Release Notes for Cisco IOS Release 12.2SXF and Rebuilds

March 29, 2011

Release Notes for Cisco IOS Release 12.2(33)SXH and Later Releases

For Release 12.2(33)SXH and later releases, see this publication:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/release/notes/ol_14271.html

Release Notes for Cisco IOS Release 12.2(18)SXF and Rebuilds

This publication applies to these platforms with Release 12.2(18)SXF and rebuilds:

- CAT6000-SUP720/MSFC3
- 7600-SUP720/MSFC3
- CAT6000-SUP32/MSFC2A (not supported in all releases)
- 7600-SUP32/MSFC2A (not supported in all releases)
- CAT6000-SUP2/MSFC2 (not supported in all releases)
- 7600-SUP2/MSFC2 (not supported in all releases)

See this product bulletin for information about the standard maintenance and extended maintenance 12.2SX releases:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd804f0694.html

These release notes are for Cisco IOS Release 12.2(18)SXF and rebuilds on both the supervisor engine and the MSFC. If you are running the Catalyst operating system on the supervisor engine and Cisco IOS Release 12.2SX only on the MSFC, refer to this publication:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_end-of-life_notice0900aecd80699ddb.html

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

The most current version of these release notes are available on Cisco.com at this URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html

Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

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

Participate in the Technical Documentation Ideas forum

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

Chronological List of Releases

Note

- See the "Feature Sets" section on page 115 for information about which releases are deferred.
- See the "Hierarchical List of Releases" section on page 4 for information about parent releases.

This is a chronological list of the 12.2SX releases:

- 29 Mar 2011—Release 12.2(18)SXF17b
- 19 Mar 2010—Release 12.2(18)SXF17a
- 30 Sep 2009—Release 12.2(18)SXF17
- 05 Mar 2009—Release 12.2(18)SXF16
- 29 Oct 2008—Release 12.2(18)SXF15a
- 05 Sep 2008—Release 12.2(18)SXF15
- 09 May 2008—Release 12.2(18)SXF14
- 17 Feb 2008—Release 12.2(18)SXF13
- 15 Jan 2008—Release 12.2(18)SXF12a
- 19 Nov 2007—Release 12.2(18)SXF12
- 21 Sep 2007—Release 12.2(18)SXF10a
- 18 Sep 2007—Release 12.2(18)SXF11
- 16 Jul 2007—Release 12.2(18)SXF10
- 21 May 2007—Release 12.2(18)SXF9
- 07 Mar 2007—Release 12.2(18)SXF8
- 30 Jan 2007—Release 12.2(18)SXE6b
- 12 Dec 2006—Release 12.2(18)SXD7b

- 30 Nov 2006—Release 12.2(18)SXF7
- 22 Sep 2006—Release 12.2(18)SXF6
- 18 Sep 2006—Release 12.2(18)SXE6a
- 15 Sep 2006—Release 12.2(18)SXD7a
- 10 Jul 2006—Release 12.2(18)SXF5
- 08 Jun 2006—Release 12.2(18)SXE6
- 17 Apr 2006—Release 12.2(17d)SXB11a
- 27 Mar 2006—Release 12.2(18)SXF4
- 16 Feb 2006—Release 12.2(18)SXF3
- 13 Feb 2006—Release 12.2(18)SXE5
- 20 Jan 2006—Release 12.2(18)SXF2
- 22 Dec 2005—Release 12.2(18)SXF1
- 15 Dec 2005—Release 12.2(18)SXD7
- 17 Nov 2005—Release 12.2(17d)SXB11
- 10 Oct 2005—Release 12.2(18)SXE4
- 12 Sep 2005—Release 12.2(18)SXF
- 22 Aug 2005—Release 12.2(18)SXE3
- 22 Aug 2005—Release 12.2(18)SXD6
- 16 Aug 2005—Release 12.2(17d)SXB10
- 21 Jul 2005—Release 12.2(17d)SXB9
- 23 Jun 2005—Release 12.2(18)SXE2
- 16 May 2005—Release 12.2(18)SXD5
- 02 May 2005—Release 12.2(17d)SXB8
- 18 Apr 2005—Release 12.2(18)SXE1
- 11 Apr 2005—Release 12.2(18)SXE
- 24 Mar 2005—Release 12.2(18)SXD4
- 01 Mar 2005—Release 12.2(17d)SXB7
- 21 Dec 2004—Release 12.2(17d)SXB6
- 13 Dec 2004—Release 12.2(18)SXD3
- 01 Nov 2004—Release 12.2(17d)SXB5
- 22 Oct 2004—Release 12.2(18)SXD2
- 30 Sep 2004—Release 12.2(18)SXD1
- 07 Sep 2004—Release 12.2(17d)SXB4
- 17 Aug 2004—Release 12.2(17d)SXB3
- 26 Jul 2004—Release 12.2(18)SXD
- 21 Jul 2004—Release 12.2(17d)SXB2
- 01 Jun 2004—Release 12.2(17d)SXB1
- 23 Apr 2004—Release 12.2(17a)SX4

- 22 Apr 2004—Release 12.2(17b)SXA2
- 05 Mar 2004—Release 12.2(17d)SXB
- 05 Mar 2004—Release 12.2(17a)SX3
- 29 Jan 2004—Release 12.2(17a)SX2
- 31 Dec 2003—Release 12.2(17b)SXA
- 30 Oct 2003—Release 12.2(17a)SX1
- 06 Oct 2003—Release 12.2(17a)SX
- 01 Jul 2003—Release 12.2(14)SX2 (MSFC3 only)
- 28 May 2003—Release 12.2(14)SX1
- 14 Apr 2003—Release 12.2(14)SX

Hierarchical List of Releases

These releases support the hardware listed in the "Supported Hardware" section on page 33:

- Release 12.2(18)SXF17b:
  - Date of release: 29 Mar 2011
  - 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)SXF17a
- Release 12.2(18)SXF17a:
  - Date of release: 19 Mar 2010
  - 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)SXF17
- Release 12.2(18)SXF17:
  - Date of release: 30 Sep 2009
  - 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)SXF16
- Release 12.2(18)SXF16:
  - Date of release: 05 Mar 2009
  - 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)SXF15a
- Release 12.2(18)SXF15a:
  - Date of release: 29 Oct 2008
  - 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)SXF15
- Release 12.2(18)SXF15:
  - Date of release: 05 Sep 2008
  - 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)SXF14

- Release 12.2(18)SXF14:
  - Date of release: 09 May 2008
  - 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)SXF13
- Release 12.2(18)SXF13:
  - Date of release: 17 Feb 2008
  - 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)SXF12
- Release 12.2(18)SXF12a:
  - Date of release: 15 Jan 2008
  - 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)SXF12
- Release 12.2(18)SXF12:
  - Date of release: 19 Nov 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)SXF11
- Release 12.2(18)SXF11:
  - Date of release: 18 Sep 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)SXF10
- Release 12.2(18)SXF10a:
  - Date of release: 21 Sep 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)SXF10
- Release 12.2(18)SXF10:
  - Date of release: 16 Jul 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)SXF9
- Release 12.2(18)SXF9:
  - Date of release: 21 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)SXF8
- Release 12.2(18)SXF8:
  - Date of release: 07 Mar 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
- Release 12.2(18)SXF7:
  - Date of release: 30 Nov 2006

  - 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)SXF6
- Release 12.2(18)SXF6:
  - Date of release: 22 Sep 2006
  - 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)SXF5
- Release 12.2(18)SXF5:
  - Date of release: 10 Jul 2006
  - 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)SXF4
- Release 12.2(18)SXF4:
  - Date of release: 27 Mar 2006
  - 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)SXF3
- Release 12.2(18)SXF3:
  - Date of release: 16 Feb 2006
  - 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)SXF2
- Release 12.2(18)SXF2:
  - Date of release: 20 Jan 2006
  - 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)SXF1, Release 12.2(18)SXE4, Release 12.2(18)SXD7, and Release 12.2(17d)SXB11
- Release 12.2(18)SXF1:
  - Date of release: 22 Dec 2005
  - 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)SXF
- Release 12.2(18)SXF:
  - Date of release: 12 Sep 2005
  - 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)SXE3, Release 12.2(18)SXD6, and Release 12.2(17d)SXB10
- Release 12.2(18)SXE6b:
  - Date of release: 30 Jan 2007
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE6
- Release 12.2(18)SXE6a:
  - Date of release: 18 Sep 2006
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)

  - Rebuild based on Release 12.2(18)SXE6
- Release 12.2(18)SXE6:
  - Date of release: 08 Jun 2006
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE5
- Release 12.2(18)SXE5:
  - Date of release: 13 Feb 2006
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE4
- Release 12.2(18)SXE4:
  - Date of release: 10 Oct 2005
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE3
- Release 12.2(18)SXE3:
  - Date of release: 22 Aug 2005
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE2
- Release 12.2(18)SXE2:
  - Date of release: 23 Jun 2005
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE1
- Release 12.2(18)SXE1:
  - Date of release: 18 Apr 2005
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXE
- Release 12.2(18)SXE:
  - Date of release: 11 Apr 2005
  - 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)SXD4 and 12.2(17d)SXB7
- Release 12.2(18)SXD7b:
  - Date of release: 12 Dec 2006
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD7a
- Release 12.2(18)SXD7a:
  - Date of release: 15 Sep 2006
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD7

- Release 12.2(18)SXD7:
  - Date of release: 15 Dec 2005
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD6
- Release 12.2(18)SXD6:
  - Date of release: 22 Aug 2005
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD5
- Release 12.2(18)SXD5:
  - Date of release: 16 May 2005
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD4
- Release 12.2(18)SXD4:
  - Date of release: 24 Mar 2005
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD3
- Release 12.2(18)SXD3:
  - Date of release: 13 Dec 2004
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD2
- Release 12.2(18)SXD2:
  - Date of release: 22 Oct 2004
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD1
- Release 12.2(18)SXD1:
  - Date of release: 30 Sep 2004
  - Parent in Release 12.2S: 12.2(18)S (not all features in Release 12.2(18)S are supported)
  - Rebuild based on Release 12.2(18)SXD
- Release 12.2(18)SXD:
  - Date of release: 26 Jul 2004
  - 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(17d)SXB2

Note For information about Release 12.2(18)S, refer to these publications on Cisco.com:
http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guides_list.html

- Release 12.2(17d)SXB11a:
  - Date of release: 17 Apr 2006
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(17d)SXB11
- Release 12.2(17d)SXB11:
  - Date of release: 17 Nov 2005
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(17d)SXB10
- Release 12.2(17d)SXB10:
  - Date of release: 16 Aug 2005
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(17d)SXB9
- Release 12.2(17d)SXB9:
  - Date of release: 21 Jul 2005
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(17d)SXB8
- Release 12.2(17d)SXB8:
  - Date of release: 24 Apr 2005
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Rebuild based on Release 12.2(17d)SXB7
- Release 12.2(17d)SXB7:
  - Date of release: 01 Mar 2005
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Rebuild based on Release 12.2(17d)SXB6
- Release 12.2(17d)SXB6:
  - Date of release: 21 Dec 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Rebuild based on Release 12.2(17d)SXB5
- Release 12.2(17d)SXB5:
  - Date of release: 01 Nov 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Rebuild based on Release 12.2(17d)SXB4
- Release 12.2(17d)SXB4:
  - Date of release: 07 Sep 2004

  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Rebuild based on Release 12.2(17d)SXB3
- Release 12.2(17d)SXB3:
  - Date of release: 17 Aug 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Rebuild based on Release 12.2(17d)SXB2
- Release 12.2(17d)SXB2:
  - Date of release: 21 Jul 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Rebuild based on Release 12.2(17d)SXB1
- Release 12.2(17d)SXB1:
  - Date of release: 01 Jun 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Rebuild based on Release 12.2(17d)SXB and Release 12.2(17a)SX4
- Release 12.2(17d)SXB:
  - Date of release: 05 Mar 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17d)
  - Based on Release 12.2(17b)SXA and Release 12.2(17a)SX3

Note For information about Release 12.2(17d), refer to these publications on Cisco.com:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

- Release 12.2(17b)SXA2 (deferred):
  - Date of release: 22 Apr 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17b)
  - Rebuild based on Release 12.2(17b)SXA.
- Release 12.2(17b)SXA (deferred):
  - Date of release: 31 Dec 2003
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17b)
  - Based on Release 12.2(17a)SX1.

Note For information about Release 12.2(17b), refer to these publications on Cisco.com:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html

- Release 12.2(17a)SX4 (deferred):
  - Date of release: 23 Apr 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17a)
  - Rebuild based on Release 12.2(17a)SX3
- Release 12.2(17a)SX3 (deferred):
  - Date of release: 05 Mar 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17a)
  - Rebuild based on Release 12.2(17a)SX2
- Release 12.2(17a)SX2 (deferred):
  - Date of release: 29 Jan 2004
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17a)
  - Rebuild based on Release 12.2(17a)SX1
- Release 12.2(17a)SX1 (deferred):
  - Date of release: 30 Oct 2003
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17a)
  - Rebuild based on Release 12.2(17a)SX
- Release 12.2(17a)SX (deferred):
  - Date of release: 06 Oct 2003
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Includes all resolved caveats from Release 12.2(17a)
  - Based on Release 12.2(14)SX1.

Note

- For information about Release 12.2(17a), refer to these publications on Cisco.com:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html
- Release 12.2(14)SX2 (01 Jul 2003) only supports the MSFC3 and is for use with the Catalyst operating system on the Supervisor Engine 720. Release 12.2(14)SX2 has only MSFC3 images. Release 12.2(14)SX2 does not have any Supervisor Engine 720 images.

- Release 12.2(14)SX1 (deferred):
  - Date of release: 28 May 2003
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)
  - Rebuild based on Release 12.2(14)SX
- Release 12.2(14)SX (deferred):
  - Date of release: 14 Apr 2003
  - Parent in Release 12.2S: 12.2(14)S (not all features in Release 12.2(14)S are supported)

Note For information about Release 12.2(14)S, refer to these publications on Cisco.com:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guides_list.html

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 12.2SX, see the "Caveats" section on page 193 and refer to this publication:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_release_notes_list.html

For a list of the Release 12.2 S caveats that apply to Release 12.2SX, see the "Caveats" section on page 193 and refer to this publication:

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

FPD Image Packages

Note

- Field Programmable Device (FPD) image packages were first introduced on the Catalyst 6500 series switches and Cisco 7600 series routers in Release 12.2(18)SXE.
- 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

In Release 12.2(18)SXE and later releases, these modules use FPD images:

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

Note With Release 12.2(18)SXE2 and later releases, 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 Upgrades

Note With Release 12.2(18)SXE2 and later releases, 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/76fpd.html

Cisco IOS Software Modularity

These sections describe Cisco IOS Software Modularity:

- Cisco IOS Software Modularity Documentation, page 13
- Cisco IOS Software Modularity Unsupported Features, page 14

Note To use Cisco IOS Software Modularity images with 6700 series switching modules, ensure that the 6700 series switching modules have switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

Cisco IOS Software Modularity Documentation

See these publications for information about Cisco IOS Software Modularity:

- Cisco IOS Software Modularity Installation and Configuration:

  http://www.cisco.com/en/US/docs/ios/swmod/configuration/guide/sw_mod_instl_cfg.html

- Cisco IOS Software Modularity Command Reference:
  http://www.cisco.com/en/US/docs/ios/swmod/command/reference/sm_book.html
- Embedded Event Manager:
  http://www.cisco.com/en/US/docs/ios/12_2sx/sw_modularity/configuration/guide/evnt_mgr.html

Cisco IOS Software Modularity Unsupported Features

Cisco IOS Software Modularity does not support these features:

- Hardware:
  - All Optical Services Modules (OSMs)
  - With releases earlier than Release 12.2(18)SXF7, all SIPs and SPAs

Note In Release 12.2(18)SXF7 and later releases, Cisco IOS Software Modularity supports 7600-SIP-400 and 7600-SIP-200. 7600-SIP-600 remains unsupported.

  - 7600-SSC-400 Services SPA Carrier (SSC) and SPA-IPSEC-2G IPsec SPA
  - ACE10-6500-K9 Application Control Engine (ACE) module
  - CE20-MOD-K9 Application Control Engine (ACE) module
  - WS-SVC-ADM-1-K9 Traffic Anomaly Detector Module
  - WS-SVC-AGM-1-K9 Anomaly Guard Module
  - WS-SVC-AON-1-K9 Application-Oriented Networking (AON) Module
  - WS-SVC-CMM Communication Media Module
  - WS-SVC-CSG-1 Content Services Gateway (CSG) Module
  - WS-SVC-IPSEC-1 IPsec VPN Acceleration Services Module
  - WS-SVC-MWAM-1 Multi-Processor WAN Application Module
  - WS-SVC-PSD-1 Persistent Storage Device Module
  - WS-SVC-SSL-1 Secure Sockets Layer (SSL) Services Module
  - WS-SVC-WEBVPN-K9 WebVPN Services Module
  - WS-SVC-WLAN-1-K9 Wireless LAN service module
  - WS-X6066-SLB-S-K9 Content Switching Module with SSL (CSM-S)
  - In Release 12.2(18)SXF4, the WS-SVC-WISM-1-K9 Wireless Services Module (WiSM)

Note In Release 12.2(18)SXF5 and later releases, Cisco IOS Software Modularity supports the WS-SVC-WISM-1-K9 Wireless Services Module (WiSM).

- Software:

Note With releases Cisco IOS software modularity image earlier than Release 12.2(18)SXF8, to avoid a reload, do not enter any IP SLA **rtr** commands. This problem is resolved in Release 12.2(18)SXF8 by CSCek65370**.** (CSCek58966)

- See the *Cisco IOS Software Modularity Command Reference* "Introduction" for detailed information about specific commands that are not supported in Cisco IOS Software Modularity images.
- IPv6 and all IPv6-related features
- MPLS and all MPLS-related features
- Bidirectional Forwarding Detection (BFD), Integrated IS-IS support for BFD over IPv4, and OSPF support for BFD over IPv4
- Control Plane DSCP Support for RSVP
- IDSM-2 EtherChannel load balancing
- Integrated IS-IS Global Default Metric
- RSVP Scalability Enhancements
- In Release 12.2(18)SXF4, Multi-VRF (VRF Lite)

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 PFC3

The PFC3 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 VLAN-based QoS with DFC3s installed.
- 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.
- You can configure QoS policy maps attached to an EtherChannel formed from interfaces on different DFC-equipped switching modules.

General Limitations and Restrictions

This section describes general limitations and restrictions:

- CSCtc06097: VPNSM: %ACE-3-TRANSERR for more than 4 deny ACEs in a crypto ACL
- CSCse75774: Slow multicast traffic recovery for sup uplinks after switchover
- CSCsx32355:Policy base routing broken due to log keyword on outgoing interface
- CSCtb09290: Problem with accounting Giant packets at FW
- With a channelized T3 SPA that is configured for MLP, packets or fragments on a multilink interface with a differential delay that is larger than 70 ms are dropped, and the counters in the output of the **show ppp multilink** command are not updated. There is no workaround. Sequential fragments on different T1 links can be delayed only up to 70 ms. A delay of up to 100 ms is currently not supported, nor is accounting for fragments (good, reordered, or lost). (CSCef82225)
- With releases Cisco IOS software modularity image earlier than Release 12.2(18)SXF8, to avoid a reload, do not enter any IP SLA **rtr** commands. This problem is resolved in Release 12.2(18)SXF8 by CSCek65370. (CSCek58966)
- When a redundant supervisor engine is in standby mode, the Ethernet ports on the redundant supervisor engine are always active.

  Note With a Supervisor Engine 2 and Release 12.2(18)SXD1 and later releases, if all the installed switching modules have DFCs, enter the **fabric switching-mode allow dcef-only** command to disable the Ethernet ports on the redundant supervisor engine, which ensures that all modules are operating in dCEF mode. (CSCec05612)

- 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. Enter a **logging event link status** command on each interface where you want the messages enabled. (CSCeb06765)

- Do not configure WS-X6708-10GE switching module ports as VACL capture ports. (CSCsb59015)
- 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)
- A distributed EtherChannel (DEC) is an EtherChannel with ports on more than one DFC-equipped module or, on a DFC-equipped dual-fabric connection module, with ports that use different fabric connections.
- In truncated mode, the Supervisor Engine 720 does not support Layer 2 denial-of-service (DoS) protection rate limiters. (CSCeb36155)
- 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)
- In rare situations, if you do an online insertion and removal (OIR) of a FlexWAN module, a WS-X6516-GBIC switching module that does not have a DFC installed might reset. (CSCec29255)
- For packet sizes beginning with 84 bytes, and at each 8-byte increment (92 bytes, 100 bytes, etc.), some packet loss occurs with line-rate traffic ingressing and egressing on a WS-X6704-10GE with a WS-F6700-DFC3A. The loss for 84-byte packets is approximately 0.01 percent and increases up to 0.04 percent for larger traffic. (CSCee39455, CSCee94670)
- In releases where caveat CSCef78235 is resolved, with any Supervisor Engine 720 hardware revision, local SPAN and RSPAN source ports do not copy VACL-redirected traffic.

  In releases where caveat CSCef78235 is not resolved:

  – With WS-SUP720, hardware revision 3.2 or higher, local SPAN source ports do not copy VACL-redirected traffic.

  – With WS-SUP720 hardware revisions lower than 3.2, local SPAN source ports copy VACL-redirected traffic.

  – With any Supervisor Engine 720 hardware revision, RSPAN source ports copy VACL-redirected traffic.

  Enter the **show module version | include WS-SUP720-BASE** command to display the hardware revision. For example:

```
Router# show module version | include WS-SUP720-BASE
 7    2  WS-SUP720-BASE     SAD075301SZ Hw :3.2
```

- 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 PFC3, EoMPLS ports cannot be SPAN sources. (CSCed51245)
- Encryption in software on the MSFC is supported only for administrative connections (SSH) to Catalyst 6500 series switches and Cisco 7600 series routers. Software-based IPsec features are not supported.
- With a PFC2 or a PFC3, 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)
- The PFC2 supports a maximum of 1 Gateway Load Balancing Protocol (GLBP) group.
- The PFC2 supports a maximum of 16 unique Hot Standby Routing Protocol (HSRP) group numbers.
  - You can use the same HSRP group numbers in different VLANs (for example, use 1 as the first group number in each VLAN, use 2 for the second, etc.).
  - If you configure more than 16 HSRP groups, this restriction prevents use of the VLAN number as the HSRP group number.
- 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)
- In these releases:
  - 12.2(17a)SX and any later 12.2(17a)SX-based releases
  - 12.2(17b)SXA and any later 12.2(17b)SXA-based releases
  - 12.2(17d)SXB and any later 12.2(17d)SXB-based releases

  When you enter the **crypto key generate rsa modulus** *modulus_value* command the *modulus_value* parameter is ignored and a prompt appears for entry of a modulus value. Pressing Enter generates a key with the default value (512).

  Workaround: Reenter the modulus value at the prompt instead of accepting the default. (CSCed60483)
- With Release 12.2(17d)SXB6, to avoid a reload, enter the **no ip multicast vrf** *vrf_name* **cache-headers** command before you enter the **no ip vrf** *vrf_name* command for the same VRF. (CSCeg43304)
- 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/ios/ipv6/configuration/guide/ip6-addrg_bsc_con_iosswrel_TSD_Products_Feature_Guide.html

  (CSCed30692)
- The PFC3A and PFC3BXL incorrectly apply egress IP ACLs to MPLS-tagged traffic. (CSCed29392, CSCed16560)
- With an ingress policer, the PFC3BXL overpolices tunnel-decapsulated packets because of the tunnel-packet length. (CSCec71389)
- In PFC3BXL mode, 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)
- When a Supervisor Engine 720 bridges traffic between HSRP routers or Virtual Router Redundancy Protocol (VRRP) routers or GLBP routers that are providing redundancy to each other through switchports that are on different DFC-equipped modules or through switchports on both DFC-equipped modules and on non-DFC-equipped modules, HSRP or VRRP or GLBP switchover times for the routers might be proportional to the Layer 2 aging interval configured for the bridging VLAN on the Supervisor Engine 720.

  Workarounds:

  - Connect the HSRP or VRRP or GLBP routers to the Supervisor Engine 720 through switchports on the same DFC-equipped module.
  - Connect the HSRP or VRRP or GLBP routers to the Supervisor Engine 720 through switchports on non-DFC-equipped modules.
  - Reduce the Layer 2 aging time on the Supervisor Engine 720 VLAN to which the HSRP or VRRP or GLBP routers are connected.
  - Configure HSRP or VRRP or GLBP routers to use the BIA (Burned-In MAC Address) instead of virtual MAC.

  (CSCec27709)
- With a PFC3A, if there is an egress QoS policy on an interface, any ingress traffic on that interface that is dropped because of an RPF check failure or a FIB miss incorrectly increments the output policy QoS counters of that interface. (CSCeb01860)
- RPR and RPR+ do not synchronize configuration done through SNMP to the redundant supervisor engine. (CSCeb07866, CSCea72373)
- The PFC3A does not provide hardware-assisted NAT or PAT for hardware-switched traffic on interfaces where you have configured bidirectional PIM. (CSCea32737)
- If the MSFC address falls within the range of a PBR ACL, traffic addressed to the MSFC is policy routed in hardware instead of being forwarded to the MSFC. To prevent policy routing of traffic addressed to the MSFC, configure PBR ACLs to deny traffic addressed to the MSFC. (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 PFC3 does not apply egress policing to traffic that is being bridged to the MSFC3.
- The PFC3 does not apply egress policing or egress DSCP mutation to multicast traffic from the MSFC3.
- With a PFC3, PFC QoS does not rewrite the ToS byte in bridged multicast traffic.
- The MSFC3 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.
- The PFC3A does not support any PFC QoS features on tunnel interfaces. The PFC3BXL supports PFC QoS features on tunnel interfaces.
- When you configure NAT and NDE on an interface, the PFC3 sends all traffic in fragmented packets to the MSFC3 to be processed in software. (CSCdz51590)
- The PFC3BXL does not provide hardware switching for ICMP traffic if you configure NAT.
- The PFC3A does not provide hardware switching for ICMP traffic if you configure NAT or Cisco IOS reflexive ACLs.
- 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 MSFC for the Unicast RPF check. Packets permitted by the ACL are forwarded in hardware without a Unicast RPF check. (CSCdz35099)
- The PFC3 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.
- Enter the **copy running-config startup-config** command and the **redundancy reload peer** command to synchronize SNMP ifIndexes when RPR+ redundancy and SNMP ifIndex persistence are configured when all modules are online after any system boot or when you insert a module while the system is running. (CSCdy16763)
- RPR+ redundancy automatic startup configuration synchronization supports only the nvram:startup-config file. With RPR+ redundancy configured, if you enter a **boot config** command that does not specify nvram:startup-config as the startup configuration file, you must manually copy the startup configuration file to the redundant supervisor engine's device specified in the boot config command. (CSCdx25320)

- RPR+ redundancy does not support configuration entered in VLAN database mode. Use global configuration mode with RPR+ redundancy.
- 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 MSFC 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 MSFC 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 MSFC.
- 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.
- FlexWAN module interfaces support dNBAR. Do not configure NBAR or dNBAR on other interfaces.
- Ingress IP Packets with TTL=1 that are not addressed to the MSFC 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 MSFC 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 MSFC 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 MSFC 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 MSFC to be dropped, which generates ICMP-unreachable messages.

  To eliminate the load imposed on the MSFC 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 ip access-list** and **show ipv6 access-list** commands display statistics only for traffic that matches ACLs processed in software on the MSFC. The commands do 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 MSFC 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 MSFC, 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 MSFC, 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)
- With the tunnel MTU size configured to 9216 bytes, tunnel packets larger than 9211 bytes are corrupted.

  Workaround: None. (CSCec04627)
- A border router that is positioned between a protocol independent multicast (PIM) dense mode router and a PIM sparse mode router might not register some indirectly connected sources. This problem occurs for traffic that is on an ingress interface configured with the **ip pim dense-mode proxy-register** command.

  Workaround: Disable the multicast routing cache on the incoming interface. This action will cause packets to be process-switched in software on the MSFC instead of fast-switched. (CSCek39668)

FlexWAN Limitations and Restrictions

- 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 MSFC. (CSCdp34896)

- With a Cisco IOS Software Modularity image and a FlexWAN module that has serial port adapters installed, you might need to do a reload if a remote registry call is blocked. (CSCsg08736)

OSM Limitations and Restrictions

- In rare situations, with redundant supervisor engines, extra internal VLANs are allocated when you configure subinterfaces on OSMs. (CSCee27158)
- OSM WAN ports do not support SPAN or RSPAN.
- With 30,000 Virtual Private LAN Service (VPLS) VCs configured, OSM interfaces stop passing traffic if an RPR+ switchover occurs during a period of high CPU usage.

  Workaround: Enter **no power enable module** *slot_number* and **power enable module** *slot_number* commands for the OSMs. (CSCed17668)
- If you use the Class-Based Weighted Fair Queueing (CBWFQ) **shape average** command and apply the configured policy map to an interface on an OSM, traffic-shaping accuracy cannot be guaranteed if the target bit rate specified is less than 256,000 bits per second. (CSCea06515)
- The PFC QoS **police** command and the PXF-based **set** command are both used to set IP precedence. However, when you configure the **set ip prec** command for an OSM VPN path, the **mls qos** command is ignored. (CSCdw83517)
- The Gigabit Ethernet WAN ports on the OSM-4GE-WAN-GBIC and OSM-2+4GE-WAN+ switching modules do not support traffic in the native VLAN of an IEEE 802.1Q trunk. Do not configure a subinterface with the **encapsulation dot1q** *vlan_id* **native** command. (CSCdx60011)
- When you apply the first policy map or remove the last policy map from an interface on an OSM-1OC48-POS-SS,-SI, -SL module traffic through the interface may be disrupted and the routing protocol may go up and down. (CSCdx94033)
- The channelized OSMs are not supported in the MPLS core. They support IP traffic on customer edge (CE) and provider edge (PE) router links only.
- Unless you enter the **mls qos** command to enable PFC QoS, when you enable MPLS and enter the **random-detect** command in the output policy map on an interface, all OSM traffic through the interface is marked with DSCP 0. (CSCdw79863)
- The WAN ports on the Gigabit Ethernet WAN modules do not support Gigabit EtherChannels.
- If you enter an input **set** command to modify IP precedence for an IP-to-Tag path, the MPLS experimental bits will continue to be derived from the prior IP-precedence setting. In order to modify the experimental bits, use the **set mpls exp** command on the ingress interface. (CSCdw66785)
- On a system configured with a Supervisor Engine 720 and an OSM-1CHOC12/T1-SI, the output of the **show policy-map interface** command might display a packet counter of 0 for a serial interface. This problem occurs when packets have been process-switched in software on the MSFC instead of fast-switched, and then a reload occurs with one of these saved configurations:
  - When you enter these commands to configure an ACL:
    access-list *199* **permit ip any any log**
    interface *s1/1.1/1:0.2*
    ip access-group *199* **out**

– When you enter these commands to configure IP header-compression:
interface *Serial1/1.1/1:0*
encapsulation frame-relay
frame-relay ip tcp header-compression
service-policy output TEST

Workarounds:

– Enter the **no frame-relay ip tcp header-compression** command or the **no frame-relay ip rtp header-compression** command, and then reload the system.

– Avoid using the **log** keyword in an IP ACL with a QoS LLQ or a CBWFQ policy. If you use the **log** keyword, counters may stay at 0 in the output of the **show policy-map interface** command.

(CSCsg58652)

Service Module Limitations and Restrictions

- DHCP snooping does not work properly if DHCP packets to or from a WS-SVC-WLAN-1-K9 Wireless LAN Service Module cross a WAN link. (CSCef08877)

  Note In Release 12.2(18)SXD and rebuilds, DHCP snooping is supported only for use with a Wireless LAN Service Module.

- When you upgrade Cisco IOS software on the supervisor engine, and then you enter the Wireless Services Module (WiSM) module commands for the allowed VLANs, continous tracebacks might display on the active and the standby consoles:

  ```
  1d21h: %NETWORK_RF_API-STDBY-3-FAILDECODEDATADESC: Cannot decode data descriptor for
  an interface or controller because the sync header cannot be decoded, descriptor
  type=3000
  -Traceback= 40CCAAEC 40CCAC48 40CCAF58 403962E4 40394468 403950E0 40391514 4038C568
  ```

  (CSCse67713, CSCse53484)

- Generating an Rivest, Shamir, and Adelman (RSA) usage key pair with modulo 360 fails.

  Workaround: Use a higher modulo value. (CSCec49861)

- In rare situations, with a Supervisor Engine 720 and an IPsec VPN Acceleration services module (WS-SVC-IPSEC-1) configured with IPsec tunnels that use a loopback address as the crypto local endpoint, a reload occurs if there are established IPsec tunnels and you remove the loopback interface. (CSCef77289)

- With an EzVPN connection to a WS-SVC-IPSEC-1 module and XAUTH with a correct group password but an incorrect user password, an IKE SA is created on the WS-SVC-IPSEC-1 module that remains in CONF_XAUTH and cannot be cleared, which might deplete IKE resources if large volumes of these SAs. (CSCed25345)

- 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 IPsec VPN Acceleration services module (WS-SVC-IPSEC-1) or from the Firewall Services Module (WS-SVC-FWM-1-K9). (CSCec79733)

- After a distributed EtherChannel (DEC) has been configured and removed from the configuration, the show monitor command does not display any SPAN sessions that you configure for a service module.

  Workaround: Reset the service module to show the SPAN session. (CSCeh03911)

Troubleshooting

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

Note To attempt recovery from MSFC 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 **show vlan virtual-port** command displays the number of virtual interfaces.
- These maximum numbers of virtual interfaces are supported:

MST	RPVST+	PVST+
50,000 total 30,000 total with Release 12.2(17b)SXA (CSCed33864[1])	10,000 total	13,000 total
6,000[2] per switching module	1,800[2] per switching module	1,800[2] per switching module

1. CSCed33864 is resolved in Release 12.2(17d)SXB and later releases.
2. 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

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

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

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

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

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

Original SSLeay License:

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

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

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

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

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

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

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

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

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

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

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

Obtaining Documentation, 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.

Supported Hardware

These sections describe the hardware supported in Release 12.2SX:

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.

Flash Memory Device Summary

- **bootflash:** on the RP of all supervisor engines.
- **sup-bootdisk:** on these supervisor engines:
  - Supervisor Engine 720 with a CompactFlash adapter and CompactFlash card.
  - Supervisor Engine 32.
- **sup-bootflash:** on these supervisor engines:
  - Supervisor Engine 720 without a CompactFlash adapter and CompactFlash card.
  - Supervisor Engine 2.
- **disk0:** on these supervisor engines:
  - Supervisor Engine 720.
  - Supervisor Engine 32.
  - Supervisor Engine 2 with a PCMCIA Advanced Technology Attachment (ATA) FlashDisk device.
- **disk1:** on a Supervisor Engine 720.
- **slot0:** on a Supervisor Engine 2 without a PCMCIA Advanced Technology Attachment (ATA) FlashDisk device.

Supervisor Engines

Supervisor Engine 720 (CAT6000-SUP720/MSFC3, 7600-SUP720/MSFC3)

Supervisor Engine 720 Common Features

- Integrated 720-Gbps Switch Fabric
- 64-MB bootflash device or CompactFlash adapter with 512 MB CompactFlash card (WS-CF-UPG=):
  - 64-MB bootflash device (**sup-bootflash:**) supported in all releases
  - WS-CF-UPG= (**sup-bootdisk:**) supported in:

    —Release 12.2(18)SXE5 and later releases

    —Release 12.2(18)SXF and later releases
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_17277.html
- 2 CompactFlash Type II slots (disk0: and disk1:)

  Note Some Supervisor Engine 720 Release 12.2SX images are larger than the bootflash device and must be stored on a CompactFlash card (sup-bootdisk: or disk0: or disk1:).
- Two Ethernet uplink ports:
  - 1-MB packet buffer per port
  - Port 1—Gigabit Ethernet SFP
  - Port 2—Configurable as Gigabit Ethernet SFP or 10/100/1000 Mbps RJ-45
- QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t**
- Port grouping:
  - Number of ports: 2
  - Number of port groups: 1
  - Port ranges per port group: 1–2
- Supervisor Engine 720 requires a high-capacity fan tray (see the "Fan Trays" section on page 102)
- Supervisor Engine 720 requires a 2500W or higher power supply (see the "Power Supplies" section on page 103)

Supervisor Engine 720 with PFC3BXL

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SUP720-3BXL	7.82 A@42 V	Supervisor Engine 720 with PFC3BXL: • 1-GB DRAM • Policy Feature Card 3BXL (PFC3BXL; see the "Policy Feature Cards" section on page 41) • Multilayer Switch Feature Card 3 (MSFC3): – 1-GB DRAM – 64-MB bootflash	12.2(17b)SXA

Note

- There are no memory upgrade options for WS-SUP720-3BXL.
- If you install WS-SUP720-3BXL=, upgrade the memory on any DFC3-equipped switching modules. See this document for DFC3 memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html

Supervisor Engine 720 with PFC3B

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SUP720-3B	6.72 A@42 V	Supervisor Engine 720 with PFC3B: • 512-MB DRAM • Policy Feature Card 3B (PFC3B; see the "Policy Feature Cards" section on page 41) • Multilayer Switch Feature Card 3 (MSFC3): – 512-MB DRAM – 64-MB bootflash	12.2(17d)SXB1

Note

- See this document for DFC3 memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3.
  - If you install WS-F6K-PFC3BXL=, upgrade the memory on any DFC3-equipped switching modules.
  - See this publication for more information about WS-F6K-PFC3BXL=:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html
- You can upgrade the WS-SUP720-3B memory to 1-GB DRAM on the Supervisor Engine 720 and 1-GB DRAM on the MSFC3.
  - If you upgrade the memory, upgrade the Supervisor Engine 720, the MSFC3, and any DFC3-equipped switching modules.
  - See this document for Supervisor Engine 720 and MSFC3 memory upgrades:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/OL_20611.html

Supervisor Engine 720 with PFC3A

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SUP720	7.50 A@42 V	Supervisor Engine 720 with PFC3A: • 512-MB DRAM • Policy Feature Card 3A (PFC3A; see the "Policy Feature Cards" section on page 41) • Multilayer Switch Feature Card 3 (MSFC3): – 512-MB DRAM – 64-MB bootflash	12.2(14)SX

Note

- See this document for DFC3 memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720 with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3.
  - If you install WS-F6K-PFC3BXL=, upgrade the memory on any DFC3-equipped switching modules.
  - See this publication for more information about WS-F6K-PFC3BXL=:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html
- Except with WS-F6K-PFC3BXL=, do not upgrade the memory on WS-SUP720 or on the MSFC3 on WS-SUP720.

Supervisor Engine 32 (CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A)

These sections describe the Supervisor Engine 32:

- Supervisor Engine 32 Restrictions, page 38
- Supervisor Engine 32 Features, page 40

Supervisor Engine 32 Restrictions

- Supervisor Engine 32 requires a high-capacity fan tray (see the "Fan Trays" section on page 102).
- In some chassis, Supervisor Engine 32 requires a high-capacity power supply (see the "Power Supplies" section on page 103).
- Supervisor Engine 32 does not support this hardware:
  - 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)
  - 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-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

- Releases earlier than Release 12.2(18)SXF do not support Cisco IOS SLB with Supervisor Engine 32.
- Supervisor Engine 32 cannot support these software features and commands:
  - Egress multicast replication
  - Multicast replication mode detection
  - All fabric configuration commands

Supervisor Engine 32 Features

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SUP32-10GE-3B	2.39 A@42 V	Supervisor Engine 32: • One 10/100/1000 Mbps RJ-45 port • WS-SUP32-10GE—two 10-Gigabit Ethernet ports (requires XENPAKs) • WS-SUP32-GE—eight Gigabit Ethernet SFP ports (requires Gigabit Ethernet SFPs) • QoS port architecture (Rx/Tx): **2q8t/1p3q8t** • 256-MB DRAM with the "IP BASE SSH LAN ONLY" image (does not apply to the "IP BASE SSH LAN ONLY (MODULAR)" image) • 512-MB DRAM with all other images • 256-MB bootflash • Policy Feature Card 3B (PFC3B; see the "Policy Feature Cards" section on page 41) • Multilayer Switch Feature Card 2A (MSFC2A): – 256-MB DRAM with the "IP BASE SSH LAN ONLY" image (does not apply to the "IP BASE SSH LAN ONLY (MODULAR)" image) – 512-MB DRAM with all other images – 64-MB bootflash	12.2(18)SXF
WS-SUP32-GE-3B	1.89 A@42 V		

Note See this publication for Supervisor Engine 32 hardware information:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Module_Installation/Sup_Eng_Guide/supe_gd.html

Supervisor Engine 2 (CAT6000-SUP2/MSFC2, 7600-SUP2/MSFC2)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6K-S2U-MSFC2 **WS-X6K-S2-MSFC2**	3.46 A@42 V	Supervisor Engine 2 with Policy Feature Card 2 (PFC2): • ROMMON version 7.1(1) or later • 32-MB bootflash device • 256-MB DRAM (minimum) • dual-port 1000BASE-X GBIC uplinks • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Number of ports: 2 Number of port groups: 1 Port ranges per port group: 1–2 • Multilayer Switch Feature Card 2 (MSFC2) with 256-MB DRAM (minimum)	12.2(17d)SXB

Note

- Some Supervisor Engine 2 Release 12.2SX images are larger than the bootflash device. Supervisor Engine 2 ROMMON version 7.1(1) or later supports the MEM-C6K-ATA-1-64M= (64 MB) PCMCIA ATA FlashDisk device. See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_13488.html
- To use WS-X6K-S2-MSFC2 with 12.2SX releases, upgrade the memory.
  - MSFC2 DRAM—See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_6953.html
  - Supervisor Engine 2 DRAM—See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12693.html
  - Supervisor Engine 2 Bootflash—See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12667.html
- Supervisor Engine 2 supports all GBICs supported by Release 12.2(17d)SXB and later releases.

Policy Feature Cards

Policy Feature Card Guidelines and Restrictions

- A Supervisor Engine 2 always has a PFC2; there are no PFC options for Supervisor Engine 2.
- The PFC2 supports a theoretical maximum of 128 K MAC addresses (32 K MAC addresses recommended maximum).
- The PFC3 supports a theoretical maximum of 64 K MAC addresses (32 K MAC addresses recommended maximum).
- The PFC3 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 MSFC in software.

  The defaults for XL mode are:

  - IPv4 unicast and MPLS—512,000 routes
  - IPv4 multicast and IPv6 unicast and multicast—256,000 routes

  The defaults for Non-XL mode are:

  - IPv4 unicast and MPLS—192,000 routes
  - IPv4 multicast and IPv6 unicast and multicast—32,000 routes

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

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

  - XL mode:
    - IPv4 and MPLS—Up to 1,007,000 routes
    - IPv4 multicast and IPv6 unicast and multicast—Up to 503,000 routes
  - Non-XL mode:
    - IPv4 and MPLS—Up to 239,000 routes
    - IPv4 multicast and IPv6 unicast and multicast—Up to 119,000 routes

  Enter the 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.

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

- You cannot use one type of PFC3 (PFC3BXL, PFC3B, or PFC3A) on one supervisor engine and a different type on the other supervisor engine for redundancy. You must use identical policy feature cards for redundancy.
- With Release 12.2(17d)SXB and later releases, enter the **show platform hardware pfc mode** command to display the PFC3 mode.

- With Release 12.2(17b)SXA and Release 12.2(17b)SXA2, enter the **show platform earl-mode** command to display the PFC3 mode.
- PFC3A—These restrictions apply to a configuration with a PFC3A and these DFCs:
  - PFC3A and DFC3A—No restrictions (PFC3A mode).
  - PFC3A and DFC3B—The PFC3A restricts DFC3B functionality: the DFC3B functions as a DFC3A (PFC3A mode).
  - PFC3A and DFC3BXL—The PFC3A restricts DFC3BXL functionality: the DFC3BXL functions as a DFC3A (PFC3A mode).
  - PFC3A and DFC3C—The PFC3A restricts DFC3C functionality: the DFC3C functions as a DFC3A (PFC3A mode).
  - PFC3A and DFC3CXL—The PFC3A restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3A (PFC3A mode).
- PFC3B—These restrictions apply to a configuration with a PFC3B and these DFCs:
  - PFC3B and DFC3A—PFC3B functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3B functions as a PFC3A (PFC3A mode).
  - PFC3B and DFC3B—No restrictions (PFC3B mode).
  - PFC3B and DFC3BXL—The PFC3B restricts DFC3BXL functionality: after a reload with a DFC3BXL-equipped module installed, the DFC3BXL functions as a DFC3B (PFC3B mode).
  - PFC3B and DFC3C—The PFC3B restricts DFC3C functionality: the DFC3C functions as a DFC3B (PFC3B mode).
  - PFC3B and DFC3CXL—The PFC3B restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3B (PFC3B mode).
- PFC3BXL—These restrictions apply to a configuration with a PFC3BXL and these DFCs:
  - PFC3BXL and DFC3A—PFC3BXL functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3BXL functions as a PFC3A (PFC3A mode).
  - PFC3BXL and DFC3B—PFC3BXL functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3BXL functions as a PFC3B (PFC3B mode).
  - PFC3BXL and DFC3BXL—No restrictions (PFC3BXL mode).
  - PFC3BXL and DFC3C—Each restricts the functionality of the other: the PFC3BXL functions as a PFC3B and the DFC3C functions as a DFC3B (PFC3B mode).
  - PFC3BXL and DFC3CXL—The PFC3BXL restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3BXL (PFC3BXL mode).
- Summary of the PFC modes:
  - PFC3A mode—Operating mode with a PFC3A or any DFC3As
  - PFC3B mode—Operating mode with PFC3B and any DFC3Bs or DFC3BXLs
  - PFC3BXL mode—Operating mode with PFC3BXL and any DFC3BXLs
- The features that require the PFC3BXL or PFC3B are not supported in PFC3A mode.
- With a PFC3BXL or PFC3B and no DFC3A-equipped switching modules installed at bootup, any DFC3A-equipped switching module installed after bootup remain powered down.

- To use DFC3A-equipped switching modules with a PFC3BXL or PFC3B, the DFC3A-equipped switching modules must be installed at bootup.
- To use DFC3B-equipped switching modules with a PFC3BXL, the DFC3B-equipped switching modules must be installed at bootup.

Policy Feature Card 3BXL

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-PFC3BXL	2.57 A@42 V	Policy Feature Card 3BXL (PFC3BXL)	
		Supported only with Supervisor Engine 720	12.2(17b)SXA

Note

- There are no memory upgrade options for WS-F6K-PFC3BXL.
- Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720 or WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3. See this publication for more information:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

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 720	12.2(17d)SXB1
		With Supervisor Engine 32	12.2(18)SXF

Note

- There are no memory upgrade options for WS-F6K-PFC3B.
- Use WS-F6K-PFC3BXL= to upgrade a WS-SUP720-3B with a PFC3BXL. WS-F6K-PFC3BXL= includes 1 GB memory upgrades for the Supervisor Engine 720 and the MSFC3. See this publication for more information:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16220.html

Policy Feature Card 3A

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-PFC3A	2.25 A@42 V	Policy Feature Card 3A (PFC3A)	
		Supported only with Supervisor Engine 720	12.2(14)SX

Note

- There are no memory upgrade options for WS-F6K-PFC3A.
- WS-F6K-PFC3A is available only on WS-SUP720. It is not orderable.

Distributed and Centralized Forwarding Cards

Note See the "Policy Feature Cards" section on page 41 for Policy Feature Cards (PFC) and Distributed Forwarding Card (DFC) restrictions.

Distributed Forwarding Card 3CXL

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3CXL	2.35 A@42 V	Distributed Forwarding Card 3CXL (DFC3CXL) for use on CEF720 modules	
		Supported only with Supervisor Engine 720 and WS-X6708-10GE	12.2(18)SXF5

Distributed Forwarding Card 3C

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3C	1.65 A@42 V	Distributed Forwarding Card 3C (DFC3C) for use on CEF720 modules	
		Supported only with Supervisor Engine 720 and WS-X6708-10GE	12.2(18)SXF5

Distributed Forwarding Card 3BXL

WS-F6700-DFC3BXL

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3BXL	3.30 A@42 V	Distributed Forwarding Card 3BXL (DFC3BXL) for use on CEF720 modules	
		Supported only with Supervisor Engine 720	12.2(17d)SXB6

Note

- WS-F6700-DFC3BXL uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3BXL upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html

WS-F6K-DFC3BXL

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC3BXL	1.47 A@42 V	Distributed Forwarding Card 3BXL (DFC3BXL) for use on dCEF256 and CEF256 modules	
		Supported only with Supervisor Engine 720	12.2(18)SXD3

Note

- See this publication for information about WS-F6K-DFC3BXL memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Supervisor Engine 720 supports a WS-F6K-DFC3BXL on these WS-X6516-GBIC switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html

Distributed Forwarding Card 3B

WS-F6700-DFC3B

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3B	2.70 A@42 V	Distributed Forwarding Card 3B (DFC3B) for use on CEF720 modules	
		Supported only with Supervisor Engine 720	12.2(17d)SXB6

Note

- WS-F6700-DFC3B uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3B upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html

WS-F6K-DFC3B

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC3B	1.67 A@42 V	Distributed Forwarding Card 3B (DFC3B) for use on dCEF256 and CEF256 modules	
		Supported only with Supervisor Engine 720	12.2(18)SXD3

Note

- See this publication for information about WS-F6K-DFC3B memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Supervisor Engine 720 supports a WS-F6K-DFC3B on these WS-X6516-GBIC switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html

Distributed Forwarding Card 3A

WS-F6700-DFC3A

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-DFC3A	3.00 A@42 V	Distributed Forwarding Card 3A (DFC3A) for use on CEF720 modules	
		Supported only with Supervisor Engine 720	12.2(17a)SX

Note

- WS-F6700-DFC3A uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3A memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html

WS-F6K-DFC3A

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC3A	2.57 A@42 V	Distributed Forwarding Card 3A (DFC3A) for use on dCEF256 and CEF256 modules	
		Supported only with Supervisor Engine 720	12.2(14)SX

Note

- See this publication for information about WS-F6K-DFC3A memory upgrades:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html
- Supervisor Engine 720 supports a WS-F6K-DFC3A on these WS-X6516-GBIC switching module hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC switching module hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information about Supervisor Engine 720 and a DFC3 on WS-X6516-GBIC switching modules:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html

Distributed Forwarding Card (WS-F6K-DFC)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6K-DFC	2.10 A@42 V	Distributed Forwarding Card (DFC) for use on dCEF256 and CEF256 modules	
		Supported only with Supervisor Engine 2	12.2(17d)SXB
		Note Not supported in Release 12.2(18)SXE and Rebuilds	

Note

- Release 12.2(18)SXE does not support Supervisor Engine 2.
- WS-F6K-DFC requires a Switch Fabric Module.
- See this publication for information about WS-F6K-DFC memory upgrades:
  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_12409.html

Centralized Forwarding Card (WS-F6700-CFC)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-F6700-CFC	0.75 A@42 V	Centralized Forwarding Card (CFC) for use on CEF720 modules	
		Supported only with Supervisor Engine 720	12.2(17a)SX
Note There are no memory upgrade options for WS-F6700-CFC.			

Switch Fabric Modules

Note

- Switch fabric modules are supported only with Supervisor Engine 2.
- Except in 13-slot chassis, WS-X6500-SFM2 and WS-C6500-SFM can be used together to provide redundancy.
- 3-slot chassis do not support WS-X6500-SFM2 or WS-C6500-SFM.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6500-SFM2	3.09 A@42 V	Switch Fabric Module, version 2, to support dCEF256 modules	
		Supported only with Supervisor Engine 2	12.2(17d)SXB
Note WS-C6500-SFM2 supports all chassis except 3-slot chassis.			
WS-C6500-SFM	2.79 A@42 V	Switch Fabric Module to support dCEF256 modules	
		Supported only with Supervisor Engine 2	12.2(17d)SXB
Note WS-C6500-SFM does not support 13-slot chassis or 3-slot chassis.			

Transceivers

X2 Modules

Note WS-X6708-10GE does not support X2 modules shipped before the release of the WS-X6708-10GE switching module. The unsupported X2 modules are labeled with a number that ends with -01.

Product ID (append "=" for spares)	Product Description	Minimum Software Version
X2-10GB-LRM	10GBASE-LRM for FDDI-grade multimode fiber (MMF) **Note** Not supported by the **show idprom** command. (CSCsj35671)	12.2(18)SXF8
X2-10GB-CX4	10GBASE for CX4 (copper) cable	12.2(18)SXF5
X2-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(18)SXF5
X2-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(18)SXF5
X2-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	12.2(18)SXF5
X2-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	12.2(18)SXF5

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)SXF11
XENPAK-10GB-ZR	10GBASE for any SMF type	12.2(18)SXF
XENPAK-10GB-LW	10GBASE-LW XENPAK Module with WAN PHY for SMF	12.2(18)SXE
	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.	
DWDM-XENPAK	10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid	12.2(18)SXE
WDM-XENPAK-REC	10GBASE receive-only wavelength division multiplexing (WDM)	12.2(18)SXE
XENPAK-10GB-CX4	10GBASE for CX4 (copper) cable	12.2(17d)SXB1
XENPAK-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	12.2(17a)SX1
XENPAK-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	12.2(17a)SX1

Product ID (append "=" for spares)	Product Description	Minimum Software Version
XENPAK-10GB-ER+	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(17a)SX
XENPAK-10GB-ER	10GBASE-ER Serial 1550-nm extended-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(17a)SX
	Note Release 12.2(17d)SXB1 and later releases do not support XENPAK-10GB-ER units with Part No. 800-24557-01, as described in this external field notice (CSCee47030): http://www.cisco.com/en/US/ts/fn/200/fn29736.html	
XENPAK-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(17a)SX
XENPAK-10GB-LR+	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(17a)SX

Small Form-Factor Pluggable (SFP) Modules

These sections describe SFPs:

- Gigabit Ethernet SFPs, page 52
- Fast Ethernet SFPs, page 53

Gigabit Ethernet SFPs

Note See the "Unsupported Hardware" section on page 114 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)SXF8
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-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-5092	1000BASE-DWDM 1550.92 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-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-4373	1000BASE-DWDM 1543.73 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-4214	1000BASE-DWDM 1542.14 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-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-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-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	
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	12.2(18)SXE

Product ID (append "=" for spares)	Product Description	Minimum Software Version
GLC-BX-U	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength	12.2(18)SXE
GLC-ZX-SM	1000BASE-ZX SFP module	12.2(17d)SXB1
CWDM-SFP	1000BASE coarse wavelength-division multiplexing (CWDM) SFP module	12.2(17a)SX
GLC-T	1000BASE-T 10/100/1000 SFP module **Note** Supported only at 1000 Mbps in supervisor engines.	12.2(17a)SX
GLC-LH-SMD GLC-LH-SM	1000BASE-LX/LH SFP	12.2(17a)SX
GLC-SX-MMD GLC-SX-MM	1000BASE-SX SFP	12.2(14)SX

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)SXF2
GLC-FE-100BX-D	100BASE-BX10-D SFP	12.2(18)SXF2
GLC-FE-100EX	100BASEEX SFP	12.2(18)SXF
GLC-FE-100ZX	100BASEZX SFP	12.2(18)SXF
GLC-FE-100FX	100BASEFX SFP	12.2(18)SXF
GLC-FE-100LX	100BASELX SFP	12.2(18)SXF

Gigabit Interface Converters (GBICs)

Note The support listed in this section applies to all modules that use GBICs, including OSM LAN ports and OSM Gigabit Ethernet WAN ports, except as noted.

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WDM-GBIC-REC	Receive-only wavelength division multiplexing (WDM) GBIC	12.2(18)SXE
DWDM-GBIC	Dense wavelength division multiplexing (DWDM) GBIC	12.2(17a)SX

Product ID (append "=" for spares)	Product Description	Minimum Software Version
CWDM-GBIC-1470	Cisco 1000BASE-CWDM GBIC, 1470 nm (Gray)	12.2(17a)SX
CWDM-GBIC-1490	Cisco 1000BASE-CWDM GBIC, 1490 nm (Violet)	
CWDM-GBIC-1510	Cisco 1000BASE-CWDM GBIC, 1510 nm (Blue)	
CWDM-GBIC-1530	Cisco 1000BASE-CWDM GBIC, 1530 nm (Green)	
CWDM-GBIC-1550	Cisco 1000BASE-CWDM GBIC, 1550 nm (Yellow)	
CWDM-GBIC-1570	Cisco 1000BASE-CWDM GBIC, 1570 nm (Orange)	
CWDM-GBIC-1590	Cisco 1000BASE-CWDM GBIC, 1590 nm (Red)	
CWDM-GBIC-1610	Cisco 1000BASE-CWDM GBIC, 1610 nm (Brown)	
WS-G5483	1000BASET GBIC **Note** 1000BASET GBIC transceivers are not supported on OSM LAN ports and OSM Gigabit Ethernet WAN ports.	12.2(14)SX
WS-G5484	Short wavelength, 1000BASE-SX	12.2(14)SX
WS-G5486	Long wavelength/long haul, 1000BASE-LX/LH	12.2(14)SX
WS-G5487	Extended distance, 1000BASE-ZX	12.2(14)SX

10-Gigabit Ethernet Switching Modules

Product ID (append "=" for spares)	**Power Required**	**Product Description**	**Minimum Software Version**
WS-X6708-10G-3C (**WS-X6708-10GE** with WS-F6700-DFC3C)	10.58A @42 V	8-port 10-Gigabit Ethernet X2module • dCEF720 • Supports egress multicast replication • QoS port architecture (Rx/Tx): **8q4t/1p7q4t** • Dual switch-fabric connections Fabric Channel #1: Ports 2, 3, 6, 8 Fabric Channel #2: Ports 1, 4, 5, 7 • Number of ports: 8 Number of port groups: 8 Port ranges per port group: 1 port in each group	
WS-X6708-10G-3CXL (**WS-X6708-10GE** with WS-F6700-DFC3CXL**)**	11.28A @ 42V		
		Supported only with Supervisor Engine 720	12.2(18)SXF5

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

Note

- To use Cisco IOS Software Modularity images with 6700 series switching modules, ensure that the 6700 series switching modules have switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

- WS-X6708-10G-3C and WS-X6708-10G-3CXL are the orderable product IDs.
- The front panel is labeled WS-X6708-10GE.
- Cisco IOS software commands display WS-X6708-10GE with either WS-F6700-DFC3C or WS-F6700-DFC3CXL.
- To configure WS-X6708-10GE port oversubscription, refer to the **hw-module oversubscription** command in the command reference at this URL:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-f1.html#GUID-B5F8BEA0-B5DD-47BE-82F5-183765DF0F64

- In these chassis, operation of a WS-X6708-10GE switching module without over-temperature alarms is supported only with operating temperatures up to 40° C:
  - WS-C6513
  - CISCO7613
  - WS-C6509
  - WS-C6509-NEB
  - OSR-7609
  - WS-C6506
  - CISCO7606

  Full NEBS-compliance requires support for operating temperatures up to 55° C, which is available in all other chassis that support WS-X6708-10GE.

  Note All E-Series chassis provide NEBS compliance.

- Support in the WS-C6509-NEB-A chassis requires two FAN-MOD-09 modules.
- WS-X6708-10GE ports do not support VACL capture. (CSCsb59015)
- WS-X6708-10GE is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6708-10GE is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6708-10GE ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6708-10GE ports that interconnect network devices. (CSCsg86315)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6704-10GE	6.28 A@42 V	4-port 10-Gigabit Ethernet XENPAK • CEF720 with WS-F6700-CFC (adds 0.75 A@42 V) • dCEF720 with WS-F6700-DFC3BXL (adds 3.30 A@42 V) • dCEF720 with WS-F6700-DFC3B (adds 2.70 A@42 V) • dCEF720 with WS-F6700-DFC3A (adds 3.00 A@42 V) • Supports egress multicast replication • QoS port architecture (Rx/Tx): – With DFC3: **8q8t/1p7q8t** – With CFC: **1q8t/1p7q8t** • Dual switch-fabric connections Fabric Channel #1: Ports 3 and 4 Fabric Channel #2: Ports 1 and 2 • Number of ports: 4 Number of port groups: 4 Port ranges per port group: 1 port in each group	
		Supported only with Supervisor Engine 720	12.2(17a)SX

Note

- To use Cisco IOS Software Modularity images with 6700 series switching modules, ensure that the 6700 series switching modules have switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

- WS-X6704-10GE requires one of the following:
  - WS-F6700-DFC3BXL (3.30 A@42 V)
  - WS-F6700-DFC3B (2.70 A@42 V)
  - WS-F6700-DFC3A (3.00 A@42 V)
  - WS-F6700-CFC (0.75 A@42 V)
- WS-X6704-10GE ships with WS-F6700-CFC installed unless ordered with WS-F6700-DFC3BXL, WS-F6700-DFC3B, or WS-F6700-DFC3A.
- WS-X6704-10GE is supported in the WS-C6503-E chassis.
- WS-X6704-10GE is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6704-10GE is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6704-10GE ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6704-10GE ports that interconnect network devices. (CSCsg86315)

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 • With Supervisor Engine 720: – dCEF256 with WS-F6K-DFC3BXL (adds 1.47 A@42 V) – dCEF256 with WS-F6K-DFC3B (adds 1.67 A@42 V) – dCEF256 with WS-F6K-DFC3A (adds 2.57 A@42 V) • With Supervisor Engine 2, dCEF256 with WS-F6K-DFC (adds 2.10 A@42 V) • 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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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(14)SX
WS-G6483		10GBASE-ER serial 1550 nm extended-reach OIM	12.2(14)SX

Gigabit Ethernet Switching Modules

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6748-SFP	5.32 A@42 V	48-port Gigabit Ethernet SFP • CEF720 with WS-F6700-CFC (adds 0.75 A@42 V) • dCEF720 with WS-F6700-DFC3BXL (adds 3.30 A@42 V) • dCEF720 with WS-F6700-DFC3B (adds 2.70 A@42 V) • dCEF720 with WS-F6700-DFC3A (adds 3.00 A@42 V) • Supports egress multicast replication • QoS architecture: – With DFC3: **2q8t/1p3q8t** – With CFC: **1q8t/1p3q8t** • Dual switch-fabric connections Fabric Channel #1: Ports 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48 Fabric Channel #2: Ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47 • Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
		Supported only with Supervisor Engine 720	12.2(17d)SXB

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

Note

- To use Cisco IOS Software Modularity images with 6700 series switching modules, ensure that the 6700 series switching modules have switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

- WS-X6748-SFP requires one of the following:
  - WS-F6700-DFC3BXL (3.30 A@42 V)
  - WS-F6700-DFC3B (2.70 A@42 V)
  - WS-F6700-DFC3A (3.00 A@42 V)
  - WS-F6700-CFC (0.75 A@42 V)
- WS-X6748-SFP ships with WS-F6700-CFC installed unless ordered with WS-F6700-DFC3BXL, WS-F6700-DFC3B, or WS-F6700-DFC3A.
- WS-X6748-SFP is supported in the WS-C6503-E chassis.
- WS-X6748-SFP is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6748-SFP is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6748-SFP ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6748-SFP ports that interconnect network devices. (CSCsg86315)
- See the "Small Form-Factor Pluggable (SFP) Modules" section on page 51.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6724-SFP	2.23 A@42 V	24-port Gigabit Ethernet SFP • CEF720 with WS-F6700-CFC (adds 0.75 A@42 V) • dCEF720 with WS-F6700-DFC3BXL (adds 3.30 A@42 V) • dCEF720 with WS-F6700-DFC3B (adds 2.70 A@42 V) • dCEF720 with WS-F6700-DFC3A (adds 3.00 A@42 V) • Supports egress multicast replication • QoS architecture: – With DFC3: **2q8t/1p3q8t** – With CFC: **1q8t/1p3q8t** • Number of ports: 24 Number of port groups: 2 Port ranges per port group: 1–12, 13–24	
		Supported only with Supervisor Engine 720	12.2(17a)SX
		WS-X6724-SFP HW rev 2.3 or later (supported only with Supervisor Engine 720)	12.2(17d)SXB1

Note

- To use Cisco IOS Software Modularity images with 6700 series switching modules, ensure that the 6700 series switching modules have switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

- WS-X6724-SFP requires one of the following:
  - WS-F6700-DFC3BXL (3.30 A@42 V)
  - WS-F6700-DFC3B (2.70 A@42 V)
  - WS-F6700-DFC3A (3.00 A@42 V)
  - WS-F6700-CFC (0.75 A@42 V)
- WS-X6724-SFP ships with WS-F6700-CFC installed unless ordered with WS-F6700-DFC3BXL, WS-F6700-DFC3B, or WS-F6700-DFC3A.
- WS-X6724-SFP is supported in the WS-C6503-E chassis.
- WS-X6724-SFP is not supported in the WS-C6503 and CISCO7603 chassis.
- WS-X6724-SFP is supported in all slots of a 13-slot chassis.
- On WS-X6724-SFP ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6724-SFP ports that interconnect network devices. (CSCsg86315)
- See the "Small Form-Factor Pluggable (SFP) Modules" section on page 51.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6816-GBIC		16-port Gigabit Ethernet GBIC • dCEF256 • QoS port architecture (Rx/Tx): **1p1q4t/1p2q2t** • Dual switch-fabric connections Fabric Channel #1: Ports 1–8 Fabric Channel #2: Ports 9–16 • Number of ports: 16 Number of port groups: 2 Port ranges per port group: 1–8, 9–16	
	3.84 A@42 V	With Supervisor Engine 720	12.2(14)SX
	5.94 A@42 V	With Supervisor Engine 2	12.2(17d)SXB

Note

- WS-X6816-GBIC requires one of these for use with Supervisor Engine 720:
  - WS-F6K-DFC3BXL (adds 1.47 A@42 V)
  - WS-F6K-DFC3B (adds 1.67 A@42 V)
  - WS-F6K-DFC3A (adds 2.57 A@42 V)
- WS-X6816-GBIC requires WS-F6K-DFC for use with Supervisor Engine 2.
- In a 13-slot chassis, WS-X6816-GBIC is supported only in slots 9 through 13 and does not power up in other slots.

WS-X6516A-GBIC	3.62 A@42 V	16-port Gigabit Ethernet GBIC • CEF256 • With Supervisor Engine 720: – dCEF256 with WS-F6K-DFC3BXL (adds 1.47 A@42 V) – dCEF256 with WS-F6K-DFC3B (adds 1.67 A@42 V) – dCEF256 with WS-F6K-DFC3A (adds 2.57 A@42 V) • With Supervisor Engine 2, dCEF256 with WS-F6K-DFC (adds 2.10 A@42 V) • 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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6516-GBIC	3.40 A@42 V	16-port Gigabit Ethernet GBIC • CEF256 • With Supervisor Engine 720: – dCEF256 with WS-F6K-DFC3BXL (adds 1.47 A@42 V) – dCEF256 with WS-F6K-DFC3B (adds 1.67 A@42 V) – dCEF256 with WS-F6K-DFC3A (adds 2.57 A@42 V) • With Supervisor Engine 2, dCEF256 with WS-F6K-DFC (adds 2.10 A@42 V) • 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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Note

- Supervisor Engine 720 supports a DFC3 on these WS-X6516-GBIC hardware revisions:
  - Lower than 5.0
  - 5.5 and higher
- Supervisor Engine 720 does not support a DFC3 on WS-X6516-GBIC hardware revisions 5.0 through 5.4. With a Supervisor Engine 720 and with a DFC3 installed, WS-X6516-GBIC hardware revisions 5.0 through 5.4 do not power up.
- With a Supervisor Engine 720 but without a DFC3, WS-X6516-GBIC hardware revisions 5.0 through 5.4 operate in bus mode.
- See external field notice 24494 for more information:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html

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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Note

- Caveat CSCec65943 prevents support of the WS-X6408-GBIC switching module in Release 12.2(17a)SX.
- Caveat CSCec65943 is resolved in Release 12.2(17a)SX1 and later releases.

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 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(18)SXF2
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-RJ-45V (replace with WS-X6148-45AF-UG=). • WS-X6148-RJ-21 or WS-X6148-RJ-21V (replace with WS-X6148-21AF-UG=).	
		With Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-F6K-VPWR-GE	0.42 A@42 V	PoE daughtercard for WS-X6548-GE-TX and WS-X6148-GE-TX	
		With Supervisor Engine 720	12.2(17a)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

10/100/1000 Ethernet Switching Modules

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6748-GE-TX	7.00 A@42 V	48-port 10/100/1000 RJ-45 • CEF720 with WS-F6700-CFC (adds 0.75 A@42 V) • dCEF720 with WS-F6700-DFC3BXL (adds 3.30 A@42 V) • dCEF720 with WS-F6700-DFC3B (adds 2.70 A@42 V) • dCEF720 with WS-F6700-DFC3A (adds 3.00 A@42 V) • Supports egress multicast replication • QoS architecture: – With DFC3: **2q8t/1p3q8t** – With CFC: **1q8t/1p3q8t** • Dual switch-fabric connections Fabric Channel #1: Ports 25–48 Fabric Channel #2: Ports 1–24 • Number of ports: 48 Number of port groups: 4 Port ranges per port group: 1–12, 13–24, 25–36, 37–48	
		Supported only with Supervisor Engine 720	12.2(17a)SX

Note

- To use Cisco IOS Software Modularity images with 6700 series switching modules, ensure that the 6700 series switching modules have switching module ROMMON version 12.2(18r)S1 or later. To display the switching module ROMMON version, enter the **remote command module** *module_slot_number* **show version | include ROM** command. To upgrade the switching module ROMMON, see this document:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/rommon/OL_6143.html

- WS-X6748-GE-TX requires one of the following:
  - WS-F6700-DFC3BXL (3.30 A@42 V)
  - WS-F6700-DFC3B (2.70 A@42 V)
  - WS-F6700-DFC3A (3.00 A@42 V)
  - WS-F6700-CFC (0.75 A@42 V)
- WS-X6748-GE-TX ships with WS-F6700-CFC installed unless ordered with WS-F6700-DFC3BXL, WS-F6700-DFC3B, or WS-F6700-DFC3A.
- WS-X6748-GE-TX is supported in the WS-C6503-E chassis.
- WS-X6748-GE-TX is not supported in the WS-C6503 and CISCO7603 chassis.
- In a 13-slot chassis, WS-X6748-GE-TX is supported only in slots 9 through 13 and does not power up in other slots.
- On WS-X6748-GE-TX ports, STP BPDUs are not exempt from Traffic Storm Control multicast suppression. Do not configure multicast suppression on STP-protected WS-X6748-GE-TX ports that interconnect network devices. (CSCsg86315)

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 • 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 • The aggregate bandwidth of each set of 8 ports (1–8, 9–16, 17–24, 25–32, 33–40, and 41–48) is 1 Gbps.	
WS-X6548V-GE-TX	3.40 A@42 V		
WS-X6548-GE-45AF	3.16 A@42 V		
		With Supervisor Engine 720 (except WS-F6K-GE48-AF or WS-F6K-48-AF)	12.2(17a)SX
		WS-F6K-GE48-AF or WS-F6K-48-AF with Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		WS-F6K-GE48-AF or WS-F6K-48-AF with Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
		WS-F6K-GE48-AF or WS-F6K-48-AF with Supervisor Engine 2	12.2(17d)SXB

Note

- Release 12.2(17b)SXA and later releases provide support for more than 1 Gbps of traffic per EtherChannel on the WS-X6548-GE-TX (and voice-power daughtercard equipped) switching modules.
- WS-X6548-GE-TX and WS-X6548V-GE-TX do not support these features:
  - With Release 12.2(17a)SX and Release 12.2(17a)SX1, more than 1 Gbps of traffic per EtherChannel
  - DFCs
  - ISL trunking
  - Jumbo frames
  - 802.1Q tunneling
  - Traffic storm control

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
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 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(18)SXF2

Note WS-X6148A-GE-TX and WS-X6148A-GE-45AF do not support these features:

- WS-F6K-DFC3A, WS-F6K-DFC3B, or WS-F6K-DFC3BXL
- 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 • 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 • The aggregate bandwidth of each set of 8 ports (1–8, 9–16, 17–24, 25–32, 33–40, and 41–48) is 1 Gbps.	
WS-X6148V-GE-TX	2.89 A@42 V		
WS-X6148-GE-45AF	2.65 A@42 V		
		With Supervisor Engine 720 (except WS-F6K-GE48-AF or WS-F6K-48-AF)	12.2(17a)SX
		WS-F6K-GE48-AF or WS-F6K-48-AF with Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		WS-F6K-GE48-AF or WS-F6K-48-AF with Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
		WS-F6K-GE48-AF or WS-F6K-48-AF with Supervisor Engine 2	12.2(17d)SXB

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
- WS-F6K-DFC3A, WS-F6K-DFC3B, or WS-F6K-DFC3BXL
- ISL trunking
- Jumbo frames
- 802.1Q tunneling
- Traffic storm control

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6516-GE-TX	3.45 A@42 V	16-port 10/100/1000BASE-T • CEF256 • With Supervisor Engine 720: – dCEF256 with WS-F6K-DFC3BXL (adds 1.47 A@42 V) – dCEF256 with WS-F6K-DFC3B (adds 1.67 A@42 V) – dCEF256 with WS-F6K-DFC3A (adds 2.57 A@42 V) • With Supervisor Engine 2, dCEF256 with WS-F6K-DFC (adds 2.10 A@42 V) • 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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

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 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(18)SXF2

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6524-100FX-MM	1.90 A@42 V	24-port 100FX Ethernet multimode • CEF256 • With Supervisor Engine 720: – dCEF256 with WS-F6K-DFC3BXL (adds 1.47 A@42 V) – dCEF256 with WS-F6K-DFC3B (adds 1.67 A@42 V) – dCEF256 with WS-F6K-DFC3A (adds 2.57 A@42 V) • With Supervisor Engine 2, dCEF256 with WS-F6K-DFC (adds 2.10 A@42 V) • 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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6324-100FX-SM	1.52 A@42 V	24-port 100FX Ethernet	
WS-X6324-100FX-MM	1.52 A@42 V	• 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	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

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 • With Supervisor Engine 720: – dCEF256 with WS-F6K-DFC3BXL (adds 1.47 A@42 V) – dCEF256 with WS-F6K-DFC3B (adds 1.67 A@42 V) – dCEF256 with WS-F6K-DFC3A (adds 2.57 A@42 V) • With Supervisor Engine 2, dCEF256 with WS-F6K-DFC (adds 2.10 A@42 V) • 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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6548-RJ-21	2.90 A@42 V	48-port 10/100TX RJ-21 • CEF256 • With Supervisor Engine 720: – dCEF256 with WS-F6K-DFC3BXL (adds 1.47 A@42 V) – dCEF256 with WS-F6K-DFC3B (adds 1.67 A@42 V) – dCEF256 with WS-F6K-DFC3A (adds 2.57 A@42 V) • With Supervisor Engine 2, dCEF256 with WS-F6K-DFC (adds 2.10 A@42 V) • 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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6148X2-RJ-45	2.65 A@42 V	96-port 10/100TX RJ-45	
WS-X6148X2-45AF	3.07 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 720	12.2(18)SXF3
		With Supervisor Engine 32	12.2(18)SXF3
		With Supervisor Engine 2	12.2(18)SXF3
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 720	12.2(18)SXF3
		With Supervisor Engine 32	12.2(18)SXF3
		With Supervisor Engine 2	12.2(18)SXF3
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-X6148A-RJ-45	1.00 A@42 V	48-port 10/100TX RJ-45	
WS-X6148A-45AF	2.57 A@42 V	• 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 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(18)SXF2

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-RJ-45V 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 720 (except with WS-F6K-48-AF)	12.2(14)SX
		WS-F6K-48-AF with Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		WS-F6K-48-AF with Supervisor Engine 32	
		With Supervisor Engine 2	12.2(17d)SXB
		WS-F6K-48-AF with Supervisor Engine 2	
WS-X6148-RJ-21	2.39 A@42 V	48-port 10/100TX RJ-21	
WS-X6148-RJ21V	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 720 (except with WS-F6K-48-AF)	12.2(14)SX
		WS-F6K-48-AF with Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
		WS-F6K-48-AF with Supervisor Engine 32	
		With Supervisor Engine 2	12.2(17d)SXB
		WS-F6K-48-AF with Supervisor Engine 2	

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 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Optical Services Modules (OSMs)

OSM Guidelines and Restrictions

- Cisco IOS Software modularity does not support OSMs.
- Supervisor Engine 32 does not support OSMs.
- With Release 12.2(18)SXD and later releases, OSMs require a minimum of 128 MB of dynamic random-access memory (SDRAM)—See this publication for memory upgrade procedures:

  http://www.cisco.com/en/US/docs/routers/7600/Hardware/Module_and_Line_Card_Installation_Guides/7600_Series_Router_Module_Installation_Guide/osmodule.html
- OSMs are CEF256 modules.
- OSM WAN port numbering starts with 1.
- On OSMs with Gigabit Ethernet GBIC Layer 2 LAN ports:
  - OSM LAN port numbering starts with 1.
  - The LAN ports are in a single port group.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-WLAN-1-K9 has not been tested with OSMs.

- The OSM-2+4GE-WAN+ and the OC-12 Packet-over-SONET OSMs have been tested with the service modules and WS-SUP720.
- In releases earlier than Release 12.2(18)SXD1, except for the OSM-2+4GE-WAN+ and the OC-12 Packet-over-SONET OSMs, the following service modules have not been tested with other OSMs:
  - WS-X6066-SLB-APC content switching module (CSM)
  - WS-SVC-IDSM2-K9 intrusion detection system module
  - WS-SVC-NAM-2 and WS-SVC-NAM-1 network analysis modules (NAMs)
  - WS-SVC-SSL-1 SSL services module

Gigabit Ethernet WAN

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-4GE-WAN-GBIC	3.59 A@42 V	4-port Gigabit Ethernet WAN (GBIC); CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-2+4GE-WAN+	5.08 A@42 V	4-port Gigabit Ethernet WAN (GBIC) with two Layer 2 LAN ports; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

OC-48 Packet over SONET

Note Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-1OC48-POS-SS **OSM-1OC48-POS-SI** **OSM-1OC48-POS-SL**	4.25 A@42 V	1-port OC-48/STM-16 SONET/SDH OSM, SM-SR; CEF256 1-port OC-48/STM-16 SONET/SDH OSM, SM-IR; CEF256 1-port OC-48/STM-16 SONET/SDH OSM, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-1OC48-POS-SI+ **OSM-1OC48-POS-SL+** **OSM-1OC48-POS-SS+**	3.90 A@42 V	Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-IR; CEF256 Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-LR; CEF256 Enhanced 1-port OC-48/STM-16 SONET/SDH OSM, SM-SR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

OC-48 DPT/Packet over SONET

Note Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-2OC48/1DPT-SS **OSM-2OC48/1DPT-SI** **OSM-2OC48/1DPT-SL**	5.75 A@42 V	2-port OC-48 DPT/POS, SM-SR; CEF256 2-port OC-48 DPT/POS, SM-IR; CEF256 2-port OC-48 DPT/POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

OC-12 Packet over SONET

Note Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-4OC12-POS-MM **OSM-4OC12-POS-SI** **OSM-4OC12-POS-SL**	4.78 A@42 V	4-port OC-12c/STM-4c POS, MM; CEF256 4-port OC-12c/STM-4c POS, SM-IR; CEF256 4-port OC-12c/STM-4c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-4OC12-POS-SI+	4.55 A@42 V	Enhanced 4-port OC-12c/STM-4c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-2OC12-POS-MM+ **OSM-2OC12-POS-MM** **OSM-2OC12-POS-SI** **OSM-2OC12-POS-SL**	3.36 A@42 V	2-port OC-12c/STM-4c POS, MM; CEF256 2-port OC-12c/STM-4c POS, MM; CEF256 2-port OC-12c/STM-4c POS, SM-IR; CEF256 2-port OC-12c/STM-4c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-2OC12-POS-SI+	3.36 A@42 V	Enhanced 2-port OC-12c/STM-4c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

OC-3 Packet over SONET

Note Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-16OC3-POS-MM **OSM-16OC3-POS-SI** **OSM-16OC3-POS-SL**	5.09 A@42 V	16-port OC-3c/STM-1c POS, MM; CEF256 16-port OC-3c/STM-1c POS, SM-IR; CEF256 16-port OC-3c/STM-1c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-16OC3-POS-SI+	4.80 A@42 V	Enhanced 16-port OC-3c/STM-1c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-8OC3-POS-MM **OSM-8OC3-POS-SI** **OSM-8OC3-POS-SL**	3.57 A@42 V	8-port OC-3c/STM-1c POS, MM; CEF256 8-port OC-3c/STM-1c POS, SM-IR; CEF256 8-port OC-3c/STM-1c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-8OC3-POS-SI+ **OSM-8OC3-POS-SL+**	3.57 A@42 V	Enhanced 8-port OC-3c/STM-1c POS, SM-IR; CEF256 Enhanced 8-port OC-3c/STM-1c POS, SM-LR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-4OC3-POS-SI	2.44 A@42 V	4-port OC-3c/STM-1c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-4OC3-POS-SI+	2.44 A@42 V	Enhanced 4-port OC-3c/STM-1c POS, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

OC-12 Channelized

Note Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-1CHOC12/T3-SI **OSM-1CHOC12/T1-SI**	4.40 A@42 V 2.80 A@42 V	1-port channelized OC-12, SM-IR; CEF256 1-port channelized OC-12, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

CT3/T1 Channelized/Unchannelized

Note OSM-12CT3/T1 has mini-SMB connectors for use with 75-Ohm copper coax cable.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-12CT3/T1	2.80 A@42 V	12-port channelized/unchannelized CT3/T1; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

OC-12 ATM

Note Also has four Layer 2 LAN ports.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
OSM-2OC12-ATM-MM **OSM-2OC12-ATM-SI**	3.62 A@42 V	2-port OC-12/STM-4 ATM OSM, MM; CEF256 2-port OC-12/STM-4 ATM OSM, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
OSM-2OC12-ATM-MM+ **OSM-2OC12-ATM-SI+**	4.00 A@42 V	Enhanced 2-port OC-12/STM-4 ATM OSM, MM; CEF256 Enhanced 2-port OC-12/STM-4 ATM OSM, SM-IR; CEF256	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB

Shared Port Adapter (SPA) Interface Processors (SIPs)

Note

- See the "FPD Image Packages" section on page 12 for information about additional procedures required to support SIPs with Release 12.2(18)SXE and later releases.
- 7600-SIP-400 and 7600-SIP-600 are not supported in PFC3A mode.
- With releases earlier than Release 12.2(18)SXF7, Cisco IOS Software modularity does not support SIPs.
- In Release 12.2(18)SXF7 and later releases, Cisco IOS Software Modularity supports 7600-SIP-400 and 7600-SIP-200.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
7600-SIP-600	8.14 A@42 V	SPA Interface Processor-600 (not supported in PFC3A mode) **Note** 7600-SIP-600 has a WS-F6700-DFC3BXL.	
		Supported only with Supervisor Engine 720	12.2(18)SXF

Note

- Supervisor Engine 32 does not support 7600-SIP-600.
- 7600-SIP-600 is not supported when a 7600-SSC-400 and SPA-IPSEC-2G are installed.
- 7600-SIP-600 is not supported in Release 12.2(33)SXH and rebuilds.

7600-SIP-400	6.31 A@42 V	SPA Interface Processor-400 (not supported in PFC3A mode)	
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 32	12.2(18)SXF
7600-SIP-200	5.72 A@42 V	SPA Interface Processor-200	
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 32	12.2(18)SXF

Shared Port Adapters (SPAs)

These sections describe SPAs:

Note

- With releases earlier than Release 12.2(18)SXF7, Cisco IOS Software modularity does not support SIPs.
- In Release 12.2(18)SXF7 and later releases, Cisco IOS Software Modularity supports 7600-SIP-400 and 7600-SIP-200.

Ethernet SPAs

These sections describe Ethernet SPAs:

- 10-Gigabit Ethernet SPAs, page 86
- Gigabit Ethernet SPAs, page 86

10-Gigabit Ethernet SPAs

Product ID (append "=" for spares)	SIP Support	Product Description	Minimum Software Version
SPA-1XTENGE-XFP	7600-SIP-600	1-port 10-Gigabit Ethernet SPA, LANPHY XFP Optics	12.2(18)SXF
XFP Modules Supported in SPA-1XTENGE-XFP			
XFP-10GLR-OC192LR	10-Gigabit Ethernet LR (10 km)		

Gigabit Ethernet SPAs

Product ID (append "=" for spares)	SIP Support	Product Description	Minimum Software Version
SPA-10X1GE	7600-SIP-600	10-port Gigabit Ethernet SPA, SFP Optics	12.2(18)SXF
SPA-5X1GE	7600-SIP-600	5-port Gigabit Ethernet SPA, SFP Optics	12.2(18)SXF
SPA-2X1GE	7600-SIP-400	2-port Gigabit Ethernet SPA, SFP Optics	12.2(18)SXF
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)SXF10
SPA-OC192POS-VSR	7600-SIP-600	1-port OC-192c/STM-64 POS/RPR SPA, VSR-1	12.2(18)SXF2

Product ID (append "=" for spares)	SIP Support	Product Description	Minimum Software Version
SPA-2XOC3-POS	7600-SIP-200 7600-SIP-400	2-port OC-3c/STM-1c POS SPA **Note** Requires SFPs.	12.2(18)SXE
SPA-4XOC3-POS	7600-SIP-200 7600-SIP-400	4-port OC-3c/STM-1c POS SPA **Note** Requires SFPs.	12.2(18)SXE
SPA-1XOC12-POS	7600-SIP-400	1-port OC-12c/STM-4c POS SPA **Note** Requires an SFP.	12.2(18)SXE
SPA-OC192POS-LR	7600-SIP-600	1-port OC-192c/STM-64 POS/RPR SPA, SM-LR	12.2(18)SXF
SPA-OC192POS-XFP	7600-SIP-600	1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics	12.2(18)SXF
		XFP Modules Supported in SPA-OC192POS-XFP	
		XFP-10GLR-OC192SR Single-Mode (SM) Short Reach (SR)	
		XFP-10GER-OC192IR Single-Mode (SM) Intermediate Reach (IR-2)	
SPA-OC192POS-VSR	7600-SIP-600	1-port OC-192c/STM-64 POS/RPR SPA, VSR-1	12.2(18)SXF1

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)SXE
SPA-4XOC3-ATM	7600-SIP-200 7600-SIP-400	4-port OC-3c/STM-1c ATM SPA **Note** Requires SFPs.	12.2(18)SXE
SPA-1XOC12-ATM	7600-SIP-400	1-Port OC-12c/STM-4c ATM SPA **Note** Requires an SFP.	12.2(18)SXE
SPA-1XOC48-ATM	7600-SIP-400	1 port OC-48c/STM-16 ATM SPA	12.2(18)SXF

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)SXE
SPA-2XT3/E3	7600-SIP-200	2-port Clear Channel T3/E3 SPA	12.2(18)SXE
SPA-4XT3/E3	7600-SIP-200	4-port Clear Channel T3/E3 SPA	12.2(18)SXE
SPA-2XCT3/DS0	7600-SIP-200	2-port Channelized T3 to DS0 SPA	12.2(18)SXE
SPA-4XCT3/DS0	7600-SIP-200	4-port Channelized T3 to DS0 SPA	12.2(18)SXE

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 720	12.2(18)SXE2
		With Supervisor Engine 32	12.2(18)SXF2

Note

- 7600-SSC-400 does not maintain state when an NSF with SSO redundancy mode switchover occurs.
- 7600-SSC-400 is not supported when a 7600-SIP-600 is installed.

Services SPAs

Note See the "FPD Image Packages" section on page 12 for information about additional procedures required to support SPA-IPSEC-2G with Release 12.2(18)SXE and later releases.

Product ID (append "=" for spares)	Carrier	Product Description	Minimum Software Version
SPA-IPSEC-2G	7600-SSC-400	IPsec SPA	12.2(18)SXE2
Note SPA-IPSEC-2G does not support TACACS+ authentication for IPsec. (CSCee33200)			

FlexWAN and Enhanced FlexWAN Modules

Note

- In releases earlier than Release 12.2(18)SXD1, WS-SVC-WLAN-1-K9 has not been tested with the FlexWAN or Enhanced FlexWAN modules.
- The following service modules have not been tested with the Enhanced FlexWAN module and Release 12.2(17b)SXA, Release 12.2(17b)SXA2, or Release 12.2(17d)SXB:
  - WS-X6066-SLB-APC content switching module (CSM)
  - WS-SVC-IDSM2-K9 intrusion detection system module
  - WS-SVC-NAM-2 and WS-SVC-NAM-1 network analysis modules (NAMs)
  - WS-SVC-SSL-1 SSL services module

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 720	12.2(17b)SXA
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
Note See the "FPD Image Packages" section on page 12 for information about additional procedures required to support WS-X6582-2PA with Release 12.2(18)SXE and later releases.			
WS-X6182-2PA	2.38 A@42 V	FlexWAN Module	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 2	12.2(17d)SXB

Note

- Support for WS-X6182-2PA was unintentionally disabled in Release 12.2(18)SXF7 Cisco IOS Software modularity images. (CSCsg97079)
- Supervisor Engine 32 does not support WS-X6182-2PA.

FlexWAN and Enhanced FlexWAN Module Port Adapters

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PA-2FE	2-port Fast Ethernet Port Adapter (supported only in WS-X6582-2PA)	12.2(18)SXE
PA-1FE	1-port Fast Ethernet Port Adapter (supported only in WS-X6582-2PA)	12.2(18)SXE
PA-POS-1OC3	1-port Packet over SONET OC3c/STM1 Port Adapter	12.2(18)SXE
PA-POS-2OC3	2-port POS OC3c/STM1	12.2(17b)SXA
SFPs for PA-POS-2OC3		
SFP-OC3-MM	Short range, multimode fiber	12.2(17b)SXA
SFP-OC3-IR1	Intermediate range, single-mode fiber	12.2(17b)SXA
SFP-OC3-LR1	Long range, single-mode fiber	12.2(17b)SXA
PA-POS-OC3MM **PA-POS-OC3SMI** **PA-POS-OC3SML**	Packet over SONET (OC-3)	12.2(14)SX
PA-A6-OC3MM	1-port ATM OC-3c/STM-1 multimode port adapter, enhanced	12.2(14)SX
PA-A6-OC3SMI	1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced	12.2(14)SX
PA-A6-OC3SML	1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced	12.2(14)SX
PA-A6-T3	1-port ATM DS3 port adapter, enhanced	12.2(14)SX
PA-A6-E3	1-port ATM E3 port adapter, enhanced	12.2(14)SX
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.	12.2(14)SX
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(14)SX
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	12.2(14)SX
PA-4E1G/75 **PA-4E1G/120**	T1/E1	12.2(17)SX

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PA-MC-8TE1+	Multichannel T1/E1 8PRI **Note** This port adapter does not support ISDN PRI when installed in the FlexWAN module.	12.2(14)SX
PA-H **PA-2H**	HSSI	12.2(14)SX
PA-MC-STM-1	Multichannel STM-1	12.2(14)SX

Service Modules

Note

- For any service modules that runs its own software, see the service module software release notes for information about the minimum required service module software version.
- With SPAN configured to include a port-channel interface to support a service module, be aware of CSCth03423 and CSCsx46323.

Application Control Engine (ACE) Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Versions
ACE10-6500-K9 **ACE20-MOD-K9**	5.23 A@42 V	Application Control Engine (ACE) module	
		With Supervisor Engine 720	12.2(18)SXF4

The ACE module runs its own software—See these publications:

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

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

Note

- Cisco IOS Software modularity does not support ACE10-6500-K9 or ACE20-MOD-K9.
- Supervisor Engine 32 does not support ACE10-6500-K9 or ACE20-MOD-K9.
- Supervisor Engine 2 does not support ACE10-6500-K9 or ACE20-MOD-K9.

Wireless Services Module (WiSM)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Versions
WS-SVC-WISM-1-K9	6.07 A@42 V	Wireless Services Module (WiSM)	
		With Supervisor Engine 720	12.2(18)SXF2

WS-SVC-WISM-1-K9 runs its own software—See these publications:

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

See the WS-SVC-WISM-1-K9 software release notes for information about the minimum required WS-SVC-WISM-1-K9 software version.

Note

- In Release 12.2(18)SXF4, Cisco IOS Software modularity does not support WS-SVC-WISM-1-K9.
- In Release 12.2(18)SXF5 and later releases, Cisco IOS Software modularity supports WS-SVC-WISM-1-K9.
- Supervisor Engine 32 does not support WS-SVC-WISM-1-K9.
- Supervisor Engine 2 does not support WS-SVC-WISM-1-K9.
- In a 13-slot chassis, WS-SVC-WISM-1-K9 is supported only in slots 9 through 13 and does not power up in other slots.

Application-Oriented Networking Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Versions
WS-SVC-AON-1-K9	4.00 A@42 V	Application-Oriented Networking (AON) Module	
		With Supervisor Engine 720	12.2(18)SXE1

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Versions
WS-SVC-AON-1-K9 runs its own software—See these publications: http://www.cisco.com/en/US/products/ps6480/prod_release_notes_list.html See the WS-SVC-AON-1-K9 software release notes for information about the minimum required WS-SVC-AON-1-K9 software version.			

Note

- Cisco IOS Software modularity does not support WS-SVC-AON-1-K9.
- Supervisor Engine 32 does not support WS-SVC-AON-1-K9.
- Supervisor Engine 2 does not support WS-SVC-AON-1-K9.

WebVPN Services Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Versions
WS-SVC-WEBVPN-K9	2.94 A@42 V	WebVPN Services Module	
		With Supervisor Engine 720	12.2(18)SXE2 12.2(17d)SXB7
		With Supervisor Engine 32	12.2(18)SXF
WS-SVC-WEBVPN-K9 runs its own software—See these publications: http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html#anchor24 See the WS-SVC-WEBVPN-K software release notes for information about the minimum required WS-SVC-WEBVPN-K software version.			

Note

- Cisco IOS Software modularity does not support WS-SVC-WEBVPN-K9.
- Supervisor Engine 2 does not support WS-SVC-WEBVPN-K9.

Anomaly Guard Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-AGM-1-K9	4.00 A@42 V	Anomaly Guard Module	
		With Supervisor Engine 720	12.2(18)SXD3
		With Supervisor Engine 2	12.2(18)SXD3

WS-SVC-AGM-1-K9 runs its own software—See these publications:

http://www.cisco.com/en/US/products/ps6236/tsd_products_support_model_home.html

See the WS-SVC-AGM-1-K9 software release notes for information about the minimum required WS-SVC-AGM-1-K9 software version.

Note

- Cisco IOS Software modularity does not support WS-SVC-AGM-1-K9.
- Supervisor Engine 32 does not support WS-SVC-AGM-1-K9.
- In Release 12.2(18)SXD3 and rebuilds, WS-SVC-AGM-1-K9 has not been tested with OSMs or FlexWAN modules.

Traffic Anomaly Detector Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-ADM-1-K9	4.00 A@42 V	Traffic Anomaly Detector Module	
		With Supervisor Engine 720	12.2(18)SXD3
		With Supervisor Engine 2	12.2(18)SXD3

WS-SVC-ADM-1-K9 runs its own software—See these publications:

http://www.cisco.com/en/US/products/ps6236/tsd_products_support_model_home.html

See the WS-SVC-ADM-1-K9 software release notes for information about the minimum required WS-SVC-ADM-1-K9 software version.

Note

- Cisco IOS Software modularity does not support WS-SVC-ADM-1-K9.
- Supervisor Engine 32 does not support WS-SVC-ADM-1-K9.
- In Release 12.2(18)SXD3 and rebuilds, WS-SVC-ADM-1-K9 has not been tested with OSMs or FlexWAN modules.

Wireless LAN Service Module (WLSM)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-WLAN-1-K9	3.10 A@42 V	Wireless LAN service module	
		With Supervisor Engine 720	12.2(18)SXD

WS-SVC-WLAN-1-K9 runs its own software—See these publications:

http://www.cisco.com/en/US/products/ps5865/tsd_products_support_eol_model_home.html

See the WS-SVC-WLAN-1-K9 software release notes for information about the minimum required WS-SVC-WLAN-1-K9 software version.

Note

- Cisco IOS Software modularity does not support WS-SVC-WLAN-1-K9.
- Supervisor Engine 32 does not support WS-SVC-WLAN-1-K9.
- Supervisor Engine 2 does not support WS-SVC-WLAN-1-K9.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-WLAN-1-K9 has not been tested with OSMs or FlexWAN modules.

Persistent Storage Device (PSD) Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-PSD-1	4.00 A@42 V	Persistent Storage Device Module	
		With Supervisor Engine 720	12.2(18)SXD1
		With Supervisor Engine 32	12.2(18)SXF7
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-PSD-1 runs its own software—See these publications:

http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html#anchor21

See the WS-SVC-PSD-1 software release notes for information about the minimum required WS-SVC-PSD-1 software version.

Note

- Cisco IOS Software modularity does not support WS-SVC-PSD-1.
- With Release 12.2(18)SXD1 and later, WS-SVC-PSD-1 maintains state when an NSF with SSO redundancy mode switchover occurs.

Multi-Processor WAN Application Module (MWAM)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-MWAM-1	3.57 A@42 V	Multi-Processor WAN Application Module	
		With Supervisor Engine 720	12.2(18)SXD1
		With Supervisor Engine 32	12.2(18)SXF5
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-MWAM-1 runs its own software—See these publications:

http://www.cisco.com/en/US/docs/wireless/pdsn/12.28zb/mwan_install_config/mwamhwrn.html

See the WS-SVC-MWAM-1 software release notes for information about the minimum required WS-SVC-MWAM-1 software version.

Note

- Cisco IOS Software modularity does not support WS-SVC-MWAM-1.
- With Release 12.2(18)SXD1 and later releases, WS-SVC-MWAM-1 maintains state when an NSF with SSO redundancy mode switchover occurs.
- With Releases earlier than Release 12.2(18)SXD1, WS-SVC-MWAM-1 does not maintain state when an NSF with SSO redundancy mode switchover occurs.

