



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

March 15, 2010

This publication applies to these platforms:

- CAT6000-VS-S720-10G/MSFC3
- CAT6000-SUP720/MSFC3
- CAT6000-SUP32/MSFC2A
- ME6524

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(33)SXH or later on both the switch processor and the route processor. If you are running a release earlier than Release 12.2(33)SXH, refer to this publication:

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

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

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



Americas Headquarters:

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

© 2006–2008 Cisco Systems, Inc. All rights reserved.
Cisco Systems, Inc. All rights reserved.

**Caution**

Cisco IOS running on the switch processor and the route processor supports redundant configurations where the switch processor and the route processor are identical. If they are not identical, one switch processor and the route processor will boot first and become active and hold the other in a reset condition.

Chronological List of Releases

**Note**

- See the [“Feature Sets” section on page 113](#) for information about which releases are deferred.
- See the [“Hierarchical List of Releases” section on page 2](#) for information about parent releases.

This is a chronological list of the 12.2SX releases starting with Release 12.2(33)SXH:

- 15 Mar 2010—Release 12.2(33)SXH7
- 04 Nov 2009—Release 12.2(33)SXI3
- 21 Oct 2009—Release 12.2(33)SXH6
- 03 Sep 2009—Release 12.2(33)SXI2a
- 17 Jul 2009—Release 12.2(33)SXI2
- 20 Apr 2009—Release 12.2(33)SXH5
- 31 Mar 2009—Release 12.2(33)SXI1
- 14 Nov 2008—Release 12.2(33)SXH4
- 11 Nov 2008—Release 12.2(33)SXI
- 29 Sep 2008—Release 12.2(33)SXH3a
- 29 Jul 2008—Release 12.2(33)SXH3
- 28 Apr 2008—Release 12.2(33)SXH2a
- 31 Mar 2008—Release 12.2(33)SXH2
- 18 Jan 2008—Release 12.2(33)SXH1
- 20 Aug 2007—Release 12.2(33)SXH

Hierarchical List of Releases

This list shows the relationship between releases:

- Release 12.2(33)SXI3:
 - Date of release: 04 Nov 2009
 - Based on Release 12.2(33)SXI2a
- Release 12.2(33)SXI2a:
 - Date of release: 03 Sep 2009
 - Based on Release 12.2(33)SXI2

- Release 12.2(33)SXI2:
 - Date of release: 17 Jul 2009
 - Based on Release 12.2(33)SXI1 and SXH5
- Release 12.2(33)SXI1:
 - Date of release: 31 Mar 2009
 - Based on Release 12.2(33)SXI and SXH4
- Release 12.2(33)SXI:
 - Date of release: 11 Nov 2008
 - Based on Release 12.2(33)SXH3a
- Release 12.2(33)SXH7:
 - Date of release: 15 Mar 2010
 - Based on Release 12.2(33)SXH6
- Release 12.2(33)SXH6:
 - Date of release: 21 Oct 2009
 - Based on Release 12.2(33)SXH5
- Release 12.2(33)SXH5:
 - Date of release: 20 Apr 2009
 - Based on Release 12.2(33)SXH4
- Release 12.2(33)SXH4:
 - Date of release: 14 Nov 2008
 - Based on Release 12.2(33)SXH3a
- Release 12.2(33)SXH3a:
 - Date of release: 29 Sep 2008
 - Based on Release 12.2(33)SXH3
- Release 12.2(33)SXH3:
 - Date of release: 29 Jul 2008
 - Based on Release 12.2(33)SXH2a
- Release 12.2(33)SXH2a:
 - Date of release: 28 Apr 2008
 - Based on Release 12.2(33)SXH2
- Release 12.2(33)SXH2:
 - Date of release: 31 Mar 2008
 - Based on Release 12.2(33)SXH1 and Release 12.2(18)SXF13
- Release 12.2(33)SXH1:
 - Date of release: 18 Jan 2008
 - Based on Release 12.2(33)SXH and Release 12.2(18)SXF12

- Release 12.2(33)SXH:
 - Date of release: 20 Aug 2007
 - Based on Release 12.2(18)SXF10

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 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 this publication:

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

For general product information about the Catalyst 6500 series switches, refer to the Catalyst 4000, 5000, and 6000 Family Software Product Bulletins at the URLs below:

<http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/index.shtml>

Universal Boot Loader Image

A new supervisor engine contains one of the following initial software images:

- Cisco IOS software
- Catalyst operating system software
- Universal Boot Loader (UBL) software

The UBL software is a minimal network-aware image that can download and install either a Cisco IOS image or a Catalyst operating system image from a running active supervisor engine in the same chassis.

When newly installed as a standby supervisor engine in a redundant application, a supervisor engine running the UBL software automatically attempts to copy the image of the running active supervisor engine in the same chassis. This feature requires the active supervisor engine to be running either Cisco IOS software Release 12.2SXH or later, or Catalyst operating system software Release 8.6(1) or later.



Note

When a standby supervisor engine copies a Catalyst operating system software image using UBL, the downloaded image will not include the Multilayer Switch Feature Card (MSFC) software. A Cisco IOS software image that is downloaded using UBL will include the MSFC software.

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, page 5](#)
- [FPD Upgrades, page 5](#)

FPD-Image Dependant Modules

These modules use FPD images:

- Shared Port Adapter (SPA) Interface Processors (SIPs)
- Shared Port Adapters

FPD Upgrades

See this publication:

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

Cisco IOS Software Modularity

These sections describe Cisco IOS Software Modularity:

- [Cisco IOS Software Modularity Documentation, page 5](#)
- [Cisco IOS Software Modularity Unsupported Features, page 5](#)

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_4t/netmgmt/configuration/guide/t_eemo.html

Cisco IOS Software Modularity Unsupported Features

None.

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.

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, page 6](#)
- [General Limitations and Restrictions, page 6](#)
- [FlexWAN Limitations and Restrictions, page 14](#)
- [Service Module Limitations and Restrictions, page 14](#)

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:

Identifier	Technology	Description
CSCsl38289	Security	12.2SR/SX: PKI trustpoint enrollment fails if CA server keysize = 4096
CSCek70681	Unknown	naxos wred counter drops seen for larger packet size
CSCsj44811	Unknown	DMVPN Spoke-to-Spoke Tunnel Setup is Much Longer if Spoke is in FVRF
CSCsk54693	Unknown	OIR naxos with 8G traffic, "sh cry eli" granikos in intialising state
CSCsl71635	Unknown	B2B: some tunnels flapping after reverting back from vpn module.
CSCsl86574	Unknown	Some commands are not getting converted when converting vs to standalone
CSCsm13662	Unknown	IPsec SA counter displays a huge encap/decap value after B2B failover
CSCsm43234	Unknown	%ISSU_PROCESS-SP-3-SYSTEM: Not enough space in NVRAM;Fail to set bootvar
CSCsm48844	Unknown	MVRP cannot be enabled on 61xx,63xx,65xx linecards (with few Exception)
CSCsm59426	Unknown	UDE/UDLR: OSPF neighbourship is not getting formed with UDE/UDLR link
CSCsm92866	Unknown	C2W2: one bad LC in slot 1 cause NTI error and other LCs fail booting up
CSCsq60055	Unknown	System reset after reverting the spanning tree mode from PVST to MSTP

Identifier	Technology	Description
CSCsq71514	Unknown	After ISSU RV LPIP DHCP hosts are not posture validated till statusquery
CSCsr05186	Unknown	Access lists not applied when multicast traffic is sent over GRE tunnel
CSCsr98197	Unknown	WiSM Manual LAG not supported in SXI
CSCsu50427	Unknown	ME6524 EoMPLS does not insert tag for type4 vc
CSCsv00977	Unknown	IPv6 VTI, Tunnels flap during B2B operation
CSCsw67926	Unknown	C2W2: CFM Draft1 does not support in Whitney2.0.
CSCsy31055	Unknown	Support for patching modular IOS images deferred
CSCtb09290	Unknown	Problem with accounting Giant packets at FW
CSCtd31237	Unknown	standby track is detected when SSO switchover but standby sso enabled

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

The Ethernet ports on all other LAN switching 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. (Search for “Dual switch-fabric connections” in this document.)
- Layer 2 denial-of-service (DoS) protection rate limiters are not supported in truncated mode. (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-GBICswitching 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)
- EoMPLS ports cannot be SPAN sources. (CSCed51245)
- IPsec in software on the MSFC is supported only for administrative connections to Catalyst 6500 series switches and Cisco 7600 series routers.
- 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)
- There is no hardware support for fragmented multicast VPN traffic. (CSCef08631)

