF
CSCse84695	c7600	osm-ct3	Standby supervisor may crash when configuring osm card past FREEDM limit
CSCsc25557	c7600	osm-pos	PORT3: Router crashed in CWAN OIR Handler in attempt to lock a semaphore
CSCsi77083	c7600	osm-ucode	Fix for CSCsh21998 in v122_18_sxf_throttle is erroneous
CSCsi48550	c7600	vipmlp	dMLP: account lost_frags& rx discards as bundle intf input error
CSCsg22769	cat6000	ata-filesystem	CPU utilization goes beyond 99% due to dfs_disk1.proc.
CSCdy11156	cat6000	atmcommon	13E:12E:RP crashed while applying config on ATM-PA,mgd_timer_stop
CSCsd08468	cat6000	c7600-mpls	SP crash at %EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR due to invalid packets
CSCsg62119	cat6000	c7600-mpls	Cat6K Spurious Memory access
CSCsg91545	cat6000	cat6000-acl	ACL TCAM inconsistency seen if ipv6 acl with 2k mask is used
CSCsf29400	cat6000	cat6000-cmm-voice	Native IOS Sup discards or filters ARP replies from CMM for ACT module
CSCsg07525	cat6000	cat6000-diag	Periodic (30sec) traffic loss/dup over dis port-cha due to wrong RBH
CSCsh37008	cat6000	cat6000-env	Need to enable Malabar8 in WS-C6509-NEB-A chassis with one fan
CSCsb61381	cat6000	cat6000-filesys	Multiple Crashes due to bus error after issuing dir all-filesystems
CSCsh49043	cat6000	cat6000-firmware	Output drops in Queue3 after changes in cos-map config on 6148A-GETX
CSCsh66367	cat6000	cat6000-firmware	Wrong Ubin Images committed to v122_18_sxf_throttle on CSCsh61396
CSCsh89589	cat6000	cat6000-firmware	ARP fails on FWSM with SFM or SFM2 and S2/MSFC2
CSCsc77287	cat6000	cat6000-ha	SIERRA: Telnet/console: freeze by remote command module slot
CSCsg08304	cat6000	cat6000-ha	JQL: UDLD failure detected on neighbor switch after RPR switchover
CSCsh45258	cat6000	cat6000-ha	delay execution of redundancy force switchover in case stdby nrd
CSCek68281	cat6000	cat6000-hw-fwding	Syslog instead of crashing on correctable FIB SSRAM ECC errors

Identifier	Product	Component	Description
CSCsd95877	cat6000	cat6000-hw-fwding	%MLS_ACL_COMMON-SP-4-MLS_ACL_CONSIST appears on active SP on sso.
CSCse90572	cat6000	cat6000-hw-fwding	FIB TCAM exception related enhancements
CSCsg97079	cat6000	cat6000-infra-mdlr	18SXF7 ION image should also bundle FlexWan1
CSCsf20751	cat6000	cat6000-l2	FlowControl inconsistency between Po and gig interfaces after SW upgrade
CSCsh38443	cat6000	cat6000-l2	Removing associated vlan would trigger the mac-add to get purge every 5m
CSCsh48947	cat6000	cat6000-l2	PWR_DENY Port 47/48 on each LC max PWR support Backplane per LC or VDB
CSCsd74091	cat6000	cat6000-mcast	Misc. fixes for GCE handling for standby as DFC
CSCse37364	cat6000	cat6000-mcast	traceback @ hal_get_dist_job on toggling mmls
CSCsg64306	cat6000	cat6000-mcast	%MCAST-SP-6-L2_HASH_BUCKET_COLLISION
CSCsg76239	cat6000	cat6000-mcast	Fast Path mcast pkts hit RP cpu if ACL configured on OIF
CSCsi57912	cat6000	cat6000-mpls	6PE: router mac not programmed for the IPV6 MPLS reserved vlan after SSO
CSCse10113	cat6000	cat6000-netflow	Missing hwidb for fibhwidb netflow_vlan1038 (ifindex 216) :
CSCsh42914	cat6000	cat6000-netflow	Cat6500 Netflow does not export all flows with sampled netflow
CSCsf11787	cat6000	cat6000-oir	EARL bus idle error occurs when the switching bus stall occurs
CSCsa97042	cat6000	cat6000-portsecur	Secured port dropping traffic after applying & removing mac-filter
CSCsg02391	cat6000	cat6000-portsecur	PORT_SECURITY-SP-2-INELIGIBLE error after module reset
CSCsg34141	cat6000	cat6000-portsecur	Secure mac learnt on non secure port creates a static entry
CSCsg69489	cat6000	cat6000-routing	Reroute of LSP between two link with label constitutes to traffic loss
CSCsg80948	cat6000	cat6000-routing	Uneven load-sharing for 4-path ECMP case
CSCsh85155	cat6000	cat6000-routing	mls adjacency has extra punt entry after FRR cutover
CSCsh93083	cat6000	cat6000-routing	Hadware uRFP with ACL stops after reboot
CSCsg77142	cat6000	cat6000-snmp	Memory leak in Cat6k SNMP Trap process
CSCsg49395	cat6000	cat6k-vs-infra	%BIT-SP-4-OUTOFRANGE: bit is not in the expected range
CSCsb44267	cat6000	cwpa	bus error crash when forwarding IPX over GRE
CSCsg09757	cat6000	ios-infra	MP(Maintenance Pack) information missing in the MIB
CSCeh54725	cat6000	laminar	MIB object go into loop during snmp query
CSCsg01366	cat6000	laminar	CSM config sync cause stacks to run low and crash router
CSCsh96773	cat6000	laminar	CSM FT : unable to track port-channel interfaces
CSCsi73534	cat6000	laminar	CSM: CSCsb84087 breaks config-Sync feature
CSCsb01373	cat6000	msfc-filesys	MSFC3: Free NVRAM space reduces every time config is written to memory
CSCsc08947	cat6000	msfc-routing	6k IOS Autostate: L3 int up/up if last L2 port disabled while L3 is shut
CSCsg87037	cat6000	osm-atm	ATM OSM has compatibility issue with 3rd vendor device
CSCse88708	cat6000	osm-ct3	Early stop of Bert test on OSM-1CHOC12/T1-SI produces error

Identifier	Product	Component	Description
CSCsg45480	cat6000	osm-ucode	Prevent Invalid IP Packets from OSM causing L2/L3 errors and SP crash
CSCsh21998	cat6000	osm-ucode	MPLS: Sup2 OSM sending TTL=0 packets with aggregate summary-only
CSCsh41006	cat6000	osm-ucode	change earl reset patch-limit crash disable test cmd to a config cmd
CSCse66269	cat6000	packetmgr	ION free memory dropping during mcast failovers but no process leaking
CSCsi31102	cat6000	pisa-sw	NBAR - directconnect protocol not classified correctly
CSCsi88239	cat6000	pisa-sw	PISA:NBAR PD top-n cntrs not incrementing after stop/start of trf
CSCsf25728	cat6000	sr-bridging	Unable to session to FWSM when source-bridge ring-group is configured
CSCsd19181	cat6000	vpn-sm	Crypto connect command is dropped from serial interface after reload
CSCsg38618	wism	wlc-infra	Session to a 24 bit address fails on WiSM

Resolved Caveats for Product '3750' and Component '802.1x'

- CSCsb45696—Resolved in 12.2(18)ZY1

  Symptoms: A platform may reload in response to malformed 802.1x EAP traffic.

  Conditions: This symptom is observed on a Cisco Catalyst 3750 that runs Cisco IOS Release 12.2(25)SEC. However, the symptom is both platform- and release-independent.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'aaa'

- CSCsd49317—Resolved in 12.2(18)ZY1

  Symptoms: When you enter the **no tacacs-server administration** command, the router may crash because of processor memory corruption.

  Conditions: This symptom is observed when you enter the **no tacacs-server administration** command while the **tacacs-server administration** command was not previously configured.

  Workaround: Do not enter the **no tacacs-server administration** command while the **tacacs-server administration** command was not previously configured.