Content Services Gateway (CSG) Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-CSG-1	3.00 A@42 V	Content Services Gateway (CSG) Module	
		With Supervisor Engine 720	12.2(18)SXD1
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-CSG-1 runs its own software—See these publications:

http://www.cisco.com/en/US/products/sw/wirelssw/ps779/tsd_products_support_series_home.html

See the WS-SVC-CSG-1 software release notes for information about the minimum required WS-SVC-CSG-1 software version.

Note

- Cisco IOS Software modularity does not support WS-SVC-CSG-1.
- Supervisor Engine 32 does not support WS-SVC-CSG-1.

Communication Media Module (CMM)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-CMM	6.00 A@42 V	Communication Media Module	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB
WS-SVC-CMM runs its own software—See these publications: http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/cmm/release/notes/OL_4847.html See the WS-SVC-CMM software release notes for information about the minimum required WS-SVC-CMM software version.			
Note Cisco IOS Software modularity does not support WS-SVC-CMM.			
Communication Media Module Port Adapters			
WS-SVC-CMM-6E1		6-Port E1 Interface Port Adapter	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 2	12.2(17d)SXB
WS-SVC-CMM-6T1		6-Port T1 Interface Port Adapter	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 2	12.2(17d)SXB
WS-SVC-CMM-ACT		Adhoc Conferencing and Transcoding Port Adapter	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 2	12.2(17d)SXB
WS-SVC-CMM-24FXS		24-Port FXS Interface Port Adapter	
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 2	12.2(17d)SXB

IPsec VPN Acceleration Services Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-IPSEC-1	1.89 A@42 V	IPsec VPN Acceleration Services Module	
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 2	12.2(17d)SXB
WS-SVC-IPSEC-1 uses the Cisco IOS software that is running on the switch.			

Note

- Cisco IOS Software modularity does not support WS-SVC-IPSEC-1.
- Supervisor Engine 32 does not support WS-SVC-IPSEC-1.
- With Release 12.2(18)SXE and later releases, WS-SVC-IPSEC-1 requires an advanced services image (see the "Feature Sets" section on page 115).
- With releases earlier than Release 12.2(18)SXE, WS-SVC-IPSEC-1 requires a k9 image (see the "Feature Sets" section on page 115).
- WS-SVC-IPSEC-1 does not support TACACS+ authentication for IPsec. (CSCee33200)
- WS-SVC-IPSEC-1 does not maintain state when an NSF with SSO redundancy mode switchover occurs.
- WS-SVC-IPSEC-1 does not maintain state when a single router mode with stateful switchover (SRM with SSO) redundancy mode switchover occurs.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-IPSEC-1 has not been tested with OSM-1CHOC12/T1-SI or OSM-12CT3/T1.
- To avoid reloads with software releases where caveat CSCed17605 is not resolved (CSCed17605 is resolved in Release 12.2(17d)SXB and later releases), do not configure the single router mode with stateful switchover (SRM with SSO) redundancy mode with a WS-SVC-IPSEC-1 module installed. In software releases where caveat CSCed17605 is not resolved, the WS-SVC-IPSEC-1 module does not maintain state when an SRM with SSO redundancy mode switchover occurs.

Content Switching Module with SSL (CSM-S)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6066-SLB-S-K9	2.15 A@42 V	Content Switching Module with SSL (CSM-S)	
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 2	12.2(18)SXD

WS-X6066-SLB-S-K9 runs its own software—See these publications:

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/tsd_products_support_model_home.html

See the WS-X6066-SLB-S-K9 software release notes for information about the minimum required WS-X6066-SLB-S-K9 software version.

Note

- Cisco IOS Software modularity does not support WS-X6066-SLB-S-K9.
- Supervisor Engine 32 does not support WS-X6066-SLB-S-K9.
- With Release 12.2(18)SXD1 and later releases, WS-X6066-SLB-S-K9 maintains state when an NSF with SSO redundancy mode switchover occurs.
- WS-X6066-SLB-S-K9 does not maintain state when a single router mode with stateful switchover (SRM with SSO) redundancy mode switchover occurs.
- The OSM-2+4GE-WAN+ and the OC-12 Packet-over-SONET OSMs have been tested with the WS-X6066-SLB-S-K9 content switching module.
- In releases earlier than Release 12.2(18)SXD1, the WS-X6066-SLB-S-K9 content switching module has not been tested with other OSMs or the Enhanced FlexWAN module.

Content Switching Module (CSM)

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6066-SLB-APC	3.00 A@42 V	Content Switching Module	
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 2	12.2(17d)SXB

WS-X6066-SLB-APC runs its own software—See these publications:

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/tsd_products_support_model_home.html

See the WS-X6066-SLB-APC software release notes for information about the minimum required WS-X6066-SLB-APC software version.

Note

- Supervisor Engine 32 does not support WS-X6066-SLB-APC.
- With Release 12.2(18)SXD1 and later releases, WS-X6066-SLB-APC maintains state when an NSF with SSO redundancy mode switchover occurs.
- WS-X6066-SLB-APC does not maintain state when a single router mode with stateful switchover (SRM with SSO) redundancy mode switchover occurs.
- The OSM-2+4GE-WAN+ and the OC-12 Packet-over-SONET OSMs have been tested with the WS-X6066-SLB-APC content switching module and WS-SUP720.
- In releases earlier than Release 12.2(18)SXD1, WS-X6066-SLB-APC has not been tested with other OSMs or the Enhanced FlexWAN module.

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 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

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 Release 12.2(18)SXD3 and later Cisco IOS releases and 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.
- WS-SVC-FWM-1-K9 does not maintain state when a single router mode with stateful switchover (SRM 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 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

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

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

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

Note

- WS-SVC-IDSM2-K9 has been tested with OSM-2+4GE-WAN+ and the OC-12 Packet-over-SONET OSMs.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-IDSM2-K9 has not been tested with other OSMs or the Enhanced FlexWAN module.

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 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

WS-SVC-NAM-2 and WS-SVC-NAM-1 run their own software—See this publication for more information:

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/tsd_products_support_model_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.

Note

- With Release 12.2(17b)SXA and rebuilds and Release 12.2(17d)SXB and rebuilds, WS-SVC-NAM-2 and WS-SVC-NAM-1 support single router mode with stateful switchover (SRM with SSO) redundancy mode.
- WS-SVC-NAM-2 and WS-SVC-NAM-1 have been tested with OSM-2+4GE-WAN+ and the OC-12 Packet-over-SONET OSMs.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-NAM-2 and WS-SVC-NAM-1 have not been tested with other OSMs or the Enhanced FlexWAN module.

Secure Sockets Layer (SSL) Services Module

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-SSL-1	2.94 A@42 V	Secure Sockets Layer (SSL) Services Module	
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF
		With Supervisor Engine 2	12.2(17d)SXB

Note

- Cisco IOS Software modularity does not support WS-SVC-SSL-1.
- WS-SVC-SSL-1 does not maintain state when an NSF with SSO redundancy mode switchover occurs.
- WS-SVC-SSL-1 does not maintain state when a single router mode with stateful switchover (SRM with SSO) redundancy mode switchover occurs.
- WS-SVC-SSL-1 has been tested with OSM-2+4GE-WAN+ and the OC-12 Packet-over-SONET OSMs.
- In releases earlier than Release 12.2(18)SXD1, WS-SVC-SSL-1 has not been tested with other OSMs or the Enhanced FlexWAN module.

Fan Trays

- High-Capacity Fan Trays, page 103
- Standard-Capacity Fan Trays, page 103

Note

- Enter the **show environment status | include fan** command or the **show environment cooling** command to display information about the installed fan trays.
- To use a high-capacity fan tray with a Supervisor Engine 2, you must enter the **hw-module fan-tray version 2** command and then remove and quickly reinsert the fan tray.

High-Capacity Fan Trays

These high-capacity fan trays support both all supervisor engines and 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(14)SX
	Note In releases earlier than Release 12.2(18)SXD, WS-C6503-E-FAN requires the same power as FAN-MOD-3HS.		
FAN-MOD-3HS	2.98 A@42 V	High-capacity fan tray for WS-C6503 and CISCO7603 chassis	12.2(14)SX
FAN-MOD-6HS	4.29 A@42 V	High-capacity fan tray for CISCO7606 chassis	12.2(14)SX
WS-C6506-E-FAN	2.35 A@42 V	High-capacity fan tray for WS-C6506-E chassis	12.2(14)SX
WS-C6K-6SLOT-FAN2	12 V fan	High-capacity fan tray for WS-C6506 chassis	12.2(14)SX
FAN-MOD-09	5.75 A@42 V	High-capacity fan tray for WS-C6509-NEB-A and CISCO7609 chassis	12.2(14)SX
WS-C6509-V-E-FAN	5.75 A@42 V	High-capacity fan tray for WS-C6509-V-E chassis	12.2(18)SXF10
WS-C6509-E-FAN	3.58 A@42 V	High-capacity fan tray for WS-C6509-E chassis	12.2(14)SX
WS-C6K-9SLOT-FAN2	12 V fan	High-capacity fan tray for WS-C6509 chassis	12.2(14)SX
WS-C6K-13SLT-FAN2	7.10 A@42 V	High-capacity fan tray for WS-C6513 and CISCO7613 chassis	12.2(14)SX

Standard-Capacity Fan Trays

These standard-capacity fan trays support only Supervisor Engine 2.

Product ID (append "=" for spares)	Power Allocated at 42 V	Product Description	Minimum Software Version
FAN-MOD-3	None	Standard-capacity fan tray for WS-C6503 and CISCO7603 chassis	12.2(17d)SXB
FAN-MOD-6	None	Standard-capacity fan tray for CISCO7606 chassis	12.2(17d)SXB
WS-C6K-6SLOT-FAN	12 V fan	Standard-capacity fan tray for WS-C6506 chassis	12.2(17d)SXB
WS-C6509-NEB-FAN	12 V fan	Standard fan tray for WS-C6509-NEB chassis	12.2(17d)SXB
WS-C6K-9SLOT-FAN	12 V fan	Standard-capacity fan tray for WS-C6509 chassis	12.2(17d)SXB
WS-C6K-13SLT-FAN	12 V fan	Standard-capacity fan tray for WS-C6513 and CISCO7613 chassis	12.2(17d)SXB

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)SXE
PWR-2700-DC	2700 W DC power supply	12.2(18)SXE

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)SXE
PWR-2700-DC/4	2700 W DC power supply	12.2(18)SXE

WS-C6503, WS-C6503-E, and CISCO7603 Power Supplies

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PWR-1400-AC	1,400 W AC power supply	12.2(17a)SX
PWR-950-AC	950 W AC power supply	12.2(14)SX
PWR-950-DC	950 W DC power supply	12.2(14)SX

All Other Power Supplies

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

- Catalyst 6503
- Catalyst 6503-E
- CISCO7603
- Catalyst 6504-E
- CISCO7604

Product ID (append "=" for spares)	Product Description	Minimum Software Version
WS-CAC-8700W-E	8,700 W AC power supply	12.2(18)SXF8
	Note • Limited to 6,000 W in the WS-C6513 and CISCO7613 chassis. • 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	
PWR-6000-DC	6,000 W DC power supply	12.2(18)SXF13
	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-6000W	6,000 W AC power supply	12.2(18)SXD
	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 • With releases earlier than Release 12.2(18)SXD, limited to 4,000 W in the WS-C6506-E and WS-C6509-E chassis.	

Product ID (append "=" for spares)	Product Description	Minimum Software Version
PWR-4000-DC	4,000 W DC power supply	12.2(14)SX
WS-CAC-4000W	4,000 W AC power supply	12.2(14)SX
+WS-CAC-3000W	3,000 W AC power supply	12.2(17a)SX
	Note • Required with Supervisor Engine 720 in WS-C6509-NEB or OSR7609 chassis. • Included in the WS-6509-NEB-UPGRD= upgrade kit.	
WS-CAC-3000W	3,000 W AC power supply	12.2(14)SX
WS-CAC-2500W	2,500 W AC power supply	12.2(14)SX
WS-CDC-2500W	2,500 W DC power supply	12.2(14)SX

Chassis

13-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6513-E	Catalyst 6513-E chassis: • 13 slots • 64 chassis MAC addresses • Does not support these modules: – Supervisor Engine 2 – WS-C6500-SFM • These modules are supported only in slots 9 through 13 and do not power up in other slots: – WS-X6700 series switching modules except WS-X6724-SFP – WS-X6816-GBIC switching modules – WS-SVC-WISM-1-K9	
	With Supervisor Engine 720	12.2(18)SXF14
	With Supervisor Engine 32	12.2(18)SXF14

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6513	Catalyst 6513 chassis: • 13 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720 requires WS-C6K-13SLT-FAN2 • Does not support WS-C6500-SFM • These modules are supported only in slots 9 through 13 and do not power up in other slots: – WS-X6708-10GE – WS-X6704-10GE – WS-X6748-SFP – WS-X6748-GE-TX – WS-X6816-GBIC – WS-SVC-WISM-1-K9	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
CISCO7613	Cisco 7613 chassis: • 13 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720 requires WS-C6K-13SLT-FAN2 • Does not support WS-C6500-SFM • These modules are supported only in slots 9 through 13 and do not power up in other slots: – WS-X6708-10GE – WS-X6704-10GE – WS-X6748-SFP – WS-X6816-GBIC – WS-X6748-GE-TX – WS-SVC-WISM-1-K9	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

9-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6509-V-E	Catalyst 6509-V-E chassis: • 9 vertical slots • 64 chassis MAC addresses • Requires WS-C6509-V-E-FAN • Required power supply: – 2,500 W DC or higher – 3,000 W AC or higher • Supervisor Engine 2 is not supported in WS-C6509-V-E.	
	With Supervisor Engine 720	12.2(18)SXF10
	With Supervisor Engine 32	12.2(18)SXF10
WS-C6509-E	Catalyst 6509-E chassis: • 9 horizontal slots • Chassis MAC addresses: – Before April 2009—1024 chassis MAC addresses – Starting in April 2009—64 chassis MAC addresses **Note** Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.** • Requires WS-C6509-E-FAN • Requires 2,500 W or higher power supply • With releases earlier than Release 12.2(18)SXD, WS-CAC-6000W is limited to 4,000 W in WS-C6509-E	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append "=" for spare)	Product Description	Minimum Software Version
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 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
WS-C6509-NEB	Catalyst 6509-NEB chassis: • 9 vertical slots • 1024 chassis MAC addresses • Use with Supervisor Engine 720 or Supervisor Engine 32 requires the WS-6509-NEB-UPGRD= upgrade kit—refer to this publication: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16162.html	
	With Supervisor Engine 720	12.2(17a)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
CISCO7609	Cisco 7609 chassis • 9 vertical slots • 64 chassis MAC addresses • No fan tray upgrade required for use with Supervisor Engine 720	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append "=" for spare)	Product Description	Minimum Software Version
OSR-7609	Cisco 7609 chassis: • 9 vertical slots • 1024 chassis MAC addresses • Use with Supervisor Engine 720 or Supervisor Engine 32 requires the WS-6509-NEB-UPGRD= upgrade kit—refer to this publication: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_16162.html	
	With Supervisor Engine 720	12.2(17a)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

6-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6506-E	Catalyst 6506-E chassis: • 6 slots • Chassis MAC addresses: – Before April 2009—1024 chassis MAC addresses – Starting in April 2009—64 chassis MAC addresses **Note** Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. **Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology.** • Requires WS-C6506-E-FAN • Requires 2,500 W or higher power supply • With releases earlier than Release 12.2(18)SXD, WS-CAC-6000W is limited to 4,000 W in WS-C6506-E	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append "=" for spare)	Product Description	Minimum Software Version
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 limited to 4,000 W in WS-C6506	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
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 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

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 • Does not support: – Supervisor Engine 2 – WS-X6500-SFM2 – WS-C6500-SFM – WS-F6K-DFC	
	With Supervisor Engine 720	12.2(18)SXE
	With Supervisor Engine 32	12.2(18)SXF

Product ID (append "=" for spare)	Product Description	Minimum Software Version
CISCO7604	Cisco 7604 chassis: • 4 slots • 64 chassis MAC addresses • Does not support: – Supervisor Engine 2 – WS-X6500-SFM2 – WS-C6500-SFM – WS-F6K-DFC	
	With Supervisor Engine 720:	12.2(18)SXE
	With Supervisor Engine 32	12.2(18)SXF

3-Slot Chassis

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6503-E	• 3 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720 requires WS-C6503-E-FAN • With Release 12.2(18)SXD and later releases, WS-C6503-E supports: – WS-X6704-10GE – WS-X6748-SFP – WS-X6724-SFP – WS-X6748-GE-TX • With releases earlier than Release 12.2(18)SXD, WS-C6503-E has the same support restrictions as WS-C6503. • WS-C6503-E does not support: – WS-X6500-SFM2 – WS-C6500-SFM – WS-F6K-DFC	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB

Product ID (append "=" for spare)	Product Description	Minimum Software Version
WS-C6503	Catalyst 6503 chassis: • 3 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720 or Supervisor Engine 32 requires FAN-MOD-3HS • Does not support: – WS-X6708-10GE – WS-X6704-10GE – WS-X6748-SFP – WS-X6724-SFP – WS-X6748-GE-TX – WS-X6500-SFM2 – WS-C6500-SFM – WS-F6K-DFC	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
	With Supervisor Engine 2	12.2(17d)SXB
CISCO7603	Cisco 7603 chassis: • 3 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720 requires FAN-MOD-3HS • Does not support: – WS-X6708-10GE – WS-X6704-10GE – WS-X6748-SFP – WS-X6724-SFP – WS-X6748-GE-TX – WS-X6500-SFM2 – WS-C6500-SFM – WS-F6K-DFC	
	With Supervisor Engine 720:	12.2(14)SX
	With Supervisor Engine 2	12.2(17d)SXB

Note Supervisor Engine 32 is not supported in CISCO7603.

Unsupported Hardware

The following hardware is not supported:

- DWDM-SFP-5817—1000BASE-DWDM 1558.17 nm SFP (100-GHz ITU grid) SFP module
- DWDM-SFP-4692—1000BASE-DWDM 1546.92 nm SFP (100-GHz ITU grid) SFP module
- See the "Supervisor Engine 32 (CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A)" section on page 38 for information about hardware that is not supported with the Supervisor Engine 32.
- With a Supervisor Engine 720, WS-X6516-GBIC hardware revisions 5.0 through 5.4 with a DFC3 installed.

  Supervisor Engine 720 supports a DFC3 on these WS-X6516-GBIC hardware revisions:

  - Lower than 5.0
  - 5.5 and higher

  With a Supervisor Engine 720 and a DFC3 installed, WS-X6516-GBIC hardware revisions 5.0 through 5.3 do not power up. Without a DFC3, WS-X6516-GBIC hardware revisions 5.0 through 5.4 operate in bus mode.

  See external field notice 24494 for more information:

  http://www.cisco.com/en/US/ts/fn/200/fn24494.html
- These service modules:
  - WS-X6381-IDS Intrusion Detection System (IDS) Module
  - WS-X6380-NAM Network Analysis Module (NAM)
- Supervisor Engine 1 (WS-X6K-S1A-MSFC2, WS-X6K-SUP1A-MSFC)
- 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.

Feature Sets

These sections describe the feature sets in Release 12.2SX:

Feature Set Guidelines and Restrictions

These are the feature set guidelines and restrictions:

- This product bulletin explains the feature sets used in Release 12.2(18)SXE and later releases:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps5460/prod_bulletin0900aecd80281b17_ps708_Products_Bulletin.html
- There are no 12.2SX boot loader images: none are required.
- 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
- Many TFTP server implementations cannot transfer 16 MB or larger files. To transfer 16 MB or larger files, you might need to use FTP or rcp. See this online publication for procedures:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf008.html
- These features are not supported in Release 12.2(18)SXD and later releases:
  - 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
- With releases earlier than Release 12.2(18)SXE, use of the EGP, BGP4, and IS-IS routing protocols requires the additional purchase of the InterDomain Routing Feature License (FR-IRC6), except when the price of the feature set already includes FR-IRC6.

- In Release 12.2(17d)SXB and later releases, the price of any Cisco 7600 series router feature set (part numbers starting with "S763") includes FR-IRC6.
- In Release 12.2(17b)SXA and later releases, the price of the "IP MPLS, IPv6, and BGP Feature Set" image (S733ZK9M-122* or S763ZK9M-122*) includes FR-IRC6.

Feature Set Descriptions

This section lists all of the features that are unique to each feature set and some of the features that are common to all feature sets. See the "New Features" section on page 117 for a more complete list of supported features.

Feature Name	IP Base	IP Services	Advanced IP Services	Enterprise Services	Advanced Enterprise Services
Firewall Feature Set **Note** Not required with the WS-SVC-FWM-1-K9 Firewall Services Module.					X
TCP Intercept					X
IPsec Network Security **Note** • The SPA-IPSEC-2G and the IPsec VPN Acceleration Services Module support IPsec Network Security in hardware. • Without a SPA-IPSEC-2G or IPsec VPN Acceleration Services Module, the IPsec Network Security feature (configured with the **crypto ipsec** command) is supported in software only for administrative connections to Catalyst 6500 series switches and Cisco 7600 series routers.			X		X
MPLS			X		X
VPNs			X		X
DECNet				X	X
ISO CLNS				X	X
Novell IPX				X	X
IPv6 (Search for "IPv6" in the "New Features" section on page 117 for information about supported IPv6 features.)			X	X	X
SLB (Search for "SLB" in the "New Features" section on page 117 for information about supported SLB features.)			X	X	X
IS-IS			X	X	X
BGP4		X	X	X	X
MBGP		X	X	X	X
VRF Lite (Search for "VRF Lite" in the "New Features" section on page 117 for information about supported VRF Lite features.)		X	X	X	X
Bidirectional PIM		X	X	X	X

Feature Name	IP Base	IP Services	Advanced IP Services	Enterprise Services	Advanced Enterprise Services
EIGRP		X	X	X	X
MSDP		X	X	X	X
OSPF		X	X	X	X
PBR (Search for "PBR" in the "New Features" section on page 117 for information about supported PBR features.)		X	X	X	X
NetFlow (Search for "NetFlow" in the "New Features" section on page 117 for information about supported NetFlow features.)	X	X	X	X	X
EIGRP Stub Routing	X	X	X	X	X
HSRP	X	X	X	X	X
IGMP	X	X	X	X	X
IPsec Triple DES Encryption (3DES) for SSH **Note** • The SSH k9 images support SSH 3DES access in software on the MSFC. • The k9 images in Release 12.2(17d)SXB and later releases support both SSHv2 server and SSHv2 client features. • The k9 images in releases earlier than Release 12.2(17d)SXB support only SSHv2 server features.	X	X	X	X	X
PIMv1, PIMv2 (Search for "PIM" in the "New Features" section on page 117 for information about supported PIM features.)	X	X	X	X	X
RIPv1, RIPv2	X	X	X	X	X

New Features

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 12.2SX 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 12.2SX releases.

New Features in Release 12.2(18)SXF17b

These sections describe the new features in Release 12.2(18)SXF17b 29 Mar 2011:

New Hardware Features in Release 12.2(18)SXF17b

None.

New Software Features in Release 12.2(18)SXF17b

None.

New Features in Release 12.2(18)SXF17a

These sections describe the new features in Release 12.2(18)SXF17a, 19 Mar 2010:

New Hardware Features in Release 12.2(18)SXF17a

None.

New Software Features in Release 12.2(18)SXF17a

None.

New Features in Release 12.2(18)SXF17

These sections describe the new features in Release 12.2(18)SXF17, 30 Sep 2009:

New Hardware Features in Release 12.2(18)SXF17

None.

New Software Features in Release 12.2(18)SXF17

Subinterface Crypto connect vlan support for E-Flexwan/FE PA—See this publication:

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

New Features in Release 12.2(18)SXF16

These sections describe the new features in Release 12.2(18)SXF16, 05 Mar 2009:

New Hardware Features in Release 12.2(18)SXF16

None.

New Software Features in Release 12.2(18)SXF16

None.

New Features in Release 12.2(18)SXF15a

These sections describe the new features in Release 12.2(18)SXF15a, 29 Oct 2008:

New Hardware Features in Release 12.2(18)SXF15a

None.

New Software Features in Release 12.2(18)SXF15a

None.

New Features in Release 12.2(18)SXF15

These sections describe the new features in Release 12.2(18)SXF15, 05 Sep 2008:

New Hardware Features in Release 12.2(18)SXF15

None.

New Software Features in Release 12.2(18)SXF15

None.

New Features in Release 12.2(18)SXF14

These sections describe the new features in Release 12.2(18)SXF14, 09 May 2008:

New Hardware Features in Release 12.2(18)SXF14

None.

New Software Features in Release 12.2(18)SXF14

None.

New Features in Release 12.2(18)SXF13

These sections describe the new features in Release 12.2(18)SXF13, 17 Feb 2008:

New Hardware Features in Release 12.2(18)SXF13

- 6,000 W DC power supply (PWR-6000-DC)

New Software Features in Release 12.2(18)SXF13

None.

New Features in Release 12.2(18)SXF12a

These sections describe the new features in Release 12.2(18)SXF12a, 15 Jan 2008:

New Hardware Features in Release 12.2(18)SXF12a

None.

New Software Features in Release 12.2(18)SXF12a

None.

New Features in Release 12.2(18)SXF12

These sections describe the new features in Release 12.2(18)SXF12, 19 Nov 2007:

New Hardware Features in Release 12.2(18)SXF12

None.

New Software Features in Release 12.2(18)SXF12

None.

New Features in Release 12.2(18)SXF11

These sections describe the new features in Release 12.2(18)SXF11, 18 Sep 2007:

New Hardware Features in Release 12.2(18)SXF11

None.

New Software Features in Release 12.2(18)SXF11

None.

New Features in Release 12.2(18)SXF10a

These sections describe the new features in Release 12.2(18)SXF10a, 21 Sep 2007:

New Hardware Features in Release 12.2(18)SXF10a

None.

New Software Features in Release 12.2(18)SXF10a

None.

New Features in Release 12.2(18)SXF10

These sections describe the new features in Release 12.2(18)SXF10, 16 Jul 2007:

New Hardware Features in Release 12.2(18)SXF10

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

- Supported only with 7600-SIP-400
- See this publication:

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

New Software Features in Release 12.2(18)SXF10

None.

New Features in Release 12.2(18)SXF9

These sections describe the new features in Release 12.2(18)SXF9, 21 May 2007:

New Hardware Features in Release 12.2(18)SXF9

None.

New Software Features in Release 12.2(18)SXF9

None.

New Features in Release 12.2(18)SXF8

These sections describe the new features in Release 12.2(18)SXF8, 07 Mar 2007:

New Hardware Features in Release 12.2(18)SXF8

- 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
- DWDM SFP transceivers (see the "Gigabit Ethernet SFPs" section on page 52)

New Software Features in Release 12.2(18)SXF8

None.

New Features in Release 12.2(18)SXF7

These sections describe the new features in Release 12.2(18)SXF7, 30 Nov 2006:

New Hardware Features in Release 12.2(18)SXF7

- Persistent Storage Device (PSD; WS-SVC-PSD-1) support with Supervisor Engine 32:
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html#anchor21

New Software Features in Release 12.2(18)SXF7

- With Cisco IOS software modularity images, support for 7600-SIP-400 and 7600-SIP-200.

New Features in Release 12.2(18)SXF6

These sections describe the new features in Release 12.2(18)SXF6, 22 Sep 2006:

- New Hardware Features in Release 12.2(18)SXF6, page 125
- New Software Features in Release 12.2(18)SXF6, page 125

New Hardware Features in Release 12.2(18)SXF6

None.

New Software Features in Release 12.2(18)SXF6

- 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

New Features in Release 12.2(18)SXF5

These sections describe the new features in Release 12.2(18)SXF5, 10 Jul 2006:

- New Hardware Features in Release 12.2(18)SXF5, page 125
- New Software Features in Release 12.2(18)SXF5, page 126

New Hardware Features in Release 12.2(18)SXF5

- 8-port 10-Gigabit Ethernet X2switching module (WS-X6708-10GE).

Note To configure WS-X6708-10GE port oversubscription, refer to the **hw-module oversubscription** command in the command reference at this URL: http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-f1.html#GUID-B5F8BEA0-B5DD-47BE-82F5-183765DF0F64

- With Cisco IOS software modularity images, support for WS-SVC-WISM-1-K9.
- Multi-Processor WAN Application Module (MWAM) support with Supervisor Engine 32:
  - WS-SVC-MWAM-1
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 2
  - See these publications for more information:

    http://www.cisco.com/en/US/docs/wireless/pdsn/12.28zb/mwan_install_config/mwamhwrn.html

    http://www.cisco.com/en/US/docs/wireless/pdsn/12.28zb/mwan_install_config/mwamhwrn.html

New Software Features in Release 12.2(18)SXF5

- Autostate - Firewall Capability for the Firewall service module—See this publication:

  http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html
- Cisco IOS software modularity images for the Supervisor Engine 32.
- With Cisco IOS software modularityimages, support for Multi-VRF (VRF Lite).
- With Cisco IOS software images, Embedded Event Manager (EEM) 2.1 (previously supported with Cisco IOS software modularity images)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/sw_modularity/configuration/guide/evnt_mgr.html
- Cisco IOS server load balancing (Cisco IOS SLB):
  - Initial support on Supervisor Engine 32.
  - Previously supported on Supervisor Engine 720.
  - Previously supported on Supervisor Engine 2.

  See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxd1.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.
- DSCP-based Queue Mapping (supported only on WS-X6708-10GE)—See this publication:

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

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/stgrpsxf.html
- QoS - Ignore Port Trust—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/qos.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
- SRR (Shaped Round Robin)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/qos.html
- WCCP L2 Return—With Supervisor Engine 2, you can configure WCCP to use the Layer 2 return WCCP feature.

New Features in Release 12.2(18)SXF4

These sections describe the new features in Release 12.2(18)SXF4, 27 Mar 2006:

- New Hardware Features in Release 12.2(18)SXF4, page 127
- New Software Features in Release 12.2(18)SXF4, page 127

New Hardware Features in Release 12.2(18)SXF4

- Application Control Engine (ACE) module (ACE10-6500-K9)

New Software Features in Release 12.2(18)SXF4

- IPS Inline VLAN Pairing for WS-SVC-IDSM2-K9—See this publication for more information:

  http://www.cisco.com/en/US/docs/security/ips/5.1/configuration/guide/cli/cliguide.html
- Cisco IOS Software Modularity images for the Supervisor Engine 720—See these sections for information about Cisco IOS Software Modularity:
  - Cisco IOS Software Modularity Documentation, page 13
  - Cisco IOS Software Modularity Unsupported Features, page 14

New Features in Release 12.2(18)SXF3

These sections describe the new features in Release 12.2(18)SXF3, 16 Feb 2006:

- New Hardware Features in Release 12.2(18)SXF3, page 127
- New Software Features in Release 12.2(18)SXF3, page 128

New Hardware Features in Release 12.2(18)SXF3

- 96-port 10/100TX RJ-45 switching module (WS-X6148X2-RJ-45, WS-X6148X2-45AF)
- 96-port 10/100TX RJ-21 switching module (WS-X6196-RJ-21, WS-X6196-21AF)
- IEEE 802.3af PoE daughtercard for WS-X6148X2-RJ-45 and WS-X6196-RJ-21 (WS-F6K-FE48X2-AF)

New Software Features in Release 12.2(18)SXF3

None.

New Features in Release 12.2(18)SXF2

These sections describe the new features in Release 12.2(18)SXF2, 20 Jan 2006:

New Hardware Features in Release 12.2(18)SXF2

- Wireless Services Module (WiSM):
  - WS-SVC-WISM-1-K9
  - Not supported with Cisco IOS software modularity images until Release 12.2(18)SXF5
- 1-port OC-192c/STM-64 POS/RPR SPA, VSR-1 (SPA-OC192POS-VSR):
  - Supported only with 7600-SIP-600
  - See this publication:

    http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- 100BASE SFPs for use with WS-X6148-FE-SFP:
  - 100BASE-BX10-U SFP (GLC-FE-100BX-U)
  - 100BASE-BX10-D SFP (GLC-FE-100BX-D)
- Support with Supervisor Engine 32 for these modules:
  - 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)
  - Also supported with Supervisor Engine 720
  - SPA-IPSEC-2G supports the features that were previously supported with WS-SVC-IPSEC-1.
  - See this publication:

    http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- Support with Supervisor Engine 2 for these modules:
  - 48-port 10/100TX RJ-45 switching module (WS-X6148A-RJ-45, WS-X6148A-45AF)
  - 48-port 10/100/1000 Mbps switching module (WS-X6148A-GE-TX, WS-X6148A-GE-45AF)
  - 48-port 100BASE-FX switching module (WS-X6148-FE-SFP), with these SFPs:

    100BASE-BX10-U SFP (GLC-FE-100BX-U)

    100BASE-BX10-D SFP (GLC-FE-100BX-D)

100BASEEX SFP (GLC-FE-100EX)

100BASEZX SFP (GLC-FE-100ZX)

100BASEFX SFP (GLC-FE-100FX)

100BASELX SFP (GLC-FE-100LX)

- Fast Ethernet port adapters (PA-2FE, PA-1FE)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html

- 1-port Packet over SONET OC3c/STM1 port adapter (PA-POS-1OC3)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/port_adapters/install_upgrade/multichannel_serial/pa-pos-1oc3_install_config/6514_1oc.html

- Receive-only coarse or dense Wavelength Division Multiplexing (WDM) GBIC (WDM-GBIC-REC)

New Software Features in Release 12.2(18)SXF2

- NAC - L2 IP; Network Admission Control (NAC) Layer 2 Layer 2 IP validation (not supported with Supervisor Engine 2)—See this publication:

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

- 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

- RSVP Scalability Enhancements—See this publication:

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

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

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_Dot1q_Transparency_for_EoMPLS

- 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#RFC_1483_Spanning-Tree_Interoperability_Enhancements

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

- Support with Supervisor Engine 32 for:
  - NetFlow v9 Export Format, including NetFlow Export of BGP Nexthop Information
  - NetFlow multicast support
  - PIM snooping DR flooding enhancement
- Support with Supervisor Engine 2 for these features, which are already supported with other Supervisor Engines:
  - Any transport over MPLS (AToM): HDLC over MPLS (HDLCoMPLS)

- Any transport over MPLS (AToM): PPP over MPLS (PPPoMPLS)
- ATM OAM ping
- ATM VC access trunk emulation
- Bandwidth command for HQoS parent class support
- BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN
- BGP support for TTL security check
- Bidirectional forwarding detection (BFD) standard implementation
- Bridge control protocol (BCP)
- Bridging using RFC1483 routed encapsulation (BRE)
- Clear hardware interface counters
- CNS interactive CLI
- Configurable per VLAN MAC learning (PVL)
- CSG: content services gateway release 6
- DE/CLP and EXP mapping on FR/ATMoMPLS VC
- Digital optical monitoring (DOM)
- Distributed MLPPP (dMLPPP) on FlexWAN module interfaces
- Dynamic Multipoint VPN (DMVPN) phase 2
- EIGRP MPLS VPN PE-CE Site of Origin (SoO)
- Embedded network management improvements
- EtherChannel enhancement - 128 EtherChannels support
- EtherChannel Min-Links
- Ethernet over MPLS (EoMPLS) per VLAN QoS
- Flex Links
- Frame Relay Virtual Circuit (VC) bundling
- Hardware capacity monitoring
- HQoS support for Ethernet over MPLS (EoMPLS) VC
- H-VPLS with MPLS edge
- IDSM-2 EtherChannel load balancing
- IEEE 802.1s - Multiple Spanning Tree (MST) standard compliance
- Integrated IS-IS global default metric
- Integrated IS-IS protocol shutdown support maintaining configuration parameters
- Integrated IS-IS support for BFD over IPv4
- Invalid Special Parameter Index (SPI) recovery
- IP routing of RFC1483 ATM Bridge Encapsulation (RBE)
- IP unnumbered for VLAN-SVI interfaces
- IS-IS caching of redistributed routes
- IS-IS support for priority-driven IP prefix RIB installation
- Key rollover for certificate renewal

- Layer 2 traceroute
- MPLS LDP - inbound label binding filtering
- MPLS LSP ping/traceroute and AToM VCCV
- MQC: distribution of remaining bandwidth
- Multicast-VPN: multicast support for MPLS VPN
- Multipoint Bridging (MPB)
- NetFlow - bridged flow statistics
- OSPF link state database overload protection
- OSPF Link-Local Signaling (LLS) per interface basis
- OSPF MIB support of RFC 1850 and latest extensions
- OSPF support for BFD over IPv4
- OSPF support for forwarding adjacencies over MPLS traffic engineered tunnels
- OSPF support for unlimited software VRFs per Provider Edge (PE) router
- Packet classification based on layer3 packet-length (supported on WAN ports)
- Per interface sticky ARP
- Per port MAC limiting
- Per VLAN load balancing for advanced QinQ service mapping
- PIM snooping DR flooding enhancement
- PKI AAA authorization using the entire subject name
- 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
- Protected private key storage
- QoS: aggregated DSCP / precedence values for WRED
- QoS: ingress shaping on FlexWAN module interfaces
- QoS: match VLAN on OSMs
- QoS: percentage based policing on WAN ports
- Query mode definition per trustpoint
- Query multiple servers during certificate revocation check
- RADIUS Load Balancing (RLB) IMSI sticky
- Re-enroll using existing certificate
- RFC-1490 bridging on FlexWAN interfaces
- SafeNet IPsec VPN client support
- SCP health monitoring for enhanced-FlexWAN
- Show diagnostic sanity
- Show Top-N

- SLB: interface-aware
- SLB: stateful failover within single chassis
- SPAN destination port permit list
- Strict priority low latency queueing (LLQ)
- Sub interface features - phase 1
- Unicast flood blocking (UFB)
- Uni-Directional Link Routing (UDLR)
- verify certificate chain command
- VLANs over IP unnumbered sub-interfaces

New Features in Release 12.2(18)SXF1

These sections describe the new features in Release 12.2(18)SXF1, 22 Dec 2005:

- New Hardware Features in Release 12.2(18)SXF1, page 132
- New Software Features in Release 12.2(18)SXF1, page 132

New Hardware Features in Release 12.2(18)SXF1

None.

New Software Features in Release 12.2(18)SXF1

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

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

New Features in Release 12.2(18)SXF

These sections describe the new features in Release 12.2(18)SXF, 12 Sep 2005:

- New Hardware Features in Release 12.2(18)SXF, page 132
- New Software Features in Release 12.2(18)SXF, page 135

New Hardware Features in Release 12.2(18)SXF

Note Initial support for these modules is now in Release 12.2(18)SXF3:

- 96-port 10/100TX RJ-45 switching module (WS-X6148X2-RJ-45, WS-X6148X2-45AF)
- 96-port 10/100TX RJ-21 switching module (WS-X6196-RJ-21, WS-X6196-21AF)
- IEEE 802.3af PoE daughtercard for WS-X6148X2-RJ-45 and WS-X6196-RJ-21 (WS-F6K-FE48X2-AF)

(CSCsd16853)

- Compact Flash Adapter in Bootflash Slot (WS-CF-UPG=):
  - CompactFlash adapter with 512 MB CompactFlash card that replaces the bootflash device.
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_17277.html
- Supervisor Engine 32 (WS-SUP32-10GE-3B, WS-SUP32-GE-3B)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Module_Installation/Sup_Eng_Guide/supe_gd.html

  Note See the "Supervisor Engine 32 (CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A)" section on page 38 for the list of features not supported with Supervisor Engine 32.
- 48-port 10/100/1000 Mbps switching module (WS-X6148A-GE-TX, WS-X6148A-GE-45AF)
- 48-port 100BASE-FX switching module (WS-X6148-FE-SFP), with these SFPs:
  - 100BASEFX SFP (GLC-FE-100FX)
  - 100BASELX SFP (GLC-FE-100LX)
- 48-port 10/100TX RJ-45 switching module (WS-X6148A-RJ-45, WS-X6148A-45AF)
- SPA Interface Processor-600 (7600-SIP-600)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- 1-port 10-Gigabit Ethernet SPA, LANPHY XFP Optics (SPA-1XTENGE-XFP), with this XFP module: 10-Gigabit Ethernet LR (10 km; XFP-10GLR-OC192LR)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- 10-port Gigabit Ethernet SPA, SFP Optics (SPA-10X1GE)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- 5-port Gigabit Ethernet SPA, SFP Optics (SPA-5X1GE)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- 2-port Gigabit Ethernet SPA, SFP Optics (SPA-2X1GE), with these SFPs:
  - Extended Temperature SX SFP (SFP-GE-S)
  - Extended Temperature LX/LH SFP (SFP-GE-L)
  - Extended Temperature ZX SFP (SFP-GE-Z)

  See this publication:

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

- 1-port OC-192c/STM-64 POS/RPR SPA, SM-LR (SPA-OC192POS-LR)—See this publication:

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

- 1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics (SPA-OC192POS-XFP), with these XFP modules:
  - Single-Mode (SM) Short Reach (SR; XFP-10GLR-OC192SR)
  - Single-Mode (SM) Intermediate Reach (IR-2; XFP-10GER-OC192IR)

  See this publication:

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

- 1 port OC-48c/STM-16 ATM SPA (SPA-1XOC48-ATM)—See this publication:

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

- Firewall Services module support with Supervisor Engine 32:
  - WS-SVC-FWM-1-K9
  - Also supported with Supervisor Engine 720.
  - Also supported with Supervisor Engine 2.
  - See this publication for more information:

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

- Network Analysis Module support with Supervisor Engine 32:
  - WS-SVC-NAM-1 and WS-SVC-NAM-2
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

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

- Intrusion Detection System Module 2 support with Supervisor Engine 32:
  - WS-SVC-IDSM2-K9
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

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

- Secure Sockets Layer (SSL) Services Module support with Supervisor Engine 32:
  - WS-SVC-SSL-1
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ssl/2.1/release/notes/OL_5277.html

New Software Features in Release 12.2(18)SXF

Note See the "Supervisor Engine 32 (CAT6000-SUP32/MSFC2A, 7600-SUP32/MSFC2A)" section on page 38 for the list of features not supported with Supervisor Engine 32.

- 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#H-VPLS_with_MPLS_Edge_Configuration_Example
- '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
- EtherChannel Min-Links—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/channel.html
- Flex Links—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/flexlink.html
- Hardware Capacity Monitoring—See this publication:

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

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/mst.html
- IP Unnumbered for VLAN-SVI interfaces—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/layer3.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
- 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
- Multicast enhancement - egress replication performance improvement—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/mcastv4.html
- Multicast Enhancement - Replication Mode Detection—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/mcastv4.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)SXF and later 12.2SX 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)SXF and later 12.2SX releases.
- Per Interface Sticky ARP—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dos.html
- PIM snooping DR flooding enhancement—See this publication:

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

New Features in Release 12.2(18)SXE6b

These sections describe the new features in Release 12.2(18)SXE6a, 29 Dec 2006:

- New Hardware Features in Release 12.2(18)SXE6b, page 136
- New Software Features in Release 12.2(18)SXE6b, page 136

New Hardware Features in Release 12.2(18)SXE6b

None.

New Software Features in Release 12.2(18)SXE6b

None.

New Features in Release 12.2(18)SXE6a

These sections describe the new features in Release 12.2(18)SXE6a, 18 Sep 2006:

- New Hardware Features in Release 12.2(18)SXE6a, page 136
- New Software Features in Release 12.2(18)SXE6a, page 137

New Hardware Features in Release 12.2(18)SXE6a

None.

New Software Features in Release 12.2(18)SXE6a

None.

New Features in Release 12.2(18)SXE6

These sections describe the new features in Release 12.2(18)SXE6, 08 Jun 2006:

- New Hardware Features in Release 12.2(18)SXE6, page 137
- New Software Features in Release 12.2(18)SXE6, page 137

New Hardware Features in Release 12.2(18)SXE6

None.

New Software Features in Release 12.2(18)SXE6

None.

New Features in Release 12.2(18)SXE5

These sections describe the new features in Release 12.2(18)SXE5, 13 Feb 2006:

- New Hardware Features in Release 12.2(18)SXE5, page 137
- New Software Features in Release 12.2(18)SXE5, page 137

New Hardware Features in Release 12.2(18)SXE5

- Compact Flash Adapter in Bootflash Slot (WS-CF-UPG=):
  - CompactFlash adapter with 512 MB CompactFlash card that replaces the bootflash device.
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_17277.html

New Software Features in Release 12.2(18)SXE5

- 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

New Features in Release 12.2(18)SXE4

These sections describe the new features in Release 12.2(18)SXE4, 10 Oct 2005:

- New Hardware Features in Release 12.2(18)SXE4, page 138
- New Software Features in Release 12.2(18)SXE4, page 138

New Hardware Features in Release 12.2(18)SXE4

None.

New Software Features in Release 12.2(18)SXE4

None.

New Features in Release 12.2(18)SXE3

These sections describe the new features in Release 12.2(18)SXE3, 22 Aug 2005:

New Hardware Features in Release 12.2(18)SXE3

None.

New Software Features in Release 12.2(18)SXE3

None.

New Features in Release 12.2(18)SXE2

These sections describe the new features in Release 12.2(18)SXE2, 23 Jun 2005:

New Hardware Features in Release 12.2(18)SXE2

Support with Supervisor Engine 720 for these modules:

- 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):
- Also supported with Supervisor Engine 32
- SPA-IPSEC-2G supports the features that were previously supported with WS-SVC-IPSEC-1.
- See this publication:

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

New Software Features in Release 12.2(18)SXE2

None.

New Features in Release 12.2(18)SXE1

These sections describe the new features in Release 12.2(18)SXE1, 18 Apr 2005:

- New Hardware Features in Release 12.2(18)SXE1, page 139
- New Software Features in Release 12.2(18)SXE1, page 139

New Hardware Features in Release 12.2(18)SXE1

- Application-Oriented Networking (AON) Module (WS-SVC-AON-1-K9) support with Supervisor Engine 720—See these publications:

  http://www.cisco.com/en/US/products/ps6480/prod_release_notes_list.html
- WebVPN Services Module (WS-SVC-WEBVPN-K9; not supported with Supervisor Engine 2)—See this publication:

  http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html#anchor24

New Software Features in Release 12.2(18)SXE1

None.

New Features in Release 12.2(18)SXE

These sections describe the new features in Release 12.2(18)SXE, 11 Apr 2005:

- New Hardware Features in Release 12.2(18)SXE, page 139
- New Software Features in Release 12.2(18)SXE, page 141

New Hardware Features in Release 12.2(18)SXE

- Anomaly Guard Module (WS-SVC-AGM-1-K9)—See this publication:

  http://www.cisco.com/en/US/prod/collateral/modules/ps2706/end_of_life_c51-573493.html
- Traffic Anomaly Detector Module (WS-SVC-ADM-1-K9)—See this publication:

  http://www.cisco.com/en/US/prod/collateral/modules/ps2706/end_of_life_c51-573493.html
- 2700 W AC power supply for CISCO7606 chassis (PWR-2700-AC)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/cis_76xx.html
- 2700 W DC power supply for CISCO7606 chassis (PWR-2700-DC)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/cis_76xx.html

- 2700 W AC power supply for 4-slot chassis (PWR-2700-AC/4)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/cis_76xx.html

- 2700 W DC power supply for 4-slot chassis (PWR-2700-DC/4)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/cis_76xx.html

- Catalyst 6500 series switch 4-slot chassis (WS-C6504-E)—See this publication:

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

- Cisco 7600 series router 4-slot chassis (CISCO7604)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/Hardware/Chassis_Installation/7600_Series_Router_Installation_Guide/cis_76xx.html

- Cisco 7600 Series SPA Interface Processor-200 (7600-SIP-200)—See this publication:

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

- Cisco 7600 Series SPA Interface Processor-400 (7600-SIP-400)—See this publication:

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

- Cisco 1-Port OC-12c/STM-4c ATM Shared Port Adapter (SPA-1XOC12-ATM)—See this publication:

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

- Cisco 1-Port OC-12c/STM-4c POS Shared Port Adapter (SPA-1XOC12-POS)—See this publication:

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

- Cisco 8-Port Channelized T1/E1 Shared Port Adapter (SPA-8XCHT1/E1)—See this publication:

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

- Cisco Channelized T3 to DS0 Shared Port Adapter (SPA-2XCT3/DS0, SPA-4XCT3/DS0)—See this publication:

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

- Cisco Clear Channel T3/E3 Shared Port Adapter (SPA-2XT3/E3, SPA-4XT3/E3)—See this publication:

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

- Cisco OC-3c/STM-1c ATM Shared Port Adapter (SPA-2XOC3-ATM, SPA-4XOC3-ATM)—See this publication:

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

- Cisco OC-3c/STM-1c POS Shared Port Adapter (SPA-2XOC3-POS, SPA-4XOC3-POS)—See this publication:

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

- Fast Ethernet port adapters (PA-2FE, PA-1FE)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html

- 1-port Packet over SONET OC3c/STM1 port adapter (PA-POS-1OC3)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/port_adapters/install_upgrade/multichannel_serial/pa-pos-1oc3_install_config/6514_1oc.html

- Content Switching Module with SSL (CSM-S; WS-X6066-SLB-S-K9)—See this publication:

  http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/csms/1.1.1/release/notes/78_16597.html

- 10GBASE-LW XENPAK Module with WAN PHY for SMF (XENPAK-10GB-LW)
- 10GBASE dense wavelength-division multiplexing (DWDM) 100-GHz ITU grid (DWDM-XENPAK)
- 10GBASE receive-only wavelength division multiplexing (WDM; WDM-XENPAK-REC)
- 1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength (GLC-BX-D)
- 1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength (GLC-BX-U)
- Receive-only coarse or dense Wavelength Division Multiplexing (WDM) GBIC (WDM-GBIC-REC)

New Software Features in Release 12.2(18)SXE

- 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/mpls.html#HDLC_Over_MPLS

- 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/mpls.html#PPP_Over_MPLS

- ATM VC access trunk emulation—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.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 support for TTL security check—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/12-2sx/irg-neighbor.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 and Cisco 7600 routers support BFD only on Ethernet, Fast Ethernet (except PA-2FE and PA-1FE), Gigabit Ethernet, Gigabit Ethernet WAN (GE-WAN), 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."
- 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/flexwan-config-guide.html
- **clear hardware interface counters** command.
- 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 aborted 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 abort a command before its normal termination (similar to manually aborting 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/ios-xml/ios/interface/command/ir-l2.html#GUID-326D5509-3E03-4E0B-8C69-3084E21D97BE
- CSG: Content Services Gateway Release 6—See this publication:

  http://www.cisco.com/en/US/products/sw/wirelssw/ps779/tsd_products_support_series_home.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#DE/CLP_and_EXP_Mapping_on_FR/ATMoMPLS_VC

- DHCP Snooping (supported only with PFC3)—See this publication:

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

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

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s4.html#GUID-73B23B10-A62E-4F88-9F4D-F37A9C14D8D8

  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

- Dynamic ARP Inspection (DAI; supported only with PFC3)—See this publication:

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

- Dynamic Multipoint VPN (DMVPN) Phase 2
  - In Release 12.2(18)SXE2 and later releases, supported with SPA-IPSEC-2G.
  - In Release 12.2(18)SXE and later releases, supported with WS-SVC-IPSEC-1.
  - See this publication:

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

- Egress ACL support for remarked DSCP (supported only with PFC3)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/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 network management improvements—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.html

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

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

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

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/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#Ethernet_over_MPLS

- 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.
- Frame Relay virtual circuit (VC) bundling—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- HQoS support for Ethernet over MPLS (EoMPLS) VC—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.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
- 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.”
- 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
- IP routing of RFC1483 ATM bridge encapsulation (RBE)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- PFC3 hardware support for IPv4 multicast over point-to-point GRE tunnels—See this publication:

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

  Note Releases earlier than Release 12.2(18)SXE supported IPv4 multicast over point-to-point GRE tunnels in software on the MSFC. The PFC3 does not provide hardware acceleration for tunnels configured with the **tunnel key** command.
- IPv6 access services: DHCPv6 prefix delegation—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/15-sy/ipv6-15-sy-library.html

- IPv6 hardware: multicast assist—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/mcastv6.html

- IPv6 multicast RPR/RPR+ support—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/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 Multicast: HW assisted egress replication—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/mcastv6.html

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

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

- 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

- Layer 2 traceroute—See this publication:

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

- MLD snooping—See this publication:

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

- 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_4t/12_4t11/ht_lspng.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/12.2SXF/native/configuration/guide/mvpn.html

  Note Support for MVPN also includes support for multicast VRF (MVRF). MVRF is also known as multicast over VRF-lite. MVPN and MVRF are supported in PFC3B or PDC3BXL mode.

- 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/pos.html#Configuring_Multipoint_Bridging

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

- NetFlow - Bridged Flow Statistics—See this publication:

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

- Netflow Multiple Export Destinations:
  - In Release 12.2(18)SXF and later releases, supported with Supervisor Engine 32
  - In Release 12.2(18)SXE and later releases, supported with Supervisor Engine 720
  - In Release 12.2(18)SXD and later releases, supported with Supervisor Engine 2
  - Allows entry of a second **ip flow-export destination** command
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/nde.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/routers/7600/technical_references/7600_mib_guides/MIB_Guide_ver_6/mibgde6.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 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 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 port MAC limiting—See the **mac-address-table limit** command in this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/lanswitch/command/lsw-m1.html#GUID-6B40F1F2-BB7D-45CD-B9CE-5B3E0FE019A5

- 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#Per_VLAN_Load_Balancing_for_Advanced_QinQ_Service_Mapping

- 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

- 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, and port security with sticky MAC addresses—See this publication:

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

- Protected private key storage—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-deploy-rsa-pki.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/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- QoS: match VLAN on OSMs—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/qos.html#Configuring_QoS:_Match_VLAN
- 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
- Re-enroll using existing certificate—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/12-2sx/sec-cert-enroll-pki.html
- Redundant Supervisor Engine 720 system high availability enhancement:
  - When a module is inserted or removed (OIR), a data integrity mechanism engages to ensure that no corrupt data is transferred on the backplane bus. This mechanism can cause a minimal amount of packet loss during OIR in a non-DFC-based system. For a DFC-based system, this mechanism does not have an effect on any traffic during OIR.

    This feature causes the redundant supervisor engine to operate as a DFC-based module (the redundant supervisor engine operates as a non-DFC-based module by default), which protects the redundant supervisor engine from any packet loss during module OIR because it is disconnected from the backplane bus.

    This feature only applies to a system with redundant supervisor engines and DFCs on all the modules. The supervisor engine uplink ports (on both standby and active) cannot be used with this configuration.
  - See the **fabric switching-mode allow dcef-only** command in this publication:

    http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-f1.html#GUID-A815D749-F21A-4624-9DCB-81390BBE369E
- RFC-1490 bridging on FlexWAN interfaces—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- RADIUS Load Balancing (RLB) IMSI sticky—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.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.
- Show diagnostic sanity—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/diags.html
- Show Top-N—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/topn.html
- SLB: stateful failover within single chassis—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.html
- SLB: interface-aware—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.html
- SPAN destination port permit list—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/span.html
- SSM mapping for IPv6—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/15-sy/ipv6-15-sy-library.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/qos.html#Configuring_Low_Latency_Queuing
- Sub interface features - phase 1—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/layer3.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/mpls.html#Creating_the_Parent_Policy_Map_and_Attaching_It_to_the_Egress_Interface
- Uni-Directional Link Routing (UDLR)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/ude_udlr.html
- Unicast flood blocking (UFB)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/blocking.html
- **verify certificate chain** command—Allows the use of the Layer 2 overhead specification for shaping.
- 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
- ATM OAM ping—See this publication:

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

New Features in Release 12.2(18)SXD7b

These sections describe the new features in Release 12.2(18)SXD7b, 12 Dec 2006

New Hardware Features in Release 12.2(18)SXD7b

None.

New Software Features in Release 12.2(18)SXD7b

None.

New Features in Release 12.2(18)SXD7a

These sections describe the new features in Release 12.2(18)SXD7a, 15 Sep 2006

New Hardware Features in Release 12.2(18)SXD7a

None.

New Software Features in Release 12.2(18)SXD7a

None.

New Features in Release 12.2(18)SXD7

These sections describe the new features in Release 12.2(18)SXD7, 15 Dec 2005:

New Hardware Features in Release 12.2(18)SXD7

None.

New Software Features in Release 12.2(18)SXD7

None.

New Features in Release 12.2(18)SXD6

These sections describe the new features in Release 12.2(18)SXD6, 22 Aug 2005:

New Hardware Features in Release 12.2(18)SXD6

None.

New Software Features in Release 12.2(18)SXD6

None.

New Features in Release 12.2(18)SXD5

These sections describe the new features in Release 12.2(18)SXD5, 16 May 2005:

New Hardware Features in Release 12.2(18)SXD5

None.

New Software Features in Release 12.2(18)SXD5

None.

New Features in Release 12.2(18)SXD4

These sections describe the new features in Release 12.2(18)SXD4, 24 Mar 2005:

New Hardware Features in Release 12.2(18)SXD4

None.

New Software Features in Release 12.2(18)SXD4

None.

New Features in Release 12.2(18)SXD3

These sections describe the new features in Release 12.2(18)SXD3, 13 Dec 2004:

New Hardware Features in Release 12.2(18)SXD3

- Distributed Forwarding Card 3BXL (DFC3BXL; WS-F6K-DFC3BXL) for use on dCEF256 and CEF256 modules—See the "Distributed and Centralized Forwarding Cards" section on page 45.
- Distributed Forwarding Card 3B (DFC3B; WS-F6K-DFC3B) for use on dCEF256 and CEF256 modules—See the "Distributed and Centralized Forwarding Cards" section on page 45.
- Anomaly Guard Module (WS-SVC-AGM-1-K9)—See this publication:

  http://www.cisco.com/en/US/prod/collateral/modules/ps2706/end_of_life_c51-573493.html
- Traffic Anomaly Detector Module (WS-SVC-ADM-1-K9—See this publication:

  http://www.cisco.com/en/US/prod/collateral/modules/ps2706/end_of_life_c51-573493.html

New Software Features in Release 12.2(18)SXD3

- Source Specific Multicast (SSM) Mapping:
  - Do not configure SSM mapping in a VLAN that supports IGMPv3 multicast receivers.
  - See this publication:

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

New Features in Release 12.2(18)SXD2

These sections describe the new features in Release 12.2(18)SXD2, 22 Oct 2004:

New Hardware Features in Release 12.2(18)SXD2

None.

New Software Features in Release 12.2(18)SXD2

None.

New Features in Release 12.2(18)SXD1

These sections describe the new features in Release 12.2(18)SXD1, 30 Sep 2004:

New Hardware Features in Release 12.2(18)SXD1

Note In Release 12.2(18)SXD1, all service modules have been tested with OSMs, the FlexWAN module, and the Enhanced FlexWAN module.

- Persistent Storage Device (PSD; WS-SVC-PSD-1) support with Supervisor Engine 720:
  - Also supported with Supervisor Engine 32
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html#anchor21
- Multi-Processor WAN Application Module (MWAM) support with Supervisor Engine 720:
  - WS-SVC-MWAM-1
  - Also supported with Supervisor Engine 32
  - Also supported with Supervisor Engine 2
  - See these publications for more information:

    http://www.cisco.com/en/US/docs/wireless/pdsn/12.28zb/mwan_install_config/mwamhwrn.html

    http://www.cisco.com/en/US/docs/wireless/pdsn/12.28zb/mwan_install_config/mwamhwrn.html

    Note With Release 12.2(18)SXD1 and later releases, WS-SVC-MWAM-1 maintains state when an NSF with SSO redundancy mode switchover occurs. With Release 12.2(18)SXD, WS-SVC-MWAM-1 does not maintain state when an NSF with SSO redundancy mode switchover occurs.
- Content Services Gateway (CSG) support with Supervisor Engine 720
  - WS-SVC-CSG-1
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/products/sw/wirelssw/ps779/tsd_products_support_series_home.html

New Software Features in Release 12.2(18)SXD1

- 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)

- VRF Aware IPsec:
  - In Release 12.2(18)SXE2 and later releases, supported with SPA-IPSEC-2G.
  - In Release 12.2(18SXD1 and later releases, supported with Supervisor Engine 720 and WS-SVC-IPSEC-1.
  - Not supported with Supervisor Engine 2 and WS-SVC-IPSEC-1.
  - See this publication:

    http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_vrf_aware_ipsec.html
- Hardware Control Plane Interface for Control Plane Policing (CoPP):
  - With Cisco IOS 12.2SX releases, only the PFC3 supports CoPP.
  - The PFC3 does not support CoPP output rate limiting (policing).
  - The PFC3 does not support the CoPP silent operation mode.
  - The PFC3 does not support the **match protocol arp** command.
  - The PFC3 automatically installs the CoPP service policy on all DFC-equipped switching modules.
  - See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dos.html
- Web Cache Control Protocol (WCCP) support with Supervisor Engine 720—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-2sx/iap-wccp.html
- The **fabric switching-mode allow dcef-only** command support with Supervisor Engine 2 (CSCec05612):
  - By default, the two Gigabit Ethernet ports on a redundant Supervisor Engine 2 rely on the PFC on the active supervisor engine for all forwarding decisions.
  - The **fabric switching-mode allow dcef-only** command disables the Gigabit Ethernet ports on the redundant Supervisor Engine 2 to ensure that all modules are operating in dCEF mode.
  - Module OIR is nondisruptive when all active switching modules are dCEF-enabled.

New Features in Release 12.2(18)SXD

These sections describe the new features in Release 12.2(18)SXD, 26 Jul 2004:

- New Hardware Features in Release 12.2(18)SXD, page 155
- New Software Features in Release 12.2(18)SXD, page 155

New Hardware Features in Release 12.2(18)SXD

Note With Release 12.2(18)SXD and later releases, OSMs require a minimum of 128 MB of dynamic random-access memory (SDRAM)—See this publication for memory upgrade procedures:

http://www.cisco.com/en/US/docs/routers/7600/Hardware/Module_and_Line_Card_Installation_Guides/7600_Series_Router_Module_Installation_Guide/osmodule.html

- WS-F6700-DFC3BXL Distributed Forwarding Card 3BXL (DFC3BXL) for use on CEF720 modules—See the "Distributed and Centralized Forwarding Cards" section on page 45
- Distributed Forwarding Card 3B (DFC3B; WS-F6700-DFC3B) for use on CEF720 modules—See the "Distributed and Centralized Forwarding Cards" section on page 45
- Wireless LAN service module (WS-SVC-WLAN-1-K9) support with Supervisor Engine 720—See this publication:

  http://www.cisco.com/en/US/products/ps6526/tsd_products_support_eol_model_home.html
- WS-X6066-SLB-S-K9 Content Switching Module with SSL (CSM-S) with Supervisor Engine 2:
  - Also supported with Supervisor Engine 720
  - See this publication:

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/csms/1.1.1/release/notes/78_16597.html
- 6000 W AC power supply (WS-CAC-6000W)

New Software Features in Release 12.2(18)SXD

- Cisco Nonstop Forwarding (NSF) with stateful switchover (SSO) supervisor engine redundancy on Supervisor Engine 720 and Supervisor Engine 2—See this publication:

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

Note
- Release 12.2(18)SXD and later releases do not support the SRM with SSO redundancy mode (see the "New Software Features in Release 12.2(17b)SXA" section on page 170).
- With PFC3, 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.

- The following modules do not maintain state when an NSF with SSO redundancy mode switchover occurs:
  - IPsec VPN Acceleration services module (WS-SVC-IPSEC-1).
  - WS-X6066-SLB-APC (CSM; with Release 12.2(18)SXD1 and later releases, WS-X6066-SLB-APC maintains state when an NSF with SSO redundancy mode switchover occurs).
  - WS-SVC-FWM-1-K9 firewall services module (with Release 12.2(18)SXD3 and later Cisco IOS releases and 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).
  - WS-SVC-SSL-1 secure sockets layer (SSL) services module.
  - WS-SVC-MWAM-1 (with Release 12.2(18)SXD1 and later releases, WS-SVC-MWAM-1 maintains state when an NSF with SSO redundancy mode switchover occurs).
  - WS-SVC-PSD-1 (with Release 12.2(18)SXD1 and later releases, WS-SVC-PSD-1 maintains state when an NSF with SSO redundancy mode switchover occurs).

- ARP ACLs for QoS Filtering (supported only with PFC3)—See this publication:

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

  Note Supervisor Engine 2 applies IP ACLs to ARP traffic.

- Protocol-Independent MAC ACL Filtering (supported only in PFC3BXL or PFC3B mode)—See this publication:

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

- Netflow Multiple Export Destinations:
  - In Release 12.2(18)SXE and later releases, supported with Supervisor Engine 720
  - In Release 12.2(18)SXD and later releases, supported with Supervisor Engine 2
  - Allows entry of a second **ip flow-export destination** command
  - See this publication:

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

- For the IPsec VPN Acceleration services module (WS-SVC-IPSEC-1):

  Note In Release 12.2(18)SXE2 and later releases, these features are also supported with SPA-IPSEC-2G.

  - Easy VPN Server features—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

  - Distinguished Name-Based Crypto Maps—See this publication:

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

- IKE: Initiate Aggressive Mode—See this publication:

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

- Real-Time Resolution for IPsec Tunnel Peer—See this publication:

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

- IPsec VPN Accounting—See this publication:

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

- Trusted Root Certification Authority—See this publication:

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

- Certificate Security Attribute-Based Access Control—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

- Trustpoint CLI—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—See this publication:

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

- Manual Certificate Enrollment (TFTP and Cut-and-Paste)—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—See this publication:

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

- IP Security VPN Monitoring—See this publication:

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

- Encrypted Preshared Key—See this publication:

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

- Crypto Conditional Debug Support—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—See this publication:

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

- Cisco IOS server load balancing (Cisco IOS SLB):
  - Initial support on Supervisor Engine 720 including GGSN-SLB Messaging
  - Also supported on Supervisor Engine 32
  - Previously supported on Supervisor Engine 2
  - Initial support for Home Agent Loadbalancing on Supervisor Engine 720 and Supervisor Engine 2

  See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxd1.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.

- Cisco IOS 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.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

- 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_bgpdpg.html

- BGP Route Map Continue—See this publication:

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

- BGP Route-Map Policy List Support—See this publication:

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

- BGP Restart Session After Max-Prefix Limit—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/12-2sx/irg-neighbor.html

- BGP Increased Support of Numbered AS-path Access Lists to 500—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.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 Incremental SPF—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isisispf.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
- 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
- OSPF Support for Fast Hellos—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fasthelo.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 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 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 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
- On LAN ports, 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_MPLS

  Note Multi-VRF for CE Routers (VRF Lite) with the PFC3 supports multi-VRF CE functionality with EIGRP, OSPF, BGP and RIPv2 routing protocols running on a per VRF basis. Static routes are also supported. Also supported on WAN ports.

- 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 Traffic Engineering Forwarding Adjacency—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fstefa_3.html
- MPLS Traffic Engineering (TE) Interarea Tunnels—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiarea3.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-xml/ios/iproute_eigrp/configuration/12-2sx/ire-mpls-vpn.html

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

- You can use the **set ip dscp** and **set ip precedence** policy map class commands on non-IP traffic to mark the internal DSCP value, which is the basis of the egress Layer 2 CoS value. (CSCec34212)
- Support for the **mls netflow maximum-flows** command. (CSCee28200)
- Support for the allowed VLAN list to filter the traffic transmitted from a SPAN destination trunk port. (CSCeb01318)
- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for the Cisco Catalyst 6500 Series Switch 1.1 (CVDM-C6500)

    Resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for the Cisco Catalyst 6500 Series SSL Services Module 1.1 (CVDM-SSLSM)

    Enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for the Cisco Content Switching Module 1.1 (CVDM-CSM)

    Enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.
  - CiscoView Device Manager for the Cisco IPsec VPN Acceleration services module (WS-SVC-IPSEC-1) 1.1 (CVDM-VPNSM)

    Allows users to manage VLANs, create and configure VPNs, and configure settings such as IPsec rules on their VPN module. It is a task-based tool that allows users to control the versatility of their Cisco VPN module by offering configuration wizards based on recommended practices in tasks such as creating Site-to-Site VPNs and configuring GRE tunnels.

  To access all CiscoView Device Manager documentation, go to this URL:

  http://www.cisco.com/en/US/products/sw/cscowork/ps4565/index.html

New Features in Release 12.2(17d)SXB11a

These sections describe the new features in Release 12.2(17d)SXB11a, 17 Apr 2006:

- New Hardware Features in Release 12.2(17d)SXB11a, page 161
- New Software Features in Release 12.2(17d)SXB11a, page 161

New Hardware Features in Release 12.2(17d)SXB11a

None.

New Software Features in Release 12.2(17d)SXB11a

None.

New Features in Release 12.2(17d)SXB11

These sections describe the new features in Release 12.2(17d)SXB11, 17 Nov 2005:

New Hardware Features in Release 12.2(17d)SXB11

None.

New Software Features in Release 12.2(17d)SXB11

None.

New Features in Release 12.2(17d)SXB10

These sections describe the new features in Release 12.2(17d)SXB10, 16 Aug 2005:

New Hardware Features in Release 12.2(17d)SXB10

None.

New Software Features in Release 12.2(17d)SXB10

None.

New Features in Release 12.2(17d)SXB9

These sections describe the new features in Release 12.2(17d)SXB8, 21 Jul 2005:

New Hardware Features in Release 12.2(17d)SXB9

None.

New Software Features in Release 12.2(17d)SXB9

None.

New Features in Release 12.2(17d)SXB8

These sections describe the new features in Release 12.2(17d)SXB8, 02 May 2005:

New Hardware Features in Release 12.2(17d)SXB8

None.

New Software Features in Release 12.2(17d)SXB8

None.

New Features in Release 12.2(17d)SXB7

These sections describe the new features in Release 12.2(17d)SXB7, 01 Mar 2005:

New Hardware Features in Release 12.2(17d)SXB7

- WebVPN Services Module (WS-SVC-WEBVPN-K9; not supported with Supervisor Engine 2)—See this publication:

  http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html#anchor24

New Software Features in Release 12.2(17d)SXB7

None.

New Features in Release 12.2(17d)SXB6

These sections describe the new features in Release 12.2(17d)SXB6, 21 Dec 2004:

New Hardware Features in Release 12.2(17d)SXB6

- Distributed Forwarding Card 3BXL (DFC3BXL; WS-F6700-DFC3BXL) for use on CEF720 modules—See the "Distributed and Centralized Forwarding Cards" section on page 45.
- Distributed Forwarding Card 3B (DFC3B; WS-F6700-DFC3B) for use on CEF720 modules—See the "Distributed and Centralized Forwarding Cards" section on page 45.

New Software Features in Release 12.2(17d)SXB6

None.

New Features in Release 12.2(17d)SXB5

These sections describe the new features in Release 12.2(17d)SXB5, 01 Nov 2004:

New Hardware Features in Release 12.2(17d)SXB5

None.

New Software Features in Release 12.2(17d)SXB5

None.

New Features in Release 12.2(17d)SXB4

These sections describe the new features in Release 12.2(17d)SXB4, 07 Sep 2004:

New Hardware Features in Release 12.2(17d)SXB4

None.

New Software Features in Release 12.2(17d)SXB4

None.

New Features in Release 12.2(17d)SXB3

These sections describe the new features in Release 12.2(17d)SXB3, 17 Aug 2004:

New Hardware Features in Release 12.2(17d)SXB3

None.

New Software Features in Release 12.2(17d)SXB3

- You can use the **set ip dscp** and **set ip precedence** policy map class commands on non-IP traffic to mark the internal DSCP value, which is the basis of the egress Layer 2 CoS value. (CSCee56918)

New Features in Release 12.2(17d)SXB2

These sections describe the new features in Release 12.2(17d)SXB2, 21 Jul 2004:

- New Hardware Features in Release 12.2(17d)SXB2, page 164
- New Software Features in Release 12.2(17d)SXB2, page 164

New Hardware Features in Release 12.2(17d)SXB2

None.

New Software Features in Release 12.2(17d)SXB2

- Initial support for the **mls rate-limit multicast non-rpf** command. (CSCee95301)
- Initial support for the **mls ip cef load-sharing** [**full**] [**simple** | **optimized**] command. (CSCed74512)

New Features in Release 12.2(17d)SXB1

These sections describe the new features in Release 12.2(17d)SXB1, 01 Jun 2004:

- New Hardware Features in Release 12.2(17d)SXB1, page 164
- New Software Features in Release 12.2(17d)SXB1, page 165

New Hardware Features in Release 12.2(17d)SXB1

Note Release 12.2(17d)SXB1 and later releases do not support XENPAK-10GB-ER units with part number 800-24557-01, as described in this external field notice (CSCee47030):

http://www.cisco.com/en/US/ts/fn/200/fn29736.html

- WS-SUP720-3B Supervisor Engine 720 with Policy Feature Card 3B (PFC3B)—See the "Supervisor Engines" section on page 34
- WS-F6K-PFC3B= Policy Feature Card 3BXL (PFC3B)—See the "Policy Feature Cards" section on page 41
- 1000BASE-ZX GBIC (GLC-ZX-SM)
- 10GBASE-CX4 XENPAK Module for CX4 (copper) cable (XENPAK-10GB-CX4)

New Software Features in Release 12.2(17d)SXB1

- GGSN-SLB Messaging (supported only with Supervisor Engine 2)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxb2.html
- Initial support for the **mls netflow usage notify** global configuration mode command to configure NetFlow table usage monitoring. (CSCdz64998)
- Initial support in the **show mls statistics** command for display of the approximate Layer 2 switching rate in packets-per-second. (CSCee28215; see resolved caveat CSCee92338)
- 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

New Features in Release 12.2(17d)SXB

These sections describe the new features in Release 12.2(17d)SXB, 05 Mar 2004:

- New Hardware Features in Release 12.2(17d)SXB, page 165
- New Software Features in Release 12.2(17d)SXB, page 167

New Hardware Features in Release 12.2(17d)SXB

- 48-port Gigabit Ethernet SFP switching module (WS-X6748-SFP; supported only with Supervisor Engine 720)
- IEEE 802.3af PoE daughtercard (WS-F6K-GE48-AF, WS-F6K-48-AF)
- Supervisor Engine 2, PFC2, and MSFC2
  - WS-X6K-S2U-MSFC2
  - WS-X6K-S2-MSFC2 with upgraded memory

  See the "Supported Hardware" section on page 33 for information about the hardware supported with Supervisor Engine 2.
- Distributed Forwarding Card (DFC; WS-F6K-DFC); requires Switch Fabric Module; supported only with Supervisor Engine 2
- The Switch Fabric Module (SFM; WS-C6500-SFM); does not support 13-slot chassis; supported only with Supervisor Engine 2
- WS-X6500-SFM 2 Switch Fabric Module version 2 (SFM2); supports all chassis; supported only with Supervisor Engine 2
- Persistent Storage Device (PSD) support with Supervisor Engine 2:
  - WS-SVC-PSD-1
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 32
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_notes_list.html#anchor21

- Multi-Processor WAN Application Module (MWAM) support with Supervisor Engine 2:
  - WS-SVC-MWAM-1
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 32
  - See this publication for more information:

    http://www.cisco.com/en/US/docs/wireless/pdsn/12.28zb/mwan_install_config/mwamhwrn.html
- Content Services Gateway (CSG) support with Supervisor Engine 2:
  - WS-SVC-CSG-1
  - Also supported with Supervisor Engine 720
  - See this publication for more information:

    http://www.cisco.com/en/US/products/sw/wirelssw/ps779/tsd_products_support_series_home.html
- Firewall Services module support with Supervisor Engine 2:
  - WS-SVC-FWM-1-K9
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 32
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html
- Network Analysis Module support with Supervisor Engine 2:
  - WS-SVC-NAM-1 and WS-SVC-NAM-2
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 32
  - See this publication for more information:

    http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_notes_list.html
- Intrusion Detection System Module 2 support with Supervisor Engine 2:
  - WS-SVC-IDSM2-K9
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 32
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/tsd_products_support_model_home.html
- Content Switching Module (CSM) support with Supervisor Engine 2:
  - WS-X6066-SLB-APC
  - Also supported with Supervisor Engine 720
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/tsd_products_support_model_home.html

- Secure Sockets Layer (SSL) Services Module support with Supervisor Engine 2:
  - WS-SVC-SSL-1
  - Also supported with Supervisor Engine 720
  - Also supported with Supervisor Engine 32
  - See this publication for more information:

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ssl/2.1/release/notes/OL_5277.html

New Software Features in Release 12.2(17d)SXB

- 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-secure-shell-v2.html
- Generic Online Diagnostics (GOLD) for Supervisor Engine 2—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/diags.html
- Enhanced support for interface link status messages (CSCeb06765). See the following publication for more information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-l1.html#GUID-54AC5D19-D058-4DF0-BB6E-380E0684D643
- Support for the **mls qos trust** [**dscp** | **ip-precedence** | **cos**] command on WS-X6148-RJ-45, WS-X6148-RJ-45V, WS-X6148-RJ-21, and WS-X6148-RJ-21V switching modules. (CSCec30649)
- VACL capture on LAN and WAN ports—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/vacl.html

  Note VACL capture is not supported on WS-X6708-10GE ports.
- Hardware-supported counters for hardware-supported ACLs, displayed by the **show tcam interface** command (supported only in PFC3BXL or PFC3B mode). See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-s6.html#GUID-1D17939B-1C8F-422C-83CE-64B096DAD13D
- Optimized ACL logging (supported only with PFC3)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/acl.html
- Release 12.2(17d)SXB provides initial Release 12.2SX support for Supervisor Engine 2. Support for Supervisor Engine 2 in Release 12.2SX has all the Supervisor Engine 2 features supported by Release 12.1(20)E, including these:
  - Web Cache Control Protocol (WCCP) support with Supervisor Engine 2—See this publication:

    http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-2sx/iap-wccp.html
  - Cisco IOS server load balancing (SLB) support with Supervisor Engine 2—See this publication:

    http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slb17sxb.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.

  - Network-Based Application Recognition (NBAR) for LAN ports; supported only with Supervisor Engine 2—See this publication:

    http://www.cisco.com/en/US/docs/ios/12_4t/qos/configuration/guide/qsnbar1.html

  - Unknown unicast flood protection (UUFP; supported only with Supervisor Engine 2)—See the **mac-address-table unicast-flood** command at this URL:

    http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_m1.html#mac-address-table_unicast-flood

- Release 12.2(17d)SXB provides initial support with Supervisor Engine 2 for these features in software. These features are already supported with Supervisor Engine 720 in hardware:
  - IPv6 unicast traffic on LAN and WAN interfaces—See this publication:

    http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/config_library/15-sy/ipv6-15-sy-library.html

  - Bidirectional Protocol Independent Multicast (PIM)—See this publication:

    http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/mcastv4.html

- Release 12.2(17d)SXB provides initial support with Supervisor Engine 2 for these features. These features are already supported with Supervisor Engine 720:
  - Gateway Load Balancing Protocol (GLBP)—See this publication:

    http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_glbp2.html

  - Interior Border Gateway Protocol (IBGP) multipath—See this publication:

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

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

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

  - Virtual Private LAN Services (VPLS) on the Optical Services Modules—See this publication:

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

  - Any Transport over MPLS (AToM) features:

    —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#Any_Transport_over_MPLS

  - TDR cable diagnostics—See "TDR cable diagnostics" in the "New Software Features in Release 12.2(17a)SX" section on page 178.

- 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

- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.1 (CVDM-C6500)

    CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.1 (CVDM-SSLSM)

    CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for Cisco Content Switching Module 1.1 (CVDM-CSM)

    CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

  To access all CiscoView Device Manager documentation, go to this URL:

  http://www.cisco.com/en/US/products/sw/cscowork/ps4565/index.html

New Features in Release 12.2(17b)SXA2

These sections describe the new features in Release 12.2(17b)SXA2, 22 Apr 2004:

- New Hardware Features in Release 12.2(17b)SXA2, page 169
- New Software Features in Release 12.2(17b)SXA2, page 169

New Hardware Features in Release 12.2(17b)SXA2

None.

New Software Features in Release 12.2(17b)SXA2

None.

New Features in Release 12.2(17b)SXA

These sections describe the new features in Release 12.2(17b)SXA, 31 Dec 2003:

- New Hardware Features in Release 12.2(17b)SXA, page 170
- New Software Features in Release 12.2(17b)SXA, page 170

New Hardware Features in Release 12.2(17b)SXA

- WS-SUP720-3BXL Supervisor Engine 720-3BXL—see the "Supervisor Engines" section on page 34
- WS-F6K-PFC3BXL Policy Feature Card 3BXL (PFC3BXL)—See the "Policy Feature Cards" section on page 41
- Optical Service Modules (OSMs; see the "Optical Services Modules (OSMs)" section on page 80)
- WS-X6582-2PA Enhanced FlexWAN module—See the "FlexWAN and Enhanced FlexWAN Modules" section on page 89
- 2-port Packet-over-SONET OC-3c/STM-1 Port Adapter (PA-POS-2OC3)
- IPsec VPN Acceleration services module (WS-SVC-IPSEC-1)
- To avoid reloads with software releases where caveat CSCed17605 is not resolved (CSCed17605 is resolved in Release 12.2(17d)SXB and later releases), do not configure the single router mode with stateful switchover (SRM with SSO) redundancy mode with a WS-SVC-IPSEC-1 module installed. In software releases where caveat CSCed17605 is not resolved, the WS-SVC-IPSEC-1 module supports only RPR and RPR+ redundancy modes.

New Software Features in Release 12.2(17b)SXA

Note

- With a PFC3BXL or PFC3B functioning in PFC3A mode, there is no support for features that require the PFC3BXL (see the "Policy Feature Cards" section on page 41).
- In a system with a PFC3BXL or PFC3B, DFC3A modules are not recognized if inserted while the system is online.
- In a system with a PFC3BXL or PFC3B, after a reboot, any DFC3A modules are active, but the system functions in PFC3A mode and does not support the PCF3BXL or PFC3B mode features.

- BGP Policy Accounting—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgppa.html
- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.0 and 1.1 (CVDM-C6500)

    CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 and 1.1 (CVDM-SSLSM)

    CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for Cisco Content Switching Module 1.0 and 1.1 (CVDM-CSM)

    CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

To access all CiscoView Device Manager documentation, go to this URL:

http://www.cisco.com/en/US/products/sw/cscowork/ps4565/index.html

- Cisco IP Phone support 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.
- TDR cable diagnostics—See "TDR cable diagnostics" in the "New Software Features in Release 12.2(17a)SX" section on page 178.
- Support for more than 1 Gbps of traffic per EtherChannel on the WS-X6548-GE-TX and WS-X6548V-GE-TX switching modules.
- Hardware support for Network Address Translation (NAT) and Port Address Translation (PAT) of UDP traffic (supported only in PFC3BXL or PFC3B mode).
- Support for PFC QoS features on tunnels (supported only in PFC3BXL or PFC3B mode).
- Support for per-VLAN and CoS-based QoS filtering in MAC ACLs (supported only in PFC3BXL or PFC3B mode).
- Population of the NDE Layer 4 source port field with the ICMP type and code values (supported only in PFC3BXL or PFC3B mode).
- Hardware switching for ICMP traffic when Cisco IOS reflexive ACLs are configured (supported only in PFC3BXL or PFC3B mode). (CSCeb20666)
- VLAN translation—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/vlans.html
- Received ToS byte preservation—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/qos.html
- Ingress CoS mutation on IEEE 802.1Q tunnel ports—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/qos.html
- Single router mode with stateful switchover (SRM with SSO) redundancy mode for unicast traffic.

Note

- All releases that support SRM with SSO have been deferred.
- Release 12.2(18)SXD and later releases do not support SRM with SSO.

- Release 12.2(17b)SXA, rebuilds of Release 12.2(17b)SXA, Release 12.2(17d)SXB, and rebuilds of Release 12.2(17d)SXB support SRM with SSO on Supervisor Engine 720.
- SRM with SSO is not supported on Supervisor Engine 2 in any release.
- SRM with SSO redundancy mode does not support stateful switchover for multicast traffic. When a switchover occurs, all multicast hardware switching entries are removed and are then recreated and reinstalled in the hardware by the newly active MSFC.
- SRM with SSO redundancy mode does not support MPLS. If you configure MPLS, use the RPR or RPR+ redundancy mode.
- SRM with SSO redundancy mode does not support the IPsec VPN Acceleration services module (WS-SVC-IPSEC-1) in software releases where caveat CSCed17605 is not resolved (CSCed17605 is resolved in Release 12.2(17d)SXB and later releases).
- The following modules do not maintain state when an SRM with SSO redundancy mode switchover occurs:
  - IPsec VPN Acceleration services module (WS-SVC-IPSEC-1)
  - WS-X6066-SLB-APC (CSM)
  - WS-SVC-FWM-1-K9 firewall services module
  - WS-SVC-SSL-1 secure sockets layer (SSL) services module

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

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/atm.html
- On WAN ports, 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_MPLS

  Note Multi-VRF for CE Routers (VRF Lite) with the PFC3 supports multi-VRF CE functionality with EIGRP (Release 12.2(18)SXD and later releases), OSPF, BGP and RIPv2 routing protocols running on a per VRF basis. Static routes are also supported. Also supported on LAN ports (Release 12.2(18)SXD and later releases).
- Virtual Private LAN Services (VPLS) on the Optical Services Modules (supported only in PFC3BXL or PFC3B mode)—See this publication:

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

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

- Route Processor Redundancy (RPR) with:
  - Release 12.2(17b)SXA and rebuilds
  - Release 12.2(17d)SXB and rebuilds
- RPR+ with Release 12.2(18)SXD and rebuilds
- In Release 12.2(18)SXD and rebuilds, 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 (MPLS; supported only in PFC3BXL or PFC3B mode)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/pfc3mpls.html
- MPLS Label Distribution Protocol (LDP; supported only in PFC3BXL or PFC3B mode)—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_MPLS
- MPLS Virtual Private Networks (MPLS VPN; supported only in PFC3BXL or PFC3B mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsmvpns.html
- MPLS VPN Carrier Supporting Carrier (supported only in PFC3BXL or PFC3B mode)—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—Inter-AS—IPv4 BGP Label Distribution (supported only in PFC3BXL or PFC3B mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiaslbl.html
- MPLS VPN ID (supported only in PFC3BXL or PFC3B mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/vpnid2.html
- Any Transport over MPLS (AToM) Features:
  - Not supported with PFC3A
  - 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#Any_Transport_over_MPLS

- MPLS VPN—OSPF and Sham-Link Support (supported only in PFC3BXL or PFC3B mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_sham_link.html
- Cisco IOS IPv6 Provider Edge Router (6PE) over MPLS (supported only in PFC3BXL or PFC3B mode)—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/12-2sy/ip6-over-mpls.html
- Distributed Multilink Frame Relay (FRF.16)—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/dmfr.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
- IPv6 Support on WAN Interfaces—See this publication:

  http://www.cisco.com/en/US/tech/tk872/tech_white_papers_list.html
- OSPF Shortest Path First Throttling—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_spftrl.html
- Gateway Load Balancing Protocol—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_glbp2.html

New Features in Release 12.2(17a)SX4

These sections describe the new features in Release 12.2(17a)SX4, 23 Apr 2004:

- New Hardware Features in Release 12.2(17a)SX4, page 174
- New Software Features in Release 12.2(17a)SX4, page 174

New Hardware Features in Release 12.2(17a)SX4

None.

New Software Features in Release 12.2(17a)SX4

None.

New Features in Release 12.2(17a)SX3

These sections describe the new features in Release 12.2(17a)SX3, 05 Mar 2004:

- New Hardware Features in Release 12.2(17a)SX3, page 175
- New Software Features in Release 12.2(17a)SX3, page 175

New Hardware Features in Release 12.2(17a)SX3

None.

New Software Features in Release 12.2(17a)SX3

None.

New Features in Release 12.2(17a)SX2

These sections describe the new features in Release 12.2(17a)SX2, 29 Jan 2004:

- New Hardware Features in Release 12.2(17a)SX2, page 175
- New Software Features in Release 12.2(17a)SX2, page 175

New Hardware Features in Release 12.2(17a)SX2

None.

New Software Features in Release 12.2(17a)SX2

None.

New Features in Release 12.2(17a)SX1

These sections describe the new features in Release 12.2(17a)SX1, 30 Oct 2003:

- New Hardware Features in Release 12.2(17a)SX1, page 175
- New Software Features in Release 12.2(17a)SX1, page 175

New Hardware Features in Release 12.2(17a)SX1

- 10GBASE-SR Serial 850-nm short-reach XENPAK (XENPAK-10GB-SR; see the "10-Gigabit Ethernet Switching Modules" section on page 55)
- 10GBASE-LX4 Serial 1310-nm multimode fiber (MMF) XENPAK (XENPAK-10GB-LX4; see the "10-Gigabit Ethernet Switching Modules" section on page 55)

New Software Features in Release 12.2(17a)SX1

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

  http://www.cisco.com/en/US/docs/ios/12_4t/qos/configuration/guide/qsnbar1.html
- Hardware support 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
- Software support 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
- Software support for IPv6 routing:
  - 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
- Switching support for IPv6:
  - Process
  - CEFv6
  - Distributed CEFv6
- Software support 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/ipv6/config_library/15-sy/ipv6-15-sy-library.html

For command reference information, refer to this publication:

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

New Features in Release 12.2(17a)SX

These sections describe the new features in Release 12.2(17a)SX, 06 Oct 2003:

- New Hardware Features in Release 12.2(17a)SX, page 177
- New Software Features in Release 12.2(17a)SX, page 178

New Hardware Features in Release 12.2(17a)SX

- 48-port 10/100/1000 Ethernet RJ-45 switching module (WS-X6748-GE-TX)
- 24-port Gigabit Ethernet SFP switching module (WS-X6724-SFP)
- 4-port 10-Gigabit Ethernet XENPAK switching module (WS-X6704-10GE)
- XENPAK-10GB-LR 10GBASE-LR Serial 1310-nm long-reach XENPAK
- XENPAK-10GB-LR+ 10GBASE-LR Serial 1310-nm long-reach XENPAK
- XENPAK-10GB-ER 10GBASE-ER Serial 1550-nm extended-reach XENPAK
- 1000BASE-DWDM GBIC (DWDM-GBIC)
- 1000BASE-CWDM SFP (CWDM-SFP)
- 1000BASE-LX/LH SFP (GLC-LH-SM)
- 1000BASE-T SFP (GLC-T)
- 48-port 10/100/1000 Mbps switching module (WS-X6548-GE-TX and WS-X6548V-GE-TX; WS-X6548V-GE-TX has WS-F6K-VPWR-GE).

Note The WS-X6548-GE-TX and WS-X6548V-GE-TX do not support the following:
—With Release 12.2(17a)SX and Release 12.2(17a)SX1, more than 1 Gbps of traffic per EtherChannel
—WS-F6K-DFC3A
—ISL trunking
—Jumbo frames
—802.1Q tunneling
—Traffic storm control

- 48-port 10/100/1000 Mbps switching module (WS-X6148-GE-TX and WS-X6148V-GE-TX; WS-X6148V-GE-TX has WS-F6K-VPWR-GE).

Note The WS-X6148-GE-TX and WS-X6148V-GE-TX do not support the following:
—More than 1 Gbps of traffic per EtherChannel
—WS-F6K-DFC3A
—ISL trunking
—Jumbo frames
—802.1Q tunneling
—Traffic storm control

- PWR-1400-AC 1,400 W AC power supply

New Software Features in Release 12.2(17a)SX

- TDR cable diagnostics—TDR is supported on these switching modules:
  - In Release 12.2(17a)SX and later releases:
    —WS-X6148-GE-TX
    —WS-X6148V-GE-TX
    —WS-X6148-GE-45AF
    —WS-X6548-GE-TX
    —WS-X6548V-GE-TX
    —WS-X6548-GE-45AF
  - In Release 12.2(18)SXE and later releases, WS-X6748-GE-TX
  - In Release 12.2(18)SXF and later releases:
    —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/12.2SXF/native/configuration/guide/intrface.html
  - The **test cable-diagnostics** command in the command reference at this URL:

    http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/test_cable-diagnostics_through_xmodem.html#GUID-9EC19973-42B5-434D-9872-6A089E38441E
- 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/ios-xml/ios/interface/command/ir-l1.html#GUID-ED398440-82A6-4553-906A-4EDE90143CD8
- Custom IEEE 802.1Q Ethertypes:
  - Supported on these modules:

    —Supervisor engines
    —WS-X6516-GE-TX
    —WS-X6748-GE-TX
    —WS-X6748-SFP
    —WS-X6724-SFP
    —WS-X6704-10GE
    —WS-X6816-GBIC
    —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/12.2SXF/native/configuration/guide/layer2.html

- PIM Snooping—See this publication:

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

- 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-12-2sx-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-book.html

- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.0 and 1.1 (CVDM-C6500)

    CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 and 1.1 (CVDM-SSLSM)

    CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for Cisco Content Switching Module 1.0 and 1.1 (CVDM-CSM)

    CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

  To access all CiscoView Device Manager documentation, go to this URL:

  http://www.cisco.com/en/US/products/sw/cscowork/ps4565/index.html

New Features in Release 12.2(14)SX1

These sections describe the new features in Release 12.2(14)SX1, 28 May 2003:

- New Hardware Features in Release 12.2(14)SX1, page 180

- New Software Features in Release 12.2(14)SX1, page 181

New Hardware Features in Release 12.2(14)SX1

- Content Switching Module (CSM) support with Supervisor Engine 720:
  - WS-X6066-SLB-APC
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/tsd_products_support_model_home.html

Note Support with Supervisor Engine 720 requires CSM module software release 3.1(4) or later.

- Intrusion Detection System Module 2 support with Supervisor Engine 720:
  - WS-SVC-IDSM2-K9
  - Also supported with Supervisor Engine 32
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/tsd_products_support_model_home.html
- Firewall Services module support with Supervisor Engine 720:
  - WS-SVC-FWM-1-K9
  - Also supported with Supervisor Engine 32
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html
- Network Analysis Module support with Supervisor Engine 720:
  - WS-SVC-NAM-1 and WS-SVC-NAM-2
  - Also supported with Supervisor Engine 32
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_release_notes_list.html
- Secure Sockets Layer (SSL) Services Module support with Supervisor Engine 720:
  - WS-SVC-SSL-1
  - Also supported with Supervisor Engine 32
  - Also supported with Supervisor Engine 2
  - See this publication for more information:

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ssl/2.1/release/notes/OL_5277.html

New Software Features in Release 12.2(14)SX1

- Half-Bridging on FlexWAN ATM interfaces (CSCin27157)
- RFC 1483 hardware bridging on FlexWAN (CSCea70308)
- VACL capture to support the WS-SVC-IDSM2-K9 Intrusion Detection System Module 2 and the WS-SVC-NAM-2 and WS-SVC-NAM-1 network analysis modules.

Note Caveat CSCec75140 prevents use of VACL capture on WAN ports in releases earlier than Release 12.2(17b)SXA. Caveat CSCec75140 is resolved in Release 12.2(17b)SXA.

- Support for embedded CiscoView—See this publication:

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

- Support for these CiscoView Device Managers:
  - CiscoView Device Manager for Cisco Catalyst 6500 Series Switch 1.0 and 1.1 (CVDM-C6500)

    CVDM-C6500 resides in the switch and manages several Layer 2 and Layer 3 features for a single chassis. It is a task-based tool that eases the initial setup and deployment of end-to-end services across modules by offering configuration templates based on recommended practices.
  - CiscoView Device Manager for Cisco Catalyst 6500 Series SSL SM 1.0 and 1.1 (CVDM-SSLSM)

    CVDM-SSLSM enables users to easily configure Secure Socket Layer (SSL) services on their SSL services module. It is a task-based tool that allows users to take advantage of the versatility of their SSL services module. It offers configuration wizards based on best practices in tasks such as setting up Trustpoints and proxy services.
  - CiscoView Device Manager for Cisco Content Switching Module 1.0 and 1.1 (CVDM-CSM)

    CVDM-CSM enables users to easily configure content load-balancing services on their CSMs. It is a task-based tool that allows users to control the versatility of their CSM by offering configuration based on recommended practices in tasks, such as setting up virtual servers, creating server farms, and applying advanced policies.

  To access all CiscoView Device Manager documentation, go to this URL:

  http://www.cisco.com/en/US/products/sw/cscowork/ps4565/index.html

New Features in Release 12.2(14)SX

These sections describe the new features in Release 12.2(14)SX, 14 Apr 2003:

- New Hardware Features in Release 12.2(14)SX, page 182
- New Software Features in Release 12.2(14)SX, page 182

New Hardware Features in Release 12.2(14)SX

- WS-SUP720 Supervisor Engine 720—See the "Supervisor Engines" section on page 34
- Communication Media Module (WS-SVC-CMM)—See these publications:
  - Release 12.2(13)ZP3:

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/cmm/release/notes/OL_4847.html
  - Release 12.2(2)YK1:

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/cmm/release/notes/ol_3137.html
  - Release 12.2(13)ZC:

    http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/cmm/release/notes/OL_3732.html
- 1000BASE-SX SFP (GLC-SX-MM)
- Distributed Forwarding Card 3A (DFC3A; WS-F6K-DFC3A)—See the "Distributed and Centralized Forwarding Cards" section on page 45
- 16-port Gigabit Ethernet switching module (WS-X6516A-GBIC)
- FlexWAN port adapters:
  - 1-port ATM OC-3c/STM-1 multimode port adapter, enhanced (PA-A6-OC3MM)
  - 1-port ATM OC-3c/STM-1 single-mode (IR) port adapter, enhanced (PA-A6-OC3SMI)
  - 1-port ATM OC-3c/STM-1 single-mode (LR) port adapter, enhanced (PA-A6-OC3SML)
  - 1-port ATM DS3 port adapter, enhanced (PA-A6-T3)
  - 1-port ATM E3 port adapter, enhanced (PA-A6-E3)
- 4000 W DC-power supply (PWR-4000-DC)

New Software Features in Release 12.2(14)SX

- Generic Online Diagnostics (GOLD)—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/diags.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
- Bidirectional Protocol Independent Multicast (PIM) in hardware—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/mcastv4.html
- 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/12.2SXF/native/configuration/guide/snooigmp.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/12.2SXF/native/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/12.2SXF/native/configuration/guide/qos.html

- Egress DSCP mutation—See this publication:

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

- 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/12.2SXF/native/configuration/guide/qos.html

- Hardware-assisted NetFlow Aggregation—See this publication:

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

- Hardware-assisted Multiple-path Unicast Reverse Path Forwarding (Unicast RPF)—See this publication:

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

- Hardware-assisted Network Address Translation (NAT) and Port Address Translation (PAT) for IPv4 unicast and multicast traffic—Note the following information about hardware-assisted NAT:

  – The PFC3A does not support NAT or PAT for UDP traffic.