- When a port becomes a member port of a Layer 2 EtherChannel, any service policy on that member port is displayed by the **show mls qos ip** command as being on the port-channel interface, but the service policy is not applied to the EtherChannel. (CSCec34784)
- The time taken to execute the **show spanning-tree** interface command is proportional to the number of VLANs configured. With many VLANs configured, there might be a noticeable delay in the output of the command while Cisco IOS scans the VLANs for spanning tree ports. (CSCec65860)
- If you set the MTU size on an LACP port-channel interface, the configured MTU size propagates to the member ports. If you change the MTU size on some of the member ports of an LACP EtherChannel, the change does not propagate to the port-channel interface. The ports configured with a different MTU size than the port-channel interface form a secondary LACP EtherChannel. The port-channel interface of a secondary LACP EtherChannel is not configurable. (CSCed18149)
- See this publication for information about the supported IPv6 address formats:
http://www.cisco.com/en/US/docs/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 overpolicies 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 redundancy mode does 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. (CSCe32737)
- 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. (CSCe86399)
- SPAN and RSPAN destination ports transmit VACL-redirected traffic. (CSCe57673)
- 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. (CSCe23571)
- PFC QoS does not rewrite the payload ToS byte in tunnel traffic.
- PFC QoS does not rewrite the ToS byte in bridged multicast 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.
- 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.
- 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. (CSCe53554)
- 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)
- 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)
- Cisco IOS software Release 12.2SX does 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.
- Cisco IOS software Release 12.2SX does 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)
- Cisco IOS software Release 12.2SX does 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 in Cisco IOS software Release 12.2SX. 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 unreachable** 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 unreachable** 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.
- 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)

Service Module Limitations and Restrictions

- Generating an Rivest, Shamir, and Adelman (RSA) usage key pair with modulo 360 fails.
Workaround: Use a higher modulo value. (CSCec49861)
- When the NAM is configured as the NDE destination and the NAM is down, the NDE traffic is flooded.
Workaround: Clear the NDE configuration for the NAM or enter the **clear arp-cache** command. (CSCdy55261)
- You cannot SPAN ingress traffic from the Firewall Services Module (WS-SVC-FWM-1-K9). (CSCec79733)
- 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)

Important Notes

Cisco IOS Behavior Changes

Behavior changes describe the minor modifications to the way a device works that are sometimes introduced in a new software release. These changes typically occur during the course of resolving a software defect and are therefore not significant enough to warrant the creation of a stand-alone document. When behavior changes are introduced, existing documentation is updated with the changes described in these sections:

- [Cisco IOS Release 12.2\(33\)SXH7, page 15](#)
- [Cisco IOS Release 12.2\(33\)SXH6, page 16](#)
- [Cisco IOS Release 12.2\(33\)SXH5, page 18](#)

Cisco IOS Release 12.2(33)SXH7

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXH7:

- MTU on PA-1FE and PA-2FE port adapters

Old Behavior: MTU is not configurable on PA-1FE and PA-2FE port adapters. When a you attempted to configure the interface MTU, the following message was printed:

```
% Interface {Interface Name} does not support user settable mtu
```

New Behavior: You can configure the interface MTU on PA-1FE and PA-2FE port adapters (PAs).

Additional Information: See the *MPLS MTU Command Changes* document at the following URL:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_mtu_cmd_changes.html

- IPv6 packets with extension headers

Old Behavior: IPv6 packets with extension headers are processed in hardware.

New Behavior: In releases where CSCtc71597 is resolved, to address the issues described in CSCtc71597, you can enable software processing of IPv6 packets with extension headers. If your IPv6 traffic does not specify a L4 protocol, software processing of IPv6 packets with extension headers is unnecessary. If your IPv6 traffic specifies a L4 protocol, enable software processing of IPv6 packets with extension headers.

Additional Information: Enter the **platform ipv6 acl punt extension-header** global configuration command to enable software processing of IPv6 packets with extension headers.

Enter the **mls rate-limit unicast acl input 100 pps** command to limit the number of packets sent to the RP for processing in software.

- NTP mode 7 packet processing

Old Behavior: Cisco IOS Software releases process NTP mode 7 packets.

New Behavior: Cisco IOS Software releases where CSCtd75033 is resolved do not process NTP mode 7 packets, and instead, if debugs for NTP are enabled, display "NTP: Receive: dropping message: Received NTP private mode packet. 7".

Additional Information: To have Cisco IOS Software process NTP mode 7 packets, enter the **ntp allow mode private** command (disabled by default).

Cisco IOS Release 12.2(33)SXH6

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXH6:

- Dynamic NAT entries do not time out correctly in certain cases.
Old Behavior: If NAT was configured with the `ip nat translation max-entries` command and the limit was reached, incoming packets could not create any new entries in a NAT table. To remedy this situation, packets were sent to the process path. Eventually, the packets sent to the process path were dropped. This behavior caused a high CPU usage problem.
New Behavior: Packets received after the max-entries limit has been reached are dropped at the CEF path.
Additional Information: None.
- CLI change to `bgp aggregate-timer` command to suppress more specific routes.
Old Behavior: More specific routes are advertised and withdrawn later, even if `aggregate-address summary-only` is configured. The BGP table shows the specific prefixes as suppressed.
New Behavior: The `bgp aggregate-timer` command now accepts the value of 0 (zero), which disables the aggregate timer and suppresses the routes immediately.
Additional Information: None.
- Update `show environment status` command to include power input 4
Old Behavior: In releases where CSCtb57321 is not resolved, the `show environment status` output displays power inputs 1-3 but not 4.
New Behavior: In releases where CSCtb57321 is resolved, all 4 power inputs are displayed.
Additional Information: None.
- New option, (**exclude vlan**) is added for **port-channel load-balance** command for PFC3C mode chassis.
Old Behavior: There is no option to exclude VLAN in the IP-related load distribution.
New Behavior: The **exclude vlan** option is added for IP-related load balance methods such as **dst-ip**, **dst-mixed-ip-port**, **src-dst-ip**, **src-dst-mixed-ip-port**, **src-ip**, and **src-mixed-ip-port**. Using this option excludes the VLAN in the IP-related load distribution.
Additional Information:
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_o1.html#wp1013233
- New CLI allows VACL capture of software-switched WAN packets
Old Behavior: Software-switched WAN packets are not subjected to ACL lookup in the ACL TCAM and are therefore not affected by hardware-only features. As a result, VACL capture will fail for software-switched WAN packets.
New Behavior: The platform `cwan acl software-switched` command allows software-switched WAN packets to be subjected to ACL lookup, and VACL capture will capture software-switched WAN packets. The `show platform acl software-switched` command displays the state of this feature.
Additional Information:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.html#VACL_Configuration_Guidelines
- New command (**mls ip slb purge global**) no longer causes ISSU failure

Old Behavior: When you perform an ISSU to a new version that introduces support for the **mls ip slb purge global** command, the command, which is enabled by default, appears in the generated configuration. During the ISSU **runversion** phase, when the updated active device attempts to synchronize configuration with the standby device, the standby device does not recognize the **mls ip slb purge global** command, and the ISSU fails.

New Behavior: The **mls ip slb purge global** command, which is enabled by default, does not appear in the generated configuration unless the configuration disables the feature. When you perform an ISSU to a new version that introduces support for the **mls ip slb purge global** command, the new command will not appear in the running configuration or generated configuration and will not cause an ISSU failure.

- Loopback interfaces are shut down on dual-active detection

Old Behavior: An active chassis that detects a dual-active condition shuts down all of its non-VSL physical interfaces except interfaces configured to be excluded from shutdown. Loopback interfaces are not shut down.

New Behavior: An active chassis that detects a dual-active condition shuts down all of its non-VSL physical and loopback interfaces except interfaces configured to be excluded from shutdown.

Additional Information:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Recovery_Actions

- Support for the VLAN translation on ME6500 switches and WS-X6148A-GE-TX switching modules

Old Behavior: In releases where CSCsy34566 is not resolved, the VLAN translation CLI is available on ME6500 switches and WS-X6148A-GE-TX switching modules, but does not function correctly.

New Behavior: In releases where CSCsy34566 is resolved, the VLAN translation CLI is not available on ME6500 switches and WS-X6148A-GE-TX switching modules.