- CSCsg43322—Resolved in 12.2(18)ZY1

  Symptoms: When you attempt to configure an authentication, authorization, and accounting (AAA) list for a network, the following error message may be generated:

  AAA: No free accounting lists for "network".

  Condition: This symptom is observed on a Cisco router that has not yet reached its maximum of 1024 authentication lists, 1024 authorization lists, and 1024 accounting lists.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'ata-filesystem'

- CSCek42751—Resolved in 12.2(18)ZY1

  Symptoms: The running configuration may not be accessible after you have copied a small file to the running configuration.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system after you have rebooted the router.

  Workaround: Reboot the router once more.

Resolved Caveats for Product 'all' and Component 'bgp'

- CSCef84062—Resolved in 12.2(18)ZY1

  Symptoms: A Cisco router that runs BGP may crash because of a bus error at a low address when you enter the **show bgp ipv6** *network* command.

  Conditions: This symptom is observed on a Cisco 7505 router that runs Cisco IOS 12.2(15)T8 after BGP configuration changes. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsd32373—Resolved in 12.2(18)ZY1

  Symptoms: Multipath load-balancing may not function for internal BGP (iBGP) paths, and routes are not learned through multipath routing, even after you have cleared BGP.

  Conditions: This symptom is observed after an RP switchover has occurred.

  Workaround: There is no workaround.

- CSCse04220—Resolved in 12.2(18)ZY1

  Symptoms: The BGP table version remains stuck at 1, and the router may crash.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6. The symptom may also occur when you enter the **clear bgp nsap uni *** command for a network service access point (NSAP) address family.

  Workaround: Enter the **clear ip bgp *** command to clear the sessions, purge the BGP table, and prevent the router from crashing.

- CSCsf20947—Resolved in 12.2(18)ZY1

  Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

  Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

  Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsg55209—Resolved in 12.2(18)ZY1

  Symptoms: When BGP updates are received, stale paths are not removed from the BGP table, causing the number of paths for a prefix to increase. When the number of BGP paths reaches the upper limit of 255 paths, the router resets.

  Conditions: This symptom is observed on a Cisco router when the **neighbor soft-reconfiguration inbound** command is enabled for each BGP peer.

  Workaround: Remove the **neighbor soft-reconfiguration inbound** command. A router that runs a Cisco IOS software image that has a route refresh capability, storing BGP updates is usually not necessary.

- CSCsi06948—Resolved in 12.2(18)ZY1

  Symptoms: A switch or router may crash because of a bus error after a BGP dampening-related command is entered.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that has a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF7 but may also affect other platforms and releases.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'cat6000-dot1x'

- CSCsg40391—Resolved in 12.2(18)ZY1

  Symptoms: When a dot1x port is authenticated and assigned a VLAN by an AAA server and then the line card for the port is reset, the assigned VLAN becomes the configured access VLAN for the port. You can see this situation in the running configuration for the port.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the access VLAN for the port to the old value.

  Further Problem Description: If, at a later time, you unconfigure dot1x on the port but do not unconfigure the access VLAN, the configuration for the assigned VLAN remains in place, causing the port to have access to whatever VLAN was previously assigned.

Resolved Caveats for Product 'all' and Component 'cat6000-env'

- CSCse97422—Resolved in 12.2(18)ZY1

  Symptoms: When you enter the **show tech** command with long a regular expression, the platform may crash during the display of the command output. For example, this situation may occur when you enter the following command:

  show tech | e (0.00% 0.00% 0.00%|cmd_sts|0 0|last clearing|packets input|packets output|SESs|LMI enq|cast queue|Last input|OAM cells input|reliability 255)

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 720.

  Workaround: Do not use a long regular expression when you enter the **show tech** command.

- CSCsg37435—Resolved in 12.2(18)ZY1

  Symptoms: The output of the **show snmp mib ifmib ifindex** command does not show the SNMP Interface Index identification numbers (ifIndex values) for 802.1Q VLAN subinterfaces.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router after you have performed an OIR of a Gigabit Ethernet module.

  Workaround: Reload the platform.

Resolved Caveats for Product 'all' and Component 'cat6000-hw-fwding'

- CSCsh94940—Resolved in 12.2(18)ZY1

  Symptoms: An active supervisor engine may crash because of memory corruption in the SP processor pool, and the following error message may be generated:

  %SYS-SP-3-BADFREEMAGIC: Corrupt free block at [...] (magic [...])

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 32 when a periodic SNMP query is made to the L2 MAC table. Because of a race condition, freed memory may be written by another thread, causing memory corruption.

  Note that the symptom does not occur with a Supervisor Engine 1 and Supervisor Engine 2.

  Workaround: Disable the SNMP query to the L2 MAC table.

Resolved Caveats for Product 'all' and Component 'dlsw'

- CSCsf28840—Resolved in 12.2(18)ZY1

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070110-dlsw.html

Resolved Caveats for Product 'all' and Component 'fib'

- CSCea53765—Resolved in 12.2(18)ZY1

  Symptoms: Adding a /31 netmask route on a Cisco router may not overwrite an existing /32 CEF entry.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.1(13)E4, Release 12.2, other 12.1 E releases, or Release 12.3.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables prefixes that are derived from adjacencies in the FIB to be periodically validated against covering prefixes that originate from the RIB. Validation ensures that an adjacency prefix is only active when it points out of the same interface as a covering attached prefix. To enable this validation, enter the **ip cef table adjacency-prefix validate** global configuration command.

  Note that because validation is periodic, there could be a time lag between RIB changes and subsequent validation or withdrawal of covered adjacencies in the FIB.

- CSCeg03019—Resolved in 12.2(18)ZY1

  Symptoms: CEF may not work over different tunnels.

  Conditions: This symptom has been observed when both GRE and IPIP tunnels are configured and the packet traverses both.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'ftp'

- CSCsg16908—Resolved in 12.2(18)ZY1

  Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

  The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

  This vulnerability does not apply to the IOS FTP Client feature.

  This advisory is posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070509-iosftp.

Resolved Caveats for Product 'all' and Component 'high-ipqos'

- CSCeh82893—Resolved in 12.2(18)ZY1

  Symptoms: The police drop rate counter in the output of the **show policy-map interface** command does not increment.

  Conditions: This symptom is observed only for the interface of a SPA that is installed in a SIP-400.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'ifs'

- CSCek55001—Resolved in 12.2(18)ZY1

  Symptoms: A router may crash when you enter the **dir /recursive** command.

  Conditions: This symptom is observed on a router that has a Cisco IOS File System (IFS) and occurs only when 40 subdirectories are created. The symptom does not occur when you enter the **dir** command without the **/recursive** keyword.

  Workaround: When more than 40 subdirectories are created, do not use the **dir /recursive** command. Rather, use the **show disk** command.

- CSCek64188—Resolved in 12.2(18)ZY1

  Symptoms: An error message indicating memory leak and pending transmission for IPC messages is displayed as follows:

  *Dec 3 01:31:31.792: %IPC-5-WATERMARK: 25642 messages pending in xmt for the port Primary RFS Server Port(10000.C) from source seat 2150000
  *Dec 3 01:32:01.489: %SYS-2-MALLOCFAIL: Memory allocation of 4268 bytes failed from 0x9F32944, alignment 32

  Conditions: This issue is triggered by CSCeb05456 and is applicable only if your Cisco IOS image has integrated the fix of CSCeb05456.

  Workaround: Periodically, reload the router so that the IPC buffer pool will be reinitialized.

Resolved Caveats for Product 'all' and Component 'ios-authproxy'

- CSCeg02918—Resolved in 12.2(18)ZY1

  Symptoms: A Cisco router that is configured with an HTTP authentication proxy may reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs a crypto image of Cisco IOS Release 12.3(9) or Release 12.3(10). Note that the symptom is not release-specific.

  Workaround: Disable the HTTP authentication proxy. If this is not an option, there is no workaround.