  Note PFC3B and PFC3BXL modes support NAT and PAT for UDP traffic.

  – The PFC3 does not support NAT or PAT for multicast traffic.

  – The PFC3 does not support NAT or PAT configured with a route map that specifies length.

  – The PFC3 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 PFC3 sends all traffic in fragmented packets to the MSFC3 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 MSFC, 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/ios/security/command/reference/sec_m2.html#mls_rate-limit_unicast_acl

(CSCea23296)

- Hardware-assisted IP-in-IP tunneling and generic routing encapsulation (GRE) tunneling—The PFC3 and DFC3s support 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 MSFC3. The PFC3 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 address. Hardware-assisted tunnels cannot share a source address even if the destination addresses are different. Use secondary addresses on loopback interfaces or create multiple loopback interfaces. Failure to use unique source addresses may result in control plane failures when software path congestion occurs. (CSCdy72539)
  - Each tunnel interface uses one internal VLAN.
  - Each tunnel interface uses one additional router MAC address entry per router MAC address.
  - The PFC3A does not support any PFC QoS features on tunnel interfaces.
  - The PFC3B and PFC3BXL support PFC QoS features on tunnel interfaces.
  - In releases earlier than Release 12.2(18)SXE, the PFC3 does not support GRE tunnel encapsulation and de-encapsulation of multicast traffic.

  - The MSFC 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.

- Hardware-assisted Cisco IOS Firewall Features—refer to this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/fw.html

Note For a complete listing of hardware-assisted features, refer to this publication:

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

- FlexWAN features:
  - 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

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

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

  - Voice over Frame Relay (VoFR) FRF.11 and FRF.12—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 and the Cisco 7600 series routers 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.

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

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

  - RFC 1889 Compressed Real-Time Protocol (cRTP)—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.

Software Features from Earlier Releases

- Hardware-assisted TCP intercept—See this publication:

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

- Hardware-assisted policy-based routing (PBR) 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:

  - Releases earlier than Release 12.2(33)SXH use the syntax from Release 12.1, which supports **preempt** as a keyword for the **standby priority** command:

    http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/command/fhp-s2.html#GUID-5A848994-88AD-4B7D-A046-3F20AFD1EF9E

  - 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 MSFC address falls within the range of a PBR ACL, traffic addressed to the MSFC is policy routed in hardware instead of being forwarded to the MSFC. To prevent policy routing of traffic addressed to the MSFC, configure PBR ACLs to deny traffic addressed to the MSFC. (CSCse86399)
  - Any options in Cisco IOS ACLs that provide filtering in a PBR route map that would cause flows to be sent to the MSFC3 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)

- Hardware support for directed broadcasts with the **mls ip directed-broadcast** command—See this publication:

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-l2.html#GUID-C2BDF601-4096-470F-A2D8-CF2B35F4A3E8

- Cisco IP Phone Support—See this publication:

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

- IEEE 802.1X Port-Based Authentication—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dot1x.html

- Port Security—See this publication:

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

- Remote SPAN—See this publication:

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

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

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

- SNMP ifindex persistence—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/swcg.html

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

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

- NDE—See this publication:

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

- Route Processor Redundancy Plus (RPR+) redundancy—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/redund.html

- 4096 Layer 2 VLANs—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/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.

- IEEE 802.1Q tunneling—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dot1qtnl.html

- IEEE 802.1Q protocol tunneling—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/dot1qtnl.html

- IEEE 802.1s, multiple spanning tree (MST)—See this publication:

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

- IEEE 802.3ad, link aggregation control protocol (LACP)—See this publication:

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

- PortFast BPDU filtering—See this publication:

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

- Traffic storm control—Prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.
- 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-RJ-45V 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.

- Private VLANs—“Configuring Private VLANs”
- QoS Data Export—“Configuring QoS”
- VLAN Access Control Lists (VACLs)—“Configuring VLAN ACLs (VACLs)”
- VACL Deny Logging—“Configuring Network Security”
- Router-Port Group Management Protocol (RGMP)—See this publication:

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

- UniDirectional Link Detection—See this publication:

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

- VLANs—See this publication:

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

- VLAN Trunk Protocol (VTP) and VTP domains—See this publication:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/vtp.html

- EtherChannel—See this publication:

  http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/vtp.html

- Spanning Tree Protocol—See this publication:

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

- IGMP snooping and IGMP snooping querier—See this publication:

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

- The ip local-proxy-arp command.

  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 the ip proxy-arp command documentation.

- 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

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

  http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcfdlsw_ps1835_TSD_Products_Configuration_Guide_Chapter.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

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

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

- Boot Protocol (BOOTP) relay—See this publication:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf012.html

- Multiple-Hot Standby Routing Protocol—See this publication:

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

- Cisco Discovery Protocol (CDP); (refer to the “Configuring CDP” chapter)
- NetFlow Data Export (refer to the “Configuring NDE” chapter)
- Access control using several supported authentication methods (refer to the “Configuring the Supervisor Engine” chapter)
- Switched Port Analyzer (SPAN); (refer to the “Configuring SPAN” chapter)
- Redundant supervisor engines (refer to the “Configuring the Supervisor Engine” chapter)
- Quality of Service (QoS); (refer to the “Configuring QoS” chapter)
- 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.

- 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

Unsupported Features and Commands

Note See also the "Supervisor Engine 32 Restrictions" section on page 38 and the "Cisco IOS Software Modularity Unsupported Features" section on page 14.

- Hardware—See the "Unsupported Hardware" section on page 114.
- 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**
- In Release 12.2(18)SXE and later releases, these QoS interface commands are no longer supported on FlexWAN and OSM interfaces:
  - **traffic shape**
  - **priority-group**
  - **custom-queue-list**
  - **tx-queue-limit**
- In Release 12.2(18)SXE and later releases, these QoS interface commands are no longer supported on OSM interfaces, but they are still supported on FlexWAN interfaces:
  - **fair-queue**
  - **random-detect**
  - **rate-limit**
  - **tx-ring-limit**
  - **max-reserved-bandwidth**
- Random Sampled NetFlow (**flow-sampler** commands)
- These features are not supported in Release 12.2(18)SXD and later releases:
  - 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
- With PFC3:
  - Unknown unicast flood protection
  - Network-based application recognition (NBAR) for LAN interfaces
- 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 MSFC 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

Caveats

Note

- All caveats in Release 12.2(18)S also apply to Release 12.2(18)SXD and later 12.2SX releases. 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(17d)SXB and rebuilds.
- All caveats in Release 12.2(17b) also apply to Release 12.2(17b)SXA and rebuilds.
- All caveats in Release 12.2(17a) also apply to Release 12.2(17a)SX and rebuilds.
- 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/products/sw/iosswrel/ps1835/prod_release_notes_list.html
- All caveats in Release 12.2(14)S also apply to Release 12.2(14)SX and later 12.2SX releases. 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

Caveats in Release 12.2(18)SXF and Rebuilds

Note

- The caveat information for Release 12.2(18)SXF and rebuilds is updated frequently.
- Release 12.2(18)SXF2 includes all fixes that are in Release 12.2(18)SXF1, Release 12.2(18)SXE4, Release 12.2(18)SXD7, and Release 12.2(17d)SXB11.
- Release 12.2(18)SXF includes all fixes that are in Release 12.2(18)SXE3, Release 12.2(18)SXD6, and Release 12.2(17d)SXB10.
- If you have a Cisco.com account that supports access to the Bug Toolkit, you can search for the most current Release 12.2SX caveat information at this URL:

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

Open Caveats in Release 12.2(18)SXF and Rebuilds

Identifier	Technology	Description
CSCin96568	Infrastructure	FTS-7514-1: CISCO-PROCESS-MIB support for modular IOS
CSCsb92309	Infrastructure	reimplementation of cache_interface_state under CSCdw09607
CSCsf03710	Infrastructure	ION - Process and Mempool MIB - collapse of ion_mibs_all branch
CSCee25454	Unknown	SADB peering process leaks memory after overnight test

Resolved Caveats in Release 12.2(18)SXF17b

Resolved Infrastructure Caveats

- CSCti25339—Resolved in 12.2(18)SXF17b

  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 LegacyProtocols Caveats

- CSCtf74999—Resolved in 12.2(18)SXF17b

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

  Conditions: Cisco IOS devices configured for DLSw.

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

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

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

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

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

- CSCth69364—Resolved in 12.2(18)SXF17b

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

  Cisco has released free software updates that address this vulnerability.

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

Resolved WAN Caveats

- CSCtd75033—Resolved in 12.2(18)SXF17b

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

Further Description

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

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

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

Other Resolved Caveats in Resolved in 12.2(18)SXF17b

Identifier	Technology	Description
CSCsv82285	Unknown	Cat6k: UDP port 10000 is opened by default
CSCtd09117	Unknown	CSM config sync timing out

Resolved Caveats in Release 12.2(18)SXF17a

Resolved Multicast Caveats

- CSCtc68037—Resolved in 12.2(18)SXF17a

  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 Resolved Caveats in Resolved in 12.2(18)SXF17a

Identifier	Technology	Description
CSCei16552	Infrastructure	cannot remove snmp-server engineID from running-config
CSCsc33389	Infrastructure	When snmp-server host is deleted, the trap is not sent to other hosts
CSCsx32841	Infrastructure	ceImageDescription may exceed 255 characters

Identifier	Technology	Description
CSCsz72591	IPServices	Router configured as a DHCP client crashes with crafted DHCP packet.
CSCtc26840	IPServices	HSRP-CISCO-MIB snmpwalk results in "OID not incrementing" error
CSCsd91182	Security	crypto pki export pkcs12 hangs when used with SCP
CSCsx42304	Security	Traceback during SCP copy
CSCsc92676	Unknown	Rainier:Traffic captured even after vacl config is removed
CSCsu31088	Unknown	Not able to execute any commands under intf after running SPA FPGA bert

Resolved Caveats in Release 12.2(18)SXF17

Resolved Security Caveats

- CSCsh97579—Resolved in 12.2(18)SXF17

  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://www.cisco.com/en/US/products/csa/cisco-sa-20090923-tunnels.html.

- CSCsx70889—Resolved in 12.2(18)SXF17

  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://www.cisco.com/en/US/products/csa/cisco-sa-20090923-tunnels.html

- CSCsq31776—Resolved in 12.2(18)SXF17

  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://www.cisco.com/en/US/products/csa/cisco-sa-20090923-tunnels.html

Resolved Unknown Caveats

- CSCsy15227—Resolved in 12.2(18)SXF17

  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://www.cisco.com/en/US/products/csa/cisco-sa-20090923-auth-proxy.html

Other Resolved Caveats in Release 12.2(18)SXF17

Identifier	Technology	Description
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

Identifier	Technology	Description
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
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
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.
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
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

Identifier	Technology	Description
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
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
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

Identifier	Technology	Description
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"
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

Identifier	Technology	Description
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
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
CSCta12382	Unknown	Udld port config does not sync to standby in rpr-plus mode
CSCta12543	Unknown	Linecard takes MAC address from the linecard.
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
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
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)SXF16

Resolved AAA Caveats

- CSCsv73509—Resolved in 12.2(18)SXF16

  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)SXF16

  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)SXF16

  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://www.cisco.com/en/US/products/csr/cisco-sr-20090114-http.html

  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)SXF16

  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://www.cisco.com/en/US/products/csr/cisco-sr-20090114-http.html

  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)SXF16

  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://www.cisco.com/en/US/products/csa/cisco-sa-20090325-udp.html

- CSCsv04836—Resolved in 12.2(18)SXF16

  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://www.cisco.com/en/US/products/csa/cisco-sa-20090908-tcp24.html.

- CSCsw18636—Resolved in 12.2(18)SXF16

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

  Conditions: This problem occurs on SUP32 running 12.2(33)SXI. This problem does not occur on SUP720. The problem is only seen when you have bridge-group CLI being used which lead to arp pkts with protocol types as 0x1000 being bridged. The problem does not apply for IP ARP packets.

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

  Additional Information: This problem is now isolated to command ordering in the startup-config file. The **bridge <>** command is saved before the **bridge-group <>** command (which is run in the interface-config mode) is saved. The linking of IDB to bridge structure is not happening correctly and some check fails in the bridge code that lets the packet to be processed again and again instead of being dropped.

  If the **bridge-group <>** command is removed in the startup-config and only applied after the **bridge <>** command is run, the problem will go away. Please use this workaround until a fix is put in.

- CSCsr29468—Resolved in 12.2(18)SXF16

  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://www.cisco.com/en/US/products/csa/cisco-sa-20090325-tcp.html

- CSCsm27071—Resolved in 12.2(18)SXF16

  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://www.cisco.com/en/US/products/csa/cisco-sa-20090325-ip.html

Resolved LAN Caveats

- CSCsv05934—Resolved in 12.2(18)SXF16

  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://www.cisco.com/en/US/products/csr/cisco-sr-20081105-vtp.html

Resolved Multicast Caveats

- CSCso90058—Resolved in 12.2(18)SXF16

  Symptom: MSFC crashes with RedZone memory corruption.

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

  Workaround: None known at this time.

Resolved Routing Caveats

- CSCsx73770—Resolved in 12.2(18)SXF16

  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.

Other Resolved Caveats in Resolved in 12.2(18)SXF16

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
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
CSCso54027	IPServices	Spurious memory access in ttcp_rcv_stats

Identifier	Technology	Description
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 on GSR runing 12.0(33)S1 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.
CSCsr09312	Multicast	crash when doing mrm stop
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
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
CSCsi03434	Routing	Memory leak @ ospf_redist_work_enqueue
CSCsj09838	Routing	RR some prefix might not be sent after bgp neighbor flaps .

Identifier	Technology	Description
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
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
CSCsr67361	Routing	I/O memory leaks when BGP neighbor points to a local address
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
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
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
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 .

Identifier	Technology	Description
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
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
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

Identifier	Technology	Description
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
CSCsw35155	Unknown	reduce move count for SAs in SXF
CSCsw38075	Unknown	%SYS-2-GETBUF: Bad getbuffer error messages after IOS upgrade
CSCsw43953	Unknown	Error message seen if 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
CSCei77073	WAN	NTP client need to reset auto learnt source IP address

Resolved Caveats in Release 12.2(18)SXF15a

Identifier	Technology	Description
CSCsu45425	MPLS	FIB/LFIB not updated correctly on GSR runing 12.0(33)S1 after route-flap

Resolved Caveats in Release 12.2(18)SXF15

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

- CSCsk69927—Resolved in 12.2(18)SXF15

  Symptoms:

  All the BGP routes are dropped when IOS device receives BGP update with atomic-aggregate length as 254 (0xfe).

Conditions:

The topology consists of two eBGP peers with test traffic across the link. The BGP process does not crash, and routes are not restored after the event.

Workaround:

None.

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

- CSCsa49019—Resolved in 12.2(18)SXF15

  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.

Other Resolved Caveats in Release 12.2(18)SXF15

Identifier	Product	Component	Description
CSCsg18288	all	aaa	Enable authentication ignores Tacacs+ configuration in rare situation
CSCso95426	all	aaa	Exposure of Radius-Keys in debugs.
CSCei33231	all	atmcommon	ATM PVC bundle protected group test failed with bumping exhausted
CSCek74474	all	atmcommon	no/default proto ip inarp cmd ineffective until ATM VC bounced.
CSCsd92325	all	bgp	Config sync: no neighbor 192.168.240.34 triggers standby reset
CSCsf06946	all	bgp	Removing loopback interface causes continuous standby RP reloading
CSCsi27696	all	bgp	oldest ebgp bestpath not retained in eibgp multpath cases
CSCsi68795	all	bgp	PE wrongly assigns local label to a vpnv4 confederation prefix
CSCsi98730	all	bgp	CEF/BGP table MPLS label mismatch in IOS 12.4(6)T5
CSCsl92283	all	bgp	Unable to add into routing table if static route use interface + gateway
CSCso62166	all	bgp	Crash @ bgp_netlist_validate when ibgp established with metric
CSCso93535	all	bgp	Upon removing a VRF, BGP route timers in other VRF's get reset
CSCsq13938	all	bgp	reload on 'show ip bgp vpnv4' when import src delinked by BGP deconfig
CSCsq21198	all	bgp	PE loses VPNv4-MDTs from a RR when another RR fails (or shuts neighbor)
CSCsl04386	all	cat6000-env	%BIT-STDBY-4-OUTOFRANGE : Traceback on Bootup .
CSCse53517	all	cat6000-wireless	WiSM: Tracebacks seen after SSO switchover

Identifier	Product	Component	Description
CSCsm78651	all	csg	malloc memory issue in standby SP supervisor
CSCsi15183	all	eigrp	change MTU value causes %DUAL-3-INTERNAL in ipigrp2_add_item_dest
CSCsm70580	all	ftp	c2w2:ciscoFtpClientMIB: ftp_fs.proc extra processes can deadlock & crash
CSCsi76936	all	glbp	Crash in GLBP if debug is enabled and it rcvs pkt from unknown group
CSCsl70070	all	hsrp	CPUHOG when doing HSRP SNMP query
CSCsq29165	all	install	Rockies-sup3:UUT hangs during installation
CSCsm45634	all	ip	BGP VPNv4 route is not actived immediately after receving update
CSCsl60092	all	ipc	Active SP crashed @ipc_fragment_cleanup with VSL shut/no shut test
CSCsl92316	all	ipmulticast	LNS: %SYS-3-CPUHOG when clear l2tp tunnel, sessions have multicast
CSCsl26998	all	ip-pbr	Switch crashes on applying PBR with next-hop verify-availability
CSCsm04442	all	ip-rip	Router crash at rip_find_sum_idb
CSCeg35237	all	ipsec-core	Watchdog crash after sh crypto session
CSCsm13389	all	ipsec-routing	RRI is not called be if QM rekey timer expiry forces SA deletion
CSCsh38140	all	isis	CEF drops when using CEF LB paths and active link recovers from failure
CSCsm30973	all	mpls-lfib	bgp multipath with ipv4+label nexthop: label missing in cef
CSCso22730	all	mpls-lfib	Prefixes get assigned imp-null local label after OIR linecard
CSCsi77983	all	netflow-switch	RP crashed ipflow_pak_pre_check on shutdown the trunk port
CSCso87348	all	netflow-switch	Corruption in subflow code
CSCsm04256	all	neutrino	CPUHOG and crash after 'show memory detailed all statistics' issued
CSCsm69827	all	neutrino	%SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3
CSCsg32308	all	ntp	copy/paste of ntp-authentication-key statement is not possible
CSCek58956	all	os	Need process_ok_to_reschedule check in process_may_suspend
CSCsq50429	all	osm-qos	OSM card unexpected reload @ cwtlc_qos_create_global_qid_info
CSCsa73179	all	ospf	Memory corruption/crash when 'no default-information orig' under RIP
CSCsm91801	all	ospf	ASBR not updating metric in LSA-5 redistributing from 2-nd OSPF process
CSCsm01126	all	parser	PRE-B crashes while in progress to standby cold-config
CSCsj49293	all	pas-2pos-7xxx	POS Interface Output Rate (200 mbps) > Line rate (155 Mbps)
CSCsd14706	all	pim	PIMV2 router send PIMV1 RP-reachable messages loading recieve router CPU
CSCsq14151	all	pim	RPF of (S,G) is set to NULL, When (S, G, R) entry is convered to (S, G)
CSCsd62013	all	snmp	Traceback on Standby RP@add_lpmapping_entry_private+74
CSCsj91738	all	spa-ipsec-2g	Non-ip packet with mcast-mac addr cause high CPU with VPN-SPA VRF mode.
CSCso26788	all	ssh	Re-work CSCin91851 for SXF
CSCsr60782	all	ssh	Fix SA warnings in ssh2_support.c
CSCsr85093	all	ssh	SXF15: SSH session fails withRSA signature verification failed after SSO

Identifier	Product	Component	Description
CSCsq48201	all	trans-bridging	c7300:Bridge IRB-Router crash and traffic flow issue
CSCsi63649	all	ts	%SYS-3-TIMERNEG:Cannot start timer with negative offset,TTY Background
CSCsd37499	c12000	ifs	%IFS-3-FSMAX: Failed to add ?, maximum filesystems 64 msg with Traceback
CSCsq48271	c6venus-slb	laminar	adding redundant CSM causes config sync to indicate in sync when not
CSCsk32095	c7200	pas-2fast-ethernet	PA-2FE-TX port flaps on applying qos policy
CSCsq20970	c7500	7x00-t1e1	ATM option missing, while configuring T1 controller for mode atm
CSCsg22830	c7600	c7600-ha	Standby not coming up after sso switchover
CSCsj43677	c7600	c7600-ha	Active Sup720 crash when removing Standy supervisor
CSCsq19146	c7600	c7600-sip-200	FPD creation for new pegasus rx (1.6) FPA image for Sip-1 CR
CSCsm32363	c7600	cat6000-acl	Netflow SLB sw-installed entries not aging out
CSCek78066	c7600	cat6000-env	Whitney:CLI & MIB mismatch for aux-1 temperature Sensor SUP32
CSCsi41749	c7600	cs7	ITP-76:%SYS-2-INTSCHED: 'sleep for' at level 2 (Process- "MIP Mailbox")
CSCsq60553	c7600	cwpa2	Create cwslc-rommon3.bin for cwpa2 to accomodate release Rommon (1.8)
CSCsr99933	c7600	loadbal	FWLB: High purge rate causes CPU to increase by 15%
CSCsm87735	c7600	osm-choc-ds0	OSM CHOC12/T1 - t1 shutdown does not disable Serial interface
CSCso78097	c7600	osm-ct3	OSM-ct3 MFR interface is flapping
CSCsq47166	c7600	osm-gigwan	GE-WAN interface stays down with autonegotiation enabled
CSCso59971	c7600	osm-pos	OSM OC3 POS : Wrong traffic counters
CSCsq19159	c7600	snmp	RP crashes in chassismib_add_sub_card_entry after linecard reload
CSCsq19476	c7600	spa-ipsec-2g	DMVPN over POS - wrong spa vlan in cef adj after boot, gre sent in clear
CSCso89823	c7600	spa-pos-oc12	Pos interface "rxload" and "input bytes" counters incorrectly increment
CSCsc69804	c7600	vipmlp	SIP1-ChOC3:Initial packets fail with SW-MLP on SIP-200
CSCsq12119	c7600	vpn-sm	SXF13 Crash on VPNSM OIR due to chunk memory double free.
CSCsi00712	cat6000	c6k-wan-common	Connected ipv4 routes for WAN interfaces missing on reload
CSCsi99875	cat6000	c6k-wan-common	BOOM: spa_eeprom_read_bit on BOOTUP
CSCsg39754	cat6000	cat6000-acl	DHCP snooping redirect ACL permits more than just bootpc and bootps port
CSCso97524	cat6000	cat6000-acl	Packet drop after TCAM exception happened
CSCsf17163	cat6000	cat6000-cm	TCAM mask/entry resource not released after conf/unconf pacl
CSCsm53873	cat6000	cat6000-diag	Module 1/0 failed in health monitoring configuration (error code 23)
CSCsq53822	cat6000	cat6000-env	Monitor session removal may affect traffic through WS-X6148A-RJ-45
CSCsq47140	cat6000	cat6000-fabric	67xx module may not come online
CSCsr54630	cat6000	cat6000-fabric	Patch workaround and s222 build fix for CSCso53756
CSCso87838	cat6000	cat6000-filesys	HSRP: with aggressive timers HSRP peer flaps when "wr mem"
CSCsk93587	cat6000	cat6000-firmware	TestFabricCh0Health test failure with unidir traffic via Ch1on Berytos

Identifier	Product	Component	Description
CSCsl39710	cat6000	cat6000-firmware	cat6000 mac-address-table does not add entries for local fwsm mac . .
CSCsq14259	cat6000	cat6000-firmware	TX Flowcontrol goes on when link negotiation is disabled
CSCsq79253	cat6000	cat6000-firmware	Pinnacle interrupts not re-enabled after memory inconsistency detected
CSCsq85850	cat6000	cat6000-firmware	Opnext GLC-LH-SM :remote port stays up when local RX cable is removed
CSCsq41311	cat6000	cat6000-hw-fwding	I/O memory leak in Medium buffers
CSCsq77464	cat6000	cat6000-hw-fwding	mls rate-limit unicast cef receive value re-written upon TCAM exception
CSCsr28305	cat6000	cat6000-hw-fwding	Packet drops on L2 portchannel on WS-X6708-10G
CSCsl72912	cat6000	cat6000-ipc	VS2: WS-X6708 DFC crash in local_cb1(Segment violation)
CSCsr09554	cat6000	cat6000-ipc	Move SIBYTE SB_RMON_OVRFL messages under debug
CSCsu03772	cat6000	cat6000-l2	Dot1q native vlan tagging is not working with "switchpot nonegotiate"
CSCsq59297	cat6000	cat6000-l2-infra	port-channel IDB gets mixed up
CSCsh16213	cat6000	cat6000-mcast	Disabling MLDsnooping does not clean special MACs 3333.0000.0016, 3333.0
CSCsm59926	cat6000	cat6000-mcast	RP receives 2 copies of each PIM register with MVPN
CSCso44072	cat6000	cat6000-mcast	High CPU due to multicast traffic getting punted to software
CSCso71355	cat6000	cat6000-mcast	PVLAN - 6500 - Multicast flood broken from pvlan port to promiscuous
CSCsg19793	cat6000	cat6000-portsecur	Psecure absolute aging on DFC causes MAC inconsistency w/ Central EARL
CSCsq04355	cat6000	cat6000-span	Fix in CSCso81632 is not complete
CSCso85395	cat6000	cat6000-svc	Unable to add the 256th vlan
CSCso84567	cat6000	cat6000-wccp	6500 with WCCP and CoPP punts non-TCP packets into CoPP policy.
CSCsb60078	cat6000	cat6k-v6-mcast	After SSO switchover, mcast ergess Vlan gets out of sync among DFCs
CSCsj28026	cat6000	cat6k-vs-snmp	WhitneyVS: Unable to mibwalk clcFdbVlanInfoTable . .
CSCsq68529	cat6000	decnet	After reload, there is no mac-address on SVI not running DECnet
CSCso68344	cat6000	dhcp	Switch acting as DHCP server crashes on issuing no service dhcp command.
CSCsq37376	cat6000	elam	Packet Buffer Capture May Crash a 6500 in IOS
CSCsm82958	cat6000	loadbal	radius sticky entry deleted even if the idle timer is not 0
CSCso30038	cat6000	mcast-vpn	A OIL is not registerd properly in mroute table with static igmp group
CSCsl90285	cat6000	pas-pos	POS-APS: CWPA-3-NODISPATCH messages seen when configuring APS
CSCsi74360	cat6000	spa-ipsec-2g	packet loops between icpu and ocpu while sending clear mcast traffic
CSCsq39079	cat6000	spa-ipsec-2g	SPA-IPSEC-2G Crash under load due to IKE session establishment
CSCsq37078	cat6000	vipmlp	Input errors incrementing on Multilink 5 in admin down state
CSCso00793	itp	cwpa2	ITP-76: Flexwan Memory version "VI4DP647228EBK-MD" causes reload

Resolved Caveats in Release 12.2(18)SXF14

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

- CSCsk25697—Resolved in 12.2(18)SXF14

  Symptom:

  A router with DNS server configured may show CPUHOG tracebacks when it receives repeated crafted udp packets to its port 53.

  Sample for 3800 router:

  %SYS-3-CPUHOG: Task is running for (40004)msecs, more than (2000)msecs (5/0),process = DNS Server Input.

  -Traceback= 0x60D68CDC 0x6033D984 0x6180E58C FFFFFFA0 3F 4E 60 0x708DFD18 06 FFFFFFFE FFFFFF88 FFFFFFA5 FFFFFFA3 FFFFFF92 FFFFFFA7 FFFFFF8B 7A 3A FFFFFFF5 17 FFFFFF9B FFFFFFC9 FFFFFF9B FFFFFFA2

  Conditions:

  Router needs to have dns server configured and listen to udp port 53

  ```
  conf t
  ip dns server
  end
  ```

  Workaround:

  Apply rate limit to port 53 to interfaces facing untrusted networks:

  ```
  access-list 100 permit udp any any eq domain
  access-list 100 deny ip any any
  interface GigabitEthernet0/0
  ip address 10.2.2.2 255.255.255.0
  rate-limit input access-group 100 8000 1500 2000 conform-action transmit exceed-action
  drop
  ```

Resolved Caveats for Product 'cat6000' and Component 'cat6000-sw-fwding'

- CSCek49649—Resolved in 12.2(18)SXF14

  Symptom: 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

Further Problem Description:

None

Other Resolved Caveats in Release 12.2(18)SXF14

Identifier	Technology	Description
CSCdu79630	AAA	Username on vty not displayed if accounting is not configured
CSCsl57645	AAA	tacacs-server directed-request fails for enable authentication on 6500
CSCsj88665	Access	Bus error with PA-MC-2T3+ when deleting channel-group
CSCsm12247	Content	WCCP: hash assignment may be lost after service group change
CSCsk70446	Infrastructure	NRT: tracebacks @ data_inconsistency_error - 7200 for HTTP config .
CSCsl06515	Infrastructure	Sup720 Crash with 11 eFlexWan linecards
CSCso99219	Infrastructure	Match ip address with Named ACL not work in route-map
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
CSCsm36306	IPServices	NAT creates overlapping translation entries using the same IG address
CSCsm59037	IPServices	no service dhcp command causes switch to reload
CSCsk94676	LegacyProtocols	dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH
CSCsl78965	MPLS	High CPU in SNMP engine, mplsVpnVrfRouteEntry
CSCso47703	MPLS	Spurious Access error on rsvp_frr_event_lsp_down_psb
CSCek75931	Multicast	LNS: %SYS-3-CPUHOG When sessions have multicast
CSCsk26429	Multicast	Router configured for IGMP Proxy may not send IGMP Join
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
CSCse40966	PPP	MLP links down after SSO switchover if aaa new-model cfged
CSCsj60595	QoS	SIP-400 : offered rate in sh policy-map int is not accurate
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

Identifier	Technology	Description
CSCek47667	Routing	clear bgp ipv6 unicast * does not work .
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
CSCse65277	Routing	MU:default isis metric maximum returns parser error
CSCse85383	Routing	OSPFv3: Restructure link-state request list (CSCsd03021)
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
CSCsm43938	Routing	stby resets when large config/arp table to sync over to it
CSCso60089	Routing	7200: KBOOT image build failed
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
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
CSCef71952	Unknown	EzVPN server disconnects all PAT users of same IP address
CSCek74347	Unknown	Router crash after ip address slarp retry
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
CSCsd82457	Unknown	EOU Policy can't exempt Cisco 7935 Conference Station & Wireless phones
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
CSCsi52715	Unknown	PISA:SIP200 and FW2 reboots on SSO switchover
CSCsi97434	Unknown	A router may crash when ipsec is established
CSCsj25906	Unknown	Configuration changes made after scheduling a reload do not get saved
CSCsj48453	Unknown	AW: CAT6k does not forward multicast traffic to WISM in L3 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

Identifier	Technology	Description
CSCsk80552	Unknown	Shut and no shut of interface causes the delay in forming rp mapping
CSCsk82877	Unknown	METROPOLIS #0 cnt=1 reg:[1B0]kic_kic_int 02
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
CSCsl02812	Unknown	TCP SYN packet lost for web applications when NAT outside IF is ATM
CSCsl18958	Unknown	IOS-SLB: Multicast packets are droped in SUP22 when FWLB is operational
CSCsl32344	Unknown	Group of 4 ports on 6708 stops passing traffic
CSCsl52748	Unknown	SUP32 crash in tyfib_get_hw_index
CSCsl71339	Unknown	Prevent ssa interrupts from corrupting sfp i2c accesses
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
CSCsl94393	Unknown	OPNEXT / Sup32 uplink port stays up when far-end port down.
CSCsl98238	Unknown	QoS statistics-export only exports to directly-connected destinations
CSCsm11898	Unknown	IOS:SLB: Incorrect NAT Translation when Nat client is enabled
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
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
CSCsm59039	Unknown	Message "ME_AR#0 WARNING: Cannot FLUSH Dic#0" seen for WS-X6708A-10 LC
CSCsm69112	Unknown	Multicast output drop w/ IGMP snooping @ near line rate 1Gbps
CSCsm70774	Unknown	Router crashes at cfg_kron_plcy_sbmd_cmd.
CSCsm73173	Unknown	Spurious memory access seen @ slb_lam_cfg_ft_track_interf
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
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
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

Identifier	Technology	Description
CSCsm99170	Unknown	Memory Leak seen in fw_lcp process
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.
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
CSCso53741	Unknown	VPNSPA does not handle duplicate IPSec SA correctly in nested tunnel
CSCso81945	Unknown	removing natpool doesn't remove from the slb-policy automatically
CSCso89550	Unknown	cat6k crash due to SP: Supervisor has bad local fabric channel
CSCsq00884	Unknown	"mls qos trust" cmd lost under port-channel interface when upgrading IOS

Resolved Caveats in Release 12.2(18)SXF13

Resolved Infrastructure Caveats

- CSCsk33054—Resolved in 12.2(18)SXF13

  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://www.cisco.com/en/US/products/csr/cisco-sr-20070912-regexp.html

Resolved Security Caveats

- CSCsi17158—Resolved in 12.2(18)SXF13

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

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

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

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

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

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

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

Resolved Unknown Caveats

- CSCsg35077—Resolved in 12.2(18)SXF13

  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.

Other Resolved Caveats in Release 12.2(18)SXF13

Identifier	Technology	Description
CSCee89849	AAA	Router reloaded at vtemplate_build_command_strings
CSCsc98046	AAA	TACACS Accounting isn't sending stop time in the stop packet.

Identifier	Technology	Description
CSCsf30451	AAA	radius-server attrib 32 include-in-access-req/accounting-req not sent
CSCsh46990	AAA	Console hangs with enable/line as aaa fall-back methods
CSCsl33966	AAA	C6509 : attribute 32 nas-Id not sent for Auth (missed by CSCsf30451) .
CSCsm06740	AAA	Memory Leak in AAA accounting and Virtual Exec
CSCsl41784	Access	ION: ARP Input memory leak with "mobile ip arp"
CSCsd84347	ATM	PVC stops sending OAM loopback if AIS/RDI received
CSCse13374	ATM	IMA ports on 7600 always initialized to default clocking on bootup .
CSCsl65335	Content	WCCP: reload following ACL update
CSCsa65031	Infrastructure	show rtr distriution-statistics inactive status
CSCsb66972	Infrastructure	show memory shows negative numbers with 4GB RAM
CSCsh42866	Infrastructure	Static analysis on SNMP code
CSCsi15080	Infrastructure	RP crash when listing files by using the context-sensitive help
CSCsj83966	Infrastructure	Syslog traps cause CPUHOG when lot of interface come up at same time. .
CSCsk06492	Infrastructure	snmp-server drop vrf-traffic implementation in 12.2 SRB train
CSCsk37278	Infrastructure	BFD clients flaps when boot string is removed from "show running" .
CSCsg60447	IPServices	7200: BVI stops receiving CLNS/ISIS packets
CSCsh58099	IPServices	ftp process should call a registry cleanup- Message Could not register..
CSCsj29841	IPServices	Port forwarding breaks NAT-overload on a 6509
CSCsk29013	IPServices	IGMP groups in the vrf not rejoined after executing a cle ip mr vrf
CSCsk39022	IPServices	Modular IOS: ip directed-broadcast not working
CSCsl10348	IPServices	Crash writing to or from ftp/tftp server in modular IOS
CSCsl36293	IPServices	Bus Error crash at standby_arp_add_if while config-change .
CSCsm54171	IPServices	Crash seen with "copy runn tftp" and large hostname in modular IOS
CSCsh34949	LegacyProtocols	DLSW router crash with Bus Error
CSCdy83805	MPLS	%MPLS_TE-3-CONSISTENCY: consider replacing errmsg with buginf
CSCsa70235	MPLS	LDP doesnt withdraw all labels after routes gone
CSCsd55004	MPLS	FRR path gets reoptimized while in Active state
CSCsk30567	MPLS	local label for inter-as vpn not programmed on LC Eng 5 on an ASBR .
CSCsk36276	MPLS	SXF11: on SSO switchover tracebacks are seen at network_redist_ndb_updat
CSCsk55768	MPLS	TAG adj doesn't recover after flap
CSCsl72702	MPLS	MPLS should not allocate labels on standby RP in HA setup
CSCeg85087	Multicast	S,G expire timer set to 3:00 when no downstream pim join
CSCsg95192	Multicast	no ip rp-address <ACL name> causes an address error
CSCsh56720	Multicast	CPUHOG/Watchdog timeout when using igmp static group class-map cmd
CSCsh78277	Multicast	Sierra: mwheel CPUhog on RPF link failure causing crash .
CSCsl20422	platform-76xx	PXF points incorrect adjacency
CSCsl27840	PPP	Router may Crash / Hang, Module Reset @ Shut ATM member + MLPOA

Identifier	Technology	Description
CSCse18146	QoS	SIP1-CT3: SIP1 crashed after switchover @giant_node_process .
CSCsi73132	QoS	Multicast DSCP value not copied to PIM-SM RP-register packet
CSCsk53642	QoS	RSVP PATH msg not forwarded to MCAST receiver .
CSCsk63794	QoS	FlexWAN WS-X6582-2PA + T3+ Serial PA may crash/reload
CSCsk79703	QoS	SIP-200 crashes when moving MFR bundle from OSM to SIP-200
CSCsl70734	QoS	Commiting CSCsk53642 broke build.
CSCee04303	Routing	Spurius Memory access during boot while processing an isis update
CSCeg25475	Routing	Distribute-list configured in ipv4 acts in vpnv4 address-family
CSCsf00171	Routing	summary route not flushed from ospf database
CSCsh82953	Routing	EIGRP pece routes missing extcomm attrs after redistribution to BGP .
CSCsi80057	Routing	RIP default-information originate with route-map not working correctly .
CSCsj78403	Routing	clear ip bgp causes crash to RR client with conditional route injection
CSCsj99269	Routing	BGP: VPNv4 general scanner runtime close to 1 hour at boot time .
CSCsk34344	Routing	Wrong share-count 1:10 via confed-external BGP peers using dmzlink-bw
CSCsk70844	Routing	%SYS-4-REGEXP: new engine: regexp compilation had failed -BGP Router
CSCsl07297	Routing	SXF11: BGP "no neighbor" command caused Address Error exception .
CSCsl47915	Routing	Redistribution of ospf in rip with prefix-list not working properly
CSCsm17391	Routing	ISIS routes are not learned through interfaces
CSCsm27979	Routing	router may crash for "address error exception" doing sh ip route vrf
CSCsg48392	Security	Resuming SSH Session Fails After Disconnecting Another One (Not Console)
CSCsj45031	Security	Cat6k unable to SCP files from Tectia ssh server
CSCsm22805	Security	hsrp crypto map config got removed after reload
CSCsm32840	Security	Router crash in dmvpn-vrf setup after cheronia reset
CSCeb69473	Unknown	connect '/terminal-type' command memory corruption
CSCee13737	Unknown	CSM - sho mod csm # sticky reports invalid # of connections
CSCei28317	Unknown	PIM-6-INVALID_RP_JOIN reports 0.0.0.0 for source of invalid neighbor
CSCei49932	Unknown	Out-Discard counter showing value of zero on WS-X6148-GE-TX
CSCek45036	Unknown	Interuppt throttling to be implemented for Sibyte Modular IOS images.
CSCek55870	Unknown	fabric buffer-reserve queue default issues
CSCek76062	Unknown	Router crashed @ validmem_complete_interrupt .
CSCin67287	Unknown	NxDS0 BERT capability on PA-MC-8TE1+
CSCin89549	Unknown	Router crashes if AAA returns ipv4 address attrib with no xauth
CSCsb36463	Unknown	RF-bit not set in the DBUS hdr for the FS switched+RTD port snooped pkt
CSCsc56179	Unknown	mac-address is not purge when interface is shutdown .
CSCsd18278	Unknown	Host backpressure is not handled by SPA IPC firmware code
CSCsd66406	Unknown	SP error msg is not printed part of syslog levels
CSCsd90173	Unknown	TestIPSecEncrypDecrypPkt HM test config init error reporting is needed

Identifier	Technology	Description
CSCse31973	Unknown	NF double counts packets when span is configured.
CSCsf32441	Unknown	ALIGN-3-CORRECT: messages from process_t1e1s
CSCsg27123	Unknown	Learning not disabled on SPAN dest without learning option
CSCsg29305	Unknown	hw-module subslot reload crashes the router .
CSCsh17328	Unknown	WS-SVC-WISM-1-K9 reports 0.0 in entPhysicalVendorType
CSCsh23961	Unknown	Multicast netflow not working for Vlan interface (SVI)
CSCsh64639	Unknown	VS2: [dead threads] process takes a large chunk of CPU util
CSCsh83109	Unknown	HapiEchoTest fails on SPA-IPSEC-2G when reset.
CSCsh84657	Unknown	STP Loopguard: Ability to disable loopguard for Po270 and higher for FWM
CSCsh85531	Unknown	E1 channels down after PE reload
CSCsh88532	Unknown	Auto-LAG EtherChannel not configurable; doesn't trust QoS. .
CSCsh97395	Unknown	IDSM: Monitor config was removed after RPR switchover
CSCsi00706	Unknown	Sierra: upon fib tcam exception to use ratelimiter and not reload
CSCsi52382	Unknown	radius attribute 5 nas-port not sent in access-request for RA VPN users
CSCsi74194	Unknown	18SXF: Egress SPAN may cause high CPU
CSCsi79991	Unknown	VACL capture not supported for the GE-WAN or GigabitEthernet on SIP-400
CSCsi98587	Unknown	Excessive MET refs and memleak after ipv4 stress, crash follows .
CSCsj00385	Unknown	logging event link-status default negates existing interface config
CSCsj07935	Unknown	%CONST_DIAG-SP-2-HM_MOD_RESET:Failed TestFabricCh0Health .
CSCsj10375	Unknown	802.1X: VLAN Changing on port causes link to go down
CSCsj27352	Unknown	RX Priority q-limit is set to default after reload
CSCsj37078	Unknown	permit missing for internal vlan acl - causing vrf connectivity failure
CSCsj72438	Unknown	Control plane instability and %EARL-DFC3-2-SWITCH_BUS_IDLE: Switching bu
CSCsj83102	Unknown	crash upon card type configuration on WS-X6582-2PA / PA-MC-8TE1+
CSCsk30146	Unknown	Router crashed %DUMPER-3-PROCINFO: pid = 12315: (sbin/ios-base) SIGBUS
CSCsk40931	Unknown	Port Security Inactivity Aging is not working as expected
CSCsk41134	Unknown	ISAKMP SA neg not successful for in tunnel mode w/ RSA-SIG
CSCsk55423	Unknown	7600's SPD implementation allow COS 5 or above in Extended headroom
CSCsk58040	Unknown	WS-X6148A-GE-45AF retains previous modules MACs after OIR
CSCsk77164	Unknown	Connectivity problems to addresses switched based on aggregate label
CSCsk84237	Unknown	SIGSEGV, Segmentation violation in rf_proxy_fatal_error . .
CSCsk84944	Unknown	unidirectional Ethernet UDE is broken on WS-6704 after SW upgrade
CSCsk91267	Unknown	Module fails to come up with (FRU-power failed)
CSCsl00130	Unknown	GRE tunnel not HW accelerated after reboot when source from HSRP address
CSCsl08912	Unknown	Vlan access list not working when have "xconnect vfi #" under the SVI
CSCsl08952	Unknown	rapid link changes causes memory leak on sup32 int with service policy
CSCsl12827	Unknown	Handling Transit IpSec in VRF mode

Identifier	Technology	Description
CSCsl18765	Unknown	6500-7600 : SPAN of EoMPLS port causes packet reflection or loop
CSCsl19708	Unknown	Naxos : Disable Telesto Internal TERMINATION For Reference Clock, PB RAM
CSCsl21106	Unknown	Tunnel destination command crashes MSFC running in hybrid mode .
CSCsl26033	Unknown	Modifying the BFG doesn't re-create the SA's
CSCsl26997	Unknown	Catalyst 6500 may crash when reseting VPNSM module .
CSCsl27236	Unknown	%SYS-3-CPUHOG: Task is running for (126000)msecs, causes RP crash .
CSCsl30750	Unknown	Memory leak after create-apply-remove-delete policies on QM Process RP
CSCsl32122	Unknown	Remote Access for certificate users fails during mode config
CSCsl34647	Unknown	18SXF: RPR RF Keep alive swover not working
CSCsl49734	Unknown	IF_INDEX_ILLEGAL errors and crash due to memory corruption on standby RP
CSCsl51380	Unknown	Sup720 and Sup32 TCAM & SSRAM Consistency Checkers refinement
CSCsl52092	Unknown	DHCP db agent considers port-channel interface (poX) as invalid
CSCsl53494	Unknown	C7600-SSC-400: Error message display incorrect product name
CSCsl59553	Unknown	SIP-400: bursty traffic causes packet drop even in low rates
CSCsl61086	Unknown	urpf global disable even some intf with urpf
CSCsl63311	Unknown	6500 May Experience High CPU due to NAT traffic
CSCsl68327	Unknown	Packet loss during rekey
CSCsl70148	Unknown	PIM enabled p2p Crypto GRE Tunnels not installed in Hardware
CSCsl70634	Unknown	67xx EC tx/rx traffic dependency resulting in low throughput
CSCsl75136	Unknown	Cat6k with Sup32 failed to boot up after power cycle.
CSCsl75719	Unknown	sxf13 show int tunnel with blank display
CSCsl83211	Unknown	Sup32 running ION image fails to bootup after a power-cycle.
CSCsl84317	Unknown	Active crashes on applying acl to EoMPLS subif on SIP-600
CSCsl89069	Unknown	Zamboni crashed at illegal event/state combinationin CfgMonInd, clear sa
CSCsl89176	Unknown	Cat6k may crash when vlanTrunkPortEntry is polled via snmp
CSCsl97653	Unknown	bcm2_5421_isr bcm2_num: 1 messages seen in the log
CSCsm01129	Unknown	Back-out the ubins commit done in CSCse31973
CSCsm01399	Unknown	Bus idle recovery may cause 10GE interface to remain down
CSCsm05486	Unknown	mtu mis probram in adj thru tunnel interface after b2b failover
CSCsm08419	Unknown	debounce timer issue on sup32 10GE uplink and 6708
CSCsm15350	Unknown	vpnspa crashed at assert failure in l2-mcpu.c on line
CSCsm17983	Unknown	Memory corruption by l3_mgr_e7_fmask_init_platform
CSCsm21126	Unknown	C7600-SSC-400: Resync fabric interface on fabric error
CSCsm32493	Unknown	Backout of CSCsh94882
CSCsm35364	Unknown	SPA-IPSEC-2G get reload automatically by RP
CSCsm67778	Unknown	To make CSCsl68327 patch friendly and restore the symbols
CSCsj68446	WAN	NTP will not sync - NTP packets received but ignored by NTP process .

Resolved Caveats in Release 12.2(18)SXF12a

Identifier	Product	Component	Description
CSCsm06740	all	aaa	Memory Leak in AAA accounting and Virtual Exec

Resolved Caveats in Release 12.2(18)SXF12

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

- CSCsj91123—Resolved in 12.2(18)SXF12

  Symptom:

  Double freeing of freed memory. Router reloads after authentication attempt fails on vty/console.

  Conditions:

  While performing aaa accounting, the accounting structure was freed twice. Which results in crash. The below CLI is configured **"aaa accounting send stop-record authentication failure"** which sends a stop record for authentication failure.

  Workaround:

  Remove **"aaa accounting send stop-record authentication failure"** , which will disable sending of the stop record at authentication failure.

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

- CSCsk73104—Resolved in 12.2(18)SXF12

  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)SXF12

  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.

Other Resolved Caveats in Release 12.2(18)SXF12

Identifier	Product	Component	Description
CSCsj89305	all	aaa	RADIUS/NAS-IP address is sent out as 0.0.0.0
CSCse20115	all	ata-filesystem	System hangs when writing to a file, when the disk space is full
CSCek61180	all	atmcommon	crash @ write_to_url, doprintc_core, atm_remove_vc
CSCsc75426	all	bgp	Crash when BGP sends update with bad attribute .
CSCsg16778	all	bgp	router may crash at bgp_update_nbrsoo after deleting BGP neighbor .

Identifier	Product	Component	Description
CSCsg55591	all	bgp	MPLS VPN Local label not allocated/programmed for sourced BGP network
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
CSCsa79984	all	comm-serv	CTRLC_ENBL should be cleared when line is reset
CSCsi58303	all	eigrp	eigrp resync peer graceful-restart repeatedly after reload .
CSCsj25940	all	eigrp	%SYS-2-NOTQ: unqueue didn't find 6433F698 in queue .
CSCsc38968	all	fr	Frame-relay EEK failure does not keep subinterface down
CSCsj84641	all	install	some patches failed to commit during install commit of 41 patches.
CSCek76776	all	ip	ip interface settings persistent after deleting/adding sub-interface
CSCsk46195	all	ip	Arp entry does not age out with private vlans and no ip sticky-arp
CSCsk26719	all	ip-acl	show ip access crash with per-user acl
CSCsk26973	all	ipsec-dmvpn	Memory leak in nhrp_cache_delete for incomplete cache entries
CSCsk21328	all	ipv6	6504 crashes in IPV6
CSCsk65482	all	loadbal	clear ip slb CLI is defined with wrong privilege level
CSCsf13044	all	mcast-vpn	MVPN: Bidir mroute OIF missing - pim joins not received from MDT tunnel
CSCej00319	all	mpls-ldp	RP Crash for E2 E3 E4 E4P interaction
CSCsk05059	all	mpls-lfib	NRT: traceback tfib_post_table_change_ tfib_ipfib_ ip_fib_table_
CSCsk52331	all	mpls-lfib	Xconnect configuration triggers entire fib table walk
CSCsb67427	all	mpls-vpn	Label not allocated for imported iBGP in ASBR/PE after flap 'mpls ip'
CSCeh56158	all	nat	NAT outside source translation fails for GRE packets .
CSCsd80770	all	netflow-switch	Netflow exports UDP packets with source port 0
CSCir01217	all	neutrino	name_svr.proc[64]: Could not register interest
CSCsj17820	all	nhrp	Hub crashes during unconfiguration due to program counter error
CSCek33384	all	ospf	Tunnels stay down after cutover at MPLS head test cases
CSCsl14632	all	ospf	SXF12:%LDP-5-NBRCHG: LDP Neighbor is down after SSO Switchover .
CSCef54653	all	ppp	Members inactive in a multilink bundle except the first member. .
CSCsd30719	all	ppp	A2A: Stdby sup crashes @ mlp_remove_link .
CSCek78675	all	qos	SIP200 crash at hqf_cwpa_pak_enqueue_local during qos test .
CSCsh91974	all	security	PIM CLI causes RP crash when issued under control-plane subconfig prompt
CSCsg39295	all	snmp	Syslog Displays Password if SCP or FTP Selected in CISCO-COPY-CONFIG-MIB
CSCsk61555	all	socket	Bus Error Exception in sock_tcp_directwakeup . .
CSCsk81396	all	socket	NAM process crash in 12.2SXF .
CSCsj60938	all	ssh	SCP with redirect option locks up console or VTY line .
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 .

Identifier	Product	Component	Description
CSCsj89544	all	tcp	TCP retransmissions get dropped below IP layer. .
CSCsk80935	all	udp	SXF12, SNMP response being broadcast .
CSCsh31782	all	vpn-sm	Bus error crash - show crypto isakmp sa
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
CSCsl06110	c7600	c7600-acl	DHCP snooping agent: parse failures when importing the DB
CSCsk89335	c7600	c7600-env	After SSO switchover, see 6K DC power supplies mismatched .
CSCsk06769	c7600	c7600-lcsw-bridge	shut on L2 int cause packets to loop back on T1 int causing traffic loss
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 .
CSCsj58538	c7600	ha-idb-sync	Lots of prowler/patriot interface go down for few second during sso swov
CSCsk66339	c7600	isis	ISIS fails remove native path from local RIB / del path from global RIB
CSCsk08765	c7600	osm-choc-ds0	Bus error when executing 'encapsulation frame-relay mfr' .
CSCsj76268	c7600	osm-ct3	Autosense LMI stops responding invalid lmi type on OSM-12CT3/T1
CSCsk19333	c7600	osm-gigwan	GE-WAN interface shows incorrect link state with ws-g5483 GBIC
CSCsk82821	c7600	tcp	The UUT not able to receive the Large ICMP message.
CSCsi51649	cat6000	cat6000-acl	RP crashes@fm_send_inband_install_message+21C in many cases with NAT
CSCsj60883	cat6000	cat6000-acl	Error msg. Unable to change flowmask to full-flow because Cx is configur
CSCsk21414	cat6000	cat6000-acl	NAC : Buffer leak in small buffer pool .
CSCsk34237	cat6000	cat6000-acl	Egress multicast replication broken due to wccp .
CSCsj68911	cat6000	cat6000-cm	DFC mem leak in SP Logger Proces when redundancy force-switchover issued
CSCsc98471	cat6000	cat6000-diag	show diagnostic sanity fails to check software modularity boot string .
CSCsk60874	cat6000	cat6000-diag	show tech needs 'show diagnostic results' and 'show diagnostic events' .
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
CSCsk33661	cat6000	cat6000-fabric	show platform hardware capacity should include LTL usage .
CSCsk83646	cat6000	cat6000-firmware	BX10 ports don't link-up after Centaurus resets . .
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 . .
CSCsk18206	cat6000	cat6000-hw-fwding	TCAM adjacency hardware programming problem with PBR and NAT .
CSCsk70087	cat6000	cat6000-hw-fwding	Sup720 TLB exception created by fill_earl_vlan_stats_hdr .
CSCsc75381	cat6000	cat6000-l2	Native vlan mismatch is not detected if native not allowed on trunk .
CSCsg50698	cat6000	cat6000-l2	18SXF: set entPhysicalAlias of XENPAK cause stdby-reset .
CSCsk33724	cat6000	cat6000-l2	DOM does not work anymore for cwdm gbic/sfp
CSCsh33518	cat6000	cat6000-l2-infra	STP information is not in sync with Active .
CSCsh97848	cat6000	cat6000-l2-infra	Sierra: LACP pdus should be untagged .
CSCsk83524	cat6000	cat6000-l2-infra	L3 physical interface input drop counter is incorrect .

Identifier	Product	Component	Description
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
CSCsk02962	cat6000	cat6000-mcast	Supervisor Reload after SSO switchover on Multicast MET reconstruction .
CSCsk03679	cat6000	cat6000-netflow	VS2: show mls nde intermittently causes ALIGN-3-SPURIOUS T/B's
CSCsd43185	cat6000	cat6000-qos	Tx queue cos maps for even ports of card WS-X6416-GBIC are incorrect.
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
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
CSCsg21809	cat6000	cat6000-statistics	Add bridge asic status collection support .
CSCsk24272	cat6000	cat6000-sw-fwding	SUP720-3B RP Crash due to I/O Buffer Leak by NDE w/ NAM 127.0.0.x Addr
CSCsj85485	cat6000	eigrp	EIGRP NSF - MSFC switchover causes hello's to be sent over passive intf
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 .
CSCek39186	cat6000	spa-ipsec-2g	MAC-address for HSRPs VIP not in FVRF vlan if tunnel redirected .
CSCsd92208	cat6000	spa-ipsec-2g	vlan map ocpu is wrong in the active vpnspa after sso+b2b failover .
CSCsk33740	cat6000	spa-ipsec-2g	replay window size of 1024 causes IPSec Policy Check and Replay Failure
CSCsl13477	cat6000	spa-ipsec-2g	SSO not working with crypto maps terminating at same peer address .
CSCsc77148	unknown	novell	Router crash while issuing show ipx cache command. Cleanup SA warnings.

Resolved Caveats in Release 12.2(18)SXF11

Identifier	Technology	Description
CSCsh23142	AAA	aaa local authentication not happening for authproxy .
CSCsh59019	AAA	Avoiding AAA client hangs, if a protocol subsystem is not present.
CSCsj97165	AAA	%AAA-3-BADMETHODERROR: Router crash @ aaa_get_new_acct_reg_type .
CSCsc57207	Access	itevent flooding: code 10 arg0 0 arg1 0 arg2 0 error messages on 7200
CSCsi00099	Access	Spurious Memory Access Error @ ct3sw_check_freedm_fifo
CSCsj37071	Access	PA-MC-E3 will not recover after workload stress
CSCed17607	ATM	Reapplying oam-pvc manage does not send oam cells until shut/no shut
CSCsj57084	ATM	Voice packets in LLQ experience latency
CSCsj78525	ATM	%ALIGN-3-CORRECT, %ALIGN-3-TRACE on the 7500 with 123-22
CSCeg88630	Infrastructure	E3 GE:Linkdown trap via snmp not properly raised
CSCei79855	Infrastructure	IOS resilience fails to work properly with secure boot command .
CSCek56630	Infrastructure	race condition in process_sleep_on_timer code

Identifier	Technology	Description
CSCsb95806	Infrastructure	Incorrect 64bit counter on 1Gb MPLS interface via SNMP .
CSCsg15939	Infrastructure	Switches crash after remove/plug in compact flash
CSCsg43466	Infrastructure	%IPC-5-INVALID: Invalid Dest Port w/ TB @ ipc_xmt_account after SSO
CSCsg71381	Infrastructure	Disabling cisco-specific lsa and tty, removea all ospf trapa from conf
CSCsh28948	Infrastructure	High CPU for sh run/wr mem with PTA sessions up
CSCsh48919	Infrastructure	Embedded spaces in DOSFS dirs/file names cause crash in some platforms
CSCsj58223	Infrastructure	Bus Error after 'show memory' .
CSCsj92874	Infrastructure	Catalyst 6500 May Not Send linkup/linkdown SNMP Traps and may reload
CSCsk10335	Infrastructure	Traceback @ ipc_send_message_blocked during bootup .
CSCsk38461	Infrastructure	Show platform hardware command getting rejected .
CSCeb76035	IPServices	Spurious access or crash from snmp_trap_for_tty
CSCeh65511	IPServices	Connected int IP may not be reachable with a static NAT trans
CSCsg97662	IPServices	Cant disable skinny (tcp 2000) .
CSCsi10974	IPServices	Error configuring dhcp option 67
CSCse13882	LegacyProtocols	Show dlsw peer caused router to crash
CSCsj98895	LegacyProtocols	v2-single-tcp peer connection is established on a non confg/prom peer
CSCsg88433	Management	IP Telephone issues seen with Dhcp snooping and NAC posture validation
CSCsk09197	MPLS	RSVP hello instance remains at shut-down interfaces
CSCek26940	Multicast	Need to unhide interval for send-rp-discovery
CSCsg24505	Multicast	PIM-DM Assert winner does not always send prune
CSCsi03359	Multicast	Sending extra PIM hello if the first one does not go through
CSCsj64230	Multicast	bidir DF election should not be restarted on a downstream interface
CSCsi98355	platform-76xx	LOP does not bring the line protocol down on OSM-1OC48-POS
CSCsj64023	platform-76xx	MPLS: Sup2 OSM sending TTL=0 packets on MPLS VPN
CSCsj93609	platform-76xx	Missing DS3-MIB table entries for OSM-1CHOC12/T3
CSCsj93636	platform-76xx	Incorrect value returned for dsx3TotalUASs
CSCse28421	PPP	%AAAA-3-BADSTR error when Multilink interface goes down .
CSCsd17641	QoS	SIP-400 QOS: after changing hier. policy, the policy no longer attaches
CSCee04271	Routing	eigrp does not send update of poisoned route to stub router
CSCee19119	Routing	IP installs route for PPP interfaces that did not complete IPCP
CSCee73221	Routing	Split Horizon is in effect on redistributed static routes .
CSCei93768	Routing	check heaps CHUNKBADMAGIC crash at BGP Router when remove dmzlink ba .
CSCek62005	Routing	ip prefix list deletes lists before sending notif (causing rtr crash
CSCsc73725	Routing	EIGRP packet pacing should have lower minimum value
CSCsc83742	Routing	BGP MAXPFX Sylog message does not include VRF tableid info
CSCsc98835	Routing	CPUHOG when access-list is modified causes OSPF and BGP session drops .
CSCsd11019	Routing	Rainier:After RPR-Plus switchover standby RP crashes

Identifier	Technology	Description
CSCsd74189	Routing	show ip bgp vpnv4 vrf NAME community-list NAME gives error mesg.
CSCsf05579	Routing	ISIS passive-interface default problem in IOS 12.2(18)SXF
CSCsg21418	Routing	Bus error related to CLNS fast switching
CSCsg40507	Routing	SIERRA:ISIS/BFD session doesnt come up after changing ip-addr of interf
CSCsg71797	Routing	bgp bestpath as-path multipath-relax - command crashes Supervisor card
CSCsg95101	Routing	ALIGN-3-SPURIOUS: Spurious memory access
CSCsh57509	Routing	RIPv2 does not delete redundant paths with different next hops .
CSCsh88825	Routing	bgp: advertisement-interval not nvgened for peer-groups
CSCsi11438	Routing	OSPF does not remove maxage LSAs and age goes to bigger than 16 bit
CSCsi14346	Routing	EIGRP: neighbor command missing in VRF.
CSCsi20281	Routing	Static route redistribution into RIP fails on ACL change
CSCsi25729	Routing	ISIS doesn't enable BFD except after micro reload
CSCsi57971	Routing	ISIS does not advertise prefix of passive interface
CSCsi58867	Routing	CPUHOG After show ip route static or show ip route connected
CSCsj06265	Routing	Switch crashes when doing clear ip ospf process
CSCsj17950	Routing	ISIS redistributed static routes might not be advertised
CSCsj72039	Routing	Prefix not in ISIS database if serial interface and passive
CSCsj77819	Routing	After SSO traffic is punted to the CPU for 20 seconds
CSCsk27685	Routing	FIB-DFC2-4-FIBMSG: Invalid message received On bootup .
CSCdz55178	Unknown	QoS profile name of more then 32 chars will crash the router .
CSCef82084	Unknown	Spurious memory access in pot1e1_tx_interrupt
CSCei76590	Unknown	Different wattage WS-CAC-4000W-US caused PSREDUNDANTMISMATCH output
CSCej02181	Unknown	SLB: cannot configure weight 0
CSCek66590	Unknown	C7600-SSC-400: Crash in show hw-m subslot x status volt
CSCek67701	Unknown	SPA-IPSEC-2G: Crashdump not getting saved on NMI .
CSCek68218	Unknown	sip-600 crashing with diagnostics error online_wan_diag_rp_request
CSCek72777	Unknown	%CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR for 7600 SIP card .
CSCin67370	Unknown	Changing ACL or the crypto map leaves it empty ident tree .
CSCsb29131	Unknown	show crypto ipsec sa identity detail causes system to reload
CSCsb62762	Unknown	Crash no vlan access-map test .
CSCsc28731	Unknown	chassisFanStatus is minorFault when one fan is present on WS-C6509-NEB-A
CSCsd13448	Unknown	IOS SLB custom udp probes don't support faildetect
CSCsd66276	Unknown	IDSM: monitor session dest config removed after two sso switchovers .
CSCsd77622	Unknown	show policy-map interface doesn't show drop counters .
CSCsd88768	Unknown	%SYS-2-BADSHARE: Bad refcount in datagram_done fix for PA-MCX-8TE1
CSCse17175	Unknown	Line down on some serilal interfaces for Chann STM-1 SMI PA
CSCse32876	Unknown	dot1x:cli missing for Ten Gig Ports for dot1x initialize/ reauthenticate

Identifier	Technology	Description
CSCse33420	Unknown	LACP: config for some other port-channel gets removed on bundling ports
CSCsf03730	Unknown	interface remains down even after E1 level local loopback on STM1
CSCsf17739	Unknown	Sup720 SVI does not show multicast traffic rate
CSCsf98341	Unknown	UDLD failed to receive PDU when linked to L3 port.
CSCsg09423	Unknown	IPSEC SAs dont recover after rekey with 3000 IKE SAs and PKI (RSA-Sig) .
CSCsg11616	Unknown	iprouting restart crashes Sup due to Block overrun at 5E64940 (red zone
CSCsg52355	Unknown	RHI Injected routes lost after SUP switchover
CSCsg52740	Unknown	OC48 OSM replicates same packet at line rate
CSCsg55315	Unknown	Packets duplicated out of Gig1/1 when SPAN Monitor session enabled
CSCsg72976	Unknown	CSM - need to add standby state to mib object slbRealServerState
CSCsg99914	Unknown	sip-200 power-cycles after BGP flap (not responding to keepalive)
CSCsh18773	Unknown	Incorrect link behavior with Xenpak
CSCsh33770	Unknown	contrl vlan not set; zamboni remains in initializing state .
CSCsh48983	Unknown	Sup720 GE uplink SFP port ->err-disable on reload of adj switch
CSCsh52941	Unknown	AUTHPROXY:CLI to increase the number of HTTP Proxy process
CSCsh53141	Unknown	IKE SA not getting deleted after clear crypto session
CSCsh80130	Unknown	Add warning/comments to interfaces when Auto Lag is used for interface
CSCsh92031	Unknown	Sierra: Standby RP crashed at auth_proxy_posture_clear_nacl
CSCsi09388	Unknown	VPNSM SA deleted by idle timeout
CSCsi10945	Unknown	Http Auth-proxy with OTP does not display token/SNK challange
CSCsi11874	Unknown	Sup720 DFC forwarding some packets to MSFC instead of hw switching
CSCsi22243	Unknown	Memory leak in *Dead* process due to HTTP Proxy Server
CSCsi24069	Unknown	Collect additional debug info for Modular IOS kernel crashes
CSCsi32655	Unknown	MOD CSG <#> config mode command applied to a running CSM clears config
CSCsi65363	Unknown	Not able to run to t1 loopback when using a PA-MC-T3 with flexwan
CSCsi76115	Unknown	r3:WiSM hw-module reset causes traceback. Cannot decode data descriptor
CSCsi87837	Unknown	IF-MIB does not support gig interfaces on SPA-IPSEC-2G
CSCsi90816	Unknown	show policy-map interface caused sup32 crash . .
CSCsi91324	Unknown	MCAST packet drop when other interface goes down on DFC
CSCsi93273	Unknown	Leak in Big buffer pool on SIP card with NetFlow-export version 9
CSCsi94863	Unknown	New xenpak background task .
CSCsi99234	Unknown	RP crash at validblock with %SYS-6-BLKINFO: Corrupted redzone blk
CSCsi99991	Unknown	When CMM is rebooted, FE goes into ErrDisabled state
CSCsj03722	Unknown	exit command is subject to authorization
CSCsj10744	Unknown	Input queue wedged with Inband Edit Packets on SIP-400
CSCsj11561	Unknown	Inconsistent MTU for Adj. entries used by MLS Netflow and MLS CEF
CSCsj14847	Unknown	crypto connect command dropped after reload on unchannelized 2CT3+ .

Identifier	Technology	Description
CSCsj18014	Unknown	Caller ID string received with extra characters
CSCsj18494	Unknown	Leak +MN to pfc to avoid flooding due to tx span .
CSCsj29583	Unknown	Add warning message to 12.2SXF when configuring PACL
CSCsj30109	Unknown	Cat6k with FlexWan & IPSEC AM making as unreachable BGP neighbors
CSCsj33042	Unknown	Cat6k crashes when unconfiguring vserver (CSM)
CSCsj34552	Unknown	ip address of vlan interface not programmed into spa-ipsec-2g
CSCsj35776	Unknown	Some of the VCs are INACTIVE after SPA OIR
CSCsj40286	Unknown	Interface counters stop working under heavy load
CSCsj42303	Unknown	6K installs ffff.ffff.ffff in CAM table under very specific conditions
CSCsj45951	Unknown	DOM Polling May Cause Link Flaps on Some Xenpak Transceivers .
CSCsj52192	Unknown	FE stays up when remote 'inline powered' is shutdown w/ 100Mbps/Full
CSCsj53663	Unknown	EEM: RP crashed at fh_fd_syslog_event_match
CSCsj56102	Unknown	Upgrade of DFC rommon fails in 12.2SX train IOS
CSCsj56703	Unknown	SSO failover causes RSTP forwarding and physical interfaces blocking .
CSCsj58287	Unknown	7600-SSC-400 crashes on reload
CSCsj61101	Unknown	FRR goes down after few mints when Explicit-null is enabled .
CSCsj64453	Unknown	HSRP support in protocol policing
CSCsj66829	Unknown	Switch crash with clear ip igmp snoop stat and show ip igmp snoop st
CSCsj67096	Unknown	Issue w/NATed traffic on PortChannel (WS-X6408 and WS-X6516) on Sup720
CSCsj68774	Unknown	SIP-600 SXF bus error in const_mpls_collect_imp_te_stats .
CSCsj72251	Unknown	BOOTP replies dropped if DHCP snooping is enabled
CSCsj73669	Unknown	Disable DOM hardware periodic updates (xenpaks/x2s)
CSCsj81067	Unknown	IPSec VPN SPA: OLD-CISCO-CHASSIS-MIB does not return cardType
CSCsj81502	Unknown	show pagp clis are not displaying the correct information .
CSCsj82051	Unknown	Cachelines not invalidated on ICPU in error case .
CSCsk09302	Unknown	CDP packets not received on WS-6704-10GE/CFC links with MLS QoS enabled
CSCsk12525	Unknown	Disabling 67xx line cards with DFC3C/DFC3CXL except WS-X6708-10GE
CSCsk16974	Unknown	Sup2 - Bus Asic #0 out of sync error .
CSCsk17205	Unknown	OSM:MFR LMI packets are not send out through the MFR i/f
CSCsk19590	Unknown	Mem Leak in IKE NODE causes router crash . .
CSCsk20887	Unknown	Packets are route cached on multilink bundle .
CSCsk28585	Unknown	stats is wrong for TE tunnel, right for physical interface for ip2tag .
CSCei22295	WAN	Traceback is seen at fr_svc_teardown_calls
CSCsb87686	WAN	Spurious Access when attempting to configure a connection on MFR bundle

Resolved Caveats in Release 12.2(18)SXF10a

- CSCsj92874—Catalyst 6500 May Not Send linkup/linkdown SNMP Traps and may reload

Resolved Caveats in Release 12.2(18)SXF10

Resolved IPServices Caveats

- CSCsh04686—Resolved in 12.2(18)SXF10

  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)SXF10

  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 Security Caveats

- CSCsg40567—Resolved in 12.2(18)SXF10

  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 Unknown Caveats

- CSCsi01470—Resolved in 12.2(18)SXF10

  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.

- CSCsi86396—Resolved in 12.2(18)SXF10

  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.

- CSCsi99869—Resolved in 12.2(18)SXF10

  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)SXF10

  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.

- CSCsg70474—Resolved in 12.2(18)SXF10

  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 Resolved Caveats in Release 12.2(18)SXF10

Identifier	Technology	Description
CSCse69002	AAA	Accounting of auth failure doesn't work with some switches
CSCsb23106	Access	7206vxr with NPE-G1 bus error crash when OIR PA-2T3+
CSCdv70135	ATM	ATM QoS classes can not be configured.
CSCek39364	ATM	CLI: HA Standby router reloads while unconfiguring atm bundle .
CSCsb26631	ATM	Memory leak - ATM_PVCTRAP process
CSCsb54857	ATM	ATM shaping parameters removed from ATM vc-class for IMA upon bootup

Identifier	Technology	Description
CSCsg30875	Content	wccp blocking telnet to router
CSCsh98343	Content	WCCP redirect-list and mask-acl merge results in wrong redirect info
CSCsi05906	Content	WCCP:appliance failover does not update TCAM adjacency
CSCef66939	Infrastructure	VRF aware SNMP may generate trap with incorrect address
CSCeh65692	Infrastructure	Align Spurious memory access errors .
CSCeh74715	Infrastructure	SNMPv1 should not send traps with counter64
CSCsd13491	Infrastructure	show memory statistics history displays wrong values in processor pool
CSCsd46517	Infrastructure	Huge Memory allocation on c1721 during snmpwalk .
CSCse98807	Infrastructure	Traceback, Process=SNMP Timers, %SCHED-3-STUCKMTMR during regression .
CSCsi22502	Infrastructure	installer imf.tar file not being zipped creates uninstallable image
CSCsi99930	Infrastructure	%Error opening slavedisk0:/<filename> (Cluster chain broken on file)
CSCek66164	IPServices	show command pipeline redirect into rcp crashes the router
CSCsd43344	IPServices	isis-nsf info doesnt sync with standby in SSO mode .
CSCsd87810	IPServices	IOS tftp server should not differentiate between / and backslash in path
CSCsh31939	IPServices	c2w1:ciscoFtpClientMIB:Get & Set opration cause process deadlock & crash
CSCsi29875	IPServices	3/27: SP: oir_rf_reload_self: icc_req_imm failed, node not booting
CSCsi45840	IPServices	ARP requests for HSRP virtual IP may fail after switchport cmd is used .
CSCsi77774	IPServices	On modular IOS,Telnet on VRF int is allowed irrespective of vrf-also key
CSCsi78162	LegacyProtocols	SNASw %DATACORRUPTION-1-DATAINCONSISTENCY messages
CSCsg05873	Management	Buffer leak with SNA Focalpoint PU consuming middle buffers with NMVTs
CSCse22161	QoS	RP pool Memory corruption SXF4 - checkheaps_process/validblock crash
CSCsi05251	QoS	bus error crash at get_rateinterval_from_service_policy at subint delete
CSCef34800	Routing	BGP changes to accept max value for MED attribute
CSCeg43753	Routing	Router crashes at bgp_vpnv4_revise_route_update - corrupt PC & Sig10 .
CSCeg58039	Routing	BGP: changing the max-paths value may cause a crash .
CSCsb63652	Routing	bgp aggregate-address results in high BGP Router process utilization .
CSCsb96034	Routing	Traffic down for too long after SSO switchover .
CSCsd41237	Routing	vrf import map is not working .
CSCsd52225	Routing	BGP soft-reconfiguration keeps the old next-hop
CSCsd72747	Routing	nssa summary to null0 disappears after 'clear ip ro *'
CSCse91962	Routing	prefix stays in BGP table with RD 0:0 even after vrf's RD is configured
CSCsf32449	Routing	Sup720 MVPN PE - Tunnel does not come back up after reload .
CSCsg14026	Routing	Routers/Switches forward traffic destined to Class E Addresses
CSCsg52336	Routing	Crash at ospf_flush_area_summary_lsa after 'no ip vrf' of unassigned vrf
CSCsh61119	Routing	High CPU due to ARP refresh triggered by Serial interface flap
CSCsh80008	Routing	BGP: soft reconfiguration inbound and neighbor weight has no effect
CSCsi45422	Routing	iprouting.iosproc process reloads when making changes to static routes

Identifier	Technology	Description
CSCsi62559	Routing	SPD classifies OSPF IP Precedence 0 as priority .
CSCsj23579	Routing	Invalid memory action (malloc) @ SSO Switchover .
CSCei07548	Security	ocsp response timestamps are mishandled
CSCei85164	Security	OCSP fails when timezone is configured
CSCsh37957	Security	IPsec MIB entries not populated, IKE entries seem OK
CSCei52830	Unknown	Banner command sync is broken by CSCin86483 .
CSCej32124	Unknown	no mls verify commands doesnt take effect on standby supervisor
CSCek37222	Unknown	FR-flat:classification is broken in class-default with random-detect .
CSCek54572	Unknown	crash at ace_create_cm_head_node .
CSCek57760	Unknown	IP MTU of GRE tunnel not used by SPA-IPSEC
CSCek68265	Unknown	Major alarm on active caused syst. shutdn instead of swover to stdby
CSCek75394	Unknown	High CPU after enabling MPLS on interface .
CSCek77954	Unknown	test platform firm get cu-sfp-phy print-reg <port> <reg-no> .
CSCsa75285	Unknown	WS-X6582-2PA crashing cisco7600 when booting up with PA-MC-STM-1SMI
CSCsb13358	Unknown	failaction gtp purge doesnt delete some gtp stickies when probe fail
CSCsb14543	Unknown	t/b pm_port_counters_lock on module reset of active supervisor
CSCsb57042	Unknown	%SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs
CSCsc11689	Unknown	Configure/Unconfigure PACL may cause memory leak.
CSCsc33080	Unknown	%PFINIT-SP-1-CONFIG_SYNC_FAIL_RETRY: Sync'ing the private configuration
CSCsc83961	Unknown	Both APS protect & working ports forwarding traffic
CSCsd33992	Unknown	%PM-SP-STDBY-3-INTERNALERROR: when boot up
CSCsd77207	Unknown	Bidir traffic changed from HW to SW switch after add 200 sub-inf quickly
CSCsd79536	Unknown	Standby RP crashes once at reload after installing set of patches .
CSCse54191	Unknown	CSM fails over when incorrect HSRP group fails
CSCse98369	Unknown	class-default bandwidth percent 100% - SPA ATM fails
CSCse98795	Unknown	bus error while printing access-list
CSCsf18752	Unknown	mls ip slb search wildcard rp breaks gtp slb if 2 sfarms are confgd
CSCsf23115	Unknown	SUP720 does not recognize FAN2 after one of fans failed. .
CSCsg06577	Unknown	'Desc ordr internal vlan allocation' brings up sup with major diag error
CSCsg07870	Unknown	crash seen on switchover at pf_redun_sync_port_asic_on_swover .
CSCsg16272	Unknown	Catalyst6500 LinkDown snmp trap does not generate while performing OIR .
CSCsg30355	Unknown	OIR of redundant sup w/ CatOS crash the Cat6500 System running IOS
CSCsg38231	Unknown	'crypto eng gre vpnblade' cmd does make the tunnels to be accelerated by
CSCsg55237	Unknown	L2 flooding stops when new MAC address entries are learnt
CSCsg92670	Unknown	7600 : MLS FIB frozen, Sanity Check of MLS FIB s/w structures failed
CSCsh20211	Unknown	'Complete' diags fail TestNetflowInlineRewrite test on Service Modules
CSCsh33128	Unknown	MMLS/MVPN: Partial SC internal vlan not included in (*,G)

Identifier	Technology	Description
CSCsh34872	Unknown	With mls mpls recirc configd primary internal vlan has vpn-num .
CSCsh36377	Unknown	crypto connect cmd not updated in standby RP for ATM subif .
CSCsh38728	Unknown	Show int displays half even if port is hard coded to full
CSCsh39318	Unknown	10K / PRE-2 crashes at %MROUTE-4-ROUTELIMIT
CSCsh49239	Unknown	After redundancy failover Mcast packets drop for 60-90sec on SUP uplink
CSCsh54951	Unknown	PBR: TCAM incorectly programmed when match statement is NOT used
CSCsh61061	Unknown	VPM-SM:ISAKMP Lifetimes do not replicate correctly in interchassis setup
CSCsh62565	Unknown	SSH keys regenerated every hour cause route flaps due to high CPU load
CSCsh68976	Unknown	memory leak at xcvr_idprom when executing show hw-module all tranceiver
CSCsh77220	Unknown	SSO failover causes certain configs being removed .
CSCsh94882	Unknown	Unity client not initiating mode config should be rejected
CSCsh98909	Unknown	VRRP traffic not hardware switched on Sup2/MSFC2
CSCsh99351	Unknown	Packet reflection on EoMPLS links
CSCsi00173	Unknown	Bus error at crypto_ipsec_unlock_peer .
CSCsi02885	Unknown	OSM-1CHOC12/T1-SI incrementing abort, interface administrativel
CSCsi12289	Unknown	FWSM Does Not Display Correct Timezone for DST
CSCsi15191	Unknown	BOM messages observed while activation of rollback on stndby supervisor
CSCsi16904	Unknown	VPN-SPA does not send ISAKMP packet with notification payload included
CSCsi40628	Unknown	Dual RSPAN session causes loop between 2 6500 chassis .
CSCsi41791	Unknown	Leak: SPA-IPSEC-2G crash-> No More Free Buffers ; SPA_IPSEC-3-PWRCYCLE .
CSCsi42270	Unknown	IOS-SLB Radius Server LB may not mark a real as failed
CSCsi42517	Unknown	SRB Crashes when upgrading from SXF to SRB with SLB stateful config
CSCsi52209	Unknown	7600-sip-600 crash at PXF-DFC1-2-FAULT: T0 OHB Exception: SLIP FIFO full
CSCsi60125	Unknown	Hosts receive TCP RST due to incorrect NAT translation on cat6k .
CSCsi64204	Unknown	SXF:SIP400:ATMSPA Noticeable delay in output of show int atm command
CSCsi69350	Unknown	Newly active crashed on upgrading rp rommon @ emt_call .
CSCsi76192	Unknown	r3:show wism status not populated until standby up after SSO
CSCsi90011	Unknown	User Auth after Machine Auth causes dot1x security violation
CSCsi91875	Unknown	Cat6k crashes when unconfiguring vserver during snmp poll
CSCsi97192	Unknown	Vrf Agg label is not programmed in vpn-cam, SP thinks it as Ipv6 Agg lab
CSCsi98993	Unknown	Block FPD for Intel SPROM based ATM SPAs
CSCsj01891	Unknown	%SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs
CSCsj04905	Unknown	IOS-SLB: FWLB sticky config not get removed
CSCsj16292	Unknown	DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCsj23211	Unknown	'Complete' diags fail TestNetflowInlineRewrite test on Service Modules
CSCsj27811	Unknown	EOBC buffer leak caused by CMM module .
CSCsj28277	Unknown	Sup720 ignores IGMPv3 report if first group in Exclude list is 224.0.0.x

Identifier	Technology	Description
CSCsj30444	Unknown	SUP-2 Router crashes after boot UP
CSCsj40706	Unknown	incorrect ifIndex from multi HC OID Get to various cards
CSCsj47546	Unknown	POS: RDI-P must not be sent when the interface detects PLM-P
CSCsj60722	Unknown	TestNetflowInlineRewrite: diag failure on bootup
CSCsi33554	WAN	Connected net for virtual-template is not created in vrf routing table

Resolved Caveats in Release 12.2(18)SXF9

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

- CSCsd95616—Resolved in Release 12.2(18)SXF9

  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://www.cisco.com/en/US/products/csa/cisco-sa-20080924-multicast.html.

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

- CSCse56501—Resolved in 12.2(18)SXF9

  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

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

- CSCsc19259—Resolved in 12.2(18)SXF9

  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)SXF9

  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 'c2800' and Component 'voice-xgcp'

- CSCsd81407—Resolved in 12.2(18)SXF9

  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)SXF9

  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 Resolved Caveats in Release 12.2(18)SXF9

Identifier	Product	Component	Description
CSCsh82746	all	7x00-t1e1	Input Errors Counter not incrementing properly with Runt Errors
CSCsb45696	all	802.1x	Crafted EAP Response Identity packet may cause device to reload
CSCef27578	all	aaa	The router crashes when test aaa stop CLI is issued
CSCsh74025	all	atmcommon	clns packets not being punted by an enhanced flexwan .

Identifier	Product	Component	Description
CSCsd32373	all	bgp	BGP does not flag multipath correctly, causing loadbalancing issues .
CSCse04220	all	bgp	Clearing IPv6 BGP sessions can cause crash .
CSCsi06948	all	bgp	Bus error when issuing BGP dampening related commands .
CSCsi58259	all	c7600-atom	EARL7 PFC EoMPLS: CE to CE connectivity is broken with ATM as core
CSCsb19159	all	cat6000-filesys	Command copy const_nvram:vlan.dat startup-config might crash switch .
CSCsh94940	all	cat6000-hw-fwding	Supervisor crash by memory corruption (BADFREEMAGIC) in free block .
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
CSCsi34572	all	dot1x-ios	PC does not get a new DHCP address for machine authentication dot1x
CSCeh78345	all	eventmgr	Ensure EEM policies close tty session properly upon exit.
CSCea53765	all	fib	Facility to periodically validate adjacency prefix against RIB
CSCsh76592	all	fib	Crash in mtrie_longest_match when VRF is removed from config
CSCsa72748	all	fr	router crash due to watchdog timeout on frame relay broadcast
CSCek55001	all	ifs	Dir /recursively with many directories crashes the router
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' .
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 .
CSCse44079	all	ipmulticast	Multicast UDL - High CPU in IGMP Input when UDL interface down .
CSCsd50828	all	ip-pbr	AS-path based redistribution fails
CSCsg42246	all	ip-rip	CPUHOG in IP Background, and router reload .
CSCsh57795	all	ip-rip	Removing 1 RIP neighbor removes all neighbors
CSCsh85355	all	ipsec-core	Address Error exception at crypto_ipsec_clear_peer_sas
CSCsg99872	all	ipsec-isakmp	VPNSM: IPSEC accounting (start/stop) not sent under some conditions
CSCsg47462	all	ip-tunnels	Address error crash at tunnel_ep_addr_compare
CSCsb07279	all	isis	Adding new on route-map which is redistributed by ISIS, is not seen
CSCsi41944	all	isis	Virtual Exec CPUHOG
CSCsd32192	all	mcast-switching	GRE Tunnel With Checksum Enabled Does Not Transmit Multicast Packets
CSCsd40153	all	mpls-ldp	Rainier: label is not advertise to downstream ldp neighbor after reload
CSCsf98345	all	mpls-ldp	vrf-interface down cause LDP peer reset
CSCsh83034	all	mpls-lfib	High CPU on Supervisor caused by FIB Control Task process
CSCsh82993	all	mpls-vpn	Aggregate label missing if static route exists for same network
CSCsc93633	all	nbar	Software bus error crash on 7206VXR w/12.3(14)T3 w/ NBAR configured
CSCsd59610	all	os	%SYS-4-REGEXP: new engine: regexp compilation had failed.

Identifier	Product	Component	Description
CSCsg42072	all	os	Virtual Exec sessions not freeing memory
CSCsi62514	all	os	SXF9: ION image not bootable ROCKIES3_INTEG_070423
CSCek70058	all	osm-qos	OSMs may crash due to memory corruption on applying certain qos config.
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
CSCsg92954	all	pas-chstm1	Poor Voice Quality over congested Links
CSCef89952	all	pim	Router crashes when state-refresh message is rcvd for non-dense grp .
CSCsd16043	all	pim	Auto-RP for multicast may prematurely expire the group to RP mappings .
CSCeg38418	all	pki	Router crash when OCSP server use key hash as id
CSCsd09892	all	qos	no fair-queue causing VIP crash .
CSCse94388	all	qos	SIP200 crash at dlfi_do_fragment on HQF with priority .
CSCsi01422	all	qos	Hierarchical Frame-Relay QoS does not work .
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.
CSCsh83559	all	remote-registry	Modular IOS: memory leak in xdr_reference
CSCse80032	all	snmp	Mediation Device cannot resync SNMP engine time after 7600 reload .
CSCse95758	all	snmp	Access Lists support for all CONFIG-COPY-MIB protocols under snmp-server
CSCsh79371	all	snmp	SNMP memory leak for Modular IOS on 12.2(18)SXF6 .
CSCsi08777	all	spa-ipsec-2g	Memory Leak seen in Chunk Manager process .
CSCsi42769	all	spa-ipsec-2g	VPNSPA crashes with large certificates (PKI) .
CSCsf32211	all	spa-pos-oc3-12	Input bytes counter continues incrementing when a line protocol is down
CSCsb74409	all	ssh	IOS ssh client blocks Virtual Exec / SSH Process
CSCse79611	all	ssh	SSH source-interface command not working
CSCse53090	all	tcl-bleeding	After console timeout, access can be done to standby console.
CSCed95187	all	tcp	IP ID field is predictable for connectionless RST packets .
CSCef13860	all	tcp	Invalid TCB pointer traceback on exiting from a CPU session
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 .
CSCsb86257	all	telnet	Named ACL configured on VTY in with VRF
CSCsd42600	all	telnet	%SYS-3-BAD_RESET alongwith SegV exception crash
CSCsh56081	all	trans-bridging	Spanning tree of vlan-bridge is operated incorrectly
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
CSCsh75069	all	udp	Input Queue Wedge with UDP Echo packets .

Identifier	Product	Component	Description
CSCsi23203	all	vipmlp	Remove service policy from T1 prior to adding it to the multilink bundle
CSCuk61773	all	wccp	WCCP: ignore redirect assignment messages with identical content
CSCsd76528	c10000	qos	Queues not released after deletion of mtch vlan for HQoS policies .
CSCsa46154	c12000	ip-pbr	12.0(27)S03.1118 Deleting 100 Route-Maps at a time forces failover to RP
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.
CSCsh74881	c6venus-slb	laminar	CSM with a pair of bridged vlans can cause a variable to not function
CSCsg79810	c7600	c7600-sip-400	The MPLS MTU is overruled by the ip mtu on ATM interface
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
CSCsi77083	c7600	osm-ucode	Fix for CSCsh21998 in v122_18_sxf_throttle is erroneous
CSCsh46565	c7600	qos	PWAN2 HQoS(LLQ): shape ave rate is not applied .
CSCsi48550	c7600	vipmlp	dMLP: account lost_frags& rx discards as bundle intf input error
CSCsd08468	cat6000	c7600-mpls	SP crash at %EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR due to invalid packets
CSCsg91545	cat6000	cat6000-acl	ACL TCAM inconsistency seen if ipv6 acl with 2k mask is used .
CSCsh76923	cat6000	cat6000-acl	Memory Corruption or bus error crash on cat6k running NAT .
CSCsf29400	cat6000	cat6000-cmm-voice	Native IOS Sup discards or filters ARP replies from CMM for ACT module
CSCsh49043	cat6000	cat6000-firmware	Output drops in Queue3 after changes in cos-map config on 6148A-GETX .
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
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
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
CSCsb85030	cat6000	cat6000-l2	lost connectivity after port security disabled/removed - packets drop
CSCsf20751	cat6000	cat6000-l2	FlowControl inconsistency between Po and gig interfaces after SW upgrade

Identifier	Product	Component	Description
CSCsh38443	cat6000	cat6000-l2	Removing associated vlan would trigger the mac-add to get purge every 5m
CSCsh98208	cat6000	cat6000-mcast	PIM Snooping strips out Prune List in a (*,g) Join (s,g) RPT prune msg .
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) : .
CSCsg47044	cat6000	cat6000-netflow	NDE is not exporting packets
CSCsf11787	cat6000	cat6000-oir	EARL bus idle error occurs when the switching bus stall occurs
CSCsg72678	cat6000	cat6000-oir	TCAM entries not displayed for DFC card after OIR .
CSCsh93083	cat6000	cat6000-routing	Hadware uRFP with ACL stops after reboot
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 .
CSCsh96773	cat6000	laminar	CSM FT : unable to track port-channel interfaces
CSCsi73534	cat6000	laminar	CSM: CSCsb84087 breaks config-Sync feature
CSCse34615	cat6000	loadbal	Radius Acct on-off messages are dropped by Vserver
CSCse56921	cat6000	loadbal	GTP SLB Reloads at the time of session/sticky creation in multiple vserv
CSCsb01373	cat6000	msfc-filesys	MSFC3: Free NVRAM space reduces every time config is written to memory
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
CSCsf25728	cat6000	sr-bridging	Unable to session to FWSM when source-bridge ring-group is configured
CSCsg38618	wism	wlc-infra	Session to a 24 bit address fails on WiSM

Resolved Caveats in Release 12.2(18)SXF8

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

- CSCsf28840—Resolved in 12.2(18)SXF8

  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 'ftp'

- CSCsg16908—Resolved in 12.2(18)SXF8

  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 'pki'

- CSCsd85587—Resolved in 12.2(18)SXF8

  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 'ssl'

- CSCsb12598—Resolved in 12.2(18)SXF8

  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 'cat6000' and Component 'osm-ucode'

- CSCsg40425—Resolved in 12.2(18)SXF8

  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.

Other Caveats Resolved in 12.2(18)SXF8

Identifier	Technology	Description
CSCsd49317	AAA	no tacacs-server administration causes router hang .
CSCsg43322	AAA	AAA: No free authorization/accounting lists for network
CSCsa91863	Access	PA-E3 may reports LOF on reload
CSCse06752	Access	LAM /32 cef entry shows unresolved
CSCdy11156	ATM	13E:12E:RP crashed while applying config on ATM-PA,mgd_timer_stop .

Identifier	Technology	Description
CSCea82222	Infrastructure	timeout login response is broken on TTY and VTY lines with no AAA
CSCek42751	Infrastructure	%Error opening system:/running-config (No such file or directory)
CSCek58966	Infrastructure	Remove IPSLA Feature CLI From Modular IOS
CSCek64188	Infrastructure	Fragmentation fix of CSCek64051 is incomplete
CSCek65370	Infrastructure	Disable IP SLA CLI/SNMP from modular ios image in SXF
CSCsc04397	Infrastructure	Spurious memory access made at Fcheck_interface_state
CSCsc09336	Infrastructure	fix memory leak in display_posix_memory_info ion_lib_show_memory.c .
CSCse56676	Infrastructure	Some SNMP notifications go to the wrong host
CSCsg22769	Infrastructure	CPU utilization goes beyond 99% due to dfs_disk1.proc. .
CSCsh23981	Infrastructure	IPC ISSU: First message to seat 0x2070000 not found .
CSCee30364	IPServices	ip ftp username not used after username was previously used in URI .
CSCek12203	IPServices	File system issues after unsuccessful FTP operation. .
CSCsb27868	IPServices	DHCP Relay should unicast offer/ack on unnum ethernet sub- int
CSCsc12899	IPServices	SSM Mapping configuration inside a VRF broken
CSCse05736	IPServices	A router running RCP can be reloaded with a specific packet .
CSCsg49987	IPServices	HSRP learned groups appear in SNMP MIB
CSCsh29830	IPServices	NAT: Clear IP NAT translation * creates hardware entry for RSHELL.
CSCsc68540	MPLS	mplsTeNotifyPrefix trap emitted instead of correct TE trap name
CSCsg44555	MPLS	7600 MPLS TE mid-point stuck at up/down and Juniper headend up/up
CSCsg86806	MPLS	Client over MPLS unable to ping interfaces
CSCsh58729	MPLS	crash while configuring multiple back up path tunnels
CSCsc25557	platform-76xx	PORT3: Router crashed in CWAN OIR Handler in attempt to lock a semaphore
CSCsg21429	platform-76xx	STM-16 interface in OSM line card flaps endlessly upon SUP switchover .
CSCsg40425	platform-76xx	OSM-1OC48-POS-SI+ keeping reset due to POSLC-3-SOP .
CSCsg87037	platform-76xx	ATM OSM has compatibility issue with 3rd vendor device
CSCsh41006	platform-76xx	change earl reset patch-limit crash disable test cmd to a config cmd
CSCse91675	PPP	SWMLP: all intf are going down w/46 byte pkt size 8links/bundles@LR trfc
CSCeh82893	QoS	PP:R3:SIP400:QOS: LLQ+police drop rate counters are broken
CSCek34117	QoS	SIP1+ATM(OC3 SPA): Crashed at hqf_walk_and_police_inline() .
CSCsd56696	QoS	A2A: FR Adaptive shaping is not accurate .
CSCef15420	Routing	router reload at ed_get_reuseintervals Part II
CSCef84062	Routing	Bus error in bpath_unlock due to null path .
CSCeg03019	Routing	cef not working between different tunnels .
CSCek48274	Routing	clear ip bgp soft in may not delete all the BGP prefix
CSCsa49922	Routing	EIGRP internal route remains in RT but not in topology table
CSCsb34032	Routing	ISIS: router exception at mgd_timer when un-config isis cmds
CSCsc46337	Routing	BGP peer doesnt have an Index, session will not establish .