Additional Information: None.

- Support for the **mls cef tunnel fragment** command in PFC3A and PFC3B modes

Old Behavior: In releases later than 12.2(18)SFX and rebuilds, the **mls cef tunnel fragment** command is not supported in PFC3A and PFC3B modes.

New Behavior: In releases where CSCsy69228 is resolved, the **mls cef tunnel fragment** command is supported in PFC3A and PFC3B modes.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_i1.html#mls_cef_tunnel_fragment

- New CLI allows VACL capture of software-switched WAN packets

Old Behavior: Software-switched WAN packets are not subjected to ACL lookup in the ACL TCAM and are therefore not affected by hardware-only features. As a result, VACL capture will fail for software-switched WAN packets.

New Behavior: The platform **cwan acl software-switched** command allows software-switched WAN packets to be subjected to ACL lookup, and VACL capture will capture software-switched WAN packets. The **show platform acl software-switched** command displays the state of this feature.

Additional Information:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.html#VACL_Configuration_Guidelines

- Added support for the **powerdown** keyword on the **environment-monitor shutdown temperature** command for the Catalyst 6500 switches.

Old Behavior: In releases where CSCtb58571 is not resolved, when a major temperature alarm is detected on the active supervisor engine, the system is forced to ROMMON.

New Behavior: In releases where CSCtb58571 is resolved, when a major temperature alarm is detected on the active supervisor engine, the system is forced to ROMMON only if configured with the **rommon** keyword. If the **powerdown** keyword is configured then the active supervisor is powered down.

Additional Information: None.

- Support added to actively detect the rogue DHCP Servers.

Old Behavior: None of the old behavior has been changed. Additional feature has been introduced.

New Behavior: DHCPDISCOVER messages will be sent out on untrusted ports and when the response comes back they are logged. User needs to specify list of VLANs on which the spurious DHCP server detection is required. The messages will be simultaneously sent out on all untrusted ports belonging to those VLANs at a configurable interval. The source MAC address of DHCPDISCOVER messages will be that of the switch.

The enhanced logging will trigger syslog for DHCPDISCOVER, DHCPACK, DHCPNAK, DHCPLEASEQUERY messages on untrusted ports. There are no trigger mechanisms on trusted ports. These syslogs will be rate-limited.

Further all the responses for bogus messages will be logged in a database. The database will not be persistent across a reload/SSO. CLI will be provided to clear the database. Database fields will include MAC + IP + VLAN + Interface + Last Seen + Count.

Additional Information: None.

Cisco IOS Release 12.2(33)SXH5

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXH5:

- RPF check behavior changed when an RPF neighbor is learned via BGP

Old Behavior: When a potentially better RPF neighbor is learned via BGP and PIM hellos from that RPF neighbor have not been received over the MDT tunnel, the RPF check will fail resulting in traffic loss because the RPF interface is set to NULL.

New Behavior: When a potentially better RPF neighbor is learned via BGP and PIM hellos from that RPF neighbor have not been received over the MDT tunnel, the RPF check will set the RPF interface to the MDT tunnel instead of NULL, thereby preventing traffic loss.

Additional Information: None.

- DHCP: Ports UDP 67 and 68 are now closed in the Cisco IOS DHCP/BOOTP default configuration.

Old Behavior: DHCP services are enabled by default and ports UDP 67 and 68 are open in the Cisco IOS DHCP/BOOTP default configuration.

New Behavior: There are now two logical parts to the **service dhcp** command: **service enabled** and **service running**. The DHCP service is enabled by default, but port 67 (the server port) is not opened until the DHCP service is running. Port 68 (the DHCP client port) is closed by default when a router loads. The client port is opened when certain DHCP processes start.

Additional information:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_svr_cfg.html

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_client.html

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

- DHCP: the **renew deny unknown** DHCP pool configuration command configures the DHCP server renewal policy for unknown DHCP clients.

Old Behavior: The DHCP server ignores a client request for an IP address that is not currently leased to the client.

New Behavior: If the DHCP server is configured to secure ARP table entries to DHCP leases and the **renew deny unknown** command is configured, the DHCP server can acknowledge the request and start the process of lease negotiation with the client.

Additional information:

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_acct_sec.html

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_book.html

- **snmp mib flash cache** command introduced.

Old Behavior: No cache was maintained for CISCO-FLASH-MIB.

New Behavior: The **snmp mib flash cache** command has been added to start a process that constructs and maintains a cache.

Additional Information:

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_17.html#snmp_mib_flash_cache

- SNMP query for **cdpCacheAddress** provides a global unicast IPv6 address.

Old Behavior: The SNMP query for **cdpCacheAddress** provided a link-local IPv6 address.

New Behavior: SNMP query for **cdpCacheAddress** provides a global unicast IPv6 address.

Additional Information: None.

- Default Change

Old Behavior: The maximum value of **queue-depth hello** and **queue-depth update** is displayed as 4294967295.

New Behavior: The maximum value of **queue-depth hello** and **queue-depth update** is changed to 2147483647.

Additional Information:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_q1.html#queue-depth

- CLI output change for **show ip traffic** command.

Old Behavior: The **show ip traffic** command displays the ARP (proxy) reply counter as the number of ARP replies for real proxies and for virtual IP addresses.

New Behavior: The **show ip traffic** command displays the ARP (proxy) reply counter as the number of ARP replies for real proxies only.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipapp/command/reference/iap_s2.html#show_ip_traffic

- CLI change for bidirectional forwarding detection (BFD).

Old Behavior: Cisco IOS software incorrectly allows for configuration of BFD on virtual-template and virtual-access (dialer) interfaces.

New Behavior: Cisco IOS software no longer allows configuration of BFD on these types of interfaces.

Additional information:

http://www.cisco.com/en/US/docs/ios/iproute_bfd/configuration/guide/irb_bfd_ps6017_TSD_Products_Configuration_Guide_Chapter.html

- For a virtual switch (VS), the **show tech-support** command now includes information about the active and standby switches.

Old Behavior: When the **show tech-support** command is entered on a virtual switch (VS), the command output includes the output of the **show module** command and the **show power** command for only the active switch.

New Behavior: When the **show tech-support** command is entered on a virtual switch (VS), the command output includes the output of the **show module** command and the **show power** command for both the active and standby switches.

Additional Information:

http://www.cisco.com/en/US/docs/ios/vswitch/command/reference/vs_book.html

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_s2.html#show_tech-support

- **ipsec manual** keyword not supported by the VPN SPA.

Old Behavior: When the **ipsec-manual** keyword is entered, the following message appears beneath the entry line: “This new crypto map will remain disabled until a peer and a valid access list have been configured.”

New Behavior: The **ipsec-manual** keyword is not supported by the VPN SPA. If the **ipsec-manual** keyword is entered, the following error message appears beneath the keyword entry line: “Manually-keyed crypto map configuration is not supported by the current crypto engine.” The change is only to the message printed. Manual keying for the VPN SPA was removed.

Additional Information:

[http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html#crypto_map_\(global_IPSec\)](http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html#crypto_map_(global_IPSec))

- Supported interfaces are now described in the **bfd** command.

Old Behavior: BFD supported interfaces were not listed in the **bfd** command.

New Behavior: Supported interfaces are now listed in the **bfd** command. The supported interfaces are Ethernet, Serial, Frame Relay, ATM, and dot1q vlan subinterfaces (with IP address on the dot1q subinterface). A note has been added to the **bfd** command documentation that states that other interfaces are not supported by BFD.

Additional Information:

http://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_pi1.html#bfd

- CLI behavior change for **show etherchannel** and **port-channel port load defer** commands.

Old Behavior: When a port is activated as part of an EtherChannel, the load share and LTL/FPOE are computed and programmed in the hardware immediately. When activation occurs during recovery of a dropped connection to a failed VSS chassis, data loss occurs, especially for multicast traffic, because the VSS chassis is not immediately ready to receive data.

New Behavior: The **show etherchannel port-channel** command is updated to display the new information provided by the **port-channel port load-defer** command syntax. By enabling the newly added **port load share deferral** feature, the load share and LTL/FPOE programming of a port are deferred for a period configurable by the user. Two new CLI commands are added: the new **port-channel port load-defer** command enables the feature on a port channel and the new **port-channel load-defer** command allows configuration of the deferral period. New fields are added to the **show etherchannel** command to display the feature configuration and state.

Additional Information:

http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s3.html#show_etherchannel

http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_o1.html#port-channel_port_load-defer

- New syslog message when VLAN addition fails.