Resolved Caveats for Product 'all' and Component 'ios-firewall-aic'

- CSCsg70474—Resolved in 12.2(18)ZY1

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

Resolved Caveats for Product 'all' and Component 'ip-acl'

- CSCsg99155—Resolved in 12.2(18)ZY1

  Symptoms: When you configure an extended access control list (ACL) with the maximum sequence number and check the configuration with the **show access-list** command, the output does not show the maximum sequence number but a number that has one digit less than the configured maximum sequence number.

  Conditions: This symptom is observed on a Cisco 7500 series that has an RSP. However, the symptom is platform-independent.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'ip-rip'

- CSCsg42246—Resolved in 12.2(18)ZY1

  Symptoms: High CPU use may occur in the "IP Background" process, and the router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP and that receives a RIP host route that is subsequently replaced by a route that is dynamically assigned to an interface. For example, this situation may occur on a PPP interface that has the **ip address negotiated** command enabled.

  Workaround: Use a route map to block the advertised route.

Resolved Caveats for Product 'all' and Component 'ip-tunnels'

- CSCse40423—Resolved in 12.2(18)ZY1

  Symptoms: A tunnel interface cannot ping the other end of an IP tunnel.

  Conditions: This symptom is observed when ATM is configured and when the tunnel interface is up.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the tunnel interface.

- CSCsg47462—Resolved in 12.2(18)ZY1

  Symptoms: A router that is configured with at least one multipoint GRE tunnel may crash with an address error.

  Conditions: This symptom is observed when a T3 interface bounces while the CPU usage of the router is at 100 percent.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'ip'

- CSCed84633—Resolved in 12.2(18)ZY1

  Symptoms: The *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command do not function.

  Conditions: This symptom is observed on a Cisco platform that integrates the fix for caveat CSCea59206. A list of the affected releases can be found at http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCea59206. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

  Further Problem Description: The fix for CSCed84633 re-enables the *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command for both VRF interfaces and non-VRF interfaces.

- CSCsd59023—Resolved in 12.2(18)ZY1

  Symptoms: ARP entries that are associated with the default interface (of the default route or network) are refreshed when they should not be refreshed.

  Conditions: This symptom is observed on a Cisco router when other interfaces change their state or when the IP configuration of other interfaces is changed.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'ipc'

- CSCsh23981—Resolved in 12.2(18)ZY1

  Symptoms: During an HA switchover while IPC traffic is sent between the standby RP and standby SP, the newly active RP may crash.

  Conditions: This symptom is observed on Cisco Catalyst 6500 series switches and Cisco 7600 series routers. For Cisco Catalyst 6500 series switches, the symptom occurs in Release 12.2SX and Release 12.2SXF, in which ISSU is not supported. For Cisco 7600 series router, the symptom occurs in Release 12.2(33)SRB, in which ISSU is supported.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'ipsec-isakmp'

- CSCsg03739—Resolved in 12.2(18)ZY1

  Symptoms: A memory leak may occur in the "Crypto IKMP" process.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an IPSec VPN SPA (SPA-IPSEC-2G).

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'isis'

- CSCsb07279—Resolved in 12.2(18)ZY1

  Symptoms: When an IPv4 prefix list is used in a redistribution command for the IS-IS router process, a change in the prefix list is not immediately reflected in the routing tables of a router and its neighbor. The change may take up to 15 minutes to take effect.

  Conditions: Normal operation

  Workaround: To have a change take effect immediately, enter the "no redistribute route-map" command followed by the "redistribute route-map" command for the IS-IS router process.

- CSCsb34032—Resolved in 12.2(18)ZY1

  Symptoms: A router may reload unexpectedly when you remove the IS-IS configuration at the interface or router level.

  Conditions: This symptom is observed when the following conditions are present:

  - The router is HA-capable.
  - The **isis protocol shutdown** interface configuration command is enabled on the interface.
  - You enter an interface configuration command that enables IS-IS such as an **isis** command, a **clns** command, or the **ipv6 router isis** command before you enter a router configuration command such as the **net** command.

  When you remove the IS-IS configuration at the interface or router level, the router may reload.

  Workaround: Remove the **isis protocol shutdown** interface configuration command before you remove IS-IS from the interface or router level.

- CSCsc83821—Resolved in 12.2(18)ZY1

  Symptoms: The "MT IPv6 IP Reach 237" information (for a Multi-Topology Reachable IPv6 Prefixes TLV) may not be found in the IS-IS database, even though the information was previously learned from a peer. Expected behavior is that the following type of information is listed in the IS-IS database, however, this information is not present:

  Metric: 10 IPv6 (MT-IPv6) 22:1:2:2:2:2:2:2/128

  Conditions: This symptom is observed under the following conditions:

  1) You change the IS-IS IPv6 process by replacing the **multi-topology** command by the **multi-topology transition** command.

  2) You now enter the **isis metric** command with a non-default value on one of interfaces that are part of the IS-IS configuration.

  3) The **isis metric** command remains enabled on the interface when you change the IS-IS IPv6 process again by entering the **multi-topology** command.

  Workaround: Correct the state of the database by disabling the **isis metric** command.

- CSCse34050—Resolved in 12.2(18)ZY1

  Symptoms: IS-IS may not advertise a passive interface when it should do so, or IS-IS may advertise a passive interface when it should not do so.

  Conditions: This symptom is observed on a Cisco router when IS-IS misinterprets an interface "shutdown" event as an UP event.

  Workaround: Enable IS-IS on the interface by entering the **ip router isis** command and then make the interface passive by entering the **no ip router isis** command followed by the **passive-interface** *interface-type interface-number* command.

- CSCsf26043—Resolved in 12.2(18)ZY1

  Symptoms: IS-IS protocol packets may not be classified as high-priority. When this situation occurs during stress conditions and when the IS-IS protocol packets are mixed with other packets, the IS-IS protocol packets may be dropped because of their low-priority.

  Conditions: This symptom is observed on a Cisco platform that is configured for Selective Packet Discard (SPD).

  Workaround: Ensure that DSCP rewrite is enabled and then enter the following command:

  ```
  mls qos protocol isis precedence 6
  ```

- CSCsi41944—Resolved in 12.2(18)ZY1

  Symptoms: After redistribution-related configuration changes have been made, a CPUHOG condition may occur in the Virtual Exec process, causing loss of IS-IS adjacencies.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2(18)SXF when the **redistribute maximum-prefix** command is configured under the **router isis** command and when BGP is configured to be redistributed into IS-IS. The symptom could also affect a Cisco 7600 series router that runs Release 12.2SR.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'mpls-ldp'

- CSCsd40153—Resolved in 12.2(18)ZY1

  Symptoms: An ASBR has "No Label" as its outgoing label for a peer ASBR interface address.

  Conditions: This symptom is observed when the following conditions occur:

  - An ISP network (ISP network A) has two ASBRs that peer with one ASBR in another ISP network (ISP network B).
  - IGP routing (OSPF or any other IGP) is configured between the ASBRs in ISP network A.
  - A BGP session between one ASBR in ISP network A and the ASBR in ISP network B flaps.

  After about 5 minutes, all routes that are reachable via the ASBRs in ISP network A and the ASBR in ISP network B have "No Label" as their outgoing label.

  Workaround: Enter the **clear ip route** *network* command.

- CSCsf98345—Resolved in 12.2(18)ZY1

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

  Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

Resolved Caveats for Product 'all' and Component 'mpls-lfib'

- CSCsh58729—Resolved in 12.2(18)ZY1

  Symptoms: A router that is configured for MPLS FRR may crash.

  Conditions: This symptom is observed on a Cisco 7600 series but is platform-independent.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'os'

- CSCsc09336—Resolved in 12.2(18)ZY1

  Symptoms: When you enter the **show memory detailed** command, memory leaks in the process that this command is applied to.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured for Cisco IOS Software Modularity.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'osm-qos'

- CSCek70058—Resolved in 12.2(18)ZY1

  Symptoms: An Optical Services Module (OSM) may crash because of a memory corruption.