Identifier	Technology	Description
CSCsc83821	Routing	ISIS: TLV 237 not found in database when isis metric is configured
CSCsd59023	Routing	RP Arping for adjacent next-hop bringing up PTA sessions with AAA .
CSCse24873	Routing	Default-information originate in BGP shouldnt be tied to peer group
CSCse34050	Routing	ISIS keep advertizing passive interface, even after doing shutdown
CSCsf20947	Routing	BGP 'neighbor default-originate' advertisement ignored after link flap.
CSCsf26043	Routing	Cat6k Selective Packet Discard not classify ISIS at high-priority
CSCsg11830	Routing	12.2(18)SX Default-information originate does not generate default route
CSCsg26492	Routing	Error: can not find acl. Abort - msg when removing permit entry in ACL .
CSCsg43140	Routing	Switch may crash due to bgp over vpn .
CSCsg46638	Routing	BGP does not send withdraw when distribute-list is configured
CSCsg55209	Routing	BGP paths increase, with same prefix and next-hop under soft-reconfig .
CSCsg65298	Routing	OSPF: connected network learnt via ospf after interface shutdown #2
CSCsb54378	Security	watchdog timeout crash when starting ssh session from the router .
CSCsd76601	Security	Resuming SSH Session Fails After Other Session Has Been Disconnected .
CSCsd92405	Security	router crashed by repeated SSL connection with malformed finished messag
CSCse40423	Security	With ATM, tunnel interfaces do not ping until a shut-noshut is done .
CSCec76468	Unknown	crash in show route-map when delete route-map during concurrent conf
CSCef56327	Unknown	PA-MC-STM1: Cannot set/keep clock source line in config
CSCeg02918	Unknown	Bus Error at auth_proxy_proc_profile
CSCeh54725	Unknown	MIB object go into loop during snmp query
CSCei09247	Unknown	Local serial link goes up/down when remote link is admin down
CSCei12353	Unknown	Flow End sysUpTime higher value than the Router sysUpTime
CSCek55639	Unknown	Failed to assert Physical Port Administrative State Down alarm
CSCek65022	Unknown	7600-SSC-400: SPA-IPSEC-2g EFC clock hardware issue .
CSCek66277	Unknown	Diagnostics test 18 TestAclDeny should be marked Disruptive .
CSCsa97042	Unknown	Secured port dropping traffic after applying & removing mac-filter
CSCsb64767	Unknown	Unconf/confg port of L2 Eth chnl stop Mcast Traffic fwding out the port
CSCsc08947	Unknown	6k IOS Autostate: L3 int up/up if last L2 port disabled while L3 is shut
CSCsc69076	Unknown	SIP1-ChOC3: Spurious access at swsb_delete on unconfig of T1 chnl group
CSCsc73699	Unknown	Bus error at ipflow_get_template_id with NetFlow v9 .
CSCsd19181	Unknown	Crypto connect command is dropped from serial interface after reload .
CSCsd74091	Unknown	Misc. fixes for GCE handling for standby as DFC
CSCsd98852	Unknown	EEM does not allow read from stdin
CSCse37364	Unknown	traceback @ hal_get_dist_job on toggling mmls
CSCse39956	Unknown	VPLS:UCODE:Replication broken when CW followed by NO_CW VC
CSCse49388	Unknown	Tunnel int fails to receive traffic when links of a diff tunnel shut .
CSCse65726	Unknown	command no tacacs-server admin resets router

Identifier	Technology	Description
CSCse66269	Unknown	ION free memory dropping during mcast failovers but no process leaking
CSCse84602	Unknown	Error messages from Standby Sup when configuring OSM card channelization
CSCse84695	Unknown	Standby supervisor may crash when configuring osm card past FREEDM limit
CSCse88708	Unknown	Early stop of Bert test on OSM-1CHOC12/T1-SI produces error
CSCse97422	Unknown	crash on sup720, when executing 'sh tech' with long regexpr .
CSCsf10605	Unknown	crypto session count incorrect after ungraceful disconnect
CSCsf31458	Unknown	R3Vail: SupW image - entPhysicalTable is not SSO aware. .
CSCsg01366	Unknown	CSM config sync cause stacks to run low and crash router
CSCsg02241	Unknown	SUP720/SUP32 NAT translates incorrectly
CSCsg02391	Unknown	PORT_SECURITY-SP-2-INELIGIBLE error after module reset
CSCsg03739	Unknown	cat6k with vpnsm several possible crypto ikmp leaks .
CSCsg07525	Unknown	Periodic (30sec) traffic loss/dup over dis port-cha due to wrong RBH
CSCsg08200	Unknown	JQL: Bootup diagn for LC detect major failure after RPR swover .
CSCsg08304	Unknown	JQL: UDLD failure detected on neighbor switch after RPR switchover .
CSCsg16425	Unknown	show ip slb reals command displays huge connections value
CSCsg24609	Unknown	Whitney: snmp CISCO-L2-CONTROL-MIB getmany errors .
CSCsg34141	Unknown	Secure mac learnt on non secure port creates a static entry
CSCsg35506	Unknown	JQL: port-channel member in suspend due to flowcontrol mismatch .
CSCsg37435	Unknown	ifIndex missing for 802.1Q vLAN subif after GigEth card OIR .
CSCsg40391	Unknown	Dot1x: Port config on authenticated port changed after linecard reset
CSCsg51230	Unknown	VS2: MLS multicast operating state is IDLE, after SSO switch over
CSCsg51724	Unknown	cbQosCMDropPkt stays at 0 while CLI counters shows positive values
CSCsg61773	Unknown	MMLS: Egress mode, OIF inconsistent between SP/RP, traffic blackholed
CSCsg62119	Unknown	Cat6K Spurious Memory access
CSCsg64170	Unknown	SSO switchover causes service module to appear down for 10-30 secs .
CSCsg64306	Unknown	%MCAST-SP-6-L2_HASH_BUCKET_COLLISION
CSCsg69489	Unknown	Reroute of LSP between two link with label constitutes to traffic loss .
CSCsg72398	Unknown	SLB:Packets getting process switched w/ multiple UDP Vservers
CSCsg73179	Unknown	bi-dir mls rp doesnt get updated after a change in topology .
CSCsg76239	Unknown	Fast Path mcast pkts hit RP cpu if ACL configured on OIF .
CSCsg77142	Unknown	Memory leak in Cat6k SNMP Trap process
CSCsg80948	Unknown	Uneven load-sharing for 4-path ECMP case
CSCsg90190	Unknown	Software does not limit 96 Ports LC inline Power based on HW Limitation
CSCsg97079	Unknown	18SXF7 ION image should also bundle FlexWan1
CSCsh01749	Unknown	mls qos marking ignore port-trust has no effect with EoMPLS configurat .
CSCsh05800	Unknown	Mcast egress replication - VDB is not updated on L3 PO subinterfaces
CSCsh07037	Unknown	OSM may crash with CHUNKBADMAGIC error, when WRED threshold is conf > 2k

Identifier	Technology	Description
CSCsh17979	Unknown	Ports PWR_DENY not enough system PWR/chassis BackPlane PWR (Not Real)
CSCsh20950	Unknown	18SXF8: PRBS support needs to be disabled on the Malabar8 module
CSCsh22835	Unknown	Major Error is seen with module 6 after swithover in rpr mode. .
CSCsh25976	Unknown	C2W1: SSO sync issue with PSFANINCOMPAT & PSFANFAIL sensor .
CSCsh29863	Unknown	New active crashes after switchover in rpr mode .
CSCsh31306	Unknown	T1 serial o/p drops / no QOS drops - flexwan - T1 multichannel PA.
CSCsh32199	Unknown	Input queue drop counter incrementing even when interface disconnected
CSCsh37008	Unknown	Need to enable Malabar8 in WS-C6509-NEB-A chassis with one fan .
CSCsh41192	Unknown	Memory leak in IPSEC key engine process .
CSCsh42914	Unknown	Cat6500 Netflow does not export all flows with sampled netflow
CSCsh44288	Unknown	Hybrid: Remove uRPF check w/ACL knob from hybrid IOS images
CSCsh48947	Unknown	PWR_DENY Port 47/48 on each LC max PWR support Backplane per LC or VDB
CSCsh54325	Unknown	SIP600/ES20 PXF punt path broken when sup slot is 1 or 2
CSCsh61396	Unknown	R3.8: Hydra module resets during to excessive LCP_FW_ERR Qchip msgs
CSCsh66367	Unknown	Wrong Ubin Images committed to v122_18_sxf_throttle on CSCsh61396
CSCsh85155	Unknown	mls adjacency has extra punt entry after FRR cutover .
CSCsb46223	Voice	Bus error crash at Tcl_DStringAppend

Resolved Caveats in Release 12.2(18)SXF7

Resolved LegacyProtocols Caveats

- CSCsf28840—Resolved in 12.2(18)SXF7

  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 Management Caveats

- CSCsf07847—Resolved in 12.2(18)SXF7

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

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

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

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

Other Caveats Resolved in 12.2(18)SXF7

Identifier	Technology	Description
CSCsa93523	Access	7200 PA-E3 incrementing carrier transitions and packet drops
CSCea26450	ATM	PVC may stay down when interface cable is pulled out/put back rapidly
CSCsd20327	Content	WCCP going up/down
CSCeh85133	Infrastructure	Memory leak in Syslog Traps process
CSCsd29469	Infrastructure	Cat6000 SNMP stops responding while polling from ciscoEnhancedMemPoolMIB
CSCsd49133	Infrastructure	Alarms are not pouplated in ceAlarmTable - ceAlarmList is empty.
CSCsg32222	Infrastructure	Need the support for 64 bit bit/second OID on Cat6k/7600
CSCsg70355	Infrastructure	adopt new default summer-time rules from Energy Policy Act of 2005.
CSCei93982	IPServices	Modified ALG classification base on src & dst port
CSCsc78813	IPServices	DNS reply payload does not get translated in the NAT router.
CSCsd51530	IPServices	autocommand-options nohangup is removed on line vty 0-4
CSCse04560	IPServices	tftp-server allows for information disclosure .
CSCdz80245	LAN	SNMP: Need ifDescr output without description
CSCsg01823	LegacyProtocols	DECnet mac-address (aa00.0400.###) missing from interface after reload
CSCsb52900	MPLS	mpls forwarding table label inconsistency after switchover
CSCse92050	Multicast	With mis-configuration, router may reload at twheel_running
CSCse11678	PPP	SIP: Ping fails after removal of primary link from multilink bundle.
CSCsg02881	PPP	MLP: Bandwidth of down MLP group should be sum of member bandwidths
CSCsd37025	QoS	CPUHOG and crash when removing nbar policy-map
CSCse25833	QoS	%SYS-2-CHUNKBADMAGIC every 10 sec with 12.2(18)SXF4
CSCsf11353	QoS	Autobahn:FW2 kept crash at hqf_dp_set_blt_quantum and dlfi_inform_config
CSCei29944	Routing	RP crashes at bgp_get_msg_count while sho ip bgp summ
CSCei32930	Routing	EBGP+label : soft-reconfig inbound broken
CSCsb50606	Routing	Leak in dead process due to TCBs from BGP active connections
CSCsc43989	Routing	CEF adjacency inconsistent with NHRP cache entry
CSCsd03383	Routing	OSPF:TE Tunnel route not installed if parallel path eq max-path
CSCsd53402	Routing	ABR delets OSPF summary route for 5sec after DR is changed
CSCsd74396	Routing	eigrp authenticaion fails with md5 enabled
CSCsd81600	Routing	OSPF Stub-links should advertise LSInfinity when max-metric configured
CSCse41484	Routing	DMVPN / VPN-SPA / few GRE packets not encrypted when negotiating the SAs
CSCse51804	Routing	DMVPN tunnels not stable; keeps flapping
CSCse89119	Routing	OSPF discard route (Null0) is disappeared from RIB when AD is changed
CSCsf99057	Routing	JQL: OSPF Stub-router should work with SSO/RPR-Plus if NSF is disabled
CSCsg16748	Routing	ABR deletes OSPF type 3 LSA after it received max-aged type 2 LSA
CSCsb47257	Security	bus error crash @ pki_add_to_obj_list
CSCsf05479	Security	Address error at gre_ipip_fastsend

Identifier	Technology	Description
CSCsg10671	Security	No message when CA re-enrollment fails
CSCdy47789	Unknown	Non-directed LDP neighbors showing up under targetted discovery list
CSCeg41330	Unknown	crypto isakmp client config max-logins is case sensitive
CSCeh95801	Unknown	IPSec Accounting: DN not sent in group-id with EzVPN + CERT
CSCei58681	Unknown	port channel does not form after minlinks added and removed
CSCej78221	Unknown	CSG Refund policy with more than 10 entries causes cat6K to crash
CSCej83614	Unknown	Multicast packets punted with deny acl on outgoing interface
CSCej86174	Unknown	Need a command to disable EOBC JAM recovery
CSCek54981	Unknown	Incorrect ICMP MTU proposal for outgoing ESP packets
CSCsc55951	Unknown	SPA-4XOC3-ATM has compatibility issue with 3rd vendor device
CSCsc64718	Unknown	persistent-store command not available on SUP32 Images
CSCsc69851	Unknown	Port Security does not show offending MAC address in syslog
CSCsd69480	Unknown	%HYPERION-4-HYP_RESET on flexwan2 chSTM1 card
CSCse00115	Unknown	mcast egress replication -- Wrong output interface index for msc
CSCse37587	Unknown	DHCP snooping in conjunction with VRF breaks DHCP
CSCse43709	Unknown	supw nmi support
CSCse63054	Unknown	Remove VLAN IDB from VRF if_list when releasing a rserved VLAN
CSCse75904	Unknown	VPNSM: periodic accounting is still sent for disconnected vpn users
CSCse87210	Unknown	Enable service cards to operate in crossbar mode with Dist Etherchannels
CSCse87618	Unknown	cRTP and Interleave doesnt work together on Virtual-Template Interface.
CSCse98692	Unknown	12.2SX code not showing int trust state in sh mls qos cmd
CSCsf03986	Unknown	spurious at fm_wccp_format_adj_entry after upgrade
CSCsf07232	Unknown	tclsh stdio operations do not output to current terminal
CSCsf08368	Unknown	Prevent NBAR configuration on non-FlexWAN interfaces
CSCsf10116	Unknown	Reflexive ACL not getting Sw Installed.
CSCsf11639	Unknown	WS-X6148-FE-SFP interface counter increments even if the link is down
CSCsf14994	Unknown	SIP1-ChOC3:Some of the MLP links wont ping, if deleted & configred again
CSCsf23326	Unknown	IOS SLB does not on 7600 with SXF4 if Client is behind MPLS cloud
CSCsg00845	Unknown	'no logging event link-status' is lost after reload
CSCsg02605	Unknown	Rapid reboot does not work
CSCsg03503	Unknown	NAt Netflow entries need to be purged on routing change
CSCsg07765	Unknown	Sierra: scp_fpoe_req: memory allocation error, subopcode=10, count=9
CSCsg17923	Unknown	IKE Notifiies (DPD, Deletes,...) not processed -- dropped
CSCsg23979	Unknown	Crashes in iprouting.iosproc produce no tracebacks
CSCsg25416	Unknown	flash information is missing from show hardware output in ION
CSCsg26450	Unknown	move enum value at the end of the list
CSCsg28959	Unknown	rwindex = 0xFFFF on the non PI causing all mcast traffic to be dropped

Identifier	Technology	Description
CSCsg36726	Unknown	Bonham parity errors may cause packet loss on a 7600-SIP-400 module.
CSCsg38092	Unknown	Pre-Pilot:EEPROM (feature_bits) needs to upate to no floating capable
CSCsg38930	Unknown	7600 SPA-IPSEC-2G - Multicast data is not forwarded through GRE Tunnel
CSCsg40401	Unknown	SUP32 unstable to communicate with all neighbors after reload.
CSCsg41552	Unknown	Module fails to come online first time after reset
CSCsg58917	Unknown	mls ip cef load-sharing and mls ip cef rate-limit missing in Sup22
CSCsg62154	Unknown	18SXF7: ltl_alloc_index_at: T/Bs are seen after multiple switchover
CSCuk57037	Unknown	IGMP: crash at at ../ipmulticast/igmp.c:3162
CSCsc50986	WAN	NTP unsynchronizes when packets out of order at STEP
CSCsd19880	WAN	ATM pvc does not come up with new style legacy command
CSCse55004	WAN	NTP clients wont associate

Resolved Caveats in Release 12.2(18)SXF6

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

- CSCsf12082—Resolved in Release 12.2(18)SXF6

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

  OSPF and MPLS VPNs are not enabled by default.

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

Resolved 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

Other Resolved Caveats in Release 12.2(18)SXF6

Identifier	Technology	Description
CSCsd71301	AAA	Depending on Attriubut order send from aaa server priv level assigned.
CSCsd95752	AAA	6500 TACACS message sent to wrong server .
CSCse45735	AAA	%AAAA-3-NOREG: authentication method 5 has no registry! T/B
CSCdw26914	ATM	show atm vc truncating outputs
CSCei39688	ATM	ATM subinterface fails to pass traffic due to CEF initialization failure
CSCse64269	ATM	show ip int br shows member link state down for PA-A3-8T1/8E1IMA
CSCse29465	Content	CASA traceback routing agent in process causing CPUHOG
CSCse45427	Content	debug ip casa packet displays incorrect values
CSCse76405	Content	CASA wildcard updates dropped
CSCdy11174	Infrastructure	ciscoFlashCopyTable/ciscoFlashMiscOpTable obj unreadable @ creation
CSCeb56615	Infrastructure	ATA_Status time out waiting for 1
CSCee23195	Infrastructure	Spurious memory access in show ipc queue .
CSCef49904	Infrastructure	No option in snmp to source the interface for Informs
CSCek51851	Infrastructure	Standby does not come up during switchover with slavenvram in access
CSCin97208	Infrastructure	Standby does not come up during switchover with slavenvram in access
CSCsc14034	Infrastructure	Master RSP crashes on bootup w/ snmp mib notification-log default
CSCee32814	IPServices	Source port selection is predictable, should be harder to guess
CSCeg51303	IPServices	VRRP responds with int MAC instead of VMAC afetr shut/no shut
CSCsd23056	IPServices	reverse telnet (tty daemon) broken by TCL feature
CSCsd33013	IPServices	FHRPs fail to clear ARP entry after Duplicate IP event
CSCsd69052	IPServices	Netbios/NAT optimization
CSCse23548	IPServices	modular ios (ION) : logging source-interface command ignored
CSCsf16715	IPServices	TCP will leak TCBs if app closes in notification callback context
CSCsf33034	IPServices	T/B tcb_isvalid+7C during bootup and when EOMPLS vc is configured.
CSCek46996	LAN	Cwan FA-PA port need to be in promiscous mode if IP address not conf
CSCsc95736	Management	cns config partial command causes cpu up 25%
CSCef32748	MPLS	tfib_ipfib_post_table_change needs to check for recursive routes
CSCek31478	Multicast	ip multicast boundry cmd does not take effect after modify ACL
CSCek42421	Multicast	One prune not processed on receiving batched join/prune message
CSCsd49955	Multicast	RPF info created by (S,G) RPT-bit prune does not change by (S,G) join
CSCse09435	Multicast	PGM router assist on GRE causes small pool buffer leak
CSCse20714	Multicast	MSDP doesnt send triggered SA for non-directly connected PIM-DM source
CSCee93983	platform-76xx	osm : egress CE router is missing in traceroute in MPLS/VPN

Identifier	Technology	Description
CSCeh32595	platform-76xx	Ping fails across atm interface after configuring routing protocols
CSCsd25766	platform-76xx	OSM-1OC48-POS: APS Protect-Inactive port is receiving and fwding packets
CSCsd80632	platform-76xx	12.2(18)SXE2 ifHCInOctetssub interface traffic is not close to the main
CSCsd88401	platform-76xx	input packet drop w/ gt48520 mac_rx_error at port2 on OSM-2+4GE-WAN+
CSCse26606	platform-76xx	packet drop occur when issuing shut/no shut on other sub-if /w OSPF
CSCeg26728	QoS	BGP fails to establish a peer with policy bw 199K
CSCek44025	QoS	Hierarchy is not collapsed when FRF.12 is configured
CSCsc00993	QoS	Lower tx-ring-limit for ATM VCs with higher SCR when QoS is enabled
CSCse02510	QoS	Crash with ALIGN-1-FATAL at hqf_process_wfq_command
CSCse54611	QoS	WS-X6582-2PA bus error crash on hqf_cwpa_pak_enqueue_local
CSCee71850	Routing	Router crashes while unconfiguring IPX GRE
CSCee77180	Routing	Static routes with space in name not recognized after reload
CSCei26931	Routing	fragment option is not in access-list command
CSCej42121	Routing	clear adj hangs router
CSCin85894	Routing	Reflexive acl when used as ext. acl gives T/bks & crashes with std.
CSCsc37212	Routing	ISIS: Redistributed routes might not be advertised if interface flaps
CSCse52184	Routing	unrelated MPLS TE tunnel flapping cause unnecessary fib/lfib updates
CSCse61025	Routing	ip http auth aaa is not needed for Authproxy to work
CSCsb62045	Security	scp connection fails with error: unexpected filename:
CSCse29545	Security	Crypto pki trustpoint loses ip-address command upon reload
CSCec42435	Unknown	crypto map local-addr command may disappear on E1and T1 interfaces
CSCeh52424	Unknown	OC3 ATM/SPA: Input CRC errors caused SIP200_SPIRX-3-SPI4_LINKERROR
CSCej08637	Unknown	Inline power sensors needed on standby to support entity mib SSO.
CSCek22782	Unknown	CSM: Configuration sync check does not work in all cases
CSCek28561	Unknown	SIP1/ChOC3: T1/E1 BERT unusable after first run
CSCek36288	Unknown	EoMPLS VC down with SIP1 as core facing interface
CSCek50720	Unknown	Improve error handling for DLL centering algorithm
CSCsa77785	Unknown	Router crashes when L2 redirection is configured with HTTP traffic
CSCsa95306	Unknown	SNMPWALK does not get all CSG user group information
CSCsa96972	Unknown	Dbus header err int be triggered when recovery procedure on DFC3
CSCsb41923	Unknown	isakmp key ending in backslash will be lost after device reboot
CSCsb80468	Unknown	Hvpls: MAC Addresses May Not Be Flushed When VC Goes Down
CSCsb82048	Unknown	%ALIGN-3-CORRECT: Alignment correction made at 0x402B4BA4
CSCsc20064	Unknown	Ping fails on changing removing and reconfiguring controller for ChSTM1.
CSCsc25952	Unknown	Need to print out error message for unsupported marking on OSM
CSCsc56766	Unknown	Slow convergence of DEC for mac-address moving from one FE to another FE
CSCsc59025	Unknown	UDLD config on 2nd uplinki of act/sby sup change after switchover

Identifier	Technology	Description
CSCsc75397	Unknown	sup32 enables fix for CSCeb49514 with cross-module etherchannel
CSCsc81300	Unknown	uRPF check ACL programming spikes RP CPU
CSCsd46882	Unknown	OSM-CT3 Port in Unchannelized mode stays UP/UP when looped towards line
CSCsd47475	Unknown	cat6k unable to resolve arp request when using flexwan, pa-fe-tx and vpn
CSCsd53513	Unknown	%ALIGN-3-SPURIOUS_SO: Spurious memory access seen with tracebacks
CSCsd64103	Unknown	'mls qos trust dscp' not working for traffic coming from FWSM
CSCsd80745	Unknown	bus error or alignment err at crypto_isakmp_profile_contain_xauth_info.
CSCsd94439	Unknown	I/O mem corruption on SP with mld snooping report-suppression enabled
CSCsd95575	Unknown	RP-Crash @ draco2_pa_eobc_intr
CSCsd96121	Unknown	Mac's don't get purged when the port is blocking during topology change
CSCse09460	Unknown	Agg ram is not programmed properly after switch over
CSCse15906	Unknown	CAT6500/7600 Sup2 show int counters output drops double the qos drops
CSCse16512	Unknown	Egress Queuing on WS-6148-21AF broken
CSCse19732	Unknown	Not able to apply policy on a port -which is earlier part of l3 port-cha
CSCse29001	Unknown	ISIS did not update when encap frame-relay on POS SPA of SIP-400
CSCse29419	Unknown	Need SNMP support for traffic counters given by 'show vlan counters'
CSCse33257	Unknown	Intf Flap causes memory Hog in mls-msc on DFC installed Sup720 system
CSCse33395	Unknown	HSRP track interface in down state in ITASCA though active on SUP
CSCse33488	Unknown	DS1: Back to back connectivity not successful between T1/E1 SPA-PA
CSCse35278	Unknown	VPNSM drops transit NAT-T packets
CSCse47430	Unknown	Need boundry check in heartbeat_create_recv_info
CSCse47811	Unknown	Guard output does not reach GRE tunnels on SUP-720
CSCse50503	Unknown	Hybrid fix for CSCed74512
CSCse50607	Unknown	SPA-8XCHT1E1 IPC failure causes latency and MLPPP lockups
CSCse51577	Unknown	Sup2/MSFC2: Memory leak at Dead/FM VMR chunk when pasting in NAT config
CSCse54768	Unknown	CASA traffic not CEF switched
CSCse59777	Unknown	WLSM: CPUHOG on L3mm process
CSCse61121	Unknown	Memory leak in FIB Control Task
CSCse61252	Unknown	ION : reset reason displayed incorrectly in show version
CSCse62117	Unknown	cbQosCMDropByte reset after clear counters
CSCse63856	Unknown	Sup720 Doesn't Terminate GRE Properly - Packet Recieved on Wrong Int.
CSCse67650	Unknown	SIP600 WRED fails to forward ARP packets
CSCse69713	Unknown	Redirect traffic punted to software when all CEs in the group are lost
CSCse69748	Unknown	CLI for IMAP retcode in CSG refunding is broken
CSCse73539	Unknown	c7600 - crash of active sup720 after inserting a second one
CSCse85399	Unknown	traffic does not go over crypto tunnel after a no shut.
CSCse86602	Unknown	Cat6500 IOS does not set correct portAdminSpeed

Identifier	Technology	Description
CSCse87417	Unknown	FlexLink : ARP frames w/ known opcodes cause interop issues.
CSCse88171	Unknown	PA-MC-8TE1+: cRTP compression failure
CSCse98354	Unknown	SIP-200: SYNC FAILED not initialized. Interfaces up/down.
CSCsf00089	Unknown	Packets not HW switched after test crash invoked
CSCsf03566	Unknown	Memory corruption crash trying to free unassigned block
CSCsf04301	Unknown	Multicast on ATM SPA with P2MP sub-interfaces does not work
CSCsf13325	Unknown	Commit of CSCse95804 broke v122_18_sxf_throttle s3223-adventerprisek9_wa
CSCsf15527	Unknown	ION: Reset Reason Does Not Change on Normal Reload
CSCsf31504	Unknown	TestFabricFlowControlStatus: Monitor interval is to be reduced to 100ms
CSCef01547	WAN	7200 tx-ring resets to default after OIR
CSCek27504	WAN	NTP crash during show runn after deletion of NTP ref-peer
CSCse95146	WAN	Sup720 with cross module etherchannel duplicates all packets

Resolved Caveats in Release 12.2(18)SXF5

Resolved Infrastructure Caveats

- CSCsc64976—Resolved in 12.2(18)SXF5

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

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

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20051201-http.html

Resolved LAN Caveats

- CSCsd34759—Resolved in 12.2(18)SXF5

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

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

  Further Information

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

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

  These vulnerabilities are addressed by Cisco IDs:

  - CSCsd52629/CSCsd34759 -- VTP version field DoS
  - CSCse40078/CSCse47765 -- Integer Wrap in VTP revision

- CSCsd34855/CSCei54611 -- Buffer Overflow in VTP VLAN name

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

http://www.cisco.com/en/US/products/csr/cisco-sr-20060913-vtp.html

Resolved Routing Caveats

- CSCsd40334—Resolved in 12.2(18)SXF5

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

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

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

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html

Resolved Unknown Caveats

- CSCsd68605—Resolved in 12.2(18)SXF5

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

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

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

- CSCsd75273—Resolved in 12.2(18)SXF5

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

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

  A Cisco Security Advisory for this vulnerability is posted at
  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

- CSCsd37415—Resolved in 12.2(18)SXF5

  Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

  MPLS packets can only be sent from the local network segment.

A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-mpls.html

- CSCse52951—Resolved in 12.2(18)SXF5

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

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

  A Cisco Security Advisory for this vulnerability is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

Resolved Voice Caveats

- CSCsc60249—Resolved in 12.2(18)SXF5

  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 Resolved Caveats in Release 12.2(18)SXF5

Identifier	Technology	Description
CSCsb11698	AAA	Input Queue Wedge with TACACs
CSCei71142	ATM	autovc handling stopped
CSCse35684	ATM	OSPF adjacency does not recover from OIR active supervisor
CSCsc94191	Content	WCCP does not GRE Redirect TCP FIN packet that would fragment
CSCed21186	Infrastructure	Incorrect GE output IFMIB counters when CAR is configured
CSCee24395	Infrastructure	SYS-3-BADMAGIC after GetNextObjectInstance clogHistoryEntry_get
CSCei85359	Infrastructure	%SCHED-3-SEMLOCKED: IP RTR Probe MaxName attempted to lock a semapho
CSCek24385	Infrastructure	ION config checkpoint for process restart must handle SNMP, HTTP
CSCin62031	Infrastructure	Crash when SNMPset rttMonCtrlAdminStatus to 1 (IP SLA Probe activation)

Identifier	Technology	Description
CSCsa61284	Infrastructure	snmpset rttMonCtrlOperState to 7 (restart) cause rttMonCtrlAdminStatus 2
CSCsb08386	Infrastructure	PRP crash by show ip bgp regexp
CSCsb16702	Infrastructure	Configuring using http forced sw-crash on standby supervisor
CSCsb34180	Infrastructure	Rockies 3 SNMP: PS in entPhysicalChildIndex not in incremental order
CSCsc06891	Infrastructure	no traps are sent when CF is inserted or removed.
CSCsc85922	Infrastructure	IOS changes its implementation of what is an unknown community tring
CSCsc97279	Infrastructure	Takes long time (more than 2 minutes) on wr mem
CSCsd32923	Infrastructure	Bus Error in Exec attempting command completion in a full command buffer
CSCsd77751	Infrastructure	IOS - SUP720 - sends empty/blank syslog messages
CSCec10091	IPServices	DHCP relay agent forwards requests with src. 0.0.0.0
CSCed93425	IPServices	DHCP Database fails to write to local flash.
CSCeh35083	IPServices	NAT-PPTP change Call ID wrongly
CSCsd80754	IPServices	HSRP Active-Router not respond to ARP request about VIP
CSCec87736	LAN	SNMP counters on FE subif not updated for dcef
CSCsc69537	LAN	GigE sub-interfaces not registered with SNMP after LC reload
CSCsd34855	LAN	VTP update with a VLAN name >100 characters causes buffer overflow .
CSCsd94687	LAN	sh vlans counters and SNMP counters are incosistent for subif
CSCsd55300	LegacyProtocols	DLSw ER LLC session fails to connect with SUP720 or SUP32
CSCse17611	LegacyProtocols	DLSw Circuits Connect outside of DLSW ER to switch with passive mapping
CSCef78565	Management	cdp not advertising ifName
CSCek35484	MPLS	FRR: MP tears down protected lsp if local protection des flag rese
CSCsc94359	MPLS	BGP table and CEF forwarding table have mismatched labels
CSCsd41981	MPLS	TFIB on SUP720 PFC is broken when an OSM (GE-WAN) card was disabled
CSCsd57678	MPLS	Label inconsistency between BGP and forwarding tables for remote routes
CSCei77227	Multicast	PE router crashes @ igmp_delete_group while unconfiguring vrf
CSCej20707	Multicast	igp and pim neighbor goes down during mcast stress testing
CSCej78303	Multicast	RP crash @ pim_tt_grange_first after CMD: no ipv6 unicast-routing
CSCsb76434	Multicast	PIM: auto-rp group stuck in registering when sparse-mode
CSCsb85290	Multicast	IPv6 BSR: BSM forwarding breaks with ipv6 vrf implementation
CSCsc69155	Multicast	ciscoIpMRouteIfInMcastOctets counts decrease
CSCsc96746	Multicast	PIM-sm chooses wrong RPF interface in equal cost multipath network
CSCsc98828	Multicast	PIMV6: SR flag set on RP acting as first hop
CSCsd64138	Multicast	ip multicast rpf not configurable in 12.2(18)SXF3
CSCsd68993	Multicast	Fluctuation in IPv6 mcast trffic fwdng happns with large numbr of strms
CSCse05960	Multicast	PIM leaking memory used for xdr messages
CSCse64256	Multicast	FHR crashes on starting Embedded RP stream
CSCsb64975	platform-76xx	Rate counters are erratic for a bi-dir traffic more than 2 Gig

Identifier	Technology	Description
CSCse05336	platform-76xx	Packet drop on OSM-2+4GE-WAN+ if sub-if is created or deleted
CSCsc33562	PPP	SNMP ifInOctets shows negative value for MLP interface
CSCsc37902	PPP	Standby MSFC may experience bus error after RP_MLP-4-MISCONFIGLINK.
CSCsd34741	PPP	dMLP: line card might crash with cRTP enabled.
CSCec80902	QoS	Router crashes with Bus Error at 0xFD011147
CSCsa68661	QoS	LC crashes when service-policy is configured on channelized interface
CSCdt69452	Routing	scaling: need ability to do clear ip arp A.B.C.D.
CSCea71711	Routing	Missing cef table for tableid 2829 during Table removal event
CSCee47792	Routing	OSPF Traps does not use IpAddress. Uses type integer at present
CSCee81606	Routing	LSAs not generated when redistributing connected subnets into OSPF
CSCef11304	Routing	MIB walk on OSPF-MIB involving ospfExtLsdbTable crashes switch
CSCef17647	Routing	NPE-G1:tracebacks when high nmbr of RIP neigh/low update timer
CSCeg16631	Routing	CSCee32557 breaks RIP distribute-list w/ VRF interface
CSCeg52659	Routing	BGP route may not get withdrawn under rare condition
CSCeh54086	Routing	ABR fail to update LSA type3 in response to shut interface.
CSCei45669	Routing	OSPF router may fail to flush its self-originated LSA
CSCej89011	Routing	LSA received via Demand Circuit may show aging
CSCek45564	Routing	iprouting crash with corrupted block on mpath config change
CSCsb36755	Routing	BGP does not delete multi-path route when receiving worse metric UPDATE
CSCsc07467	Routing	OSPF route lost after interface flap.
CSCsc10494	Routing	Partial SPF may skip an LSA
CSCsc63871	Routing	Only 1 clns adjacency on ethernet but several neighbors
CSCsd00028	Routing	OSPF: spurious access in ospf_generate_trap
CSCsd03882	Routing	SUP720 RACL Deny ACE not being implemented
CSCsd64173	Routing	Bus error crash IPV6 due to OSPF summary prefix command
CSCsd84489	Routing	Crash in ospf_add_all_stub_routes on topology change
CSCsd99760	Routing	After iprouting.iosproc Process Restart Routing table not updated
CSCuk58462	Routing	Routes are not filtered even when route-map rule sets deny the rule
CSCsc72722	Security	CBAC - firewall resets TCP idle timer upon receiving invalid TCP packets
CSCsd43903	Security	Memory leak in Crypto IKMP process when using certificate authentication
CSCse11457	Security	show crypto ca timers shows static output
CSCse12154	Security	Bus error crash after executing secure copy (scp)
CSCea24341	Unknown	SLB real to real ICMP traffic broken with FWLB
CSCeb68312	Unknown	IOS SLB HTTP probe uses :0 in host tag
CSCeb77318	Unknown	IOS SLB: Incorrect checksum of forwarded icmp unreachable
CSCed61394	Unknown	Easy VPN(with RSA) does not work with XAuth
CSCef21434	Unknown	isakmp profiles only use one trustpoint.

Identifier	Technology	Description
CSCeg86665	Unknown	Trust state - Tunnel decap side, modify the original packets dscp
CSCeh21210	Unknown	MF: DHCP Snooping crash when server send invalid option 82
CSCeh42489	Unknown	cbQosCMDropByte64 always shows the same value as cbQosCMPrePolicyByte64
CSCeh78411	Unknown	Failed IKE sessions does not get deleted in certain conditions
CSCei37299	Unknown	clear crypto session remote ip may crash router if client reconnect
CSCei93025	Unknown	Etherchannel config changes not synched to inactive member ports
CSCei95384	Unknown	PP:R3:8xT1/E1-SPA MLP: EFC ERROR/inactive after link added to bundle
CSCej86188	Unknown	MLS packet error syslogs should be configurable and no service int
CSCek22536	Unknown	SLB high cpu with second VIP inservice and user->real traffic
CSCek22595	Unknown	SLB vserver access commands break user->real traffic
CSCek24053	Unknown	Sup720_rp: spurious memory accesses in cardifmib_get_card_index
CSCek26155	Unknown	EEM cli ED can enter recursive loop with action cli commands.
CSCek26158	Unknown	IOS TCL leaks memory when EEM policy triggered.
CSCek28863	Unknown	Need to change default SCP keepalive timeout on IOS to CSM module
CSCek30589	Unknown	WS-X6196-RJ-21/ WS-F6K-FE48X2-AF inline power auto detect
CSCek31437	Unknown	6516 with Sup32 should not be powered down as unsupported module
CSCek32555	Unknown	MFR i/f lineprotocol takes too long to come up after RPR+ switch
CSCek35417	Unknown	NVRAM write failed on runtime image for Rommon Upgrade.
CSCek35770	Unknown	Need show module power equivalent in IOS
CSCek35951	Unknown	Priority queue with policing configured doesnt work
CSCek37181	Unknown	Loopback on controller for online diagn of wism card
CSCek42027	Unknown	SPA FPD upgrade fails with sip1-CR
CSCek47714	Unknown	The supervisor crashed after second switchover in rpr-plus mode
CSCin96942	Unknown	BAD_RESET and HARIKARI messages with linewatch_timer and crash
CSCin98448	Unknown	controller shut throws up error msg and remote end is not going down
CSCsa76455	Unknown	Sup32:Pkts switched out with incorrect DA MAC for VRF adjacency
CSCsa98081	Unknown	up/downgrade in SXB code w/ crypto connect, BGP fails
CSCsa99158	Unknown	Unexpected START records triggered by IPSec - unreliable AAA records
CSCsb29028	Unknown	Processor Memory leak in Crypto IKMP process
CSCsb53810	Unknown	sup720 outbound acl not denying traffic, hitting incorrect tcam entry
CSCsb61021	Unknown	IP Spoofed packets from CE are not hw switched with egress WCCP
CSCsb72854	Unknown	CONFIG_FILE ROMMON var and boot config support for c6k
CSCsb79306	Unknown	C2R3: cbeDot1dTpVlanIndex is out of sync w/ CLI causes standby sup reset
CSCsb85024	Unknown	WS-X6148A-GE-TX corrupt counter dot3StatsInternalMacReceiveErrors
CSCsb86198	Unknown	show port-sec int <int-name> add not sync with stdby after SO
CSCsb91644	Unknown	IPv6 MFIB entry is updated on RP and delayed to update MFIB on SP & DFC
CSCsc05015	Unknown	SNA packet is not bridged when VLAN1025 is used on bridged interface

Identifier	Technology	Description
CSCsc08857	Unknown	LPIP:eou_sm_post_event traceback on clear ip device tracking all
CSCsc10914	Unknown	Tracking fails at reload for inteface with switchport enabled
CSCsc18986	Unknown	IOS SLB causes high CPU
CSCsc22552	Unknown	low address access crash upon malloc_fail for tcl script output
CSCsc26237	Unknown	Bus error at hqf_police_update
CSCsc29942	Unknown	Could not retreive/set EEM MIB objects values from snmp workstation
CSCsc30268	Unknown	linecards crash @ free_qos_set_if_sub_structures
CSCsc38892	Unknown	slb http and tcp probes not working with access ints/vrf
CSCsc43862	Unknown	SPA ping failure caused by SIP-200 serial primary channel sync failure
CSCsc46301	Unknown	Crash in GTP SLB imsi sticky
CSCsc51357	Unknown	Unicast Flood Protection causes CSM redundancy to transition
CSCsc54382	Unknown	RE: L3 DEC activates EC purging
CSCsc54552	Unknown	mac-address-table static configuration problem
CSCsc61809	Unknown	Min-links feature doesn't work intermittently even just on shut/no shut
CSCsc62574	Unknown	ifHCInUCastPkts are decremening between 2 polls
CSCsc71245	Unknown	sup720:High CPU and traceback in ipsec_db_get_ipsec_sa_list with VPNSM
CSCsc77703	Unknown	SYS-SP-3-CPUHOG process = FIB Control Task
CSCsc84683	Unknown	crash observed on removal of certain mcast mac address
CSCsc86540	Unknown	SIP-400 Tracebacks occur when upgrading FPD on SIP 400
CSCsc87117	Unknown	slowness in updating DF in HW after doing shut or no shut RPF link
CSCsc89229	Unknown	Traceback & crash at pm_get_standby_vlan on Sup720
CSCsc89979	Unknown	EEM traceback for,action x info cli frequenc; if cli history table empty
CSCsc90782	Unknown	dsx1FarEndInterval not available in 12.2(18)SXF on a c7609
CSCsc94171	Unknown	FIBTCAMSSRAM on Ant24/NikeXL fails if running FIBTCAM in Aph in parallel
CSCsc95631	Unknown	Rapid PVST does not automatically recover from ROOT_Inc (Root Guard)
CSCsd01719	Unknown	SIP-600: SPA OIR with DOT1Q tunnel on port-channel can crash RP
CSCsd03416	Unknown	Active RP Crashed after doing rerouting in PIM SM Stress Test
CSCsd05513	Unknown	7600 CBQOS-MIB is missing info which is present in CLI
CSCsd08411	Unknown	EEM Tcl policy execution delayed relative to config size
CSCsd14307	Unknown	PA-MC-8TE1+ PA shows alarm led red even with all controllers shut down
CSCsd15806	Unknown	r2.5:Tcam is not programmed after shut/no shut on interface
CSCsd16407	Unknown	Ingress service-policy on SPA10X1GE interface fails to police traffic
CSCsd17174	Unknown	SLB Connection states get into loop on snmp query
CSCsd17992	Unknown	After PS fails and powered on, PS fan fail msg. display even if PS on
CSCsd25447	Unknown	bill-of-materials file update failed on rollback activation
CSCsd25532	Unknown	High SP-CPU utili occurs when c7600 recieves IPv6 Multicast traffic
CSCsd25611	Unknown	MPLS VPN forwarding broken for new vrfs on PE 7600 SUP720

Identifier	Technology	Description
CSCsd28870	Unknown	Entries from redirect acl list with log keyword not programmed into tcam
CSCsd28995	Unknown	ip default-network is not installed if it is ip2tag fib
CSCsd29927	Unknown	6500 BIT-SP-4-OUTOFRANGE error with voice vlan dot1p and monitor session
CSCsd31503	Unknown	Cat6k Selective Packet Discard drops OSPF packets
CSCsd35622	Unknown	session timeout TCL causes CPU hog/crash
CSCsd37537	Unknown	ipMRouteInterfaceOutMcastOctets not incrementing, remains zero
CSCsd37634	Unknown	SCCP portion of Skinny packet is not being NATd
CSCsd39189	Unknown	ALIGN-3-CORRECT with DHCP Snooping when using Option 82
CSCsd40211	Unknown	Sup720 : Delay in arp result after interface shut/no shut
CSCsd42247	Unknown	Config rspan, remove rspan and then config span cause unidirect. traffic
CSCsd42850	Unknown	mGRE broadcast issue, invalid checksum seen on IP Header Checksum
CSCsd43185	Unknown	Tx queue cos maps for even ports of card WS-X6416-GBIC are incorrect.
CSCsd43481	Unknown	EoMPLS drops OSPF multicast packets with mls ip verify length minimum
CSCsd45167	Unknown	Memory leak in Crypto IKMP Process
CSCsd49280	Unknown	show idprom should work with non-cisco xenpaks
CSCsd49723	Unknown	Memory leak in Crypto IKMP Process when using certificate authentication
CSCsd49767	Unknown	Memory leak in Crypto IKMP process
CSCsd52633	Unknown	VPN-Spa stop forwarding traffic if any changes on ATM traffic shaping
CSCsd56549	Unknown	GRE doesnt get the same port that it req, PPTP change Call ID wrongly
CSCsd58552	Unknown	cwpa2: TCP to NAT addresses cause FR encap change from IETF to cisco
CSCsd59274	Unknown	MLD snooping report-suppression does not work correctly
CSCsd59975	Unknown	WS-X6704-10GE causing CRC errors on WS-X6502-10GE interfaces
CSCsd64158	Unknown	%MLSCEF-SP-2-FREEZE: hw switching disabled due to mls cef sanity failure
CSCsd64741	Unknown	SLB IMSI sticky idle timeout queries fail to reach GGSN when vrf-aware
CSCsd65434	Unknown	igmp snooping fails when leave is processed during igmp general query
CSCsd67341	Unknown	WS-X6148A-45AF compatible issue with 3rd party Video Camera
CSCsd67456	Unknown	VPN-SPA: IPSec SA comes up with wrong lifetime in KB
CSCsd68266	Unknown	input errors increment on 10/half port
CSCsd70494	Unknown	Bidir-Multicast Packets are dropped when using G/m entries
CSCsd70948	Unknown	After SSO switchover all CDP and BPDU are lost if L2 rate limiting is on
CSCsd71047	Unknown	NAT cef entry is not changed after IP address change MAC address
CSCsd74975	Unknown	Clearly indicate customer friendly bus stall log messages.
CSCsd75069	Unknown	IPC RX FIFO FULL err w/ high traffic&LC CPU (IO-FPGA Pat-Mav2.5/Pro1.5)
CSCsd75929	Unknown	Sup32 fails to get DHCP snooping binding table on switchover
CSCsd81263	Unknown	After reload, sup32 system unable to communicate with all neighbors
CSCsd86340	Unknown	After unplugging PC from back of phone into new port - error disable
CSCsd90501	Unknown	Minimum/Maximum WRED thresholds for default DSCP stays at 32/64

Identifier	Technology	Description
CSCsd94127	Unknown	COS aligned to IPP for routed multicast traffic
CSCsd94541	Unknown	Multiple T3 controllers bounce on the SPA
CSCsd95279	Unknown	VPNSM uses incorrect MTU if egress interface is down at boot time
CSCsd96511	Unknown	Interface admin down: egress TCAM default program as bridge
CSCsd98390	Unknown	WS-X6148A-45AF module may not bootup/lose config on switch power-cycle.
CSCsd98421	Unknown	MPLS:VPN:QoS:set mpls exp fail at ingress PE OSM interface
CSCsd98887	Unknown	SP Memory Leak In mls-msc Process
CSCse00284	Unknown	ION Code crashes active sup under heavy stress and show proc cpu cmd
CSCse11333	Unknown	Native IOS does not syslog thermal warnings from IDSM-2 Cat6k card.
CSCse12195	Unknown	6816: Interface 3/4 flapping when interface 3/1 is not connected
CSCse15495	Unknown	sip-600 and 10GE SPA - incorrect cbQosCMPostPolicyByte64
CSCse15728	Unknown	VPNSM does not perform invalid spi recovery in vrf mode
CSCse23889	Unknown	Bus error when configuring xconnect vfi from int vlan
CSCse41480	Unknown	cos vlan priority is not preserved for MPLS traffic over EoMPLS tunnel
CSCse41963	Unknown	RSPAN+VACL is broken when DEC is configured in system
CSCse54041	Unknown	CSM config sync timemout with large configs
CSCse60601	Unknown	Standby Sup crash due to ACLDeny bug in TYCHO
CSCse70423	Unknown	change WS-X6708-10GE default behavior for non-E chassis

Resolved Caveats in Release 12.2(18)SXF4

Resolved LAN Caveats

- CSCsd34759—Resolved in 12.2(18)SXF4

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

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

  Further Information

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

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

  These vulnerabilities are addressed by Cisco IDs:

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

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

  http://www.cisco.com/en/US/products/csr/cisco-sr-20060913-vtp.html

Resolved Unknown Caveats

- CSCsd28570—Resolved in 12.2(18)SXF4

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

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

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

  Workaround: This advisory with appropriate workarounds is posted at http://www.cisco.com/en/US/products/csr/cisco-sr-20060125-aaatcl.html

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

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

Other Resolved Caveats in Release 12.2(18)SXF4

Identifier	Technology	Description
CSCsb12329	ATM	ifAdminStatus of ATM sub-interface is down without shutdown command
CSCsc72066	Content	MNLB - incorrect affinities installed
CSCsb14936	Infrastructure	SNMPv3 EngineID (default value) not established correctly
CSCsb85983	Infrastructure	bootflash corruption seen even with CSCei17174 fix
CSCeg61169	IPServices	Traceback recorded in tcb_isvalid by TCP Remote Shell Process .
CSCsc47919	IPServices	VRRP does not correctly interoperate with Proxy ARP
CSCsd34855	LAN	VTP update with a VLAN name >100 characters causes buffer overflow .
CSCeh67947	Multicast	Auto-RP group 224.0.1.40 Pruned after Assert.
CSCek26627	Multicast	CPUHOG when RPF change affects ~30k mroutes
CSCsc16148	Multicast	Allow (S,G) expiry timer to be configurable
CSCeh62084	PPP	ifStackStatus drops ifIndex when interface is OperStatus down
CSCsb97950	PPP	dLFIoATM: Packets with CLP set, get punted to RP.
CSCee58986	QoS	fair-queue nvgen does not happen
CSCsc98510	QoS	Ehanced Flexwan reloads with VRF/MLPPP/QoS
CSCsd71119	QoS	ALL ATM PVC DOWN IN FLEXWAN WITH PA-A3-OC3 AND OAM
CSCed82273	Routing	IPV6 I-BGP does not reach established state
CSCef35386	Routing	BGP does not inform PIM of the second best VPNv4-MDT
CSCeg77104	Routing	EIGRP neigh over ATM IMA link flaps due to Authentication failure
CSCsa64947	Routing	High CPU seen after clear arp
CSCsa68988	Routing	route-map cache for soft-reconfig is not made when BGP peer comes up
CSCsb78345	Routing	ipv6: Sup720/3b-XL crash when show ipv6 cef after OSVFv3 cost change

Identifier	Technology	Description
CSCsc59089	Routing	BGP: updates missing if route-refresh received while updates on OutQ
CSCsc67367	Routing	set ip next-hop in-vrf not working with import maps
CSCsc73436	Routing	BGP: touching neighbor policies causes peer's table version to reset
CSCsc76327	Routing	EIGRP PE-CE: Constant route-flap with a redistributed VRF-static-route
CSCsd11631	Routing	7600: Spurious accesses originated by OSPF process
CSCsd12904	Routing	OSPF sham-links do not come up
CSCsa63387	Security	Router may crash when CRL expires
CSCei27448	Unknown	Router crashes while displaying sh ip pim mdt bgp
CSCek26158	Unknown	IOS TCL leaks memory when EEM policy triggered.
CSCek26186	Unknown	ATM SPA: setup vp fails.
CSCek32944	Unknown	GLOBAL,DONTWAIT registries broken
CSCsb12969	Unknown	MQC: Router crashes when a service-policy is added to atm or FR pvc
CSCsb33258	Unknown	RP crash while mvpns come up - MDFS buildup
CSCsb61514	Unknown	Packet drop for size > 1526B between SUP <-> MWAM
CSCsb94412	Unknown	SIP1: RBE: OAM Packets being accounted as input errors
CSCsc22552	Unknown	low address access crash upon malloc_fail for tcl script output
CSCsc46105	Unknown	Not carryover ToS value if enabling mls qos on Native IOS
CSCsc55406	Unknown	Tcl scripts leak memory upon every run
CSCsc57156	Unknown	Hardware fault on FWSM ports not causing FWSM redundancy failover
CSCsc65256	Unknown	Connection Count incorrect after ungraceful disconnect/reconnect
CSCsc68250	Unknown	Packet flow halt on 7600-SIP-400
CSCsc86600	Unknown	SNMP:subinterface aal5 layer: Ifindex counter for ATM SPA not updated
CSCsc91075	Unknown	IPSEC Connection Count incorrect after unsuccesfull connection attempt
CSCsd02881	Unknown	Spanning tree issue with vlan mapping and trunk port
CSCsd10975	Unknown	IOS TCL uses ifs_close to close a tcp socket in tclIosChan.c
CSCsd19203	Unknown	SIP400:ATM:new LLQ traffic stop flowing on dynamic changes to Policy
CSCsd33647	Unknown	ER: Improve C2 MET programming under heavy traffic scenarios
CSCsd44517	Unknown	flow control needs to be toggle off/on to become active after no shut
CSCsd45479	Unknown	Process restarts not guaranteed if installer is in list of processes ...
CSCsd47734	Unknown	Additional memory leak fixes by ActiveState
CSCsd04219	WAN	Add feature support for ACLs in 12.2SXE on virtual templates

Resolved Caveats in Release 12.2(18)SXF3

Resolved Routing Caveats

- CSCec12299—Resolved in 12.2(18)SXF3

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

  Workarounds are available to help mitigate this vulnerability.

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

  This issue cannot be deterministically exploited by an attacker.

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

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20080924-vpn.html

Other Resolved Caveats in Release 12.2(18)SXF3

Identifier	Technology	Description
CSCeg62070	Infrastructure	Tracebacks noticed with Radius configs through HTTP Post
CSCsb69614	QoS	data bus error - NBAR match_heuristic_label w/RTP UDP traffic
CSCsc95511	QoS	Bus error crash at hqf_scheduler_info_init
CSCsa81039	Routing	EIGRP PE-CE:routing loop when a prefix has no cost-community
CSCsc24102	Unknown	Fabric sync errors if WS-X6704-10GE is on slot 4 on 7606
CSCsc39902	Unknown	Sup720 SNMPGET of dot1dTpFdbPort returns variable does not exist
CSCsc55949	Unknown	C2 Frequent fabric channel sync errors and rxErrors
CSCsc57156	Unknown	Hardware fault on FWSM ports not causing FWSM redundancy failover
CSCsc68250	Unknown	Packet flow halt on 7600-SIP-400
CSCsc89044	Unknown	IO memory leak with big buffers and EOBC0/0
CSCsd01885	Unknown	Flexwan module, when pvc is down, mac-address are not flushed
CSCsd10156	Unknown	crashinfo missing Additional Subsystem section if core file configured
CSCsd12976	Unknown	Installing image/patch fails on internal compact flash adapter
CSCsd16853	Unknown	X6196-RJ-21 or X6148X2-RJ-45 may fail to boot when running Sup IOS
CSCsd20092	Unknown	Device crashes with fabric error on bootup starting from 28th build
CSCsc86344	WAN	NNI fr intfs with keepalives enabled remain down/down after reload

Resolved Caveats in Release 12.2(18)SXF2

Resolved AAA Caveats

- CSCed09685—Resolved in 12.2(18)SXF2

  Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

Other Resolved Caveats in Release 12.2(18)SXF2

Identifier	Technology	Description
CSCsc33348	AAA	AAA Down: AAA Memory Leak
CSCsb27358	Access	PA-T3+ goes down when seeing two bursts of AIS less than 1 second each
CSCec17185	ATM	PA-A3: VBR traffic shaping inaccurate when PCR=SCR.
CSCsc49134	ATM	Router crashes while creating ATM subinterface - ATM pvc discovery
CSCsc62474	ATM	Some of the PVC might not get deleted through ATM periodic process
CSCsb21972	Content	Tracebacks when both WCCP and Netflow are configured
CSCeb05456	Infrastructure	nvram file locking incorrect for remote file operations
CSCeb62508	Infrastructure	ATA disk corruptions caused by ATA device re-entrant
CSCec75641	Infrastructure	GRP-B: Switchover due to bus error with ip as-path access-list
CSCef11195	Infrastructure	MIPS platforms take Address Error Exception in malloc()
CSCeh44660	Infrastructure	Router crashed while writing the crashinfo to disk
CSCei32102	Infrastructure	Need an option to disable snmp traps for link during switch failover
CSCej08355	Infrastructure	Memory corruption on MSFC with syncnlmTable
CSCej42935	Infrastructure	Incorrect use of directory entry buffer by dfs_next()
CSCsb67916	Infrastructure	SNMP Authentication Failure Trap source ip address 0.0.0.0
CSCsb81704	Infrastructure	SNMP SSO: OID Set on multiple MIBs reset stdby Sup ALIGN-1-FATAL
CSCsb89834	Infrastructure	Config is not saved after write mem from config mode then changing cfg
CSCsb93316	Infrastructure	%CPU_MONITOR-NOT-HEARD causes RP/SP ios-base crash
CSCsc08741	Infrastructure	Sup720 may experience Memory leak in *Dead*/Parser-Mode History Table pr
CSCsc44237	Infrastructure	memory leak in client applications iterating over an empty idb list
CSCsc82214	Infrastructure	Bus error crash at SrCheckClassMIBView
CSCsa51150	IPServices	NAT translation not timing out correctly when a TCP session closes
CSCsb51019	IPServices	TCP session stuck in FINWAIT1 after BGP password changed
CSCsc39357	IPServices	TCP sessions flap under zero window scenario
CSCeh18295	LegacyProtocols	circuit cant get connected via DLSw ER
CSCeh18390	LegacyProtocols	DLSw load-balance doesnt distribute the load evenly with cir count

Identifier	Technology	Description
CSCsa45750	LegacyProtocols	DLSw load-balancing not working as remote mac is not in reachability
CSCeh51720	MPLS	TE LM floods link in wrong area after links area is changed in ospf
CSCsa62908	MPLS	OSPF Opaque LSA not advertised after shut/no shut on MPLS TE interface
CSCsa69210	MPLS	Cannot create VRF in RPR mode
CSCsb16512	MPLS	High CPU in CEF Process and CEF scanner due to prefix reresolve
CSCsc40027	MPLS	corrupted program counter crash - IP-3-LOOPPAK
CSCef65806	Multicast	CISCO-PIM MIB object cpimLastErrorRP truncated when polled
CSCeh93087	Multicast	Need triggered Bidir RP Cache update
CSCei13579	Multicast	consolidation of some post-reload PIM blackhole issues
CSCsb60206	Multicast	TB@bc_odd_src_dst with CPU HOG on SSO sw/o crashes New Active RP
CSCsb61487	Multicast	(*,G) prune not processed on non-DR router
CSCsb64585	Multicast	RP is down but multicast routing continues to work
CSCsc76666	Multicast	PIM Sparses converges at <10K vs 30K+ groups (vs R2.2) on RPF change
CSCsc73288	platform-76xx	OSM asic error:SRIC packet data CRC error
CSCei76630	PPP	PP:R3:FW2+ATM:MLPPPoA+dLFI: I/O Pool MALLOCFAIL after PORT DOWN/UP
CSCsb74603	PPP	Router generated traffic does not match output policy
CSCeg31032	QoS	service-policy stops working on reload
CSCeh88604	QoS	VIP keeps crashing - with PCI DEVSEL timeout @ classify_packet
CSCej77367	QoS	RP crash at hqf_check_vc_layertype during qos testing
CSCsc35609	QoS	Crash in rvsp tail-end while shuting down egress interface on mid
CSCsc98510	QoS	Ehanced Flexwan reloads with VRF/MLPPP/QoS
CSCdv07156	Routing	rip crashes when link up/down.
CSCea34586	Routing	Bus error crash in ip_arp_merge process
CSCed67358	Routing	PIM/OSPF neighbor loss due to improper multicast MAC filter removal
CSCed87897	Routing	sh ip route missed default gateway after ip default-net command
CSCee01688	Routing	NAS crashes at ip2access_add_acl_item() while running stress test
CSCef46230	Routing	per-user ACL not removed upon call termination (regr. CSCee01688)
CSCeg12616	Routing	RIP v2 routes stuck in the RT after interface shut down.
CSCei53226	Routing	BGP: fix updgrps for non private-as peers with remove-private-as
CSCei65553	Routing	OSPF must accept LSID with a mix of 0/1s in the host portion
CSCei77396	Routing	enable ip routing causes error msg %FIB-2-IF_NUMBER_ILLEGAL: Attempt
CSCej08670	Routing	IPFAST-CFC8-2-FASTPORTOPENERR msg after switchover
CSCej21891	Routing	crash in rip_update_dbase when default-information originate used
CSCsa53394	Routing	T/B ospf_generate_trap after Trap enabled on the module
CSCsa79783	Routing	Loosing routes after reload/OIR when ispf enabled
CSCsa99924	Routing	High transient memory usage during EIGRP convergence
CSCsb09852	Routing	BGP: pathless nets not freed when updgrp members are out of sync

Identifier	Technology	Description
CSCsb24535	Routing	clear ip bgp update-group [ip address] clears all the bgp peers
CSCsb37553	Routing	IPv6 : nexthop address inaccesible after clear bgp ipv6 nei soft
CSCsb39749	Routing	router crashes upon isis removal on redundant system
CSCsb40115	Routing	BGP: Failed to find expected # of multipath entries
CSCsb44220	Routing	ipfast needs to retry openning the ipc port in the background
CSCsb59555	Routing	Line Card stuck in request reload
CSCsb74588	Routing	SUP720 crashes when OSPFv3 comes up afer neigh router SSOfailover
CSCsb79759	Routing	External LSAs are not being installed correctly
CSCsb79895	Routing	RIP protocol with MD5 authentication fails
CSCsb80866	Routing	PE global IP address shows up in traceroute VRF
CSCsb83521	Routing	%SCHED-3-STUCKMTMR - Process= IPC LC Port Opener after SSO
CSCsc03828	Routing	OSPF continues to advertise a def route to NSSA w/no default route in RT
CSCsc50692	Routing	Global static route w/ non /32 mask to vrf loopback is unroutable
CSCuk54191	Routing	MP-iBGP routes not installed in VRF RIB
CSCee32606	Security	SSH server crashes when re-generating RSA keys
CSCsa67272	Security	Serial number in certificate subject is incorrect
CSCsc52105	Security	ipsec may leak Crypto IKMP memory blocks
CSCed34190	Unknown	Cannot configure LACP timeout (long or short)
CSCee84918	Unknown	DHCP snooping on 3550 drops DHCPNAKs recieved when renewing old IP
CSCee86692	Unknown	LAN-to-LAN tunnel doesnt get established with DPD configured
CSCeg03733	Unknown	Sprious Alignment and crash with MIB walk in Cisco Class Based QoS
CSCeh17756	Unknown	ASSERT may not function properly with dual PEs and CEs
CSCeh61467	Unknown	Router crashes at pim_reset_updated_nbr on uncfging mdt group
CSCeh78028	Unknown	7600 Port-Sec: traffic fails to recover after reload
CSCei37672	Unknown	chevys/c2lc take ~ 180s before resetting following a mandatory proc exit
CSCei46182	Unknown	c6msfc2a/sup32 DEC MOP packet internally looping
CSCei49919	Unknown	WRR Queue buffer allocation does not work for Q3
CSCei60249	Unknown	VPNSM:default ip mtu sent to VPNSM must be same as IOS
CSCei72033	Unknown	1xcSTM-1 SPA goes OOS upon adding 12 serial links to MFR bundle
CSCei80006	Unknown	Same Proxy, Multiple Peers, both RRI routes deleted
CSCei80699	Unknown	multicast tunnel if_number numbers being duplicated
CSCei86256	Unknown	Crash when typing show lacp neighbors
CSCei86937	Unknown	Sup22 NDE does not export all flows
CSCei88140	Unknown	Sup32:RPR/SSO,standby crashes with exception & goes to rommon.
CSCei92291	Unknown	Message on reload:Error in setting Reload Reason
CSCej00341	Unknown	CSM Configuartion Sync timing out for large configurations
CSCej11090	Unknown	PP:R31:MSC-600/MSC-400: bogus fabric channel error counters

Identifier	Technology	Description
CSCej21515	Unknown	ATM SPA DLL tuning may miss valid lock points
CSCej21520	Unknown	ATM SPA: Removing APS on Protect interface causes locked console
CSCej21698	Unknown	EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
CSCej22954	Unknown	fh_server.proc crash with show ev man hist events max
CSCej29710	Unknown	EEM applet SNMP notifications broken.
CSCej32688	Unknown	CSM: Problem in FT show command with gateway, config sync with more vlan
CSCej37803	Unknown	cT3 SPA:Upgrade to IOFPGA rev2.1
CSCej57810	Unknown	ifOperStatus for Control Plane Interface is always down
CSCej87462	Unknown	SNMP set not-in-service to crcERSpanIFEntry corrupts mem
CSCek03772	Unknown	zamboni: crashes for double fragmentaion
CSCin85363	Unknown	Server crashes while showing peer struct if peer struct is removed
CSCsa58710	Unknown	Supervisor Crashes with hw-module module reset
CSCsa79630	Unknown	Cat6500 Netflow does not export all flows
CSCsa80620	Unknown	ct3 spa: serial interface efc queue stuck on deleting/adding mlp bundle
CSCsa93545	Unknown	UTIL-3-TREE and L3MM-4-MN_IPDB_ADD messages and crashes in wavl and l3mm
CSCsb02848	Unknown	VPNSM does not log messages in datetime format
CSCsb18498	Unknown	SNMP polling broken in cat6k SXE1 image
CSCsb21148	Unknown	Rx SPAN may not work when outbound ACL is applied to source interface
CSCsb21941	Unknown	Supervisor reload with Large sized packet stream
CSCsb31368	Unknown	ATM Multipoint bridging on c65xx is broken after SW upgrade
CSCsb34213	Unknown	Few destination ports removed from RSPAN vlan flood index after SSO
CSCsb34983	Unknown	EEM: Trackback and software-forced crash detected
CSCsb43860	Unknown	CSM tracking interface broken when link flapping multiple times quickly
CSCsb48739	Unknown	GTP SLB:Session reassigned even when sticky entry exists
CSCsb49326	Unknown	Cat6K crashes after EPLD upgrade of WS-X6548-GE-TX
CSCsb59010	Unknown	ceExtProcessorRam implementation inconsistent between RP and LC
CSCsb60453	Unknown	Need improved logs for severe fabric errors which triggers fab swover
CSCsb62566	Unknown	Add an option to power-down the LC when fabric error is detected
CSCsb62581	Unknown	const_mpls_prog_vlan_recirc_adj msg on hw-mod reset, pkts hit CPU
CSCsb62773	Unknown	Guaranteed bandwidth not consistent with hier shaping configured
CSCsb66248	Unknown	no logging event link-status does not prevent SP to send link messages
CSCsb66799	Unknown	URL match statement removed from configuration after reload
CSCsb67152	Unknown	MET inconsistent on DFC, multicast traffic is blackholed for an OIF
CSCsb68513	Unknown	Mcast packets not always forwarded through VPNSM on 6500 with SUP720
CSCsb70335	Unknown	Flexwan crash when fragmentation is enabled under MFR interface
CSCsb70973	Unknown	igmp snooping explicit tracking and report suppression issues
CSCsb70996	Unknown	IOS SLB drops trailing fragments in VRF and misroutes SLB msgs to GGSN

Identifier	Technology	Description
CSCsb72291	Unknown	NetflowTCAM Test failed on Sup7203B with an error code 0x1
CSCsb74212	Unknown	Logical & Phy Port run Configs lost on toggling no sw / sw frm VTY
CSCsb76540	Unknown	Missing global label in TCAM if multi-paths to NH for internet access
CSCsb77592	Unknown	7600/6500 crash by removing ACL tied with vpn configuration.
CSCsb77716	Unknown	dot1x:SP crash at sm_destroy_instance on OIR or link flap
CSCsb79031	Unknown	Clear counter caused the MSFC to reload the SUP due to RPC timeout
CSCsb80141	Unknown	IOS-SLB: no mls ip slb search icmp does not work.
CSCsb80590	Unknown	Enhance IPC buffer usage and IOMEM buffer allocation for Flexwan
CSCsb84405	Unknown	dscp mutation not working after reload
CSCsb84746	Unknown	Memory leak ed at qm_process_enqueue/qm_mqc_mesg_to_process
CSCsb84998	Unknown	MLS-MSC ASSERTION FAILED with T/Bs after hw-module reset
CSCsb85049	Unknown	cwpa2 bridged/routed ATM PDUs lost between Flexwan2 and SUP720
CSCsb85229	Unknown	Hierarchical classification rejected on ATM EGRESS interface
CSCsb85326	Unknown	Error Message SP: MLS-MSC ASSERTION FAILED gce->oif_count in mscdb_gce
CSCsb85589	Unknown	enable explicit-null cause ldp keeps flapping after switchover
CSCsb85748	Unknown	Attempt to open FIB Master failure warning msg occurs after SSO
CSCsb88963	Unknown	WRR queue-limit remains at 0 when WRR bandwidth set to >0 on queues 4-7
CSCsb89241	Unknown	BRE LTL is not populated properly after reload for flexwan2
CSCsb90472	Unknown	Small AToM packets from Flexwan2 dropped if forward by 6548-GE-TX
CSCsb93068	Unknown	WS-x6148-FE-SFP shows incorrect value in CISCO-STACK-MIB::PortTable
CSCsb95563	Unknown	cat6k crashes while releasing mem blocks after unconfig regd. EM Policy
CSCsb95851	Unknown	Cat6K crashing by bus error at msc_sc2vdb_unlink
CSCsc00603	Unknown	Sup22 :uRPF check is disabled globally when disabled on any single i/f
CSCsc03429	Unknown	JQL: Linecard in the slot for SUP reloaded by changing redundancy mode
CSCsc03864	Unknown	Service Module sourced packet dropped when recirculation required
CSCsc04015	Unknown	cbQosCMStatsTable doesn't return byte statistic for FastEthernet PAs
CSCsc05500	Unknown	ENTITY-MIB: SFP in Gi1/1 is not displayed in show inventory
CSCsc05838	Unknown	Changing Sticky Cookie from Dynamic to Insert will corrupt sticky table
CSCsc06620	Unknown	Memory corruption when span session is removed from service module
CSCsc07793	Unknown	Stdby sup reloads after setting stpxMSTInstanceEditVlansMap
CSCsc08498	Unknown	SCHED-3-THRASHING traceback from MWAM_CONSOLE Background Process
CSCsc08602	Unknown	RLB errors with code 50 and access messages without username
CSCsc09557	Unknown	Dot1x authenticated ports loosing states after SSO
CSCsc12302	Unknown	Core MTU change is not reflecting in label HW-ADJ in PE for CSC
CSCsc13720	Unknown	llq functionality with _match input vlan_ broken
CSCsc18551	Unknown	Spurious Access on OSM line card
CSCsc18707	Unknown	No error msg when event manger run nonexist policy

Identifier	Technology	Description
CSCsc18728	Unknown	Sup720 HW PAT (NAT overload) punts frames with valid MTU
CSCsc21581	Unknown	syslogED: value for built-in variable _syslog_msg is incorrect
CSCsc22043	Unknown	Event manager tcl script cannot monitor debug output on vty session
CSCsc24089	Unknown	rspan not working with sup2 and OSM gig ports
CSCsc26048	Unknown	Cat6k: CPUHOG in PIM Snooping Process
CSCsc26490	Unknown	wrong static mac address entry in case of GLBP virtual mac
CSCsc30532	Unknown	PIM snooping not populating mac-address table properly on auto rp group
CSCsc31921	Unknown	Flexwan configured for frame-relay switching causes LMI sequence reset
CSCsc32198	Unknown	IGMP per-port leave with multiple leave nested cases disturbs mcast strm
CSCsc32801	Unknown	Traceback seen after configuring 8 channel-members in etherchannel
CSCsc33110	Unknown	Sip-400 MPB: ST instance not created on SUPW when a PVC is created
CSCsc33990	Unknown	Enhancements and Optimizations to TestSPRP InbandPing
CSCsc38127	Unknown	Standby RP crash in qm_stile_adjust_sb_nbar_flags
CSCsc39939	Unknown	Cat6K : MSTI CAM table not flushed when boundary port generates TC
CSCsc44293	Unknown	Jagger failed on loopback diag.
CSCsc48986	Unknown	WS-X6148-FE-SFP boards may fail to bootup in Supervisor IOS
CSCsc52306	Unknown	IDSM: span tree not blocking when two IDSM in inline mode
CSCsc52645	Unknown	SIP1-CT3: Whole T1 goes down while doing timeslot BERT on CT3 SPA
CSCsc59207	Unknown	IKE SAs not replicating to standby chassis
CSCsc59332	Unknown	CPUHOG: WS-X6748-SFP/WS-X6724-SFP with many copper SFPS installed
CSCsc61086	Unknown	TCAM entry optimization needed for NAT outside i/fs with big NAT cfg
CSCsc61257	Unknown	Software watchdog timeout in Active-SP causes both sups to crash/reload.
CSCsc66102	Unknown	JAC:Minor Error on Ant48, show mod faulty, reset come online
CSCsc74828	Unknown	Rockies3.1: need diags coverage after RPR+ swover due to asic issues
CSCsc80822	Unknown	VPN-SPA - Router fails to decrypt certificate payload during IKE negotia
CSCsc85990	Unknown	EEM policy causes switch to go in tight loop and leak memory
CSCsc88725	Unknown	SPRP ping not triggering the recovery action if only one FIBTCAM device
CSCsc92114	Unknown	Port Power Mismapped On 6148-rj21AF
CSCsc93283	Unknown	R2.5: no mls qos mpls trust exp CLI not effective after reload
CSCsc94266	Unknown	Memory corruption due to Corrupted previous pointer
CSCsc95559	Unknown	R2.5: policy trust effective tho no mls qos mpls tr exp is not config
CSCeg47659	WAN	cRTP packet drops with Enhanced Flexwan
CSCeh48548	WAN	ntp doesnt sync over reconfigured channel-groups
CSCin46297	WAN	show aps shows different status on the master and slave
CSCsb67941	WAN	PA-8T-V35 - MFR config remains even if PA is removed
CSCsb86675	WAN	Multicast Packets are forwarded out on down PVC on ATM Bundle

Resolved Caveats in Release 12.2(18)SXF1

Identifier	Technology	Description
CSCeb05456	Infrastructure	nvram file locking incorrect for remote file operations
CSCsb64585	Multicast	RP is down but multicast routing continues to work
CSCsc73288	platform-76xx	OSM asic error:SRIC packet data CRC error
CSCeh88604	QoS	VIP keeps crashing - with PCI DEVSEL timeout @ classify_packet
CSCsb85748	Unknown	Attempt to open FIB Master failure warning msg occurs after SSO
CSCsb98702	Unknown	Breakpoint (signal 5 exception) when ltl profiling .
CSCsc38127	Unknown	Standby RP crash in qm_stile_adjust_sb_nbar_flags

Resolved Caveats in Release 12.2(18)SXF

Resolved AAA Caveats

- CSCee45312—Resolved in 12.2(18)SXF

  Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

  Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

  Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

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

  More details can be found in the security advisory which posted at the following URL http://www.cisco.com/en/US/products/csa/cisco-sa-20050629-aaa.html

Resolved LAN Caveats

- CSCsa67294—Resolved in 12.2(18)SXF

  Symptom:

  A Cisco Catalyst Switch may reload upon receipt of a malformed VTP packet.

  Conditions:

  The malformed VTP packet must meet the following requirements:

  - Must be received on a port configured for ISL or 802.1q trunking AND
  - Must correctly match the VTP domain name

  This does not affect switch ports configured for the voice vlan.

  Affected platforms:

  Cisco 2900XL Series Cisco 2900XL LRE Series Cisco 2940 Series Cisco 2950 Series Cisco 2950-LRE Series Cisco 2955 Series Cisco 3500XL Series Cisco IGESM

  No other Cisco devices are known to be vulnerable to this issue.

  Workarounds:

  Customers may want to connect ports configured for trunking to known, trusted devices.

Resolved Routing Caveats

- CSCin95836—Resolved in 12.2(18)SXF

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

This advisory is posted at http: //www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml.

Resolved Security Caveats

- CSCeb47225—Resolved in 12.2(18)SXF

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

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

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

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

  Workaround is to remove the “tunnel key”.

Resolved Unknown Caveats

- CSCee71911—Resolved in 12.2(18)SXF

  In Cisco IOS software that includes LSP Verification (LSPV) support, an “LSP Verification Manager” process may be created even if there are no MPLS applications. The process consumes a small amount of memory, but should not consume any CPU resources. The UDP port 3503 is also opened even if there are no MPLS applications.

  There is no workaround.

- CSCsa67611—Resolved in 12.2(18)SXF

  For packets incoming MPLS Tagged and going out as untagged IP (tag to IP case) if output features (like egress ACL, egress WCCP) are applied upon a reload of a switch one may find that the egress features no longer get applied.

  This has been seen with 12.2(17b)SXB6 and 12.2(18d)SXD2.

  Packet impacted Concern : Incoming packet hitting the 6500 with sup720 with one label and exiting the switch on a non mpls int (tag to ip path) on which some output feature are configured (like output acl , output wccp or...)

  Impact : these packet should always be recirculated as there are some output feature. After a reload of the switch recirculation do not happen anymore and as a result all packet bypass the ACL or any output feature.

  Workaround: disable and reapply all output features on the output interface and output feature will start to work again.

- CSCsb52717—Resolved in 12.2(18)SXF

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

  Conditions: Affects all IOS versions that support mVPN MDT.

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

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

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

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

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

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

Other Resolved Caveats in Release 12.2(18)SXF

Identifier	Technology	Description
CSCef77265	AAA	router crashes receiving certain TACACS+ packets
CSCeh84727	AAA	LPIP ARP entries become incompleted after a while
CSCei18359	AAA	AAA leaks memory fragments w/ HQM stack traceback
CSCsa74002	AAA	Input queue - wedged when traffic punted to the CPU
CSCei12574	Access	MPLS-ATOM:FR:VC failed to come up after an OIR of some slot.
CSCei51155	Access	PP:R3:PA-MC-2T3+: Saturation rate drop 50% due to input overrun
CSCsa47223	Access	Packet loss when running software compression with encapsulation PPP.
CSCsb07696	Access	HYPERION-4-HYP_RESET: Hyperion Error Interrupt
CSCsb21867	Access	PA-MC-8TE1+ in Flexwan: ctrlr detects LOS after restart does not recover
CSCdw25402	ATM	RPM-PR card crashed when provisioning bulk connections from CWM
CSCed29265	ATM	Router crash while unconfiguring OSM-ATM interface
CSCeg03837	ATM	ALIGN-3-SPURIOUS traceback in Standby RP when subinterface is configured
CSCeh56916	Content	Router crashed due to WCCP going over allocated buffer.
CSCed56085	Infrastructure	Show flash command for ATA flash device may cause corruption
CSCee73380	Infrastructure	SNMP message processing priorities needs to be changed
CSCee83917	Infrastructure	long snmp cmd line crashes RP with write mem
CSCee92763	Infrastructure	SNMP replies do not source VRF interfaces
CSCef35192	Infrastructure	Exec-timeout not working at more prompt as expected by customer
CSCef59378	Infrastructure	DNS probe fails for fully qualified target name
CSCef78145	Infrastructure	Slave crashed at channel_clear_llc_stats
CSCeh42292	Infrastructure	dLFIoLl mlp-qos : %SCHED-7-WATCH: at bootup with tracebacks
CSCeh49492	Infrastructure	snmpEnginetime gets reset when sysUptime counter rolls over .

Identifier	Technology	Description
CSCeh62781	Infrastructure	%IPC-5-WATERMARK FAST.control.RIL(2070000.E) seat 2070000
CSCeh91772	Infrastructure	extending existing files corrupts filesystem
CSCin88077	Infrastructure	Active SP stuck in slcp process after Test Crash on Active RP
CSCsa58550	Infrastructure	Alignment correction at ipc_process_raw_pak
CSCsa82886	Infrastructure	RP crashes when argument for tftp-server command longer than 67 char
CSCsa86252	Infrastructure	Delete startup-config when show startup is executed
CSCsa86572	Infrastructure	NVRAM corrupts, write erase followed by write mem crashes router
CSCsa92394	Infrastructure	The secondary processor fails to boot after loading the image
CSCsa98777	Infrastructure	Memory corruption on MSFC with syncnlmTable
CSCsb22489	Infrastructure	supervisor crashes on removal of IP VRFs in VRF-LITE config
CSCsb27249	Infrastructure	RP crash @ heartbeat_fatal and RPC timeout message @ Standby SP
CSCsb44308	Infrastructure	Cat6k crashes with no snmp-server
CSCds33629	IPServices	Closing Telnet session crashes router..
CSCeg06261	IPServices	Cat4000: Active FTP fails with 12.2(20)EWA
CSCeg15044	IPServices	Not able to telnet to card (No Free TTYs error)
CSCeh05654	IPServices	HSRP MAC can be set same as i/f MAC, can cause loss of connectivity
CSCeh48684	IPServices	Identification field is 0 in every tacacs packet with SYN
CSCsa57888	IPServices	service tcp-keepalive-in doesnt work on Sup720
CSCsb15224	IPServices	HSRP: wrong HSRP mac addr in ARP reply if multiple HSRP groups are used
CSCsb65340	LAN	i82543: OSPF hellos dropped after sh/no sh of the peer
CSCea48658	LegacyProtocols	DLSw+ is broken with the usage of VRFs
CSCeb47150	LegacyProtocols	Unable to Establish DLSw Peer Connection Through VPN/NAT Tunnel
CSCec64333	Management	Memory leak in SNMP ENGINE while retrieving ciscoIPSEC MIBS
CSCdy86197	MPLS	TE Topology Database Does not show Psuedonodes link-type correctly
CSCef87449	MPLS	RRR LM: Admin shut handler does not preempt LSPs
CSCeh05594	MPLS	MPLS-TE FRR: Router crash in tfib during FRR operation
CSCeh78455	MPLS	Interface description duplication on MPLS/LDP enabled int:ifAlias
CSCeh85817	MPLS	PP:R3:L3vPN:pervrfaggr label:invalid intag,intag=0,on sh/no shu
CSCei51486	MPLS	mpls ldp missing local binding for a loopback intf (imp null)
CSCsa56129	MPLS	MPLS TE tunnel commands not syncd properly
CSCsa77411	MPLS	RP crash at rrr_lm_unlock_bandwidth
CSCsa85588	MPLS	Per VRF Aggregate Label not in lfib
CSCsb04721	MPLS	Targeted LDP session is not established
CSCsb09190	MPLS	Next-hop label missing for non-vpn prefixes with dual RRs
CSCsb32695	MPLS	PE lost aggregate label after shut/no-shut
CSCeg83460	Multicast	c6msfc:bidir pim df not elected with multiple RPs after link down
CSCeh01390	Multicast	MSDP does not create (S,G) when IGMP modifies the (*,G) olist

Identifier	Technology	Description
CSCeh15639	Multicast	crash due to freed nbr while sending PIM hello
CSCeh47667	Multicast	A ddts to commit CSCef60452 to pikespeak
CSCeh50392	Multicast	Static Default Mroute ignores the eigrp unicast routes
CSCeh95160	Multicast	bi-directional PIM DF winner may receive an incorrect unicast metric
CSCei33038	Multicast	multicast helper-map : make TTL option visible
CSCsa79597	Multicast	ip multicast longest-match does not influence PIM BSR RPF
CSCsa89976	Multicast	Software forced reload @ checkheaps_process due to UDP packet forwarding
CSCsb02976	Multicast	MSDP: Need msdp RP non-dr to send triggered SA immediately
CSCsb23433	Multicast	Need to minimize mcast packet loss with intermittent sources
CSCsb27969	Multicast	After SSO switchover IPv6 PIM Encap Tunnel is down, doesnt recover
CSCsb29318	Multicast	Access-list type conflict with filter-sa-request
CSCed52844	platform-76xx	Display of the mcast LTL are incorrect for OSM. Traffic works fine
CSCsa93725	platform-76xx	MR-APS: Working router power cycle causes significant traffic loss
CSCsa95421	platform-76xx	OSM-1OC48-POS-SS+ drops packets
CSCsb13441	platform-76xx	GE-WAN tag-switching MTU broken for RP handled packets again
CSCsb15183	platform-76xx	OSM:Asic [0] error: TXIF: RXPB bad packet len (low)
CSCef07167	PPP	dLFIoFR : VIP crash at dlfi_disable_fragmentation on OIR/micro rel
CSCeg24422	PPP	packet drops with >55% 100B and rest 1500B on dMLP and dMLFR links
CSCeh41652	PPP	Packet classification fails on MFR after RPR-Plus switchover
CSCei08458	PPP	dLFIoATM : FIBDISABLE when 6 sub-interface are created
CSCin44386	PPP	Multilink interface flaps after a router reload
CSCin88026	PPP	VIP may crash @vip_mlp_process_reassemble+0x318 w/dlfi on flap
CSCin91163	PPP	Re-assembly drops seen on peer when sending traffic across bundles
CSCin96524	PPP	LDP/OSPF flap in MLP core with more than line rate traffic
CSCsa56959	PPP	Show policy output counters not updated for process swiched packets
CSCdt12296	QoS	RSVP Path message packets are process switched when data is CEF swit
CSCdv87113	QoS	cbQoSMIB shows random large values for class of service monitor mibs
CSCea64025	QoS	Path tear not forwarded by Merge Point
CSCea65031	QoS	Loading and unloading pdlms removes port-map config from running-con
CSCeb60432	QoS	One resv debug not subject to ACL filters on a Resv change
CSCec26696	QoS	RSVP shows wrong allocated bw in show ip rsvp interface
CSCed71844	QoS	show policy interface locks up the c7500
CSCed75295	QoS	FRR LSP fails to protect with N-Nhop backup tunnel
CSCee56209	QoS	ACL counters double counting
CSCef32588	QoS	RSVP is dropping ResvConfirms on a router with equal cost links
CSCeh31441	QoS	Flexwan module powercycles with shaping+dLFIoATM
CSCeh54083	QoS	random-detect aggregate cmd not working for virtual-template

Identifier	Technology	Description
CSCeh84740	QoS	VIP crash on RPR+ switchover with qos config and high load traffic
CSCei10181	QoS	PP:R3:FW+MLP+MLFR:MALLOCFAIL for LLQ+CBWFQ to hit the LC crash
CSCei16615	QoS	Neighber crash at avl_get_first when shut/no shut tunnel on LSP-head
CSCei24965	QoS	PP:R3: Block qos policy with bandwidth guarantee of > 100%
CSCei65865	QoS	Policy doesnt send modified path to downstream with refresh reductio
CSCsa57101	QoS	Crash in k_rsvpSenderEntry_get
CSCsa87178	QoS	violate-action policed-dscp-transmit defaulted to Drop after bootup
CSCsb01188	QoS	ATM interface on FW/FW2 PA stops tx on add/remove service policy
CSCsb25607	QoS	dLFIoFR: all lp pkts dropped on oversubscribed mixed traffic
CSCsb36818	QoS	Service policies lost on interface bw reconfiguration
CSCdt51547	Routing	Packet drop with ip verify unicast reverse-path.
CSCea49016	Routing	Fix CPUHOG issue with a number of code paths in EIGRP
CSCee19880	Routing	EIGRP routes stuck in routing table when using no ip-next-hop-self
CSCee23634	Routing	OSPF should detect if the neighbor MTU is smaller than our
CSCee26209	Routing	%FIB-4-FIBCBLK: Missing cef table for tableid
CSCee52317	Routing	MFIB: Mcast pkts fail to switch over IPv6-in-IP tunnel
CSCef61721	Routing	IPv6 CEF incorrect entry
CSCef93058	Routing	ARP req was send with delay when each VRF uses same dest IP
CSCeg04110	Routing	MSFC incorrectly ARPS with bridge irb and bridge-group command
CSCeg06612	Routing	Incomplete eigrp config causes memory leak in BGP router
CSCeg07274	Routing	BGP IO process uses excessive CPU during convergence
CSCeg51291	Routing	Ping vrf failed to reach OSPF neighbor interface via sham link
CSCeh00090	Routing	ISIS access-list modification problem
CSCeh09588	Routing	300 second traffic loss with 100 OSPF neighbor after SSO switchover
CSCeh13489	Routing	BGP shouldn't propogate an update w excessive AS Path > 255
CSCeh16989	Routing	BGP number of attributes is constantly increasing, consuming more memory
CSCeh20051	Routing	RIPv2: some statics not redistributed in vrf using rip.
CSCeh31691	Routing	CWAN-MFI: Pos interfaces do not work with PPP encap
CSCeh33504	Routing	Receiving 102K vpnv4 routes, but RRs only reporting 76245 routes.
CSCeh41328	Routing	Multi-topology transition deletes IPv6 routes from RT
CSCeh46993	Routing	distance should not affect ospf path selection within single process
CSCeh53906	Routing	Stale non-bestpath mpath stuck in RIB with soft-reconfiguration
CSCeh54460	Routing	router reloads when two dmvpn tunnels are brought up
CSCeh59619	Routing	traceback@ip_fib_show_path_for_exact,show_ip_forwarding_exact_sessio
CSCeh61778	Routing	GRP crash by SYS-2-WATCHDOG in process IS-IS Update
CSCeh92012	Routing	OSPF did not redistribute route expectedly
CSCei04683	Routing	PP:R3:IPV6:Default ISIS Route Generated from L1/L2 to L2 Router

Identifier	Technology	Description
CSCei06089	Routing	Conditional default-originate with route-map does not work in 28S3
CSCei07805	Routing	PP:R3:SUP3:FIBDISABLE w/ 500 vrf and 200 IPv6 routes after SSO
CSCei12603	Routing	30ms traffic loss on reoptimzation while BW change over TE tunnel
CSCei13040	Routing	ospf routes not installed in the RIB after sub-second intf flap
CSCei26899	Routing	LSNT:Missing prefixes after card reload
CSCei39285	Routing	MALLOCFAIL and CPUHOG traceback-CEF Reloader with bulk CEF entries
CSCei48972	Routing	VPN on FR-sub (vpn1) does not recover after rpr+ switchover
CSCei58597	Routing	RP crashes at ospf_router_lsa_max_metric_cmd during bootup
CSCei58655	Routing	ISIS not aging version of LSP in isis local rib
CSCei75375	Routing	OSPFv3: Router crashes when area deleted
CSCin65241	Routing	ISIS: redistribute commands not being synced to standby RP
CSCsa50971	Routing	Access-list resequence command causes unexpected reload
CSCsa51095	Routing	ISIS authentication not working on p2p LAN links after reload
CSCsa61872	Routing	isis routes disappeared from routing table after shut/no shut GE int
CSCsa70039	Routing	OSPF: connected network learnt via ospf after interface flap or shutdown
CSCsa70188	Routing	LC marked as FIB Disable even after OIR
CSCsa73843	Routing	DMVPN - Buffer leak due to delayed NHRP processing
CSCsa73847	Routing	Static arp entry removed from running configuration with NAT enabled
CSCsa74271	Routing	OSPF NSF not working, traffic drops for a few seconds
CSCsa75512	Routing	PP: RP crash at ospf_flood_over_one_idb
CSCsa78259	Routing	IOS reload due to specific BGP routing update
CSCsa80861	Routing	BGP to IGP redistribution broken with mutual redistribution points
CSCsa87034	Routing	clear bgp ipv4 unicast command does not clear Routing table
CSCsa87473	Routing	BGP:MPLS/VPN: After reload PE missing prefixes from RR.
CSCsa88145	Routing	fib tracebacks at sso when large number of tunnel interfaces are config
CSCsa90719	Routing	Configuring pasive/no passive for ISIS crashes router
CSCsa95973	Routing	OSPF processes summaries from non-BB links after switchover on ABR
CSCsa97090	Routing	FIBNULLIDB in pre-rewrite CEF
CSCsa97101	Routing	FIBNULLIDB in create path due to race condition
CSCsa98059	Routing	OSPF not flushing external LSA from BGP redist on route change
CSCsb08380	Routing	iSPF does not check existing route when attaching stub network
CSCsb12896	Routing	SSO:routes in a vrf is not synced in CEF between active and standby
CSCsb18066	Routing	ip routing protocol purge interface does not work
CSCsb28595	Routing	Ospf NSSA N1/N2 routes causing summary route to be maxaged and flushed
CSCsb36550	Routing	CPUHOG by OSPF Router process
CSCsb36589	Routing	7600 hits breakpoint exception just when ospf neighbors lost.
CSCsb46607	Routing	msfc3 crashed in chunk_free_with_pc with %SYS-2-CHUNKNOROOT

Identifier	Technology	Description
CSCsb49133	Routing	summary-add nssa LSA does not get updated when FA interface goes down
CSCsb69773	Routing	Router Crash with BGP at bgp_netlist_validate
CSCuk57124	Routing	Handling of seq epoch after switchover needs to be robust
CSCdy80670	Security	SCHED-3-THRASHING error messages in TTY Background process
CSCed84769	Security	DMVPN: IKE/IPsec SAs expire/rebuild every 2 minutes
CSCsa77158	Security	Router stops accepting SSH IPv6 connections, IPv4 SSH still works
CSCsa78580	Security	Crypto IKMP process can get blocked if router fails to fetch CRL
CSCsa81928	Security	CRL checking fails if PKI URI recevied for CDP is UPPER CASE
CSCdz84448	Unknown	Spurious memory access when querying the cbQosREDClassStatsTable
CSCeb70508	Unknown	Dirty bit is not synced over to Standby
CSCeb82779	Unknown	Server sockets cause the VTY lines to lock up
CSCec21114	Unknown	show memory summary shows junk pointing to tcl_chunk_malloc_create
CSCec21537	Unknown	Per-VRF radius source-interface not used in legacy code path
CSCec70695	Unknown	Remove "compact-only" sw mode restriction for ERSPAN's working on Sup720
CSCec72111	Unknown	RADIUS: pre-PAPAPA code does not use the per SG source-interface
CSCec84396	Unknown	CLI: tclsh causes router crash
CSCed21601	Unknown	Need to syslog excessive system controller resets
CSCed33129	Unknown	Crash at Tcl_FindCommand while loading script
CSCed94829	Unknown	IOS reloads due to malformed IKE messages
CSCee01435	Unknown	show power command shows PS-Fan status as n/a
CSCee07889	Unknown	Server sockets cause the VTY line to lock up
CSCee42846	Unknown	Aborting TCL gets command via Ctrl-c in tclsh causes CPU hog/crash
CSCee46575	Unknown	Enhanced object tracking improvements, including IP addr detection
CSCee58827	Unknown	SLB crash with replicate slave enabled without replicate casa
CSCee93598	Unknown	LSP ping/trace explicit null shimming capability
CSCef07048	Unknown	SecurID New PIN mode fails with VPN Client
CSCef46923	Unknown	Group of 4 ports on WS-X6516-xx modules may stop forwarding traffic
CSCef80151	Unknown	Switch should create vlan.dat if not present
CSCef84400	Unknown	Tcl typeahead command causes router to crash on SIGBUS
CSCeg02753	Unknown	CDP broken with native vlan other then 1
CSCeg07394	Unknown	router reload @ tcl_chunk_free
CSCeg39518	Unknown	Infinite loop on dsx1FarEndIntervalIndex
CSCeg54004	Unknown	packet loss with ACL range statement
CSCeh17426	Unknown	Memory leak in mfib_const_handle_gce_ltl_event after stress
CSCeh19465	Unknown	CSG, impossible to apply a content/policy pair to a service
CSCeh23943	Unknown	SIP1:dCRTP:Not all pkts compressed at Tx, errors at Rx
CSCeh24021	Unknown	PM_SCP-SP-4_UNK_OPCODE:Received unsolicited messge on SSO swover

Identifier	Technology	Description
CSCeh25105	Unknown	The Router crashes during Event Manager Policy registration process.
CSCeh29617	Unknown	PP:Sup3:FRoMPLS:CHOC:pkts dropped on egr (PE-CE)link (ping fails)
CSCeh31230	Unknown	FIB-STDBY-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF int errors
CSCeh31550	Unknown	MPLS:VPN:MLPPP:ce-pe B2B ping fails with multilink and vrf configure
CSCeh34089	Unknown	CSCeg07394 causes router crash when EEM Tcl policies run
CSCeh35237	Unknown	7600: 6748GE LC OIR causes spurious mem access and traceback
CSCeh35849	Unknown	New PIN mode and next token code fail with vpn client
CSCeh37316	Unknown	align-3-spurious:spurious memory access with sup720
CSCeh40465	Unknown	NSF/SSO failover time too long when using supervisor uplinks
CSCeh41511	Unknown	PP::mls qos ip output broken for policy without drop action
CSCeh41997	Unknown	EEM Tcl policies leak significant memory upon every run
CSCeh42348	Unknown	PP:CWAN-QOS:DWRED is broken
CSCeh43531	Unknown	CAT6K: router reloaded under stress
CSCeh45653	Unknown	EEM applets need to pass session username to EEM cli library.
CSCeh47169	Unknown	c38/2800 crashed by resetting CUE at get_block
CSCeh49742	Unknown	sup720: NMI not working and show version has wrong reason
CSCeh51395	Unknown	Trunk vlan wont revert to the original when reconfigured
CSCeh51894	Unknown	12.2SXE2: TestLoopback and TestInlineRewrite failed diags
CSCeh53682	Unknown	MACs Learned on EtherChannel across L2 Fwding Engine Get Off-sync
CSCeh53775	Unknown	catalyst 6500 does not answer ipv6 traceroute
CSCeh54217	Unknown	GTP-SLB should not reassign session when sticky object exists
CSCeh54386	Unknown	Ucast flooding due to MACs losing PI_E flag when SPAN is configured
CSCeh54533	Unknown	IOS SLB with Egress ACL under SVI breaks L2 icmp traffic
CSCeh55293	Unknown	Physical EVC to poch EVC conversion may fail if poch has no member
CSCeh56398	Unknown	T48+, G+-CR2 in C+/Legacy configuration boot with multiple errors
CSCeh56439	Unknown	ATM SPA may reject wred policy
CSCeh59654	Unknown	Ucast flooding due to +MN received on DFC/PFC when DEC is configured
CSCeh62351	Unknown	ALIGN-1-FATAL:Corrupted program counter. Show Tech cause router cash
CSCeh62522	Unknown	igmp snooping source only doesnt work for certain range of group ad
CSCeh62562	Unknown	acctg type change implies content config erased in SXD4 image
CSCeh65221	Unknown	VPNSM: Pkt looping to wmac
CSCeh65615	Unknown	Rockies2:TestL3VlanMet failed online diag on T48+
CSCeh69436	Unknown	VTP mode ignored in startup-config
CSCeh71584	Unknown	7600 as dmvpn spoke does not work with VRFs
CSCeh73049	Unknown	tclsh mode bypasses aaa command authorization check
CSCeh73110	Unknown	Ucast flooding due to +MN/-MN race condition
CSCeh80649	Unknown	SPA: Packets stop passing after T3 line flap