Old Behavior: When the user attempts to add a VLAN to the VLAN database, no syslog message is sent if the operation fails.

New Behavior: When a VLAN cannot be added to the VLAN database, the following syslog message is sent:

```
%SW_VLAN-4-VLAN_ADD_FAIL: Failed to add VLAN [dec] to vlan database: [chars]
```

The user is now alerted to the condition and can investigate the cause.

Additional Information:

http://www.cisco.com/en/US/docs/ios/12_2sx/system/messages/sm2sx09.html#SW_VLAN-4

- The **TestL3HealthMonitoring** diagnostic no longer runs automatically.

Old Behavior: The **TestL3HealthMonitoring** diagnostic default automatic run setting is **enabled**.

New Behavior: The **TestL3HealthMonitoring** diagnostic default automatic run setting is **disabled**. The diagnostic can be enabled by the user after the module is online.

Additional Information:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/diagtest.html#TestL3HealthMonitoring>

Troubleshooting

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

- [System Troubleshooting, page 22](#)
- [Module Troubleshooting, page 22](#)
- [VLAN Troubleshooting, page 22](#)
- [Spanning Tree Troubleshooting, page 23](#)
- [Additional Troubleshooting Information, page 24](#)



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:

Per-switch limits:	MST	RPVST+	PVST+
• These per-switch limits apply to the following: – Release 12.2(33)SXI and later releases – Supervisor Engine 720-10GE – Supervisor Engine 720	100,000 total	12,000 total	15,000 total
	Note Messages with the per-switch limits from earlier releases are still displayed in Release 12.2(33)SXI. Messages for the per-switch limits in effect in Release 12.2(33)SXI are displayed in Release 12.2(33)SXI1 and later releases. (CSCsx62912)		
• All other releases and supervisor engines:	50,000 total	10,000 total	13,000 total

Per-module limits:	6,000	1,800	1,800

Note

- In Release 12.2(33)SXI1 and later releases, these limits do not apply to WS-X67xx and WS-X65xx switching modules. (CSCsu30263)
- 10/100 Mb 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 virtual interfaces.

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

Additional Troubleshooting Information

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

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

System Software Upgrade Instructions

See this publication:

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

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2. These documents consist of software installation guides, Cisco IOS configuration and command references, system error messages, and other documents.

Documentation is available as printed manuals or electronic documents.

Use these release notes with the documents and tools described in the following sections:

- [Release-Specific Documents, page 24](#)
- [Platform-Specific Documents, page 25](#)
- [Cisco Feature Navigator, page 25](#)
- [Cisco IOS Software Documentation Set, page 25](#)

Release-Specific Documents

The following document is specific to Cisco IOS Release 12.2 and is located on Cisco.com:

- Caveats for Cisco IOS Release 12.2

See *Caveats for Cisco IOS Release 12.2* for caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: Release Notes: Caveats

**Note**

If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, **log in** to Cisco.com and click **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to this URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Platform-Specific Documents

These publications are available for Release 12.2(33)SXH and later releases:

- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Module Installation Guide*
- *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

The Cisco IOS software documentation set is available on Cisco.com.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2: Configuration Guides and Command References

Release 12.2 Documentation Set

[Table 1](#) lists the contents of the Cisco IOS Release 12.2 software documentation set.



Note

You can find the most current Cisco IOS documentation on Cisco.com.

On Cisco.com at:

Technical Documents: Cisco IOS Software: Cisco IOS Release 12.2

Table 1 *Cisco IOS Release 12.2 Documentation Set*

Books	Major Topics
- Cisco IOS Configuration Fundamentals Configuration Guide - Cisco IOS Configuration Fundamentals Command Reference	Cisco IOS User Interfaces File Management System Management
- Cisco IOS Bridging and IBM Networking Configuration Guide - Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2 - Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server

Table 1 **Cisco IOS Release 12.2 Documentation Set (continued)**

Books	Major Topics
• Cisco IOS Dial Technologies Configuration Guide • Cisco IOS Dial Technologies Command Reference	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
• <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i>	LAN Interfaces Serial Interfaces Logical Interfaces
• Cisco IOS IP Configuration Guide • Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services • Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols • Cisco IOS IP Command Reference, Volume 3 of 3: Multicast	IP Addressing and Services IP Routing Protocols IP Multicast
• Cisco IOS AppleTalk and Novell IPX Configuration Guide • Cisco IOS AppleTalk and Novell IPX Command Reference	AppleTalk Novell IPX
• Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide • Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• Cisco IOS Voice, Video, and Fax Configuration Guide • <i>Cisco IOS Voice, Video, and Fax Command Reference</i>	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• Cisco IOS Quality of Service Solutions Configuration Guide • <i>Cisco IOS Quality of Service Solutions Command Reference</i>	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 1 *Cisco IOS Release 12.2 Documentation Set (continued)*

Books	Major Topics
• Cisco IOS Security Configuration Guide • <i>Cisco IOS Security Command Reference</i>	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• Cisco IOS Switching Services Configuration Guide • Cisco IOS Switching Services Command Reference	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• Cisco IOS Wide-Area Networking Configuration Guide • Cisco IOS Wide-Area Networking Command <i>Reference</i>	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
• Cisco IOS Mobile Wireless Configuration Guide • Cisco IOS Mobile Wireless Command Reference	General Packet Radio Service
• Cisco IOS Terminal Services Configuration Guide • Cisco IOS Terminal Services Command Reference	ARA LAT NAS1 Telnet TN3270 XRemote X.28 PAD Protocol Translation
• <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • Cisco IOS Debug Command Reference • Cisco IOS Software System Error Messages • Release Notes (Release note and caveat documentation for 12.2-based releases and various platforms)	

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

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

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

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

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

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

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

Original SSLeay License:

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

© 2003–2010, Cisco Systems, Inc.
All rights reserved.

Supported Hardware

These sections describe the hardware supported in Release 12.2(33)SXH and later releases:

- [Cisco ME 6500 Series Ethernet Switches \(ME6524\), page 34](#)
- [Supervisor Engines, page 36](#)
- [Policy Feature Cards, page 43](#)
- [Distributed and Centralized Forwarding Cards, page 48](#)
- [Transceivers, page 55](#)
- [10-Gigabit Ethernet Switching Modules, page 62](#)
- [Gigabit Ethernet Switching Modules, page 69](#)
- [Power over Ethernet Daughtercards, page 77](#)
- [10/100/1000 Ethernet Switching Modules, page 78](#)
- [Fast Ethernet Switching Modules, page 84](#)
- [Ethernet/Fast Ethernet \(10/100\) Switching Modules, page 85](#)
- [Shared Port Adapter \(SPA\) Interface Processors \(SIPs\), page 89](#)
- [Shared Port Adapters \(SPAs\), page 90](#)
- [Services SPA Carrier \(SSC\), page 93](#)
- [Services SPAs, page 94](#)
- [Enhanced FlexWAN Module, page 94](#)
- [Enhanced FlexWAN Module Port Adapters, page 95](#)
- [Service Modules, page 96](#)
- [Fan Trays, page 101](#)
- [Power Supplies, page 101](#)
- [Chassis, page 105](#)

**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 the SP of these supervisor engines:
 - Supervisor Engine 720-10GE.
 - Supervisor Engine 720 with a [CompactFlash adapter](#) and CompactFlash card sold by Cisco Systems, Inc., for use in Supervisor Engine 720-10GE.
 - Supervisor Engine 32.
 - **sup-bootflash:** on the SP of these supervisor engines:
 - Supervisor Engine 720 without a CompactFlash adapter and CompactFlash card sold by Cisco Systems, Inc., for use in Supervisor Engine 720.
 - ME 6500.
 - **disk0:** on these supervisor engines:
 - Supervisor Engine 720-10GE.
 - Supervisor Engine 720.
 - Supervisor Engine 32.
 - ME 6500.
 - **disk1:** on a Supervisor Engine 720.