  Conditions: This symptom is observed when you apply a QoS configuration with WRED.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'pas-chstm1'

- CSCef56327—Resolved in 12.2(18)ZY1

  Symptoms: You may not be able to configure the **clock source line** command during the configuration of the SONET controller on a Cisco router in which a PA-MC-STM1 port adapter is installed.

  When you enter the **clock source line** command during the configuration of the SONET controller, the output of the **show running-config** command indicates that the clock source is set to line. However, the output of the **show controllers sonet** command indicates that the clock is set to internal, and when you enter the **show running-config** command again, the output indicates this time that the clock source is set to internal.

  Conditions: This symptom is observed when the PA-MC-STM1 port adapter is connected back-to-back via dark fiber to another PA-MC-STM1 port adapter.

  Workaround: Enter the **overhead s1byte ignore** command on the SONET controller before you configure the clock source.

Resolved Caveats for Product 'all' and Component 'pim'

- CSCsd16043—Resolved in 12.2(18)ZY1

  Symptoms: A Cisco IOS platform that is configured for Auto-RP in a multicast environment may periodically lose the RP to group mappings.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(17) when the RP drops the Auto-RP announce messages, which is shown in the output of the **debug ip pim auto-rp** command. This situation may cause a loss of multicast connectivity while the RP mappings are purged from the cache. See the following output example:

  ```
  Auto-RP(0): Received RP-announce, from ourselves (X.X.X.x), ignored
  ```

  Note that the symptom may also affect Cisco IOS Release 12.4 and Release 12.4T.

  Workaround: Create a dummy loopback interface (do not use the configured IP address in the whole network) and use the **ip mtu** to configure the size of the MTU for the RP interface to 1500 and the size of the MTU for the dummy loopback interface to 570, as in the following examples:

  ```
  interface Loopback1 ip address 10.10.10.10 255.255.255.255 ip mtu 570 ip pim
  sparse-mode end
  ```

(This example assumes that the Auto-RP interface is loopback 0.)

```
interface Loopback0 ip address 10.255.1.1 255.255.255.255 ip mtu 1500 ip pim
sparse-dense-mode end
```

Resolved Caveats for Product 'all' and Component 'pki'

- CSCsd85587—Resolved in 12.2(18)ZY1

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070522-crypto.html .

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070522-SSL.html

Resolved Caveats for Product 'all' and Component 'qos'

- CSCse94388—Resolved in 12.2(18)ZY1

  Symptoms: A SIP-200 that is configured with distributed Multilink Point-to-Point (dMLP) bundles and that has some of the bundles interleaved may crash.

  Conditions: This symptom is observed when you send traffic at line rate through all of the bundles.

  Workaround: There is no workaround.

- CSCsi01422—Resolved in 12.2(18)ZY1

  Symptoms: Frame Relay traffic shaping in a configuration with a child policy and hierarchical QoS does not function. Traffic does not respond to BECN or FECN marking.

  Conditions: This symptom is observed on a Cisco 7600 series when a service policy is configured under a Frame Relay map class. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

Resolved Caveats for Product 'all' and Component 'remote-registry'

- CSCsh83559—Resolved in 12.2(18)ZY1

  Symptoms: A Cisco Catalyst 6500 series switch may leak memory in the IP Input task in the Cisco IOS-BASE process. The memory is leaked in a small amount per packet that is process switched over a VRF on the switch. Non-VRF traffic is not affected.

  Conditions: This symptom is seen on a Cisco Catalyst 6500 series switch that is running Cisco IOS Modularity. This can only happen if there are VRFs configured on the switch.

  Workaround: Do not use VRFs.

Resolved Caveats for Product 'all' and Component 'snmp'

- CSCse80032—Resolved in 12.2(18)ZY1

  Symptoms: An SNMP Manager that uses SNMPv3 may not resynchronize the timer for the SNMP engine after the router has been reloaded.

  Conditions: This symptom is observed on Cisco Catalyst 6500 series switch and Cisco 7600 series router that have been reloaded and occurs because a parameter is incorrectly set in the REPORT message, causing a mediation device to register an SNMP timeout instead of a reload.

  Workaround: You may be able to restart the SNMP Manager to force the timer for the SNMP engine to resynchronize. Note, however, that doing so causes a 100-percent outage for all wiretaps that are served by the SNMP Manager. If you cannot restart the SNMP Manager, there is no workaround.

  Further Problem Description: This issue is specifically tied to doing lawful intercept. If you are not directed by some higher authority to be capable of lawful intercept, then you are not using it.

  The mediation device is what kicks off the lawful intercept process by doing snmp gets and sets using the following MIBs. The mediation device is a third party device designed specifically to be a mediation device.

Resolved Caveats for Product 'all' and Component 'socket'

- CSCse56501—Resolved in 12.2(18)ZY1

  Symptoms: When two sockets are bound to the same port, the first File Descriptor always receives the requests.

  Conditions: This symptom is observed on a Cisco router when two sockets such as one IPv4 socket and one IPv6 socket are connected to the same UDP port.

  Workaround: Use different UDP ports for different sockets.

Resolved Caveats for Product 'all' and Component 'ssh'

- CSCsb54378—Resolved in 12.2(18)ZY1

  Symptoms: A router may reload due to software forced crash.

  Conditions: This problem has been observed when initiating a Secure Shell (SSH) session from the router or when copying a file to/from the router via SCP.

  Workaround: Do not initiate SSH or SCP sessions from the router.

  Further Problem Description: This was observed on a Cisco 2811 router that was running Cisco IOS Release 12.4(4)T. Note that the symptom is not platform- or release-specific.

  Prior to the crash, the router logs a series of %SYS-3-CPUHOG messages and will eventually crash with %SYS-2-WATCHDOG. See the following example:

  %SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs (1426/5),process = Virtual Exec.
  -Traceback= 0x41DC8E2C 0x41DC9098 0x41BAA6E0 0x41BA6990 0x41B96B4C 0x41BA6768 0x41BA7490 0x41BA7750 0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 0x41834200
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec.
  -Traceback= 0x41A23CC8 0x41BAA3D8 0x41BA6A08 0x41B96B4C 0x41BA6768 0x41BA7490 0x41BA7750 0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 0x41834200 0x418341E4

  %Software-forced reload

- CSCsb74409—Resolved in 12.2(18)ZY1

  Symptoms: A router may keep the vty lines busy after finishing a Telnet/Secure Shell (SSH) session from a client. When all vty lines are busy, no more Telnet/SSH sessions to the router are possible.

  Conditions: This symptom is observed on a Cisco router that is configured to allow SSH sessions to other devices.

  Workaround: Clear the SSH sessions that were initiated from the router to other devices.

- CSCsc19259—Resolved in 12.2(18)ZY1

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070808-scp.html.

- CSCse24889—Resolved in 12.2(18)ZY1

  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

Resolved Caveats for Product 'all' and Component 'ssl'

- CSCsb12598—Resolved in 12.2(18)ZY1

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-SSL.html

  Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
  http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-crypto.html

  A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto.

- CSCsd92405—Resolved in 12.2(18)ZY1

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

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

  Cisco IOS is affected by the following vulnerabilities:

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

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

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-SSL.html

Note: Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
http://www.cisco.com/en/US/products/csa/cisco-sa-20070522-crypto.html

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20070522-crypto.

Resolved Caveats for Product 'all' and Component 'tcl-router'

- CSCsb46223—Resolved in 12.2(18)ZY1

  Symptoms: A router may crash because of a bus error when several Telnet users simultaneously run Tcl scripts. The problem is exacerbated by using scripts that take a long time to complete such as the following Tcl script:

  ```
  set ver [exec "show tech-support"] puts $ver
  ```

  When two users connect to the router through Telnet sessions and run the above Tcl script at the same time, the router may crash.

  Conditions: This symptom is observed when the Tcl scripts send text to the Telnet sessions simultaneously.

  The symptom may also occur when a single user connects to the router through a Telnet session, then from this Telnet session establishes another Telnet session into the same router, and runs a Tcl script that produces text output.