Identifier	Technology	Description
CSCeh81794	Unknown	chassis crash due to memory corruption
CSCeh82971	Unknown	Router crashed at watcher_delete_common during FPD upgrade
CSCeh85087	Unknown	WCCP stops after a redirect list is configured
CSCeh85135	Unknown	CSG SUP720 support missing for IPSERVICES images
CSCeh87476	Unknown	show platform tech-support ipmulticast needs support for BiDir
CSCeh96957	Unknown	Need to disable Turbo ACL support for Sup2 and Sup720 in 12.2SX
CSCei00856	Unknown	CWAN-QOS:oc-3:col2 crash with external memory address
CSCei01237	Unknown	SLB: %SYS-3-CPUHOG messages and crash running slb processes
CSCei02695	Unknown	PP:R3:SIP-200: BCP functionality is broken after linecard OIR
CSCei02826	Unknown	PP:R3:All VoIP(even UDP port) cRTP PKTs were dropped in input queue
CSCei06406	Unknown	Ping failure/Wrong C-Shim Hdr on Serial Intf. removed from MLP
CSCei09755	Unknown	SPA-CT3/CHOC-Serial intf line proto down after removing from bundle
CSCei10218	Unknown	Cronos APS: APS states not getting sync in SSO
CSCei10228	Unknown	CHOC12/DS0 APS:LC power cycles with SSO s/o, APS state wrong on stdb
CSCei12585	Unknown	Crash while configuring from VTY and Console simultaneously
CSCei13379	Unknown	no ip add sec deletes all mls ip mult connect entries in vlan
CSCei16701	Unknown	PP:R3: SPA ATM/FR MPB: Failed to forward MCAST PKTs from SVI INTF
CSCei18018	Unknown	Diagnostics HM crash
CSCei20107	Unknown	DFC3A reloaded due to sman interrupt after memory allocation failure.
CSCei20996	Unknown	MPLS-VPN:Ping packet doesnt go through with osm srp interface.
CSCei21293	Unknown	PP:R3:OC-48 ATM SPA: LC OIR causing traceback + %ENT_API-4-NOALIAS
CSCei22697	Unknown	mvpn tunnel is miss-matched to different VPN rte/fwd table
CSCei24139	Unknown	PP:R3:SIP-200: CPU 1 crash on doing linecard reset with ATM SPA
CSCei30764	Unknown	PP:R3:MVPN:multiple diff tunnels created on some VRFs
CSCei30999	Unknown	PP:R3:SIP-200 drops 30% of VoIP traffics on cRTP sessions
CSCei32920	Unknown	Tracking reports wrong line pcol status for dot1q trunk (switchport cmd)
CSCei33598	Unknown	PP:R3:SIP-200:CT3 SPA:T3 contr stays down after remote router reload
CSCei37465	Unknown	After a firmware upgrade the firmware.cfg is corrupted
CSCei37692	Unknown	GTP SLB broken when <mls ip slb search wildcard rp> configured
CSCei38036	Unknown	layer 2 entry not removed when no int vlan
CSCei38898	Unknown	Facility to cache and display process_may_suspend events trigger by MDSS
CSCei39029	Unknown	JAC:show CBL fail to display port state after clear trunk
CSCei39181	Unknown	SIP200/POS-SPA:APS states not synced to standby in SSO
CSCei40939	Unknown	PP:R3:MLFR SPA:MEM corruption Bad deqeueue & dmfr_process_rcv_packet
CSCei41088	Unknown	MVPN Tunnel interface not created with BGP Confedetration
CSCei41653	Unknown	ISIS neighbor can not be setup on WS-SVC-IPSEC-1
CSCei48635	Unknown	ChOC3/STM-1 SPA: many MFR interfaces remain down following microcode

Identifier	Technology	Description
CSCei51175	Unknown	PP:R3:SIP-200:1490 bridging - CPU1 crash with egress pol on main int
CSCei52441	Unknown	default ACL programming not correct under certain condition
CSCei61913	Unknown	PP R3:CHOC12/DS0 SSO:no shut not synced to stdby, traffic stop on HA
CSCei63781	Unknown	Inlinerewrite test fails on WS-X6148A-GE-TX
CSCei64940	Unknown	Service Module sourced packet dropped when recirculation required
CSCei67673	Unknown	Memory leak during execute-on
CSCei76358	Unknown	cleanup of user interface data
CSCei86192	Unknown	PP:R3:FlexWAN+PA-8xT1/E1: RP crashed MALLOCFAIL due to loveletter
CSCei93397	Unknown	SPA-CTE1: Fails at configuration if HW version is 2.0 or greater
CSCej08820	Unknown	Cannot apply vacl on rspan vlan
CSCin78324	Unknown	PA-MC-8TE1+: check to drop runts packets missing in driver code
CSCin78325	Unknown	PA-MC-8TE1+ admindown serial interfaces continue to process packets
CSCin90971	Unknown	Enhanced FlexWAN FPD Package needs to be bundled with IOS image
CSCin91290	Unknown	show ip slb replicate output mismatch in Active and Standby
CSCin91381	Unknown	dmfr: Linecard may crash @dmfr_process_rcv_packet on intf flap
CSCin92518	Unknown	ERSPAN filter vlan CLI rejected for vlan range
CSCin94752	Unknown	SLB crash in slb_probe_wc_install
CSCin96328	Unknown	Switching fails with sip-200 reset followed by sup switchover
CSCsa48259	Unknown	VPN-SM: rp crash triggered by crypto_ss_print_table
CSCsa56229	Unknown	Traceback mesg seen when standby SUP comes online on Port security
CSCsa57222	Unknown	Intermittent RP Crash seen with maximum mflow plcrs
CSCsa58933	Unknown	Flapping occurs after converting L2 Portchannel to L3
CSCsa60107	Unknown	Traffic drop with IGMPv3 on a snooping enabled VLAN
CSCsa62758	Unknown	Spanning-tree statistics inaccurate in show interface accounting
CSCsa68043	Unknown	MPB:FR: Mac-address table entries are unknown on standby sup on bootup
CSCsa68717	Unknown	ATM subinterfaces no found in IF-MIB after module power down/up
CSCsa69060	Unknown	packets tagged with agg label not matched by CPP
CSCsa70104	Unknown	leak in flexwan with netflow and AAA together
CSCsa70274	Unknown	LSP trace crash when rx of dsmap with multipath length set to 0.
CSCsa70494	Unknown	TX Chnl Queue Overflow events on freedm with traffic + router reload
CSCsa70679	Unknown	NDE record has extra record after reload
CSCsa70835	Unknown	SUp720 may see random packet loss when host leaves or joins; OIF +- 85
CSCsa71097	Unknown	WS-X6148-45AF/WS-X6148-21AF in Sup slot, wrong power allocated
CSCsa71295	Unknown	show mod indicates Unknown diag status for SIP cards after switchover
CSCsa71875	Unknown	%ALIGN-3-SPURIOUS With SNMP and Dot3 Stats
CSCsa73607	Unknown	SLB probes not restarted on real admin flap
CSCsa74075	Unknown	show interface capability show duplex = none on WS-X6704-10GE module

Identifier	Technology	Description
CSCsa74464	Unknown	Bus error after config synch of CSM
CSCsa74926	Unknown	CDP enabled on FWSM gig interfaces.
CSCsa76016	Unknown	NAT netflow entyr created without reason
CSCsa76530	Unknown	Mcast over GRE Tunn gets S/W switched after SSO when over L3 PortChannel
CSCsa76801	Unknown	Major bootup failure on Sup720 causing other linecards to PwrDown
CSCsa76812	Unknown	ICC gets stuck after reload if RM agiing is configured to no_aging
CSCsa76833	Unknown	%PFINIT-SP-5-CONFIG_SYNC: Sync'ing the startup to stb...index set to 147
CSCsa77084	Unknown	IntMacRx-Err counts TX errors
CSCsa77105	Unknown	LSP ping shouldn't be sent out untagged interfaces
CSCsa77410	Unknown	CSM:C2R2: show mod csm sticky cmd shows garbage real server ip address
CSCsa77655	Unknown	System keeps crashing if PF_REDUN_CRASH_COUNT is not set properly
CSCsa78705	Unknown	Memleak in l3_mgr_tunnel_is_hw_not_supported_internal after stress
CSCsa79713	Unknown	linecard image download fails after RPR, causes crash
CSCsa80358	Unknown	Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks
CSCsa81282	Unknown	Flowcontrol Oper status On when port is shutdown
CSCsa81344	Unknown	Incorrect flowcontrol output for LACP Sub-portchannels
CSCsa82334	Unknown	SUPW crashes with invalid VTP packet & wit debugs enabled for vtp
CSCsa82640	Unknown	LSP ping/traceroute times out at untagged hop for MFI images
CSCsa82912	Unknown	CPUHOG for scp_lc_event_mgr on switchover of sup2
CSCsa83541	Unknown	qm_chkpt_add_plcr_to_label msg seen on standby on applying policy
CSCsa85123	Unknown	Cisco 7609 :OSM-1CHOC12DS0-SI :RFI bit should be undefined for VC-12
CSCsa85229	Unknown	CPUHOGs and watchdog timeout at earl_well_known_adj
CSCsa85752	Unknown	H/w entry creation for SSM over GRE Tunnel toggles cont. after reload
CSCsa86103	Unknown	gre keepalives are not punted to rp on return path, tunnel flaps
CSCsa86954	Unknown	PortSec adds specific addr to secure table when rx cdp packet.
CSCsa87127	Unknown	Some features using re-direct index fail on RPR+ switchover SSO working
CSCsa89506	Unknown	WS-X6704-10GE flowcontrol negotiation does not work
CSCsa89917	Unknown	unable to change dot1x max-req vlaue and dot1x timeout tx-period
CSCsa90830	Unknown	WCCP ingress redirect in Mask assign/GRE mode not using ACL TCAM Adj
CSCsa91166	Unknown	GTP SLB : Cannot assign same sticky group to two different gtp vservers
CSCsa91175	Unknown	no login authentication appears as default after vty is configured
CSCsa91749	Unknown	A router may reload when trying to free memory at clear_path_ids
CSCsa91816	Unknown	c6k sends notPresent Temperature StatusValue Value =0 trap
CSCsa92571	Unknown	WS-X6704 line card fails fabric test upon reload
CSCsa94063	Unknown	Rockies2: Mroute Active Rate counter is not updated properly
CSCsa95287	Unknown	MIB OID csgQuotaMgrStats missing in the snmpwalk
CSCsa95660	Unknown	SP may crash if it follows some code path

Identifier	Technology	Description
CSCsb01009	Unknown	Bidir RP *,G/m entries not populated in hardware in some cases
CSCsb01086	Unknown	CSG: Newly configured VLAN not allowed on trunk until module reload
CSCsb01729	Unknown	show platform tech-support ipmulticast command problems on EARL7
CSCsb01861	Unknown	cat6000: 'mls acl tcam default-result permit' command is broken
CSCsb02590	Unknown	Changing the RP bridge from 0x381 to 0x387
CSCsb03192	Unknown	VPNSMi:DMVPN: incorrect socket created in spoke after hub add changed
CSCsb04346	Unknown	crash l2_aging_proc after changing Spantree mode
CSCsb05822	Unknown	Make *,G/m hardware programming consistent with IOS software behavior
CSCsb06233	Unknown	Lepus: RP Crashed @mdss_scan_mroute_mvrf_cache with neg Test
CSCsb06413	Unknown	Output RACL with UDP range command breaks multicast
CSCsb08236	Unknown	QoS Merge called for every modification of IP named ACL
CSCsb08489	Unknown	vlan delete breaks SPAN
CSCsb09997	Unknown	Enhanced FlexWAN: dropping IS-IS 01:80:C2:00:00:14-15 packets as BPDUs
CSCsb10031	Unknown	Catalyst 6500 Rapid-PVST port will not recover from PVID inconsistent
CSCsb10226	Unknown	DMVPN: rp crash trig by crypto_ss_print in the hub
CSCsb10662	Unknown	PI_E lost on Supervisror after +MN received on DEC with Plus
CSCsb11224	Unknown	system crashes soon after changes in cos-mutation map
CSCsb12076	Unknown	VPN-SM: GRE RP pkts coming to IPSec with tvlan causing route flaps
CSCsb13267	Unknown	Traffic lost on Sup720 Etherchannel after standby reloaded
CSCsb13885	Unknown	Tracebacks at process_watch_boolean & sm_post_event after switchover.
CSCsb14175	Unknown	SLB real servers stay at MAXCONN after open/close IP PDP with sticky on
CSCsb14185	Unknown	SLB reals move to failed on PROBE_ABDICATE with per-packet vservers
CSCsb14306	Unknown	GTP SLB may reload when gtp sticky unconfiged during PDP deletion
CSCsb14855	Unknown	s720 : Packet might be dropped in case IOS-SLB and egress ACL used.
CSCsb15156	Unknown	Missing MAC addr cause LDP flap after switchover if explicit-null set
CSCsb16051	Unknown	traffic should not flood to all LC in L3 distrinuted port-channel
CSCsb16146	Unknown	FREEBAD: Bus error at ace_polo_send_hapi
CSCsb16396	Unknown	Unicast flooding with Shut on one of the DEC members
CSCsb16475	Unknown	Etherchannel throughput limited message with WS-X6548-GE-TX
CSCsb17320	Unknown	Mcast src-only timer does not work for configured timer intervals
CSCsb18740	Unknown	High cpu utilisation with heavy WCCP-redirected traffic
CSCsb23906	Unknown	spurious memory accesses with 12.2(18)SXE1 in cwan_convert_mac_address
CSCsb24320	Unknown	PP:R3:VPLS+QoS:PWAN2: shaping queue is not created after bootup
CSCsb26773	Unknown	Cat6500 Sup720: Inbound ACL may cause WCCP redirection to fail
CSCsb29783	Unknown	Cat6500 may crash if dot1x auth is disabled during authentication
CSCsb29951	Unknown	IEEE 802.1x authentication time is high (~150 sec for 270 supplicants)
CSCsb32028	Unknown	%CPU_MONITOR-2-NOT_RUNNING: CPU_MONITOR tracebacks and crash

Identifier	Technology	Description
CSCsb32099	Unknown	Packet with Less than 33 bytes payload gets dropped
CSCsb33744	Unknown	service-policy stops packets via MPLS / VPN
CSCsb34354	Unknown	netflow process hogs SP cpu even after netflow is disabled
CSCsb34985	Unknown	const_mpls_prog_vlan_recirc_adj: bad params vlan keep logged & CPU high
CSCsb36874	Unknown	DHCP packet corruption with snooping enabled
CSCsb37618	Unknown	GTP SLB: Doesnt relay create response to SGSN even after max reassigns
CSCsb38242	Unknown	LSP Traceroute shows no labels when last hop P is a 7600 12.2 18 SXE
CSCsb38273	Unknown	L3 Traffic flood over DEC due to incorrect Flood region FPOE
CSCsb38396	Unknown	No traffic passes out MFR sub ints after shut / no shut on 1xCHOC3/ChSTM
CSCsb38885	Unknown	RRI routes dont get deleted after VPNSM reload with HA configuration
CSCsb41562	Unknown	Unable to change flowmask after enable NAT
CSCsb44185	Unknown	24port and 12port restrictions with PVLAN will go off after OIR of card
CSCsb46887	Unknown	MET entry misprogrammed due to high rate of multicast traffic
CSCsb48015	Unknown	All bundle links do not recover following MFR bundle flap
CSCsb49530	Unknown	Device crashes while unconfig switchport
CSCsb49891	Unknown	module clear-config should decrease interface count shown in show ver
CSCsb50559	Unknown	Need fix for MWAM for CSCee10005
CSCsb50995	Unknown	PP:R3: VPLS: memory fragmentation on SP by AToM LC smgr code
CSCsb54233	Unknown	ISIS hello not rcved on dot1q sub interface on a WS-X6582-2PA
CSCsb55343	Unknown	linkDown trap sent out for control plane interface when sys bootup
CSCsb59349	Unknown	Standby RP crashed on applying policy to 1k SVI
CSCsb61530	Unknown	show mls netflow ip command tree changes
CSCsb63090	Unknown	syntax for action_switch parsed incorrectly
CSCsb70303	Unknown	CSM: CSM hang or both become active/active after rpr+ switchover
CSCsb71242	Unknown	MMLS NSF/SSO: Mcast Failover time very high for the first switchover
CSCec40868	WAN	FlexWan interfaces dont appear in ifTable when using one SUP
CSCef71011	WAN	Trans/Bridging: All pings fail when serial(atm-dxi) in use.
CSCeg04325	WAN	CPUHOG in process = Serial Background
CSCeh17470	WAN	traffic shape traceback seen while modifying FR interface dlci num
CSCeh34067	WAN	FlexWAN+PAs: SUP3 RP crash at mfr_set_output_seq() under stress
CSCeh35068	WAN	Frame-relay:CEF adjacency is not established until flap the interfac
CSCeh41080	WAN	PP:FW2:MIV:Marking does not work,either basic or with policer.
CSCeh68965	WAN	large ospf packets truncated when f/r ietf
CSCeh97017	WAN	PP:R3:(FlexWAN+cRTP): show ip rtp header-compression fails to count
CSCsa43553	WAN	After RPR+ switchover, flexwans ingress traffic doesnt hit SLB
CSCsa80223	WAN	Error adding idb to macaddr idb list messages are logged on console

Identifier	Technology	Description
CSCsb09250	WAN	Flexwan - spurious accesses at cwpa_egress
CSCsb64812	WAN	Memory Leak Net Background process

Caveats in Release 12.2(18)SXE and Rebuilds

Open Caveats in Release 12.2(18)SXE and Rebuilds

Identifier	Technology	Description
CSCsa87178	QoS	violate-action policed-dscp-transmit defaulted to Drop after bootup
CSCee25454	Unknown	SADB peering process leaks memory after overnight test
CSCeh52330	Unknown	SPA-CT3: EFC Parity Error reported by SPA FPGA
CSCsa57222	Unknown	Intermittent RP Crash seen with maximum mflow plcrs

Resolved Caveats in Release 12.2(18)SXE6b

Resolved Infrastructure Caveats

- CSCsc64976—Resolved in 12.2(18)SXE6b

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

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

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20051201-http.html

Resolved LegacyProtocols Caveats

- CSCsf28840—Resolved in 12.2(18)SXE6b

  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 Management Caveats

- CSCsf07847—Resolved in 12.2(18)SXE6b

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

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

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

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

Resolved Security Caveats

- CSCsb12598—Resolved in 12.2(18)SXE6b

  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/warp/public/707/cisco-sa-20070522-SSL.shtml

  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.

Other Resolved Caveats in Release 12.2(18)SXE6b

Identifier	Technology	Description
CSCsg70355	Infrastructure	adopt new default summer-time rules from Energy Policy Act of 2005.
CSCse78963	Infrastructure	adopt new default summer-time rules from EPA BADCODE BUG
CSCse04560	IPServices	tftp-server allows for information disclosure .
CSCsd92405	Security	router crashed by repeated SSL connection with malformed finished messag

Identifier	Technology	Description
CSCsg36726	Unknown	Bonham parity errors may cause packet loss on a 7600-SIP-400 module.
CSCsd44517	Unknown	flow control needs to be toggle off/on to become active after no shut

Resolved Caveats in Release 12.2(18)SXE6a

Resolved Infrastructure Caveats

- CSCsf04754—Resolved in 12.2(18)SXE6a

  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 Unknown Caveats

- CSCsd75273—Resolved in 12.2(18)SXE6a

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

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

  A Cisco Security Advisory for this vulnerability is posted at
  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

- CSCse52951—Resolved in 12.2(18)SXE6a

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

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

  A Cisco Security Advisory for this vulnerability is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

Resolved Voice Caveats

- CSCsc60249—Resolved in 12.2(18)SXE6a

  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 Resolved Caveats in Release 12.2(18)SXE6a

Identifier	Technology	Description
CSCek44025	QoS	Hierarchy is not collapsed when FRF.12 is configured
CSCse73539	Unknown	c7600 - crash of active sup720 after inserting a second one

Resolved Caveats in Release 12.2(18)SXE6

Resolved LAN Caveats

- CSCsd34759—Resolved in 12.2(18)SXE6

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

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

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

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

  These vulnerabilities are addressed by Cisco IDs:

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

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

http://www.cisco.com/en/US/products/csr/cisco-sr-20060913-vtp.html

Resolved Routing Caveats

- CSCsd40334—Resolved in 12.2(18)SXE6

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

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

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

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html

Resolved Unknown Caveats

- CSCsd68605—Resolved in 12.2(18)SXE6

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

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

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

Other Resolved Caveats in Release 12.2(18)SXE6

Identifier	Technology	Description
CSCsb11698	AAA	Input Queue Wedge with TACACs
CSCsb12329	ATM	ifAdminStatus of ATM sub-interface is down without shutdown command
CSCef11195	Infrastructure	MIPS platforms take Address Error Exception in malloc()
CSCei32102	Infrastructure	Need an option to disable snmp traps for link during switch failover
CSCeg61169	IPServices	Traceback recorded in tcb_isvalid by TCP Remote Shell Process .
CSCeh35083	IPServices	NAT-PPTP change Call ID wrongly
CSCsd80754	IPServices	HSRP Active-Router not respond to ARP request about VIP
CSCsd34855	LAN	VTP update with a VLAN name >100 characters causes buffer overflow .
CSCsd94687	LAN	sh vlans counters and SNMP counters are incosistent for subif
CSCsd41981	MPLS	TFIB on SUP720 PFC is broken when an OSM (GE-WAN) card was disabled
CSCsb76434	Multicast	PIM: auto-rp group stuck in registering when sparse-mode
CSCse05336	platform-76xx	Packet drop on OSM-2+4GE-WAN+ if sub-if is created or deleted
CSCeh62084	PPP	ifStackStatus drops ifIndex when interface is OperStatus down

Identifier	Technology	Description
CSCsd71119	QoS	ALL ATM PVC DOWN IN FLEXWAN WITH PA-A3-OC3 AND OAM
CSCed87897	Routing	sh ip route missed default gateway after ip default-net command
CSCef11304	Routing	MIB walk on OSPF-MIB involving ospfExtLsdbTable crashes switch
CSCef35386	Routing	BGP does not inform PIM of the second best VPNv4-MDT
CSCeg07274	Routing	BGP IO process uses excessive CPU during convergence
CSCeg52659	Routing	BGP route may not get withdrawn under rare condition
CSCeg77104	Routing	EIGRP neigh over ATM IMA link flaps due to Authentication failure
CSCei26899	Routing	LSNT:Missing prefixes after card reload
CSCsa81039	Routing	EIGRP PE-CE:routing loop when a prefix has no cost-community
CSCsc73436	Routing	BGP: touching neighbor policies causes peer's table version to reset
CSCsc76327	Routing	EIGRP PE-CE: Constant route-flap with a redistributed VRF-static-route
CSCsd03882	Routing	SUP720 RACL Deny ACE not being implemented
CSCsd12904	Routing	OSPF sham-links do not come up
CSCsa63387	Security	Router may crash when CRL expires
CSCsc72722	Security	CBAC - firewall resets TCP idle timer upon receiving invalid TCP packets
CSCsd43903	Security	Memory leak in Crypto IKMP process when using certificate authentication
CSCse11457	Security	show crypto ca timers shows static output
CSCse12154	Security	Bus error crash after executing secure copy (scp)
CSCee34346	Unknown	%EARL-SP-4-EBUS_SEQ_ERROR: Out of Sync error. Errorcode 0x4C10020
CSCeh21210	Unknown	MF: DHCP Snooping crash when server send invalid option 82
CSCeh78411	Unknown	Failed IKE sessions does not get deleted in certain conditions
CSCei06406	Unknown	Ping failure/Wrong C-Shim Hdr on Serial Intf. removed from MLP
CSCei27448	Unknown	Router crashes while displaying sh ip pim mdt bgp
CSCek26186	Unknown	ATM SPA: setup vp fails.
CSCek42027	Unknown	SPA FPD upgrade fails with sip1-CR
CSCin98448	Unknown	controller shut throws up error msg and remote end is not going down
CSCsa85229	Unknown	CPUHOGs and watchdog timeout at earl_well_known_adj
CSCsa86954	Unknown	PortSec adds specific addr to secure table when rx cdp packet.
CSCsa87388	Unknown	cat6000 : ciscoEnvMonTempStatusChangeNotif to many traps - VDB inlet
CSCsb18740	Unknown	High cpu utilisation with heavy WCCP-redirected traffic
CSCsb33258	Unknown	RP crash while mvpns come up - MDFS buildup
CSCsb80141	Unknown	IOS-SLB: no mls ip slb search icmp does not work.
CSCsb91644	Unknown	IPv6 MFIB entry is updated on RP and delayed to update MFIB on SP & DFC
CSCsc24102	Unknown	Fabric sync errors if WS-X6704-10GE is on slot 4 on 7606
CSCsc43862	Unknown	SPA ping failure caused by SIP-200 serial primary channel sync failure
CSCsc65256	Unknown	Connection Count incorrect after ungraceful disconnect/reconnect
CSCsc75381	Unknown	Native vlan mismatch is not detected if native not allowed on trunk .

Identifier	Technology	Description
CSCsc91075	Unknown	IPSEC Connection Count incorrect after unsuccesfull connection attempt
CSCsc92114	Unknown	Port Power Mismapped On 6148-rj21AF
CSCsd05513	Unknown	7600 CBQOS-MIB is missing info which is present in CLI
CSCsd14307	Unknown	PA-MC-8TE1+ PA shows alarm led red even with all controllers shut down
CSCsd19203	Unknown	SIP400:ATM:new LLQ traffic stop flowing on dynamic changes to Policy
CSCsd25532	Unknown	High SP-CPU utili occurs when c7600 recieves IPv6 Multicast traffic
CSCsd33647	Unknown	ER: Improve C2 MET programming under heavy traffic scenarios
CSCsd45167	Unknown	Memory leak in Crypto IKMP Process
CSCsd49723	Unknown	Memory leak in Crypto IKMP Process when using certificate authentication
CSCsd49767	Unknown	Memory leak in Crypto IKMP process
CSCsd56549	Unknown	GRE doesnt get the same port that it req, PPTP change Call ID wrongly
CSCsd58552	Unknown	cwpa2: TCP to NAT addresses cause FR encap change from IETF to cisco
CSCsd90501	Unknown	Minimum/Maximum WRED thresholds for default DSCP stays at 32/64
CSCsd94541	Unknown	Multiple T3 controllers bounce on the SPA
CSCsd98887	Unknown	SP Memory Leak In mls-msc Process
CSCse15728	Unknown	VPNSM does not perform invalid spi recovery in vrf mode

Resolved Caveats in Release 12.2(18)SXE5

Resolved AAA Caveats

- CSCed09685—Resolved in 12.2(18)SXE5

  Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

Other Resolved Caveats in Release 12.2(18)SXE5

Identifier	Technology	Description
CSCeg62070	Infrastructure	Tracebacks noticed with Radius configs through HTTP Post
CSCeh62781	Infrastructure	%IPC-5-WATERMARK FAST.control.RIL(2070000.E) seat 2070000
CSCej08355	Infrastructure	Memory corruption on MSFC with syncnlmTable
CSCsb22489	Infrastructure	supervisor crashes on removal of IP VRFs in VRF-LITE config
CSCsc08741	Infrastructure	Sup720 may experience Memory leak in *Dead*/Parser-Mode History Table pr
CSCsc44237	Infrastructure	memory leak in client applications iterating over an empty idb list
CSCsc82214	Infrastructure	Bus error crash at SrCheckClassMIBView
CSCsb16512	MPLS	High CPU in CEF Process and CEF scanner due to prefix reresolve

Identifier	Technology	Description
CSCei13579	Multicast	consolidation of some post-reload PIM blackhole issues
CSCek26627	Multicast	CPUHOG when RPF change affects ~30k mroutes
CSCsb23433	Multicast	Need to minimize mcast packet loss with intermittent sources
CSCsb64585	Multicast	RP is down but multicast routing continues to work
CSCsc16148	Multicast	Allow (S,G) expiry timer to be configurable
CSCsc73288	platform-76xx	OSM asic error:SRIC packet data CRC error
CSCin44386	PPP	Multilink interface flaps after a router reload
CSCsa56959	PPP	Show policy output counters not updated for process swiched packets
CSCsb74603	PPP	Router generated traffic does not match output policy
CSCsb97950	PPP	dLFIoATM: Packets with CLP set, get punted to RP.
CSCee58986	QoS	fair-queue nvgen does not happen
CSCsb36818	QoS	Service policies lost on interface bw reconfiguration
CSCsc25204	QoS	Divide by zero at udivmoddi4 when using the show policy-map command
CSCsc95511	QoS	Bus error crash at hqf_scheduler_info_init
CSCea34586	Routing	Bus error crash in ip_arp_merge process
CSCef61721	Routing	IPv6 CEF incorrect entry
CSCeh16989	Routing	BGP number of attributes is constantly increasing, consuming more memory
CSCeh53906	Routing	Stale non-bestpath mpath stuck in RIB with soft-reconfiguration
CSCei07805	Routing	PP:R3:SUP3:FIBDISABLE w/ 500 vrf and 200 IPv6 routes after SSO
CSCei53226	Routing	BGP: fix updgrps for non private-as peers with remove-private-as
CSCei75375	Routing	OSPFv3: Router crashes when area deleted
CSCsa79783	Routing	Loosing routes after reload/OIR when ispf enabled
CSCsa87473	Routing	BGP:MPLS/VPN: After reload PE missing prefixes from RR.
CSCsb09852	Routing	BGP: pathless nets not freed when updgrp members are out of sync
CSCsb24535	Routing	clear ip bgp update-group [ip address] clears all the bgp peers
CSCsb36550	Routing	CPUHOG by OSPF Router process
CSCsb37553	Routing	IPv6 : nexthop address inaccesible after clear bgp ipv6 nei soft
CSCsb40115	Routing	BGP: Failed to find expected # of multipath entries
CSCsb80866	Routing	PE global IP address shows up in traceroute VRF
CSCsc03828	Routing	OSPF continues to advertise a def route to NSSA w/no default route in RT
CSCsc50692	Routing	Global static route w/ non /32 mask to vrf loopback is unroutable
CSCsa67272	Security	Serial number in certificate subject is incorrect
CSCsc52105	Security	ipsec may leak Crypto IKMP memory blocks
CSCee84918	Unknown	DHCP snooping on 3550 drops DHCPNAKs recieved when renewing old IP
CSCee86692	Unknown	LAN-to-LAN tunnel doesnt get established with DPD configured
CSCee93598	Unknown	LSP ping/trace explicit null shimming capability
CSCeg39518	Unknown	Infinite loop on dsx1FarEndIntervalIndex

Identifier	Technology	Description
CSCeh17756	Unknown	ASSERT may not function properly with dual PEs and CEs
CSCeh49742	Unknown	sup720: NMI not working and show version has wrong reason
CSCeh80649	Unknown	SPA: Packets stop passing after T3 line flap
CSCei10218	Unknown	Cronos APS: APS states not getting sync in SSO
CSCei10228	Unknown	CHOC12/DS0 APS:LC power cycles with SSO s/o, APS state wrong on stdb
CSCei21293	Unknown	PP:R3:OC-48 ATM SPA: LC OIR causing traceback + %ENT_API-4-NOALIAS
CSCei22697	Unknown	mvpn tunnel is miss-matched to different VPN rte/fwd table
CSCei30764	Unknown	PP:R3:MVPN:multiple diff tunnels created on some VRFs
CSCei33598	Unknown	PP:R3:SIP-200:CT3 SPA:T3 contr stays down after remote router reload
CSCei37672	Unknown	chevys/c2lc take ~ 180s before resetting following a mandatory proc exit
CSCei38036	Unknown	layer 2 entry not removed when no int vlan
CSCei39181	Unknown	SIP200/POS-SPA:APS states not synced to standby in SSO
CSCei48635	Unknown	ChOC3/STM-1 SPA: many MFR interfaces remain down following microcode
CSCei61913	Unknown	PP R3:CHOC12/DS0 SSO:no shut not synced to stdby, traffic stop on HA
CSCei67673	Unknown	Memory leak during execute-on
CSCei80699	Unknown	multicast tunnel if_number numbers being duplicated
CSCei86192	Unknown	PP:R3:FlexWAN+PA-8xT1/E1: RP crashed MALLOCFAIL due to loveletter
CSCej21698	Unknown	EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
CSCej57810	Unknown	ifOperStatus for Control Plane Interface is always down
CSCej78055	Unknown	Patch CSCei31646,CSCei19659 and CSCej25957 to SXE4 LATEST
CSCej87462	Unknown	SNMP set not-in-service to crcERSpanIFEntry corrupts mem
CSCek03772	Unknown	zamboni: crashes for double fragmentaion
CSCin96328	Unknown	Switching fails with sip-200 reset followed by sup switchover
CSCsa70494	Unknown	TX Chnl Queue Overflow events on freedm with traffic + router reload
CSCsa80620	Unknown	ct3 spa: serial interface efc queue stuck on deleting/adding mlp bundle
CSCsa83541	Unknown	qm_chkpt_add_plcr_to_label msg seen on standby on applying policy
CSCsa85123	Unknown	Cisco 7609 :OSM-1CHOC12DS0-SI :RFI bit should be undefined for VC-12
CSCsa85752	Unknown	H/w entry creation for SSM over GRE Tunnel toggles cont. after reload
CSCsb00473	Unknown	CT3: Scaled config in T1 SF mode fails
CSCsb01861	Unknown	cat6000: 'mls acl tcam default-result permit' command is broken
CSCsb08512	Unknown	SCP subcmd SUBCMD_GET_LTLS_FOR_INDEX_RANGE response is corrupted
CSCsb11224	Unknown	system crashes soon after changes in cos-mutation map
CSCsb12969	Unknown	MQC: Router crashes when a service-policy is added to atm or FR pvc
CSCsb15156	Unknown	Missing MAC addr cause LDP flap after switchover if explicit-null set
CSCsb31368	Unknown	ATM Multipoint bridging on c65xx is broken after SW upgrade
CSCsb34213	Unknown	Few destination ports removed from RSPAN vlan flood index after SSO
CSCsb38396	Unknown	No traffic passes out MFR sub ints after shut / no shut on 1xCHOC3/ChSTM

Identifier	Technology	Description
CSCsb46887	Unknown	MET entry misprogrammed due to high rate of multicast traffic
CSCsb49326	Unknown	Cat6K crashes after EPLD upgrade of WS-X6548-GE-TX
CSCsb50559	Unknown	Need fix for MWAM for CSCee10005
CSCsb54233	Unknown	ISIS hello not rcved on dot1q sub interface on a WS-X6582-2PA
CSCsb62566	Unknown	Add an option to power-down the LC when fabric error is detected
CSCsb66799	Unknown	URL match statement removed from configuration after reload
CSCsb67152	Unknown	MET inconsistent on DFC, multicast traffic is blackholed for an OIF
CSCsb70996	Unknown	IOS SLB drops trailing fragments in VRF and misroutes SLB msgs to GGSN
CSCsb79031	Unknown	Clear counter caused the MSFC to reload the SUP due to RPC timeout
CSCsb80590	Unknown	Enhance IPC buffer usage and IOMEM buffer allocation for Flexwan
CSCsb84746	Unknown	Memory leak ed at qm_process_enqueue/qm_mqc_mesg_to_process
CSCsb85049	Unknown	cwpa2 bridged/routed ATM PDUs lost between Flexwan2 and SUP720
CSCsb85589	Unknown	enable explicit-null cause ldp keeps flapping after switchover
CSCsb89241	Unknown	BRE LTL is not populated properly after reload for flexwan2
CSCsb98702	Unknown	Breakpoint (signal 5 exception) when ltl profiling .
CSCsc00603	Unknown	Sup22 :uRPF check is disabled globally when disabled on any single i/f
CSCsc03429	Unknown	JQL: Linecard in the slot for SUP reloaded by changing redundancy mode
CSCsc03864	Unknown	Service Module sourced packet dropped when recirculation required
CSCsc04015	Unknown	cbQosCMStatsTable doesn't return byte statistic for FastEthernet PAs
CSCsc05210	Unknown	Incoming dscp not trusted after upgrading from 12.2SXD to 12.2SXE
CSCsc05500	Unknown	ENTITY-MIB: SFP in Gi1/1 is not displayed in show inventory
CSCsc05838	Unknown	Changing Sticky Cookie from Dynamic to Insert will corrupt sticky table
CSCsc06620	Unknown	Memory corruption when span session is removed from service module
CSCsc07793	Unknown	Stdby sup reloads after setting stpxMSTInstanceEditVlansMap
CSCsc13720	Unknown	llq functionality with _match input vlan_ broken
CSCsc26048	Unknown	Cat6k: CPUHOG in PIM Snooping Process
CSCsc26490	Unknown	wrong static mac address entry in case of GLBP virtual mac
CSCsc32198	Unknown	IGMP per-port leave with multiple leave nested cases disturbs mcast strm
CSCsc33990	Unknown	Enhancements and Optimizations to TestSPRP InbandPing
CSCsc52306	Unknown	IDSM: span tree not blocking when two IDSM in inline mode
CSCsc52645	Unknown	SIP1-CT3: Whole T1 goes down while doing timeslot BERT on CT3 SPA
CSCsc55949	Unknown	C2 Frequent fabric channel sync errors and rxErrors
CSCsc57156	Unknown	Hardware fault on FWSM ports not causing FWSM redundancy failover
CSCsc59207	Unknown	IKE SAs not replicating to standby chassis
CSCsc61086	Unknown	TCAM entry optimization needed for NAT outside i/fs with big NAT cfg
CSCsc61257	Unknown	Software watchdog timeout in Active-SP causes both sups to crash/reload.
CSCsc68250	Unknown	Packet flow halt on 7600-SIP-400

Identifier	Technology	Description
CSCsc88725	Unknown	SPRP ping not triggering the recovery action if only one FIBTCAM device
CSCsc89044	Unknown	IO memory leak with big buffers and EOBC0/0
CSCsc93283	Unknown	R2.5: no mls qos mpls trust exp CLI not effective after reload
CSCsc93607	Unknown	R2.5:RP crash when del service policy after del no mls qos mpls tr exp
CSCsc94266	Unknown	Memory corruption due to Corrupted previous pointer
CSCsc95559	Unknown	R2.5: policy trust effective tho no mls qos mpls tr exp is not config
CSCsd15806	Unknown	r2.5:Tcam is not programmed after shut/no shut on interface
CSCsd20092	Unknown	Device crashes with fabric error on bootup starting from 28th build
CSCeg47659	WAN	cRTP packet drops with Enhanced Flexwan
CSCeh48548	WAN	ntp doesnt sync over reconfigured channel-groups
CSCin46297	WAN	show aps shows different status on the master and slave
CSCsb67941	WAN	PA-8T-V35 - MFR config remains even if PA is removed
CSCsd04219	WAN	Add feature support for ACLs in 12.2SXE on virtual templates

Resolved Caveats in Release 12.2(18)SXE4

Resolved Routing Caveats

- CSCin95836—Resolved in 12.2(18)SXE4

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070808-nhrp.html.

Resolved Unknown Caveats

- CSCsb52717—Resolved in 12.2(18)SXE4

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

  Conditions: Affects all IOS versions that support mVPN MDT.

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

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

  ```
  !
  ```

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

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

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

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

Other Resolved Caveats in Release 12.2(18)SXE4

Identifier	Technology	Description
CSCei51155	Access	PP:R3:PA-MC-2T3+: Saturation rate drop 50% due to input overrun
CSCsb21867	Access	PA-MC-8TE1+ in Flexwan: ctrlr detects LOS after restart does not recover
CSCdw25402	ATM	RPM-PR card crashed when provisioning bulk connections from CWM
CSCsb44308	Infrastructure	Cat6k crashes with no snmp-server
CSCds33629	IPServices	Closing Telnet session crashes router..
CSCeg06261	IPServices	Cat4000: Active FTP fails with 12.2(20)EWA
CSCeh48684	IPServices	Identification field is 0 in every tacacs packet with SYN
CSCsb15224	IPServices	HSRP: wrong HSRP mac addr in ARP reply if multiple HSRP groups are used
CSCec64333	Management	Memory leak in SNMP ENGINE while retrieving ciscoIPSEC MIBS
CSCsb09190	MPLS	Next-hop label missing for non-vpn prefixes with dual RRs
CSCsb32695	MPLS	PE lost aggregate label after shut/no-shut
CSCeh93087	Multicast	Need triggered Bidir RP Cache update
CSCeh95160	Multicast	bi-directional PIM DF winner may receive an incorrect unicast metric
CSCsb02976	Multicast	MSDP: Need msdp RP non-dr to send triggered SA immediately
CSCsa93725	platform-76xx	MR-APS: Working router power cycle causes significant traffic loss
CSCsb15183	platform-76xx	OSM:Asic [0] error: TXIF: RXPB bad packet len (low)
CSCdt12296	QoS	RSVP Path message packets are process switched when data is CEF swit
CSCed71844	QoS	show policy interface locks up the c7500
CSCee56209	QoS	ACL counters double counting
CSCeh31441	QoS	Flexwan module powercycles with shaping+dLFIoATM
CSCsb01188	QoS	ATM interface on FW/FW2 PA stops tx on add/remove service policy
CSCsb25607	QoS	dLFIoFR: all lp pkts dropped on oversubscribed mixed traffic
CSCee01688	Routing	NAS crashes at ip2access_add_acl_item() while running stress test
CSCeh09588	Routing	300 second traffic loss with 100 OSPF neighbor after SSO switchover

Identifier	Technology	Description
CSCeh20051	Routing	RIPv2: some statics not redistributed in vrf using rip.
CSCeh92012	Routing	OSPF did not redistribute route expectedly
CSCej21891	Routing	crash in rip_update_dbase when default-information originate used
CSCin65241	Routing	ISIS: redistribute commands not being synced to standby RP
CSCsa50971	Routing	Access-list resequence command causes unexpected reload
CSCsa87034	Routing	clear bgp ipv4 unicast command does not clear Routing table
CSCsa95973	Routing	OSPF processes summaries from non-BB links after switchover on ABR
CSCsb08380	Routing	iSPF does not check existing route when attaching stub network
CSCsb69773	Routing	Router Crash with BGP at bgp_netlist_validate
CSCdy80670	Security	SCHED-3-THRASHING error messages in TTY Background process
CSCdz84448	Unknown	Spurious memory access when querying the cbQosREDClassStatsTable
CSCee01435	Unknown	show power command shows PS-Fan status as n/a
CSCef07048	Unknown	SecurID New PIN mode fails with VPN Client
CSCeg03733	Unknown	Sprious Alignment and crash with MIB walk in Cisco Class Based QoS
CSCeh35237	Unknown	7600: 6748GE LC OIR causes spurious mem access and traceback
CSCeh35849	Unknown	New PIN mode and next token code fail with vpn client
CSCeh41511	Unknown	PP::mls qos ip output broken for policy without drop action
CSCeh53682	Unknown	MACs Learned on EtherChannel across L2 Fwding Engine Get Off-sync
CSCeh55293	Unknown	Physical EVC to poch EVC conversion may fail if poch has no member
CSCeh61467	Unknown	Router crashes at pim_reset_updated_nbr on uncfging mdt group
CSCeh73049	Unknown	tclsh mode bypasses aaa command authorization check
CSCeh73110	Unknown	Ucast flooding due to +MN/-MN race condition
CSCeh81794	Unknown	chassis crash due to memory corruption
CSCeh87476	Unknown	show platform tech-support ipmulticast needs support for BiDir
CSCei01237	Unknown	SLB: %SYS-3-CPUHOG messages and crash running slb processes
CSCei02695	Unknown	PP:R3:SIP-200: BCP functionality is broken after linecard OIR
CSCei02826	Unknown	PP:R3:All VoIP(even UDP port) cRTP PKTs were dropped in input queue
CSCei09755	Unknown	SPA-CT3/CHOC-Serial intf line proto down after removing from bundle
CSCei16701	Unknown	PP:R3: SPA ATM/FR MPB: Failed to forward MCAST PKTs from SVI INTF
CSCei20107	Unknown	DFC3A reloaded due to sman interrupt after memory allocation failure.
CSCei20996	Unknown	MPLS-VPN:Ping packet doesnt go through with osm srp interface.
CSCei24139	Unknown	PP:R3:SIP-200: CPU 1 crash on doing linecard reset with ATM SPA
CSCei30999	Unknown	PP:R3:SIP-200 drops 30% of VoIP traffics on cRTP sessions
CSCei33393	Unknown	Drops on sup720 with certain queue-limit and WRED threshold values
CSCei37465	Unknown	After a firmware upgrade the firmware.cfg is corrupted
CSCei37692	Unknown	GTP SLB broken when <mls ip slb search wildcard rp> configured
CSCei41088	Unknown	MVPN Tunnel interface not created with BGP Confedetration

Identifier	Technology	Description
CSCei51175	Unknown	PP:R3:SIP-200:1490 bridging - CPU1 crash with egress pol on main int
CSCei52441	Unknown	default ACL programming not correct under certain condition
CSCei64940	Unknown	Service Module sourced packet dropped when recirculation required
CSCei76358	Unknown	cleanup of user interface data
CSCei80006	Unknown	Same Proxy, Multiple Peers, both RRI routes deleted
CSCei93397	Unknown	SPA-CTE1: Fails at configuration if HW version is 2.0 or greater
CSCin78325	Unknown	PA-MC-8TE1+ admindown serial interfaces continue to process packets
CSCin94752	Unknown	SLB crash in slb_probe_wc_install
CSCsa69060	Unknown	packets tagged with agg label not matched by CPP
CSCsa70274	Unknown	LSP trace crash when rx of dsmap with multipath length set to 0.
CSCsa76801	Unknown	Major bootup failure on Sup720 causing other linecards to PwrDown
CSCsa76812	Unknown	ICC gets stuck after reload if RM agiing is configured to no_aging
CSCsa77655	Unknown	System keeps crashing if PF_REDUN_CRASH_COUNT is not set properly
CSCsa80358	Unknown	Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks
CSCsa82640	Unknown	LSP ping/traceroute times out at untagged hop for MFI images
CSCsa82912	Unknown	CPUHOG for scp_lc_event_mgr on switchover of sup2
CSCsa91175	Unknown	no login authentication appears as default after vty is configured
CSCsa95287	Unknown	MIB OID csgQuotaMgrStats missing in the snmpwalk
CSCsa95660	Unknown	SP may crash if it follows some code path
CSCsb01086	Unknown	CSG: Newly configured VLAN not allowed on trunk until module reload
CSCsb02590	Unknown	Changing the RP bridge from 0x381 to 0x387
CSCsb03192	Unknown	VPNSMi:DMVPN: incorrect socket created in spoke after hub add changed
CSCsb04346	Unknown	crash l2_aging_proc after changing Spantree mode
CSCsb10662	Unknown	PI_E lost on Supervisror after +MN received on DEC with Plus
CSCsb12076	Unknown	VPN-SM: GRE RP pkts coming to IPSec with tvlan causing route flaps
CSCsb14175	Unknown	SLB real servers stay at MAXCONN after open/close IP PDP with sticky on
CSCsb14306	Unknown	GTP SLB may reload when gtp sticky unconfiged during PDP deletion
CSCsb16146	Unknown	FREEBAD: Bus error at ace_polo_send_hapi
CSCsb16396	Unknown	Unicast flooding with Shut on one of the DEC members
CSCsb16475	Unknown	Etherchannel throughput limited message with WS-X6548-GE-TX
CSCsb23906	Unknown	spurious memory accesses with 12.2(18)SXE1 in cwan_convert_mac_address
CSCsb24320	Unknown	PP:R3:VPLS+QoS:PWAN2: shaping queue is not created after bootup
CSCsb29783	Unknown	Cat6500 may crash if dot1x auth is disabled during authentication
CSCsb29951	Unknown	IEEE 802.1x authentication time is high (~150 sec for 270 supplicants)
CSCsb33744	Unknown	service-policy stops packets via MPLS / VPN
CSCsb34354	Unknown	netflow process hogs SP cpu even after netflow is disabled
CSCsb34985	Unknown	const_mpls_prog_vlan_recirc_adj: bad params vlan keep logged & CPU high

Identifier	Technology	Description
CSCsb36874	Unknown	DHCP packet corruption with snooping enabled
CSCsb37618	Unknown	GTP SLB: Doesnt relay create response to SGSN even after max reassigns
CSCsb38242	Unknown	LSP Traceroute shows no labels when last hop P is a 7600 12.2 18 SXE
CSCsb38273	Unknown	L3 Traffic flood over DEC due to incorrect Flood region FPOE
CSCsb38885	Unknown	RRI routes dont get deleted after VPNSM reload with HA configuration
CSCsb48015	Unknown	All bundle links do not recover following MFR bundle flap
CSCsb48739	Unknown	GTP SLB:Session reassigned even when sticky entry exists
CSCsb55343	Unknown	linkDown trap sent out for control plane interface when sys bootup
CSCsb60453	Unknown	Need improved logs for severe fabric errors which triggers fab swover
CSCsb70303	Unknown	CSM: CSM hang or both become active/active after rpr+ switchover
CSCsb70335	Unknown	Flexwan crash when fragmentation is enabled under MFR interface
CSCsb70973	Unknown	igmp snooping explicit tracking and report suppression issues
CSCsb71242	Unknown	MMLS NSF/SSO: Mcast Failover time very high for the first switchover
CSCsb77592	Unknown	7600/6500 crash by removing ACL tied with vpn configuration.
CSCsb77716	Unknown	dot1x:SP crash at sm_destroy_instance on OIR or link flap
CSCsb79590	Unknown	MST: designated port doesnt become boundary geting TC from other region
CSCsb84405	Unknown	dscp mutation not working after reload
CSCsb84998	Unknown	MLS-MSC ASSERTION FAILED with T/Bs after hw-module reset
CSCsb95851	Unknown	Cat6K crashing by bus error at msc_sc2vdb_unlink
CSCeg04325	WAN	CPUHOG in process = Serial Background
CSCeh97017	WAN	PP:R3:(FlexWAN+cRTP): show ip rtp header-compression fails to count
CSCsa43553	WAN	After RPR+ switchover, flexwans ingress traffic doesnt hit SLB
CSCsa80223	WAN	Error adding idb to macaddr idb list messages are logged on console
CSCsb09250	WAN	Flexwan - spurious accesses at cwpa_egress
CSCsb64812	WAN	Memory Leak Net Background process
CSCsb86675	WAN	Multicast Packets are forwarded out on down PVC on ATM Bundle

Resolved Caveats in Release 12.2(18)SXE3

Identifier	Technology	Description
CSCsb09190	MPLS	Next-hop label missing for non-vpn prefixes with dual RRs
CSCei76358	Unknown	cleanup of user interface data
CSCeh73049	Unknown	tclsh mode bypasses aaa command authorization check

Resolved Caveats in Release 12.2(18)SXE2

Resolved AAA Caveats

- CSCee45312—Resolved in 12.2(18)SXE2

  Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

  Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

  Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

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

  More details can be found in the security advisory which posted at the following URL http://www.cisco.com/en/US/products/csa/cisco-sa-20050629-aaa.html

Resolved Security Caveats

- CSCeb47225—Resolved in 12.2(18)SXE2

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

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

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

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

  Workaround is to remove the “tunnel key”.

Other Resolved Caveats in Release 12.2(18)SXE2

Identifier	Technology	Description
CSCei12574	Access	MPLS-ATOM:FR:VC failed to come up after an OIR of some slot.
CSCsa82886	Infrastructure	RP crashes when argument for tftp-server command longer than 67 char
CSCsa98777	Infrastructure	Memory corruption on MSFC with syncnlmTable
CSCef87449	MPLS	RRR LM: Admin shut handler does not preempt LSPs
CSCeh05594	MPLS	MPLS-TE FRR: Router crash in tfib during FRR operation
CSCeh78455	MPLS	Interface description duplication on MPLS/LDP enabled int:ifAlias
CSCsa85588	MPLS	Per VRF Aggregate Label not in lfib
CSCeg83460	Multicast	c6msfc:bidir pim df not elected with multiple RPs after link down
CSCeh01390	Multicast	MSDP does not create (S,G) when IGMP modifies the (*,G) olist
CSCsb13441	platform-76xx	GE-WAN tag-switching MTU broken for RP handled packets again

Identifier	Technology	Description
CSCeh41652	PPP	Packet classification fails on MFR after RPR-Plus switchover
CSCeh54083	QoS	random-detect aggregate cmd not working for virtual-template
CSCsa57101	QoS	Crash in k_rsvpSenderEntry_get
CSCeh13489	Routing	BGP shouldn't propogate an update w excessive AS Path > 255
CSCeh61778	Routing	GRP crash by SYS-2-WATCHDOG in process IS-IS Update
CSCsa73843	Routing	DMVPN - Buffer leak due to delayed NHRP processing
CSCsa74271	Routing	OSPF NSF not working, traffic drops for a few seconds
CSCsa78259	Routing	IOS reload due to specific BGP routing update
CSCsa80861	Routing	BGP to IGP redistribution broken with mutual redistribution points
CSCsa98059	Routing	OSPF not flushing external LSA from BGP redist on route change
CSCsb18066	Routing	ip routing protocol purge interface does not work
CSCsa78580	Security	Crypto IKMP process can get blocked if router fails to fetch CRL
CSCsa81928	Security	CRL checking fails if PKI URI recevied for CDP is UPPER CASE
CSCee58827	Unknown	SLB crash with replicate slave enabled without replicate casa
CSCeh40945	Unknown	Same MAC addreees are learnt by different VLAN
CSCeh51894	Unknown	12.2SXE2: TestLoopback and TestInlineRewrite failed diags
CSCeh54217	Unknown	GTP-SLB should not reassign session when sticky object exists
CSCeh54533	Unknown	IOS SLB with Egress ACL under SVI breaks L2 icmp traffic
CSCeh56398	Unknown	T48+, G+-CR2 in C+/Legacy configuration boot with multiple errors
CSCeh56439	Unknown	ATM SPA may reject wred policy
CSCeh62351	Unknown	ALIGN-1-FATAL:Corrupted program counter. Show Tech cause router cash
CSCeh62522	Unknown	igmp snooping source only doesnt work for certain range of group ad
CSCeh65221	Unknown	VPNSM: Pkt looping to wmac
CSCeh65615	Unknown	Rockies2:TestL3VlanMet failed online diag on T48+
CSCeh71584	Unknown	7600 as dmvpn spoke does not work with VRFs
CSCeh82971	Unknown	Router crashed at watcher_delete_common during FPD upgrade
CSCei00856	Unknown	CWAN-QOS:oc-3:col2 crash with external memory address
CSCei16381	Unknown	Same MAC addreees are learnt by different VLAN
CSCei18018	Unknown	Diagnostics HM crash
CSCin78324	Unknown	PA-MC-8TE1+: check to drop runts packets missing in driver code
CSCin90971	Unknown	Enhanced FlexWAN FPD Package needs to be bundled with IOS image
CSCsa48259	Unknown	VPN-SM: rp crash triggered by crypto_ss_print_table
CSCsa70835	Unknown	SUp720 may see random packet loss when host leaves or joins; OIF +- 85
CSCsa77084	Unknown	IntMacRx-Err counts TX errors
CSCsa78705	Unknown	Memleak in l3_mgr_tunnel_is_hw_not_supported_internal after stress
CSCsa87127	Unknown	Some features using re-direct index fail on RPR+ switchover SSO working
CSCsa89917	Unknown	unable to change dot1x max-req vlaue and dot1x timeout tx-period

Identifier	Technology	Description
CSCsa90830	Unknown	WCCP ingress redirect in Mask assign/GRE mode not using ACL TCAM Adj
CSCsa91166	Unknown	GTP SLB : Cannot assign same sticky group to two different gtp vservers
CSCsa91749	Unknown	A router may reload when trying to free memory at clear_path_ids
CSCsa91816	Unknown	c6k sends notPresent Temperature StatusValue Value =0 trap
CSCsa94063	Unknown	Rockies2: Mroute Active Rate counter is not updated properly
CSCsb01729	Unknown	show platform tech-support ipmulticast command problems on EARL7
CSCsb09997	Unknown	Enhanced FlexWAN: dropping IS-IS 01:80:C2:00:00:14-15 packets as BPDUs
CSCsb10226	Unknown	DMVPN: rp crash trig by crypto_ss_print in the hub
CSCsb17320	Unknown	Mcast src-only timer does not work for configured timer intervals
CSCeh68965	WAN	large ospf packets truncated when f/r ietf

Resolved Caveats in Release 12.2(18)SXE1

Identifier	Technology	Description
CSCsa76290	Unknown	Inter-fabric throughput in MPLS CE to PE is much lower than 18SXD.

Resolved Caveats in Release 12.2(18)SXE

Resolved Infrastructure Caveats

- CSCee18471—Resolved in 12.2(18)SXE

  Symptom: v1/v2c users and snmp community acl is not synced to standby.

  Workaround: Use communities instead of v1/v2c users. There is no workaround for acl not being synced to standby.

  Condition: The device should support HA/SSO.

Resolved IPServices Caveats

- CSCee50294—Resolved in 12.2(18)SXE

  Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20041110-dhcp .

  There are multiple workarounds for this issue: There are four possible workarounds for this vulnerability:

  - Disabling the dhcp service
  - Control Plane Policing
  - Two versions of Access Control Lists

  Disabling the DHCP Service

  This vulnerability can be mitigated by utilizing the command:

  ```
  no service dhcp
  ```

  However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

  Control Plane Policing Feature

  The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

  ```
  access-list 140 deny   udp host 192.168.13.1 any eq bootps
  access-list 140 deny   udp any host 192.168.13.1 eq bootps
  access-list 140 deny   udp any host 255.255.255.255 eq bootps
  access-list 140 permit udp any any eq bootps

  class-map match-all bootps-class
    match access-group 140

  policy-map control-plane-policy
    class bootps-class

       police 8000 1500 1500 conform-action drop exceed-action drop

  control-plane
   service-policy input control-plane-policy
  ```

For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

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

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 140 deny   udp host 192.168.13.1 any eq bootps
access-list 140 deny   udp any host 192.168.13.1 eq bootps
access-list 140 deny   udp any host 255.255.255.255 eq bootps
access-list 140 permit udp any any eq bootps

class-map match-all bootps-class
  match access-group 140

policy-map control-plane-policy
  class bootps-class

     police 8000 1500 1500 conform-action drop exceed-action drop

control-plane
 service-policy input control-plane-policy
```

For this example 192.168.13.1 is a legitimate DHCP server.

Additional information on the configuration and use of the CPP feature can be found at this link:

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

This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
access-list 100 deny   udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
access-list 100 deny   udp any host 192.168.13.2 eq bootps
access-list 100 remark deny bootps from any to router loopback1
```

```
access-list 100 deny   udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any

access-list 100 is applied to f0/0 and f1/0 physical interfaces.

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround.

This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny   udp any any eq bootps

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

- CSCef84255—Resolved in 12.2(18)SXE

  Description: An IOS router that is NOT configured for MSDP and connected to a peer router that is configured for MSDP may see packets remaining in the input queue.

  Symptoms: The interface input queue of a router may fill with packets, denying further traffic from being received on that interface.

  Workarounds: MSDP traffic can be filtered from the offending peer, or appropriately configure MSDP on the affected device.

- CSCed78149—Resolved in 12.2(18)SXE

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Resolved LAN Caveats

- CSCsa67294—Resolved in 12.2(18)SXE

  Symptom: A Cisco Catalyst Switch may reload upon receipt of a malformed VTP packet.

  Conditions: The malformed VTP packet must meet the following requirements:

  - Must be received on a port configured for ISL or 802.1q trunking AND
  - Must correctly match the VTP domain name

  This does not affect switch ports configured for the voice vlan.

  Affected platforms:

  - Cisco 2900XL Series
  - Cisco 2900XL LRE Series
  - Cisco 2940 Series
  - Cisco 2950 Series
  - Cisco 2950-LRE Series
  - Cisco 2955 Series
  - Cisco 3500XL Series
  - Cisco IGESM

  No other Cisco devices are known to be vulnerable to this issue.

  Workarounds: Customers may want to connect ports configured for trunking to known, trusted devices.

Resolved Management Caveats

- CSCdz54403—Resolved in 12.2(18)SXE

  Symptoms: A Cisco router may crash when IPSec IKE SNMP variables are retrieved, and a bus error and a traceback may be logged.

  Conditions: This symptom is observed when at least one SA is established. The symptom does not always occur, but when you retrieve the IPSec IKE SNMP variables once every 10 minutes, the router eventually crashes after a few hours.

  Workaround: The workaround is to block access to the CISCO-IPSEC-FLOW-MONITOR-MIB - [or just the cikeTunnelTable] using SNMP views so that no one walks this MIB and cause this crash.

- CSCed11835—Resolved in 12.2(18)SXE

  Symptoms: A Cisco 7200 VXR router that terminates a large number of IPSec tunnels may restart unexpectedly.

  Conditions: This symptom is observed when IKE MIB variables are being polled on the router.

  Workaround: Avoid polling of IKE MIB variables.

Resolved MPLS Caveats

- CSCsa52940—Resolved in 12.2(18)SXE

  Symptoms: A Cisco HE router running MPLS traffic engineering may crash with a memory corruption footprint or with a bus error. If the P and PE routers are running a release prior to 12.0(26)S or 12.2S Cascades, then all of the downstream midpoint routers may crash with similar symptoms.

  Conditions: More than 10 LSPs for a single MPLS-TE session must be signalled in a specific way, which is not supported nor used by Cisco IOS.

  Multiple LSPs for a single session will only happen when the router is under great stress because of many tunnels or breakage somewhere else in the network.

  Note that this is not a problem when MPLS-TE tunnels are signalled with verbatim LSPs, because Cisco routers signal verbatim LSPs do not use this type of signalling.

  Workaround: None

Resolved Routing Caveats

- CSCee67450—Resolved in 12.2(18)SXE

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command bgp log-neighbor-changes configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  Cisco has made free software available to address this problem.

  This issue is tracked by CERT/CC VU#689326.

  This advisory will be posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050126-bgp.html

- CSCef48336—Resolved in 12.2(18)SXE

  OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89.

  A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

  Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

  Using OSPF Authentication can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice.

  A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack.

  Workarounds:

  – Using OSPF Authentication

    OSPF authentication may be used as a workaround. OSPF packets without a valid key will not be processed. MD5 authentication is highly recommended, due to inherent weaknesses in plain text authentication. With plain text authentication, the authentication key will be sent unencrypted over the network, which can allow an attacker on a local network segment to capture the key by sniffing packets.

Refer to http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtml for more information about OSPF authentication.

- Infrastructure Access Control Lists

  Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered 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 white paper "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs:

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

- CSCef68324—Resolved in 12.2(18)SXE

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

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

  More details can be found in the security advisory that is posted at:

  http://www.cisco.com/en/US/products/csa/cisco-sa-20050729-ipv6.html

- CSCef61610—Resolved in 12.2(18)SXE

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Dont' Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCeb88239—Resolved in 12.2(18)SXE

  Symptoms: A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.

  Conditions: This symptom is observed when the **ipv6 debug rip** command is enabled on the router. Malformed packets can normally be sent locally. However, when the **ipv6 debug rip** command is enabled, the crash can also be triggered remotely. Note that RIP for IPv4 is not affected by this vulnerability.

  Workaround: There is no workaround.

- CSCec85929—Resolved in 12.2(18)SXE

  Sympotom: Router may reload when users issue **show running-config**.

  Conditions: If users configures ISIS with tag name longer than 42 characters, router may reload when users issue **show running-config**

  Workaround: Use ISIS tag name short than 42 characters.

- CSCef60659—Resolved in 12.2(18)SXE

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

- CSCec71950—Resolved in 12.2(18)SXE

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet’s IP header. No other IP protocols are affected by this issue.

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

  There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing.

This advisory is available at:

http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-crafted-ip-option.html

- CSCef67682—Resolved in 12.2(18)SXE

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

  The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

  This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognises as its own.

  This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

  We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html contain fixes for this issue.

Resolved Security Caveats

- CSCed65285—Resolved in 12.2(18)SXE

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the “Workarounds” section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050406-ssh.html

Resolved Unknown Caveats

- CSCee59999—Resolved in 12.2(18)SXE

  Symptoms: When auto-reconnect is configured on an EzVPN server and an EzVPN client attempts to connect, failures may occur in AAA accounting.

  The output of the **debug crypto isakmp aaa** command on the EzVPN server shows an error message such as the following:

```
ISAKMP AAA: Unable to send AAA Accounting Start %CRYPTO-4-IPSEC_AAA_START_FAILURE:
IPSEC Accounting was unable to send start record
```

Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3 or Release 12.3(8)T or a later release and that functions as an EzVPN server.

Workaround: There is no workaround.

- CSCef90002—Resolved in 12.2(18)SXE

  Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

  MPLS packets can only be sent from the local network segment.

  A Cisco Security Advisory for this vulnerability is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-mpls.html

- CSCeg11009—Resolved in 12.2(18)SXE

  Symptoms: Platforms that support IPC may show IPC-2-INVALIDZONE error message:

  Conditions: This condition is not performance impacting

  Workaround: There is no workaround for this issue.

- CSCin82407—Resolved in 12.2(18)SXE

  Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

  Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

  This advisory will be posted to
  http://www.cisco.com/en/US/products/csa/cisco-sa-20050406-xauth.html

- CSCsa54996—Resolved in 12.2(18)SXE

  Symptom: XAUTH may be bypassed if NAT is present between the client and concentrator

  Conditions: Concentrator and client are negotiating a VPN session with XAUTH.

  Workarounds: None.

- CSCsa67611—Resolved in 12.2(18)SXE

  For packets incoming MPLS Tagged and going out as untagged IP (tag to IP case) if output features (like egress ACL, egress WCCP) are applied upon a reload of a switch one may find that the egress features no longer get applied.

  This has been seen with 12.2(17b)SXB6 and 12.2(18d)SXD2.

  Packet impacted Concern : Incoming packet hitting the 6500 with sup720 with one label and exiting the switch on a non mpls int (tag to ip path) on which some output feature are configured (like output acl , output wccp or...)

  Impact : these packet should always be recirculated as there are some output feature. After a reload of the switch recirculation do not happen anymore and as a result all packet bypass the ACL or any output feature.

  Workaround: disable and reapply all output features on the output interface and output feature will start to work again.

- CSCef44225—Resolved in 12.2(18)SXE

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Dont' Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Other Resolved Caveats in Release 12.2(18)SXE

Identifier	Technology	Description
CSCed05135	AAA	12.2S:Enable encryped kerberos telnet cause switches crash
CSCed88768	AAA	console/vty/telnet password fails after upgrade to 12.2(18)S images
CSCeg06605	AAA	Radius Accounting record send with source port zero
CSCeg16606	AAA	Calling-station-ID twice in access-request with dot.1x authenticatio
CSCsa41535	AAA	show aaa servers, response time counter shows incorrect value
CSCsa74002	AAA	Input queue - wedged when traffic punted to the CPU
CSCed25363	Access	PA-MCT3 will not come online after being down with no cable attached
CSCed90084	Access	No SNMP trap Generated for Up/Down(looped) situation on 7500 Router
CSCee49862	Access	PA-MC-2T3+ does not adhere to ANSI T1.231 standard
CSCee70591	Access	PA-2T3+ does not adhere to the ANSI T1.231 standard
CSCee82681	Access	Counter: Counters stuck on serial interface
CSCef73120	Access	Pikespeak:Fw2 with E3 Serial PA:Interface BW does not get modified
CSCef85293	Access	E1 ports of a PA-MC-8TE1+ are up without any cable attached
CSCeg55131	Access	Spurious access @mip_unchain_idb while configuring t1 controller
CSCeg67788	Access	Interface counters incorrect with PA-MC-8ET1+
CSCeh16887	Access	FW2+PA-MC-2T3: RP crash without coredump after channel-group removed

Identifier	Technology	Description
CSCin60835	Access	Show controller serial not showing all 15 min intervals
CSCin76828	Access	Multi-channel T1 PA's in FlexWAN module fail boot-up diagnostics
CSCin79495	Access	FW2-HYB:%CWAN_RP-4-SEMAHOG observed with 256 channels on PA-MC-8TE1+
CSCin79544	Access	Large values of tx_polling_high cause high latency on ct3/ce3 PAs
CSCin88303	Access	Unchannelised mode of PA-MC-2t3+ Not working, Interfaces up/down
CSCsa46643	Access	input/output counters stop incrementing on serial interface counter
CSCdx79081	ATM	ATM vc bundle member adjacencies not getting deleted
CSCdy07583	ATM	scaling: loops in atm_pvc_range_command contribute to line card flap
CSCeb01205	ATM	LSNT:CPUHOG with Switch1 logged after clear interface sw1
CSCeb06797	ATM	error message %ATMPA-3-BADVCD after deleting & re-adding pvc
CSCec31381	ATM	Need message on OSM that UBR+ is unsupported.
CSCec51408	ATM	VBR-NRT Under PVC missing after reload router
CSCec80784	ATM	Memory leak in ATMSIG Input (atmSmap_enter_vcnum_in_map)
CSCed00033	ATM	oam-pvc manage 0 is broken after AIS
CSCed21813	ATM	SAR1 crash when VC QoS parameters are modified
CSCee04747	ATM	memory leak when removing ATM VCs
CSCee42236	ATM	Atm Static mapping not show up in configuration using in PVC bundle
CSCef10826	ATM	CAR broken on IMA with DCEF enabled
CSCef55463	ATM	VBR-NRT shaping not accurate under load
CSCef83201	ATM	ATM OAM F5 segment RDI not transmitted out ATM interface
CSCeg03153	ATM	ifAdminStatus does not follow cli for ATM sub-interface
CSCeg19298	ATM	Router crashes while sh run is issued after atm pvc bundle config
CSCeg83467	ATM	Router crash at atm_arp_process
CSCin31767	ATM	crash on show atm map after deleting subint with static map bundle
CSCin32888	ATM	Crash on removing bundle-member with ipx inarp config
CSCin41371	ATM	dLFIoATM : VIP crash on interface flap
CSCin65182	ATM	OAM PVC on IMA interface doesnt come up after OIR
CSCin77553	ATM	ATM-IMA stops passing traffic after some time, rx_no_buffers seen
CSCin79468	ATM	ATM SSO: PVC state not in sync between active/sdby after a sh/no-sh
CSCin84694	ATM	Workaround fix for PA-A3/A6 SAR hardware issue
CSCin86002	ATM	Quick shut/no-shut on member link reduces bandwidth of IMA-grp intf
CSCin86455	ATM	PA-A3/A6: Performance optimization and code cleanup
CSCea31640	Content	WCCP packet return handling - webpage is partially downloaded & hang
CSCeb28941	Content	IOS NAT and WCCP do not work together
CSCed16561	Content	DFP agent not able to send keepalives or weights to the manager
CSCee02118	Content	Reqs. from CE get sent back to the CE; CE configured with two ifaces
CSCee31118	Content	WCCP Bypass URl doesnt work with CEF/dCEF immediately after reload

Identifier	Technology	Description
CSCeh13292	Content	WCCP Multiple Configurations causes high CPU
CSCin79644	Content	Flowmask do not change when wccp redirection changed from L2 to GRE
CSCuk50878	Content	Spurious memory access in wccp_srvc_grp_find
CSCdk41322	Infrastructure	Cannot do show buff input-interface on virtual-access interface
CSCdx62060	Infrastructure	Interface names made to display full while show int summary done
CSCdy01705	Infrastructure	High cpu at process TTY Background
CSCdy32629	Infrastructure	cpmCPUTotalPhysicalIndex changes w/o OIR or Restart
CSCdz27562	Infrastructure	snmpwalk on loopback interface gets response from physical int. IP.
CSCdz60577	Infrastructure	Spurious memory access and Traceback after changing SNMP engine ID
CSCea20169	Infrastructure	erase nvram: is not prevented when issued with write mem
CSCea36491	Infrastructure	Input Wedged with SNMP traffic
CSCea62212	Infrastructure	ATA_status timeout errors
CSCea69601	Infrastructure	Disk Corruption on C6400 and/or RSP compatible platforms
CSCea87766	Infrastructure	<interface> is a static pool and cannot be tuned message displayed
CSCeb48835	Infrastructure	Bootvar does not update on PRP
CSCeb69892	Infrastructure	SNMP: traceback int timer_start
CSCeb79675	Infrastructure	SNMP reply packets do not use the correct source address
CSCec21583	Infrastructure	%SYS-3-CPUHOG: SNMP ENGINE
CSCec22574	Infrastructure	IPC-5-REGPORTFAIL: after rsh command executed on GSR LC
CSCec39376	Infrastructure	Flash Card is not recognized when its moved from Master to Slave
CSCec47356	Infrastructure	Active and Standby run-config essentially different
CSCec55147	Infrastructure	Memory leak in IFS
CSCec69091	Infrastructure	PCMCIA disk 0 is formatted from a diff router error
CSCed08172	Infrastructure	wr mem introduces 550ms latency in packet forwarding on npe-g1 PE
CSCed15410	Infrastructure	CLI:syscon IP longstring will crash router
CSCed16920	Infrastructure	Constant high CPU in TTY background
CSCed35964	Infrastructure	Interop issue observed reading Viking 48MB flash on 7200 routers
CSCed41231	Infrastructure	Fix alignment handler to use proper jump target register value
CSCed42330	Infrastructure	Unable to boot using IOS image in second flash partition
CSCed45942	Infrastructure	Bus error due to corrupted managed timer structure
CSCed46843	Infrastructure	compiler change breaks PUTLONGLONG macro
CSCed48158	Infrastructure	atomic_increment() leaks memory
CSCed51952	Infrastructure	Hotswapping linecards while configuring i/f can crash the box
CSCed54444	Infrastructure	Malloc failures and tracebacks on LAC when disconnecting L2TP sess
CSCed59079	Infrastructure	Modified FAT sectors written for wrong device
CSCed63357	Infrastructure	show disk#: and dir disk#: inconsistent
CSCed64664	Infrastructure	SYS-2-LINKED: Bad enqueue messages when terminating multilink vpdn

Identifier	Technology	Description
CSCed76117	Infrastructure	Unable to squeeze flash filesystem via snmp ciscoFlashMiscOpCommand
CSCed86286	Infrastructure	Software forced crash at ssh_process_message_events
CSCed88967	Infrastructure	NVRAM not protected from access by local app during write mem
CSCee00868	Infrastructure	ATA Format Flash increases verification/bootup time
CSCee12118	Infrastructure	ifs_remove / ifs_open with TRUNc mode doesnt work at startup
CSCee18018	Infrastructure	%Error opening nvram:/startup-config at reload
CSCee23750	Infrastructure	%Error formatting flash (Invalid DOS media or no media in slot)
CSCee29138	Infrastructure	ciscoMemoryPoolType returns wrong value
CSCee29214	Infrastructure	NRT: %Error formatting disk0: (No such device)
CSCee30986	Infrastructure	warm reboot command takes more than 500ms for nvgen
CSCee42363	Infrastructure	ip ftp username not used after username was previously used in URI
CSCee47120	Infrastructure	writ mem gives a prompt when saving config with 3 rsa keys
CSCee56618	Infrastructure	attach command may crash router
CSCee58083	Infrastructure	CSCed57948 breaks RPC-R fragmentation
CSCee63808	Infrastructure	CLI: router reloads at [show monitor event-trace merged-list ..]
CSCee66206	Infrastructure	Router crash when booting with bootimage 12.1(22.3)E1
CSCee66688	Infrastructure	status read error on Intel series 2+ cards due to CSCec21583
CSCee83183	Infrastructure	test ipc port remove should only remove Test ports
CSCee91044	Infrastructure	SNMP Trap Sent In Error Upon Every IKE Lifetime Expiry
CSCee96231	Infrastructure	CIP and xCPA ucode fail to load after CSCee13801
CSCef01725	Infrastructure	pak_realign driving up CPU usage
CSCef06881	Infrastructure	dir disk0: takes > 12 min. when easybake file system on disk0
CSCef28657	Infrastructure	Router crash at ip_snmp
CSCef49110	Infrastructure	disk operation fails with read_file/dir failed
CSCef63909	Infrastructure	Crashinfo not written to disk in some cases
CSCef68103	Infrastructure	Disk0 operations fails with NPE-G1 IO controller
CSCeg11566	Infrastructure	SNMP May Consume all the I/O Memory
CSCeg16786	Infrastructure	Device not loading with the image and SP crashes
CSCeg19038	Infrastructure	The entCacheFlag should not be shared with several entity tables.
CSCeg23300	Infrastructure	show mem 0x<addr> needs to be an internal command
CSCeg61032	Infrastructure	Memleak or dead memory when internal OS registry call is made
CSCeg64124	Infrastructure	SAA not sending packets to line after a period of time
CSCeh25393	Infrastructure	CSM:C2R2: memory leak if config and delete VLANs repeatly on msfc
CSCin39040	Infrastructure	Router crashes copying running config from/to tftp server
CSCin43799	Infrastructure	VFC option is missing in copy command
CSCin49362	Infrastructure	RSP16:%SERVER_CLOCK_SYNC-3-BADREQ: seen on rpr+ switchover
CSCin53807	Infrastructure	Warm Reboot Decompression may fail for certain images

Identifier	Technology	Description
CSCin55436	Infrastructure	software forced reload at ipc_open_port
CSCin80221	Infrastructure	FSCK crashes when number of sectors per cluster is zero in boot sect
CSCin86483	Infrastructure	RP crash on terminating router banner on same line with empty banner
CSCsa45568	Infrastructure	Changing RTR config causes Sup720 SSO getting out of sync
CSCsa49566	Infrastructure	%FIB-2-IF_NUMBER_ILLEGAL creating Virtual If (lpb,Virt) after CSCuk55348
CSCsa65096	Infrastructure	Router may crash when nv->textptr is dereferenced
CSCsa68352	Infrastructure	v1 view is attached to default community string
CSCuk51673	Infrastructure	malloc_aligned adds unnecessary padding
CSCdy31356	IPServices	as5300 crashes with DHCP stack overflow error
CSCea03340	IPServices	HSRP virtual address responds to traceroute
CSCea25073	IPServices	IOS FTP client code rewrite
CSCea81029	IPServices	show ip igmp int crashed router
CSCeb07106	IPServices	BGP and md5 authentication issues - TCP-6-TOOBIG
CSCec38667	IPServices	Unified configuration storage broken for 16 character hostname
CSCec50485	IPServices	copy ftp flash fails with 3COM ftpserver
CSCed21865	IPServices	TCP watchdog crash in tcp_putstring
CSCed52163	IPServices	Crash or CPUHOG when doing HSRP SNMP query
CSCed82551	IPServices	VRRP: problem with dynamic reconfiguration of secondary IP addresses
CSCed83616	IPServices	Simultaneously configuring and display HSRP crashes IOS
CSCef35459	IPServices	HSRP - Bogus Error message while adding Virtual IP address
CSCef46191	IPServices	Unable to telnet
CSCef66899	IPServices	Bridge-group causes OSPF neigh to go INIT/DROTHER
CSCef67721	IPServices	Prefix in binding but released in local pool
CSCeg82109	IPServices	VRRP stays in Init status after cable unplug/replug
CSCin78000	IPServices	LDP session in xmit state if MPLS flapped at high traffic on L2 SUP3
CSCin82758	IPServices	Disabled STP on an interface becomes enabled on reload
CSCsa52643	IPServices	The command ip dhcp limited-broadcast-address breaks DHCP forwarding
CSCee02270	LAN	show list cause router reload
CSCee82479	LAN	Tracebacks on cwan_poseidon_dot1q_encap and dot1q_encap_vlan_table
CSCef79968	LAN	snmpget shows No Such Instance for 4GE-SFP-LC sub-interface
CSCeg21175	LAN	ipv6 traffic not going on directly connected serial i/f of RSP
CSCsa52236	LAN	Spurious memory access at dec21140_fastsend after PA OIR
CSCdy43326	LegacyProtocols	Bus Error at address 0xD0D0D11
CSCed14392	LegacyProtocols	DLSW configuration breaks OSPF and HSRP
CSCed88563	LegacyProtocols	No Decnet routing causes buss error
CSCee88936	LegacyProtocols	Removing DECnet Routing causes %ALIGN-3-SPURIOUS error message
CSCef06820	LegacyProtocols	Remote-MAC of 1st TEST F is not converted with dlsw timer explorer-.

Identifier	Technology	Description
CSCea22886	Management	Memory leak in SNMP PING
CSCeb52330	Management	NVGEN-one-command o/p for interface commands is different than sh ru
CSCec25430	Management	IOS may reload from specific packet
CSCed57925	Management	CNS Events not getting generated for ATM PVC provisioning
CSCee58479	Management	Neighbor on PA-MC-8TE1 interface sometimes crashes - CDP traceback
CSCef88326	Management	cns config retrieve fails to pull a config
CSCeg71686	Management	Router crash with reset PWAN2 card - QoS Portchannel config.
CSCeg73883	Management	cikePeerLocalAddr is not augmenting properly
CSCdu28706	MPLS	ARP rejects requests from interfaces in different vrfs
CSCdv91301	MPLS	can not create vrf static route to global connected interface
CSCdx83597	MPLS	TDP running; needs TDP Identifier; no tag-enabled ints -- config OK
CSCdz33630	MPLS	Stanby RP crashes when SSO switchover in the HA MPLS co-existence
CSCdz85325	MPLS	TFIB not get updated after delete and re-add static route
CSCea41043	MPLS	LSR MIB: Would like to remove memory address XC indexing issue
CSCeb19802	MPLS	MPLS MIB Capability statements need to be updated
CSCeb40653	MPLS	Bus error crash at vrf_interface_print when deleting vrf config
CSCeb52414	MPLS	Notify Path Errors fatal to MPLS-TE LSP
CSCeb87433	MPLS	Follow-up on CSCdz75507
CSCec03017	MPLS	Need bundling enabled on VRF Checkpointing
CSCec10116	MPLS	MPLS VPN PE uses global addresses on some packets originated in VRF
CSCec45051	MPLS	VPN MIB: PerfRoutesAdded and PerfRoutesDeleted incorrect
CSCec86102	MPLS	Inconsistent tag info between RSP and VIP
CSCed03539	MPLS	IGP prefixes in the FRR database showing up as vpn prefixes
CSCed21063	MPLS	TE Tunnel Destination Label Missing
CSCed22837	MPLS	Bus error ALIGN-1-FATAL:Corrupted program counter
CSCed25539	MPLS	VRF maximum routes cmd causes pkt loss, drop
CSCed28093	MPLS	Enabling send-label under IPv6 causes LDP updates to BGP-IPv4
CSCed39059	MPLS	LFIB is inconsistent when P-AIS injected on APS interface
CSCed45746	MPLS	duplicate tag between 2 VRFs
CSCed52578	MPLS	vrf route thru recursive tagged loadshared global route bogus label
CSCed54416	MPLS	GRP crash in tfib when pos fiber is disconnected or connected
CSCed55962	MPLS	Connected subnet not in TFIB
CSCed57281	MPLS	CPU hog in CEF reloader while adding a vrf interface
CSCed68723	MPLS	MPLS VPN CEF entry does not have tag information
CSCed81317	MPLS	can not see bgp routes from CE after import map
CSCee00239	MPLS	F/R bridge-group and tag ip cannot coexist despite other subintf
CSCee07279	MPLS	TFIB NULLADJ errmsg triggered, fix root cause of null tagout_adj

Identifier	Technology	Description
CSCee12408	MPLS	%REDUNDACY-3-CONFIG_SYNC: Active and Standby lbl when config ldp nei
CSCee26700	MPLS	memory leak caused by LSR MIB queries
CSCee37430	MPLS	Missing LFIB tag rewrite on LC after loss of /32 entry to its next-hop
CSCee56225	MPLS	Alignment errors in tfib_request_all_tags
CSCee59585	MPLS	Duplicate label in sh ip cef on LC
CSCee62326	MPLS	TFIB-7-SCANSABORTED: TFIB Scan not completing error
CSCee67207	MPLS	Recursive route not labeled on E4/E4P if send-label configured
CSCee78118	MPLS	E3 4oc12: Linecard crashes at alpha_update_deaggregate_vrf
CSCee84732	MPLS	CPU 99 % with Tagcon Addr process taking up 80% to 90%
CSCee93228	MPLS	Process watchdog in ip_trace_show_extended
CSCef14446	MPLS	mpls vpn: recirculation vlan for agg label is not mapped to vpn
CSCef18515	MPLS	FRR:RP and LC not consistent after clear cef line.
CSCef22069	MPLS	Glean adjacency not completing arp for VRF interfaces
CSCef25866	MPLS	Blackholing of traffic during FRR reconnect with invalid cache adj
CSCef51239	MPLS	NRT:after remove ldp tcp block and toggle mpls ip, ping not worked
CSCef58522	MPLS	TFIB-7-SCANSABORTED: TFIB scan not completing. Unresolved adjacency
CSCef59275	MPLS	Traffic drop forever in FRR active state because of wrong FRR label
CSCef59507	MPLS	Dead LDP session still shows up after new session established
CSCef80349	MPLS	GSR midpoint rejects RESV after link flap
CSCef85231	MPLS	Standby will reload due to mpls ldp target command out of sync
CSCef89647	MPLS	memd alignment error and bus error @ rsp_drop_iptag_pkt
CSCef97536	MPLS	LDP label not populate in forwarding table after clear ip route
CSCeg03885	MPLS	TE label missed on MPLS TE tunnel
CSCeg12649	MPLS	A follow up to CSCef22069
CSCeg27836	MPLS	suspect vrf leak following foreign ebgp flap
CSCeg90033	MPLS	Missing labels in MPLS/VPN forwarding table
CSCeh23047	MPLS	TAG2IP traffic does not recover after SSO switchover ingress E3/E4+
CSCin35896	MPLS	Explicit withdraw of a Label causes IPv4 BGP to not update the LFIB
CSCsa53117	MPLS	MLS cef hardware Freeze
CSCsa77411	MPLS	RP crash at rrr_lm_unlock_bandwidth
CSCec03024	Multicast	NATing Payload of (S,G) Join in SSM Environment
CSCec19125	Multicast	Payload field have been changed after NAT
CSCec23559	Multicast	show ip msdp peer x.x.x.x advertised-SAs may cause reload
CSCec37022	Multicast	Join delay timer issue when receiving successive Prunes
CSCec58348	Multicast	SDP/SAP: need to implement support for payload-type in SAP
CSCec80252	Multicast	PIM:(S,G) join on RPF interface does not trigger a RPF check
CSCed12688	Multicast	PIM SSM Prune Latency Under Certain Topology

Identifier	Technology	Description
CSCed45452	Multicast	PIM-DM state-refresh not working after reload
CSCed50220	Multicast	Const2:C2MCAST SP and RP mfib tables are not in sync.
CSCed85752	Multicast	router generating tracebacks when using qos/ipsec/multicast
CSCee02125	Multicast	syslog messages needed for pim neighbor loss
CSCee03081	Multicast	PIMv6: Source address for the register tunnel should be configurable
CSCee19831	Multicast	MLD EXCLUDE for SSM not ignored completely when explict-tracking
CSCee24899	Multicast	router crashed at mwheel_twheel_start
CSCee65066	Multicast	ciscoPimInvalidJoinPrune trap contains wrong VARBIND
CSCee66936	Multicast	Router reload, traceback at dvmrp_mbgp_walk
CSCee84457	Multicast	Uptime for VRF multicast routes dont go beyond 7w- sh ip mroute vrf
CSCee89438	Multicast	MSDP doesnt build S,G state after rxing *,G join
CSCee93574	Multicast	Unable to delete RP when groups are overlapped with another RP
CSCef36986	Multicast	no mls ip multicast non-rpf cef added to sup2/msfc2 by default
CSCef53297	Multicast	ip pim accept-register list does not deny ICMP registers
CSCef60452	Multicast	possible blackout when receiving Join on RPF interface (iif)
CSCef89240	Multicast	Crash in sh ipv6 pim topo command in pim_show_add_mroute
CSCeg28814	Multicast	Duplicated mcast packet due to wrong FPOE in egress replication mode
CSCeg39601	Multicast	IPV6 encap tunnel is always down
CSCeh15639	Multicast	crash due to freed nbr while sending PIM hello
CSCeh47667	Multicast	A ddts to commit CSCef60452 to pikespeak
CSCsa45490	Multicast	Spurious memory access at pim_receive_autorp_packet
CSCuk49673	Multicast	MRIB: No multicast forwarding after no ipv6 multicast; ipv6 multicas
CSCeb64018	platform-75xx	traceback at tagsw_forward_inline
CSCec24167	platform-75xx	Bus Error Crash while reading PCMCIA Flash: pcmcia_read()
CSCed33110	platform-75xx	VIP crash induces RSP to hold memory leading to a crash
CSCee35740	platform-75xx	FIB DISABLE after a VIP crash
CSCee65997	platform-75xx	Flapping GE on GSR P router causes PE POS int to flap
CSCec22452	platform-76xx	QOS/RT/DB: LC crashed with TxSOP Errors
CSCec46892	platform-76xx	OSM-ATM:Mcast pkts are dropped over 1483 bridged PVCs
CSCec59550	platform-76xx	OSM-POS crash @ sky4302_enter_drop_mode
CSCec62800	platform-76xx	20E:CWAN-QOS:Increased PQ latency when increasing default queue traf
CSCec74760	platform-76xx	7600 w/BRE configured replies to ARP even with Interface down/down
CSCed07253	platform-76xx	512 Meg SODIMM chip not recognized and shows 256 instead
CSCed19898	platform-76xx	:ATMoMPLS VCs freeze/vanallen error/w toggling core loopback
CSCed51835	platform-76xx	OSM/POS/BB1: OC12 IP 64 bytes performance may degrade
CSCed78077	platform-76xx	LRDI is not reported after reload on OSM-2OC12-ATM-SI PRDI is seen
CSCee14301	platform-76xx	OSM GE Autonegotiation interoperability issues with Ciena K2

Identifier	Technology	Description
CSCee45508	platform-76xx	OSM CHOC-OC12 freezes up while proccessing PPP keepalives
CSCee55056	platform-76xx	OSM interface byte counts are inaccurate
CSCef08790	platform-76xx	PWAN-1:Hidden vlans overlap .1q vlans on same PWAN sub-intf
CSCef12193	platform-76xx	FABRIC-SP-6-TIMEOUT_ERR: Fabric in slot 8 reported timeout error
CSCef12304	platform-76xx	PWAN2:Connectivity is broken between GE-WAN if one end shut/no shut
CSCef19811	platform-76xx	MPLS:VPN:MLPPP:PE not receiving packets from connected CE
CSCef35398	platform-76xx	OSM-2OC12-ATM-SI+ - SRIC IPM parity error
CSCef45881	platform-76xx	aps force from protect to working does not notify routing of change
CSCef74227	platform-76xx	LAN GE of OSM incorrectly increments giants on dot1q trunk port
CSCef76828	platform-76xx	connectivity broken after config/unconfig tunnel interfaces
CSCef82720	platform-76xx	add dot1Q subinterface in ifTable for GE-WAN card
CSCeg05604	platform-76xx	OSM-1CHOC12/T3-SI Detects False AIS when a Remote NM-1T3/E3 is Shut
CSCeg10236	platform-76xx	PWAN2:GBIC type shown as not connected in show int
CSCeg55750	platform-76xx	PP: L2 port on OSM-GE-WAN drop to err-disable when UPE is rebooted
CSCeg77503	platform-76xx	SAA Packets do not hit the outbound service policer
CSCeh11457	platform-76xx	NRT:during mpls testing, ge-wan interface not ocming up
CSCeh23737	platform-76xx	While using L2PT on ATM OSM BPDUs are not filtered
CSCsa47099	platform-76xx	IPX broke on wan link of OSM-2OC12-ATM
CSCsa53708	platform-76xx	OSM crashes under stress when having to pad packets
CSCeb07656	PPP	dMLP:Not receiving packets from multilink int until shut/no shut
CSCeb36360	PPP	Spurious access at ppp_notify_cb_configured
CSCed67708	PPP	IfStackTable is not updated when MLPPP interface is created
CSCee44086	PPP	Multilink PPP cant forward traffic after RP switch-over
CSCee69493	PPP	dMLP fails if control is given to IOS MLPPP
CSCee72906	PPP	dLFIoLL mlp-qos:VIP crash when bundle is reset while traffic is ON
CSCee94294	PPP	Spurious memory access with dLFI interface
CSCef15095	PPP	7500:dLFIoATM: VIP might crash under missed DLFI down events
CSCef44786	PPP	ATMPA-3-BADVCD seen when running MLPPP at low speed
CSCef94525	PPP	Linecard crashes when fib disabled with more than 37 MLP bundles
CSCeg57219	PPP	Unable to ping packets greater than 1022 across MLPPP after sup SW
CSCeg80996	PPP	Second PPP SSO switchover causes pings to fail
CSCeh20758	PPP	MLP interface stays shutdown post SSO switchover
CSCdw01772	QoS	Router may reload if distributed NBAR is configured
CSCeb63310	QoS	Bus Error increment_wred_matched_stats
CSCec23982	QoS	Packet fragmentation causes high CPU at interrupt level with NBAR
CSCec25534	QoS	Memory limit for NBAR wrong when over 214.8MB of free memory
CSCec26626	QoS	RSVP: crash in rsvp_db_msgid_compare() when memory is exhausted.

Identifier	Technology	Description
CSCec27278	QoS	Memory leak in hqf_rp_mlp_blt_setup
CSCec27338	QoS	NBAR should gracefully handle traffic streams with dropped fragments
CSCec46485	QoS	match dscp and match prec matches do not take effect.
CSCed12831	QoS	MQC: should block the non-supported acl with log
CSCed37615	QoS	Watchdog timeout after renaming policy-map.
CSCed46785	QoS	LC crashed at packet classify
CSCed51640	QoS	dWFQ isnt diplayed in sh run anymore, so is lost after reload
CSCed54236	QoS	Router reloads due to memory leak
CSCed54330	QoS	WFQ on virtual-template causes allocation error and tracebacks
CSCed55794	QoS	MSC-200-QOS: RP crashed @ipfib_apply_input_police after move police
CSCed60987	QoS	dCEF path broken when configuring output service-policy
CSCed62637	QoS	CWPA: priority traffic latency varies with default traffic load
CSCed65075	QoS	VIP4-80 crash at hqflayer_config
CSCed67734	QoS	MQC: set atm-clp causes packets to be dropped at receiving end
CSCed70198	QoS	malloc failure and Line protocol down when frame relay frag configur
CSCed76109	QoS	after pvc flap, some pvcs stay down with ATM interface up/up
CSCed79634	QoS	police percent conversions are incorrect in 2nd and 3rd lvl policies
CSCed88854	QoS	VIP crash with bus error in hqf_blt_delete_from_driver
CSCed89629	QoS	Applying service-policy crashes VIP4-80
CSCee05729	QoS	dCEF gets disable after QoS config
CSCee12235	QoS	Bus error when reapplying renamed policy-map to ATM PVC
CSCee18883	QoS	output stuck on interface causes cbus-complex and IPC timeout
CSCee22810	QoS	Router stops sending LMI with QOS configured
CSCee24349	QoS	Crash at fib_post_download_processing when reloading
CSCee31618	QoS	C2SUP2/FW2/CT3+:Voice packet drops at low rates with cRTP+LLQ conf
CSCee36050	QoS	VIP crash when re-use channel group with set service policy
CSCee38324	QoS	VIP crash at hqf_svip_ifc_dtq_consumer when traffic go through
CSCee47275	QoS	card resets due to [no] fair-queue cleanup loops
CSCee66909	QoS	ct3 spa: qos configs should be blocked on multilink member links
CSCef02160	QoS	long router boot time due to processing in stile_in_policymap
CSCef06034	QoS	Sup720 crashes after SSO Failover with nbar configured
CSCef25953	QoS	dwred statistics are not updated in show policy-map int output
CSCef46134	QoS	CPUHOG at CEF MQC IPC Background on SIP-600 on remove/apply qos
CSCef47829	QoS	Physical int out of BW: no error message that MQC policy cant apply
CSCef66517	QoS	packet drop on flexwan when traffic shaping
CSCef70739	QoS	MAXMEMORYUSED Error with 4 GB active links
CSCef91275	QoS	RSVP: policy does not retry outbound request after failure

Identifier	Technology	Description
CSCeg25493	QoS	VIP Bus error crash in get_same_id_actiongroup
CSCeg31912	QoS	QoS does not see correct interface bandwidth on dMLFR interfaces
CSCeg33229	QoS	VIP crash when service policy removed from MFR int with traffic
CSCeh13583	QoS	MQC: ipv6 acls changes not notified to the platform clients
CSCin52060	QoS	After the policy got rejected hqf was not cleaned on vip
CSCin61140	QoS	mfr: LC crahses with LFI/mqc enabled
CSCin70454	QoS	dLFIoAT : RSP is stuck at LCP timeout
CSCin72437	QoS	MQC: Concurrent access crashes the Flexwan during switchover
CSCin86096	QoS	Classification matching on IPv6 acl fails
CSCsa53001	QoS	vip crashes in hqf_svip_ifc_dtq_consumer after serial-subint flap
CSCuk49453	QoS	Traceback when configuring nbar
CSCdk23784	Routing	EIGRP next-hop is not used
CSCdt38401	Routing	Frame-relay packets processed by cpu due to CEF inconsistency
CSCdt51547	Routing	Packet drop with ip verify unicast reverse-path.
CSCdu59038	Routing	- show ip eigrp neighbor - may crash router
CSCdv12472	Routing	BGP does not remove confed-AS-path on eBGP links
CSCdv76375	Routing	OSPF neighbor command unsupported in VPN routing instance
CSCdv84363	Routing	Routes not installed across MPLS TE tunnels after clearing OSPF
CSCdv90022	Routing	Interface not recieve traffic after shut/no shut
CSCdw51691	Routing	ISIS MPLS TE adj pointer mem leak, may cause mem fragmentation
CSCdw78242	Routing	PE-CE: Backdoor link always preferred over VPN
CSCdy23644	Routing	ghost config in router after line card swap
CSCdy60008	Routing	NRT:rsp router crashed at ipigrp2_route_adjust+0x5c
CSCdy77097	Routing	RIP Jumbo fix for VPN and Performance
CSCdz38670	Routing	CEF adjacency for arp with alias keyword is lost after reload
CSCdz50424	Routing	Handling of ICMP Type 15 responses
CSCdz54344	Routing	static route adjustement trigger delay
CSCdz69672	Routing	unable to redistirbute secondary connected routes
CSCdz81659	Routing	CEF doesnt delete adjacency of Virtual IP on HSRP transition
CSCea01837	Routing	%SYS-2-NULLCHUNK in ip_apply_input_mac_acc
CSCea09852	Routing	%FIB-3-FIBBADXDRSLOT: Invalid XDR slot. Type/len/slot 30/77/7
CSCea15115	Routing	hybrid-cli doesnt work for v6-afs
CSCea19918	Routing	BGP: need to do multipath with different as-paths
CSCea31201	Routing	Crash in ip_fast_accumulate_acctg
CSCea33138	Routing	Packets dropped while building mGRE spoke-spoke link
CSCea47597	Routing	RIP Routes Stuck In Routing Table
CSCea49910	Routing	as-override breaks eBGP with multiple CE peers in the same VRF

Identifier	Technology	Description
CSCea56883	Routing	Router hangs due to bus error at network_check
CSCea58973	Routing	BGP NSF: Some VPNv4 BGP routes get purged after RP switchover
CSCea59206	Routing	Distribute-list command does not stay under address-family ipv4
CSCea64161	Routing	E3 ch/oc12: IS-IS Update CPUHOG for 840 ppp isis intfs
CSCea66299	Routing	%BGP-3-NEGCOUNTER messages appear during route flapping
CSCea76840	Routing	PER-USER cosmetic bug in SHOW IP PROTOCOL
CSCea78615	Routing	SFC at mgd_timer_first_running related to NHRP
CSCea80821	Routing	Eigrp topo not updated after redist if floating static present
CSCea83086	Routing	NHRP and VRFs do not interact well
CSCea85395	Routing	BGP supressed prefixes not reinstated after condition removed
CSCea92690	Routing	registration packet gets lost when tunnel protection comes up
CSCea92893	Routing	unknown gateway info. for sh ip proto vrf
CSCeb07288	Routing	Crash in NHRP managed timers
CSCeb08101	Routing	EIGRP: high bandwidth metrics are not nvgened properly
CSCeb27742	Routing	invalid input detected at exit-address-family after boot
CSCeb43353	Routing	Default-information originate in BGP shouldnt be tied to peer group
CSCeb53542	Routing	Inconsistency between CEF adjacency and ARP tables; unicast pkt loss
CSCeb54519	Routing	NHRP should retransmit registration requests
CSCeb57086	Routing	After issuing bgp upgrade-cli redundancy sync fails
CSCeb65685	Routing	ip cef load-sharing algorithm tunnel command lost upon reset of rpm-
CSCeb66602	Routing	peer-group nlri multicast command adds unicast in upgrade to25S1
CSCeb69972	Routing	Set Community None broken
CSCeb74105	Routing	Counters on the rules that are reflected are not updated
CSCeb75489	Routing	Named ACL does not allow duplicate remark statements
CSCeb77653	Routing	second vty freezes while editing prefix list
CSCeb84144	Routing	BGP aggregate route not cleared after removing from the config
CSCeb86068	Routing	passive-interface support needed for router ospf vrf
CSCec00165	Routing	RIP updates lost under heavy load
CSCec04708	Routing	OSPFv3: default-info originate not working properly with route-map
CSCec05264	Routing	BGP: Peer-group configuration is deleted, when last peer is removed
CSCec07566	Routing	Packets for interface with named ACL are not dcef switched
CSCec07592	Routing	NRT: With bgp deterministic med config, best path not chosen correct
CSCec07636	Routing	snmpwalk on ospfnbrrtrld does not display all switch1 interfaces
CSCec07941	Routing	%FIB-3-FIBDISABLE msg after booting while ip routing is disabled
CSCec08795	Routing	Memory leak in CEF process during deferred delete
CSCec16245	Routing	BGP set metric-type internal doesnt work with set metric +/- cmd
CSCec20352	Routing	BGP table version changes for locally sourced vpnv4 routes

Identifier	Technology	Description
CSCec21709	Routing	ping of 10.0.0.0/8 in the CEF path does not work
CSCec22723	Routing	Router may reload unexpectedly due to ISPF(OSPF)
CSCec23167	Routing	Interface input queue backs up during BGP scalability test
CSCec25744	Routing	reload when connecting spoke to spoke
CSCec27454	Routing	Watchdog reload at nhrp_cache_count_nbma_subr
CSCec30677	Routing	IOS device pauses indefinitely when reload command is issued
CSCec32738	Routing	IPCP: Install route to <IP address> is missing.
CSCec39973	Routing	RP crash at isis_add_is_neighbors_to_lsp
CSCec40535	Routing	BGP: a single slow peer impacts convergence of other peers
CSCec42871	Routing	clear adj and/or generate error mesg. when md5 auth. not matching
CSCec44271	Routing	MBGP: Route Reflector not advertise nlri multicast
CSCec47079	Routing	EIGRP variance should install equal cost route
CSCec48142	Routing	Unable to globally disable proxy ARP
CSCec48833	Routing	NRT:Load sharing verification failed
CSCec55608	Routing	BGP redistribution in IGP based on std communities/as-path not work
CSCec61594	Routing	Route-maps with continue fails to match a community list
CSCec67985	Routing	Clear ip bgp external vrf <name> cause all VRFs to flap
CSCec70664	Routing	BGP stays in READ_ONLY mode longer after CSCeb54512
CSCec73316	Routing	Load-balancing ratio over TE tunnels not the same as configured
CSCec79860	Routing	EIGRP unequal balancing breaks with MLPPP reducing bandwidth
CSCec82398	Routing	BGP needs to modify a route instead of delete/add
CSCec85207	Routing	DMZlink-BW for neighbor on ATM subinterface is set to 0
CSCec85804	Routing	router crashed at rip_onoff_idb under low mem test
CSCec90041	Routing	BGP: update generation deadlocked when outbound policy changed
CSCed02844	Routing	Adjs out of p2p interface fail to repopulate
CSCed15990	Routing	tag forwarding entry not deleted when BGP dampening is configured
CSCed17879	Routing	adtvertise ipv4 routes across ipv6 BGP peers not working
CSCed25969	Routing	NHRP shouldnt delete static cache entry upon route removal
CSCed26048	Routing	IP Background Process very high when OSPF or EIGRP catch-all present
CSCed28920	Routing	Dynamic NHRP cache entry deleted due to BGP peer change
CSCed36386	Routing	APS:Ping fail on alternate packets after revertive switching
CSCed41641	Routing	reload when removing tunnel interface with nhrp
CSCed43597	Routing	Add PRC for eigrp interface and nsf related commands
CSCed46066	Routing	%ALIGN-1-FATAL: Corrupted program counter after vpn-gre unconfig
CSCed46438	Routing	default-information originate not working for ISISv6
CSCed53358	Routing	Pings fail on ethernet to VLAN interworking over L2TPv3, irdp fails
CSCed59370	Routing	OSPF Type 5 LSA not updated when forwarding address changes

Identifier	Technology	Description
CSCed60289	Routing	delay in route update on interface down cause scalability issue
CSCed60800	Routing	Routing Table not updated when BGP next hop is withdrawn
CSCed61503	Routing	in dmvpn hub-spoke nhrp does not show spoke pre-nat private ip
CSCed62479	Routing	next-hop-unchanged does not work w confed ebgp
CSCed63342	Routing	RIP-Unicast updates not sent to configured RIP neighbors
CSCed63876	Routing	BGP: router crashes pointing to ed_decay_penalty
CSCed66144	Routing	EIGRP: next-hop self routes incorrectly deleted from RIB
CSCed72283	Routing	eigrp variance not considered under address-family
CSCed74812	Routing	A few packets loss when vpnv4-bgp switchback on RR redundancy
CSCed77612	Routing	network option missing in isis interface command
CSCed82706	Routing	tracebacks in ipigrp2_add_item when NAT configured
CSCed83891	Routing	BGP prefixes current field counter wrong in sh ip bgp neigh comman
CSCed86069	Routing	Software forced crash- crashdump is_chunk_bad checkchunk-
CSCed93630	Routing	router crashed at bgp4_format_mp_attr
CSCed94589	Routing	alignment error in ipigrp2_passive_interface_command upon reload
CSCed96206	Routing	Crash after <no neighbor> command
CSCee01550	Routing	Per-user access-lists disappear after first show ip access-lists
CSCee01628	Routing	conditiona debug ip packet display all ip packets
CSCee05779	Routing	CLNS partition avoidance not working
CSCee16068	Routing	Equal cost default route remains in RT after changing interface cost
CSCee19691	Routing	RP crashed on rip_process_mgd_timers on clear ip route *
CSCee19880	Routing	EIGRP routes stuck in routing table when using no ip-next-hop-self
CSCee21928	Routing	OSPF not installing multiple next hops to single neighbor
CSCee23517	Routing	Inconsistent Fib tables between RP and LCs
CSCee26387	Routing	Removal of static routes from the routing table may take 60 seconds
CSCee27357	Routing	bus error when configuring advertise-map with the set command
CSCee28466	Routing	set metric + or - does not correctly adjust MED metric for BGP
CSCee30718	Routing	BGP max community limit should be removed
CSCee39853	Routing	CEF getting disable on Standby PRE
CSCee40207	Routing	Memory leak in BGP Open Process After SSO RP Switchover
CSCee41172	Routing	BGP: maximum-path import purges wrong paths
CSCee42285	Routing	constant route flap with eigrp SOO if route not injected from eigrp
CSCee43166	Routing	BGP: reduce CPU load for processing inbound VPNv4 updates
CSCee50846	Routing	BGP: converge an update-group independently from other update-groups
CSCee52822	Routing	Process-switched RPFv6 doesnt check if CEFv6 is enabled
CSCee54672	Routing	ISIS does not function properly, creating loop, route flapping.
CSCee56976	Routing	rip non direct neighbor is broken

Identifier	Technology	Description
CSCee59315	Routing	MPLS-VPN:Corrupted BGP table showing stale and/or poisoned paths
CSCee63163	Routing	BGP IPv6 recursive lookup problems
CSCee70840	Routing	DMVPN: daisy-chained HUBs loose sockects between themselves
CSCee75996	Routing	SSO:IPv6:Spurious memory access at ipv6fib_find_fib
CSCee76562	Routing	Spurious Access traceback @ipigrp2_add_item_dest
CSCee83098	Routing	BGP deletes the static VPN route with global keyword in extranet
CSCee85202	Routing	Long delay for vrf to be removed from vrf table when un-configured
CSCee85488	Routing	Net LSA is not originated on PE-CE link
CSCee85676	Routing	BGP does not import updated prefixes into VPNv4 table
CSCee86530	Routing	MP-BGP fails to report martian next-hop when nh is all 1s or martian
CSCee88898	Routing	ALIGN-3-SPURIOUS in show_ipprotocol
CSCef00037	Routing	SSO:T/B DUAL-3-INTERNAL IP-EIGRP(0) internal error after S/W
CSCef00296	Routing	router crash at bgp_upd_candidate
CSCef00535	Routing	RP crash on validblock when neighbor did SSO switchover
CSCef08044	Routing	no clns route-cache broke vaccess subinterface
CSCef08797	Routing	static routes not advertised to BGP peers
CSCef10480	Routing	%IPC-5-INVALID: Dest Port 1020007 Invalid Port Index=0x0
CSCef11737	Routing	OSPF passive-interface default bleeds to OSPF VRF interfaces
CSCef16804	Routing	On switchover cef entries learned through uplink port dont purged
CSCef19137	Routing	arp table not flushing entries on idb flap and missing adjs
CSCef24703	Routing	default-information originate with route-map not working correctly
CSCef26976	Routing	Removing one vrf messes up ospf config of other vrf
CSCef29091	Routing	Redistributed RIPv2 Subnets Matching Major Net Not Sent
CSCef30437	Routing	dynamic arp entries not cleared on interface link down
CSCef39466	Routing	Redistributed RIPv2 Route Matching Major Net Not Sent
CSCef45830	Routing	Staled BGP route remains in table in bgp multipath testing.
CSCef50427	Routing	System crashed when show ip bgp XX.
CSCef57803	Routing	Missing iBGP refresh after fixing a duplicate address
CSCef65500	Routing	ospf_db_timer_tick cpuhog process OSPF
CSCef77174	Routing	NHRP fails on mGRE tunnel if network-id a multiple of 256
CSCef77648	Routing	Excessive replication of locally generated multicast on mGRE
CSCef81489	Routing	MPLS/VPN Inter-AS: Withdraw not sent on ASBR
CSCef89529	Routing	BGP neighbor advertisement-interval does not work
CSCef93215	Routing	router crash at ospf_build_one_paced_update
CSCef95026	Routing	Bus Error due to OSPF accessing freed LSDB entry
CSCef95474	Routing	static arp cannot be removed and other issues
CSCef95821	Routing	static with global next-hop marked as best in BGP but not in vrf RIB

Identifier	Technology	Description
CSCef96650	Routing	IS-IS passive-interface not work
CSCef97268	Routing	NHRP: Wrong NBMA address for spoke-spoke when hub behind NAT
CSCef97340	Routing	ipv6 mcast:mrib client not seen on sp/dfc on reload
CSCef97738	Routing	BGP/MVPN: incorrect update-source is passed from BGP to MVPN
CSCeg00610	Routing	PP: RP crash at isis_ispf_clean_one_list
CSCeg05830	Routing	BGP: Update peer-group remove-private-as functionality
CSCeg07725	Routing	EIGRP redistributing BGP inconsistently after BGP topology changes
CSCeg08344	Routing	with cef/dcef enabled & compression on, tcp frames getting dropped
CSCeg09032	Routing	ospf routes not updated when link cost changes and ispf enabled
CSCeg13958	Routing	peers missing from ibgp vpnv4 peer-group
CSCeg16620	Routing	PE-CE: Need deterministic path selection for equal cost routes on PE
CSCeg19442	Routing	crash on pdb_ospf_hello_BLOCK
CSCeg20212	Routing	ISIS process restarts upon receiving LSP with max sequence number
CSCeg21842	Routing	EIGRP BFD: crashes in igrp2_peer_destroy with lots of link flaps
CSCeg26378	Routing	Dest CEF entry is missing in DCEF table. All pkts are punted to RP.
CSCeg30291	Routing	BGP fails to send update/withdraw to some peers
CSCeg31951	Routing	BGP: Put peers with as-override & rem-pvt-as in separate updgrps
CSCeg35811	Routing	no ip routing cause the master sw to crash
CSCeg41363	Routing	OSPF SHAM-LINK ON PARRALLEL PATH DOESNT WORK
CSCeg41727	Routing	BGP wrongly sets next-hop for redistributed static routes
CSCeg49796	Routing	BGP peer wont stay shutdown
CSCeg52889	Routing	Rockies2: MPLS TE Tunnel dont come up after adding loopback int
CSCeg62496	Routing	Type-3 lsa not generated if Type-1 flaps coming from multiple areas
CSCeg70726	Routing	PP:mVPN:RP crashes on configuring mdt default @iprib_idb2tableid
CSCeg72989	Routing	IPv6 static neighbor broken
CSCeg74205	Routing	OSPF LSA Type 3 causes SPF execution every minute
CSCeg74772	Routing	Tunnel idbs not reused on the LC when clear cef linecard is issued
CSCeh00680	Routing	router may reload when isis mt is configured
CSCeh04837	Routing	Arp entries purged on SSO
CSCeh05567	Routing	Sham-Link cost changes cause wrong next-hop recalculation
CSCeh07510	Routing	Rockies2: OSPF Trace found after no router ospf command
CSCeh07809	Routing	BGP leaves a stale CEF entry
CSCeh11984	Routing	Missing prefix update when the recursive route is deleted.
CSCeh12233	Routing	12.2SX: fibtype2fibmsg crash - backout CSCef30577
CSCeh14015	Routing	Routes are not redistributed properly
CSCeh27783	Routing	IPv6: 500 manual tunnel script cause IOS crash
CSCeh28320	Routing	IPHC does not commuicate with RP after HA switchover

Identifier	Technology	Description
CSCin33082	Routing	problem with changing distance for static routes
CSCin73487	Routing	BGP Conditional advertisement broken
CSCin84644	Routing	Routes are not seen on neighbors after switchover on eigrp stub rtr
CSCin87277	Routing	FEonCWPA2:%SYS-3-CPUHOG due to process = OSPF for scaled subints
CSCsa39998	Routing	NHRP shouldn't trigger CEF to refresh an NHRP Registration Entry
CSCsa40588	Routing	Routes are not withdrawn from routing table after BGP routes are removed
CSCsa43135	Routing	NHRP: Incomplete mapping entry stays in table too long
CSCsa44181	Routing	ospf virtual-link (DC) flaps during md5 key rollover
CSCsa51951	Routing	Virtual-Link stuck in extstart/exchange
CSCsa53911	Routing	OSPF type3 LSA filtering for 0.0.0.0/0 not effect immediately
CSCsa55048	Routing	Static exported in vrf has wrong cef entry
CSCsa59600	Routing	IPSec PMTUD not working [after CSCef44225]
CSCsa60015	Routing	OSPF: <no ip ospf> issued in interface mode removes global ospf config
CSCuk41411	Routing	HA: show cef linecard doesnt display RRP as expected
CSCuk45392	Routing	BGP ipv6 neighbor cannot inherit peer-policy template
CSCuk45501	Routing	BGPv6: Route-reflector cannot change nexthop for iBGP prefixes
CSCuk46249	Routing	IPv6 CEF: debug ipv6 cef ... not recognised
CSCuk48925	Routing	Adjacency update with invalid fibidb messages detected on VIP
CSCuk49384	Routing	Suppress t/bs for null fibidb->idb on newly active RP on SSO s/o
CSCuk49694	Routing	6PE: Ignoring label update from peer
CSCuk50159	Routing	DCEF not running on VIP if reconfigured after switchover
CSCuk52062	Routing	RIB link failure after memory exhaustion
CSCuk52253	Routing	IPv6 static route missing tag argument
CSCuk53957	Routing	IPv6 routes via intf stay in RIB even intf has been removed by OIR
CSCdu83050	Security	ssh needs source-address
CSCdy25784	Security	CEF switching mGRE tunnel drops packets every NHRP holdtime
CSCdz64323	Security	Software forced crash in CRL code
CSCea16871	Security	Need to improve GRE tunnel int. selection for incoming GRE pkts.
CSCea59073	Security	Downloading CRL by SCEP GetCRL fails and sometimes crashes router
CSCeb25416	Security	Router crash at C_DeleteObject(0xb905d8)+0x34 on 804 & 805
CSCeb64967	Security	IKE SA fail to come up with Solaris Unity Client using cert
CSCeb83287	Security	crypto key zeroize crashes router with http secure-server
CSCec01500	Security	CDP not supported over GRE tunnel
CSCec22308	Security	mem allocated at PKI_ParseX500Dn(0x6207eb2c)+0x34 was leaked
CSCec22391	Security	ca_req deadlock after CRL expires
CSCec31053	Security	sh cry ca cert xx causes %ALIGN-1-FATAL: Illegal access to a low add
CSCec32184	Security	RSA-SIG IKE leaks memory

Identifier	Technology	Description
CSCec32192	Security	Trustpoint source interface command rejected only on reload.
CSCec35857	Security	PKI: crash when authenticating a sub CA after auth the root
CSCec76781	Security	12.3.3 %SYS-3-CPUHOG in Crypto PKI RECV
CSCec88399	Security	CS: Enrollment request without extension fails
CSCed35711	Security	IKE fails when receiving CERT_REQ without CA issuer name
CSCed54769	Security	sh cry ca timers can crash the router
CSCed56270	Security	Box reloads on HTTPS File Get
CSCed60664	Security	import DOS-formatted text file might fail
CSCed81049	Security	PKI: not able to delete trustpoint after doing IKE
CSCed83180	Security	PKI: query mode feature is not working
CSCed91119	Security	multiple certs in SCEP CertResp might crash router
CSCed93963	Security	Enrolling with invalid subject name CA might crash router
CSCee04732	Security	Re-enroll using terminal does not replace the existing router cert.
CSCee27987	Security	CDP on Tunnel interface reports duplicate in neighbor table
CSCee39637	Security	Gre & shaping can get large output rate above physical interface
CSCee72828	Security	Router running IOS-SSHv2 doing SCP hangs
CSCef26840	Security	Router hangs after reapplying nhrp config on the tunnel interface
CSCef67660	Security	sshv2 malform client ignore msg cause demage to router
CSCef98116	Security	cat6500 12.2SX: SSH issues with privilege levels
CSCeg00663	Security	ip mtu config change not reflected in IPSec data path
CSCeg15922	Security	DMVPN:crypto socket is not open until shut/noshut tunnel interface.
CSCin70986	Security	UUT crashes when due to memory corruption when EzSDD is Configured
CSCsa42726	Security	DMVPN: Crypto socket not deleted when p-pGRE tunnel in up/down state
CSCsa59906	Security	VPNSM: Malloc failure in IPSEC key engine and router crashed
CSCuk54386	Security	Delete/create of GRE tunnel causes fixup to be disabled.
CSCdv68743	Unknown	Inefficient code in qos/qoscli_match_packet.c:match_named_acl().
CSCdy33703	Unknown	Need span support for port 1/4 & 1/3
CSCdz66609	Unknown	cat6k & ons155xx interop issues with Y-cable APS
CSCdz83100	Unknown	Multicast pkts should not be policy routed in CEF
CSCea16744	Unknown	GBIC optical 7500 router crash on attach queueing output policy
CSCea28043	Unknown	Nvgen_one_command o/p has an extra ip prefix
CSCea31672	Unknown	ping wont go through due to encapsulation failed on 7500+vip router
CSCea51450	Unknown	Incorrect number of CPUs in CISCO-PROCESS-MIB cmpCPUTotalTable
CSCeb53380	Unknown	benchmarked call setup rate ~75% of fullsail cco image (4/28)
CSCeb56814	Unknown	SUP1A connectivity problem :CAM learn 15/2 in ieee/dec and mls rp ip
CSCeb64745	Unknown	Missing RIP update when executing show run command
CSCeb65576	Unknown	Router crash in cls, used with llc2, dlsw ect.

Identifier	Technology	Description
CSCeb65671	Unknown	Wrong local vc label is programmed for data plane
CSCeb79911	Unknown	AToM: Incorrect Runt checking causes valid packets to be dropped
CSCec00930	Unknown	bus error at crypto_ipsec_clear_peer_sas
CSCec30836	Unknown	Image Verification: %SIGNATURE-4-NOT_PRESENT
CSCec34010	Unknown	OSM2-GE 64 bit main interface counters stay 0
CSCec47779	Unknown	Remove inapplicable RESETNXI errmsg and change to debug info
CSCec65024	Unknown	Multicast VPN not supported in -vz- images
CSCec72813	Unknown	Traceback at ipaccess_match_duplicate (CPUHOG)
CSCec89704	Unknown	Multicast not forwared in fast path with tunnel sequence-datagrams
CSCed07367	Unknown	Proton: show int serial input/output counters are 0
CSCed08725	Unknown	sonetMediumInvalidIntervals GET-NEXT returns errStat too big
CSCed12659	Unknown	LSNT:LSC crash,bad address for refcount
CSCed12722	Unknown	SVI bridge-group adversely impacts EIGRP when PIM config removed
CSCed33793	Unknown	Mcast uflow policer does not work on LAN for > certain rates
CSCed35960	Unknown	TETONS2: Ch/OC12DS0 crash when unconf/reconf MFR access uninit mem
CSCed45971	Unknown	Unexpected Exception crash when EzVPN server fails connect to RADIUS
CSCed50556	Unknown	memory leak in Crypto IKMP
CSCed66843	Unknown	dNBAR on 7500 with redundant RP causes ipc seat manager crash
CSCed72285	Unknown	IOS and CatOS have different tresholds to errdisable a port
CSCed82736	Unknown	SYS-2-GETBUF: Bad getbuffer, bytes= 65535
CSCed83129	Unknown	VIP crashed at vip_ip_fib_flow_fs when mdt receive info expires.
CSCed92374	Unknown	T/B seen on defaulting config on a range of ports
CSCed93264	Unknown	RP truncates the TOS byte to upper 3 bits on IP with option field
CSCed94829	Unknown	IOS reloads due to malformed IKE messages
CSCed95701	Unknown	HSRP incorrectly tracks 2 instances of the same interface
CSCee04176	Unknown	Mac-address-limiting inconsistent between LAN & VPLS
CSCee05413	Unknown	Memory leak in EARL VLAN stats subblock
CSCee09692	Unknown	Sup720: IPX traffic rate limited based on mls rate limiters
CSCee09820	Unknown	show mls cef exact-route displays wrong info on Sup2/MSFC2
CSCee10005	Unknown	Cat6500 service module connectivity issue with crossmodule etherchan
CSCee15581	Unknown	sss_mgr with invalid index into 2 arrays causes crash/traceback
CSCee15798	Unknown	CEF entries not installed on LC/SP after SSO switchover
CSCee20888	Unknown	ipv6 over isdn/serial and atm interfaces broken: could not ping
CSCee21730	Unknown	Array declaration on stack causes stack overflow
CSCee22045	Unknown	MSC-200-QOS: Traceback @vip_fr_update_idb_info when add/remove class
CSCee23087	Unknown	Router may reload when configured for Server Load Balancing (SLB)
CSCee27203	Unknown	IDBs getting mixed up on channelized interfaces on a PA-MC-8TE1+

Identifier	Technology	Description
CSCee32365	Unknown	MFR: LMI exchanges fail over MFR interfaces
CSCee33923	Unknown	IOS/SLB conn debugging causes dropped connections.
CSCee34121	Unknown	17aSX1: No crashinfo file for RP, SP crash @ make_ios_dnld_instance
CSCee37771	Unknown	67xx: Rommon Upgrade Failure
CSCee41186	Unknown	router crashed at ip_policy_forward
CSCee42657	Unknown	sup720 crashing after reload with large configuration
CSCee43191	Unknown	SLB TCAM entries not programmed properly after SSO
CSCee47766	Unknown	c2rls3 ATM PVC configuration lost after a switchover
CSCee49035	Unknown	mVPN: MTI uses a non-PIM interface as a Tunnel source address
CSCee49194	Unknown	MPLS echo replies need to be sent with echo req udp source port
CSCee54446	Unknown	PP: cant ping after FR PVC removed and reconfigured
CSCee55233	Unknown	Large L3 port-channel config with stats collection caused high CPU
CSCee55297	Unknown	EM: Failed to create event for applet 1: error from operarting sys
CSCee56009	Unknown	SP crashes in fibtype2fibmsg
CSCee56269	Unknown	Add support for the lowerLayerDown value for ifOperStatus
CSCee57336	Unknown	IPC-5-INVALID traceback on mlppp config in multicast
CSCee58127	Unknown	PBR become S/W when Security-ACL set up in same I/F
CSCee65993	Unknown	Command maxconns x sticky-override not saved in config
CSCee66778	Unknown	PBR: set next-hop conflict with IGP advertised /32 host route in CEF
CSCee67261	Unknown	Memory leak on crypto_ikmp_peer_create
CSCee68057	Unknown	MPLS TE Tunnel counters are not working with MPLS VPN CSC BGP+label
CSCee70024	Unknown	LSPV: Misinterpretation of the Vendor Enterprise Code TLV
CSCee70075	Unknown	after reset of module with DFC, PBR gets SW switched
CSCee70293	Unknown	FWLB: Intermittent creation of conns on a firewallfarm.
CSCee71793	Unknown	More stringent len check reqd during LSP ping/trace echo pkt decode
CSCee73959	Unknown	Need HW support for set interface null0 for Earl6 with a new CLI
CSCee75620	Unknown	RP crashes after enable CBAC
CSCee76272	Unknown	MPLS iBGP load balancing problem
CSCee77136	Unknown	sup720: SPAN dest port should not be shown as notconnected
CSCee78323	Unknown	Duplicate packets in ingress SPAN/RSPAN with 6516A or 6548-GE-TX
CSCee78451	Unknown	Native:Policing rate is not accurate with small packets
CSCee79753	Unknown	GLBP:Preempt behavior is different between each state change
CSCee85152	Unknown	CEF Hardware switching produces ping failure on every other packet a
CSCee86168	Unknown	active SP resets, sr7100 errata 11
CSCee89227	Unknown	%C6K_PLATFORM-SP-4-BADFLASH: Unsupported flash type in the bootflash
CSCee89232	Unknown	Configuring platform while in automore state crashes switch
CSCee89326	Unknown	SNMP cardType for Flexwan2 returns value for Flexwan1

Identifier	Technology	Description
CSCee91509	Unknown	Standby IP address unusable after deleting interface VLAN
CSCee92191	Unknown	PBR works in sofware if vlan id changes during linecard reloads
CSCee92719	Unknown	Duplicates in NDE on the Sup720
CSCee93286	Unknown	ipMRouteInterfaceOutMcastOctets not incrementing correctly
CSCee93511	Unknown	Chassis crash in crypto_ikmp_peer_struct_unlock with Gre/Ipsec
CSCee93931	Unknown	EEM(IOS): application ED doesnt work as expected
CSCee95301	Unknown	Unhide and document mls rate-limit multicast non-rpf command
CSCee95359	Unknown	disable aggressive aging timer for non-RPF
CSCee95708	Unknown	MSFC2-3-TOOBIG on sup720 in MPLS/VPN environment
CSCef00575	Unknown	enable cache parity for sup720
CSCef00888	Unknown	Cat6k: Need MIB support for CPU and memory info per DFC
CSCef01043	Unknown	T/B DFC3-5-INVALID: Sequence Structure Dest Port
CSCef02439	Unknown	FW2 reloads with Module failed SCP download
CSCef03290	Unknown	sh run does not display properly VLANs allowed in MWAM port
CSCef03723	Unknown	HA Coexistence:MPLS:VPN:VRFs not in sync between primary and standby
CSCef05282	Unknown	Removing IP address, IP route cache cef still allows pkts to switch.
CSCef05643	Unknown	SLB-MIB slbStickyObjectTableEntry view through SNMP not working
CSCef07848	Unknown	VRF over GRE traffic is s/w switched after remove/add mls mpl tu-rec
CSCef07965	Unknown	System crashed when accessing CVDM from the switch
CSCef08097	Unknown	IP RIB Update can hog memory after bgp flap leading to fib disable
CSCef08728	Unknown	slave default-slot config gives HA-3-SYNC_ERROR and reloads stby
CSCef09594	Unknown	CWPA2: High number of spurious interrupts increasing
CSCef09622	Unknown	CWPA2: Spurious access with show mpls cwlc-vpn adjacency
CSCef10192	Unknown	SSO: Standby failed with mismatch config on reading FW slot cache
CSCef13797	Unknown	TCAM Capacity Exceeded with ACL on POS Interface
CSCef14106	Unknown	IDSM2 stops detecting attack after 2nd failover
CSCef14780	Unknown	WCCP switch to software mode after applying redirect acl globally
CSCef14934	Unknown	link up/down message is abnormal
CSCef19894	Unknown	Tests on standby fab. cause min. error on fab-enable cards on swover
CSCef20654	Unknown	SP crashes due to Supervisor online diag failure-loading 0608 image
CSCef21575	Unknown	Sup720 - ACL Incorrectly Denies Packets in HW
CSCef23302	Unknown	Native vlan programmed wrong on pinnacle - register 0x0134
CSCef23498	Unknown	storm control config becomes invisible when channel-group configured
CSCef25427	Unknown	Improve the handling of EarlRecoveryPatchReset
CSCef25429	Unknown	NetflowTCAM test failed on Chevyslite err code 0x1,passed Chevys
CSCef25710	Unknown	EOS error handling changes
CSCef26512	Unknown	WS-X6582-2PA :Unable to read cwan<slot>/0-disk0:

Identifier	Technology	Description
CSCef26926	Unknown	VSEC:VPN-SM:router crashed in get_ipsec_attributes
CSCef27359	Unknown	SW and HW cef adjacency inconsistency
CSCef29929	Unknown	Exceed pkt count in CLI, but not count in SNMP police stats table
CSCef30308	Unknown	all zero source and dest mac address in show mls adj entry det
CSCef30392	Unknown	VPLS/PWAN2: SC CRC errors and VA length mismatch errors with traffic
CSCef32513	Unknown	SPAN destination ports causing latency on adjacent Pinnacle ports
CSCef33051	Unknown	Part of the traffic blackholed when new link joins etherchannel
CSCef33064	Unknown	PIM process took 64M of IO memory on SP, crash.
CSCef33311	Unknown	Flowcontrol inconsistency on Cat6000/Cat6500 native
CSCef34328	Unknown	Crash after the qos policy configuration
CSCef35707	Unknown	L2 Forwarding Table ECC error handler not working properly
CSCef35774	Unknown	Random DOM gbic missing in the show int tranc output
CSCef36367	Unknown	MMLS: High CPU after Sparse->Bidir transition
CSCef37026	Unknown	Running configuration is not synching between DR and NDR on MSFC3
CSCef39977	Unknown	Mac-addr static and no mac-addr static CLI allows diff portchann #s
CSCef40249	Unknown	power inline command appears even after removed and reloaded system
CSCef41934	Unknown	LSPV: LSP Ping packets processed in non-MPLS interfaces
CSCef42133	Unknown	HC counters stack in OSM POS
CSCef42312	Unknown	Ambiguous command: snmp-server enable traps config
CSCef43000	Unknown	Rockies1A SNMP:Traceback/Corrupt vlan db when set vlan 1002..1005 na
CSCef45495	Unknown	PIM Snooping: (s,g,r) prune handling cases
CSCef46652	Unknown	VPN-SM: IPSec SA encrypt counters incorrect
CSCef46923	Unknown	Group of 4 ports on WS-X6516-xx modules may stop forwarding traffic
CSCef47414	Unknown	VTP code fail to restore vlan database properly
CSCef47466	Unknown	High latency and packet drop when any interface goes down on OSM
CSCef47639	Unknown	no redirect-vserver REDIR1 crashes SUP
CSCef48810	Unknown	MAC Address entries learned via DFC3A not forwarded to SUP720
CSCef49330	Unknown	APS not working on the PA-MC-STM1
CSCef49811	Unknown	Router crashes while freeing memory in ace_hapi_pkt_proc
CSCef51783	Unknown	VPN Services Module does not report invalid SPI to MSFC
CSCef52858	Unknown	Any newly configured tunnels, makes the existing tunnels go down
CSCef53290	Unknown	Using config mls ip ids causes switch to reload unexpectedly
CSCef53846	Unknown	MVPN + MDS broken, all packets get punted.
CSCef55147	Unknown	DOM: global dom cli is broken, show int trans, returns null.
CSCef55352	Unknown	FIBDISABLE and IPC timeout after APS swithover on CHOC-12 OSM
CSCef56578	Unknown	VPNSM: traffic counter broken for GRE interface terminated on VPNSM
CSCef57019	Unknown	Some fabric svc-modules shouldnt force ingress mcast replication

Identifier	Technology	Description
CSCef57061	Unknown	PBR packets punted to RP after reloading the switch
CSCef58323	Unknown	%EARLY-L2_ASIC-DFC-SRCH_ENG_FAIL T/B on Berytos with L2(10k mac)Traf
CSCef58590	Unknown	Disable VTT major temp shutdown and change thresh 100/85 -> 115/100
CSCef62158	Unknown	V4/V6 qos display shows de-installed qos, while qos tcam is prgmd
CSCef62539	Unknown	PP:Router crash after powering linecard with mismatch wattage on PS
CSCef62936	Unknown	Spurious memory access at show_dss_command
CSCef63549	Unknown	Multicast MET management fix and increase OIF above 1023 per flow
CSCef64755	Unknown	Port Security: packet get lost when aging timer expires
CSCef65827	Unknown	GRE o/v IPSec with VPNSM intermittently loses connectivity
CSCef66632	Unknown	Demand Aging clearing entries every 4 seconds, without contention
CSCef67810	Unknown	get-bulk for portGrp causes cpu spike and delayed response
CSCef68801	Unknown	IPP rewritten to zero for rp originated packets
CSCef70083	Unknown	Spurious memory access made at ipfib_policy_forward
CSCef70298	Unknown	IFindex missing IDBs after deleting and adding T1 channels
CSCef70677	Unknown	CSG Module switches to CSM when trying to change ruleset
CSCef71913	Unknown	MVPN: 3 minutes duplication in Data-MDT (by SSM) redundancy
CSCef72013	Unknown	unicast flooding due to purging of some mac-addres entry with dfc3/pfc3
CSCef72117	Unknown	show crypto session detail enc/dec counters are reversed
CSCef72205	Unknown	vlan stops forwarding
CSCef72233	Unknown	no nat server cmd not taken into config with 12.2(18)SXD
CSCef72939	Unknown	SSO swover canot decode data desc. L1NULL0 msg when new stdby is up
CSCef73076	Unknown	ALIGN-SP-3-CORRECT seen in mcast_igmp_handle_igmp_pak
CSCef73256	Unknown	isolated pvlan not associated with VRF - packet-loss experienced
CSCef74373	Unknown	SW forced crash on cat6k
CSCef75411	Unknown	Traffic over TP tunnels stops after forced SSO switchover
CSCef75501	Unknown	dot1x authentication not work perfectly in sup720.
CSCef76161	Unknown	ifInDiscards are resetting,causing counter problems
CSCef77822	Unknown	VRF: Crypto maps not downloaded, ACE PL struck...
CSCef78235	Unknown	Disable egress span of vacl redirected packets
CSCef78240	Unknown	SIBYTE correctable ECC error should not logged at emergency level
CSCef78798	Unknown	OSM-CHOC-DS0:After rtr reload,2 interface line protocol down
CSCef79815	Unknown	OSM-CHOC-DS0:PSE incrementing on all STS.
CSCef80423	Unknown	Sup3: watchdog fired incorrectly when reload/incorrect bootup cause
CSCef81281	Unknown	The value of cbQosPoliceConformedByte64 provided by SNMP decrease
CSCef82367	Unknown	IP traff not frwded on G+CR2 port if toggled between routed/switched
CSCef82884	Unknown	Failed to delete billing plan errors
CSCef83162	Unknown	portEntPhysicalIndex not instantiated for WS-X6316-GE-TX

Identifier	Technology	Description
CSCef84129	Unknown	L2 entries not purged correctly during OIR with DFCs in the system
CSCef84162	Unknown	Should handle power glitches gracefully
CSCef85101	Unknown	VSEC:VPN-SM:HA and B2B replay update out of sync
CSCef85222	Unknown	policy based routing packet loss sup720 with reflexive access-list
CSCef86799	Unknown	ifType for ppp bcp on POS is wrong to propvirtual
CSCef86980	Unknown	CAT6500/7600 OSM egress policymap rejected without error message
CSCef88685	Unknown	mcast ltl cleared out on WS-X6816-GBIC after NSF/SSO failover
CSCef89139	Unknown	Adjacency pointers not Updated when 2nd Link Removed on 7600
CSCef92360	Unknown	Policy allowing 15 char. names, but not supported
CSCef93371	Unknown	bpduguard broken when access and voice vlan enabled
CSCef93632	Unknown	software force reload when slb swith mode
CSCef93909	Unknown	T/B c6k_proCMIB-SP-IPC_PORTOPEN_FAIL after SSO switchover
CSCef94120	Unknown	%MSFC2-3-IDB_INCORRECT_UNTHROTTLE_VECTOR
CSCeg00085	Unknown	DMVPN:multicast routing packets fail to be Txed on mGRE of 6k
CSCeg00687	Unknown	warning message needed for ip unreachables leaking to RP
CSCeg00698	Unknown	EOS-2-EOS_INT system error message is undocumented
CSCeg01297	Unknown	System crash caused by pkt of incorrect length/IP header checksum
CSCeg01510	Unknown	Device crashes when we configure no vlan <vlan nu>
CSCeg01543	Unknown	MLFR VIP crash in vip_fr_decode_encapsulation
CSCeg02873	Unknown	Netflow v9 config crashes router
CSCeg02893	Unknown	multicast traffic not being software switched with static NAT
CSCeg03423	Unknown	show int trans does not show ITU channel info for DWDM Xenpaks
CSCeg04004	Unknown	Netflow Data Export (NDE) from the SP disabled after reload
CSCeg05819	Unknown	CPP does not get applied in Hardware after reloading the router
CSCeg06292	Unknown	CPP: Traceback on attaching a service-policy to control-plane
CSCeg06570	Unknown	PA-MC-STM1: %CBUS-3-CCBCMDFAIL1: Controller 2, cmd (62 0x0000000E)
CSCeg06698	Unknown	COS rewritten for routed multicast traffic
CSCeg07617	Unknown	PP:Spurious Acesss when sh/no sh mlfr intf
CSCeg08389	Unknown	Interface counters do not increment on a Virtual MFR interface
CSCeg08562	Unknown	%IPC-3-NOBUFF: The main IPC message header cache is empty
CSCeg09655	Unknown	VPN-SM: Error in GRE check
CSCeg10174	Unknown	High CPU in QoS Mgr when changing long QoS access-list
CSCeg11883	Unknown	After RPR+ switchover standby keeps on crashing continuously
CSCeg13661	Unknown	MLS consistency-checker doesnt fix an inconsistency for (*,g)
CSCeg15192	Unknown	Increase period of statistics collection to lessen CPU load
CSCeg17132	Unknown	Sup720 inconsistency between MCAST GCE and MSC GCE datebase
CSCeg19103	Unknown	ALIGN-3-TRACEX : Error with debug netdr turned on

Identifier	Technology	Description
CSCeg19269	Unknown	gt 12L4 Oper in acl dest port doesnt expand corectly;pkts non-qos fw
CSCeg20856	Unknown	CONST-FIB: send_batched_packet() : cant allocate pak
CSCeg21028	Unknown	PFINIT-SP-1-CONFIG_SYNC_FAIL when primary attempts to sync to Sec.
CSCeg21548	Unknown	7200 crashes after link flap with 100 BFD/EIGRP sessions
CSCeg21620	Unknown	Inconsistencies in handling CSM configurations
CSCeg22198	Unknown	VSEC:VPN-SM:DF bit set will break Blade to Blade failover
CSCeg24287	Unknown	LDP does not recover after link failure between two NPEs in a networ
CSCeg26382	Unknown	wireless client not able to browse the Internet due to MSS issue
CSCeg26993	Unknown	Cat6000/Cat6500 dot1Q sub-int return incorrect SNMP statistics.
CSCeg29357	Unknown	Supw standby crashes after TestSPRPInbandPing failure
CSCeg29451	Unknown	standby and DFC in standby slot resets when doing write mem
CSCeg30437	Unknown	VPLS:ATOM:CWAN: Some VCs remain down, LFIB/TTFIB are ok
CSCeg32986	Unknown	CAT6500: Last output timestamp in show int for a SVI is never
CSCeg37929	Unknown	Unable to configure framed-ip sticky on conventional vservers
CSCeg38482	Unknown	MVPN one PE can not receive auto-RP information for one vrf
CSCeg38970	Unknown	sup720 in 7600 crashes on sh mpls l2transport hw-cap interface
CSCeg39091	Unknown	Abnormally long flooding with L2 DFC DEC
CSCeg40177	Unknown	Tag to Ip path has all zero src and dest mac
CSCeg40543	Unknown	some vcs do not pass traffic after supervisor switchover
CSCeg40801	Unknown	Configuring/Unconfiguring channel-group on SPA-T1E1 causes mem leak
CSCeg41623	Unknown	CSM:Only configured vlans should be allowed on trunk
CSCeg41762	Unknown	VPN-SM: MSFC3 sup720 crash managing the Crypto-ACE IPsec stats cache
CSCeg43854	Unknown	Taking Accounting no inservice also takes other Accounting no inserv
CSCeg45759	Unknown	Switch does not response to CDP packet with trigger TLV set
CSCeg48068	Unknown	After gige sub-int was deleted, no counters in show main interface
CSCeg48196	Unknown	Buffer overflow vulnerability in oakley_final_qm
CSCeg48512	Unknown	Out-Discard and Rcv-Octet counters increment on notconnect ports
CSCeg48547	Unknown	fm_netflow_earl6.c: early return results in memory leak
CSCeg51793	Unknown	MVPN: Address Error Exception after config change w/ Mvpn
CSCeg52076	Unknown	MVPN: crash in ip_show_mroute -> mem_lock while deleting VRFs
CSCeg52280	Unknown	CRCs caused by WS-X6704-10GE
CSCeg53985	Unknown	Cat6500 does not populate smonCapabilities correctly.
CSCeg55387	Unknown	EEM regression test composite cleanup
CSCeg55565	Unknown	MMLS/MVPN: crash at mls_earl_show_scmdb -> chunk_lock
CSCeg55846	Unknown	MSFC3 HYB: msfc3 hybrid IOS does not implement some EMT calls
CSCeg56052	Unknown	Active and Standby SP crash due to GC Entry memoryleak
CSCeg60530	Unknown	IOS crash on removing secondary vlan (pvlan configuration)

Identifier	Technology	Description
CSCeg65640	Unknown	Cat6000 with UDP turbo flood results in corrupted outgoing packets
CSCeg66729	Unknown	Memory corruption crash when setting TapStreamIpEntry (v3 cTAPMib)
CSCeg67986	Unknown	PA-POS-2OC3 interface 1 remains up/up with SLOS
CSCeg70376	Unknown	Sup720 : Ingress VSPAN is not working for VoIP VLAN
CSCeg71209	Unknown	Traceroute mpls or ping mpls cause %SCHED-3-THRASHING using SSH
CSCeg72385	Unknown	Power supply failure syslogs should have higher severity as in CatOS
CSCeg73678	Unknown	PR+:bandwidth is not guaranteed for dscp traffic
CSCeg74312	Unknown	getbulk on ciscoSlbExtMIB causes Spurious mem access and Traceback
CSCeg74597	Unknown	Further restrict power limit of CISCO7609/WS-C6509-NEB-A to 4536W
CSCeg77040	Unknown	Session Counts not decremented when processing IC
CSCeg77264	Unknown	CSM:C2R2: Resetting CSM cause system crash
CSCeg80506	Unknown	Need flowcontrol receive off support for 6704-10GE module
CSCeg82615	Unknown	Pinnacle SRAM SEL Recovery
CSCeg90349	Unknown	Both ends of the link are in loop-inc and will not recover
CSCeh05310	Unknown	ATM OSM MPB: One PVC failed to TX PKT if the LC in slot/port 1/7 of 7613
CSCeh08451	Unknown	Excessive Overruns and lbusDrops due heavy flow control over fabric
CSCeh11253	Unknown	dir /recursive all-filesystems causes supervisor to crash
CSCeh13200	Unknown	Active RP crash @ rf_proxy_fatal_error+0x60 when stby reloads
CSCeh17417	Unknown	IOS SLB not injecting VIP route when backup sfarm takes over
CSCeh43531	Unknown	CAT6K: router reloaded under stress
CSCeh50877	Unknown	Ondemand test for 144-bit fails sometimes
CSCeh51395	Unknown	Trunk vlan wont revert to the original when reconfigured
CSCin41024	Unknown	c2sup2:CWPA:DMLFR:FR Relay entry (sh fr map) is taking lot of time
CSCin65698	Unknown	%INTERFACE_API-3-NODESTROYSUBBLOCK msg on reconfiguring Potent PA
CSCin71744	Unknown	CCB_PLAYBACK and Insuff resources to create channel grp on 8TE1+
CSCin72469	Unknown	Pkts are not trusted for nbar type class though configured in HW
CSCin73206	Unknown	Ping fails on Ch-STM1 interface
CSCin74811	Unknown	user startup config rejected at bootup with > 1 acl match in Vacl
CSCin76284	Unknown	strict RPF works like strict RPF with allow default
CSCin76433	Unknown	Traceback at slb_backup_uname_fill_update
CSCin76456	Unknown	BRE Config/Unconfig IP on VLAN intf stops ARP response w/ fake MAC
CSCin76635	Unknown	SP crashes due to Supervisor online diag failure-loading 0608 image
CSCin76766	Unknown	Active SP reloads at ipc_send_rpc_blocked failed after RPR+ swover
CSCin77310	Unknown	Delete pending Src only GCE entry not deleted after SSO S/w over
CSCin77443	Unknown	HYB:HA:Slave crashes on configuring Virtual-Template interface
CSCin78110	Unknown	Some E1 controller does not come up if a large config on other LC
CSCin78137	Unknown	Traceback and %SCHED-SP-3-THRASHING on port-security

Identifier	Technology	Description
CSCin78242	Unknown	VLAN flooding when SPAN configured.
CSCin78773	Unknown	UFP not working after SSO with 6816 and uplink ports.
CSCin79691	Unknown	Hqf info. on LC disappears after LC reload/int sh-noshut
CSCin82741	Unknown	PBR does not work if both PBR & SLB are applied on same interface
CSCin82941	Unknown	Policer not programmed if module is powered on after switchover
CSCin83211	Unknown	TFTP gets terminated and RP goes to boot mode if CNTL-C given
CSCin83972	Unknown	Dot1x Scalability issue - Port from Tetons-2
CSCin84703	Unknown	Standby does not come up if active is 12.1E based software
CSCin84712	Unknown	Incorrect VMR entries programmed in TCAM for ICMP/IGMP fragments.
CSCin85077	Unknown	Inline power error-disabled interfaces do not recover at enough powe
CSCin87976	Unknown	Need to rate-limit EOS Error interrupts
CSCsa27033	Unknown	Half duplex displayed on 1000 Mbps ports
CSCsa39767	Unknown	mls ip multicast connected entries not set for secondary net after reset
CSCsa40934	Unknown	Strict priority queue drops are not accounted in output drops in sh int
CSCsa40962	Unknown	Memory leak in Crypto IKMP process on IOS EzVPN server .
CSCsa43724	Unknown	OSM-CHOC12: When changing E3 to E1, E1s stay down
CSCsa44926	Unknown	ifInNUcastPkts and ifOutNUcastPkts are missing for Vlan Interfaces
CSCsa44933	Unknown	CRONOS: MLPPP-QoS - LC crash during pxf stats update
CSCsa45335	Unknown	ESM causes memory leak in IP Input and ESM Logger
CSCsa45786	Unknown	VPN-SM: rp crash triggered by aaa_req_set_context
CSCsa46887	Unknown	LSPV: Invalid Echo Reply with Pad TLV in some scenarios
CSCsa47020	Unknown	Sup720/FlexWAN: FRF.16 drops 64 byte packets above 2Mb
CSCsa47573	Unknown	Memory leak in medium buffers
CSCsa49267	Unknown	mplsvrfIfUp trap refers to hidden instance of the ifTable
CSCsa49748	Unknown	sup720 reloads by software forced crash
CSCsa50132	Unknown	Both crypto and l3 mobility reg_add to MGRE tunnel_source_idb_change
CSCsa50515	Unknown	TTL=1 unicast may be dropped when mix TTL failure rate-limit and CoPP
CSCsa51770	Unknown	Configuration of RSPAN on 12.2(18)SXD3 causes high CPU
CSCsa53954	Unknown	Fix SB_RMON_OVRFL errmsg in sys/src-sibyte/sysctlr/msg_sb.c
CSCsa54711	Unknown	MVPN: Data MDT Encap incorrect after disable/enable ip mcast-routi CLI
CSCsa56770	Unknown	Crash during boot with: No memory available for capi_rp
CSCsa58470	Unknown	show epld slot command causes silent reload
CSCsa59260	Unknown	C7600 EoMPLS PE correctly does NOT send the COS value of BPDU
CSCsa62845	Unknown	Traffic leaks between PVLANs and Mac learning when VLAN is shutdown,
CSCsa63184	Unknown	Crash TestSPRPInbandPing fail after MLS global enable with Dist. Etherch
CSCsa65200	Unknown	Transmit power is output from admindown IF after system restart
CSCsa67836	Unknown	ct3 spa: all sequenced traffic dropped after mlp lfi bundle flap

Identifier	Technology	Description
CSCsa74464	Unknown	Bus error after config synch of CSM
CSCsa76031	Unknown	6748-GE-TX: Transmit fails on port hardcoded to 10/100/1000 or auto mode
CSCsa76137	Unknown	Komoto+Fornax:FWSM lost connectivity after sso switchover
CSCsa76290	Unknown	Inter-fabric throughput in MPLS CE to PE is much lower than 18SXD.
CSCdy64412	WAN	CE1-HYB: %CWAN_RP-4-SEMAHOG
CSCdz38539	WAN	Crash when configuring ntp
CSCdz67208	WAN	CWPA: Pkts generated on this router are not getting matched
CSCea30197	WAN	Frame Relay Autosensing with lmi-n391dte less than 3 not working
CSCea70822	WAN	SONET statistics are not saved in interval table
CSCec08821	WAN	:CWPA:FR:Output counters not updated in sh fr pvc
CSCec27867	WAN	PA-POS: Interface remains down/down when enabled with critical alarm
CSCec47371	WAN	%ALIGN-3-CORRECT:Alignment correction
CSCec69756	WAN	Not able to configure MTU under Virtual-Template.
CSCec70790	WAN	Bus error at mfr_input_control_paks
CSCed06290	WAN	Invalid host route in CEF table after changing frame-relay ip addr
CSCed52817	WAN	A removed frame-relay cmd from the config, reappear after switchover
CSCed95585	WAN	Frame relay map-class add/remove issues on subinterface
CSCee40223	WAN	ifStackTable goes into a loop if MFR subinterfaces are configured
CSCee53018	WAN	crash or alignment error in show frame lmi after delete MFR interfac
CSCee68930	WAN	MLFR bundle bounces when a local loop is is put on one T1 (2xT1 WIC)
CSCee84611	WAN	NTP Broadcast Client Fails to Sync
CSCef68547	WAN	MFR E0 6*CT3 & 2*ChOC3 bundles not recovering link removal/reconf
CSCef77523	WAN	Random MFR links stay down after reconfig or reload
CSCef82683	WAN	MFR inconsistent bundle when remove link lost
CSCef91994	WAN	FLEXWAN - PA-A3 - packet drop when ping 1500bytes with MPLS
CSCeg06304	WAN	CWPA:DRACO_SCP unsupported feature-id in SET_PORT_FEATURE msg 0x24
CSCeh34067	WAN	FlexWAN+PAs: SUP3 RP crash at mfr_set_output_seq() under stress
CSCin54713	WAN	CWAN SSO:CT3 Mailbox hogging CCB Block semaphore on bootup
CSCin73381	WAN	RBE Support on Flexwan/Flexwan2
CSCin79140	WAN	Router crahes at fr_subidb_class_add
CSCuk50643	WAN	Router reloads on setting ntp server association via snmp

Caveats in Release 12.2(18)SXD and Rebuilds

Open Caveats in Release 12.2(18)SXD7b

Identifier	Technology	Description
CSCin77553	ATM	ATM-IMA stops passing traffic after some time, rx_no_buffers seen
CSCef08790	platform-76xx	PWAN-1:Hidden vlans overlap .1q vlans on same PWAN sub-intf
CSCuk41411	Routing	HA: show cef linecard doesnt display RRP as expected
CSCuk49384	Routing	Suppress t/bs for null fibidb->idb on newly active RP on SSO s/o
CSCeb29888	Unknown	Bus error at chg_ipfib_excpbrg_entry
CSCed58661	Unknown	High CPU due to FIB Control Task on SP
CSCee00311	Unknown	Unexpected reload after clearing the routing table
CSCee09692	Unknown	Sup720: IPX traffic rate limited based on mls rate limiters
CSCee22821	Unknown	Bus error at stile_update_ad_tables
CSCee25454	Unknown	SADB peering process leaks memory after overnight test
CSCee70075	Unknown	after reset of module with DFC, PBR gets SW switched
CSCef20654	Unknown	SP crashes due to Supervisor online diag failure-loading 0608 image
CSCef72939	Unknown	SSO swover canot decode data desc. L1NULL0 msg when new stdby is up
CSCef75411	Unknown	Traffic over TP tunnels stops after forced SSO switchover
CSCef77822	Unknown	VRF: Crypto maps not downloaded, ACE PL struck...
CSCeg51793	Unknown	MVPN: Address Error Exception after config change w/ Mvpn
CSCeg71317	Unknown	changing CEF loadsharing to simple => all routes point to drop adj
CSCin78242	Unknown	VLAN flooding when SPAN configured.
CSCsd98887	Unknown	SP Memory Leak In mls-msc Process

Resolved Caveats in Release 12.2(18)SXD7b

Resolved Infrastructure Caveats

- CSCsc64976—Resolved in 12.2(18)SXD7b

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

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

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20051201-http.html

Resolved Management Caveats

- CSCsf07847—Resolved in 12.2(18)SXD7b

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

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

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

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

Other Resolved Caveats in Release 12.2(18)SXD7b

Identifier	Technology	Description
CSCse78963	Infrastructure	adopt new default summer-time rules from EPA BADCODE BUG
CSCse04560	IPServices	tftp-server allows for information disclosure .
CSCsd44517	Unknown	flow control needs to be toggle off/on to become active after no shut

Resolved Caveats in Release 12.2(18)SXD7a

Resolved Infrastructure Caveats

- CSCsf04754—Resolved in 12.2(18)SXD7a

  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 LAN Caveats

- CSCsd34759—Resolved in 12.2(18)SXD7a

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

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

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

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

  These vulnerabilities are addressed by Cisco IDs:

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

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

  http://www.cisco.com/en/US/products/csr/cisco-sr-20060913-vtp.html

Resolved Routing Caveats

- CSCsd40334—Resolved in 12.2(18)SXD7a

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

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

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

  This advisory is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html

- CSCec71950—Resolved in 12.2(18)SXD7a

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

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

  There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing.

This advisory is available at:

http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-crafted-ip-option.html

Resolved Unknown Caveats

- CSCsb52717—Resolved in 12.2(18)SXD7a

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

  Conditions: Affects all IOS versions that support mVPN MDT.

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

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

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

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

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

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

- CSCsd75273—Resolved in 12.2(18)SXD7a

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

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

  A Cisco Security Advisory for this vulnerability is posted at
  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

- CSCse52951—Resolved in 12.2(18)SXD7a

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

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

  A Cisco Security Advisory for this vulnerability is posted at

http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-nam.html

Resolved Voice Caveats

- CSCsc60249—Resolved in 12.2(18)SXD7a

  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 Resolved Caveats in Release 12.2(18)SXD7a

Identifier	Technology	Description
CSCsb11698	AAA	Input Queue Wedge with TACACs
CSCsd34855	LAN	VTP update with a VLAN name >100 characters causes buffer overflow .
CSCsc72722	Security	CBAC - firewall resets TCP idle timer upon receiving invalid TCP packets
CSCej21698	Unknown	EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
CSCse73539	Unknown	c7600 - crash of active sup720 after inserting a second one

Resolved Caveats in Release 12.2(18)SXD7

Resolved AAA Caveats

- CSCed09685—Resolved in 12.2(18)SXD7

  Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

Other Resolved Caveats in Release 12.2(18)SXD7

Identifier	Technology	Description
CSCsb09190	MPLS	Next-hop label missing for non-vpn prefixes with dual RRs
CSCed94829	Unknown	IOS reloads due to malformed IKE messages
CSCee84918	Unknown	DHCP snooping on 3550 drops DHCPNAKs recieved when renewing old IP
CSCef66632	Unknown	Demand Aging clearing entries every 4 seconds, without contention
CSCei37672	Unknown	chevys/c2lc take ~ 180s before resetting following a mandatory proc exit
CSCsb12076	Unknown	VPN-SM: GRE RP pkts coming to IPSec with tvlan causing route flaps
CSCsb50559	Unknown	Need fix for MWAM for CSCee10005
CSCsb98702	Unknown	Breakpoint (signal 5 exception) when ltl profiling .

Resolved Caveats in Release 12.2(18)SXD6

Identifier	Technology	Description
CSCdt12296	QoS	RSVP Path message packets are process switched when data is CEF swit
CSCeh73049	Unknown	tclsh mode bypasses aaa command authorization check
CSCei76358	Unknown	cleanup of user interface data

Resolved Caveats in Release 12.2(18)SXD5

Resolved AAA Caveats

- CSCee45312—Resolved in 12.2(18)SXD5

  Remote Authentication Dial In User Service (RADIUS) authentication on a device that is running certain versions of Cisco Internetworking Operating System (IOS) and configured with a fallback method to none can be bypassed.

  Systems that are configured for other authentication methods or that are not configured with a fallback method to none are not affected.

  Only the systems that are running certain versions of Cisco IOS are affected. Not all configurations using RADIUS and none are vulnerable to this issue. Some configurations using RADIUS, none and an additional method are not affected.

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

  More details can be found in the security advisory which posted at the following URL http://www.cisco.com/en/US/products/csa/cisco-sa-20050629-aaa.html

Resolved Unknown Caveats

- CSCsa67611—Resolved in 12.2(18)SXD5

  For packets incoming MPLS Tagged and going out as untagged IP (tag to IP case) if output features (like egress ACL, egress WCCP) are applied upon a reload of a switch one may find that the egress features no longer get applied.

  This has been seen with 12.2(17b)SXB6 and 12.2(18d)SXD2.

Packet impacted Concern : Incoming packet hitting the 6500 with sup720 with one label and exiting the switch on a non mpls int (tag to ip path) on which some output feature are configured (like output acl , output wccp or...)

Impact : these packet should always be recirculated as there are some output feature. After a reload of the switch recirculation do not happen anymore and as a result all packet bypass the ACL or any output feature.

Workaround: disable and reapply all output features on the output interface and output feature will start to work again.

Other Resolved Caveats in Release 12.2(18)SXD5

Identifier	Technology	Description
CSCsa74002	AAA	Input queue - wedged when traffic punted to the CPU
CSCeg19038	Infrastructure	The entCacheFlag should not be shared with several entity tables.
CSCeg64124	Infrastructure	SAA not sending packets to line after a period of time
CSCin53807	Infrastructure	Warm Reboot Decompression may fail for certain images
CSCeb47150	LegacyProtocols	Unable to Establish DLSw Peer Connection Through VPN/NAT Tunnel
CSCeg28814	Multicast	Duplicated mcast packet due to wrong FPOE in egress replication mode
CSCee24349	QoS	Crash at fib_post_download_processing when reloading
CSCeg49010	QoS	ISIS updates not sent when output qos police is set
CSCsa57155	QoS	nbar makes RP in cat6k crash with memory corruption when doing sso
CSCeg62496	Routing	Type-3 lsa not generated if Type-1 flaps coming from multiple areas
CSCeh13489	Routing	BGP shouldn't propogate an update w excessive AS Path > 255
CSCin84644	Routing	Routes are not seen on neighbors after switchover on eigrp stub rtr
CSCsa74271	Routing	OSPF NSF not working, traffic drops for a few seconds
CSCsa78259	Routing	IOS reload due to specific BGP routing update
CSCsa80861	Routing	BGP to IGP redistribution broken with mutual redistribution points
CSCec22308	Security	mem allocated at PKI_ParseX500Dn(0x6207eb2c)+0x34 was leaked
CSCec32184	Security	RSA-SIG IKE leaks memory
CSCee10005	Unknown	Cat6500 service module connectivity issue with crossmodule etherchan
CSCee37771	Unknown	67xx: Rommon Upgrade Failure
CSCee78451	Unknown	Native:Policing rate is not accurate with small packets
CSCee82867	Unknown	Changing dot1x host-mode = multi causes An unknown operational error
CSCef10010	Unknown	Ca6K - input errors on dot1Q trunks for pkts larger than 1496
CSCef36367	Unknown	MMLS: High CPU after Sparse->Bidir transition
CSCef56578	Unknown	VPNSM: traffic counter broken for GRE interface terminated on VPNSM
CSCef82367	Unknown	IP traff not frwded on G+CR2 port if toggled between routed/switched
CSCef93632	Unknown	software force reload when slb swith mode
CSCeg11883	Unknown	After RPR+ switchover standby keeps on crashing continuously
CSCeg56052	Unknown	Active and Standby SP crash due to GC Entry memoryleak

Identifier	Technology	Description
CSCeg62365	Unknown	rxHCDropEvents incrementing on 6704-10GE interface
CSCeh08451	Unknown	Excessive Overruns and lbusDrops due heavy flow control over fabric
CSCeh29617	Unknown	PP:Sup3:FRoMPLS:CHOC:pkts dropped on egr (PE-CE)link (ping fails)
CSCeh54533	Unknown	IOS SLB with Egress ACL under SVI breaks L2 icmp traffic
CSCeh62522	Unknown	igmp snooping source only doesnt work for certain range of group ad
CSCsa65200	Unknown	Transmit power is output from admindown IF after system restart
CSCsa70835	Unknown	SUp720 may see random packet loss when host leaves or joins; OIF +- 85
CSCsa74464	Unknown	Bus error after config synch of CSM
CSCsa76031	Unknown	6748-GE-TX: Transmit fails on port hardcoded to 10/100/1000 or auto mode
CSCsa77211	Unknown	Memory Corruption triggered while adding Microflow Policer ACL
CSCsa80358	Unknown	Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks
CSCsa85123	Unknown	Cisco 7609 :OSM-1CHOC12DS0-SI :RFI bit should be undefined for VC-12
CSCsa87388	Unknown	cat6000 : ciscoEnvMonTempStatusChangeNotif to many traps - VDB inlet
CSCsa88102	Unknown	Crash on Cat6K/Sup720 running 12.2(18)SXD3 due to the memory leak (FIB)

Resolved Caveats in Release 12.2(18)SXD4

Resolved LAN Caveats

- CSCsa67294—Resolved in 12.2(18)SXD4

  Symptom: A Cisco Catalyst Switch may reload upon receipt of a malformed VTP packet.

  Conditions: The malformed VTP packet must meet the following requirements:

  - Must be received on a port configured for ISL or 802.1q trunking AND
  - Must correctly match the VTP domain name

  This does not affect switch ports configured for the voice vlan.

  Affected platforms:

  - Cisco 2900XL Series
  - Cisco 2900XL LRE Series
  - Cisco 2940 Series
  - Cisco 2950 Series
  - Cisco 2950-LRE Series
  - Cisco 2955 Series
  - Cisco 3500XL Series
  - Cisco IGESM

  No other Cisco devices are known to be vulnerable to this issue.

  Workarounds:

  Customers may want to connect ports configured for trunking to known, trusted devices.

Resolved Management Caveats

- CSCdz54403—Resolved in 12.2(18)SXD4

  Symptoms: A Cisco router may crash when IPSec IKE SNMP variables are retrieved, and a bus error and a traceback may be logged.

  Conditions: This symptom is observed when at least one SA is established. The symptom does not always occur, but when you retrieve the IPSec IKE SNMP variables once every 10 minutes, the router eventually crashes after a few hours.

  Workaround: The workaround is to block access to the CISCO-IPSEC-FLOW-MONITOR-MIB - [or just the cikeTunnelTable] using SNMP views so that no one walks this MIB and cause this crash.

- CSCed11835—Resolved in 12.2(18)SXD4

  Symptoms: A Cisco 7200 VXR router that terminates a large number of IPSec tunnels may restart unexpectedly.

  Conditions: This symptom is observed when IKE MIB variables are being polled on the router.

  Workaround: Avoid polling of IKE MIB variables.

Resolved Routing Caveats

- CSCef68324—Resolved in 12.2(18)SXD4

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

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

  More details can be found in the security advisory that is posted at:

  http://www.cisco.com/en/US/products/csa/cisco-sa-20050729-ipv6.html

- CSCef61610—Resolved in 12.2(18)SXD4

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

CSCef60659—Resolved in 12.2(18)SXD4

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP "hard" error messages
2. Attacks that use ICMP "fragmentation needed and Dont' Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP "source quench" messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

- CSCef67682—Resolved in 12.2(18)SXD4

Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognises as its own.

This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html contain fixes for this issue.

Resolved Unknown Caveats

- CSCee59999—Resolved in 12.2(18)SXD4

  Symptoms: When auto-reconnect is configured on an EzVPN server and an EzVPN client attempts to connect, failures may occur in AAA accounting.

  The output of the **debug crypto isakmp aaa** command on the EzVPN server shows an error message such as the following:

  ISAKMP AAA: Unable to send AAA Accounting Start
  %CRYPTO-4-IPSEC_AAA_START_FAILURE: IPSEC Accounting was unable to send start record

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3 or Release 12.3(8)T or a later release and that functions as an EzVPN server.

  Workaround: There is no workaround.

- CSCef44225—Resolved in 12.2(18)SXD4

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Other Resolved Caveats in Release 12.2(18)SXD4

Identifier	Technology	Description
CSCin84694	ATM	Workaround fix for PA-A3/A6 SAR hardware issue
CSCin86455	ATM	PA-A3/A6: Performance optimization and code cleanup
CSCeh13292	Content	WCCP Multiple Configurations causes high CPU
CSCed63357	Infrastructure	show disk#: and dir disk#: inconsistent
CSCee91044	Infrastructure	SNMP Trap Sent In Error Upon Every IKE Lifetime Expiry
CSCea25073	IPServices	IOS FTP client code rewrite
CSCec50485	IPServices	copy ftp flash fails with 3COM ftpserver

Identifier	Technology	Description
CSCeg73883	Management	cikePeerLocalAddr is not augmenting properly
CSCdu28706	MPLS	ARP rejects requests from interfaces in different vrfs
CSCdz85325	MPLS	TFIB not get updated after delete and re-add static route
CSCef37186	MPLS	cpuhog/watchdog-crash on mplsXCIndexNext mib query
CSCeg27836	MPLS	suspect vrf leak following foreign ebgp flap
CSCeg90033	MPLS	Missing labels in MPLS/VPN forwarding table
CSCsa53117	MPLS	MLS cef hardware Freeze
CSCef60452	Multicast	possible blackout when receiving Join on RPF interface (iif)
CSCeg47780	platform-76xx	RFC1483 Bridging broken on BT
CSCef66517	QoS	packet drop on flexwan when traffic shaping
CSCdv76375	Routing	OSPF neighbor command unsupported in VPN routing instance
CSCed59370	Routing	OSPF Type 5 LSA not updated when forwarding address changes
CSCef50427	Routing	System crashed when show ip bgp XX.
CSCef65500	Routing	ospf_db_timer_tick cpuhog process OSPF
CSCef93215	Routing	router crash at ospf_build_one_paced_update
CSCeg07725	Routing	EIGRP redistributing BGP inconsistently after BGP topology changes
CSCeh07809	Routing	BGP leaves a stale CEF entry
CSCeh12233	Routing	12.2SX: fibtype2fibmsg crash - backout CSCef30577
CSCeh15802	Routing	OSPF vrf config lost after reload
CSCsa40588	Routing	Routes are not withdrawn from routing table after BGP routes are removed
CSCsa55048	Routing	Static exported in vrf has wrong cef entry
CSCsa59600	Routing	IPSec PMTUD not working [after CSCef44225]
CSCdu83050	Security	ssh needs source-address
CSCef67660	Security	sshv2 malform client ignore msg cause demage to router
CSCef98116	Security	cat6500 12.2SX: SSH issues with privilege levels
CSCeb79090	Unknown	snmp getmany of ciscoFlashFileTable crash the 7300 device
CSCed82736	Unknown	SYS-2-GETBUF: Bad getbuffer, bytes= 65535
CSCee67261	Unknown	Memory leak on crypto_ikmp_peer_create
CSCef72013	Unknown	unicast flooding due to purging of some mac-addres entry with dfc3/pfc3
CSCef82884	Unknown	Failed to delete billing plan errors
CSCef92360	Unknown	Policy allowing 15 char. names, but not supported
CSCef93371	Unknown	bpduguard broken when access and voice vlan enabled
CSCef96465	Unknown	WS-X6704-10GE port shows up/up state while other side is shutdown
CSCeg16684	Unknown	Some VPLS VCs fail to pass traffic after a link failure in the core
CSCeg26993	Unknown	Cat6000/Cat6500 dot1Q sub-int return incorrect SNMP statistics.
CSCeg30437	Unknown	VPLS:ATOM:CWAN: Some VCs remain down, LFIB/TTFIB are ok
CSCeg40543	Unknown	some vcs do not pass traffic after supervisor switchover

Identifier	Technology	Description
CSCeg41623	Unknown	CSM:Only configured vlans should be allowed on trunk
CSCeg48068	Unknown	After gige sub-int was deleted, no counters in show main interface
CSCeg49196	Unknown	Excessive Overruns and lbusDrops due heavy flow control over fabric
CSCeg51616	Unknown	Bus error crash at adjacency_compute_hash
CSCeg67986	Unknown	PA-POS-2OC3 interface 1 remains up/up with SLOS
CSCeg70376	Unknown	Sup720 : Ingress VSPAN is not working for VoIP VLAN
CSCeg77040	Unknown	Session Counts not decremented when processing IC
CSCeh05310	Unknown	ATM OSM MPB: One PVC failed to TX PKT if the LC in slot/port 1/7 of 7613
CSCeh13200	Unknown	Active RP crash @ rf_proxy_fatal_error+0x60 when stby reloads
CSCin87976	Unknown	Need to rate-limit EOS Error interrupts
CSCsa51770	Unknown	Configuration of RSPAN on 12.2(18)SXD3 causes high CPU
CSCsa57079	Unknown	C7600 PE does NOT send BPDU including dot1Q tag on EoMPLS
CSCsa59260	Unknown	C7600 EoMPLS PE correctly does NOT send the COS value of BPDU

Resolved Caveats in Release 12.2(18)SXD3

Resolved Unknown Caveats

- CSCef90002—Resolved in 12.2(18)SXD3

  Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

  MPLS packets can only be sent from the local network segment.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-mpls.html

Other Resolved Caveats in Release 12.2(18)SXD3

Identifier	Technology	Description
CSCee49862	Access	PA-MC-2T3+ does not adhere to ANSI T1.231 standard
CSCee70591	Access	PA-2T3+ does not adhere to the ANSI T1.231 standard
CSCef01725	Infrastructure	pak_realign driving up CPU usage
CSCeg11566	Infrastructure	SNMP May Consume all the I/O Memory
CSCed82551	IPServices	VRRP: problem with dynamic reconfiguration of secondary IP addresses
CSCin83554	Management	CDP doesnt propogates MWAM to Supervisor with 12.2(18)SXD1 image
CSCec10116	MPLS	MPLS VPN PE uses global addresses on some packets originated in VRF
CSCed57281	MPLS	CPU hog in CEF reloader while adding a vrf interface
CSCee37430	MPLS	Missing LFIB tag rewrite on LC after loss of /32 entry to its next-hop
CSCef14446	MPLS	mpls vpn: recirculation vlan for agg label is not mapped to vpn

Identifier	Technology	Description
CSCef80349	MPLS	GSR midpoint rejects RESV after link flap
CSCeg03885	MPLS	TE label missed on MPLS TE tunnel
CSCsa44122	MPLS	Missing cef table and data structure error after deleting VRF
CSCef12304	platform-76xx	PWAN2:Connectivity is broken between GE-WAN if one end shut/no shut
CSCef35398	platform-76xx	OSM-2OC12-ATM-SI+ - SRIC IPM parity error
CSCef74227	platform-76xx	LAN GE of OSM incorrectly increments giants on dot1q trunk port
CSCef76828	platform-76xx	connectivity broken after config/unconfig tunnel interfaces
CSCef82720	platform-76xx	add dot1Q subinterface in ifTable for GE-WAN card
CSCeg03144	platform-76xx	%EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR on Sup720
CSCeg10236	platform-76xx	PWAN2:GBIC type shown as not connected in show int
CSCee22810	QoS	Router stops sending LMI with QOS configured
CSCef06034	QoS	Sup720 crashes after SSO Failover with nbar configured
CSCef47829	QoS	Physical int out of BW: no error message that MQC policy cant apply
CSCed63342	Routing	RIP-Unicast updates not sent to configured RIP neighbors
CSCed63876	Routing	BGP: router crashes pointing to ed_decay_penalty
CSCee59315	Routing	MPLS-VPN:Corrupted BGP table showing stale and/or poisoned paths
CSCee85202	Routing	Long delay for vrf to be removed from vrf table when un-configured
CSCee88898	Routing	ALIGN-3-SPURIOUS in show_ipprotocol
CSCef08797	Routing	static routes not advertised to BGP peers
CSCef69650	Routing	Spurious memory access during SNMP MIB walk
CSCef89294	Routing	MPLS VPN EIBGP: Missing some multipath routes
CSCeg05830	Routing	BGP: Update peer-group remove-private-as functionality
CSCeg08344	Routing	with cef/dcef enabled & compression on, tcp frames getting dropped
CSCeg26378	Routing	Dest CEF entry is missing in DCEF table. All pkts are punted to RP.
CSCeg31951	Routing	BGP: Put peers with as-override & rem-pvt-as in separate updgrps
CSCec00930	Unknown	bus error at crypto_ipsec_clear_peer_sas
CSCed07367	Unknown	Proton: show int serial input/output counters are 0
CSCed25505	Unknown	reset of csm causes one of WS-X6248A-TEL to reset in a chassis
CSCed45971	Unknown	Unexpected Exception crash when EzVPN server fails connect to RADIUS
CSCee03625	Unknown	FWSM:VFW: Jumbo frames dont make across through the fwsm
CSCee32365	Unknown	MFR: LMI exchanges fail over MFR interfaces
CSCee55233	Unknown	Large L3 port-channel config with stats collection caused high CPU
CSCee86168	Unknown	active SP resets, sr7100 errata 11
CSCef27359	Unknown	SW and HW cef adjacency inconsistency
CSCef35707	Unknown	L2 Forwarding Table ECC error handler not working properly
CSCef37026	Unknown	Running configuration is not synching between DR and NDR on MSFC3
CSCef42312	Unknown	Ambiguous command: snmp-server enable traps config

Identifier	Technology	Description
CSCef47466	Unknown	High latency and packet drop when any interface goes down on OSM
CSCef48810	Unknown	MAC Address entries learned via DFC3A not forwarded to SUP720
CSCef53290	Unknown	Using config mls ip ids causes switch to reload unexpectedly
CSCef58323	Unknown	%EARLY-L2_ASIC-DFC-SRCH_ENG_FAIL T/B on Berytos with L2(10k mac)Traf
CSCef58932	Unknown	VACL filter out STP BPDU
CSCef70298	Unknown	IFindex missing IDBs after deleting and adding T1 channels
CSCef79592	Unknown	Class-default shows packets output 0; packet drops 0
CSCef82309	Unknown	Cache error caused standby SP crashed @ data_cache_inv after reload
CSCef87392	Unknown	Giants incorrectly counted on trunk with 67xx modules
CSCef88685	Unknown	mcast ltl cleared out on WS-X6816-GBIC after NSF/SSO failover
CSCef91572	Unknown	Software forced crash at process pm_mp_notify_cp_port_admin_state
CSCef95365	Unknown	Crash with Real cache error detected on show platform asicreg
CSCeg01297	Unknown	System crash caused by pkt of incorrect length/IP header checksum
CSCeg01510	Unknown	Device crashes when we configure no vlan <vlan nu>
CSCeg02873	Unknown	Netflow v9 config crashes router
CSCeg06570	Unknown	PA-MC-STM1: %CBUS-3-CCBCMDFAIL1: Controller 2, cmd (62 0x0000000E)
CSCeg06698	Unknown	COS rewritten for routed multicast traffic
CSCeg08389	Unknown	Interface counters do not increment on a Virtual MFR interface
CSCeg19269	Unknown	gt 12L4 Oper in acl dest port doesnt expand corectly;pkts non-qos fw
CSCeg21620	Unknown	Inconsistencies in handling CSM configurations
CSCeg22198	Unknown	VSEC:VPN-SM:DF bit set will break Blade to Blade failover
CSCeg24287	Unknown	LDP does not recover after link failure between two NPEs in a networ
CSCeg24675	Unknown	cannot modify class-map in PQ when plicy is applied to OSM
CSCeg26382	Unknown	wireless client not able to browse the Internet due to MSS issue
CSCeg31792	Unknown	Sup2 crash with AGSM
CSCeg40177	Unknown	Tag to Ip path has all zero src and dest mac
CSCeg41762	Unknown	VPN-SM: MSFC3 sup720 crash managing the Crypto-ACE IPsec stats cache
CSCeg43827	Unknown	At duplex half and speed 10, RCP failed to copy image.
CSCeg43854	Unknown	Taking Accounting no inservice also takes other Accounting no inserv
CSCej52641	Unknown	LCP_FW_ERR: 67xx linecards reset due to packet buffer P2N EEC1 error
CSCin65698	Unknown	%INTERFACE_API-3-NODESTROYSUBBLOCK msg on reconfiguring Potent PA
CSCin83972	Unknown	Dot1x Scalability issue - Port from Tetons-2
CSCin84750	Unknown	IP address in ACE ignored while doing l4op expansion
CSCsa40962	Unknown	Memory leak in Crypto IKMP process on IOS EzVPN server .
CSCef91994	WAN	FLEXWAN - PA-A3 - packet drop when ping 1500bytes with MPLS
CSCef93103	WAN	bridge-vlan on Flexwan PVC floods BPDUs

Resolved Caveats in Release 12.2(18)SXD2

Resolved Routing Caveats

- CSCee67450—Resolved in 12.2(18)SXD2

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command bgp log-neighbor-changes configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

  Cisco has made free software available to address this problem.

  This issue is tracked by CERT/CC VU#689326.

  This advisory will be posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050126-bgp.html

Other Resolved Caveats in Release 12.2(18)SXD2

Identifier	Technology	Description
CSCea19918	Routing	BGP: need to do multipath with different as-paths
CSCef63549	Unknown	Multicast MET management fix and increase OIF above 1023 per flow
CSCef70677	Unknown	CSG Module switches to CSM when trying to change ruleset
CSCef72205	Unknown	vlan stops forwarding
CSCef73076	Unknown	ALIGN-SP-3-CORRECT seen in mcast_igmp_handle_igmp_pak
CSCef82797	Unknown	Distributed EtherChannel may caused packet loss
CSCef89139	Unknown	Adjacency pointers not Updated when 2nd Link Removed on 7600
CSCef95789	Unknown	Switch Interfaces stop forwarding Traffic
CSCeg05819	Unknown	CPP does not get applied in Hardware after reloading the router
CSCin82979	Unknown	Flow mask changed from full flow to destination on switchover

Resolved Caveats in Release 12.2(18)SXD1

Resolved IPServices Caveats

- CSCed78149—Resolved in 12.2(18)SXD1

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Resolved Routing Caveats

- CSCef48336—Resolved in 12.2(18)SXD1

  OSPF is a routing protocol defined by RFC 2328. It is designed to manage IP routing inside an Autonomous System (AS). OSPF packets use IP protocol number 89.

  A vulnerability exists in the processing of an OSPF packet that can be exploited to cause the reload of a system.

  Since OSPF needs to process unicast packets as well as multicast packets, this vulnerability can be exploited remotely. It is also possible for an attacker to target multiple systems on the local segment at a time.

  Using OSPF Authentication can be used to mitigate the effects of this vulnerability. Using OSPF Authentication is a highly recommended security best practice

  A Cisco device receiving a malformed OSPF packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DOS attack.

  Workarounds:

  - Using OSPF Authentication

    OSPF authentication may be used as a workaround. OSPF packets without a valid key will not be processed. MD5 authentication is highly recommended, due to inherent weaknesses in plain text authentication. With plain text authentication, the authentication key will be sent unencrypted over the network, which can allow an attacker on a local network segment to capture the key by sniffing packets.

    Refer to http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080094069.shtml for more information about OSPF authentication.

  - Infrastructure Access Control Lists

    Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered 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 white paper “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection ACLs: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Resolved Unknown Caveats

- CSCin82407—Resolved in 12.2(18)SXD1

  Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

  Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

  This advisory will be posted to http://www.cisco.com/en/US/products/csa/cisco-sa-20050406-xauth.html

Other Resolved Caveats in Release 12.2(18)SXD1

Identifier	Technology	Description
CSCed88768	AAA	console/vty/telnet password fails after upgrade to 12.2(18)S images
CSCee82681	Access	Counter: Counters stuck on serial interface
CSCin76828	Access	Multi-channel T1 PA's in FlexWAN module fail boot-up diagnostics
CSCin79495	Access	FW2-HYB:%CWAN_RP-4-SEMAHOG observed with 256 channels on PA-MC-8TE1+
CSCin79468	ATM	ATM SSO: PVC state not in sync between active/sdby after a sh/no-sh
CSCeb28941	Content	IOS NAT and WCCP do not work together
CSCef46191	IPServices	Unable to telnet
CSCin78000	IPServices	LDP session in xmit state if MPLS flapped at high traffic on L2 SUP3
CSCed21063	MPLS	TE Tunnel Destination Label Missing
CSCed54416	MPLS	GRP crash in tfib when pos fiber is disconnected or connected
CSCef25866	MPLS	Blackholing of traffic during FRR reconnect with invalid cache adj
CSCed19898	platform-76xx	:ATMoMPLS VCs freeze/vanallen error/w toggling core loopback
CSCee72817	platform-76xx	BGP neighbor relationship flaps periodically between PEs and RRs
CSCef12193	platform-76xx	FABRIC-SP-6-TIMEOUT_ERR: Fabric in slot 8 reported timeout error
CSCef63516	platform-76xx	OSM crash: POSLC-3-SOP: TxSOP-0 SOP. (source=0x1, halt_minor0=0x8002
CSCef83690	platform-76xx	FRoMPLS:Connectivity broken if the ping packet size is < 58 byte
CSCee85257	PPP	cRTP does not work with CEF on FlexWAN controller.
CSCef44786	PPP	ATMPA-3-BADVCD seen when running MLPPP at low speed
CSCec22723	Routing	Router may reload unexpectedly due to ISPF(OSPF)
CSCec82398	Routing	BGP needs to modify a route instead of delete/add
CSCed36386	Routing	APS:Ping fail on alternate packets after revertive switching
CSCed77612	Routing	network option missing in isis interface command
CSCee43166	Routing	BGP: reduce CPU load for processing inbound VPNv4 updates
CSCef44976	Routing	MPLS traffic not forwarded from 1 vlan in multi vlan vrf
CSCdy33703	Unknown	Need span support for port 1/4 & 1/3
CSCee42657	Unknown	sup720 crashing after reload with large configuration
CSCee43191	Unknown	SLB TCAM entries not programmed properly after SSO

Identifier	Technology	Description
CSCee54446	Unknown	PP: cant ping after FR PVC removed and reconfigured
CSCee68057	Unknown	MPLS TE Tunnel counters are not working with MPLS VPN CSC BGP+label
CSCee70293	Unknown	FWLB: Intermittent creation of conns on a firewallfarm.
CSCee75620	Unknown	RP crashes after enable CBAC
CSCee83655	Unknown	CPU_MONITOR-2-NOT_RUNNING_TB: CPU_MONITOR tracebackrate_limit_loop
CSCee93511	Unknown	Chassis crash in crypto_ikmp_peer_struct_unlock with Gre/Ipsec
CSCee95708	Unknown	MSFC2-3-TOOBIG on sup720 in MPLS/VPN environment
CSCef02439	Unknown	FW2 reloads with Module failed SCP download
CSCef07017	Unknown	VACL is not working for RSPAN traffic with mcast enabled
CSCef07848	Unknown	VRF over GRE traffic is s/w switched after remove/add mls mpl tu-rec
CSCef08097	Unknown	IP RIB Update can hog memory after bgp flap leading to fib disable
CSCef10192	Unknown	SSO: Standby failed with mismatch config on reading FW slot cache
CSCef13797	Unknown	TCAM Capacity Exceeded with ACL on POS Interface
CSCef14106	Unknown	IDSM2 stops detecting attack after 2nd failover
CSCef21575	Unknown	Sup720 - ACL Incorrectly Denies Packets in HW
CSCef23843	Unknown	Module reset in getting CBL info
CSCef25710	Unknown	EOS error handling changes
CSCef26512	Unknown	WS-X6582-2PA :Unable to read cwan<slot>/0-disk0:
CSCef26926	Unknown	VSEC:VPN-SM:router crashed in get_ipsec_attributes
CSCef30308	Unknown	all zero source and dest mac address in show mls adj entry det
CSCef41228	Unknown	SSO failover causes WS-X6816-GBIC reset
CSCef43000	Unknown	Rockies1A SNMP:Traceback/Corrupt vlan db when set vlan 1002..1005 na
CSCef47414	Unknown	VTP code fail to restore vlan database properly
CSCef47639	Unknown	no redirect-vserver REDIR1 crashes SUP
CSCef49330	Unknown	APS not working on the PA-MC-STM1
CSCef49811	Unknown	Router crashes while freeing memory in ace_hapi_pkt_proc
CSCef52858	Unknown	Any newly configured tunnels, makes the existing tunnels go down
CSCef65249	Unknown	VPN-SM: ACE crashes with certain class of ACL
CSCef65827	Unknown	GRE o/v IPSec with VPNSM intermittently loses connectivity
CSCef67810	Unknown	get-bulk for portGrp causes cpu spike and delayed response
CSCef72233	Unknown	no nat server cmd not taken into config with 12.2(18)SXD
CSCef75924	Unknown	packet drop for L3 trafic over dist. etherchannel with SPAN enabled
CSCef78235	Unknown	Disable egress span of vacl redirected packets
CSCin74811	Unknown	user startup config rejected at bootup with > 1 acl match in Vacl
CSCin77443	Unknown	HYB:HA:Slave crashes on configuring Virtual-Template interface
CSCin78110	Unknown	Some E1 controller does not come up if a large config on other LC

Identifier	Technology	Description
CSCin78773	Unknown	UFP not working after SSO with 6816 and uplink ports.
CSCef60434	WAN	Need to prevent hyperion reset on receiving corrupt packets

Resolved Caveats in Release 12.2(18)SXD

Resolved IPServices Caveats

- CSCee50294—Resolved in 12.2(18)SXD

  Cisco IOS devices running branches of Cisco IOS version 12.2S that have Dynamic Host Configuration Protocol (DHCP) server or relay agent enabled, even if not configured, are vulnerable to a denial of service where the input queue becomes blocked when receiving specifically crafted DHCP packets. Cisco is providing free fixed software to address this issue. There are also workarounds to mitigate this vulnerability. This issue was introduced by the fix included in CSCdx46180 and is being tracked by Cisco Bug ID CSCee50294.

  This advisory is available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20041110-dhcp .

  There are multiple workarounds for this issue: There are four possible workarounds for this vulnerability:

  - Disabling the dhcp service
  - Control Plane Policing
  - Two versions of Access Control Lists

  Disabling the DHCP Service

  This vulnerability can be mitigated by utilizing the command:

  ```
  no service dhcp
  ```

  However, this workaround will disable all DHCP processing on the device, including the DHCP helper functionality that may be necessary in some network configurations.

  Control Plane Policing Feature

  The Control Plane Policy feature may be used to mitigate this vulnerability, as in the following example:

  ```
  access-list 140 deny   udp host 192.168.13.1 any eq bootps
  access-list 140 deny   udp any host 192.168.13.1 eq bootps
  access-list 140 deny   udp any host 255.255.255.255 eq bootps
  access-list 140 permit udp any any eq bootps

  class-map match-all bootps-class
    match access-group 140

  policy-map control-plane-policy
    class bootps-class

       police 8000 1500 1500 conform-action drop exceed-action drop

  control-plane
   service-policy input control-plane-policy
  ```

  For this example 192.168.13.1 is a legitimate DHCP server.

  Additional information on the configuration and use of the CPP feature can be found at this link:

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

  This workaround is only applicable to Cisco IOS 12.2S, as this feature is only available in Cisco IOS versions 12.2S and 12.3T. Cisco IOS 12.3T is not impacted by this advisory.

Access Lists - Two Methods

Access lists can be applied to block DHCP/BootP traffic destined to any router interface addresses, as in the following example:

In this example, the IP address192.168.13.1 represents a legitimate DHCP server, the addresses 10.89.236.147 and 192.168.13.2 represent router interface addresses, and 192.168.61.1 represents a loopback interface on the router.

In this example, any bootp/dhcp packets destined to the router interface addresses are blocked.

```
access-list 100 remark permit bootps from the DHCP server
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 remark deny bootps from any to router f1/0
access-list 100 deny   udp any host 10.89.236.147 eq bootps
access-list 100 remark deny bootps from any to router f0/0
access-list 100 deny   udp any host 192.168.13.2 eq bootps
access-list 100 remark deny bootps from any to router loopback1
access-list 100 deny   udp any host 192.168.61.1 eq bootps
access-list 100 remark permit all other traffic
access-list 100 permit ip any any
```

access-list 100 is applied to f0/0 and f1/0 physical interfaces.

```
interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

An alternate configuration for the interface access-list workaround.

This example would also need to be applied to all physical interfaces, but deny statements for all of the IP addresses configured on the router are not necessary in this approach. In this example, the address 192.168.13.1 represents a legitimate DHCP server.

```
access-list 100 permit udp host 192.168.13.1 any eq bootps
access-list 100 permit udp any host 192.168.13.1 eq bootps
access-list 100 permit udp any host 255.255.255.255 eq bootps
access-list 100 deny   udp any any eq bootps

interface FastEthernet0/0
 ip address 192.168.13.2 255.255.255.0
 ip access-group 100 in
interface FastEthernet1/0
 ip address 10.89.236.147 255.255.255.240
 ip access-group 100 in
 ip helper-address 192.168.13.1
```

Resolved Routing Caveats

- CSCec16481—Resolved in 12.2(18)SXD

  A Cisco device running Internetwork Operating System (IOS) and enabled for the Open Shortest Path First (OSPF) Protocol is vulnerable to a Denial of Service (DoS) attack from a malformed OSPF packet. The OSPF protocol is not enabled by default.

  The vulnerability is only present in IOS release trains based on 12.0S, 12.2, and 12.3. Releases based on 12.0, 12.1 mainlines and all IOS images prior to 12.0 are not affected. Refer to the Security Advisory for a complete list of affected release trains.

Further details and the workarounds to mitigate the effects are explained in the Security Advisory which is available at the following URL:

http://www.cisco.com/en/US/products/csa/cisco-sa-20040818-ospf.html

- CSCed40933—Resolved in 12.2(18)SXD

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory which is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-ipv6.

Resolved Security Caveats

- CSCed65285—Resolved in 12.2(18)SXD

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050406-ssh.html

- CSCed93836—Resolved in 12.2(18)SXD

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at
  http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html.