Cisco ME 6500 Series Ethernet Switches (ME6524)

- [Cisco ME 6500 Series Ethernet Switches Restrictions, page 34](#)
- [Cisco ME 6500 Series Ethernet Switches Features, page 35](#)

Cisco ME 6500 Series Ethernet Switches Restrictions

Cisco ME 6500 Series Ethernet switches cannot support these software features and commands:

- Egress multicast replication
- Multicast replication mode detection
- Fabric configuration commands
- RPR and SSO redundancy
- VLAN translation

Cisco ME 6500 Series Ethernet Switches Features

Product ID (append “=” for spares)	Product Description	Minimum Software Version
ME-C6524GS-8S	Cisco ME 6500 Series Ethernet switches: - Switch processor (SP): - For Cisco IOS images, 256-MB DRAM (some images require more DRAM) - For Cisco IOS modularity images, with releases earlier than Release 12.2(33)SXH3, 256-MB DRAM (some images require more DRAM) - For Cisco IOS modularity images, with Release 12.2(33)SXH3 and later releases, 512-MB DRAM required (some images require more DRAM) 128-MB bootflash (sup-bootflash:; from ROMMON, it is bootflash:) - Route processor (RP)—Multilayer Switch Feature Card 2A (MSFC2A): 512-MB DRAM (some images require more DRAM) 64-MB bootflash (bootflash:) - Policy Feature Card 3C (PFC3C) - See the “Policy Feature Cards” section on page 43) - ME 6500 switches always operate in PFC3C mode. Enter the show platform hardware pfc mode command to display the PFC3 mode. - Fan tray: FAN-C6524 - Power supplies (can be used together): - PWR-400W-DC - PWR-400W-AC 64 chassis MAC addresses - One external CompactFlash Type II slot (disk0:; supports CompactFlash Type II Flash PC cards sold by Cisco Systems, Inc., for use in Cisco ME 6500 Series Ethernet switches) - Eight SFP ports: - Requires Small Form-Factor Pluggable (SFP) Modules 1 port group: ports 25–32 - QoS port architecture (Rx/Tx): 2q8t/1p3q8t - ME-C6524GS-8S: 24 SFP ports (requires Small Form-Factor Pluggable (SFP) Modules) 4 port groups: ports 1–6, 7–12, 13–18, 19–24 - QoS port architecture (Rx/Tx): 1q2t/1p3q8t - ME-C6524GT-8S: 24 10/100/1000 Mbps RJ-45 Ethernet ports 4 port groups: ports 1–6, 7–12, 13–18, 19–24 - QoS port architecture (Rx/Tx): 1q2t/1p3q8t	12.2(33)SXH
ME-C6524GT-8S		

Note See this publication for Cisco ME 6500 Series Ethernet switch hardware information:

http://www.cisco.com/en/US/products/ps6845/tsd_products_support_series_home.html

Supervisor Engines

- [Supervisor Engine 720-10GE \(CAT6000-VS-S720-10G/MSFC3\)](#), page 36
- [Supervisor Engine 720 \(CAT6000-SUP720/MSFC3\)](#), page 38
- [Supervisor Engine 32 \(CAT6000-SUP32/MSFC2A\)](#), page 42



Note

For information about DRAM requirements on all supervisor engines, see this publication:
http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/qa_c67_457347.html

Supervisor Engine 720-10GE (CAT6000-VS-S720-10G/MSFC3)

- [Supervisor Engine 720-10GE Common Features](#), page 36
- [Supervisor Engine 720-10GE with PFC3C and PFC3CXL](#), page 37
- [Supervisor Engine 720-10GE Restrictions](#), page 37

Supervisor Engine 720-10GE Common Features

- Switch processor (SP):
 - Internal 1-GB CompactFlash card (**sup-bootdisk:**).
 - 1-GB [DRAM](#).
- Route processor (RP):
 - Internal 64-MB bootflash.
 - 1-GB [DRAM](#).
- One of these:
 - Policy Feature Card 3CXL (PFC3CXL).
 - Policy Feature Card 3C (PFC3C).
 - See the [“Policy Feature Cards”](#) section on page 43.
- Integrated 720-Gbps Switch Fabric.
- One external slot:
 - **disk0:**
 - For CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 720-10GE.
- Console port—EIA/TIA-232 (RS-232) port.
- Ports 1 and 2:
 - QoS architecture: **2q4t/1p3q4t**
 - Support for these SFPs
 - [Gigabit and 10/100/1000 Mbps Ethernet SFPs](#)
 - [Fast Ethernet SFPs](#)
- Port 3:
 - 10/100/1000 Mbps RJ-45
 - QoS architecture: **2q4t/1p3q4t**

- Ports 4 and 5:
 - Support for 10-Gigabit Ethernet [X2](#) transceivers
 - QoS architecture: **2q4t/1p3q4t**
- One port group: ports 1 through 5.
- Two Universal Serial Bus (USB) 2.0 ports (not currently enabled)

Supervisor Engine 720-10GE with PFC3C and PFC3CXL

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
VS-S720-10G-3CXL	8.65 A @42 V	Supervisor Engine 720-10GE with PFC3CXL	12.2(33)SXH ¹
VS-S720-10G-3C	8.05 A @42 V	Supervisor Engine 720-10GE with PFC3C	12.2(33)SXH ¹

1. If there are no DFC-equipped modules installed, certain configurations require Release 12.2(33)SXH1 or later and impose configuration restrictions that are described in [CSCsj95733](#).

Supervisor Engine 720-10GE Restrictions

- The 1-Gigabit Ethernet ports and the 10-Gigabit Ethernet ports have the same QoS port architecture (**2q4t/1p3q4t**) unless you disable the 1-Gigabit Ethernet ports with the **mls qos 10g-only** global configuration command. With the 1-Gigabit Ethernet ports disabled, the QoS port architecture of the 10-Gigabit Ethernet ports is **8q4t/1p7q4t**.
- In RPR redundancy mode, the ports on a Supervisor Engine 720-10GE in standby mode are disabled.
- Supervisor Engine 720-10GE requires a high-capacity fan tray (see the [“Fan Trays” section on page 101](#))
- There are no memory-only upgrade options for the Supervisor Engine 720-10GE.

Supervisor Engine 720 (CAT6000-SUP720/MSFC3)

- [Supervisor Engine 720 Common Features](#), page 38
- [Supervisor Engine 720 with PFC3BXL](#), page 39
- [Supervisor Engine 720 with PFC3B](#), page 40
- [Supervisor Engine 720 with PFC3A](#), page 41

Supervisor Engine 720 Common Features

- Integrated 720-Gbps Switch Fabric
- Internal 64-MB bootflash device (**sup-bootflash:**) or CompactFlash card (**sup-bootdisk:**), 512 MB or larger.
 - As an upgrade, WS-CF-UPG=
 - See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_17277.html
- Two external slots (disk0: and disk1:) for CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 720.



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 or 10/100/1000 Mbps Ethernet SFP](#)
 - Port 2—Configurable as:
 - [Gigabit or 10/100/1000 Mbps Ethernet SFPs](#)
 - 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 101](#))

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: - Switch processor (SP): - Internal 64-MB bootflash device (sup-bootflash:) or internal CompactFlash card (sup-bootdisk:) 1-GB or larger DRAM - Route processor (RP): 1-GB or larger DRAM 64-MB bootflash - Policy Feature Card 3BXL (PFC3BXL)—See the "Policy Feature Cards" section on page 43.	12.2(17b)SXA

Note

- With Release 12.2(33)SXI and later releases, you can upgrade the WS-SUP720-3BXL memory to 2-GB **DRAM** on the Supervisor Engine 720 and 2-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
- 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: - Switch processor (SP): - Internal 64-MB bootflash device (sup-bootflash:) or internal CompactFlash card (sup-bootdisk:) 512-MB or larger DRAM - Route processor (RP): 64-MB bootflash 512-MB or larger DRAM - Policy Feature Card 3B (PFC3B)—See the “Policy Feature Cards” section on page 43	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. Release 12.2(33)SXI and later releases support 2-GB of DRAM.
 - 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: - Switch processor - Internal 64-MB bootflash device (sup-bootflash:) or internal 512 MB CompactFlash card (sup-bootdisk:) 512-MB DRAM - Route processor: 64-MB bootflash 512-MB DRAM - Policy Feature Card 3A (PFC3A; see the "Policy Feature Cards" section on page 43)	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-PFC3B=** to upgrade a WS-SUP720 with a PFC3B. 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. Release 12.2(33)SXI and later releases support 2-GB of DRAM.
 - 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-PFC3B= or WS-F6K-PFC3BXL=, do not upgrade the memory on the switch processor or the route processor on a WS-SUP720.