  Workaround: Prevent multiple users from connecting to the router through Telnet and running Tcl scripts. In such as situation, ensure that users do not enter commands in Tcl scripts that may take a long time to display their output such as the **show tech-support** command.

  Further Problem Description: Router console connections and incoming SSH connections to the router are not affected.

Resolved Caveats for Product 'all' and Component 'tcp'

- CSCed95187—Resolved in 12.2(18)ZY1

  Symptoms: RST packets may contain a non-randomized identification value on the IP header.

  Conditions: This symptom is observed on a Cisco platform that receives a TCP SYN packet on a non-listening port.

  Workaround: There is no workaround.

  Further Problem Description: From RFC791, the description of the Identification field is as follows:

  > Identification—The choice of the Identifier for a datagram is based on the need to provide a way to uniquely identify the fragments of a particular datagram. The protocol module assembling fragments judges fragments to belong to the same datagram if they have the same source, destination, protocol, and Identifier. Thus, the sender must choose the Identifier to be unique for this source, destination pair and protocol for the time the datagram (or any fragment of it) could be alive in the internet.

It seems then that a sending protocol module needs to keep a table of Identifiers, one entry for each destination it has communicated with in the last maximum packet lifetime for the internet.

Also from RFC791, section 3.1. (Internet Header Format): The IP ID is before the flags and fragment offset fields.

- CSCek12203—Resolved in 12.2(18)ZY1

  Symptoms: When you enter the **copy ftp disk** command, the copy operation may fail and cannot be terminated, further **copy** commands may fail, and a TCP vty session for the purpose of troubleshooting the situation may fail and cannot be terminated.

  Conditions: These symptoms are observed on a Cisco platform when the FIN flag is set in the initial ESTAB message from a neighbor. You must reload the router to recover from the symptoms.

  Workaround: Do not enter the **copy ftp disk** command. Rather, enter the **copy tftp disk** command.

Resolved Caveats for Product 'all' and Component 'telnet'

- CSCsb86257—Resolved in 12.2(18)ZY1

  Symptoms: When a named ACL is used at a vty line on a PE router with an interface that is configured in a VPN VRF, making a Telnet connection from this VRF on the interface that is part of the VRF is accepted even though the **vrf-also** keyword is not configured in the **access- class** *access-list-number* command.

  When a regular numbered ACL is used, an incoming Telnet connection from an interface that is part of a VRF is rejected without the **vrf- also** keyword being configured in the **access- class** *access-list-number* command.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router in an MPLS VPN environment and that has VPN VRFs configured.

  Workaround: Use a numbered ACL instead of a named ACL on vty lines on a PE router.

Resolved Caveats for Product 'all' and Component 'trans-bridging'

- CSCsh56081—Resolved in 12.2(18)ZY1

  Symptoms: When a VLAN bridge is configured on two switches, both switches may function as the root bridge in a bridge group, preventing a blocking port from appearing in the Spanning Tree Protocol (STP) because neither of the switches can receive a Bridge Protocol Data Unit (BPDU). This situation may cause a bridging loop.

  Conditions: This symptom is observed when two Cisco switches are connected through a trunk port and when you enter a sequence of commands such as the following one:

  ```
  int vlan 2 bridge-group 1 bridge 1 protocol vlan-bridge
  ```

  Workaround: Remove the VLAN bridge and then reconfigure it by entering a sequence of commands such as the following one:

  ```
  bridge 1 protocol vlan-bridge int vlan 2 bridge-group 1
  ```

Resolved Caveats for Product 'all' and Component 'udp'

- CSCsh75069—Resolved in 12.2(18)ZY1

  Symptom: A router interface stops forwarding traffic when it receives traffic to the UDP echo port (port 7) addressed to the interface iteself.

  Condition: An input queue wedge condition exists in handling UDP traffic destined the echo service.

  Workaround: Disable the UDP echo service with the configuration command:

  ```
  no udp-small-servers
  ```

Resolved Caveats for Product 'all' and Component 'wccp'

- CSCuk61773—Resolved in 12.2(18)ZY1

  Symptoms: CPU spikes may occur on a router that is configured for Web Cache Communication Protocol (WCCP) earlier than Release 4.0.7.

  Conditions: This symptom is observed on a Cisco 7600 series when WCCP is in communication with a Cisco Wide Area Application Services (WAAS) appliance. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

Resolved Caveats for Product 'c10000' and Component 'bgp'

- CSCsc46337—Resolved in 12.2(18)ZY1

  Symptoms: When about a thousand eBGP connections are opened between two routers that are connected back-to-back, additional point-to-point eBGP connections between the routers are not established even if IP connectivity between the BGP next-hops is provided.

  Conditions: This symptom is observed when one Cisco router functions as a PE router and the other Cisco router functions as a CE router that has VRF-lite configured.

  Workaround: Reload the PE router to enable all sessions to become established, including the ones that previously were not established.

Resolved Caveats for Product 'c10000' and Component 'qos'

- CSCsd76528—Resolved in 12.2(18)ZY1

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: None of the policy classes after the first child policy of a hierarchical QoS policy take effect when you reload the router.

  Condition 1: This symptom is observed on a Cisco 7304 that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

  Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **service-policy output** interface configuration command to enable the child policies to take effect. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

  Symptom 2: On a Cisco 10000 series that is configured with hierarchical queueing policies, when you remove the **match vlan** command for a VLAN that matches a dot1q subinterface, the queues that are allocated to the subinterface are not cleared, allowing traffic to continue to flow through these queues.

  Condition 2: This symptom is observed on a Cisco 10000 series that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

  Workaround 2: There is no workaround. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

Resolved Caveats for Product 'c12000' and Component 'ip-pbr'

- CSCsa46154—Resolved in 12.2(18)ZY1

  Symptoms: A Route Processor (RP) failover occurs.

  Conditions: This symptom occurs when you enter the **show route-map** command in one session and remove several route maps in rapid succession in another session.

  Workaround: Do not enter the **show route-map** command when you remove route maps in a concurrent vty session.

Resolved Caveats for Product 'c2800' and Component 'voice-xgcp'

- CSCsd81407—Resolved in 12.2(18)ZY1

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

Resolved Caveats for Product 'c3600' and Component 'voice-sip'

- CSCeb21064—Resolved in 12.2(18)ZY1

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070808-IOS-voice.html.

Resolved Caveats for Product 'c6k-psd' and Component 'pstore'

- CSCir02111—Resolved in 12.2(18)ZY1

  Symptoms: Tracebacks and error messages may be generated on a Supervisor Engine 720.

  Conditions: This symptom is observed when the PSD module in a Cisco 7600 series is reset to the AP mode.

  Workaround: There is no workaround.

Resolved Caveats for Product 'c7300' and Component 'netflow-switch'

- CSCsc73699—Resolved in 12.2(18)ZY1

  Symptoms: A router that is configured for NetFlow v9 may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S4 or Release 12.2(27)SBC1 when the configuration is modified while the router actively exports flows. The symptom may also occur in other releases.

  Workaround: There is no workaround.

Resolved Caveats for Product 'c7600' and Component 'c7600-sip-400'

- CSCsg79810—Resolved in 12.2(18)ZY1

  Symptoms: The MPLS MTU is overruled by the IP MTU on an ATM interface.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an MPLS core when the ATM interface has the **tag-switching mtu 1508** command and the **ip mtu 1500** command enabled. In this situation, packets that are larger than 1496 bytes are dropped.

  Workaround: There is no workaround.

Resolved Caveats for Product 'c7600' and Component 'c7600-sip-600'

- CSCsh54325—Resolved in 12.2(18)ZY1

  This caveat consists of two symptoms, two conditions, and two workarounds:

  Symptom 1: When frames require PXF punting to the RP (or SP), PPP LCP frames may not be forwarded to the RP (or SP), causing link negotiation to fail. Or, HDLC keepalives may not be forwarded to the RP (or SP), causing the link to remain down.