Other Resolved Caveats in Release 12.2(18)SXD

Identifier	Technology	Description
CSCec33028	Access	PA-E3 needs shut/no shut to bring it up
CSCec73063	Access	Output wedge on multilink interface
CSCed08399	Access	NRT:Spurious Accesses seen on 7500 router (etext) for QoS tests
CSCed13350	Access	Ping from PE to CE in VRF not working with dCEF enabled
CSCed65436	Access	Spurious access @ ct3sw_tx_interrupt & ct3sw_fastsend
CSCee64499	Access	CWPA: SYS-3-INVMEMINT invalid mem action interrup level after reload
CSCin66542	Access	line protocol on T1 stays down even when T3 is hard looped
CSCin67296	Access	CWAN SSO :Fram relay PVC down after reload
CSCec03907	ATM	C7500 crashes when interface loopback 10xxxxxxx is configured
CSCec12294	ATM	cfg_atm_vcmode_bcs_func is broken
CSCee04747	ATM	memory leak when removing ATM VCs
CSCin53126	ATM	Router crashed at abort during OIR of ATM OC3 MM PA
CSCin76900	ATM	ATM-IMA stops passing ping after passing traffic for some time
CSCed92290	Content	CE4-NATIVE:wccp redirect issue after reloading the switch
CSCds71171	Infrastructure	Command show snmp ifIndex
CSCdv20075	Infrastructure	%SYS-3-CPUHOG process = IP SNMP
CSCdx30509	Infrastructure	(HUBBLE-ccCopy)no ccCopyCompletion trap sent after copyfile done.
CSCdy65658	Infrastructure	SSO: Policy-map not synched properly with the standby.
CSCdz27562	Infrastructure	snmpwalk on loopback interface gets response from physical int. IP.
CSCea69601	Infrastructure	Disk Corruption on C6400 and/or RSP compatible platforms
CSCeb35205	Infrastructure	Memory corruption and crash in SP after TFTP copying
CSCeb71693	Infrastructure	12.2S: issues with logging snmp-authfail command
CSCeb79675	Infrastructure	SNMP reply packets do not use the correct source address
CSCec55147	Infrastructure	Memory leak in IFS
CSCec63011	Infrastructure	Standby crashes in redundant systems
CSCec69091	Infrastructure	PCMCIA disk 0 is formatted from a diff router error
CSCed16920	Infrastructure	Constant high CPU in TTY background
CSCed44319	Infrastructure	copy produces corrupted files on big ATA disks
CSCed45942	Infrastructure	Bus error due to corrupted managed timer structure
CSCed64664	Infrastructure	SYS-2-LINKED: Bad enqueue messages when terminating multilink vpdn
CSCed81154	Infrastructure	SNMP retrieve configuration file crash SUP720 RP
CSCed86286	Infrastructure	Software forced crash at ssh_process_message_events
CSCin57765	Infrastructure	appending to files on disks can crash/hang system
CSCuk51673	Infrastructure	malloc_aligned adds unnecessary padding
CSCdv89039	IPServices	Bus Error in ipnat_unlock_parent_entry
CSCdw36571	IPServices	NAT: crash while nvgening static entries

Identifier	Technology	Description
CSCdx95455	IPServices	Memory leak in TCP Protocol with translate tcp
CSCea81029	IPServices	show ip igmp int crashed router
CSCeb54853	IPServices	SLB: tcp probes to failed http daemon show OPERATIONAL
CSCec13278	IPServices	IGMP: IGMP_clear_cache() invoked crashed LC when LC OIRed
CSCec29952	IPServices	bgp md5 authentication not working when configured in mpls vpn vrf
CSCec84887	IPServices	Sup720: Disabled STP for VLAN-bridge becomes to enable by shutdown
CSCed25055	IPServices	12.2S RLS3 (IOS): image crashes with copy ftp: bootflash:
CSCed37514	IPServices	HSRP not receiving Hello packets
CSCed52163	IPServices	Crash or CPUHOG when doing HSRP SNMP query
CSCed83740	IPServices	no ip nat source static command should check global and local addres
CSCee06948	IPServices	Sup720 running 12.2(17b)SXA is allowing connections to TCP port 514
CSCea71723	LAN	Qllc/dlsw sends CUR to mac-addr 0000.0000.0000 when x25 host is down
CSCea81145	LAN	SNMP/IFMIB test fails in vLAN env., when ISL in use.
CSCea39508	LegacyProtocols	DLSW SDLC FEP to FEP (NCP PU4 to NCP PU4) FAILS WITH SECONLY
CSCea42831	LegacyProtocols	DLSw FST: Bus error during file transfer on MSFC2
CSCeb22529	LegacyProtocols	Snasw hardcodes llc2 n2=10
CSCeb39238	LegacyProtocols	DLSW bridge-group config changes the bandwidth on bvi int to 56 K
CSCec26432	LegacyProtocols	Router crash when executing show ipx access-lists
CSCec68023	LegacyProtocols	Tracebacks found when executing the command dlsw bridge-group 1
CSCee24464	LegacyProtocols	Router Reload with DLSW Ethernet Redundancy
CSCee39240	LegacyProtocols	certain FE intf can not receive cdp packets with dlsw transparent ER
CSCdz32659	Management	%SYS-2-MALLOCFAIL: -Process= CDP Protocol
CSCeb37746	Management	CDP broadcasts internal address when no address on interface.
CSCec25430	Management	IOS may reload from specific packet
CSCed40563	Management	malicious cfg reload neighbor routers by <show cdp entry * protocol>
CSCin67568	Management	Memory leak in CDP process with long host names
CSCdz08851	MPLS	FRR doesnt trigger on ethernet using RSVP HELLO
CSCdz23318	MPLS	Rewrite index passed incorrectly for loadshare rewrites
CSCdz33630	MPLS	Stanby RP crashes when SSO switchover in the HA MPLS co-existence
CSCdz73149	MPLS	Static route exported between vrfs on same pe router not in vrf RT
CSCea65827	MPLS	RP/VIP Crash: OIR Flexwan/loose IGP Route to BGP next hop router
CSCea72889	MPLS	Const2: MPLS VPN CSC bad table id no mpls on RR server 1kvpn
CSCea74222	MPLS	LSNT:Lose tag rewrite information of remote PE in cef table
CSCea76134	MPLS	e-iBGP loadbalancing does not work .
CSCeb08400	MPLS	Cannot see tfib entry for remote BGP routes with CsC config
CSCeb26389	MPLS	BGP allocates same local label to two VPN prefixes
CSCeb40653	MPLS	Bus error crash at vrf_interface_print when deleting vrf config

Identifier	Technology	Description
CSCeb78347	MPLS	Cannot create a VRF
CSCec45307	MPLS	DT:No memory for the expanded TFIB PSA
CSCec56047	MPLS	TE:gtag-rrr: TSP Tunnel not up (Destination IP address not found)
CSCec69982	MPLS	MPLS-AToM: LDP is not restablished after remove/add xconnect
CSCec86102	MPLS	Inconsistent tag info between RSP and VIP
CSCed22837	MPLS	Bus error ALIGN-1-FATAL:Corrupted program counter
CSCed39059	MPLS	LFIB is inconsistent when P-AIS injected on APS interface
CSCed45746	MPLS	duplicate tag between 2 VRFs
CSCed52578	MPLS	vrf route thru recursive tagged loadshared global route bogus label
CSCed55962	MPLS	Connected subnet not in TFIB
CSCed66160	MPLS	Router crashed while verifying if FRR is active at Backup Head
CSCed72297	MPLS	CPUHOG and watchdog timeout crash in LDP process
CSCed81317	MPLS	can not see bgp routes from CE after import map
CSCed82562	MPLS	TFIB/FIB not updated for static route to interface
CSCee07279	MPLS	TFIB NULLADJ errmsg triggered, fix root cause of null tagout_adj
CSCee15974	MPLS	ICMP message generated by LSR should have TTL=255 in all labels
CSCee26700	MPLS	memory leak caused by LSR MIB queries
CSCee43569	MPLS	TE-DB corruption on headend after NHop reload
CSCee56225	MPLS	Alignment errors in tfib_request_all_tags
CSCee59585	MPLS	Duplicate label in sh ip cef on LC
CSCee61423	MPLS	Traffic drop over TE tun from PE to PE when no LDP in core
CSCuk47482	MPLS	crash after no mpls ip
CSCeb30338	Multicast	Mcast traffic loss each minute as MMLS entry deleted and reinstalled
CSCec70366	Multicast	Mwheel process aborted on watchdog timeout and then SW forced crash
CSCec70428	Multicast	DVMRP segment remain pruned when main forwarder fails
CSCed02952	Multicast	filter-autorp option denys all in announce pkt
CSCed95515	Multicast	Pkts drop in all VLANs when last host in one VLAN leave this group
CSCee88700	Multicast	TCAM entry not built for secondary subnet with multicast stub
CSCee89438	Multicast	MSDP doesnt build S,G state after rxing *,G join
CSCec59728	platform-12000	SSO: Standby RP reloads once it is fully-up
CSCea57792	platform-76xx	13E5/GBIC:GE-WAN int with 1000baseT gbic is down after oir with traf
CSCea74537	platform-76xx	GEWAN:Input counter does not work when packet was received
CSCeb61377	platform-76xx	CWTLC fabric related alignment correction
CSCec59550	platform-76xx	OSM-POS crash @ sky4302_enter_drop_mode
CSCec62800	platform-76xx	20E:CWAN-QOS:Increased PQ latency when increasing default queue traf
CSCed07253	platform-76xx	512 Meg SODIMM chip not recognized and shows 256 instead
CSCed19431	platform-76xx	GigabitEthernet negotiation is broken on 7600

Identifier	Technology	Description
CSCed33881	platform-76xx	fatal errors in lc and line protocol down after reload
CSCed48085	platform-76xx	Stats incorrect for all BB2 OSMs with SUP720
CSCed49872	platform-76xx	SYS-2-GETBUF: Bad getbuffer SCP Hybrid process tracebacks
CSCed51835	platform-76xx	OSM/POS/BB1: OC12 IP 64 bytes performance may degrade
CSCed78077	platform-76xx	LRDI is not reported after reload on OSM-2OC12-ATM-SI PRDI is seen
CSCed86778	platform-76xx	: PQ problems with HQoS policy applied to 100 PWAN2 sub-intf
CSCed92724	platform-76xx	OSM-1CHOC12/T3-SI reporting false path E3 ais after shut/no shut
CSCee01868	platform-76xx	OSM-2+4GE-WAN+:Interface UP/UP with GBIC installed but not connected
CSCee45508	platform-76xx	OSM CHOC-OC12 freezes up while proccessing PPP keepalives
CSCee54642	platform-76xx	OSM local bus out of SYNC after stress
CSCee55056	platform-76xx	OSM interface byte counts are inaccurate
CSCee59667	platform-76xx	GE-WAN+ MTU config inconsistent with other IOS devices
CSCee84887	platform-76xx	OSM interface byte counters broken with high pps + large route table
CSCef19811	platform-76xx	MPLS:VPN:MLPPP:PE not receiving packets from connected CE
CSCed09364	PPP	bridge over multilink ppp cant pass traffic larger than 1499 bytes
CSCed42332	PPP	Distributed link fragmentation and interleaving caused VIP reload
CSCin54720	PPP	Bad refcount at datagram done with mlp_transmit_fragments
CSCin61922	PPP	dLFIoATM : mlp_qos - UUT crash with ALIGN-1-FATAL send_one_bufhdr_pk
CSCin67741	PPP	RP crashes on removing encap from multilink interface
CSCuk47905	PPP	Cannot ping across distributed MLPoATM interface
CSCeb43847	QoS	policy with set cos is accepted in main interface with error msg
CSCeb61825	QoS	VIP quantum not udpdated when MTU changed on PA-A3
CSCec49042	QoS	IPP not being trusted using nbar type class map
CSCec71488	QoS	MSFC2 crashed @ stile_in_policymap when SRM switchover
CSCec75389	QoS	Packet drops not seen in class 2 due to pkt count error on POS intf.
CSCed62637	QoS	CWPA: priority traffic latency varies with default traffic load
CSCee23845	QoS	Policer stops counting on egress after ingress poicy is reapplied.
CSCee31618	QoS	C2SUP2/FW2/CT3+:Voice packet drops at low rates with cRTP+LLQ conf
CSCee68344	QoS	GE-WAN card crashes in /enqueue/process-policymap_msg/policymap_hash
CSCin52060	QoS	After the policy got rejected hqf was not cleaned on vip
CSCin72437	QoS	MQC: Concurrent access crashes the Flexwan during switchover
CSCdr28078	Routing	traceback in MLSM Process on a TRBRF interface, MLS not configured
CSCdt38401	Routing	Frame-relay packets processed by cpu due to CEF inconsistency
CSCdv33550	Routing	%ADJ-3-ADJFIBIDB: Adjacency update with invalid fibidb(8) error
CSCdv33860	Routing	cef adjacency on a lane interface may drop packets
CSCdz40426	Routing	Configuring multiple eigrp processes under a VRF reloads router
CSCdz45031	Routing	distance eigrp missing from config after reload

Identifier	Technology	Description
CSCdz54875	Routing	translate-update broken under AFI mode
CSCdz77047	Routing	network backdoor is not working
CSCea66299	Routing	%BGP-3-NEGCOUNTER messages appear during route flapping
CSCea90941	Routing	IOS Ignores EIGRP Stub Command In Startup-Config at Initial Power On
CSCeb17467	Routing	BGP: RP crashes on clearing the BGP table
CSCeb40561	Routing	[SNMP] GGSN reloads during get next operation
CSCeb41095	Routing	no spf calc or dynamic update to ospf database if better learned rte
CSCeb62136	Routing	OSPF default-information originate not advertised on force-failover
CSCeb71671	Routing	NHRP on multi-point GRE tunnel interface causes router crash
CSCeb73578	Routing	FIB Adjacencies take a long time for static ARP entries
CSCeb82273	Routing	OSPFv3:DR fail to flood Netork LSA after neighbor flapping
CSCec04496	Routing	High CPU utilization when ospfIfEntry.* objects are polled
CSCec07636	Routing	snmpwalk on ospfnbrrtrld does not display all switch1 interfaces
CSCec19811	Routing	PE ping to CE router failed due to wrong source IP address.
CSCec29953	Routing	retrans counter not getting cleared / continuous ospf neighbor flap
CSCec38322	Routing	CEF reloader holding up memory when toggling DCEF-CEF-DCEF
CSCec44556	Routing	RIP updates not sent over ATM subints
CSCec55418	Routing	router crash when trying ospf authen several times
CSCec66162	Routing	On 10Gig LC pkts are route cached on rel due to missing cef entries
CSCec72160	Routing	ospf fa suppression failed to set forwarding address to zero.
CSCec82144	Routing	NRT:Router crashed at ospf_set_rpf_nexthop_for_te_tunnel in AToM FRR
CSCec83353	Routing	type7 fw addr set to 0 if next hop address is on VA intf
CSCed12382	Routing	CONST2/IPV6: %IPV6FIB-3-ASSERT messages with traceback on reload
CSCed20042	Routing	IPv6 CEF crash when encountering a recursion loop
CSCed26217	Routing	Unnecessary ARP was sent on OSPF non broadcast network
CSCed29557	Routing	Static routes are not deleted when PEs VRF interface is shut
CSCed29745	Routing	OSPF: first dbd packet not sent when MASTERs initial seq no == 1
CSCed39619	Routing	No passive-interface virtual 0 not working
CSCed43873	Routing	MPLS TE CLNS LSPLISTER traceback mls cef max on head router
CSCed46620	Routing	Reducing reflexive timeout causes CPU to go 100% while ACL creation
CSCed52749	Routing	OSPF: route missing even though OSPF database still exists
CSCed53047	Routing	OSPFv3: indication-lsa from non-Cisco router is ignored
CSCed55180	Routing	ARP process takes too long to update after switchover
CSCed57077	Routing	Crash on displaying expired reflexive ACL entries
CSCed60800	Routing	Routing Table not updated when BGP next hop is withdrawn
CSCed62835	Routing	IPV6FIB-SP-4-RECURSION,CEF IPC STACKLOW msg followed by crash
CSCed62901	Routing	PE failed to switch from BGP route to OSPF route across Sham links

Identifier	Technology	Description
CSCed63692	Routing	input high ospf tag number = output negative value
CSCed70694	Routing	commands entered on ipv6 address family config mode gives error
CSCed70979	Routing	Bus error at db_install
CSCed72062	Routing	ABR does not flood Type3 LSA from MPLS TE Tunnel
CSCed82207	Routing	CEF inconsistenancy between RP SP
CSCed86534	Routing	EIGRP traceback in dual_restart_finish after switchover
CSCed90943	Routing	dual_process_acked_unicast crash and dual_packetize_interface trace
CSCed91798	Routing	DHCP not working when CEF enabled
CSCed96062	Routing	RP crash at mgd_timer-set_exptime_internal
CSCee02786	Routing	IPX EIGRP fails to set originating router id on startup
CSCee18136	Routing	Integrate CSCed63152 and CSCee14378 into common commit
CSCee21263	Routing	Fragments from return traffic are being dropped by reflexive ACL
CSCee23517	Routing	Inconsistent Fib tables between RP and LCs
CSCee25019	Routing	OSPFv3/modifying redistribute route-map on the fly wont take effect
CSCee28148	Routing	OSPF NSF: LSA not removed from ospf database after SSO switchover
CSCee30050	Routing	FIB-3-FIBDISABLE Fatal error, no window message, LC to RP IPC non-op
CSCee34076	Routing	CEF entry not removed even if route removed on SSO switchover
CSCee35125	Routing	RP crashed on rip_redist_check on clear ip route *
CSCee36622	Routing	Summary LSA stuck in database
CSCee36721	Routing	OSPF does not adv Net LSA when two interfaces have same address
CSCee39853	Routing	CEF getting disable on Standby PRE
CSCee49764	Routing	OSPF redistribute max prefix fails if applied after SSO switchover
CSCef00037	Routing	SSO:T/B DUAL-3-INTERNAL IP-EIGRP(0) internal error after S/W
CSCef00535	Routing	RP crash on validblock when neighbor did SSO switchover
CSCef26976	Routing	Removing one vrf messes up ospf config of other vrf
CSCin30562	Routing	a2a l2tp Et-Vl:dCEF fails in ingress dirn after rpr-plus switchover
CSCin72573	Routing	IP directed-broadcast does not work with CEF enabled
CSCin73487	Routing	BGP Conditional advertisement broken
CSCuk48314	Routing	CEF LC IPC Background - %SCHED-7-WATCH:Attempt to monitor uninit Q
CSCuk52062	Routing	RIB link failure after memory exhaustion
CSCdz84583	Security	IOS fw allowing forged packets for a session initiated from inside
CSCec35857	Security	PKI: crash when authenticating a sub CA after auth the root
CSCed35253	Security	Router crash due to corrupted data in list with IOS-firewall
CSCed69858	Security	show ssh command issued repeatedly may crash the system
CSCee34939	Security	Memory leak when SSH client closes connection after key exchange
CSCin74155	Security	SSHv2:router crashes under heavy load at tcb_isvalid
CSCdx91720	Unknown	12.1(12c):Qos:Request to support L4 port expansion in QM code

Identifier	Technology	Description
CSCdy23659	Unknown	Need a way to clear alarms from SFM display
CSCdy53121	Unknown	outbound v.110 calls fail if taking longer 10 seconds to connect
CSCdy62969	Unknown	ALIGN-3-SPURIOUS messages do not include traceback
CSCdy85215	Unknown	Incorrect busy tone played to FXS on call-disconnect
CSCdz14210	Unknown	TCP Intercept watch mode w/conn time pkts SW switched
CSCdz39541	Unknown	Crash when no internal vlan available for pchannel
CSCdz46544	Unknown	MAN: Xponder FPGA version return wrong info, when show hard detail
CSCdz46944	Unknown	MF: Vlan not added to routing table after reload
CSCdz49171	Unknown	Cat4000-Sup3 sends IGMP Leave with 0.0.0.0 source IP address
CSCdz56449	Unknown	MAN:low alarm/low warning not reported in 14e throttle image
CSCdz56613	Unknown	no shut on a layer 3 interface doesnt work sometimes
CSCdz69546	Unknown	4006 SupIII Reload on tcp_putbyte process
CSCdz71462	Unknown	cbQosPostPolicyByte had been incorrectly set to cbQosPrePolicyByte
CSCdz83820	Unknown	RPF unicast(No ACL) forwards both valid & forged pkts
CSCea05915	Unknown	dMFIB: for HW engine use stats instead of signal for liveness
CSCea08556	Unknown	MMLS: OIF inconsistency results in duplicated traffic.
CSCea50629	Unknown	c-hyb:spt-threshold with mmls causes duplicate packets to be egress
CSCea60918	Unknown	(*,g) not removed after (s,g) del results in blackholing traffic
CSCea66218	Unknown	PA-MC-STM1 - Alarmed VCs can bring other VCs down
CSCea69733	Unknown	SPD does not work on AS5300 ethernet
CSCea71016	Unknown	station-id [name
CSCea71130	Unknown	MMLS/CEF: inconsistent OIFs. Exist on SP but not on RP
CSCea80003	Unknown	IPSec HA RRI injected routes not deleted on hsrp state change
CSCea84998	Unknown	Memory leak in Crypto IKMP
CSCeb01318	Unknown	Switchport trunk allowed vlan list broken on span destination ports
CSCeb14435	Unknown	19E, 8bE14: Mcast shortcuts take long to install after become DMode
CSCeb58952	Unknown	FlexWAN II OC3 LLQ Profiling: latency and voice pkt loss issues
CSCeb64666	Unknown	SPURIOUS mem at isakmp_send send_nat_keepalive in nat
CSCec07456	Unknown	BOOT variable should not have a semi-colon at the end
CSCec09193	Unknown	HA: Fix data descriptor and IfIdx sync key fields/widths
CSCec12236	Unknown	19E:OIR of fabric capabale card on SUP1/SupW causes crash
CSCec32173	Unknown	VSEC:VPN-SM-C2: Traffic is lost if the tunnel mac address is changed
CSCec34010	Unknown	OSM2-GE 64 bit main interface counters stay 0
CSCec36878	Unknown	DEL:no traffic switched when OIF MTU smaller than IIF on EARL6
CSCec39132	Unknown	I/O memory corruption due to IGMP packet flood.
CSCec45398	Unknown	Align error on SP- Traceback: mcast_mld_accept_group
CSCec50884	Unknown	BGP Multipath failover takes very long time to cnvrge (500K)

Identifier	Technology	Description
CSCec52045	Unknown	Respond Life Notify should be processed after SA is authenticated
CSCec53057	Unknown	crypto_drop_packet causing traceback and memory corruption
CSCec53406	Unknown	ACL ODM give up
CSCec59622	Unknown	CE3-HYB:Vlan interface doesnt come up after resetting DR in SRM
CSCec60933	Unknown	ssl-proxy mod <mod-number> allowed-vlan doesnt add module to vlan
CSCec67980	Unknown	snmp-server packetsize 8192 crashes HA standby
CSCec70454	Unknown	RSPAN on SUP720 running IOS causes spanning tree loop.
CSCec72813	Unknown	Traceback at ipaccess_match_duplicate (CPUHOG)
CSCec73134	Unknown	show crypto ipsec sa cmd can crash when IPSec SAs get deleted
CSCec73525	Unknown	C-hyb: Mcast packets may get dropped if ACL TCAM is full
CSCec74016	Unknown	Const2:Router crash when ipv6 ACL removed after remove isataptunnel
CSCec76910	Unknown	C2SUP2/C2MCAST: BIT-SP-4-OUTOFRANGE, then watchdog crash in LTL MGR
CSCec80654	Unknown	Hardware shortcuts installed without RPF traffic
CSCec86976	Unknown	NATIVE: Extended ACL checks 7 bits for dscp not 6 for class-map
CSCec90162	Unknown	tracebacks seen after enabling gre keepalive
CSCed00394	Unknown	Directly connected mcast subnet are NOT programmed in the SP
CSCed05807	Unknown	NBAR stays active even if removed from config
CSCed06744	Unknown	software flood to fabric issues with cross-DFC etherchannels
CSCed11313	Unknown	Packet drop by applying output ACL on Tunnel interface
CSCed12070	Unknown	switchport configuration changed BW value in show int
CSCed12393	Unknown	CPU-HOG in PIM,MLSM & MWheel and multi-device WATCHDOG crash
CSCed17923	Unknown	Const2:no idprom for module after multiple SSO switchover
CSCed19974	Unknown	:SSO:IPv6 interface stat mismatch messages with SSO swover
CSCed22387	Unknown	Ibc input queue drops constantly incrementing on SP
CSCed22494	Unknown	VPNSM: fail to insert RRI route if dynamic cmap added on the fly
CSCed23477	Unknown	RRI: routes not removed as expected
CSCed29594	Unknown	6500 may not unicast flood packets to rp with fallback bridging
CSCed33380	Unknown	IPC failure with show mls netflow ip
CSCed33793	Unknown	Mcast uflow policer does not work on LAN for > certain rates
CSCed34259	Unknown	SUP720 shows System returned to power-on even after a reload
CSCed35745	Unknown	ARP from CSM to real servers not sent downstream after reload
CSCed35900	Unknown	:CWPA2 mpls QoS classification not working until re-add policy
CSCed36177	Unknown	Cat6000 : RP may crash at tunnel_ip_les_fastswitch
CSCed38413	Unknown	cosmos_e:In 6148-GE-TX qos, trust dscp & prec functionality reversed
CSCed38862	Unknown	g1/1 of WS-X6748-GE-TX not link up after changing speed 10M or 100M
CSCed38956	Unknown	Client Browsers see significant delay in retrieving content from ser
CSCed41095	Unknown	SRM needs enhancement to count for lose packets during config-sync

Identifier	Technology	Description
CSCed46278	Unknown	Const2:C2MCAST Standby sup is resetting continuously
CSCed48412	Unknown	L4 port intersection not happening in port expansion
CSCed48718	Unknown	DEC workaround and SPAN reflector to be mutually exclusive
CSCed49423	Unknown	Temp. values not updated in show environment temperature
CSCed49574	Unknown	12.2S: traffic loss if in/out PO bundled Active/Plus LC
CSCed50556	Unknown	memory leak in Crypto IKMP
CSCed52841	Unknown	In some circumstances, switch is not responding to SNMP requests
CSCed53595	Unknown	INTERNAL ERROR (../pas/atmphy_dsx3mib.c:1370) could not delete inter
CSCed55238	Unknown	MST : Vlans interface on MSFC down after switchover
CSCed55283	Unknown	Catalyst 6500 running IOS in L2PT core displays CEs as CDP neighbors
CSCed55342	Unknown	Jumbo frames fail across etherchannel routed on the same vlan
CSCed56658	Unknown	MSTP: no CAM flushing on boundary port when TCN rx
CSCed61632	Unknown	SUP720 may not ARP after SRM-SSO failover with bridging enabled
CSCed62337	Unknown	OSPF adjacencies fail to come up with Sup720, PFC3a and MPLS
CSCed63590	Unknown	GTP SLB doesnt work with GGSN R5.0 Call Admission Control function
CSCed63897	Unknown	shut/unshut edge port cause TC to be initiated
CSCed65372	Unknown	RP/SP software forced reloaded after removing switchport from FE int
CSCed65584	Unknown	Vip crashed when using switched PVC with mfr
CSCed66865	Unknown	SP crash at earl7_force_crash
CSCed67113	Unknown	OSM-1CHOC12/T1 displays T1 has receiver loss of signal on T1
CSCed69233	Unknown	alignment error in qm_get_card_info_for_police_action
CSCed73700	Unknown	Vlan Translation does not work on WS-X6816-GBIC
CSCed75240	Unknown	: OAL does not work if egress int is Gig Sub-intf
CSCed75689	Unknown	pm assert fail,console hang,stdby crash when toggle mls mpls tunnel-
CSCed75920	Unknown	When Glean Rate Limiter enabled Egress ACLs applied on Ingress Pkts
CSCed76200	Unknown	Un all command after (debug ip csg cpu) causes error from CSM
CSCed77033	Unknown	Rp crash on doing sh glbp interface
CSCed77519	Unknown	Sup720-3BXL:EoMPLS:VLAN_M dot1q tag handling for IPv6 pkt problem
CSCed77602	Unknown	:All ports in the etherchannel being bounced on SSO
CSCed78487	Unknown	EoMPLS: L2 traffic causes l2_lc_add_entry l2_rc(8) num_fails.
CSCed78815	Unknown	BT:Shaping with class-default does not work on ATM pvc
CSCed79251	Unknown	Unexplained ro=1: PBIF mem ECC1 P2N popping up on console
CSCed79519	Unknown	Breakpoint exception due to RPC mismatch timeout
CSCed79694	Unknown	C2SUP2: Multi-Link FR fails to forward.
CSCed79711	Unknown	:LTL_DEBUG_ASSERT: Failture on index + j
CSCed80869	Unknown	Pikespeak : mac limit per vlan feature crashed
CSCed81908	Unknown	BOC,DEL,12.2S: HighFabUtil cause Berytos HealthMonitor fail & reset

Identifier	Technology	Description
CSCed82263	Unknown	Fornax / Macedon in slot13 cant switch traffic with reflector enable
CSCed84042	Unknown	SLB-MIB reports 0.0.0.0 for named real servers
CSCed85276	Unknown	VPNSM does not correctly decapsulated nested IPsec traffic.
CSCed85411	Unknown	Rapid-PVST: Short loop forming when root moves
CSCed85509	Unknown	: CWPA Port based EoMPLS packets are corrupted and received
CSCed86486	Unknown	T1 controller errors on cronos card
CSCed88426	Unknown	Extended acl breaks on first switchover (Ctrl-C not synced to stdby)
CSCed90255	Unknown	configuring egress policy silently turns nbar on the inteface
CSCed92837	Unknown	Standby RSP hangs after switchover, never loads current image
CSCed93264	Unknown	RP truncates the TOS byte to upper 3 bits on IP with option field
CSCed93359	Unknown	Startup config synched to stdby,BOOT_STRING_INVALID message appears
CSCed93707	Unknown	VPN-SM:Different comb of DF bit, PMTUD settings in GRE must be corre
CSCed94258	Unknown	Traffic routed on L2 DEC stops when other L2 DEC becomes non DEC
CSCee04176	Unknown	Mac-address-limiting inconsistent between LAN & VPLS
CSCee05413	Unknown	Memory leak in EARL VLAN stats subblock
CSCee05653	Unknown	RPR+: Standby SP can not take over when Active SP fails
CSCee05683	Unknown	crash triggered by clear ip slb sticky radius calling-station-id
CSCee07395	Unknown	Const2:FIB Protocol Allocation mismatch
CSCee07996	Unknown	vacl capture (vlan filter) does not get applied to multilink IF
CSCee08015	Unknown	Fabric TIMEOUT error handling on the NMP.
CSCee09385	Unknown	Request to add support for VACLs on HSSI interfaces
CSCee10614	Unknown	DEV: FibTcamSSRAM test fails
CSCee10773	Unknown	mls ip multi bid gm-scan-interval 10 appears setting PIM-SM
CSCee11200	Unknown	All Firmware debug msgs should print slot# and time stamp
CSCee11672	Unknown	Some static mac entries missing in DFC after module reset
CSCee11910	Unknown	SUP720 standby rp temp sensors missing
CSCee14838	Unknown	Multicast macs added for every L3 destination with igmp snooping
CSCee15581	Unknown	sss_mgr with invalid index into 2 arrays causes crash/traceback
CSCee15798	Unknown	CEF entries not installed on LC/SP after SSO switchover
CSCee15895	Unknown	Sup720 experienced high-rate counter-up on sh int null0
CSCee17030	Unknown	Sporadic delay with multicast leave/joins on Spu 720
CSCee18977	Unknown	T3 PMON do not update/increment caused by atmphy_dsx3mib_init
CSCee19156	Unknown	6PE does not obey mpls ttl propagation command
CSCee21772	Unknown	port-channel dflt results wrong after bootup
CSCee22362	Unknown	Multicast src only detection needs to happen faster
CSCee22993	Unknown	Sup720: Diags detect error on standby Sup after SSO failover
CSCee23058	Unknown	Incorrect Netflow Byte Counts With Large Flows

Identifier	Technology	Description
CSCee23271	Unknown	ifType is incorrect for VLAN Interface
CSCee24424	Unknown	Netflow error checking code reports L3-PS-DRVR: No Req Blks msgs
CSCee28200	Unknown	Performance hit due to Netflow table hash
CSCee28215	Unknown	CLI to output actual pps performance
CSCee28288	Unknown	2 second delay in forwarding the 1st packet of mcast stream on 7600
CSCee30816	Unknown	TTL for decremented on the encap side when hardware switching
CSCee31719	Unknown	MVPN: Encap PE with FS does not send out packets on the MDT Tunnel
CSCee32151	Unknown	Crossbar MIB not working correctly
CSCee33023	Unknown	L2-Aging : l2_aging_do_rm_rma_aging, entry not found by STDBY in SSO
CSCee33136	Unknown	MPLS packets duplicated in SRP ring (OSM-DPT)
CSCee34416	Unknown	Supervisor may crash due to TestSPRPInbandPing
CSCee35193	Unknown	OSPF sessions are not coming up using pos linecards in the core
CSCee36959	Unknown	Software Forced Reload:get_rp_cpu_info
CSCee38860	Unknown	In online diag mode module reset due to TestMacNotification Failure
CSCee38898	Unknown	llq not working under child policy when Fr flat policy is configured
CSCee38924	Unknown	SP crash @ l2_throttle_debug_print
CSCee39170	Unknown	Incorrect mask value set in ACL TCAM when matching on DSCP values
CSCee39798	Unknown	dot1dBase info should be available without SPT enabled
CSCee40846	Unknown	egress multicast to slot 1 ports also goes to Sup slot
CSCee42278	Unknown	OSM-12CT3/T1 fails to boot up
CSCee43090	Unknown	RLB subscriber packets may loop due to incorrect flow-mask.
CSCee44248	Unknown	Redundant Sup fails to come online after switchover
CSCee45170	Unknown	RPVST: Loopguard blocking both sides of a link without recovery
CSCee45404	Unknown	HSRP does not forward traffic correctly after primary back up
CSCee48296	Unknown	Badevent operator_power_on seen on bootup sometimes
CSCee50911	Unknown	OSM/OC12-ds0:Router crash due to illegal input
CSCee51501	Unknown	Excessive SCP retries and drops while doing shut/no shut repeatedly
CSCee53705	Unknown	cwpa2: Turn on FIFO flow control and EOS driver changes
CSCee53706	Unknown	SSM mapping does not work correctly in presence of IGMPv3 receivers
CSCee53998	Unknown	SUP720: part of config incorrectly written to run-conf after reload
CSCee54526	Unknown	SP: const_mpls_ios_set_hw_taginfo taginfo do not own rew, but ctagre
CSCee54734	Unknown	Need to disable module if a real bad xenpak is plugged in.
CSCee56573	Unknown	L3 traff s/w switched after removing/adding port channel
CSCee59513	Unknown	Broken connectivity over OSM-ATM after VRF unconfig
CSCee59601	Unknown	Interface Input drops/flush counter increment at a high rate
CSCee60121	Unknown	SLB-MIB returns null/zero value when polling <real name xxxx>.
CSCee63221	Unknown	SP crash DIAG_PF_CONST2_TEST_HAS_FAILED

Identifier	Technology	Description
CSCee65953	Unknown	Incorrect Netflow Byte Counts With Large Flows
CSCee68052	Unknown	unsolicited igmp reports do not always reset host join timer
CSCee68381	Unknown	Packet drops on old rev WS-X6516-GBIC
CSCee69687	Unknown	UDP fragments dropped with the VACL configured on the SVI
CSCee75540	Unknown	ltl_ha_sync:Failed to get checkpoint buffer message on reset of stdb
CSCee77817	Unknown	CSM cannot communicate with servers in Private VLAN
CSCee77920	Unknown	CSM needs to FT switchover on the same chassis as HSRP failover
CSCee77961	Unknown	CSM cannot sync configs to the standby CSM system
CSCee80365	Unknown	1st hop router randomly fail to add (s,g) flows oif in HW fib table
CSCee83733	Unknown	L2 traffic/connectivity loss after spanning tree reconvergence.
CSCee85152	Unknown	CEF Hardware switching produces ping failure on every other packet a
CSCee87897	Unknown	CSM needs CLIs to configure failstate improvements
CSCee89232	Unknown	Configuring platform while in automore state crashes switch
CSCee89586	Unknown	VPN-SM:ICMP unreachable sent for pkt w/ iplen+ovhead eq mtu, DF set
CSCee90183	Unknown	Need to change RPC syslog in case of RPC request sent failure
CSCee92719	Unknown	Duplicates in NDE on the Sup720
CSCee95301	Unknown	Unhide and document mls rate-limit multicast non-rpf command
CSCef03723	Unknown	HA Coexistence:MPLS:VPN:VRFs not in sync between primary and standby
CSCef04696	Unknown	Cat6K crashed in pm_cp_vlan_stp_topology_process during HA tests
CSCef07965	Unknown	System crashed when accessing CVDM from the switch
CSCin41024	Unknown	c2sup2:CWPA:DMLFR:FR Relay entry (sh fr map) is taking lot of time
CSCin49358	Unknown	PA-MC-STM1:Serial intf down after rpr+ switchover w/ RSP16
CSCin67400	Unknown	FRF12: Checksum errors with POS, ping fails
CSCin67419	Unknown	A shut of any of the member link or cont traff brings down MFR intf
CSCin68355	Unknown	:Marking with microflow policer not working with layer2 port
CSCin71561	Unknown	Bandwidth of port-channel not sum of bw of individual interfaces
CSCin72202	Unknown	Auth-Proxy do not work with ODM merge algorithm
CSCin74123	Unknown	mst root id becomes 0 after switchover
CSCin74475	Unknown	Connectivity lost to MWAMs for reseting CSM/MWAM modules on switch
CSCin76766	Unknown	Active SP reloads at ipc_send_rpc_blocked failed after RPR+ swover
CSCin78380	Unknown	Issues with isolated private vlan
CSCuk49481	Unknown	GRE packets inot correctly processed (DF) on cat6500
CSCdt36219	Voice	Router returned to ROM by bus error at ccsip_spi_control_main
CSCea71767	Voice	cRTP doesnt work with PPP on 1750 router
CSCea84911	Voice	Gateway not initiating OLC sometimes in slow start call
CSCea85410	Voice	router crash with one T1 of ivr calls
CSCin41335	Voice	Clock goes to local oscillator instead of Priority clock source

Identifier	Technology	Description
CSCdz00624	WAN	After configure no ip cef router starting to drop packets
CSCea43177	WAN	FR-SVC: Router crashes on applying show frame-relay svc maplist
CSCea56560	WAN	Sw crash with NTP config and debug
CSCeb10672	WAN	GSR dual-PRP: standby getting reloaded due to rf timer expiration
CSCeb25177	WAN	SRP interface Fast-switches when it should DCEF switch
CSCec27867	WAN	PA-POS: Interface remains down/down when enabled with critical alarm
CSCed62698	WAN	CWPA: ATM: DSCP bits 4-6 set to zero
CSCed78803	WAN	Packets coming in a shutdown subinterface are forwarded by CEF
CSCin34959	WAN	RP fails to recognize bay 1 ATM PA after bay 0 was test crashed
CSCin47130	WAN	Flexwan support for using CSCdy30984 for rate counters
CSCin54713	WAN	CWAN SSO:CT3 Mailbox hogging CCB Block semaphore on bootup
CSCin68724	WAN	set atm-clp bit not set on outgoing packets but QoS stats increment
CSCin76078	WAN	ATM(Deluxe & IMA) driver code for Flexwan to prefer priority packets

Caveats in Release 12.2(17d)SXB and Rebuilds

Note Release 12.2(17d)SXB1 and later releases do not support XENPAK-10GB-ER units with Part No. 800-24557-01, as described in this external field notice (CSCee47030):

http://www.cisco.com/en/US/ts/fn/200/fn29736.html

Open Caveats in Release 12.2(17d)SXB11a

Identifier	Technology	Description
CSCee30050	Routing	FIB-3-FIBDISABLE Fatal error, no window message, LC to RP IPC non-op

Resolved Caveats in Release 12.2(17d)SXB11a

Resolved Routing Caveats

- CSCec71950—Resolved in 12.2(17d)SXB11a

  Cisco routers and switches running Cisco IOS or Cisco IOS XR software may be vulnerable to a remotely exploitable crafted IP option Denial of Service (DoS) attack. Exploitation of the vulnerability may potentially allow for arbitrary code execution. The vulnerability may be exploited after processing an Internet Control Message Protocol (ICMP) packet, Protocol Independent Multicast version 2 (PIMv2) packet, Pragmatic General Multicast (PGM) packet, or URL Rendezvous Directory (URD) packet containing a specific crafted IP option in the packet's IP header. No other IP protocols are affected by this issue.

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

  There are workarounds available to mitigate the effects of the vulnerability.

This vulnerability was discovered during internal testing.

This advisory is available at:

http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-crafted-ip-option.html

Other Resolved Caveats in Release 12.2(17d)SXB11a

Identifier	Technology	Description
CSCej21698	Unknown	EARL_L2_ASIC- SRCH_ENG_FAIL/ SCHED-DFC9-3-STILLWATCHING
CSCsb98702	Unknown	Breakpoint (signal 5 exception) when ltl profiling .
CSCsd50224	Unknown	FW: C2 fabric firmware improvements for Tetons3
CSCsd50881	Unknown	New fabric error recovery for 17SXB

Resolved Caveats in Release 12.2(17d)SXB11

Resolved AAA Caveats

- CSCed09685—Resolved in 12.2(17d)SXB11

  Symptoms: When command accounting is enabled, Cisco IOS routers will send the full text of each command to the ACS server. Though this information is sent to the server encrypted, the server will decrypt the packet and log these commands to the logfile in plain text. Thus sensitive information like passwords will be visible in the server's log files.

  Conditions: This problem happens only with command accounting enabled.

  Workaround: Disable command accounting.

Other Resolved Caveats in Release 12.2(17d)SXB11

Identifier	Technology	Description
CSCef87392	Unknown	Giants incorrectly counted on trunk with 67xx modules
CSCej52641	Unknown	LCP_FW_ERR: 67xx linecards reset due to packet buffer P2N EEC1 error
CSCsb90602	Unknown	After adding and removing SVI interfaces OSPF wont come up
CSCsc31677	Unknown	Enh: CLI to remove show inventory from show tech output

Resolved Caveats in Release 12.2(17d)SXB10

Identifier	Technology	Description
CSCee56573	Unknown	L3 traff s/w switched after removing/adding port channel
CSCeg29451	Unknown	standby and DFC in standby slot resets when doing write mem
CSCei76358	Unknown	cleanup of user interface data

Resolved Caveats in Release 12.2(17d)SXB9

Identifier	Technology	Description
CSCeg09691	AAA	dot1x EAP authentication not working with per-server radius key
CSCeb71693	Infrastructure	12.2S: issues with logging snmp-authfail command
CSCsa82886	Infrastructure	RP crashes when argument for tftp-server command longer than 67 char
CSCds33629	IPServices	Closing Telnet session crashes router..
CSCsa85588	MPLS	Per VRF Aggregate Label not in lfib
CSCeg28814	Multicast	Duplicated mcast packet due to wrong FPOE in egress replication mode
CSCeg83460	Multicast	c6msfc:bidir pim df not elected with multiple RPs after link down
CSCeh95160	Multicast	bi-directional PIM DF winner may receive an incorrect unicast metric
CSCsb01188	QoS	ATM interface on FW/FW2 PA stops tx on add/remove service policy
CSCeh13489	Routing	BGP shouldn't propogate an update w excessive AS Path > 255
CSCsa78259	Routing	IOS reload due to specific BGP routing update
CSCed93264	Unknown	RP truncates the TOS byte to upper 3 bits on IP with option field
CSCee37771	Unknown	67xx: Rommon Upgrade Failure
CSCee40846	Unknown	egress multicast to slot 1 ports also goes to Sup slot
CSCef32513	Unknown	SPAN destination ports causing latency on adjacent Pinnacle ports
CSCef33051	Unknown	Part of the traffic blackholed when new link joins etherchannel
CSCef40249	Unknown	power inline command appears even after removed and reloaded system
CSCef47414	Unknown	VTP code fail to restore vlan database properly
CSCef66632	Unknown	Demand Aging clearing entries every 4 seconds, without contention
CSCef88685	Unknown	mcast ltl cleared out on WS-X6816-GBIC after NSF/SSO failover
CSCeg39091	Unknown	Abnormally long flooding with L2 DFC DEC
CSCeg48547	Unknown	fm_netflow_earl6.c: early return results in memory leak
CSCeh40945	Unknown	Same MAC addreees are learnt by different VLAN
CSCeh53682	Unknown	MACs Learned on EtherChannel across L2 Fwding Engine Get Off-sync
CSCeh54386	Unknown	Ucast flooding due to MACs losing PI_E flag when SPAN is configured
CSCeh54533	Unknown	IOS SLB with Egress ACL under SVI breaks L2 icmp traffic
CSCeh56398	Unknown	T48+, G+-CR2 in C+/Legacy configuration boot with multiple errors
CSCeh59654	Unknown	Ucast flooding due to +MN received on DFC/PFC when DEC is configured
CSCeh62522	Unknown	igmp snooping source only doesnt work for certain range of group ad
CSCeh73049	Unknown	tclsh mode bypasses aaa command authorization check
CSCeh73110	Unknown	Ucast flooding due to +MN/-MN race condition
CSCei18018	Unknown	Diagnostics HM crash
CSCin72202	Unknown	Auth-Proxy do not work with ODM merge algorithm
CSCin78324	Unknown	PA-MC-8TE1+: check to drop runts packets missing in driver code
CSCsa49748	Unknown	sup720 reloads by software forced crash

Identifier	Technology	Description
CSCsa57081	Unknown	sup720 : static multicast CAM entry is not programmed after reload
CSCsa63184	Unknown	Crash TestSPRPInbandPing fail after MLS global enable with Dist. Etherch
CSCsa65200	Unknown	Transmit power is output from admindown IF after system restart
CSCsa70835	Unknown	SUp720 may see random packet loss when host leaves or joins; OIF +- 85
CSCsa76812	Unknown	ICC gets stuck after reload if RM agiing is configured to no_aging
CSCsa80358	Unknown	Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks
CSCsa96704	Unknown	MSFC3: Bus error while issuing the show mls netflow creation command
CSCsb04346	Unknown	crash l2_aging_proc after changing Spantree mode
CSCsb10662	Unknown	PI_E lost on Supervisror after +MN received on DEC with Plus
CSCsb16051	Unknown	traffic should not flood to all LC in L3 distrinuted port-channel
CSCsb16396	Unknown	Unicast flooding with Shut on one of the DEC members
CSCsb18038	Unknown	GE-WAN show interface in/out rate is always zero
CSCsb32028	Unknown	%CPU_MONITOR-2-NOT_RUNNING: CPU_MONITOR tracebacks and crash
CSCsb38273	Unknown	L3 Traffic flood over DEC due to incorrect Flood region FPOE
CSCdx86562	WAN	A interface of ntp source is changed by creating a interface

Resolved Caveats in Release 12.2(17d)SXB8

Resolved LAN Caveats

- CSCsa67294—Resolved in 12.2(17d)SXB8

  Symptom: A Cisco Catalyst Switch may reload upon receipt of a malformed VTP packet.

  Conditions: The malformed VTP packet must meet the following requirements:

  - Must be received on a port configured for ISL or 802.1q trunking AND
  - Must correctly match the VTP domain name

  This does not affect switch ports configured for the voice vlan.

  Affected platforms:

  - Cisco 2900XL Series
  - Cisco 2900XL LRE Series
  - Cisco 2940 Series
  - Cisco 2950 Series
  - Cisco 2950-LRE Series
  - Cisco 2955 Series
  - Cisco 3500XL Series
  - Cisco IGESM

  No other Cisco devices are known to be vulnerable to this issue.

  Workarounds: Customers may want to connect ports configured for trunking to known, trusted devices.

Other Resolved Caveats in Release 12.2(17d)SXB8

Identifier	Technology	Description
CSCeg19038	Infrastructure	The entCacheFlag should not be shared with several entity tables.
CSCeg64124	Infrastructure	SAA not sending packets to line after a period of time
CSCea25073	IPServices	IOS FTP client code rewrite
CSCec50485	IPServices	copy ftp flash fails with 3COM ftpserver
CSCef60452	Multicast	possible blackout when receiving Join on RPF interface (iif)
CSCee45508	platform-76xx	OSM CHOC-OC12 freezes up while proccessing PPP keepalives
CSCef19811	platform-76xx	MPLS:VPN:MLPPP:PE not receiving packets from connected CE
CSCeg77503	platform-76xx	SAA Packets do not hit the outbound service policer
CSCdv76375	Routing	OSPF neighbor command unsupported in VPN routing instance
CSCee16068	Routing	Equal cost default route remains in RT after changing interface cost
CSCef67660	Security	sshv2 malform client ignore msg cause demage to router
CSCeh18999	Security	Second CRL is not checked with VPNSM
CSCsa67272	Security	Serial number in certificate subject is incorrect
CSCsa78580	Security	Crypto IKMP process can get blocked if router fails to fetch CRL
CSCsa81928	Security	CRL checking fails if PKI URI recevied for CDP is UPPER CASE
CSCed36177	Unknown	Cat6000 : RP may crash at tunnel_ip_les_fastswitch
CSCef36367	Unknown	MMLS: High CPU after Sparse->Bidir transition
CSCef76161	Unknown	ifInDiscards are resetting,causing counter problems
CSCef80423	Unknown	Sup3: watchdog fired incorrectly when reload/incorrect bootup cause
CSCef81281	Unknown	The value of cbQosPoliceConformedByte64 provided by SNMP decrease
CSCeg08562	Unknown	%IPC-3-NOBUFF: The main IPC message header cache is empty
CSCeg19103	Unknown	ALIGN-3-TRACEX : Error with debug netdr turned on
CSCeg41623	Unknown	CSM:Only configured vlans should be allowed on trunk
CSCeg55846	Unknown	MSFC3 HYB: msfc3 hybrid IOS does not implement some EMT calls
CSCeg62365	Unknown	rxHCDropEvents incrementing on 6704-10GE interface
CSCeg70376	Unknown	Sup720 : Ingress VSPAN is not working for VoIP VLAN
CSCeh05310	Unknown	ATM OSM MPB: One PVC failed to TX PKT if the LC in slot/port 1/7 of 7613
CSCeh08451	Unknown	Excessive Overruns and lbusDrops due heavy flow control over fabric
CSCeh11253	Unknown	dir /recursive all-filesystems causes supervisor to crash
CSCeh21723	Unknown	K+NAM:span monitor session stops forward traffic to NAM after SSO
CSCeh29617	Unknown	PP:Sup3:FRoMPLS:CHOC:pkts dropped on egr (PE-CE)link (ping fails)
CSCeh51906	Unknown	All hybrid image for Sup720 wont be able to config with STI NVRAM
CSCeh59181	Unknown	Fabric buffer reserve command does not work
CSCsa69590	Unknown	Teton3: after s/w, PWAN2 inferface becomes UP for nonconnection port

Resolved Caveats in Release 12.2(17d)SXB7

Resolved Routing Caveats

- CSCef68324—Resolved in 12.2(17d)SXB7

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack from a specifically crafted IPv6 packet. The packet must be sent from a local network segment. Only devices that have been explicitly configured to process IPv6 traffic are affected. Upon successful exploitation, the device may reload or be open to further exploitation.

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

  More details can be found in the security advisory that is posted at:

  http://www.cisco.com/en/US/products/csa/cisco-sa-20050729-ipv6.html

- CSCef61610—Resolved in 12.2(17d)SXB7

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

- CSCef60659—Resolved in 12.2(17d)SXB7

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks

3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

- CSCef67682—Resolved in 12.2(17d)SXB7

  Reception of certain IPv6 fragments with carefully crafted illegal contents may cause a router running Cisco IOS to reload if it has IPv6 configured. This applies to all versions of Cisco IOS that include support for IPv6.

  The system may be protected by installing appropriate access lists to filter all IPv6 fragments destined for the system. For example:

```
interface Ethernet0/0
  ipv6 traffic-filter nofragments in
!
ipv6 access-list nofragments
  deny ipv6 any <my address1> undetermined-transport
  deny ipv6 any <my address2> fragments
  permit ipv6 any any
```

  This must be applied across all interfaces, and must be applied to all IPv6 addresses which the system recognises as its own.

  This will effectively disable reassembly of all IPv6 fragments. Some networks may rely on IPv6 fragmentation, so careful consideration should be given before applying this workaround.

  We would recommend for customers to upgrade to the fixed IOS release. All IOS releases listed in IPv6 Routing Header Vulnerability Advisory at http://www.cisco.com/en/US/products/csa/cisco-sa-20070124-IOS-IPv6.html contain fixes for this issue.

Resolved Unknown Caveats

- CSCef44225—Resolved in 12.2(17d)SXB7

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Other Resolved Caveats in Release 12.2(17d)SXB7

Identifier	Technology	Description
CSCee26700	MPLS	memory leak caused by LSR MIB queries
CSCef37186	MPLS	cpuhog/watchdog-crash on mplsXCIndexNext mib query
CSCeb51147	Multicast	Stack overflow due to inf. rec in dual-RP/E4+ mic rel
CSCeg03144	platform-76xx	%EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR on Sup720
CSCsa47099	platform-76xx	IPX broke on wan link of OSM-2OC12-ATM
CSCsa53708	platform-76xx	OSM crashes under stress when having to pad packets
CSCee72906	PPP	dLFIoLL mlp-qos:VIP crash when bundle is reset while traffic is ON
CSCeg57219	PPP	Unable to ping packets greater than 1022 across MLPPP after sup SW
CSCed51640	QoS	dWFQ isnt diplayed in sh run anymore, so is lost after reload
CSCeb40561	Routing	[SNMP] GGSN reloads during get next operation
CSCed63876	Routing	BGP: router crashes pointing to ed_decay_penalty
CSCef93215	Routing	router crash at ospf_build_one_paced_update
CSCeg08344	Routing	with cef/dcef enabled & compression on, tcp frames getting dropped
CSCeg19442	Routing	crash on pdb_ospf_hello_BLOCK
CSCsa59600	Routing	IPSec PMTUD not working [after CSCef44225]
CSCdv68743	Unknown	Inefficient code in qos/qoscli_match_packet.c:match_named_acl().
CSCed12393	Unknown	CPU-HOG in PIM,MLSM & MWheel and multi-device WATCHDOG crash
CSCee10005	Unknown	Cat6500 service module connectivity issue with crossmodule etherchan
CSCee30816	Unknown	TTL for decremented on the encap side when hardware switching
CSCee68381	Unknown	Packet drops on old rev WS-X6516-GBIC
CSCee86168	Unknown	active SP resets, sr7100 errata 11
CSCef58590	Unknown	Disable VTT major temp shutdown and change thresh 100/85 -> 115/100
CSCef82367	Unknown	IP traff not frwded on G+CR2 port if toggled between routed/switched
CSCeg10174	Unknown	High CPU in QoS Mgr when changing long QoS access-list
CSCeg49196	Unknown	Excessive Overruns and lbusDrops due heavy flow control over fabric
CSCeg51793	Unknown	MVPN: Address Error Exception after config change w/ Mvpn
CSCeg52280	Unknown	CRCs caused by WS-X6704-10GE
CSCeg55565	Unknown	MMLS/MVPN: crash at mls_earl_show_scmdb -> chunk_lock
CSCeg56052	Unknown	Active and Standby SP crash due to GC Entry memoryleak
CSCeg65640	Unknown	Cat6000 with UDP turbo flood results in corrupted outgoing packets

Identifier	Technology	Description
CSCeh11095	Unknown	SUP720 not forwarding packets for certain prefix
CSCin87976	Unknown	Need to rate-limit EOS Error interrupts
CSCsa47020	Unknown	Sup720/FlexWAN: FRF.16 drops 64 byte packets above 2Mb
CSCsa51770	Unknown	Configuration of RSPAN on 12.2(18)SXD3 causes high CPU
CSCsa57079	Unknown	C7600 PE does NOT send BPDU including dot1Q tag on EoMPLS
CSCsa59260	Unknown	C7600 EoMPLS PE correctly does NOT send the COS value of BPDU
CSCin76078	WAN	ATM(Deluxe & IMA) driver code for Flexwan to prefer priority packets

Resolved Caveats in Release 12.2(17d)SXB6

Identifier	Technology	Description
CSCee49862	Access	PA-MC-2T3+ does not adhere to ANSI T1.231 standard
CSCee70591	Access	PA-2T3+ does not adhere to the ANSI T1.231 standard
CSCec63011	Infrastructure	Standby crashes in redundant systems
CSCeb40653	MPLS	Bus error crash at vrf_interface_print when deleting vrf config
CSCee37430	MPLS	Missing LFIB tag rewrite on LC after loss of /32 entry to its next-hop
CSCef12304	platform-76xx	PWAN2:Connectivity is broken between GE-WAN if one end shut/no shut
CSCef74227	platform-76xx	LAN GE of OSM incorrectly increments giants on dot1q trunk port
CSCef76828	platform-76xx	connectivity broken after config/unconfig tunnel interfaces
CSCeg10236	platform-76xx	PWAN2:GBIC type shown as not connected in show int
CSCeg47780	platform-76xx	RFC1483 Bridging broken on BT
CSCee22810	QoS	Router stops sending LMI with QOS configured
CSCee24349	QoS	Crash at fib_post_download_processing when reloading
CSCef06034	QoS	Sup720 crashes after SSO Failover with nbar configured
CSCef66517	QoS	packet drop on flexwan when traffic shaping
CSCeg49010	QoS	ISIS updates not sent when output qos police is set
CSCeb53542	Routing	Inconsistency between CEF adjacency and ARP tables; unicast pkt loss
CSCed26217	Routing	Unnecessary ARP was sent on OSPF non broadcast network
CSCed63342	Routing	RIP-Unicast updates not sent to configured RIP neighbors
CSCee59315	Routing	MPLS-VPN:Corrupted BGP table showing stale and/or poisoned paths
CSCeg26378	Routing	Dest CEF entry is missing in DCEF table. All pkts are punted to RP.
CSCee88654	Security	IOS requests an extra prompt for SSH key generation
CSCef61978	Security	SSHv2 session hangs with large command output until key press
CSCed25505	Unknown	reset of csm causes one of WS-X6248A-TEL to reset in a chassis
CSCed73700	Unknown	Vlan Translation does not work on WS-X6816-GBIC
CSCed82736	Unknown	SYS-2-GETBUF: Bad getbuffer, bytes= 65535
CSCee85152	Unknown	CEF Hardware switching produces ping failure on every other packet a

Identifier	Technology	Description
CSCee95708	Unknown	MSFC2-3-TOOBIG on sup720 in MPLS/VPN environment
CSCef27359	Unknown	SW and HW cef adjacency inconsistency
CSCef35707	Unknown	L2 Forwarding Table ECC error handler not working properly
CSCef45495	Unknown	PIM Snooping: (s,g,r) prune handling cases
CSCef49330	Unknown	APS not working on the PA-MC-STM1
CSCef58323	Unknown	%EARLY-L2_ASIC-DFC-SRCH_ENG_FAIL T/B on Berytos with L2(10k mac)Traf
CSCef71913	Unknown	MVPN: 3 minutes duplication in Data-MDT (by SSM) redundancy
CSCef72013	Unknown	unicast flooding due to purging of some mac-addres entry with dfc3/pfc3
CSCef79592	Unknown	Class-default shows packets output 0; packet drops 0
CSCeg01297	Unknown	System crash caused by pkt of incorrect length/IP header checksum
CSCeg03423	Unknown	show int trans does not show ITU channel info for DWDM Xenpaks
CSCeg06698	Unknown	COS rewritten for routed multicast traffic
CSCeg08389	Unknown	Interface counters do not increment on a Virtual MFR interface
CSCeg09655	Unknown	VPN-SM: Error in GRE check
CSCeg11415	Unknown	PWAN2:Strange behaviour of the QoS in the module
CSCeg15012	Unknown	SP crash with bus error while processing multicast packet
CSCeg16684	Unknown	Some VPLS VCs fail to pass traffic after a link failure in the core
CSCeg19269	Unknown	gt 12L4 Oper in acl dest port doesnt expand corectly;pkts non-qos fw
CSCeg24287	Unknown	LDP does not recover after link failure between two NPEs in a networ
CSCeg24675	Unknown	cannot modify class-map in PQ when plicy is applied to OSM
CSCeg30437	Unknown	VPLS:ATOM:CWAN: Some VCs remain down, LFIB/TTFIB are ok
CSCeg38482	Unknown	MVPN one PE can not receive auto-RP information for one vrf
CSCeg40177	Unknown	Tag to Ip path has all zero src and dest mac
CSCeg40543	Unknown	some vcs do not pass traffic after supervisor switchover
CSCin65698	Unknown	%INTERFACE_API-3-NODESTROYSUBBLOCK msg on reconfiguring Potent PA
CSCin83972	Unknown	Dot1x Scalability issue - Port from Tetons-2
CSCin84750	Unknown	IP address in ACE ignored while doing l4op expansion
CSCdz67208	WAN	CWPA: Pkts generated on this router are not getting matched
CSCef93103	WAN	bridge-vlan on Flexwan PVC floods BPDUs

Resolved Caveats in Release 12.2(17d)SXB5

Resolved Routing Caveats

- CSCee67450—Resolved in 12.2(17d)SXB5

  A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command bgp log-neighbor-changes configured are vulnerable. The BGP protocol is not enabled by default, and

must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

Cisco has made free software available to address this problem.

This issue is tracked by CERT/CC VU#689326.

This advisory will be posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050126-bgp.html

Resolved Unknown Caveats

- CSCef90002—Resolved in 12.2(17d)SXB5

  Cisco Catalyst 6500 series systems that are running certain versions of Cisco Internetwork Operating System (IOS) are vulnerable to an attack from a Multi Protocol Label Switching (MPLS) packet. Only the systems that are running in Hybrid Mode (Catalyst OS (CatOS) software on the Supervisor Engine and IOS Software on the Multilayer Switch Feature Card (MSFC)) or running with Cisco IOS Software Modularity are affected.

  MPLS packets can only be sent from the local network segment.

  A Cisco Security Advisory for this vulnerability is posted at

  http://www.cisco.com/en/US/products/csa/cisco-sa-20070228-mpls.html

- CSCin82407—Resolved in 12.2(17d)SXB5

  Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

  Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

  This advisory will be posted to
  http://www.cisco.com/en/US/products/csa/cisco-sa-20050406-xauth.html

Other Resolved Caveats in Release 12.2(17d)SXB5

Identifier	Technology	Description
CSCeg11566	Infrastructure	SNMP May Consume all the I/O Memory
CSCef46191	IPServices	Unable to telnet
CSCea83675	MPLS	Enhance VRF protection while displaying VRFs
CSCed57281	MPLS	CPU hog in CEF reloader while adding a vrf interface
CSCed81317	MPLS	can not see bgp routes from CE after import map
CSCef14446	MPLS	mpls vpn: recirculation vlan for agg label is not mapped to vpn
CSCee72817	platform-76xx	BGP neighbor relationship flaps periodically between PEs and RRs
CSCef35398	platform-76xx	OSM-2OC12-ATM-SI+ - SRIC IPM parity error
CSCea64725	Routing	BGP does not send all updates to recently established peer-group mem
CSCec29953	Routing	retrans counter not getting cleared / continuous ospf neighbor flap
CSCee35125	Routing	RP crashed on rip_redist_check on clear ip route *
CSCec67602	Security	ssh: tb in process_watch_timer when sending big ssh packets
CSCdx91720	Unknown	12.1(12c):Qos:Request to support L4 port expansion in QM code

Identifier	Technology	Description
CSCed00394	Unknown	Directly connected mcast subnet are NOT programmed in the SP
CSCed35900	Unknown	:CWPA2 mpls QoS classification not working until re-add policy
CSCed52841	Unknown	In some circumstances, switch is not responding to SNMP requests
CSCed66865	Unknown	SP crash at earl7_force_crash
CSCee07395	Unknown	Const2:FIB Protocol Allocation mismatch
CSCee11672	Unknown	Some static mac entries missing in DFC after module reset
CSCee23058	Unknown	Incorrect Netflow Byte Counts With Large Flows
CSCee34416	Unknown	Supervisor may crash due to TestSPRPInbandPing
CSCee63221	Unknown	SP crash DIAG_PF_CONST2_TEST_HAS_FAILED
CSCee65953	Unknown	Incorrect Netflow Byte Counts With Large Flows
CSCee75620	Unknown	RP crashes after enable CBAC
CSCee77136	Unknown	sup720: SPAN dest port should not be shown as notconnected
CSCee78323	Unknown	Duplicate packets in ingress SPAN/RSPAN with 6516A or 6548-GE-TX
CSCef05282	Unknown	Removing IP address, IP route cache cef still allows pkts to switch.
CSCef13797	Unknown	TCAM Capacity Exceeded with ACL on POS Interface
CSCef30308	Unknown	all zero source and dest mac address in show mls adj entry det
CSCef37026	Unknown	Running configuration is not synching between DR and NDR on MSFC3
CSCef41228	Unknown	SSO failover causes WS-X6816-GBIC reset
CSCef47466	Unknown	High latency and packet drop when any interface goes down on OSM
CSCef53290	Unknown	Using config mls ip ids causes switch to reload unexpectedly
CSCef58932	Unknown	VACL filter out STP BPDU
CSCef63549	Unknown	Multicast MET management fix and increase OIF above 1023 per flow
CSCef65827	Unknown	GRE o/v IPSec with VPNSM intermittently loses connectivity
CSCef67810	Unknown	get-bulk for portGrp causes cpu spike and delayed response
CSCef70298	Unknown	IFindex missing IDBs after deleting and adding T1 channels
CSCef72205	Unknown	vlan stops forwarding
CSCef73076	Unknown	ALIGN-SP-3-CORRECT seen in mcast_igmp_handle_igmp_pak
CSCef75501	Unknown	dot1x authentication not work perfectly in sup720.
CSCef75924	Unknown	packet drop for L3 trafic over dist. etherchannel with SPAN enabled
CSCef78235	Unknown	Disable egress span of vacl redirected packets
CSCef82797	Unknown	Distributed EtherChannel may caused packet loss
CSCef89139	Unknown	Adjacency pointers not Updated when 2nd Link Removed on 7600
CSCef91572	Unknown	Software forced crash at process pm_mp_notify_cp_port_admin_state
CSCeg01510	Unknown	Device crashes when we configure no vlan <vlan nu>
CSCeg03808	Unknown	Tetons: I/O Memory is getting depleted, IPC queue exhausted
CSCin79961	Unknown	Errdisable recovery not working with UFP.
CSCin82741	Unknown	PBR does not work if both PBR & SLB are applied on same interface

Identifier	Technology	Description
CSCuk49481	Unknown	GRE packets inot correctly processed (DF) on cat6500
CSCef91994	WAN	FLEXWAN - PA-A3 - packet drop when ping 1500bytes with MPLS

Resolved Caveats in Release 12.2(17d)SXB4

Resolved IPServices Caveats

- CSCed78149—Resolved in 12.2(17d)SXB4

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Dont' Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050412-icmp.html

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected.

Other Resolved Caveats in Release 12.2(17d)SXB4

Identifier	Technology	Description
CSCee43166	Routing	BGP: reduce CPU load for processing inbound VPNv4 updates
CSCef14934	Unknown	link up/down message is abnormal
CSCef48695	Unknown	UDLR:UDE: mis-config unidirectional mode causes tx counters to stick
CSCef55147	Unknown	DOM: global dom cli is broken, show int trans, returns null.
CSCin78110	Unknown	Some E1 controller does not come up if a large config on other LC

Resolved Caveats in Release 12.2(17d)SXB3

Identifier	Technology	Description
CSCef01725	Infrastructure	pak_realign driving up CPU usage
CSCeb61377	platform-76xx	CWTLC fabric related alignment correction
CSCec49042	QoS	IPP not being trusted using nbar type class map
CSCdt38401	Routing	Frame-relay packets processed by cpu due to CEF inconsistency
CSCdy33703	Unknown	Need span support for port 1/4 & 1/3
CSCed69233	Unknown	alignment error in qm_get_card_info_for_police_action
CSCee42657	Unknown	sup720 crashing after reload with large configuration
CSCee55233	Unknown	Large L3 port-channel config with stats collection caused high CPU
CSCee68052	Unknown	unsolicited igmp reports do not always reset host join timer
CSCee83655	Unknown	CPU_MONITOR-2-NOT_RUNNING_TB: CPU_MONITOR tracebackrate_limit_loop
CSCee89586	Unknown	VPN-SM:ICMP unreachable sent for pkt w/ iplen+ovhead eq mtu, DF set
CSCef07017	Unknown	VACL is not working for RSPAN traffic with mcast enabled
CSCef14106	Unknown	IDSM2 stops detecting attack after 2nd failover
CSCef21575	Unknown	Sup720 - ACL Incorrectly Denies Packets in HW
CSCef23843	Unknown	Module reset in getting CBL info
CSCef25710	Unknown	EOS error handling changes
CSCef26512	Unknown	WS-X6582-2PA :Unable to read cwan<slot>/0-disk0:
CSCin77443	Unknown	HYB:HA:Slave crashes on configuring Virtual-Template interface

Resolved Caveats in Release 12.2(17d)SXB2

Identifier	Technology	Description
CSCed92290	Content	CE4-NATIVE:wccp redirect issue after reloading the switch
CSCdz27562	Infrastructure	snmpwalk on loopback interface gets response from physical int. IP.
CSCea81029	IPServices	show ip igmp int crashed router
CSCec13278	IPServices	IGMP: IGMP_clear_cache() invoked crashed LC when LC OIRed
CSCec84887	IPServices	Sup720: Disabled STP for VLAN-bridge becomes to enable by shutdown
CSCec25430	Management	IOS may reload from specific packet
CSCdx80484	MPLS	C10720: Removing LDP before EoMPLS may cause a crash
CSCeb78347	MPLS	Cannot create a VRF
CSCea59359	Multicast	PIM stops sending Data-header Register packets
CSCeb57662	Multicast	Static mroute configuration does not take effect
CSCec40377	Multicast	Multicast router may stop sending PIM join msgs if low on I/O memory
CSCee88700	Multicast	TCAM entry not built for secondary subnet with multicast stub
CSCee89438	Multicast	MSDP doesnt build S,G state after rxing *,G join

Identifier	Technology	Description
CSCec62800	platform-76xx	20E:CWAN-QOS:Increased PQ latency when increasing default queue traf
CSCee01868	platform-76xx	OSM-2+4GE-WAN+:Interface UP/UP with GBIC installed but not connected
CSCee54642	platform-76xx	OSM local bus out of SYNC after stress
CSCee55056	platform-76xx	OSM interface byte counts are inaccurate
CSCee59667	platform-76xx	GE-WAN+ MTU config inconsistent with other IOS devices
CSCee84887	platform-76xx	OSM interface byte counters broken with high pps + large route table
CSCec15517	QoS	RSP crash Unexpected exception, CPU signal 10
CSCee31618	QoS	C2SUP2/FW2/CT3+:Voice packet drops at low rates with cRTP+LLQ conf
CSCin52060	QoS	After the policy got rejected hqf was not cleaned on vip
CSCea35186	Routing	OSPF: DR not generating network LSA
CSCed60800	Routing	Routing Table not updated when BGP next hop is withdrawn
CSCee36721	Routing	OSPF does not adv Net LSA when two interfaces have same address
CSCeb58952	Unknown	FlexWAN II OC3 LLQ Profiling: latency and voice pkt loss issues
CSCec50884	Unknown	BGP Multipath failover takes very long time to cnvrge (500K)
CSCed38956	Unknown	Client Browsers see significant delay in retrieving content from ser
CSCed77602	Unknown	:All ports in the etherchannel being bounced on SSO
CSCed85411	Unknown	Rapid-PVST: Short loop forming when root moves
CSCee04176	Unknown	Mac-address-limiting inconsistent between LAN & VPLS
CSCee05653	Unknown	RPR+: Standby SP can not take over when Active SP fails
CSCee51501	Unknown	Excessive SCP retries and drops while doing shut/no shut repeatedly
CSCee53705	Unknown	cwpa2: Turn on FIFO flow control and EOS driver changes
CSCee54526	Unknown	SP: const_mpls_ios_set_hw_taginfo taginfo do not own rew, but ctagre
CSCee69687	Unknown	UDP fragments dropped with the VACL configured on the SVI
CSCee80365	Unknown	1st hop router randomly fail to add (s,g) flows oif in HW fib table
CSCee89232	Unknown	Configuring platform while in automore state crashes switch
CSCee90183	Unknown	Need to change RPC syslog in case of RPC request sent failure
CSCee95301	Unknown	Unhide and document mls rate-limit multicast non-rpf command
CSCef07965	Unknown	System crashed when accessing CVDM from the switch
CSCin68355	Unknown	:Marking with microflow policer not working with layer2 port
CSCin74123	Unknown	mst root id becomes 0 after switchover
CSCin76766	Unknown	Active SP reloads at ipc_send_rpc_blocked failed after RPR+ swover

Resolved Caveats in Release 12.2(17d)SXB1

Resolved Routing Caveats

- CSCed40933—Resolved in 12.2(17d)SXB1

  Cisco Internetwork Operating System (IOS) Software is vulnerable to a Denial of Service (DoS) attack from crafted IPv6 packets when the device has been configured to process IPv6 traffic. This vulnerability requires multiple crafted packets to be sent to the device which may result in a reload upon successful exploitation.

  More details can be found in the security advisory which is posted at

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050126-ipv6.

Resolved Security Caveats

- CSCed65285—Resolved in 12.2(17d)SXB1

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050406-ssh.html

- CSCed93836—Resolved in 12.2(17d)SXB1

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at
  http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html.

Other Resolved Caveats in Release 12.2(17d)SXB1

Identifier	Technology	Description
CSCee04747	ATM	memory leak when removing ATM VCs
CSCec55147	Infrastructure	Memory leak in IFS
CSCed81154	Infrastructure	SNMP retrieve configuration file crash SUP720 RP
CSCee25000	Infrastructure	Fix for CSCeb22276 and CSCed68575
CSCee06948	IPServices	Sup720 running 12.2(17b)SXA is allowing connections to TCP port 514
CSCdz32659	Management	%SYS-2-MALLOCFAIL: -Process= CDP Protocol
CSCed40563	Management	malicious cfg reload neighbor routers by <show cdp entry * protocol>
CSCin67568	Management	Memory leak in CDP process with long host names
CSCed72764	MPLS	TE tunnel(s) fail to switchback to Explicit path option
CSCeb30338	Multicast	Mcast traffic loss each minute as MMLS entry deleted and reinstalled
CSCed95515	Multicast	Pkts drop in all VLANs when last host in one VLAN leave this group
CSCea57792	platform-76xx	13E5/GBIC:GE-WAN int with 1000baseT gbic is down after oir with traf
CSCed48085	platform-76xx	Stats incorrect for all BB2 OSMs with SUP720
CSCed86778	platform-76xx	: PQ problems with HQoS policy applied to 100 PWAN2 sub-intf
CSCee55056	platform-76xx	OSM interface byte counts are inaccurate
CSCed62633	QoS	RSVP: Install tag failure leaves RSB pointing to freed REQUEST
CSCee23845	QoS	Policer stops counting on egress after ingress poicy is reapplied.
CSCee02786	Routing	IPX EIGRP fails to set originating router id on startup
CSCee36622	Routing	Summary LSA stuck in database
CSCdz84583	Security	IOS fw allowing forged packets for a session initiated from inside
CSCed35253	Security	Router crash due to corrupted data in list with IOS-firewall
CSCed69858	Security	show ssh command issued repeatedly may crash the system
CSCin74155	Security	SSHv2:router crashes under heavy load at tcb_isvalid
CSCed06744	Unknown	software flood to fabric issues with cross-DFC etherchannels
CSCed63590	Unknown	GTP SLB doesnt work with GGSN R5.0 Call Admission Control function
CSCed65372	Unknown	RP/SP software forced reloaded after removing switchport from FE int
CSCed68821	Unknown	WS-X6548-GE-TX stops transmitting
CSCed75920	Unknown	When Glean Rate Limiter enabled Egress ACLs applied on Ingress Pkts
CSCed77519	Unknown	Sup720-3BXL:EoMPLS:VLAN_M dot1q tag handling for IPv6 pkt problem
CSCed79711	Unknown	:LTL_DEBUG_ASSERT: Failture on index + j
CSCed85276	Unknown	VPNSM does not correctly decapsulated nested IPsec traffic.
CSCed87264	Unknown	WS-X6148-45AF module resets randomly when IP phones are connnected
CSCed89537	Unknown	DFC runs out of memory and reloads at L2 Aging Task
CSCed93359	Unknown	Startup config synched to stdby,BOOT_STRING_INVALID message appears
CSCed93707	Unknown	VPN-SM:Different comb of DF bit, PMTUD settings in GRE must be corre
CSCed94258	Unknown	Traffic routed on L2 DEC stops when other L2 DEC becomes non DEC

Identifier	Technology	Description
CSCee05413	Unknown	Memory leak in EARL VLAN stats subblock
CSCee10614	Unknown	DEV: FibTcamSSRAM test fails
CSCee13713	Unknown	test memory crashes the system
CSCee15581	Unknown	sss_mgr with invalid index into 2 arrays causes crash/traceback
CSCee17030	Unknown	Sporadic delay with multicast leave/joins on Spu 720
CSCee19156	Unknown	6PE does not obey mpls ttl propagation command
CSCee21772	Unknown	port-channel dflt results wrong after bootup
CSCee22362	Unknown	Multicast src only detection needs to happen faster
CSCee22993	Unknown	Sup720: Diags detect error on standby Sup after SSO failover
CSCee24422	Unknown	Tracebacks at tyfib_error_recovery and MLSCEF-SP-2-FREEZE
CSCee28215	Unknown	CLI to output actual pps performance
CSCee28288	Unknown	2 second delay in forwarding the 1st packet of mcast stream on 7600
CSCee32151	Unknown	Crossbar MIB not working correctly
CSCee33136	Unknown	MPLS packets duplicated in SRP ring (OSM-DPT)
CSCee35193	Unknown	OSPF sessions are not coming up using pos linecards in the core
CSCee36959	Unknown	Software Forced Reload:get_rp_cpu_info
CSCee39170	Unknown	Incorrect mask value set in ACL TCAM when matching on DSCP values
CSCee43090	Unknown	RLB subscriber packets may loop due to incorrect flow-mask.
CSCee44248	Unknown	Redundant Sup fails to come online after switchover
CSCee45404	Unknown	HSRP does not forward traffic correctly after primary back up
CSCee47030	Unknown	6704-10GE needs to be powered down with Intel ER Rev1 XENPAKs
CSCee54734	Unknown	Need to disable module if a real bad xenpak is plugged in.
CSCee54862	Unknown	High CPU load
CSCin74475	Unknown	Connectivity lost to MWAMs for reseting CSM/MWAM modules on switch
CSCee33103	WAN	CWPA2: CWPA2 reset by SUP due to SCP keepalive failure

Resolved Caveats in Release 12.2(17d)SXB

Resolved IPServices Caveats

- CSCed27956—Resolved in 12.2(17d)SXB

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html. ION is also impacted.

- CSCed38527—Resolved in 12.2(17d)SXB

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

Resolved MPLS Caveats

- CSCeb56909—Resolved in 12.2(17d)SXB

  Cisco Routers running Internetwork Operating System (IOS) that supports Multi Protocol Label Switching (MPLS) are vulnerable to a Denial of Service (DoS) attack on MPLS disabled interfaces.

  The vulnerability is only present in Cisco IOS release trains based on 12.1T, 12.2, 12.2T, 12.3 and 12.3T. Releases based on 12.1 mainline, 12.1E and all releases prior to 12.1 are not vulnerable.

  More details can be found in the security advisory which is posted at http://www.cisco.com/en/US/products/csa/cisco-sa-20050126-les.html

Resolved Unknown Caveats

- CSCed30113—Resolved in 12.2(17d)SXB

  A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to crash and reload.

  This vulnerability is documented as Cisco bug ID CSCed30113. There are workarounds available to mitigate the effects of this vulnerability. Cisco is providing fixed software at no charge.

  This advisory will be posted at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040408-vpnsm

Other Resolved Caveats in Release 12.2(17d)SXB

Identifier	Technology	Description
CSCed08399	Access	NRT:Spurious Accesses seen on 7500 router (etext) for QoS tests
CSCea80820	ATM	Alignment correction at atm_arp_process
CSCeb56457	ATM	IMA and ATM-deluxe PAs drop packets with certain patterns
CSCec12294	ATM	cfg_atm_vcmode_bcs_func is broken
CSCin53126	ATM	Router crashed at abort during OIR of ATM OC3 MM PA
CSCin65182	ATM	OAM PVC on IMA interface doesnt come up after OIR
CSCec87661	Infrastructure	CHUNKBOUNDS errmsg in wrong circumstance - NAT shortcuts not install
CSCea60559	MPLS	lsr mib snmp agent consumes 99% cpu forever
CSCea65827	MPLS	RP/VIP Crash: OIR Flexwan/loose IGP Route to BGP next hop router
CSCeb05519	MPLS	MPLS forwarding table has incorrect label for prefix
CSCeb26389	MPLS	BGP allocates same local label to two VPN prefixes
CSCeb27452	MPLS	Bus error at tagsw_send_icmp process
CSCeb36929	MPLS	Tunnel : bus error when performing tag imposition
CSCeb46191	MPLS	VPN labels get swapped for two iBGP neighbors on a PE-CE shut/noshut
CSCeb76642	MPLS	sh ip cef crashes the RP
CSCec15733	MPLS	MPLS LDP: router crashed while handling tagcon work item
CSCed47409	MPLS	PRP crashes when remove large number of routes
CSCuk47482	MPLS	crash after no mpls ip
CSCec59728	platform-12000	SSO: Standby RP reloads once it is fully-up
CSCec03984	platform-76xx	GE-WAN+ MPLS MTU config inconsistent with other IOS devices
CSCed19431	platform-76xx	GigabitEthernet negotiation is broken on 7600
CSCed49872	platform-76xx	SYS-2-GETBUF: Bad getbuffer SCP Hybrid process tracebacks
CSCed51835	platform-76xx	OSM/POS/BB1: OC12 IP 64 bytes performance may degrade
CSCin66010	PPP	dLFIoFR+QoS:Toggling FR encap can cause router crash
CSCin67741	PPP	RP crashes on removing encap from multilink interface
CSCeb61825	QoS	VIP quantum not udpdated when MTU changed on PA-A3
CSCec28505	QoS	Need to remove error msg showing when bootup w/ low-speed ifc
CSCed62637	QoS	CWPA: priority traffic latency varies with default traffic load
CSCeb17467	Routing	BGP: RP crashes on clearing the BGP table
CSCeb30370	Routing	Crash at ospf_flush_area_summary_lsa after no ip vrf vpn1
CSCeb52270	Routing	Missing receive entry in CEF table
CSCeb77038	Routing	System returned to ROM by bus error on MPLS/PE router
CSCec14415	Routing	BGP next-hop not being set properly amongst peer-groups
CSCec42160	Routing	OSPF Hello processing interupted during CPU intensive activity
CSCec44556	Routing	RIP updates not sent over ATM subints
CSCec85322	Routing	router crashed at i_up during ospfv3 negative testing

Identifier	Technology	Description
CSCec86420	Routing	Undebug all stops traffic with IPsec+GRE+CEF (Also see CSCeb56909)
CSCed06329	Routing	BGP-v6: Version number churns when multipath configured on BGP-v6
CSCed20042	Routing	IPv6 CEF crash when encountering a recursion loop
CSCed29557	Routing	Static routes are not deleted when PEs VRF interface is shut
CSCed57077	Routing	Crash on displaying expired reflexive ACL entries
CSCed62835	Routing	IPV6FIB-SP-4-RECURSION,CEF IPC STACKLOW msg followed by crash
CSCed51674	Security	Software-forced reload:no crypto map GRE on physical interface
CSCea57452	Unknown	SLCP Not Responding...Resetting Module 1
CSCea66218	Unknown	PA-MC-STM1 - Alarmed VCs can bring other VCs down
CSCea78589	Unknown	20E:Crash at ether_getlink on SP
CSCea80003	Unknown	IPSec HA RRI injected routes not deleted on hsrp state change
CSCeb06765	Unknown	Request for Global command to enable Syslog
CSCeb61695	Unknown	RSPAN (CAT6000 Native): VACLs cant be applied on RSPAN vlan traffic
CSCeb72859	Unknown	Bulk Config Sync triggered every exit command
CSCec08364	Unknown	Const2:EoMPLS:L2VPN vpn_num configured as zero, all pkts blocked
CSCec30649	Unknown	QoS:trust port state on 6148-rj45
CSCec36978	Unknown	router crash after no shut sonet interface
CSCec43605	Unknown	dfc: unicast flooding after aging
CSCec55377	Unknown	IOS-SLB: no inservice on RLB vserver may cause reload.
CSCec62406	Unknown	Micorflow policing drops should not charge ag hi policer bucket
CSCec68585	Unknown	CWPA/CWPA2 RP fails to recognize all Flexwans using S9 rommon image
CSCec70454	Unknown	RSPAN on SUP720 running IOS causes spanning tree loop.
CSCec74016	Unknown	Const2:Router crash when ipv6 ACL removed after remove isataptunnel
CSCec90162	Unknown	tracebacks seen after enabling gre keepalive
CSCed00441	Unknown	Rapid-PVST: loop occuring when root bridge expires
CSCed04988	Unknown	6548 + DFC module not recognized with IDPROM massage
CSCed05332	Unknown	ws-x6816 reports minor error after reload
CSCed06462	Unknown	%Error opening nvram:/startup-config (Invalid Checksum)
CSCed14506	Unknown	OIR of 6816 without DFC crashes switch to rommon
CSCed20333	Unknown	Dynamic MAC Entries May Not Age Out After Cessation of Traffic
CSCed20566	Unknown	Traffic forwarded in one direction after valn change
CSCed22387	Unknown	Ibc input queue drops constantly incrementing on SP
CSCed22494	Unknown	VPNSM: fail to insert RRI route if dynamic cmap added on the fly
CSCed29594	Unknown	6500 may not unicast flood packets to rp with fallback bridging
CSCed30061	Unknown	entPhysicalSerialNum does not show value for vendor modules.
CSCed33380	Unknown	IPC failure with show mls netflow ip
CSCed34788	Unknown	Small buffer leak @ icc_get_req_pak and leak in SNMP ENGINE

Identifier	Technology	Description
CSCed35745	Unknown	ARP from CSM to real servers not sent downstream after reload
CSCed35960	Unknown	TETONS2: Ch/OC12DS0 crash when unconf/reconf MFR access uninit mem
CSCed38862	Unknown	g1/1 of WS-X6748-GE-TX not link up after changing speed 10M or 100M
CSCed40129	Unknown	6500 running supervisor IOS may not establish DLSW connection
CSCed47381	Unknown	Cat6k: Autostate may not properly shut down vlan int in Native IOS
CSCed48718	Unknown	DEC workaround and SPAN reflector to be mutually exclusive
CSCed49423	Unknown	Temp. values not updated in show environment temperature
CSCed49574	Unknown	12.2S: traffic loss if in/out PO bundled Active/Plus LC
CSCed51894	Unknown	Egress Span doesnt work after removing RSPAN Src Session
CSCed53899	Unknown	Session struct not cleared on deleting Rspan Sessions
CSCed55342	Unknown	Jumbo frames fail across etherchannel routed on the same vlan
CSCed58110	Unknown	Memory leak under stress condition
CSCed58891	Unknown	wrong mistral timing config value for bootflash
CSCed61632	Unknown	SUP720 may not ARP after SRM-SSO failover with bridging enabled
CSCed62337	Unknown	OSPF adjacencies fail to come up with Sup720, PFC3a and MPLS
CSCed62866	Unknown	VPN-SM-C2:collapse crypto update toggles & reuse vlanidb for gre tun
CSCed63897	Unknown	shut/unshut edge port cause TC to be initiated
CSCed78815	Unknown	BT:Shaping with class-default does not work on ATM pvc
CSCed79519	Unknown	Breakpoint exception due to RPC mismatch timeout
CSCed79694	Unknown	C2SUP2: Multi-Link FR fails to forward.
CSCin41024	Unknown	c2sup2:CWPA:DMLFR:FR Relay entry (sh fr map) is taking lot of time
CSCin61989	Unknown	C2SUP2:RSPAN session not restored on source OIR.
CSCin67400	Unknown	FRF12: Checksum errors with POS, ping fails
CSCin67419	Unknown	A shut of any of the member link or cont traff brings down MFR intf
CSCed62698	WAN	CWPA: ATM: DSCP bits 4-6 set to zero
CSCin34959	WAN	RP fails to recognize bay 1 ATM PA after bay 0 was test crashed
CSCin68724	WAN	set atm-clp bit not set on outgoing packets but QoS stats increment

Caveats in Release 12.2(17b)SXA and Rebuilds

Open Caveats in Release 12.2(17b)SXA and Rebuilds

Identifier	Technology	Description
CSCec74016	Unknown	Const2:Router crash when ipv6 ACL removed after remove isataptunnel
CSCed35900	Unknown	CWPA2 mpls QoS classification not working until re-add policy
CSCee09692	Unknown	Sup720: IPX traffic rate limited based on mls rate limiters

Resolved Caveats in Release 12.2(17b)SXA2

Resolved Security Caveats

- CSCed93836—Resolved in 12.2(17b)SXA2

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html.

Other Resolved Caveats in Release 12.2(17b)SXA2

Identifier	Technology	Description
CSCdz84583	Security	IOS fw allowing forged packets for a session initiated from inside
CSCed35253	Security	Router crash due to corrupted data in list with IOS-firewall

Resolved Caveats in Release 12.2(17b)SXA

Resolved MPLS Caveats

- CSCeb16876—Resolved in 12.2(17b)SXA

  Symptoms: A Cisco router may generate a “SYS-2-GETBUF” message during the “Tag Input” process and may subsequently reload unexpectedly.

  Conditions: This symptom is observed when the router fragments a Multiprotocol Label Switching (MPLS) packet.

  Workaround: There is no workaround.

Resolved Routing Caveats

- CSCeb88239—Resolved in 12.2(17b)SXA

  Symptoms: A router that runs RIPng may crash after receiving a malformed RIPng packet, causing a Denial of Service (DoS) on the device.

  Conditions: This symptom is observed when the **ipv6 debug rip** command is enabled on the router. Malformed packets can normally be sent locally. However, when the **ipv6 debug rip** command is enabled, the crash can also be triggered remotely. Note that RIP for IPv4 is not affected by this vulnerability.

  Workaround: There is no workaround.

Resolved Security Caveats

- CSCec46274—Resolved in 12.2(17b)SXA

  New vulnerabilities in the OpenSSL implementation for SSL have been announced.

  An affected network device running an SSL server based on the OpenSSL implementation may be vulnerable to a Denial of Service (DoS) attack when presented with a malformed certificate by a client. The network device is vulnerable to this vulnerability even if it is configured to not authenticate certificates from the client. There are workarounds available to mitigate the effects of these vulnerabilities.

  This advisory will be posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20030930-ssl.

Resolved Unknown Caveats

- CSCed30113—Resolved in 12.2(17b)SXA

  A malformed Internet Key Exchange (IKE) packet may cause the Cisco Catalyst 6500 Series Switch or the Cisco 7600 Series Internet Router to crash and reload.

  This vulnerability is documented as Cisco bug ID CSCed30113. There are workarounds available to mitigate the effects of this vulnerability. Cisco is providing fixed software at no charge.

  This advisory will be posted at
  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040408-vpnsm

Other Resolved Caveats in Release 12.2(17b)SXA

Identifier	Technology	Description
CSCec42594	AAA	Spurious access on Sup720 during configuration
CSCeb34203	Access	TX Ring Limit appears to be broken for PA-MC-E3
CSCec06146	Access	Channelized interfaces fail to come up after reconfiguration or flap
CSCec79579	Access	CWPA crash due to pas interrupt
CSCin38177	Access	C2SUP3:T3 Serial PA in Flexwan crashed @ pas_init_stub_nmi_handler
CSCin60835	Access	Show controller serial not showing all 15 min intervals
CSCdx79081	ATM	ATM vc bundle member adjacencies not getting deleted
CSCea80820	ATM	Alignment correction at atm_arp_process
CSCeb64384	ATM	ATM subif created on (OC3-SMI PA) break snmp agent
CSCec68740	Content	Remove wccp commands from CLI for SUP720

Identifier	Technology	Description
CSCec42069	Infrastructure	Service Password encryption not hashing the password
CSCec87661	Infrastructure	CHUNKBOUNDS errmsg in wrong circumstance - NAT shortcuts not install
CSCin57765	Infrastructure	appending to files on disks can crash/hang system
CSCea81952	IPServices	NAT crash due to h225/h245 without RAS
CSCec10494	IPServices	Router may crash after issuing show ip igmp tracking detail
CSCin35940	IPServices	Bridging Failed when BRI interface Encapsulation is PPP
CSCdw76355	MPLS	Clear ISIS *, RRR not announce back tunnel with fast-reroute
CSCdx39482	MPLS	MPLS TE: Explicit tunnel takes wrong outgoing interface
CSCdz04196	MPLS	Encapsulation fixup flags incorrect for MPLS TE tunnels
CSCea29102	MPLS	RP crash in BGP when clear ip bgp * and OIR/flap interfaces
CSCea83647	MPLS	Invalid tag Exp-null new incoming tag at tfib_route_tag_change
CSCeb37966	MPLS	GRP crash when configuring frr for ATOM tunnel
CSCeb68673	MPLS	IAS: tfib missing entry when VRF unconfig from ASBR-PE
CSCeb79576	MPLS	eBGP+Label: label binding present in BGP, but not in LFIB and LIB
CSCeb86270	MPLS	remote systems crash when local system reloaded
CSCec26563	MPLS	GSR crashes when configuring mpls traffic-eng tunnels
CSCec31206	MPLS	Get and Set same values on MPLS MIBs caused memory leak
CSCin53682	MPLS	IAS:router crash @ neighbor flexwan oir
CSCdx32947	Multicast	FS-HYB: static RP changes to bidir by itself, 100% CPU, AutoRP loop
CSCec41693	Multicast	RP never sends register stops
CSCec73078	Multicast	sup720: egress replication breaks mcast over secondary sup uplinks
CSCeb86171	platform-76xx	Bad EEPROM GBICs force line protocol down on WAN ports
CSCec18366	platform-76xx	OSM-ATM crashes when traffic goes through
CSCec22452	platform-76xx	QOS/RT/DB: LC crashed with TxSOP Errors
CSCec39689	platform-76xx	CHOC-12/DS3 doesnt come up when remote end change status to up/up
CSCec46892	platform-76xx	OSM-ATM:Mcast pkts are dropped over 1483 bridged PVCs
CSCec48974	platform-76xx	OSM: show contr pos pm shows incorrect optics information
CSCec52228	platform-76xx	POS-OC12+ crash after interface configured
CSCec74760	platform-76xx	7600 w/BRE configured replies to ARP even with Interface down/down
CSCec79460	platform-76xx	OSM-4GE-WAN GBIC int stays up/up though connected NPE-G1 int is down
CSCec89414	platform-76xx	pos controller increments coaps rregardless of APS configuration
CSCed00781	platform-76xx	Write erase causes SLOTSCACHE to be erased
CSCec22252	PPP	MLP, PE VIP crashed after shut down 1 of the 2 phisical int (MU).
CSCec25317	PPP	VIP crash disabling dCEF on MLP interface
CSCec34606	PPP	ALIGN-1-FATAL crash while deconfiguring cRTP on Frame Relay
CSCec61738	PPP	MLP:Pkts dropped at ingress of pe under 1ce-2pe topolog
CSCec86131	PPP	STMPA crashes continously @ vip_mlp_ll_fastsend

Identifier	Technology	Description
CSCin62978	PPP	C2SUP2:dLFI+dCRTP:FW2 crash@ ct3sw_tx_interrupt on continous traffic
CSCdy77717	QoS	removing MPLS-TE tail Loopback I/F causes crash
CSCea84387	QoS	Two simultaneous policy map displays cause problems
CSCec32573	QoS	MQC:Input Marking is based on Outgoing classification
CSCec46485	QoS	match dscp and match prec matches do not take effect.
CSCec74699	QoS	NBAR not running distributed on FlexWAN
CSCin61140	QoS	mfr: LC crahses with LFI/mqc enabled
CSCdz67496	Routing	OSPF thinks Tunnel interface is down after reload.
CSCeb04048	Routing	Upgrading/reloading IOS may cause OSPF interfaces/neighbors down
CSCeb19730	Routing	Const2:RP crash at isis_install_one_ip_route under traffic stress
CSCeb30370	Routing	Crash at ospf_flush_area_summary_lsa after no ip vrf vpn1
CSCeb61700	Routing	OSPFv3: no passive-int <int-name> incorrectly added for ipv6 int
CSCec15095	Routing	Ospf database not updated completely on shut/noshut of Interface
CSCec29868	Routing	OSPFv3 adjacency flap after switchover when standby sup comes online
CSCec30212	Routing	OSPF adjacency bounces when area <x> stub
CSCec33773	Routing	OSPFv3 does not update routes when shut interface,virt-link configur
CSCec35322	Routing	RP crashed after configuring IPv6 ACL
CSCec38322	Routing	CEF reloader holding up memory when toggling DCEF-CEF-DCEF
CSCec39973	Routing	RP crash at isis_add_is_neighbors_to_lsp
CSCec40548	Routing	OSPF not installing route in RT after removing MPLS TE area config
CSCec45770	Routing	OSPFv3 not able free lsdb_chunks after reload requested
CSCec48816	Routing	Router crash at ospf_clean_if after removing network command
CSCec49499	Routing	IOS reload hangs when OSPF is configured
CSCec64382	Routing	IPv6: Adjs failed to repopulate correctly on interface flap
CSCec68467	Routing	Memory leak in OSPFv3
CSCed06329	Routing	BGP-v6: Version number churns when multipath configured on BGP-v6
CSCeb55703	Security	Cannot ssh to router -- crc comparison failed
CSCuk39887	Security	Fixup disabled on adjacencies for tunnel interfaces
CSCdw41639	Unknown	ls1010 Silently Drops OAM F5 with oam intercept enabled
CSCdx22158	Unknown	VSEC:Stress testing crashes the router after 4hrs
CSCdz55955	Unknown	Unity: client XAUTH fails if user domain name doesnt match group nam
CSCea51081	Unknown	group lock can still allow users into wrong group
CSCea69116	Unknown	L2/L3 switched counters remain 0 in sh int vlan
CSCea85342	Unknown	19E:Uplink ports on standy fail after switchover
CSCea86396	Unknown	6500 MSFC may not program static Null 0 route into HW
CSCeb21815	Unknown	FW Some of the E1/T1 channels of a STM PA protocol goes down on rel
CSCeb49514	Unknown	Const2: Distributed port channel does not forward traffic

Identifier	Technology	Description
CSCeb54694	Unknown	C2:MSFC3: Add support for NVRAM: private-config for ARIEL Platform
CSCeb57474	Unknown	FBs do not bootup after reload in both rpr+ and handover-split modes
CSCeb61144	Unknown	C2-HYB: configuring config file to flash: causes nvram failure
CSCeb64666	Unknown	SPURIOUS mem at isakmp_send send_nat_keepalive in nat
CSCeb67996	Unknown	CE2-NATIVE:mcast traffic s/w switched for few groups with intf reset
CSCeb83650	Unknown	L2 Etherchannel across DFCs has intermittent packet loss
CSCeb86653	Unknown	CE2-HYB: MSFC2 crashed at fm_tcpintrcpt_find_conn_info
CSCec00570	Unknown	VLAN without SVI set to redirect instead of bridge
CSCec08629	Unknown	RLS3(ios):C6K222:SP crash while clearing lcp session to 6816 module
CSCec08973	Unknown	Invalid counters on PA-MC-STM-1SMI
CSCec14054	Unknown	Allow users to enable/disable BPDU filtering on FWSM ports
CSCec15149	Unknown	Co-existence of distributed etherchannels and mac-move notification
CSCec27686	Unknown	CSM channel does not trust DSCP (Supervisor IOS)
CSCec30461	Unknown	13E4: MPLS - BGP Learnt Prefixes incorrectly using IP mac-sa
CSCec31276	Unknown	MPLS-tagged pkts sourced from the RP are not prioritized correctly
CSCec32173	Unknown	VSEC:VPN-SM-C2: Traffic is lost if the tunnel mac address is changed
CSCec33663	Unknown	20E:Mac addresses not learnt on convertng PO auto to trunk
CSCec36559	Unknown	20E:Traffic dropped for 40-50secs when 6816 comes up
CSCec37069	Unknown	Multicast Netflow stats being exported on Cat6k
CSCec37464	Unknown	CWAN-QOS:HQoS, Vtms Qs are not proper with microcode reload
CSCec37803	Unknown	Need scp error counters per nmp for Mcast group 5
CSCec38516	Unknown	6kIOS CLI only accepts 1st command when multi remote command run
CSCec39383	Unknown	SWITCH-ENGINE-MIB,Traceback msg when mibwlak cseTcamUsageTab
CSCec39937	Unknown	MSFC fails to boot when system is rebooted
CSCec40719	Unknown	Using NBAR and SRM crashes redundant MSFC
CSCec45398	Unknown	Align error on SP- Traceback: mcast_mld_accept_group
CSCec47779	Unknown	Remove inapplicable RESETNXI errmsg and change to debug info
CSCec48379	Unknown	Const2: pak expansion on rate limit index causes resets
CSCec48393	Unknown	SYS log msg is needed & power should be denied for unsupported cards
CSCec49438	Unknown	ALIGN-1-FATAL at dyntrk_set_tot when configure trunk over port-chan
CSCec50577	Unknown	Some multicast L2 entries not propagated to DFCs after reload
CSCec50648	Unknown	auto-MDIX doesnt work on ws-x6548-rj-21
CSCec51288	Unknown	13E11,20E:DFC cards fail to learn mac addresses
CSCec54433	Unknown	Sup720: SP alignment errors and MSFC crash in heartbeat_fatal
CSCec54471	Unknown	Const2:RPR+ IPC-SP-STDBY-5-WATERMARK msgs are seen continously.
CSCec55650	Unknown	Output packets not dcef switched on multilink interface
CSCec57672	Unknown	Unable To Retrieve Counters From Vlan Interface

Identifier	Technology	Description
CSCec58834	Unknown	dot1q vlan on subintf not usable if remove card & reinsert
CSCec59341	Unknown	PIM snooping command results in traceback
CSCec62406	Unknown	Micorflow policing drops should not charge ag hi policer bucket
CSCec62587	Unknown	giants on dot1q trunk with sup720 uplink ports
CSCec62788	Unknown	Flow dscp become 255 if agg.policy conform action modified
CSCec62945	Unknown	C2MCAST:STP doesnt work for both ieee and dec specification
CSCec63033	Unknown	v4 acl in tcam serialised mode removed on config v6acl(excep)
CSCec63462	Unknown	Support of CISCO-SYSLOG-MIB,its CLI missing from PS but in JK9S img
CSCec64282	Unknown	Failed to sync port asic on WS-6516A-GBIC and WS-6548-GE-TX
CSCec65070	Unknown	Software needs to limit total power by chassis
CSCec67234	Unknown	Multicast not working thru VPN when outside port is in routed mode
CSCec68570	Unknown	mls rate-limit unicast acl vacl-log rate limiter cfg lost on reload
CSCec68585	Unknown	CWPA/CWPA2 RP fails to recognize all Flexwans using S9 rommon image
CSCec68645	Unknown	SP crash on doing dir disk0:
CSCec77448	Unknown	System crash in idprom_ps_get_info (PS not fully inserted)
CSCec78265	Unknown	Several debugs are turned on on RP & SP after each reload
CSCec80654	Unknown	Hardware shortcuts installed without RPF traffic
CSCec80868	Unknown	lcp failed to go online after system reset
CSCec82732	Unknown	Max power limit should be increased for 6500-E chasses
CSCed13751	Unknown	VSEC:VPN-SM: Duplicate IKE sa when PIX501 is rebooted
CSCed14506	Unknown	OIR of 6816 without DFC crashes switch to rommon
CSCed15587	Unknown	System controller resets causes high cpu with 2 flow dest configured
CSCea19885	Voice	Bus error at address 0xD0D0D0B, Process CCH323_CT
CSCeb78836	Voice	h323: software forced crash if bad packet received and debug opened
CSCin56408	Voice	Tracebacks found when receiving invalid H323 setup packet
CSCeb33417	WAN	MFR: router crash during unconfiguration on MFR
CSCec59440	WAN	Small X.25 Packets Corrupted in Frame-Relay Switching on FlexWAN
CSCin53115	WAN	C2:MFRoMPLS:MFR interface goes DOWn/DOWN on sh/no sh with AToM VCs

Caveats in Release 12.2(17a)SX and Rebuilds

Open Caveats in Release 12.2(17a)SX and Rebuilds

Identifier	Technology	Description
CSCec50469	Unknown	Ethertype config accepted but not applied on 6502-10GE cards
CSCec74016	Unknown	Const2:Router crash when ipv6 ACL removed after remove isataptunnel

Resolved Caveats in Release 12.2(17a)SX4

Resolved Security Caveats

- CSCed93836—Resolved in 12.2(17a)SX4

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html.