Supervisor Engine 32 (CAT6000-SUP32/MSFC2A)

- [Supervisor Engine 32 Restrictions, page 42](#)
- [Supervisor Engine 32 Features, page 43](#)

Supervisor Engine 32 Restrictions

- Supervisor Engine 32 requires a high-capacity fan tray (see the [“Fan Trays” section on page 101](#)).
- In some chassis, Supervisor Engine 32 requires a high-capacity power supply (see the [“Power Supplies” section on page 101](#)).
- Supervisor Engine 32 cannot support this hardware:
 - DFCs (switching modules with DFCs do not power up with a Supervisor Engine 32)
 - WS-X6700 series switching modules
 - WS-X6816-GBIC switching modules
 - The WS-SVC-WISM-1-K9 Wireless Services Module (WiSM)
 - 7600-SIP-600 SPA Interface Processor-600 and SPA supported only in 7600-SIP-600.
- Supervisor Engine 32 does not support this hardware:
 - WS-F6K-PFC3A Policy Feature Card 3A (PFC3A)
 - WS-F6K-PFC3BXL Policy Feature Card 3BXL (PFC3BXL)
 - CISCO7603 3-slot chassis
- 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 SFP ports - Requires Gigabit or 10/100/1000 Mbps Ethernet SFPs - QoS port architecture (Rx/Tx): 2q8t/1p3q8t - One external slot (disk0:) for CompactFlash Type II flash PC cards sold by Cisco Systems, Inc., for use in Supervisor Engine 32 - Switch processor - Internal 256 MB CompactFlash card (sup-bootdisk:) 512-MB or more DRAM (some images require more DRAM) - Route processor: - Internal 64-MB bootflash 512-MB or more DRAM (some images require more DRAM) - Policy Feature Card 3B (PFC3B)—See the “Policy Feature Cards” section on page 43 - Two Universal Serial Bus (USB) 2.0 ports (not currently enabled)	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

Policy Feature Cards

- [Policy Feature Card Guidelines and Restrictions, page 44](#)
- [Policy Feature Card 3CXL, page 46](#)
- [Policy Feature Card 3C, page 46](#)
- [Policy Feature Card 3BXL, page 47](#)
- [Policy Feature Card 3B, page 47](#)
- [Policy Feature Card 3A, page 47](#)

Policy Feature Card Guidelines and Restrictions

- The PFC3C supports a theoretical maximum of 96 K MAC addresses (64 K MAC addresses recommended maximum).
- The PFC3A, PFC3B, and PFC3BXL support 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 processed by the route processor in software.

The defaults for [XL mode](#) are:

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

The defaults for [Non-XL mode](#) are:

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



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

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

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

Enter the [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 on one supervisor engine and a different type on the other supervisor engine for redundancy. You must use identical policy feature cards for redundancy.
- PFC3A—These restrictions apply to a configuration with a PFC3A and these DFCs:
 - PFC3A and DFC3A—No restrictions (PFC3A mode; does not support virtual switch mode).
 - PFC3A and DFC3B—The PFC3A restricts DFC3B functionality: the DFC3B functions as a DFC3A (PFC3A mode; does not support virtual switch mode).

- PFC3A and DFC3BXL—The PFC3A restricts DFC3BXL functionality: the DFC3BXL functions as a DFC3A (PFC3A mode; does not support virtual switch mode).
- PFC3A and DFC3C—The PFC3A restricts DFC3C functionality: the DFC3C functions as a DFC3A (PFC3A mode; does not support virtual switch mode).
- PFC3A and DFC3CXL—The PFC3A restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3A (PFC3A mode; does not support virtual switch 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; does not support virtual switch mode).
 - PFC3B and DFC3B—No restrictions (PFC3B mode; does not support virtual switch 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; does not support virtual switch mode).
 - PFC3B and DFC3C—The PFC3B restricts DFC3C functionality: the DFC3C functions as a DFC3B (PFC3B mode; does not support virtual switch mode).
 - PFC3B and DFC3CXL—The PFC3B restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3B (PFC3B mode; does not support virtual switch 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; does not support virtual switch 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; does not support virtual switch mode).
 - PFC3BXL and DFC3BXL—No restrictions (PFC3BXL mode; does not support virtual switch 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; does not support virtual switch mode).
 - PFC3BXL and DFC3CXL—The PFC3BXL restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3BXL (PFC3BXL mode; does not support virtual switch mode).
- PFC3C—These restrictions apply to a configuration with a PFC3C and these DFCs:
 - PFC3C and DFC3A—PFC3C functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3C functions as a PFC3A (PFC3A mode; does not support virtual switch mode).
 - PFC3C and DFC3B—PFC3C functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3C functions as a PFC3B (PFC3B mode; does not support virtual switch mode).
 - PFC3C and DFC3BXL—PFC3C functionality is restricted by the DFC3BXL: after a reload with a DFC3BXL-equipped module installed, the PFC3C functions as a PFC3BXL (PFC3BXL mode; does not support virtual switch mode).
 - PFC3C and DFC3C—No restrictions (PFC3C mode).
 - PFC3C and DFC3CXL—The PFC3C restricts DFC3CXL functionality: the DFC3CXL functions as a DFC3C (PFC3C mode).

- PFC3CXL—These restrictions apply to a configuration with a PFC3CXL and these DFCs:
 - PFC3CXL and DFC3A—PFC3CXL functionality is restricted by the DFC3A: after a reload with a DFC3A-equipped module installed, the PFC3CXL functions as a PFC3A (PFC3A mode; does not support virtual switch mode).
 - PFC3CXL and DFC3B—PFC3CXL functionality is restricted by the DFC3B: after a reload with a DFC3B-equipped module installed, the PFC3CXL functions as a PFC3B (PFC3B mode; does not support virtual switch mode).
 - PFC3CXL and DFC3BXL—PFC3CXL functionality is restricted by the DFC3BXL: after a reload with a DFC3BXL-equipped module installed, the PFC3CXL functions as a PFC3BXL (PFC3BXL mode; does not support virtual switch mode).
 - PFC3CXL and DFC3C—PFC3CXL functionality is restricted by the DFC3C: after a reload with a DFC3C-equipped module installed, the PFC3CXL functions as a PFC3C (PFC3C mode).
 - PFC3CXL and DFC3CXL—No restrictions (PFC3CXL mode).
- Switching modules that you install after bootup that are equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode remain powered down.
- You must reboot to use a switching module equipped with a DFC that imposes a more restricted PFC mode than the current PFC mode.

Policy Feature Card 3CXL

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
VS-F6K-PFC3CXL	2.50 A@42 V	Policy Feature Card 3CXL (PFC3CXL)	
		Supported only with Supervisor Engine 720-10GE	12.2(33)SXH

Note Use VS-F6K-PFC3CXL= to upgrade a [VS-S720-10G-3C](#) with a PFC3CXL. 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 3C

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
		Policy Feature Card 3C (PFC3C)	
VS-F6K-PFC3C	1.90 A@42 V	With Supervisor Engine 720-10GE	12.2(33)SXH
ME-C6524-PFC3C	—	With Cisco ME 6500 Series Ethernet switches	12.2(33)SXH

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 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 Use [WS-F6K-PFC3B=](#) to upgrade a [WS-SUP720](#) with a PFC3B. 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 WS-F6K-PFC3A is available only on [WS-SUP720](#). It is not orderable.

Distributed and Centralized Forwarding Cards

- [Distributed Forwarding Card 3CXL, page 48](#)
- [Distributed Forwarding Card 3C, page 49](#)
- [Distributed Forwarding Card 3BXL, page 49](#)
- [Distributed Forwarding Card 3B, page 51](#)
- [Distributed Forwarding Card 3A, page 53](#)
- [Centralized Forwarding Card \(WS-F6700-CFC\), page 54](#)


Note

See the “[Policy Feature Cards](#)” section on page 43 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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720 and all WS-X6700 series modules	12.2(33)SXH
		With Supervisor Engine 720 and WS-X6708-10GE	12.2(18)SXF5

Note

- Use with Release 12.2(33)SXH or later requires 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-F6700-DFC3CXL uses memory that is installed on the switching module.