  Condition 1: These symptoms are observed on a Cisco Catalyst 6503, Cisco Catalyst 6503-E, and Cisco 7604 that are configured with a SIP-600 in which a POS SPA is installed and occurs when the supervisor engine resides in slot 1 or slot 2 of the chassis.

  Workaround 1: There is no workaround.

  Symptom 2: When frames require PXF punting to the RP (or SP), CFM PDUs may not be properly forwarded to the RP (or RP).

  Condition 2: This symptom is observed on a Cisco 7604 that is configured with a SIP-600 or Ethernet Services line card (ES20) and occurs when the supervisor engine resides in slot 1 or slot 2 of the chassis.

  Workaround 2: There is no workaround.

Resolved Caveats for Product 'c7600' and Component 'osm-pos'

- CSCsg21429—Resolved in 12.2(18)ZY1

  Symptoms: The interface of an OSM-1OC48-POS-SI+ module may flap after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with redundant Supervisor Engine 720-3BXL modules that function in RPR+ mode.

  Workaround: Repeat the **redundancy force-switchover** command several times.

Resolved Caveats for Product 'c7600' and Component 'osm-qos'

- CSCsh07037—Resolved in 12.2(18)ZY1

  Symptoms: A "%SYS-2- CHUNKBADMAGIC" error may occur on an OSM module and the module may restart.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when Weighted Random Early Detection (WRED) is configured with a maximum threshold of more than 2000 packets but without a queue limit.

  Workaround: Configure a proper queue limit for the class with the WRED configuration. For example, when the **random-detect precedence 3 32000 32000 1** command is configured, configure the queue limit by entering the **queue-limit 32768** command.

Resolved Caveats for Product 'c7600' and Component 'qos'

- CSCsh46565—Resolved in 12.2(18)ZY1

  Symptoms: When the configuration of the shape average is changed, the rate is not applied, which can be shown in the output of the **show policy interface** command and detected by a traffic analyzer.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and GE-WAN subinterfaces that are configured with an HQoS (LLQ) output policy when the shape average is changed on all GE-WAN subinterfaces at the same time.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, delete the output policy and then reconfigure it on the GE-WAN subinterfaces.

Resolved Caveats for Product 'c7600' and Component 'vipmlp'

- CSCse91675—Resolved in 12.2(18)ZY1

  Symptoms: The RP may generate an "RX FIFO FULL" error message for a SPA, followed by a "VC_CONFIG" error message, and subsequently all interfaces on all SPAs that are processing traffic may go down.

  Symptoms: This symptom is observed on a Cisco 7600 series that is configured with MLP or MFR bundles on a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3), 2-port channelized T3/DS0 SPA (SPA-2XCT3/DS0), or 4-port channelized T3/DS0 SPA (SPA-4XCT3/DS0) when traffic exceeds about 350 kpps on these bundles.

  Workaround: After the symptom has occurred, reload the affected SPAs or the SIPs in which the affected SPAs are installed. There is no workaround to prevent the symptom from occurring. Therefore, configure the MLP or MFR bundles in such a manner that the 350 kpps threshold is not exceeded.

Resolved Caveats for Product 'cat6000' and Component 'c7600-sip-600-vpls'

- CSCse39956—Resolved in 12.2(18)ZY1

  Symptoms: When a pseudowire VC that has negotiated to use of the Control Word (that is, Cbit = 1) is followed by another pseudowire VC) that has negotiated to not use the Control Word (i.e., Cbit = 0), the Control Word (CW) may still be prepended to the pseudowire VC that has negotiated to not use the CW. As a result, the disposition router (or tail endpoint) does not expect a CW and cannot decapsulate the VC packet; instead, the packet is dropped at the disposition router as a corrupted packet.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a SIP-600 and that function in a VPLS environment as egress PE routers.

  Workaround: Ensure that VCs in a VPLS environment do not have a mixture of negotiated CWs (that is, Cbits). The output of the **show mpls l2transport binding** command shows the VCs and Cbits.

  Further Problem Description: One scenario in which the symptom occurs is the following:

  - A VPLS hub-spoke environment is created with a mixture of hardware-based and software-based EoMPLS VCs.
  - When the SIP-600 detects the CW setting for one VC, it assumes that the VC that follows the first VC also has the CW, and inserts the CW.
  - When a hardware-based EoMPLS VC is in the middle of the replication chain, ping failures may occur for CE routers that are located behind the hardware-based EoMPLS VC. A hardware-based EoMPLS VC does not support the CW and ping failures occur because the MAC address of the customer becomes corrupted.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-acl'

- CSCsg72398—Resolved in 12.2(18)ZY1

  Symptoms: Traffic to a Cisco IOS SLB virtual server that is configured for UDP may be process-switched.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with multiple virtual servers.

  Workaround: Enter the **mls ip slb search wildcard rp** command.

- CSCsh76923—Resolved in 12.2(18)ZY1

  Symptoms: A Cisco Catalyst 6500 series switch may crash because of memory corruption or a bus error.

  Conditions: This symptom is observed when NAT is configured. The symptom may also affect a Cisco 7600 series router.

  Workaround: There is no workaround.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-diag'

- CSCek66277—Resolved in 12.2(18)ZY1

  Symptoms: When you run the TestAclDeny diagnostic test, the output of the **show diagnostic content module** *num* command, with the *num* representing the active supervisor engine, shows the test as "N" to denote non-disruptive. This situation is shown in the following example:

  18) TestAclDeny ----------> M**N****A*** 000 00:00:05.00 n/a

  In reality, the TestAclDeny diagnostic test for the active supervisor engine is a disruptive test because the test may cause traffic forwarding issues and flapping of the first uplink port.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: Do not run the TestAclDeny diagnostic test.

  Further Problem Description: The fix for this caveat sets the flag to "D" to denote disruptive.

- CSCsg08200—Resolved in 12.2(18)ZY1

  Symptoms: The bootup diagnostics for a line card may detect a major failure after an RPR switchover has occurred, and these line cards reset repeatedly and eventually power-down.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router and occurs only with a Supervisor Engine 720 that is configured with a PFC3BXL (WS-SUP720-3BXL) or with a DFC3BXL-equipped module.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur after an SSO or RPR+ switchover has occurred.

- CSCsh22835—Resolved in 12.2(18)ZY1

  Symptoms: After an RPR switchover occurs, a major error occurs on the newly active RP.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: Reload the platform. If this not an option, there is no workaround.

- CSCsh29863—Resolved in 12.2(18)ZY1

  Symptoms: On an RPR switchover, the new active crashes during bootup diagnostics.

  Conditions: This symptom occurs when bad SFPs are plugged into the SFP- capable ports. Bad SFP means incompatible/unsupported/faulty SFP.

  Workaround: Remove incompatible/unsupported/faulty SFPs from the SFP port(s) and plug in a good one if needed.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-env'

- CSCsg90190—Resolved in 12.2(18)ZY1

  Symptoms: Without the enforcement of a voice daughterboard connector rating, the number of IP phones that can be powered up may exceed the number that the voice daughterboard can handle, that is, the available allocated inline power can exceed the VDB connector rating.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsh17979—Resolved in 12.2(18)ZY1

  Symptoms: When inline power ports can not be powered on, a command may be rejected with the following error message:

  Command rejected: theres not enough system power to be allocated to Fa1/47, or the maximum power the backplane of this chassis can support has reached the limit.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a module with a voice daughtercard.

  Workaround: There is no workaround.

- CSCsh25976—Resolved in 12.2(18)ZY1

  Symptoms: There are two symptoms:

  1) The threshold of the fan-fail sensor of the power supply may not be updated correctly, and the following error message may be generated:

  power-supply incompatible with fan: N/A

  The value should not be “N/A” but “OK”.

  2) The threshold of the fan-fail sensor of the power supply may get be added when power supply is detected. For example, information about the fan-fail sensor of the power supply may not be shown in the output of the **show environment alarm thresholds power-supply** command.