Other Resolved Caveats in Release 12.2(17a)SX4

Identifier	Technology	Description
CSCdz84583	Security	IOS fw allowing forged packets for a session initiated from inside
CSCed35253	Security	Router crash due to corrupted data in list with IOS-firewall

Resolved Caveats in Release 12.2(17a)SX3

Identifier	Technology	Description
CSCed38862	Unknown	g1/1 of WS-X6748-GE-TX not link up after changing speed 10M or 100M
CSCed79519	Unknown	Breakpoint exception due to RPC mismatch timeout

Resolved Caveats in Release 12.2(17a)SX2

Resolved IPServices Caveats

- CSCed27956—Resolved in 12.2(17a)SX2

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html. ION is also impacted.

- CSCed38527—Resolved in 12.2(17a)SX2

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-ios.html and it describes this vulnerability as it applies to Cisco products that run Cisco IOS software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/en/US/products/csa/cisco-sa-20040420-tcp-nonios.html

Other Resolved Caveats in Release 12.2(17a)SX2

Identifier	Technology	Description
CSCed15587	Unknown	System controller resets causes high cpu with 2 flow dest configured
CSCed49091	Unknown	Breakpoint Exception after 6724-SFP module problems

Resolved Caveats in Release 12.2(17a)SX1

Identifier	Technology	Description
CSCec42594	AAA	Spurious access on Sup720 during configuration
CSCec42069	Infrastructure	Service Password encryption not hashing the password
CSCdz04196	MPLS	Encapsulation fixup flags incorrect for MPLS TE tunnels
CSCec33773	Routing	OSPFv3 does not update routes when shut interface,virt-link configur
CSCec35322	Routing	RP crashed after configuring IPv6 ACL
CSCec45770	Routing	OSPFv3 not able free lsdb_chunks after reload requested
CSCec48816	Routing	Router crash at ospf_clean_if after removing network command
CSCeb55703	Security	Cannot ssh to router -- crc comparison failed
CSCuk39887	Security	Fixup disabled on adjacencies for tunnel interfaces
CSCeb49514	Unknown	Const2: Distributed port channel does not forward traffic
CSCec42766	Unknown	WS-F6K-VPWR-GE/WS-F6K-PWR should power down devices req > 7000mW
CSCec45398	Unknown	Align error on SP- Traceback: mcast_mld_accept_group
CSCec48379	Unknown	Const2: pak expansion on rate limit index causes resets
CSCec48393	Unknown	SYS log msg is needed & power should be denied for unsupported cards
CSCec54433	Unknown	Sup720: SP alignment errors and MSFC crash in heartbeat_fatal
CSCec65070	Unknown	Software needs to limit total power by chassis
CSCec68645	Unknown	SP crash on doing dir disk0:

Resolved Caveats in Release 12.2(17a)SX

Resolved Infrastructure Caveats

- CSCdz29724—Resolved in 12.2(17a)SX

  Symptoms: IOS Exec sessions return an error message of “login invalid”

  Condition: If the username does not exist in the local username database when using local authentication.

  Workaround: This bug fix will modify the behavior to wait for the password to be entered before returning the same error message as would be used if the password is incorrect.

Resolved IPServices Caveats

- CSCea34745—Resolved in 12.2(17a)SX

  Symptom: A Cisco device running IOS and enabled for Hot Standby Router Protocol (HSRP) may reset with a SYS-2-WATCHDOG error from a specifically crafted malformed HSRP packet. The HSRP protocol is not enabled by default.

  Conditions: The specifically crafted malformed HSRP packet would require local attachment to a segment that supports the HSRP group. This issue does not affect IOS releases 12.3 and later This issue affects in 12.2, 12.2T and 12.2S versions of IOS. This issue affects 12.1E releases prior to 12.1(23)E.

  Workaround: There is no workaround.

Resolved Multicast Caveats

- CSCea58105—Resolved in 12.2(17a)SX

  Symptoms: The interface of a Cisco router that functions as a Protocol Independent Multicast (PIM) Rendezvous Point may stop receiving traffic. The output of the **show interfaces** privileged EXEC command may show input queue drops.

  Conditions: This symptom is observed after the interface has received PIM register packets with the Router Alert option.

  Workaround: Reload the port adapter or line card with the affected interface.

Resolved PPP Caveats

- CSCdz22366—Resolved in 12.2(17a)SX

  In a Virtual Private Dial-up Network (VPDN) environment, if the LAC is not configured for authentication and the user does not provide any authentication information, the authentication on the LNS may be bypassed. This problem will not occur if the LAC is configured properly to authenticate the users.

  In the case of client initiated tunnels (http://www.cisco.com/warp/public/471/l2tp-win2k-cit.html), where there is no seperate LAC, all authentication may be bypassed.

  Only the IOS devices that are acting as LNS are affected. The IOS devices that are not acting as LNS are not affected.

  An attacker may exploit this vulnerability to gain unauthorized access to network resources if authentication is not configured on the LAC.

  The workaround is to configure “lcp renegotiation always” command in virtual private dialup network (VPDN) group configuration mode.

Resolved Security Caveats

- CSCdy68457—Resolved in 12.2(17a)SX

  Symptoms: Spurious memory accesses may occur on a Cisco router, and the router may reload.

  Conditions: This symptom is observed on a Cisco router that is configured for authentication proxy.

  Workaround: Disable the authentication proxy feature.

- CSCdz12098—Resolved in 12.2(17a)SX

  Symptom: When auth-proxy is enabled in an environment where DOS attacks from CodeRed or Nimda are present, it may be possible to exhaust resources if more than 40 DOS machines are attacking the router where auth-proxy is enabled.

  Conditions: See above

  Workaround: Disable auth-proxy or monitor auth-proxy cache to see attacking machines and clear viruses off machines.

- CSCea93882—Resolved in 12.2(17a)SX

  Symptoms: If Cisco Express Forwarding (CEF) is disabled, a router may reload with the following error message upon the receipt of a malformed generic routing encapsulation (GRE) packet:

  %ALIGN-1-FATAL: Illegal access to a low address addr=0xA30, pc=0x40992D3C, ra=0x405E64B8, sp=0x43562838

  Conditions: This symptom is observed on a Cisco router that has CEF disabled. The symptom even occurs without a tunnel configuration on the router.

  Workaround: Enable CEF on the router by entering the **ip cef** global configuration command.

Resolved Voice Caveats

- CSCdz44138—Resolved in 12.2(17a)SX

  Symptoms: After a Session Initiation Protocol (SIP) message is received, a memory leak may occur in the CCSIP_SPI_CONTROL process on a Cisco MC3810 and the following errors are reported:

  - Method Not Allowed
  - Invalid CallId -
  - Internal Server Error

  Conditions: This symptom is observed on a Cisco MC3810 that is running Cisco IOS Release 12.2(12).

  Workaround: There is no workaround.

Other Resolved Caveats in Release 12.2(17a)SX

Identifier	Technology	Description
CSCdx07849	AAA	Unable to save configuration due to startup-config file open failed
CSCds19651	Access	cablelength short 133 is not displayed on running config
CSCdt48893	Access	output stuck on PA-CE1
CSCdx33931	Access	dialer behavior is inconsistent with VJHC enabled and MPPP
CSCdy61602	Access	NRT: RSP-3-RESTART after changing encapsulation to lapb
CSCdy67459	Access	dialer interface does not work properly after reconfiguring
CSCdz00415	Access	%SCHED-2-EDISMSCRIT for Process= Compute load avgs
CSCdz31561	Access	Callback fails if dialer string different than calling number
CSCdz48147	Access	Incoming call rejected, exceeded max calls with x25 configuration
CSCdz50451	Access	spurious memory access ct3sw_show_controllers
CSCdz55396	Access	CRC errors dont show up on MC-8E1 interfaces
CSCdz71171	Access	CT3 reports LOS and FEAC when ports are up
CSCdz72292	Access	Output queue stuck on PA-MC-8E1 after some interface flapping
CSCdz75118	Access	Interface input / output rate not decreasing to zero after shutdown
CSCea21643	Access	Dialer Watch stalls
CSCea42252	Access	PA-MC-E3 bad index in DS1-MIB
CSCea42298	Access	PA-MC-E3: E3 controller is missing from MIBs
CSCea58283	Access	%RSP-3-NOIDB: bad vc 3840 error with CT3IP-50
CSCea63532	Access	c7200:ifEntry object disappears after OIR of PA-MC-T3
CSCea87183	Access	show interface serial 4/0/0/3:0 giving %invalid input detected
CSCeb24875	Access	Const2:FW MC-8T1 pkts > 1650 bytes are dropped on t1 interfaces
CSCeb45429	Access	Line protocol goes down on CT3 interface
CSCeb47812	Access	clear counter will cause CE3/cT3 PA invaild mem action(malloc)
CSCin23422	Access	In Flexwan with PA-MC-2T3+, unprovisioning T1 is not clean
CSCin24364	Access	Boot tftp <image> command gets skipped while reloading
CSCin26892	Access	Input counters zero for PA-MC-8TE1+ and PA-CE3

Identifier	Technology	Description
CSCin28487	Access	Traceback at clear_idb_subblocks while unconfiguring PA-MCTE1
CSCin34068	Access	Unable to create channel-group on PA-MC-8TE1+
CSCin35837	Access	PA-E3 Needs shut/no shut to come up after fault
CSCin39446	Access	Incorporating changes for FREEDM errata
CSCds30121	ATM	Incorrect ATM MAP entry cause SVC connectivity
CSCdv38344	ATM	ATM PA does not work when TokenRing PA-4R-FDX in lower slot
CSCdw68278	ATM	Z-CDS: allowed to configured vbr-rt for spvp connection
CSCdw87766	ATM	CEF drops counted as InPktDrop under atm PVC on PA-A3-OC12
CSCdy18923	ATM	LANE: Non-control traffic may get enqueued to control path
CSCdy31278	ATM	SNMP:SONET section/line/path alarms issue
CSCdy74214	ATM	PA-A2: VC output stuck
CSCdz37332	ATM	Removing PVC from pvc range clears vc-class bbinded to this PVC
CSCdz37449	ATM	multicast: RP announce not forwarded out OIL, S,G bouncing
CSCdz43056	ATM	debug atm oam vc x.yy enables the debug for all VCs configured.
CSCdz45785	ATM	protocol ppp unavailable under pvc/svc after CSCdz25164
CSCdz53151	ATM	CSCdj74418 fix for cisco 3600 (NM-1A-OC3MM)trlane
CSCdz59562	ATM	PA-A3-T3/PA-A3-E3: Framer facility statistics counters with sh cntlr
CSCdz62055	ATM	Bandwidth does not recover after link flap in IMA
CSCdz63708	ATM	AToM configurations disappear after the router reloaded.
CSCdz65823	ATM	Wrong UNI version on NRP-NSP when no atm autoconfig
CSCdz67483	ATM	Encapsulation aal0 option missing for CRoMPLS
CSCdz76166	ATM	Router reloads when show atm vc <vcd#> is issued for an SVC
CSCdz76961	ATM	sh int atm shows incorrect 5 minute output rate in congested vc
CSCdz79023	ATM	ATM Sub-int goes down after clearing last SVC. Needs Int flapping.
CSCdz80585	ATM	NSP Memory Leak with SoftVC Establishment
CSCea11344	ATM	SLT:can not config abr rate-factors properly on RPM-PR/MGX8850-PXM1
CSCea11453	ATM	C7200-NP400 router crash due to SAR crash pas-atm
CSCea19552	ATM	Some ATM PVC in inactive state, when loading this code
CSCea29435	ATM	Const2:FW Jumbo frames greater than 4470 bytes are dropped on atm pa
CSCea34340	ATM	console locks up with decnet atm flexwan int config change
CSCea38882	ATM	Modular packet cleanup for ATM PAs in 7200
CSCea39282	ATM	LE-arp getting responded on blocked ports
CSCea39354	ATM	SLB causes crash when virtual ip pinged across atm.
CSCea50251	ATM	PA-A3-OC12 does not handle OAM/routing updates with priority
CSCea51113	ATM	Const2:flxw traceback @atm_encap_common() when enabling half-bdg
CSCea51200	ATM	ATM sub-interface counter update slow
CSCea61178	ATM	Unable to configure PCR/SCR to max cell bandwidth of IMA int

Identifier	Technology	Description
CSCin17264	ATM	PA-A3/A6:Packet count shown incorrectly on pvc
CSCin26592	ATM	ATM: Multiple users configuring crashes router
CSCin26599	ATM	ATM_VPoL2TPv3:Connectivity issues aft continuous low b/w traffic
CSCin28792	ATM	Can not attach policy on ATMima Subinterface
CSCin30349	ATM	bay 1 crash while doing shut no shut
CSCin32872	ATM	back to back ping fails after bay reload due to INAC VC
CSCin33339	ATM	unnecessary trace back in debug atm event output
CSCin33561	ATM	MSFC crash when an ATM uni link is configured
CSCin33673	ATM	loki_state_change: Sending config failed - IMA interface down
CSCin33887	ATM	Bad refcount in retparticle at atmdx_buf_done_interrupt
CSCin33927	ATM	pcr is sometimes less than scr in IMA using dynamic b/w feature
CSCin34322	ATM	Flexwan crash while MSFC is booting
CSCin38132	ATM	when traffic rate > police cir ATM ima crashing
CSCin40163	ATM	ATM-PA-A3 not coming up on NPE400 and NSE-1
CSCin42584	ATM	PA-A3 not coming up on 7200 with NPE150
CSCin42799	ATM	Increase rx buffers for PA-A3/A6 on NPE-G1
CSCdz41584	CableBroadband	Downstream sync loss causes Output Stuck on uBR905
CSCdz37602	Connectivity	crash when deleting a translate x25 pvc command with login keyword
CSCdz36099	Content	CAT6K: Problems with bypass auth-traffic: GRE padding
CSCdz79996	Content	Enabling WCCP causes client TCP retransmissions
CSCuk41908	Content	WCCP redirect in may be applied to an interface incorrectly
CSCdu57101	Infrastructure	Incorrect information displayed in the ifStackTable
CSCdv20075	Infrastructure	%SYS-3-CPUHOG process = IP SNMP
CSCdv46906	Infrastructure	Incorrect LocIfReason in linkUp/Down Traps
CSCdw46392	Infrastructure	modemcap not applying on lines configured with modem DTR-active
CSCdx01536	Infrastructure	Caching not implemented correctly in entityextmib
CSCdy56342	Infrastructure	service config error messages only go to console
CSCdy87341	Infrastructure	Faulty Behaviour in Config Man Mib
CSCdz16090	Infrastructure	parser will not accept more than 256 chars in a line
CSCdz32940	Infrastructure	Crash in service Compression
CSCdz36877	Infrastructure	no echo of characters on vty exec
CSCdz40472	Infrastructure	TTY2: timer_create_bg error when telneting to router
CSCdz51138	Infrastructure	ifOperStatus shows incorrect value for PPP encap interfaces
CSCdz54372	Infrastructure	compress predictor accepted for HDLC if configured before for lapb
CSCdz54387	Infrastructure	sector read error while trying to boot/read corrupted file off disk0
CSCdz55986	Infrastructure	traceback found when reload RR router
CSCdz59591	Infrastructure	appending to files on ATA flash devies does not work

Identifier	Technology	Description
CSCdz59873	Infrastructure	ATA filesystem creates multiple identical xcpa directories
CSCdz60750	Infrastructure	Squeeze operation causes too much cpu utilization
CSCdz61503	Infrastructure	NE Crashed when trying to poll NOTIFICATION-LOG-MIB using getbulk
CSCdz72593	Infrastructure	ciscoFlashMIB loses ciscoFlashPartitionTable
CSCdz75810	Infrastructure	Should not have all traps appended to snmp-server host
CSCdz81035	Infrastructure	writing crashinfo to disk0 results in corrupted file
CSCdz85695	Infrastructure	RTR: Command rtr ping jitter unconfigures rtr key-chain
CSCdz89000	Infrastructure	3660 crash on parser code while manipulating CSB-PID DB
CSCea06647	Infrastructure	format of ATA flash card fails
CSCea15879	Infrastructure	SAA: Memory leak with rtr responder (Engine1)
CSCea17144	Infrastructure	RSP software forced crash with VIP crashes
CSCea19913	Infrastructure	Memory Protection Violation error
CSCea25697	Infrastructure	Memory leak found with default interface XYZ command
CSCea28333	Infrastructure	%IPC-2-PRECLOSE tracebacks
CSCea33897	Infrastructure	Bad Requeue leads to fragmentation crash
CSCea38774	Infrastructure	show parser cache causes crash
CSCea44786	Infrastructure	privilege command does not work correctly for named access-lists
CSCea62212	Infrastructure	ATA_status timeout errors
CSCea87766	Infrastructure	<interface> is a static pool and cannot be tuned message displayed
CSCeb64604	Infrastructure	SAA 2.1.1 Latest Oper Sense: httpError for HTTP status code 200
CSCin28606	Infrastructure	Invalid interface counters after loading the image
CSCin37630	Infrastructure	Sync Problems because of router_action attempting sync
CSCin41414	Infrastructure	Router crashes at fslib_ifs_ioctl when verify command issued
CSCuk44685	Infrastructure	SSO: RRP disabled (IPC failure) after OIR on another slot
CSCdt95129	IPServices	NAT: translation fails after manual table clearing
CSCdv34346	IPServices	IDS audit breaks policy routing on a NATd interface
CSCdv54170	IPServices	AsyncQ manager failure to adjust queued calls on remote disconnect
CSCdx46319	IPServices	CMF doesnt seem to work correctly
CSCdy57048	IPServices	MPLS/Tag switching results in invalid TCP packet
CSCdz18109	IPServices	NAT router receives self generate translated packet by itself
CSCdz36526	IPServices	NAT: missing changes in CSCdx40232 umbralla commit
CSCdz38681	IPServices	add-route wont create static route unless old entry removed first
CSCdz38987	IPServices	DD keeps checking server after it is removed
CSCdz44155	IPServices	Some NAT entries have no expiration timer set and never expire
CSCdz44758	IPServices	%STANDBY-3-DIFFVIP1 syslog message gets sent out as 3 messages
CSCdz46435	IPServices	Traceback at frame_relay_extract_addr after igmp_get_mac_or_ip_srcad
CSCdz51270	IPServices	Software forced crash due to NAT

Identifier	Technology	Description
CSCdz63000	IPServices	ICMP port unreachable creates NAT half entry
CSCdz76824	IPServices	Arp alias not set correctly after reload with static NAT configured
CSCdz78549	IPServices	7401 crashed at ip_nat_command after issuing wr t
CSCea07035	IPServices	alignment errors in IP NAT
CSCea10787	IPServices	Static inside network NAT does not work for multicast
CSCea17268	IPServices	HA: can not clear vty line
CSCea36425	IPServices	telnet source-interface affects session command
CSCea55449	IPServices	bus error while trying to age nat entry in 12.1(13)E04
CSCea60379	IPServices	Memory leak in LDP process
CSCdu15973	ISDN	ISDN should reject V110 calls based on LLC octet 5a
CSCdz61369	ISDN	ss7 gateway missing isdn service command after reload
CSCdz61729	ISDN	Need to disable Redirecting number IE for NTT
CSCdz86750	ISDN	need CLI to enable/disable fix for CSCdx12421
CSCdt55540	LAN	PA-2FE-TX does not support auto-neg so remove auto config commands
CSCdw00953	LAN	TX-ISL 1 port FE PA wont go DOWN immdly when carrier is lost
CSCdx63927	LAN	7200: reload due to memory corruption in PA-1FE
CSCdx80675	LAN	Spurious access at dec21140_rx_interrupt, possibly regression bug
CSCdy89749	LAN	lot of spurious access at fx1000_dtq_consumer_isl and vip crashes
CSCdz06957	LAN	Snasw virtual tokenring port drops null xid sent as SRE
CSCdz38604	LAN	Counter of collision is different between RSP and VIP
CSCdz45509	LAN	MPLS packets coming into GEIP dot1q sub. are dropped as ignore
CSCdz73287	LAN	VSEC: Gigabit Ethernet is in half duplex mode
CSCdz77618	LAN	PA GE show UP/UP when re-seated with Gbics with No cables connected
CSCdz84025	LAN	CWTLC PXF crash:Internal Error (0x00210001): Col0 CRASH_CODE_CMD_ID
CSCdz90090	LAN	VIP ignores unicast packets received from PA-2FE
CSCea22898	LAN	LLC2 does not follow N2 value
CSCea37647	LAN	Unable to maintain Full-Duplex setting when doing FEC
CSCea44850	LAN	SNA Host PU dropping when configured on Virtual-TokenRing interface
CSCea66198	LAN	Bus error when applying crypto map to fddi interface
CSCea82238	LAN	bus error when using % in vtp password
CSCec18181	LAN	sh pas i82543 interface giga1/0 MTA - crashes router
CSCin27090	LAN	Router crashes in update_dot1q_vlan_rp_out_counters()
CSCin31870	LAN	PA GE show UP/UP when re-seated with Gbics with No cables connected
CSCin43613	LAN	c7200 FE Data-plane performance degradation on flo_isp
CSCdu78087	LegacyProtocols	show x25 hunt-group status incorrect
CSCdx77062	LegacyProtocols	Snasw PUs (and LUs underneath) in Reset state after mainframe IPL
CSCdx79523	LegacyProtocols	X.25 DDR stops after first ISDN failure

Identifier	Technology	Description
CSCdy59779	LegacyProtocols	DLSw+: LLC session stuck in ADM state
CSCdz18119	LegacyProtocols	3640 router crashes at __doprnt while configuring ipx routing
CSCdz21952	LegacyProtocols	upstream cp-cp sessions flapping with sense 0x08890100
CSCdz22127	LegacyProtocols	DLSw+: CLS return code ignored on Confirm primitives
CSCdz24438	LegacyProtocols	HPR pathswitch time values should be configurable
CSCdz25898	LegacyProtocols	snaswitch dlur must report uplinks to ENs in TDU to DLUS
CSCdz25931	LegacyProtocols	allow snasw location with wildcard on just owning-cp
CSCdz40029	LegacyProtocols	DLSW ER: Buffer leak in the small buffer pool
CSCdz40331	LegacyProtocols	SNAsw router rejecting CP-cap in Error-Capture.cap
CSCdz60566	LegacyProtocols	QLLC needs second call to establish DLSw circuit
CSCdz60694	LegacyProtocols	SNASW uses the same FQPCID when the second REQDACTPU is sent to VTAM
CSCdz62958	LegacyProtocols	Remove Inactive entries in snasw topology table as the TGs go inacti
CSCdz83029	LegacyProtocols	Dlsw ER with GigE PA Wiseman FX1000 chipset doesnt work
CSCdz88297	LegacyProtocols	Actlu req from dspu causes snasw to queue bind requests indefinitely
CSCdz88396	LegacyProtocols	IPX-3-TOOMANYNETS displayed early when using IPXWAN interfaces
CSCea09001	LegacyProtocols	SNASw new sessions fail 0855000F Route Setup Reply sent ISR not HPR
CSCea10024	LegacyProtocols	Snasw router crash in nss_queue_handler after host IPL (99% cpu)
CSCea21073	LegacyProtocols	SNASW is causing VTAM ABEND
CSCea24708	LegacyProtocols	Ping fails while testing x25 HIC and LOC
CSCea29740	LegacyProtocols	DLSw ER broken with 7200 FE drivers in isl and dot1q encapsulation
CSCea36624	LegacyProtocols	SNASw router reloads in nba_send_ips
CSCea58092	LegacyProtocols	SYS-2-INTSCHED after unshut of a FE from portchannel with SNASw conf
CSCea60815	LegacyProtocols	SNASw PU hung in PendActPu state after host IPL
CSCea62116	LegacyProtocols	Snasw hang/crash after show snasw link, show snasw ips command
CSCea66127	LegacyProtocols	ipx eigrp packets wedge the input q on 3725
CSCea71681	LegacyProtocols	Snasw does not send REQACTPU, PU stuck Pend Actpu
CSCdz32837	Management	RM: Resource Manager Spurious access in VSNPRINTF __DOPRNT
CSCdz49271	Management	CDP broken -not receiving incoming packets
CSCea34230	Management	Router crashes while doing config change and show of CAR same time
CSCdu70170	MPLS	More than 1 vrf can assign on 1 interface and lose all vrf
CSCdv44316	MPLS	tag-switching ip propogate-ttl not recognized by parser after reload
CSCdw06558	MPLS	E4P: GRP crashes immediately after disabling mpls te tunnels
CSCdw33267	MPLS	ip_force_resolve_path not called for all parallel paths
CSCdw88145	MPLS	BGP soft reconfig make tag as explicit-null
CSCdx31291	MPLS	internet access via global keyword broken if multiple paths to NH
CSCdy09335	MPLS	MPLS: BGP updates do not occur if static route is removed
CSCdy52958	MPLS	Can not ping HSRP address from different VRF

Identifier	Technology	Description
CSCdy71876	MPLS	13E/MPLS: Spurious memory access with alignment traceback with traff
CSCdz37137	MPLS	PE to PE connectivity lost due to xtag cross-connect in DOWN state
CSCdz37794	MPLS	After SSO cutover w LC-ATM, pings not passing through
CSCdz43747	MPLS	Local label does not bind after route flapping
CSCdz51987	MPLS	concurrent mpls cos-map config overwrites current class-map var
CSCdz54206	MPLS	Debug mpls packet breaks packet forwarding in HDLC encap
CSCdz57007	MPLS	vip/rp/7200/any alignment errors or crash, mpls feature path
CSCdz61780	MPLS	Unwanted route_tag_change causes TFIB entry del and 1 sec pack loss
CSCdz66770	MPLS	LDP: Label change is not propagated/conveyed to LDP peer
CSCdz69177	MPLS	spurious access at tfib_fib_scanner_walk
CSCdz69414	MPLS	mpls ldp neighbor command garbled after ip vrf removal
CSCdz72673	MPLS	C2Sup2: system crashed on tfib_check_fib_rewrite
CSCdz75075	MPLS	Inter-AS fails with LC-ATM on ASBR and IPV4 BGP+Label exchange
CSCdz75507	MPLS	CLI should prevent config of bridge-group on an mpls interface
CSCdz81619	MPLS	MPLS packets dropped as ignored with DCEF
CSCdz85866	MPLS	MPLS/VPN: PE might fail to import some VPN prefixes
CSCdz89449	MPLS	Const2: CSC PE RP crashed when removing VRF from int tdp_get_dhcb
CSCea00530	MPLS	MPLS LDP: Label Withdraw with no label not handled properly
CSCea05061	MPLS	BOOTREPLY sourced from wrong interface in RBE MPLS/VPN setup
CSCea07570	MPLS	RSP crash at rsp_fastsend, dmlppp & mpls
CSCea09270	MPLS	CSCdt32774 reintroduced in 12.2S
CSCea25707	MPLS	LDP-MIB crashes, watchdog forced crash, where v8 upgrade not present
CSCea25789	MPLS	LDP MIB, router crash, mib walk, where v8 upgrade not present
CSCea28100	MPLS	TDP does not use configured Hello holdtime and interval
CSCea28656	MPLS	Align-3-Spurious at tagsw_tx_pak in the router of CSC-PE/ASBR/PE
CSCea35117	MPLS	Spurious memory access at bgp_bestpath_compare_pair
CSCea37722	MPLS	All rip interface showed in show ip protocol vrf xxx
CSCea56819	MPLS	crash with link failover and EoMPLS&MPLS VPN traffic
CSCea58795	MPLS	Label leaking: after VPN routes removed vpn not release local label
CSCea72654	MPLS	MPLS VPN CSC PE RP crashed after booting 410 with 1k vpn
CSCea75235	MPLS	LSC switchover - second outage found during test
CSCea80474	MPLS	Const2:FW RP crash at @ ldp_pdu_group_msgs_for_xmit during shut/nosh
CSCea84736	MPLS	CONST2: Cannot ping after shut/no-shut on POS interface with MPLS en
CSCea86724	MPLS	MVPN: P router RP crash, when the LC with VRF on PE router, CPU hog
CSCeb28065	MPLS	CONST2/MPLS: RP crash at rn_walktree_timed with overnight traffic te
CSCuk36841	MPLS	PAKSTICK Traceback @ip_fastswitch_wrapper
CSCdt82560	Multicast	mroute-cache disabled upon reload or line flap with hw compression

Identifier	Technology	Description
CSCdw75696	Multicast	Watchdog timed out during freeing of large linecard FCB queues
CSCdy60995	Multicast	Router crash in PIM RP ager after show ip pim rp mapping
CSCdz16276	Multicast	DR does not register if it already has a (S,G) with Null Olist
CSCdz37639	Multicast	Const2: Hangup or crash because of invalid radix_node chain
CSCdz39544	Multicast	MSDP: encaped data pkt with more than 1 SA entry can cause problem
CSCdz48132	Multicast	UDLR should not require a static mroute to prevent RPF failure
CSCdz52552	Multicast	PIM: Router reload, traceback at free/pim_show_interface
CSCdz59039	Multicast	Const2: Proxy join timer not reset properly, prune is not sent
CSCdz62860	Multicast	Traceback at process_send_message on cfging a frame-relay interface.
CSCdz71127	Multicast	unexpected packet can cause input queue wedge - reg to CSCdx02283
CSCea01892	Multicast	multicast fast switching not used with NAT configured
CSCea13379	Multicast	Router sends (*,G) joins instead of (*,G) join with (S,G)R prune
CSCea26993	Multicast	Dense-mode Incorrectly Sets T-flag on (s,g) if Pkt Arrives on OIF
CSCea26995	Multicast	7400:LINK-3-BADMACREG: Interface Gig0/1.251, non-existent MACADDR
CSCea29313	Multicast	CLI typo : ip multicast longest-matcch
CSCea46477	Multicast	Packets punted on (S,G)R entry
CSCea53049	Multicast	PIM Bidir does not have correct mroute table after oir
CSCea79487	Multicast	Bus Error crash in pim_jp_build_packet - CSCea24630 not fixed
CSCeb29878	Multicast	Need no mls ip multicast for ATM subinterfaces in FlexWAN
CSCeb76929	Multicast	CE3-NATIVE: Removing mcast boundary will not resume restricted traff
CSCec06466	Multicast	Const2: Crash in midb_re_queue_sorted+38 during the complex test
CSCin31057	Multicast	Mcast code crashes when delete an sub-intf with HSRP&MCAST configed.
CSCdy11785	platform-72xx	c7206VXR bus error in printf and c7100_platform_show_env_last.
CSCdy27264	platform-72xx	PXF: Div/0 risk with police in child policy
CSCdy35153	platform-72xx	OIR, slow insertion of PA causes Error Interrupt at pci_config_read
CSCdy46150	platform-72xx	7200VXR/NPE400 malloc failures with 16mb IO and 256mb memory
CSCdy68922	platform-72xx	software forced crashed by block overrun
CSCdz23373	platform-72xx	PXF External memory exception with huge ACL
CSCdz47058	platform-72xx	Channel interface link recovery
CSCdz54538	platform-72xx	PXF: inconsistent counts in show ip cache flow
CSCdz56072	platform-72xx	i82543 Port Adapters send ISL frame with 4 extra bytes
CSCea17870	platform-72xx	need to cleanup pak on the pxf punt path
CSCea25265	platform-72xx	PXF crash when receiving large amounts of video streaming
CSCea26010	platform-72xx	7206 crashes when two PA are inserted
CSCea32437	platform-72xx	QoS policing on the Cisco 7200 NSE1 does not work
CSCea35403	platform-72xx	Discarded packets by input ACLs counted as output drops
CSCeb06567	platform-72xx	catastrophic pxf netflow problems

Identifier	Technology	Description
CSCin34382	platform-72xx	LAc router crashes at bus error exception
CSCdw49053	platform-74xx	Router crashed while reloading PB image
CSCin19645	platform-74xx	Failed to establish 50 pppoeoa sessions even after 30 minutes
CSCdx51367	platform-75xx	After reload some Mueslix serial interfaces do not come UP/UP
CSCdz24676	platform-75xx	LQRs and RSP value not in sync
CSCdz46018	platform-75xx	30 second input/output rate does not match byte count
CSCdz52713	platform-75xx	CEF switched packets cannot reset Last input/output counters
CSCdz70112	platform-75xx	NRT:RSP8 and RSP4+ freeze while unconfig MTU in AToM testing
CSCdz72611	platform-75xx	usecdelay function is not working correctly on 7500, 7200, c6k
CSCea21328	platform-75xx	VIP Crashinfo file left open
CSCin29078	platform-75xx	Need a mechanisum to recover from QA errors
CSCuk38757	platform-75xx	Problem with the Agents impl of the cardIfIndexTable
CSCds76128	platform-76xx	CWTLC POS: aps deselect message keeps rolling
CSCdx08807	platform-76xx	OSM:GE: 64 bit main interface counters are not supported
CSCdz41189	platform-76xx	13E3/PWAN2:VTMS[1]: queue failed to become idle,quid 0x9
CSCdz54502	platform-76xx	13E3: SROC packet length mismatch errors seen on linecard console
CSCdz58878	platform-76xx	13E3/PWAN2: LC crash due to vtms periodic on switchfabric oir
CSCdz62725	platform-76xx	BT: Static SVC no connectivity on BT main interface
CSCdz62748	platform-76xx	output drops seen on Gig Ethernet connection in the OSM module
CSCdz74052	platform-76xx	C2SUP2/FLO_ISP: Cannot ping between PE-CE after reload
CSCdz74625	platform-76xx	FLO_ISP/GBIC:scp_idprom_msg: BAD EEPROM on module xx errcode=1
CSCdz88585	platform-76xx	13E5/GBIC/GE-WAN2: Interface down with 1000baseT gbics
CSCea02472	platform-76xx	CWTLC Sup2:Flexwan Sup3 cbus-cmd timout and pwrcycles on relo
CSCea15044	platform-76xx	Cat6500 with OSM module is not replicating mcast packets
CSCea18690	platform-76xx	POS keeps sending RDI-P for 10sec. after AIS-P is stopped.
CSCea21791	platform-76xx	HSRP/VRF standby router forwards traffic going thru virtual addr
CSCea24413	platform-76xx	BB: Input drops not accounted for in show int output
CSCea34141	platform-76xx	CWTLC:PR(OC3): 16 ports active lower perf than 8 ports
CSCea41242	platform-76xx	UCODE:CWTLC: OSM crashed with null OPCODE in src_mac magic
CSCea45053	platform-76xx	packets to unknown MAC are routed back incorrectly by GE-WAN
CSCea59633	platform-76xx	HSRP and override MAC should be available on same intf
CSCea76234	platform-76xx	Output drops seen on Gig Ethernet connection in the OSM module
CSCea78519	platform-76xx	Const2:DB-stats not updated from toaster to linecard
CSCea79793	platform-76xx	VLAN ID greater than 1005 not configurable under GE-WAN dot1Q
CSCea79844	platform-76xx	Override MAC writes top 4 bytes of Router MAC to zeroes
CSCeb00632	platform-76xx	IP PIM multipoint signaling needs to be removed from ATM-OSM CLIonly
CSCeb04954	platform-76xx	local bus congestion on G+ card causes LDP flaps over PWAN2 OSM

Identifier	Technology	Description
CSCeb13114	platform-76xx	OSM-POS card crashes on snmp stats clear
CSCeb16918	platform-76xx	disable Sculptor->Valllen flow control to protect control pkts
CSCeb18694	platform-76xx	CONST2/oc48:TxSOP crash with fatal management errors during traffic
CSCeb31997	platform-76xx	OAM VCs not created on the LC when PVP is configured
CSCin35353	platform-76xx	POS interfaces fails to come up with keepalive using FR encap
CSCin37112	platform-76xx	c2sup2:PWAN2: OSM LC unexpectedly power cycles when reset fabric Mod
CSCdy62423	PPP	Bridging lat/mop across a PPP link truncates 4 bytes
CSCdy76871	PPP	MPLS packets fail when one E1 of a multilink bundle of 2E1 fails
CSCdz51400	PPP	Per-user route not removed after diconnection
CSCdz56776	PPP	Outgoing PPP frames are stuck on MLPPP
CSCdz65797	PPP	AUTHOR/FSM: Internal state is invalid messages in log
CSCdz65899	PPP	SYS-3-CPUHOG Task Ran for 2480 msec Multilink
CSCdz76361	PPP	7200/VXR: MLPPP is not working with CEF (due to punt adj)
CSCea01472	PPP	VIP2-50 crash at ce3_exit
CSCea16664	PPP	Distributed multilink PPP results in a VIP buffer header leak
CSCea38803	PPP	Const2:FW RP crashed at ppp_send_packet on moving the member
CSCea38851	PPP	RP crashed at mlp_fastswitch_les on peer chassis reload.
CSCea39238	PPP	dLFIoATM never comes up on interface flap and VIP crash
CSCea53696	PPP	FW STM-1 MM PA crashed after applying CBWFQ on a mlppp bundle
CSCea60211	PPP	Const2:RP crashed @ mlp_fragment on adding a mem to a mlp bundle.
CSCea72496	PPP	Alignment error in PPPoE switching path.
CSCea73586	PPP	FW ATM E3 crashes cont with traff @ dlfi_atm_bundle_process
CSCec00268	PPP	Input drops and * throttles on PPP multilink interface
CSCin08082	PPP	IOS MLP crash @ mlp_clear_group while uncfg multilink-group
CSCin21688	PPP	Ingress counters for primary member link of multilink is double
CSCin36465	PPP	Router crashes when re-adding member in the multilink bundle
CSCin40374	PPP	C2Sup3 : dlfi related counters problems
CSCin44386	PPP	Multilink interface flaps after a router reload
CSCin46014	PPP	dLIoATM QoS : VIP crash at dlfi_do_fragment and runs out o memory
CSCin50167	PPP	dLFI broken after CSCin46014
CSCin50541	PPP	7200 and 7500 Routers crash when ppp multilink is configured
CSCdy47547	QoS	dTS increases output rate too quickly if no BECN received
CSCdy63247	QoS	high latency for MQC bandwidth class when c default with many flows
CSCdy78032	QoS	Can not recognized properly queuing type in sh queuing int virtual
CSCdy82043	QoS	VIP2-50 with PA-MC-8E1 crashes when issueing MLPPP commands
CSCdy87453	QoS	ip fragments are not classified properly for output queueing feature
CSCdz04423	QoS	CPUHOG when activating NBAR

Identifier	Technology	Description
CSCdz10519	QoS	Delayed boot-up due to QoS and dcef
CSCdz25848	QoS	Corrupted WRED DSCP counters in show policy interface CLI
CSCdz33759	QoS	router crashes while setting frame-relay cir
CSCdz40273	QoS	Support for finer grained scheduling
CSCdz41092	QoS	Spurious memory accesses at custom_dequeue
CSCdz50199	QoS	Router crashes when service policy is configured.
CSCdz51865	QoS	Router may reload if policymap/class-map is accessed simultaneously
CSCdz53696	QoS	RSVP: ResvError crashes the router
CSCdz64355	QoS	7500:Crash Attempted to free memory at D0D0D0D,no part of buffer
CSCdz68710	QoS	cosmos_e : Qos: Watchdog timeout at hqf_reset_all_blts_recursive
CSCdz74130	QoS	RSVP: Memory corruption crash while processing incoming PATH
CSCdz78276	QoS	Input policing and input acl with log causes input packet loss
CSCdz88368	QoS	Attaching nonexistant policy map to ATM subinterface
CSCdz89370	QoS	No more than 14% bandwidth can be reserved on GigabitEthernet int
CSCea02713	QoS	Bus error in fair_queue_update_class after malloc fail
CSCea06507	QoS	cant attach input shaping class to multiple FR DLCIs
CSCea06563	QoS	TE LSP does not come up after changing encapsulation HDLC to PPP
CSCea07020	QoS	Memory leak when configuring frame-relay WRED
CSCea07778	QoS	router reload @add_to_hunt_group.
CSCea11008	QoS	VIP crash if virtual interface is down which has policy with priorit
CSCea12346	QoS	Incorrect BW Allocation for CBWFQ
CSCea24835	QoS	adding priority in attched policy stops traffic from other classes
CSCea33288	QoS	Router reloads at qos_set_mark_wrapper
CSCea37783	QoS	Interleaving not functional on Mx Serial PA, 8 ports
CSCea47462	QoS	CPHUHOG on show shape queue
CSCea50942	QoS	set qos-group not working on MPLS P-router for atm p2p vc
CSCea55600	QoS	Serial Interface goes down/down on bootup.
CSCea66323	QoS	MPLS-TE: midpoint router crash after changing bandwidth at ingress
CSCeb08388	QoS	Pagent traffic dies down when QoS policy is applied to the DUT int.
CSCec03896	QoS	HQF: large packets not fragmented by FRF.12 when policy is enabled
CSCec27278	QoS	Memory leak in hqf_rp_mlp_blt_setup
CSCin28688	QoS	No drop via random-detect in ATM(OC3) Subinterface
CSCin39504	QoS	BADMAGIC detected by validblock_diagnose while removing the policy
CSCdt45079	Routing	OSPF: forwarding address in LSAs might be not updated on cfg changes
CSCdu06914	Routing	%IP-3-DESTHOST logged intermittently
CSCdv36378	Routing	BGP outbound route-map with next-hop or update-source supress update
CSCdw50797	Routing	GRP Bus Error crash in bgp_print_entry

Identifier	Technology	Description
CSCdw84055	Routing	EIGRP MD5 Authentication Broken
CSCdx42845	Routing	%Address-family not configure Message Seen
CSCdx81633	Routing	MLS entries not updated when the route changes in the routing table
CSCdx95505	Routing	BGP: a redistribute with a route-map is not applied automatically
CSCdy04087	Routing	OSPF RT extended community has wrong value (negative or too high)
CSCdy24940	Routing	bus error at prune_ndb_idb
CSCdy40742	Routing	CPU high after BGP reset when default-metric is configured
CSCdy80496	Routing	Disappearing the route even existing on the topology table
CSCdz11578	Routing	connected routes might be missing from EIGRP topology
CSCdz20796	Routing	No passive-interface commands in config after sub-ints are created
CSCdz21986	Routing	Redistribution of newly added static routes fails
CSCdz25963	Routing	Unequal cost load sharing does not work properly on E2 and E3
CSCdz29788	Routing	Adjacencies does not come back after beginning new adj table epoch
CSCdz30390	Routing	static with next hop network not removed when component missing
CSCdz38203	Routing	Inter-AS: Asbr advertises wrong next-hop for some VPNV4 prefixes
CSCdz39896	Routing	Pri does not reconnect with ip verify unicast reverse-path
CSCdz41087	Routing	EIGRP:Connected interface not in topology table
CSCdz41310	Routing	Const2 - Memory fragmentation on RP after route flaps
CSCdz45760	Routing	OSPF LSA refresh should not cause partial SPF
CSCdz56772	Routing	CEFv6 crash when i/f state changes & connected prefix is deleted
CSCdz58047	Routing	BGP: match ip next-hop does not work for non-IPv4 prefixes
CSCdz58674	Routing	OSPF ABR generates illegal type 4 LSA
CSCdz61787	Routing	ISIS BACKUPOVFL loop : endless SPF (every SPF Interval)
CSCdz63695	Routing	Problem redistributing RIP routes into EIGRP using Route-map
CSCdz67496	Routing	OSPF thinks Tunnel interface is down after reload.
CSCdz69000	Routing	VIP4-80 running 12.2(8)T4 crashes with CYASIC Error Interrupt
CSCdz69295	Routing	ISIS IPv6 crash with multiple next-hops
CSCdz70283	Routing	crash seen at bgp_neighbor_change
CSCdz71295	Routing	Bad voice quality after several calls with CRTP
CSCdz74211	Routing	FLO_ISP: SP crashes after running L2 and L3 traffic
CSCdz76611	Routing	Router crash when remove static EIGRP neighbor statement
CSCdz77470	Routing	ipv6 address gets truncated in sh bgp ipv6 summary
CSCdz77777	Routing	software forced crash on a router after clear ip bgp
CSCdz82284	Routing	Partial flag set on db without partial spf happening
CSCdz84521	Routing	SPD broken in 7200 & rpm
CSCdz88636	Routing	bgp table inconsistent before and after clear ip bgp
CSCea00377	Routing	IPv6 CEF: Adjacency Incomplete on FDDI

Identifier	Technology	Description
CSCea01062	Routing	GSR crashed while issuing show clns interface
CSCea01840	Routing	High CPU BGP scanner
CSCea02355	Routing	rare ip packets may cause input queue wedge
CSCea03198	Routing	SYS-2-INPUTQ: no IDB traceback if netflow packet enqueued to process
CSCea03212	Routing	sh ipv6 traffic is not count up when 6pe uses
CSCea11704	Routing	crash seen at bgp_find_next_nbr()
CSCea13075	Routing	MED is not being send across confedration eBGP
CSCea14412	Routing	Crash after distribute-list command entered
CSCea17037	Routing	Queries sent to stub remotes even after CSCdy65263
CSCea19236	Routing	router reload at bgp_routemap_check_internal
CSCea22310	Routing	nhrp auth config causes crash if 8 character string is exceeded
CSCea24313	Routing	ipv6 floating default route leads route flapping
CSCea24421	Routing	ISIS not load balancing correctly
CSCea26842	Routing	IOS crashed when acl removed
CSCea28131	Routing	router crashes upon rcv invalid packet
CSCea28472	Routing	show extended channel command causes CIP Utilization of 95%
CSCea35193	Routing	ACK for duplicate DBD request not sent by SLAVE
CSCea39371	Routing	Bus error in turbo_extended_check with compiled ACLs
CSCea40722	Routing	Tarp resolve command doesnt work
CSCea42500	Routing	BGP: default route not being advertised by BGP under vrfs
CSCea43167	Routing	BGP enabled on reload can cause OSPF instability
CSCea44570	Routing	IS-IS passive-interface not work
CSCea48609	Routing	show ipv6 traffic counts forwarded packet as Received
CSCea59374	Routing	Spurious access when NetFlow exports needs to be fragmented
CSCea93577	Routing	C10720: chunk_refcount crash in 6PE InterAS during clean_up
CSCeb04048	Routing	Upgrading/reloading IOS may cause OSPF interfaces/neighbors down
CSCeb19857	Routing	router crash on reload at ip_def_metric_configured()
CSCeb24407	Routing	Link-local address configured not shows after reload/swtover
CSCeb65685	Routing	ip cef load-sharing algorithm tunnel command lost upon reset of rpm-
CSCeb80992	Routing	Crash when ACL counters are sent from the LC to the RP
CSCec03066	Routing	Const2:IPv6:static route not removed from routing table
CSCec27239	Routing	OSPFv3: RP crashed in DoToAllChildren remove use-bia feature and wr
CSCin11611	Routing	IPX EIGRP will not establish adjacencies using SAP incremental
CSCin29995	Routing	is_rtp_header failed msg observed during shut, no shut of ctrl
CSCin40371	Routing	With no ip cef, ping to 20 net failing with 60% success
CSCin52817	Routing	OSPF: Router may reload on manually reloading the router
CSCuk40771	Routing	dCEFv6: distributed switching ipv6 pkts can cause some VIPs to crash

Identifier	Technology	Description
CSCdx05703	Security	Communication brakes when WCCP+CBAC is ena togather in some situatio
CSCdx22576	Security	VSEC: rsa-encr broken when VAM is active
CSCdx74855	Security	Cannot ping IP address of local GRE tunnel interface
CSCdx84417	Security	Peer crashes when clearing tcb for a STUN connection
CSCdy29077	Security	With fast switching, NAT and inspect final TCP ACK not forwarded
CSCdy79517	Security	VSEC:VPN-SM:RP crashed during hw stress test deconfig.
CSCdz54555	Security	Intermitten ISA card reset
CSCdz56722	Security	SegV exception, PC 0x8019C08C with Firewall Feature Set
CSCdz60229	Security	SSHredder SSH DoS Tool Reboots Router without Authentication
CSCdz74538	Security	VSEC:VAM anti-replay fw check needed on VAM
CSCdz78239	Security	ISA card reset trigger tunnel drops and router crash
CSCdz89852	Security	Preshared key with VAM limited to 64 byte size
CSCea00475	Security	GRE: frame-relay encapsulated frames get corrupted on decapsulation
CSCea17079	Security	VSEC:VAM2 Align Error and Spurious memory access
CSCea19444	Security	System crashed under stress with 500 tunnels
CSCea26901	Security	cbac inspection idle-timeout killing live sqlnet sessions
CSCea30449	Security	SSH Client source port shouldnt falls within 1-1023
CSCea31844	Security	TE tunnel has unexpected no route-cache config w/out configing it
CSCea32392	Security	Huge HTTP downloads fail when using auth-proxy and inspect
CSCea40426	Security	VAM encr/decr error:Other Error for some MTUs
CSCea56559	Security	1700 crash on boot in crypto_rng
CSCeb01608	Security	Inbound SSH sessions hang with debugs and term mon
CSCdw17400	Telephony	Transcoding: One way audio between 711A GW and 729/723 IP Phone
CSCdt30513	Unknown	radius password length is non-compliant with RFC 2865
CSCdw13108	Unknown	MOC: static arp does not work, ltl not updated correctly
CSCdw24379	Unknown	RADIUS attribute Framed-Filter attribute parsing incorrect
CSCdw36564	Unknown	CES: Unrecoverable Red Alarm (Loss of Signal) on 3600
CSCdw48796	Unknown	AutoInstall fails with the NM-4A/S
CSCdw59505	Unknown	need IOS CLI to make noise threshold a configurable option
CSCdw72560	Unknown	Customer cant configure differnt speed in s0 and S1 when doing CES.
CSCdx04081	Unknown	controller t1 reports line code violations
CSCdx22012	Unknown	Router crashes on moving bgp update-source int from global->any vrf
CSCdx23388	Unknown	Router crashes at rs8234_oam_receive_complete
CSCdx27398	Unknown	Hubble:all non dfc cards medusas are not sending mac notifications
CSCdx31265	Unknown	Dial FTP throughput on a downlink may degrade by 18 percent
CSCdx60079	Unknown	VIP crashes after configuring feature accel and netflow
CSCdx73043	Unknown	resource monitor not updating ds0 inuse channels for first isdn call

Identifier	Technology	Description
CSCdx86585	Unknown	Support for CP tone in the Czech republic
CSCdy03042	Unknown	cefcFRURemoved/cefcFRUInserted are missing on removing/insertingGBIC
CSCdy10714	Unknown	A config of a removed LC is not reflected on other LCs
CSCdy11767	Unknown	Disabling dot1qtunnel tagged frame still go through the link
CSCdy13419	Unknown	vpn accel dropping 1500 byte packets with df bit clear
CSCdy15369	Unknown	CWAN-QOS:class-default shouldnt have CIR = LR when QoS is applied
CSCdy18970	Unknown	Bus error at csm_send_event
CSCdy20760	Unknown	Software Forced Crash due to watchdog timeout(mai_modem_autotest)
CSCdy21998	Unknown	12e/13e: TFIB scan not completing messages on RP Console
CSCdy24304	Unknown	NM-1A-T3/E3 may stop passing traffic
CSCdy28282	Unknown	CWAN-QOS: police w/ drop action doesnt work for router gen. packets
CSCdy31164	Unknown	FIB: CEF disabled on the VIP (CEF-IPC: Unable to get the port info)
CSCdy34419	Unknown	Getting %DS_MODEM-3-LOW_PARTICLES:Not enough particles messages
CSCdy45007	Unknown	E1/R2 GW sends Answer Line Signal before B6 Signal ends
CSCdy47266	Unknown	Vortex:second fan-tray & clock entry miss from entPhysicalTable
CSCdy47341	Unknown	no tag-switching ip propagate-ttl still copy MPLS ttls to IP pac
CSCdy47789	Unknown	Non-directed LDP neighbors showing up under targetted discovery list
CSCdy49957	Unknown	12.1(13E): modules get wrongly power denied when PS fails
CSCdy55352	Unknown	Initial punting due to T flag not being set on ssm mroute entry
CSCdy55543	Unknown	IOS - msfc/msfc2 delayed or not booting from sup-slot0, 13E5, etc.
CSCdy57025	Unknown	13e: mem leak-proc=RPC draco-oir;pclc_g2_fw_admin_status_down_notifi
CSCdy59007	Unknown	Crashinfo on AS5400 does not include dump of corrupt memory blocks
CSCdy70191	Unknown	c1751 running 12.2T doesnt generate Cold Start Traps on Power up
CSCdy72977	Unknown	EAP MD5 (802.1x) RADIUS authentication fail
CSCdy81201	Unknown	crash in caim_complete_packet
CSCdy84113	Unknown	With dual sups, broadcast supp command returns 0 value
CSCdy84560	Unknown	C-HYB+HA_SRM: two switchover in 1 min makes cat6k send no packet
CSCdy86668	Unknown	spurious memory access made at is_caim_handle during ISDN/MLP call
CSCdz01387	Unknown	Spurious memory accesses after questioning cbQos MIB
CSCdz08234	Unknown	PA-MC-STM1:LP-RFI alarm cannot be disabled
CSCdz09522	Unknown	MSFC2-3-MISTRAL_BAD_PAK
CSCdz09551	Unknown	Tracebacks at aaa_acct_attr_add -- same as bug CSCdx85827
CSCdz15598	Unknown	VTSP should not pass bogus codec_bytes to crash dsps.
CSCdz19404	Unknown	CWAN-QOS: OSM crashes when heirarchical policy applied to main i/f
CSCdz19517	Unknown	LLQ-BC not engaging & sh cry eng qos not showing QoS counters
CSCdz21419	Unknown	Incorrect OIR-SP-3-PWRCYCLE reason
CSCdz21534	Unknown	T1 remote line loopback fails on CT3 card

Identifier	Technology	Description
CSCdz21587	Unknown	no mls 0.0.0.0/0 entry when non-zero default wins over 0.0.0.0
CSCdz24904	Unknown	helper-map group-address is helpering broadcast traffic also
CSCdz27636	Unknown	NDE: Add unique engine ID for PFC2 exported traffic
CSCdz28754	Unknown	No status change logs dont come up in MST environment
CSCdz28877	Unknown	dialin user remain conn/dead if tacacs acl not there
CSCdz29883	Unknown	Mac Notification: L3 traffic loss with a L2 etherchannel across DFCs
CSCdz30206	Unknown	12.1(13)E1: buffer leak middle pool due to Remote Console Process
CSCdz30644	Unknown	bus error in deref_pathadj in native ios
CSCdz30790	Unknown	T3 controller link up/down traps not sent for snmp
CSCdz31376	Unknown	VIP crashes on configuring feature acceleration and dcef and cef
CSCdz32064	Unknown	MSFC: loadprog: bad file magic number: 0x0
CSCdz34982	Unknown	gre/ipsec with hardware card intermittently stops passing traffic
CSCdz35884	Unknown	NPE-G1 drops packets > 1498 even with tag mtu 1508
CSCdz36181	Unknown	PBR set interface Null 0 doesnot work in HW for Earl6
CSCdz39487	Unknown	CE interface is up even when the remote end is down
CSCdz40050	Unknown	Wrong syslog message sent when PSU is removed
CSCdz40232	Unknown	DSP does not respond when scheduler command is enabled
CSCdz40248	Unknown	CWAN-QOS: BT Traffic shaping not work with flo11e image
CSCdz40483	Unknown	%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = IP I
CSCdz40971	Unknown	Unable to SSH directly to real servers after configuring SLB
CSCdz41650	Unknown	Lack of ip connectivity during few sec/min not reported as Lost pckt
CSCdz42307	Unknown	Multicast packets being routed when multicast routing is not enabled
CSCdz42549	Unknown	%CLS-3-BOGUSOP: Unknown CLS verb for STATION context.....
CSCdz43519	Unknown	VOICE-IF-MIB not populated with ISDN BRI info
CSCdz45188	Unknown	V110 callin-failure disable other callin
CSCdz46370	Unknown	CE1-HYB: Spurious memory access at const_fib_proc_sp_req_ipx_reload
CSCdz49099	Unknown	Called number gets overwritten between CCAPI layer and ISDN stack
CSCdz49276	Unknown	AGM: Gig0/0 intf throttles when rtp traffic received on wrong port
CSCdz50453	Unknown	Failed to send RPC request mapping_sp:get_current_mappings
CSCdz51275	Unknown	Memory leak in Buffer pool process packet header
CSCdz51932	Unknown	Reload after delete ACL that is used for crypto
CSCdz52398	Unknown	vrf not cleared when chE1 is removed
CSCdz52963	Unknown	c2600:ifType of ATM25 port adapter is invalid
CSCdz53958	Unknown	Setting cdpInterfaceEnable port in a channel=false reset switch
CSCdz54333	Unknown	incorrect unicast flooding seen on switchports
CSCdz55608	Unknown	memory leak in Crypto ACL
CSCdz55647	Unknown	RPR plus redundancy can not work for inter-vlan L3 traffic with ACL

Identifier	Technology	Description
CSCdz56987	Unknown	Configure ACL on channel member int break ACL on the L3 channel int
CSCdz57158	Unknown	Incorrect supervisor model and s/n displayed for sup
CSCdz58142	Unknown	%BSC-3-BADLINESTATE: Line state Tx when receiving xxx on line Serial
CSCdz58247	Unknown	Extensive frame loss upon link rejoining GEC with PAGP
CSCdz59003	Unknown	DE bit mapping for FR-ATM internetwoking is broken.
CSCdz59578	Unknown	IOS should give DSP more time for codec download
CSCdz59821	Unknown	TCP intercept connections are getting reset after 24 hrs
CSCdz60032	Unknown	SMTP reports unknown error mesage 554 when doing offramp with VXML
CSCdz60980	Unknown	Download through sup-slot0/sup-disk0 fails - checksum incorrect
CSCdz61466	Unknown	AIM VPN/MP not encrypting/decrypting packets
CSCdz62845	Unknown	Cronos:APS switchover causes RP to crash, high CPU util
CSCdz63050	Unknown	NPE-G1:Output drop and bad length count up
CSCdz65299	Unknown	Bus Error crash in ipmulticast-loopback, ipsendnet, ipwrite
CSCdz66347	Unknown	On reload, static multicast L2 entry not processed by igmp-snooping
CSCdz66927	Unknown	Voice-ports Hung and Digits not being pulsed out
CSCdz67182	Unknown	CWAN-QOS:PFC aggregate policing not work for cwtlc
CSCdz68529	Unknown	Got EARL-SP-5-EXCESSIVE_INTR:
CSCdz69161	Unknown	Reoccurance of CSCdz21420
CSCdz69690	Unknown	PRI T1 voice ports are down. Incoming calls fail
CSCdz69965	Unknown	VSEC:VPN-SM:RP/SP crash after reloading with 800 tunnels
CSCdz70721	Unknown	No Mls-cef entry for dynamically learned default enty via EIGRP.
CSCdz71296	Unknown	Removing template while configured on another tty reloads router
CSCdz71663	Unknown	5300 DSPRM dsp boot-up double-load recovery alarms problems.
CSCdz73517	Unknown	Channelised STM1 SMI PA reports line type as Multimode
CSCdz74155	Unknown	NM-HDV: Router crashes during booting sequence after reload command.
CSCdz74603	Unknown	spurious memory access in qde_get_ctrs_from_cmap_list
CSCdz76292	Unknown	Crash configing fair-que/no fair-que during stress test
CSCdz76588	Unknown	13E: RPC call failure under stress condition
CSCdz76698	Unknown	flo_isp: Sending 1000 multicast traffic, sp get Seg violation
CSCdz79139	Unknown	BGP convergence fails with FIB Control Task taking 100% CPU
CSCdz81658	Unknown	NPE-G1: Increasing MTU may cause native GE port receive ring lockup
CSCdz83037	Unknown	flo_isp/BCP:Show mac-address-table static interface is not working
CSCdz84447	Unknown	show vlan leads to high interupt driven CPU load
CSCdz85694	Unknown	SYS-2-INTSCHED: may_suspend when changing GigE config on NPE-G1
CSCdz85729	Unknown	PA-MC-STM1:E1s are not synchronized with STM1 frame
CSCdz86512	Unknown	CE1-HYB:OC12 POS card not recognised when changing from NDR to DR
CSCdz87238	Unknown	SLB: http probe GET requests not specific about file requested

Identifier	Technology	Description
CSCdz88518	Unknown	VRF-Lite not supported in Hybrid
CSCdz89162	Unknown	PWAN:Mcast packets are not hardware switched if changing ISL to .1Q
CSCdz89258	Unknown	Traffic stops after BGP prim to sec peer failover with large ACL
CSCdz90377	Unknown	spurious error at hal_tx_interrupt
CSCdz90594	Unknown	OC-48 DPT only sends multicast packets out side-A
CSCea00720	Unknown	CPU of DR goes high when hit by high rate Non-RPF dense mode traffic
CSCea01505	Unknown	Supervisor22 and DFC EOBC retry timer workaround (improved version)
CSCea02291	Unknown	RSP crashes at tagsw_flow_get
CSCea02680	Unknown	Output packet counter for SVI is incorrect
CSCea02744	Unknown	Ignore-dcd does not function on 3620 serial WIC modules
CSCea03617	Unknown	AIM-VPNII - disabled on boot up
CSCea04706	Unknown	Dangling DSP on AS5300 - DSP resource recovery
CSCea05105	Unknown	13E4:QoS:Sup2CR:cannot configure COS-MAP on uplink ports
CSCea06319	Unknown	backup commands removed from serial interface after reload
CSCea07370	Unknown	output drops when using PXF due to matches against ACL
CSCea07557	Unknown	SPD does not work on AS5300 Fast Ethernet
CSCea07643	Unknown	13E:CWAN_QOS:4Mb shaping granularity on PWAN2 is too limited
CSCea07970	Unknown	Various Trap issues in RPR, RPR+, OIR Standby Sup, etc.
CSCea09302	Unknown	RP crashes in pimv2_send_refresh when switch dense->bidir
CSCea09674	Unknown	Busyout (slot) with CT3 DFC drops all calls
CSCea11485	Unknown	Probe sends arp requests to remote real servers
CSCea13771	Unknown	ubr7100 may crash upon reload
CSCea14557	Unknown	Voice path is not cut through by SETUP_ACK
CSCea15290	Unknown	Const2:allow-default in uRPF isnt preserved in RPR+ setup
CSCea15655	Unknown	CDP neighbors for port-channels show same local interface for member
CSCea15963	Unknown	MVPN: Redundant PE sends duplicate MDT-joins
CSCea17364	Unknown	ODM breaks VACL capture
CSCea18561	Unknown	Static Multicast CAM entry disappears from the mac-addr-table
CSCea20948	Unknown	Bridging over PPP broken on rsp-pv-mz (and other images)
CSCea21064	Unknown	IDMGR-3-INVALID_ID: bad id to id_to_ptr Traceback message is seen
CSCea21781	Unknown	PBR not working in HW (hardware) with SUP2/MSFC2
CSCea25622	Unknown	NPE-G1 - Reset by hardware watchdog timeout with no traceback
CSCea26983	Unknown	GRE doent work with PXF
CSCea27037	Unknown	Unknown CPU displayed on NPE-G1(CPU:SB-1)
CSCea27138	Unknown	MVPN: MDT-data mappings on recv PE not deleted, bad refcount.
CSCea27336	Unknown	ACL with deny port eq 0 block non-initial fragmented packets
CSCea27431	Unknown	Sup1/Sup2 IOS cant ping CMM and vice versa

Identifier	Technology	Description
CSCea28325	Unknown	Fix build breakage due to CSCdx33049
CSCea28471	Unknown	VIP crash in tagsw_flow_get, at bootup or steady-state
CSCea28575	Unknown	OSM-4GE-WAN-GBIC module returns incorrect portType
CSCea29849	Unknown	Cef receive breaks with decnet config changes
CSCea31842	Unknown	HA2: Active SP crashes in VTP code for stack memory running low
CSCea34259	Unknown	Mpls netflow egress on ATM sub-intf turns on ldp address-message
CSCea35846	Unknown	Const2: No PVID, type incon, root or loop inconsistency generated
CSCea37725	Unknown	MPLS:VPN:CHOCx:MLPPP:No connectivity over Proton int. in ce-pe link
CSCea37935	Unknown	SLB VIP not responding to pings with FWLB.
CSCea38189	Unknown	config from tftp broken service config missing from show run
CSCea38945	Unknown	NPEG1: PA-2FEISL-TX crashes upon bootup or noshut
CSCea39298	Unknown	7600: sub-int ifIndex disappears when modifying vlan encapsulation
CSCea39633	Unknown	MSFC2 experiences bus error exception - const_fib_enqueue_fib_req
CSCea40015	Unknown	Native: VTP Transparent switch passes update from diff domain
CSCea41123	Unknown	Loopback receive CEF entry not present in Sup2 CEF table.
CSCea41980	Unknown	Catalyst 6000 Native crashes with Failed to send RPC request msg
CSCea42188	Unknown	autostate interoperability with lb and sensors
CSCea42504	Unknown	ICMP fail across L3 EtherChannel
CSCea43709	Unknown	Const2:Show mac-address does not respond from RP
CSCea43871	Unknown	PA-MC-STM loop on sonetPathIntervalESs
CSCea44864	Unknown	Const2:locIfCollisions return negative value for l3 vlan.
CSCea45950	Unknown	VLAN-do-not-learn-bit set for active vlan --> unicast flooding
CSCea46236	Unknown	12.1(13E): excessive collisions on EOBC channel
CSCea47314	Unknown	not able to autoboot when all vlans are down
CSCea47607	Unknown	Delay in dispatching data received on asynch WIC-2A/S interface
CSCea48170	Unknown	IOS-SLB RLB casa replication causes memory corruption and reload.
CSCea50623	Unknown	C-NATIVE: Sup11: Crash in c7100_dma_pack_coalesce in send mcast pack
CSCea51320	Unknown	MSFC2 crashes with Illegal access to a low address with IP inspect
CSCea54148	Unknown	Need tag2tag load balancing on OSM and Flexwan .
CSCea54756	Unknown	HSRP preempt causes high cpu when slb inservice standby configured
CSCea56746	Unknown	DMFR unreliable under load - %SYS-2-INLIST: Buffer in list
CSCea59575	Unknown	L2 entries dont age out after disabling and then reenabling aging
CSCea59922	Unknown	Bcast and MultiCast 64 bit counters not working on GE-WAN main int.
CSCea60527	Unknown	FWSM: Vlan 1 not working with MP , so image download fails
CSCea61460	Unknown	C2:failed to assign rate limiter to multicast non-rpf, #3 was free
CSCea61966	Unknown	IOS-SLB: RLB backup with sticky radius username may reload.
CSCea62217	Unknown	Wedged queue if inbound CAR is configured

Identifier	Technology	Description
CSCea62335	Unknown	Clear ip route all causes CPUHOG & core dump
CSCea63521	Unknown	Catos mistp bpdu not tunneled thru switch running IOS
CSCea64751	Unknown	router reload when DSL interface uses s/w with CSCdz51275
CSCea65695	Unknown	FW STM-1 PA crashed @ vip_mlp_ip_fib on starting the traffic.
CSCea66858	Unknown	%SM-SP-4-BADEVENT: Event insert is invalid Standby gone
CSCea67226	Unknown	Cat6000:With large number of NAT overload flows recir paks FIB switc
CSCea68988	Unknown	BPDU with old root bridge priority sent after max age expiry
CSCea69116	Unknown	L2/L3 switched counters remain 0 in sh int vlan
CSCea69334	Unknown	C2: ifIndex does NOT persist after RPR+ switchover and reload
CSCea70621	Unknown	VELA-SP-4-ERR_INTRPT: Interrupt ST_OVL_ERR reoccuring log message
CSCea71481	Unknown	ISIS doesnt work over GRE tunnel
CSCea71694	Unknown	Native 6500 Nam2 Module causes Autostate not to work
CSCea72405	Unknown	multicast static L2 entries not processed correctly
CSCea72468	Unknown	EoMPLS vlan needs to allow output shaping policy on CLI
CSCea72525	Unknown	Const2: default send by FM breaks feat asso betw primary & sec pvlan
CSCea72771	Unknown	netflow stats are not accurate with low fast aging times
CSCea79633	Unknown	13E: Sup crash when GBIC module is removed and stp portfast is chang
CSCea80062	Unknown	Many esp_seq_fail with MLPPP and hardware locks IPSec tunnel up
CSCea80221	Unknown	19E : Multicast traffic process switched after OIR
CSCea82353	Unknown	PIM Register & Register stop messages are looped until TTL expires
CSCea82782	Unknown	CE2-HYB:Creating 1000 vlan on RP in srm mode, resets RP
CSCea83414	Unknown	stack-mib portname command gets erased upon reboot
CSCea83603	Unknown	NDE sends ARPs when NFC is on remote network
CSCea84940	Unknown	Cannot route between 1483 PVCs in different VLANs on ATM OSM
CSCea85251	Unknown	no mls ip cef arp-throttling not NVGENed and disappears from config
CSCea85883	Unknown	Multicast flows may become software switched after rapid OIF changes
CSCea86541	Unknown	flowmask changes not enforced on command line
CSCea87362	Unknown	DMFR does not work with fast switched traffic
CSCea87671	Unknown	MPLS-QoS marking problem on PE
CSCea88502	Unknown	Proton:NXDS0 flap with LC reload while unidir traffic is flowing
CSCea89099	Unknown	after WS-X6816 reset, L3 traffic to HSRP mac, into 6816 SW switched
CSCea89468	Unknown	Continuous link flaps on port on a WS-x6348 module
CSCea90470	Unknown	Native: WS-X6348-RJ-21 no link after dis/re-connect IBM FE OSA/E
CSCea91600	Unknown	19E/C2SUP2:clear mac-add dyn int stops packet switching
CSCea93328	Unknown	mrouter configurations has no effect after reload and shut/no shut
CSCeb00126	Unknown	Default route learnt via routing protocol not updated on switch-side
CSCeb00351	Unknown	IOS-SLB: RLB - cisco msid-based access problems with HA Acct.

Identifier	Technology	Description
CSCeb00678	Unknown	sup crash while making csm config changes
CSCeb03367	Unknown	router reloads in bundle mode config at atm_getvc with SYS-3-CPUHOG
CSCeb03414	Unknown	const2: BPnfpoe index not cleared on receiving leave on port
CSCeb04343	Unknown	Fragmented Packets matching deny ACE with no L4 ports fwded in HW
CSCeb05093	Unknown	Switch may reload if insufficient initial memory for SLB.
CSCeb05464	Unknown	Some routed frames are dropped on the GEC/dot1q trunk over DFC modul
CSCeb05517	Unknown	boot variable is not added or overwriten
CSCeb05672	Unknown	SLB processed switch packets are dropped in router.
CSCeb05818	Unknown	19e: vlans ifIndex not synced to NAM
CSCeb06811	Unknown	Loop-inconsistent port has designated role
CSCeb09340	Unknown	RLB does not pass AcctStop pkts to correct SSG when maxclients excee
CSCeb11577	Unknown	Egress lookup disabled on DFC, causes flooding
CSCeb17471	Unknown	SP crashed in FATAL EXCEPTION: 0xF floating point exception
CSCeb17597	Unknown	Netflow entries installed for Non TCP/UDP flow in NAT
CSCeb18414	Unknown	ICC-SP-5-WATERMARK: pkts for class MCAST-HW-LC are waiting to proces
CSCeb18552	Unknown	Default route learnt via routing missing or incomplete in sp TCAM
CSCeb18618	Unknown	VPNSM: IKE Traffic needs to be marked as Precedence 6
CSCeb18943	Unknown	OSM-DPT: SRP Rate-limit high does not work correctly
CSCeb21202	Unknown	Undefined route-map cause intermittent loss of L3 connectivity
CSCeb21292	Unknown	MOC/SRP linecard crash with clear counter on the lc console
CSCeb22952	Unknown	SUPPORT FOR TOS BYTE PRESERVATION WITH GRE
CSCeb23191	Unknown	Const2:RPR:After switchover some C2 modules dont come online
CSCeb23201	Unknown	XCONNECT has different checks for VLAN @ provision and authorization
CSCeb27549	Unknown	19E:switch crash w/:SP: EthChnl assert failure:
CSCeb28084	Unknown	CSG: Cannot configure content defn with same IP, different VLAN.
CSCeb28275	Unknown	13E/19E: Policing doesnt work after switchover.
CSCeb29441	Unknown	CWAN-EoMPLS:Service-policy with multiple actions is broken
CSCeb32189	Unknown	sup720 crashes at process = UDLD
CSCeb33177	Unknown	Output of show mls ip non-static shows dynamic entries as well
CSCeb35612	Unknown	Module WS-X6348-RJ-45 is excessivly resetting
CSCeb36253	Unknown	Cat6K may reload with process watchdog at FIB Control Task.
CSCeb38062	Unknown	19E-renumber:no arp, adjacency is drop for static route after bootup
CSCeb38084	Unknown	Const2/BT:LC crashes on applying dss policy on atm multipoint subint
CSCeb38485	Unknown	Const2: sup720 crashes due to FM memory corruption
CSCeb40557	Unknown	CE2-NATIVE: Cannot write configs to NVRAM
CSCeb42402	Unknown	19(E1): RPR+ swover can cause cwan main interface datapath failure
CSCeb45403	Unknown	non-RPF traffic on SRP interface not HW dropped

Identifier	Technology	Description
CSCeb46918	Unknown	router crashed at ipaccess_checksum_on
CSCeb47047	Unknown	%SNMP-3-TRAPBLOCK message received with Traceback
CSCeb47151	Unknown	Uplink port config not synced upon RPR+ swover
CSCeb47607	Unknown	RPR mode fails to recognize flexwan modules at boot up
CSCeb47640	Unknown	CE2-HYB:T48:dest. router gets no tcp packets with cef route-cache
CSCeb47669	Unknown	19E:Tcp Intercept with empty ACL doesnt allow any traffic except TCP
CSCeb48670	Unknown	Cat6K : SP crashing with corrupted PC at sm_post_event
CSCeb48884	Unknown	CE2-HYB: Mcast out-of-sync between RP and SP during Anycast-RP test
CSCeb49134	Unknown	Native:HA SUP crashes due to bus error signal=10 using RPR
CSCeb49514	Unknown	Const2: Distributed port channel does not forward traffic
CSCeb49605	Unknown	CE2-NATIVE:SUP11 OIR causes mcast packet drop if OIF is L3 port
CSCeb49634	Unknown	slot/port not initialized for vlan interface in show policy-map
CSCeb50412	Unknown	Multicast packets switched by both software and hardware (FIB FULL)
CSCeb51698	Unknown	faulty fan causes SUP to crash.
CSCeb51785	Unknown	when SP is low in memory, no crashinfo is generated
CSCeb52142	Unknown	TTFIB inconsistent with TFIB on cwtlc
CSCeb52169	Unknown	Tag adjacencies point to incorrect local label on OSM
CSCeb53215	Unknown	Crash in pagp_switch_mp.c 287
CSCeb54698	Unknown	Interface rate counters do not increment on OSM-12CT3/T1
CSCeb54936	Unknown	IOS does not provide all 96 15 min intervals for T3 and T1 int
CSCeb55216	Unknown	CE2-NATIVE:All packets drop using VACL Capture and NAT with BDD
CSCeb55271	Unknown	Complementary fix to CSCdy15598 / QoS Default Bucket Policer Problem
CSCeb57796	Unknown	7603 with a 950W DC power-supply denies power to line modules
CSCeb60262	Unknown	Deleting/renaming vlans using vlan database may trigger VTP pruning
CSCeb60961	Unknown	GE OSM 64 bit SNMP counters wrap at 2^32
CSCeb62692	Unknown	CE2-NATIVE:Adding new OIF fills MET table,causing mcast packet drop
CSCeb63548	Unknown	R4: crash changing from R2 to R3/4 style configurations
CSCeb64392	Unknown	snmp-server host configuration fails
CSCeb65671	Unknown	Wrong local vc label is programmed for data plane
CSCeb67650	Unknown	WS-X6548-GE-TX & WS-X6148-GE-TX may drop frames on egress
CSCeb69582	Unknown	6500 Native IOS:in corner cases acls get applied on wrong interfaces
CSCeb72014	Unknown	Static MAC address turns dynamic on DFC card.
CSCeb72466	Unknown	IKE fsm crash on rx of bad notify
CSCeb75803	Unknown	RP crashes after CPU_MONITOR messages have not been sent for 150 sec
CSCeb76023	Unknown	TC counters not working with MST
CSCeb77077	Unknown	Spurious access occured at dot1q_ether_vlan_demux
CSCeb78428	Unknown	sup720/dfc3a: vla stats not working for mcast w/ ingress replication

Identifier	Technology	Description
CSCeb80326	Unknown	13E10: config loss in NDR running config
CSCeb80453	Unknown	CE1-NATIVE:VACL,packets sent to the destination on vlan shutdown
CSCeb83558	Unknown	VRF communication problem after adding subinterface on PE
CSCeb87003	Unknown	CE1-HYB:CBAC:tcp sessions fail after rpr+ switchover
CSCec00232	Unknown	Cat6000 - PAUSE frame causes High CPU when FC disabled
CSCec00966	Unknown	13E10:Etherchannel port comes up as suspended after reload on Sup22
CSCec02275	Unknown	CSM: vserver sticky mask changed to 255.255.255.255 on cfg dnld
CSCec03005	Unknown	13E10:L3 traff not forwarded for 10min on 6816 on doing clear mac dy
CSCec04451	Unknown	HA/RPR+ %SYS-SP-2-BADSHARE:Bad refcount in datagram_done on LC OIR
CSCec07319	Unknown	13E10:mls ip directed broadcast rpr+ swover all pkts hit software
CSCec08966	Unknown	%SYS-STDBY-2-CFORKMEM:Process creation of RFSS_server_action failed
CSCec10112	Unknown	ROMMON variables are not cleared by write erase on Sup720
CSCec10363	Unknown	FM-2-TCAM_MEMORY: Request to make error message more meaningful
CSCec14288	Unknown	13E10:L3 Traffic not forwarded across DFC for 3 minutes or more
CSCec16666	Unknown	two channel group interfaces of PA-MC-STM1 have same ifindex
CSCec18681	Unknown	C2: Berytos: Janus --> SSA CRC errors on Rx datapath
CSCec18683	Unknown	19E1:crash in l2_ufp_limit_source_flood_update_history
CSCec20522	Unknown	mem leak - Master Running Configuration Sync proc; resetting NDR
CSCec21124	Unknown	20E:Sup22 comes up with minor diagnostic error
CSCec22581	Unknown	Incorrect value for ciscoEnvMon mib objects for some modules
CSCec24628	Unknown	Sampled Netflow Stalls Under Heavy Load
CSCec31276	Unknown	MPLS-tagged pkts sourced from the RP are not prioritized correctly
CSCec32816	Unknown	%C6KPWR-SP-4-PSREDUNDANTBOTHSUPPLY message missing upon PS recovery
CSCec48379	Unknown	Const2: pak expansion on rate limit index causes resets
CSCin27542	Unknown	After reload, RP stops receiving OAMs from LC for an ima sub-intf
CSCin33181	Unknown	a2a Et-Vl: Imposition VIP crash when OIR core-facing VIP in traffic
CSCin33334	Unknown	7200: Calls failing for E1R2 non-compelled signaling
CSCin35198	Unknown	PA-MC-STM1:Sonet MIB data not getting updated
CSCin35854	Unknown	PA-MC-STM1:Controller shutdown after reload, if too many interfaces
CSCin37176	Unknown	PA-MC-STM1:RFI, RDI alarm may bring down E1 when in local loopback
CSCin37330	Unknown	Wrong return value of portType for GBIC ports in 4OC3 & 1OC48 cards
CSCin37567	Unknown	PA-MC-STM1: FIFO block 2047 never used.
CSCin37893	Unknown	PA-MC-STM1:some of the E1s remain down when Insufficient FIFOs
CSCin40363	Unknown	crash on executing no tag-switching mtu
CSCin50930	Unknown	Const2 : DCRTP command is not propagated to the flexwan with STM
CSCin51334	Unknown	SLB will be in a Loop when a GTPv0 req with destination port 2123 co
CSCin52105	Unknown	CWPA2:dmlfr:MFR bundle link flaps along with MFR bundle

Identifier	Technology	Description
CSCin56266	Unknown	Router crashes at sss_sip_info_free with FRoMPLS
CSCuk37312	Unknown	multicast static mac address entries removed on reload
CSCuk42146	Unknown	code corruption at 0x602A0244 to 0x3040000 on RRP only
CSCdu07504	Voice	sh voice dsp causes reload
CSCdw20927	Voice	Bus error when processing alert timer in CS_CutProgress
CSCdx17219	Voice	Caller ID need to support Bellcore variation in Canada
CSCdy61597	Voice	decodeAndPrintQ931IEs may cause memory corruption
CSCdz20801	Voice	Memory corruption on As5850 as Voice GW
CSCdz37574	Voice	VOFR keepalive are not restarted after it times out
CSCdz38268	Voice	Bus error at sipSPISendBye
CSCdz40015	Voice	ALIGN-1-FATAL: Illegal access to a low address
CSCdz48635	Voice	Reload @ cpm_enqueue_calls_list/cpm_dequeue_calls_list during calls
CSCdz49277	Voice	Disconected calls show as refused calls
CSCdz53326	Voice	Channel is stuck on S_TSP_WAIT_RELEASE state
CSCdz54800	Voice	RAS GW registration fails at boot time if security password too long
CSCdz60807	Voice	Router crash few hours after adding use-proxy command
CSCea22981	Voice	Using reserve <dsp> command crashes 7200 with NPE G1 on reboot
CSCea32240	Voice	H323 crashes in strncpy when receiving invalid setup packet
CSCea33065	Voice	H323 Spurious memory access in h450ProcRcvdApdus
CSCea36231	Voice	Router hangs when receive in invalid h225 setup
CSCea46342	Voice	h.323 crashes in ACFnonStandardInfo DEC_ERR=13
CSCea51030	Voice	h323: proxy crashes when malformed h225 setup message received
CSCea51076	Voice	h323: proxy crashes when processing invalid h225 setup messafe
CSCea54851	Voice	h323 proxy: crash at pxy_proc_recv_SETUP when invalid h225 setup rx
CSCea64747	Voice	VAD Agressive overides VAD configuration after reload
CSCin28504	Voice	OIR removal of uninitialized PA-MCX-8TE1 crashes router
CSCdz25535	VPDN	NAS-Port attribute is getting corrupted on multihop router
CSCdz66576	VPDN	VPDN failure manager Traceback
CSCdz67847	VPDN	l2f/l2tp needs to drop invalid PPP packets
CSCea11967	VPDN	LNS not sending SLI when LCP is renegotiated
CSCea19848	VPDN	Packets dropped at client with CEF/MLP at LNS and dialer MTU<1500
CSCea46367	VPDN	L2TP tunnel not established if user logged without realm
CSCdu05871	WAN	PA-T3 will not come up in the flexwan even if looped
CSCdv13877	WAN	Boot time is 45 minutes to 1 hour with 2000 VCs on FlexWAN
CSCdw64588	WAN	Huge delay in fast switching from tunnel to FlexWAN port
CSCdx69085	WAN	L2TP:snmp trap problem when the Virtual-Access interface up/down
CSCdy30537	WAN	Serial subint goes down after reload with frame-relay de-group

Identifier	Technology	Description
CSCdy46026	WAN	CE-HYB: %ATMPA-3-CMDFAIL: ATM8/1/0 Command Failed at ../src-rsp/rsp_
CSCdz00624	WAN	After configure no ip cef router starting to drop packets
CSCdz09542	WAN	HSSI interface wedged
CSCdz16414	WAN	The NTP on ONS15104 does not stay synchronized
CSCdz16768	WAN	The RRs that Cisco 2610 send have delay times at diverse times
CSCdz33003	WAN	Traceback found for dconfig tests with POS interface
CSCdz38136	WAN	Flexwan Multi-channel-T1 : frame-relay pvc counters skewed
CSCdz38482	WAN	Router crashes with SegV exception
CSCdz40567	WAN	Counter overflow error occurs on ip protocol
CSCdz46845	WAN	HC counters remain at 0 for POS interfaces in FlexWAN module
CSCdz48092	WAN	PA-MC-STM-1SMI interface comes up, router crashes
CSCdz58282	WAN	VIP crash - FRF.11 Annex C fragmentation
CSCdz60567	WAN	Cannot switch back to H/w compression
CSCdz61586	WAN	ATM VC bundling precedence mapping does not work on Flexwan w Hybrid
CSCdz61962	WAN	Cat6k: MLS Enabled ATM Connection Problems
CSCdz70716	WAN	POS interface doesnt increment broadcast counters
CSCdz73574	WAN	PA-POS-OC3SMI hang and needs router reload
CSCdz78099	WAN	MFR: MFR interface can no longer be configured
CSCdz85565	WAN	IPHC regression failing on M4T interfaces
CSCea12025	WAN	MFR: memory leak on 2621XM in high traffic load
CSCea17496	WAN	Flexwan with ATM pa resets due to Deadman Timer.
CSCea27953	WAN	FW 1483 bridged PVCs remain in INAC status on reload.
CSCea34094	WAN	SDLC traps flooding for unknown SDLC link
CSCea38967	WAN	Make sure pkt cleanup is complete for Mx HSSI-B PA
CSCea40836	WAN	MFR: ADD_LINK_REJ message includes Cause IE with invalid Length
CSCea46073	WAN	Running configuration does not show changes in NTP password
CSCea56687	WAN	ATM VC bundling precedence mapping does not work on Flexwan
CSCea63940	WAN	Peer reset on FW oir:Failed to allocate IPC buffer loveletter
CSCea71196	WAN	FW:hardware NAT not working on ATM flexwan PA
CSCea71729	WAN	Command srp srr enable appears after reload in SRP interface
CSCea79535	WAN	Receipt of illegal range DLCI prevents LMI exchange
CSCeb37354	WAN	Flexwan double counts input packets on frame-relay PVCs
CSCeb72381	WAN	MLFR -New MFR intf with ospf config -OSPF-6-ZERO_BANDWIDTH Traceback
CSCin08621	WAN	%CBUS-3-CMDTIMEOUT seen on reload with multiple LCs
CSCin12517	WAN	VIPMLP:Traffic loss on scaling multilink on 2CT3+
CSCin27157	WAN	c2sup2:HalfBridging:Output packet counters are not updated
CSCin41295	WAN	ATM sub-interfaces remain down after OIR

Identifier	Technology	Description
CSCin45088	WAN	Flexwan with PA-MC-E3 crashing when OIR is done
CSCin50105	WAN	IMA link protocol status displayed incorrectly
CSCdz52774	Wireless	The GGSN reloads due to Illegal access to a low address
CSCea44554	Wireless	GGSN reload with BUS error while updating fast cache
CSCea62665	Wireless	Bus error at acct_cleanup
CSCin40563	Wireless	GGSN delete all PDP contexts for a particular SGSN during update con

Caveats in Release 12.2(14)SX and Rebuilds

Open Caveats in Release 12.2(14)SX and Rebuilds

Identifier	Technology	Description
CSCdy84624	QoS	Flexwan rebooting when NBAR is configured
CSCea67226	Unknown	Cat6000:With large number of NAT overload flows recir paks FIB switc
CSCea71219	Unknown	linecard resets due to invalid fib ipc packet
CSCea71196	WAN	FW:hardware NAT not working on ATM flexwan PA

Resolved Caveats in Release 12.2(14)SX1

Identifier	Technology	Description
CSCin32872	ATM	back to back ping fails after bay reload due to INAC VC
CSCin33561	ATM	MSFC crash when an ATM uni link is configured
CSCin33673	ATM	loki_state_change: Sending config failed - IMA interface down
CSCin34322	ATM	Flexwan crash while MSFC is booting
CSCdz71127	Multicast	unexpected packet can cause input queue wedge - reg to CSCdx02283
CSCea60211	PPP	Const2:RP crashed @ mlp_fragment on adding a mem to a mlp bundle.
CSCea73586	PPP	FW ATM E3 crashes cont with traff @ dlfi_atm_bundle_process
CSCdy11767	Unknown	Disabling dot1qtunnel tagged frame still go through the link
CSCea35846	Unknown	Const2: No PVID, type incon, root or loop inconsistency generated
CSCea61460	Unknown	C2:failed to assign rate limiter to multicast non-rpf, #3 was free
CSCea62335	Unknown	Clear ip route all causes CPUHOG & core dump
CSCea65695	Unknown	FW STM-1 PA crashed @ vip_mlp_ip_fib on starting the traffic.
CSCea66858	Unknown	%SM-SP-4-BADEVENT: Event insert is invalid Standby gone

Identifier	Technology	Description
CSCea69334	Unknown	C2: ifIndex does NOT persist after RPR+ switchover and reload
CSCea71481	Unknown	ISIS doesnt work over GRE tunnel
CSCea82353	Unknown	PIM Register & Register stop messages are looped until TTL expires
CSCeb00678	Unknown	sup crash while making csm config changes
CSCeb05818	Unknown	19e: vlans ifIndex not synced to NAM
CSCeb11932	Unknown	Port-channel interfaces will not come up after RPR+ sw/over
CSCeb17471	Unknown	SP crashed in FATAL EXCEPTION: 0xF floating point exception
CSCin35854	Unknown	PA-MC-STM1:Controller shutdown after reload, if too many interfaces
CSCin27157	WAN	c2sup2:HalfBridging:Output packet counters are not updated
CSCin41295	WAN	ATM sub-interfaces remain down after OIR

Resolved Caveats in Release 12.2(14)SX

Resolved PPP Caveats

- CSCdz22366—Resolved in 12.2(14)SX

  In a Virtual Private Dial-up Network (VPDN) environment, if the LAC is not configured for authentication and the user does not provide any authentication information, the authentication on the LNS may be bypassed. This problem will not occur if the LAC is configured properly to authenticate the users.

  In the case of client initiated tunnels (http://www.cisco.com/en/US/tech/tk801/tk703/technologies_configuration_example09186a00800946f5.shtml), where there is no seperate LAC, all authentication may be bypassed.

  Only the IOS devices that are acting as LNS are affected. The IOS devices that are not acting as LNS are not affected.

  An attacker may exploit this vulnerability to gain unauthorized access to network resources if authentication is not configured on the LAC.

  The workaround is to configure “lcp renegotiation always” command in virtual private dialup network (VPDN) group configuration mode.

Other Resolved Caveats in Release 12.2(14)SX

Identifier	Technology	Description
CSCdy61602	Access	NRT: RSP-3-RESTART after changing encapsulation to lapb
CSCdz75118	Access	Interface input / output rate not decreasing to zero after shutdown
CSCin34068	Access	Unable to create channel-group on PA-MC-8TE1+
CSCdz67483	ATM	Encapsulation aal0 option missing for CRoMPLS
CSCin28792	ATM	Can not attach policy on ATMima Subinterface
CSCin38132	ATM	when traffic rate > police cir ATM ima crashing
CSCdz36877	Infrastructure	no echo of characters on vty exec
CSCdz40472	Infrastructure	TTY2: timer_create_bg error when telneting to router

Identifier	Technology	Description
CSCdz51138	Infrastructure	ifOperStatus shows incorrect value for PPP encap interfaces
CSCdz81035	Infrastructure	writing crashinfo to disk0 results in corrupted file
CSCin28606	Infrastructure	Invalid interface counters after loading the image
CSCdy57048	IPServices	MPLS/Tag switching results in invalid TCP packet
CSCdz36526	IPServices	NAT: missing changes in CSCdx40232 umbralla commit
CSCdz46435	IPServices	Traceback at frame_relay_extract_addr after igmp_get_mac_or_ip_srcad
CSCdz76824	IPServices	Arp alias not set correctly after reload with static NAT configured
CSCdy89749	LAN	lot of spurious access at fx1000_dtq_consumer_isl and vip crashes
CSCdz90090	LAN	VIP ignores unicast packets received from PA-2FE
CSCdz43747	MPLS	Local label does not bind after route flapping
CSCdz57007	MPLS	vip/rp/7200/any alignment errors or crash, mpls feature path
CSCea09270	MPLS	CSCdt32774 reintroduced in 12.2S
CSCea17870	platform-72xx	need to cleanup pak on the pxf punt path
CSCdz74858	platform-75xx	RSP16 crash in rsp_input_raw_prefetch and rsp_mip_fs
CSCdz41189	platform-76xx	13E3/PWAN2:VTMS[1]: queue failed to become idle,quid 0x9
CSCdz58878	platform-76xx	13E3/PWAN2: LC crash due to vtms periodic on switchfabric oir
CSCdz74625	platform-76xx	FLO_ISP/GBIC:scp_idprom_msg: BAD EEPROM on module xx errcode=1
CSCdz76361	PPP	7200/VXR: MLPPP is not working with CEF (due to punt adj)
CSCea38851	PPP	RP crashed at mlp_fastswitch_les on peer chassis reload.
CSCdz53696	QoS	RSVP: ResvError crashes the router
CSCdz74130	QoS	RSVP: Memory corruption crash while processing incoming PATH
CSCea02713	QoS	Bus error in fair_queue_update_class after malloc fail
CSCea06563	QoS	TE LSP does not come up after changing encapsulation HDLC to PPP
CSCea07020	QoS	Memory leak when configuring frame-relay WRED
CSCin28688	QoS	No drop via random-detect in ATM(OC3) Subinterface
CSCdz41310	Routing	Const2 - Memory fragmentation on RP after route flaps
CSCdz45760	Routing	OSPF LSA refresh should not cause partial SPF
CSCdz76611	Routing	Router crash when remove static EIGRP neighbor statement
CSCdz77777	Routing	software forced crash on a router after clear ip bgp
CSCea02355	Routing	rare ip packets may cause input queue wedge
CSCea03212	Routing	sh ipv6 traffic is not count up when 6pe uses
CSCea24313	Routing	ipv6 floating default route leads route flapping
CSCdz74538	Security	VSEC:VAM anti-replay fw check needed on VAM
CSCdy84560	Unknown	C-HYB+HA_SRM: two switchover in 1 min makes cat6k send no packet
CSCdz21419	Unknown	Incorrect OIR-SP-3-PWRCYCLE reason
CSCdz29883	Unknown	Mac Notification: L3 traffic loss with a L2 etherchannel across DFCs
CSCdz51932	Unknown	Reload after delete ACL that is used for crypto

Identifier	Technology	Description
CSCdz53958	Unknown	Setting cdpInterfaceEnable port in a channel=false reset switch
CSCdz57158	Unknown	Incorrect supervisor model and s/n displayed for sup
CSCdz59821	Unknown	TCP intercept connections are getting reset after 24 hrs
CSCdz65299	Unknown	Bus Error crash in ipmulticast-loopback, ipsendnet, ipwrite
CSCdz66347	Unknown	On reload, static multicast L2 entry not processed by igmp-snooping
CSCdz67182	Unknown	CWAN-QOS:PFC aggregate policing not work for cwtlc
CSCdz69161	Unknown	Reoccurance of CSCdz21420
CSCdz69965	Unknown	VSEC:VPN-SM:RP/SP crash after reloading with 800 tunnels
CSCdz76698	Unknown	flo_isp: Sending 1000 multicast traffic, sp get Seg violation
CSCdz87238	Unknown	SLB: http probe GET requests not specific about file requested
CSCdz89258	Unknown	Traffic stops after BGP prim to sec peer failover with large ACL
CSCea07970	Unknown	Various Trap issues in RPR, RPR+, OIR Standby Sup, etc.
CSCea13771	Unknown	ubr7100 may crash upon reload
CSCea15655	Unknown	CDP neighbors for port-channels show same local interface for member
CSCea18561	Unknown	Static Multicast CAM entry disappears from the mac-addr-table
CSCea35846	Unknown	Const2: No PVID, type incon, root or loop inconsistency generated
CSCea39633	Unknown	MSFC2 experiences bus error exception - const_fib_enqueue_fib_req
CSCea41980	Unknown	Catalyst 6000 Native crashes with Failed to send RPC request msg
CSCea43709	Unknown	Const2:Show mac-address does not respond from RP
CSCea45950	Unknown	VLAN-do-not-learn-bit set for active vlan --> unicast flooding
CSCea59575	Unknown	L2 entries dont age out after disabling and then reenabling aging
CSCea63521	Unknown	Catos mistp bpdu not tunneled thru switch running IOS
CSCin37567	Unknown	PA-MC-STM1: FIFO block 2047 never used.
CSCdz16414	WAN	The NTP on ONS15104 does not stay synchronized
CSCdz38482	WAN	Router crashes with SegV exception
CSCdz61586	WAN	ATM VC bundling precedence mapping does not work on Flexwan w Hybrid
CSCdz73574	WAN	PA-POS-OC3SMI hang and needs router reload
CSCea27953	WAN	FW 1483 bridged PVCs remain in INAC status on reload.