- See this publication for information about WS-F6700-DFC3CXL upgrades:

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

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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720 and all WS-X6700 series modules	12.2(33)SXH
		With Supervisor Engine 720 and WS-X6708-10GE	12.2(18)SXF5

Note

- Use with Release 12.2(33)SXH or later requires 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-F6700-DFC3C uses memory that is installed on the switching module.
- See this publication for information about WS-F6700-DFC3C upgrades:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_15893.html

Distributed Forwarding Card 3BXL

- [WS-F6700-DFC3BXL](#), page 49
- [WS-F6K-DFC3BXL](#), page 50

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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(17d)SXB6

Note

- Not supported in virtual switch mode.
- Use with Release 12.2(33)SXH or later requires 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-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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXD3

Note

- Not supported in virtual switch mode.
- Use with Release 12.2(33)SXH or later requires DFC 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_6010.html
- 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, page 51](#)
- [WS-F6K-DFC3B, page 52](#)

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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(17d)SXB6

Note

- Not supported in virtual switch mode.
- Use with Release 12.2(33)SXH or later requires 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-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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXD3

Note

- Not supported in virtual switch mode.
- Use with Release 12.2(33)SXH or later requires DFC 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_6010.html
- 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, page 53](#)
- [WS-F6K-DFC3A, page 54](#)

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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(17a)SX

Note

- Not supported in virtual switch mode.
- Use with Release 12.2(33)SXH or later requires 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-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

- Not supported in virtual switch mode.
- Use with Release 12.2(33)SXH or later requires DFC 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_6010.html
- 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>

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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(17a)SX

Note

- Use with Release 12.2(33)SXH or later requires 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
- There are no memory upgrade options for WS-F6700-CFC.

Transceivers

- [X2 Modules](#), page 55
- [XENPAKs](#), page 57
- [Small Form-Factor Pluggable \(SFP\) Modules](#), page 59
- [Gigabit Interface Converters \(GBICs\)](#), page 61

X2 Modules



Note

- [WS-X6708-10GE](#) and [WS-X6716-10GE](#) do not support X2 modules shipped before the release of [WS-X6708-10GE](#) with Release 12.2(18)SXF5. The unsupported X2 modules are labeled with a number that ends with -01. (This restriction does not apply to X2-10GB-LRM.)
- All X2 modules shipped since [WS-X6716-10GE](#) became available provide EMI compliance with WS-X6716-10G.
- Some X2 modules shipped before [WS-X6716-10GE](#) became available might not provide EMI compliance with WS-X6716-10G. See the information listed for each type of X2 module in the following table.
- For information about X2 modules, see the *Cisco 10GBASE X2 Modules* data sheet:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6574/product_data_sheet0900aecd801f92aa.html

Product ID (append “=” for spares)	Product Description	Minimum Software Version
CVR-X2-SFP10G	10G X2 to SFP+ Converter	12.2(33)SX12
	Note SFP-10G-SR SFP+ transceivers are supported.	

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

Product ID (append “=” for spares)	Product Description	Minimum Software Version
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) Note X2-10GB-ER modules labeled with a number that ends with -02 do not provide EMI compliance with WS-X6716-10GE .	12.2(18)SXF5
X2-10GB-LR	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF) Note X2-10GB-LR modules labeled with a number that ends with -02 or -03 do not provide EMI compliance with WS-X6716-10GE .	12.2(18)SXF5
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-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF) Note - See field notice 62840 for information about unsupported 10GBASE-LX4 modules: http://www.cisco.com/en/US/ts/fn/misc/FN62840.html - X2-10GB-LX4 modules labeled with a number that ends with -01 to -03 do not provide EMI compliance with WS-X6716-10GE.	12.2(18)SXF5
X2-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	12.2(18)SXF5

XENPAKs



Note

- For information about DWDM XENPAKs, see the *Cisco 10GBase DWDM XENPAK Modules* data sheet:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6576/product_data_sheet0900aecd801f9333.html
- For information about other XENPAKs, see the *Cisco 10GBASE XENPAK Modules* data sheet:
http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a008007cd00_ps5251_Products_Data_Sheet.html

Product ID (append “=” for spares)	Product Description	Minimum Software Version
XENPAK-10GB-LRM	10GBASE-LRM XENPAK Module for MMF Note Not supported by the show idprom command. (CSCsl21260)	12.2(33)SXH1
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; uses Infiniband connectors	12.2(17d)SXB1

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) Note XENPAK-10GB-ER units with Part No. 800-24557-01 are not supported, as described in this external field notice (CSCee47030): http://www.cisco.com/en/US/ts/fn/200/fn29736.html	12.2(17a)SX
XENPAK-10GB-ER+	10GBASE-ER Serial 1550-nm extended-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
XENPAK-10GB-LR+	10GBASE-LR Serial 1310-nm long-reach, single-mode fiber (SMF), dispersion-shifted fiber (DSF)	12.2(17a)SX
XENPAK-10GB-LW	10GBASE-LW XENPAK Module with WAN PHY for SMF Note XENPAK-10GB-LW operates at an interface speed compatible with SONET/SDH OC-192/STM-64. XENPAK-10GB-LW links might go up and down if the data rate exceeds 9Gbs. (CSCsi58211)	12.2(18)SXE
XENPAK-10GB-LX4	10GBASE-LX4 Serial 1310-nm multimode (MMF)	12.2(17a)SX1
XENPAK-10GB-SR	10GBASE-SR Serial 850-nm short-reach multimode (MMF)	12.2(17a)SX1
XENPAK-10GB-ZR	10GBASE for any SMF type	12.2(18)SXF

Small Form-Factor Pluggable (SFP) Modules

These sections describe SFPs:

- [Gigabit and 10/100/1000 Mbps Ethernet SFPs, page 59](#)
- [Fast Ethernet SFPs, page 61](#)

Gigabit and 10/100/1000 Mbps Ethernet SFPs



Note

- For information about coarse wavelength-division multiplexing (CWDM) SFPs, see the *Cisco CWDM GBIC and SFP Solutions* data sheet:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6575/product_data_sheet09186a00801a557c_ps4999_Products_Data_Sheet.html
- For information about DWDM SFPs, see the *Cisco CWDM GBIC and SFP Solutions* data sheet:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6576/product_data_sheet0900aecd80582763.html
- See the “Unsupported Hardware” section on page 110 for information about unsupported DWDM-SFPs.
- For information about other SFPs, see the *Cisco SFP Optics For Gigabit Ethernet Applications* data sheet:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6577/product_data_sheet0900aecd8033f885.html

Product ID (append “=” for spares)	Product Description	Minimum Software Version
GLC-BX-D	1000BASE-BX10 SFP module for single-strand SMF, 1490-nm TX/1310-nm RX wavelength	12.2(18)SXE
GLC-BX-U	1000BASE-BX10 SFP module for single-strand SMF, 1310-nm TX/1490-nm RX wavelength	12.2(18)SXE
GLC-LH-SM	1000BASE-LX/LH SFP	12.2(17a)SX
GLC-SX-MM	1000BASE-SX SFP	12.2(14)SX
GLC-T	1000BASE-T 10/100/1000 SFP module Note Supported only at 1000 Mbps in WS-X6748-SFP and WS-X6724-SFP .	12.2(17a)SX
GLC-ZX-SM	1000BASE-ZX SFP module	12.2(17d)SXB1

Product ID (append “=” for spares)	Product Description	Minimum Software Version
DWDM-SFP-5817	1000BASE-DWDM 1558.17 nm SFP (100-GHz ITU grid) SFP module	12.2(33)SXH
DWDM-SFP-5252	1000BASE-DWDM 1552.52 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-5172	1000BASE-DWDM 1551.72 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-5012	1000BASE-DWDM 1550.12 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4692	1000BASE-DWDM 1546.92 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4373	1000BASE-DWDM 1543.73 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4214	1000BASE-DWDM 1542.14 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3977	1000BASE-DWDM 1539.77 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3898	1000BASE-DWDM 1538.98 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3582	1000BASE-DWDM 1535.82 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3504	1000BASE-DWDM 1535.04 nm SFP (100-GHz ITU grid) SFP module	
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-5092	1000BASE-DWDM 1550.92 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4851	1000BASE-DWDM 1548.51 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4772	1000BASE-DWDM 1547.72 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4612	1000BASE-DWDM 1546.12 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4453	1000BASE-DWDM 1544.53 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4294	1000BASE-DWDM 1542.94 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-4056	1000BASE-DWDM 1540.56 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3819	1000BASE-DWDM 1538.19 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3661	1000BASE-DWDM 1536.61 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3425	1000BASE-DWDM 1534.25 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3268	1000BASE-DWDM 1532.68 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3190	1000BASE-DWDM 1531.90 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3112	1000BASE-DWDM 1531.12 nm SFP (100-GHz ITU grid) SFP module	
DWDM-SFP-3033	1000BASE-DWDM 1530.33 nm SFP (100-GHz ITU grid) SFP module	