  Condition: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: Initiate a Stateful Switchover (SSO). After the SSO, the symptom no longer occurs.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-firmware'

- CSCsg35506—Resolved in 12.2(18)ZY1

  Symptoms: After a Gigabit Ethernet (GE) interface has flapped, a mismatch may occur on a port channel, preventing the GE interface from joining the port channel. This situation occurs when the default flow control operational mode on the GE interface is unexpectedly changed from "off/off" to "on" after the GE interface has flapped.

  If the symptom occurs for the first interface of a group of interfaces that is supposed to join the port channel, none of the interfaces in the group can join the port channel, degrading the bandwidth and possibly causing severe packet drops on the channel.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router, and affects the following modules:

  - Supervisor Engines 1 and 1a
  - Supervisor Engine 2
  - WS-X6408-GBIC
  - WS-X6416-GBIC
  - WS-X6516-GBIC and WS-X6516A-GBIC

  Note that the symptom does not occur with the WS-X6724-SFP and the WS-X6748-GE-TX.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected GE interface.

  Further Problem Description:

  - Any operation that causes flow control negotiation triggers the symptom. For example. problem, entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command, resetting the module, performing an OIR, an RPR switchover, and so on.
  - The symptom tends to occur when many ports are brought up simultaneously.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-ha'

- CSCsg64170—Resolved in 12.2(18)ZY1

  Symptoms: When an SSO switchover occurs for an RSP or supervisor engine, network traffic loss may occur or the active Firewall Services Module (FWSM) may unexpectedly failover to the standby FWSM in an unusual way in that both the active and the standby FWSMs become active (that is, the active FWSM remains active and the standby FWSM becomes active). This situation causes traffic loss to and from the FWSMs until the standby FWSM enters the standby state.

  The symptom is not restricted to the FWSMs but may also occur with the following service modules:

  - WS-SVC-WEBVPN-K9
  - WS-SVC-SSL-1-K9
  - WS-SVC-FWM-1-K9
  - WS-X6066-SLB-APC
  - WS-X6066-SLB-S-K9

  Conditions: These symptoms are observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that have service modules installed in slot 1 and slot 2. The symptoms occur when two power supplies are inserted in the chassis but only one power supply is turned on or one power supply fails during normal operation, and then a SSO switchover occurs. The symptoms do not occur when both power supplies are turned on or when there is only one power supply in the chassis.

  Workaround: Ensure that both power supplies are turned on.

  Alternate Workaround: Install the service modules in any slots other than slot 1 or slot 2.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-l2'

- CSCsb85030—Resolved in 12.2(18)ZY1

  Symptoms: Packets such as DHCP packets may be dropped, and MAC addresses may not be learned on interfaces even though the interfaces are in the up/up state.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when you first configure and then remove port security.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, manually configure the MAC addresses in the MAC-address table.

  Alternate Workaround: Re-enable and then disable port security once more on the affected ports.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-mcast'

- CSCsb64767—Resolved in 12.2(18)ZY1

  Symptoms: When a Layer 2 EtherChannel is load-balancing multicast traffic on multiple member ports of a local switch or router, one port may not transmit multicast packets but may drop them. When this situation occurs, the OutMcastPkts counter for this port does not increase.

  Condition: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when an OIR is performed on a line card of the remote switch or router, causing the local port that is a member of the EtherChannel to change its state to link down and then to link up.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on affected member port of the local switch or router. Doing so re-enables multicast forwarding.

- CSCsg61773—Resolved in 12.2(18)ZY1

  Symptoms: Egress multicast forwarding may not function when an outgoing interface (OIF) flaps very quickly.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when Multicast MultiLayer Switching (MMLS) is configured (MMLS is configured by default).

  Workaround: There is no workaround.

  Further Problem Description: When an interface flaps very quickly, the module mask may not be allocated for the interface, causing the egress multicast functionality to be affected. In this situation, the interface may not function properly as an OIF.

- CSCsg73179—Resolved in 12.2(18)ZY1

  Symptoms: After a change in the routing topology, a Bidirectional PIM Rendezvous Point is not updated correctly in the hardware tables, causing Bidirectional PIM multicast flows to be software-switched.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router and occurs only when the ACL that is used to statically configure the Rendezvous Point does not have any wildcard entries.

  Workaround: Reinstall the Rendezvous Point.

- CSCsh05800—Resolved in 12.2(18)ZY1

  Symptoms: When an L3 DEC PortChannel is used with a subinterface that is created before a member of an EtherChannel is created, the first port of entry (FPOE) is not programed correctly for the member of the EtherChannel, preventing multicast traffic from being forwarded over the member of the EtherChannel even when software and/or hardware entries do exist.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router only for members of an EtherChannel that are not up when the subinterface is created. This situation may occur after the platform has been reload during the boot process when subinterfaces are created while other interfaces are not yet up.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface that was created before the member of the EtherChannel was created.

  Alternate Workaround: Configure ingress replication mode.

- CSCsh98208—Resolved in 12.2(18)ZY1

  Symptoms: PIM Snooping causes duplicate multicast packets to be delivered in the network.

  Conditions: This symptom is observed when the shared tree and SPT diverge in a VLAN on a Cisco Catalyst 6500 series switch or Cisco 7600 series router that have PIM Snooping configured. PIM Snooping may suppress the (S,G) RPT-bit prune message that is sent by the receiver from reaching the upstream router in the shared tree, causing a situation in which more than one upstream router forward the multicast traffic by using their respective (S,G)-join state, and, in turn, causing duplicate multicast packet to be delivered to the receivers. This situation lasts only for a brief moment because the PIM-ASSERT mechanism kicks in and stop the extraneous flow. However, this cycle repeats again when the next (*,G) join (S,G) RPT bit prune message is sent by one of the receivers.

  Workaround: Disable PIM Snooping in the VLAN-interface configuration.

  Alternate Workaround: If the command is available in the release that you are running, enter the **no ip pim snooping suppress sgr-prune** command to disable SGR-prune message suppression.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-netflow'

- CSCse49388—Resolved in 12.2(18)ZY1

  Symptoms: On a physical interface or subinterface on which a tunnel is configured and that encrypts or decrypts traffic, when you shut down and bring up the physical interface or subinterface multiple times, MAC entries for all VLANs that support the tunnel may be removed.

  When this situation occurs, when the "RMac reference " counter reaches 1, and when you shut down the physical interface or subinterface for the last time, packets are prevented from traversing the tunnel.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with either a Supervisor Engine 32 or a Supervisor Engine 720 and with a SIP-400 in which an IPsec VPN SPA is installed.

  Workaround: To prevent the symptom from occurring, do not shut down and bring up the physical interface or subinterface that supports the IPsec tunnel. When the symptom has occurred, reload the SIP-400 to reset the "RMac reference" counter to the original value.

  Further Problem Description: To see if the symptom has occurred, check the "RMac reference" counter as follows:

  ```
  # remote login switch
  sp# test mls net debug task 1 stat
  ...
  Netflow RMac List:
  0013.5f21.9100[14] <<-- where [n] is the reference count, in this case 14.
  Tunnel Interface(s):
  ...
  sp#
  ```

  You can check the counter each time after you have shut down and brought up the physical interface or subinterface. If, after every iteration, the reference count keeps decrementing towards 0, it means the symptom has occurred. A flapping link does not cause this problem. The "RMac reference" counter decreases each time that you shut down the physical interface or subinterface, perform and OIR of the SPA, or reset the SPA.

- CSCsg02241—Resolved in 12.2(18)ZY1

  Symptoms: Incorrect NAT translation may occur for one or more faulty Multilayer Switching (MLS) flows. You can recognize a faulty MLS flow in the output of the **show mls netflow ip** command. If any two MLS flows show the same adjacency, one of the MLS flows is faulty.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured for NAT and occurs regardless of whether or not a Supervisor Engine 32 or Supervisor Engine 720 is configured for central or distributed forwarding.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(18)SXF8 and later releases.

- CSCsg47044—Resolved in 12.2(18)ZY1

  Symptoms: NetFlow Data Export (NDE) may not export NetFlow entries for bridged flow packets.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF6. This symptom occurs when you enter the **ip flow ingress layer2-switched vlan** *vlan id* command before you have configured an IP address for the specified VLAN ID. The symptom may also occur in Release 12.2SR.

  Workaround: Enter the **ip flow ingress layer2-switched vlan** *vlan id* command after you have configured an IP address for the specified VLAN ID.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-qos'

- CSCsh01749—Resolved in 12.2(18)ZY1

  Symptoms: The **mls qos marking ignore port-trust** command may not function.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch or Cisco 7600 series router that has a Supervisor Engine 32 or Supervisor Engine 720. When you enter the **mls qos marking ignore port-trust** command for an interface that is configured with several subinterfaces, each with a service policy, the service policies are supposed to match a unique ingress CoS value and change the corresponding egress MPLS EXP value for transfer across an MPLS cloud. However, after you have entered the **mls qos marking ignore port-trust** command, all egress EXP values show up as 0 because the command has no effect.

  Workaround: There is no workaround.

Resolved Caveats for Product 'cat6000' and Component 'cat6000-snmp'

- CSCsf31458—Resolved in 12.2(18)ZY1

  Symptoms: The entPhysicalIndex object of the ENTITY-MIB may not remain the same after an SSO switchover has occurred on a Supervisor Engine 32.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsg24609—Resolved in 12.2(18)ZY1

  Symptoms: A MIB walk on the CISCO-L2-CONTROL-MIB occurs very slowly.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that do not have the **mac-address-table limit vlan** *vlan* command enabled.

  Workaround: Enter the **mac-address-table limit vlan** *vlan* command.

Resolved Caveats for Product 'cat6000' and Component 'loadbal'

- CSCse34615—Resolved in 12.2(18)ZY1

  Symptoms: A RADIUS virtual server drops RADIUS accounting on and off packets, instead of forwarding the packets to the real servers. The client never receives response packets for the RADIUS accounting on and off packets that were sent.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCse56921—Resolved in 12.2(18)ZY1

  Symptoms: A platform that is configured for GPRS Tunneling Protocol (GTP) Server Load Balancing (SLB) may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when the same International Mobile Subscriber Identity (IMSI) is sent in two or more Packet Data Protocol (PDP) requests to different virtual servers and occurs when the sticky table entries time-out.

  Workaround: There is no workaround.

- CSCsg16425—Resolved in 12.2(18)ZY1

  Symptoms: The output of the **show ip slb reals** command displays very large connection values (conns) for some real servers.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured for Cisco IOS Server Load Balancing (IOS SLB) with inter-firewall routing enabled via the **ip slb route inter-firewall** command. The symptom occurs only when the inter-firewall connections switch from one firewall real to other firewall real in the firewall farm.

  Workaround: Remove and reconfigure the real server that is part of the server farm or firewall farm.

  Further Problem Description: When the connection value for a real server becomes very large, the server may enter the "MAXCONNS" state. When this situation occurs, you can no longer clear the connections counter by entering the **clear ip slb counters** or **clear ip slb connections** command.

Resolved Caveats for Product 'cat6000' and Component 'osm-ucode'

- CSCsg40425—Resolved in 12.2(18)ZY1

  Symptoms: An Optical Services Module (OSM) may reset unexpectedly and generate the following error messages:

  %POSLC-3-SOP: TxSOP-0 SOP. (source=0x18, halt_minor0=0x4000)
  %CWANLC-3-FATAL: Fatal Management interrupt, gen_mgmt_intr_status 0x0, line_mgmt_intr_status 0x1, reloading

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

  Workaround: There is no workaround.

Resolved Caveats for Product 'cat6000' and Component 'spa-ipsec-2g'

- CSCek65022—Resolved in 12.2(18)ZY1

  Symptoms: A 7600-SSC-400 SPA services carrier may crash during the boot process of a SPA.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when an IPsec VPN Shared Port Adapter (SPA-IPSEC-2G) that is installed in the 7600-SSC-400 boots.

  Workaround: There is no workaround.

Resolved Caveats in Release 12.2(18)ZY

- CSCsd95616—Resolved in Release 12.2(18)ZY

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

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

- CSCsc19259—Resolved in 12.2(18)ZY

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070808-scp.html.

- CSCsd85587—Resolved in 12.2(18)ZY

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070522-crypto.html .

  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://www.cisco.com/en/US/products/csa/cisco-sa-20070522-SSL.html

Troubleshooting

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

- Spanning Tree Troubleshooting, page 170
- Additional Troubleshooting Information, page 171

Note To attempt recovery from PISA ROMMON, enter the **confreg 0x2102** and **reset** ROMMON commands.

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.

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 sum of all logical interfaces equals the number of trunks on the switch times the number of active VLANs on the trunks, plus the number of nontrunking interfaces on the switch.
- The **show spanning-tree summary totals** command displays the number of logical interfaces in the STP Active column.
- These maximum numbers of logical interfaces are supported:

MST	RPVST+	PVST+
50,000 total	10,000 total	13,000 total
6,000[1] per switching module	1,800[1] per switching module	1,800[1] per switching module

1. 10 Mbps, 10/100 Mbps, and 100 Mbps switching modules support a maximum of 1,200 logical interfaces per module.

Note Cisco IOS software displays a message if you exceed the maximum number of logical 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

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2. These documents consist of software installation guides, Cisco IOS configuration and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Use these release notes with the documents and tools described in the following sections:

- Release-Specific Documents, page 171
- Cisco Feature Navigator, page 172
- Cisco IOS Software Documentation Set, page 172

Release-Specific Documents

The following document is specific to Cisco IOS Release 12.2 and is located on Cisco.com:

- Caveats for Cisco IOS Release 12.2

  See *Caveats for Cisco IOS Release 12.2* for caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: Release Notes: Caveats

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, l**og in** to Cisco.com and click **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to this URL:

http://tools.cisco.com/Support/BugToolKit/

Platform-Specific Documents

These publications are available for the Catalyst 6500 series switches running Cisco IOS on the supervisor engine and PISA:

- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Catalyst 6500 Series Switch Cisco IOS System Message Guide*

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://tools.cisco.com/RPF/register/register.do

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

The Cisco IOS software documentation set is available on Cisco.com.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: Configuration Guides and Command References

Release 12.2 Documentation Set

Table 1 lists the contents of the Cisco IOS Release 12.2 software documentation set.

Note You can find the most current Cisco IOS documentation on Cisco.com.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2

Table 1 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• Cisco IOS Configuration Fundamentals Configuration Guide • Cisco IOS Configuration Fundamentals Command Reference	Cisco IOS User Interfaces File Management System Management
• Cisco IOS Bridging and IBM Networking Configuration Guide • Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2 • Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server

Table 1 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• Cisco IOS Dial Technologies Configuration Guide • Cisco IOS Dial Technologies Command Reference	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• Cisco IOS IP Configuration Guide • Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services • Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols • Cisco IOS IP Command Reference, Volume 3 of 3: Multicast	IP Addressing and Services IP Routing Protocols IP Multicast
• Cisco IOS AppleTalk and Novell IPX Configuration Guide • Cisco IOS AppleTalk and Novell IPX Command Reference	AppleTalk Novell IPX
• Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide • Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• Cisco IOS Voice, Video, and Fax Configuration Guide • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• Cisco IOS Quality of Service Solutions Configuration Guide • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 1 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• Cisco IOS Security Configuration Guide • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• Cisco IOS Switching Services Configuration Guide • Cisco IOS Switching Services Command Reference	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• Cisco IOS Wide-Area Networking Configuration Guide • Cisco IOS Wide-Area Networking Command *Reference*	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
• Cisco IOS Mobile Wireless Configuration Guide • Cisco IOS Mobile Wireless Command Reference	General Packet Radio Service
• Cisco IOS Terminal Services Configuration Guide • Cisco IOS Terminal Services Command Reference	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • Cisco IOS Debug Command Reference • Cisco IOS Software System Error Messages • *New Features in 12.2-Based Limited Lifetime Releases* • New Features in Release 12.2 T • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

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:

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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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

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.