Fast Ethernet SFPs



Note

- Fast Ethernet SFPs are supported in these modules:
 - CAT6000-VS-S720-10G/MSFC3
 - ME6524
 - WS-X6148-FE-SFP
- For information about Fast Ethernet SFPs, see the *Cisco 100BASE-X SFP For Fast Ethernet SFP Ports* data sheet:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6578/product_data_sheet0900aecd801f931c.html

Product ID (append “=” for spares)	Product Description	Minimum Software Version
GLC-FE-100BX-U	100BASE-BX10-U SFP	12.2(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



Note

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

Gigabit Interface Converters (GBICs)



Note

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

Product ID (append “=” for spares)	Product Description	Minimum Software Version
WDM-GBIC-REC	Receive-only wavelength division multiplexing (WDM) GBIC	12.2(18)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	1000BASE-T GBIC	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

- [WS-X6716-10GE 16-port 10-Gigabit Ethernet X2 Switching Module, page 63](#)
- [WS-X6708-10GE 8-port 10-Gigabit Ethernet X2 Switching Module, page 65](#)
- [WS-X6704-10GE 4-port 10-Gigabit Ethernet XENPAK Switching Module, page 66](#)
- [WS-X6502-10GE 1-port 10-Gigabit Ethernet Switching Module, page 68](#)

WS-X6716-10GE 16-port 10-Gigabit Ethernet X2 Switching Module



Note

- WS-X6716-10G-3C and WS-X6716-10G-3CXL are the orderable product IDs.
- The front panel is labeled WS-X6716-10GE.
- Cisco IOS software commands display WS-X6716-10GE with either WS-F6700-DFC3C or WS-F6700-DFC3CXL.
- To configure WS-X6716-10GE port oversubscription, use the **hw-module slot** command.
- In these chassis, operation of a WS-X6716-10GE 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-X6716-10GE.



Note

All E-Series [chassis](#) provide NEBS compliance.

- Support in the [WS-C6509-NEB-A](#) chassis requires two [FAN-MOD-09](#) modules.
- WS-X6716-10GE is not supported in the [WS-C6503](#) and [CISCO7603](#) chassis.
- In a [13-slot chassis](#), WS-X6716-10GE is supported only in slots 9 through 13 and does not power up in other slots.
- With Release 12.2(33)SXH1, WS-X6716-10GE ports in [oversubscription mode](#) do not support VACL capture. ([CSCsm46682](#))

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6716-10G-3CXL (WS-X6716-10GE with WS-F6700-DFC3CXL)	11.60 @42 V	16-port 10-Gigabit Ethernet X2 module dCEF720	
WS-X6716-10G-3C (WS-X6716-10GE with WS-F6700-DFC3C)	10.90 @42 V	- Supports egress multicast replication - QoS port architecture (Rx/Tx): - Oversubscription mode: 1p7q2t/1p7q4t - Performance mode: 8q4t/1p7q4t - Dual switch-fabric connections - Fabric Channel #1: ports 1–8 - Fabric Channel #2: ports 9–16 - Number of ports: 16 - Number of port groups: 4 - Port ranges per port group: 1–4, 5–8, 9–12, 13–16	
Note - Not supported in virtual switch links with Releases earlier than Release 12.2(33)SXI. - When not configured in oversubscription mode, supported in virtual switch links with Release 12.2(33)SXI and later releases.		With Supervisor Engine 720-10GE	12.2(33)SXH2
		With Supervisor Engine 720	12.2(33)SXH2

WS-X6708-10GE 8-port 10-Gigabit Ethernet X2 Switching Module



Note

- 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, use the **hw-module oversubscription** command.
- 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 is supported in the [WS-C6503-E](#) chassis.
- 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.
- WS-X6708-10GE ports do not support VACL capture. ([CSCsb59015](#))

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 X2 module dCEF720	
WS-X6708-10G-3CXL (WS-X6708-10GE with WS-F6700-DFC3CXL)	11.28A @ 42V	- Supports egress multicast replication - QoS port architecture (Rx/Tx): 8q4t/1p7q4t - Dual switch-fabric connections Fabric Channel #1: Ports 2, 3, 6, 8 Fabric Channel #2: Ports 1, 4, 5, 7 - Number of ports: 8 Number of port groups: 8 Port ranges per port group: 1 port in each group	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXF5

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



Note

- Use with Release 12.2(33)SXH or later requires 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-DFC3CXL (2.35 A@42 V)
 - WS-F6700-DFC3C (1.65 A@42 V)
 - 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-DFC3CXL, WS-F6700-DFC3C, 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-X6704-10GE	6.28 A@42 V	4-port 10-Gigabit Ethernet XENPAK	
		- dCEF720 with WS-F6700-DFC3CXL (adds 2.35 A@42 V) - dCEF720 with WS-F6700-DFC3C (adds 1.65 A@42 V) - dCEF720 with WS-F6700-DFC3BXL - Adds 3.30 A@42 V - Not supported in virtual switch mode - dCEF720 with WS-F6700-DFC3B - Adds 2.70 A@42 V - Not supported in virtual switch mode - dCEF720 with WS-F6700-DFC3A - Adds 3.00 A@42 V - Not supported in virtual switch mode - CEF720 with WS-F6700-CFC (adds 0.75 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	
		Note Review the ROMMON requirements .	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720 and DFC3C or DFC3CXL	12.2(33)SXH
		With Supervisor Engine 720	12.2(17a)SX

WS-X6502-10GE 1-port 10-Gigabit Ethernet Switching Module

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	
Note Not supported in virtual switch mode.		- 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) - 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	
		Note Review the ROMMON requirements .	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

Note

- Use with Release 12.2(33)SXH or later and a DFC requires DFC 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_6010.html
- 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

- [WS-X6748-SFP 48-port Gigabit Ethernet SFP Switching Module](#), page 69
- [WS-X6724-SFP 24-port Gigabit Ethernet SFP Switching Module](#), page 71
- [WS-X6816-GBIC 16-port Gigabit Ethernet GBIC Switching Module](#), page 73
- [WS-X6516A-GBIC 16-Port Gigabit Ethernet GBIC Switching Module](#), page 74
- [WS-X6516-GBIC 16-Port Gigabit Ethernet GBIC Switching Module](#), page 75
- [WS-X6416-GBIC 16-port Gigabit Ethernet GBIC Switching Module](#), page 76
- [WS-X6408A-GBIC 8-port Gigabit Ethernet GBIC Switching Module](#), page 76
- [WS-X6408-GBIC 8-port Gigabit Ethernet GBIC Switching Module](#), page 76

WS-X6748-SFP 48-port Gigabit Ethernet SFP Switching Module



Note

- Use with Release 12.2(33)SXH or later requires 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-DFC3CXL](#) (2.35 A@42 V)
 - [WS-F6700-DFC3C](#) (1.65 A@42 V)
 - [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-DFC3CXL](#), [WS-F6700-DFC3C](#), [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)

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 - dCEF720 with WS-F6700-DFC3CXL (adds 2.35 A@42 V) - dCEF720 with WS-F6700-DFC3C (adds 1.65 A@42 V) - dCEF720 with WS-F6700-DFC3BXL - Adds 3.30 A@42 V - Not supported in virtual switch mode - dCEF720 with WS-F6700-DFC3B - Adds 2.70 A@42 V - Not supported in virtual switch mode - dCEF720 with WS-F6700-DFC3A - Adds 3.00 A@42 V - Not supported in virtual switch mode - CEF720 with WS-F6700-CFC (adds 0.75 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 Note Review the ROMMON requirements.	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720 and DFC3C or DFC3CXL	12.2(33)SXH
		With Supervisor Engine 720	12.2(17d)SXB

WS-X6724-SFP 24-port Gigabit Ethernet SFP Switching Module



Note

- Use with Release 12.2(33)SXH or later requires 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-DFC3CXL](#) (2.35 A@42 V)
 - [WS-F6700-DFC3C](#) (1.65 A@42 V)
 - [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-DFC3CXL](#), [WS-F6700-DFC3C](#), [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)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6724-SFP	2.23 A@42 V	24-port Gigabit Mbps Ethernet SFP	
		- dCEF720 with WS-F6700-DFC3CXL (adds 2.35 A@42 V) - dCEF720 with WS-F6700-DFC3C (adds 1.65 A@42 V) - dCEF720 with WS-F6700-DFC3BXL - Adds 3.30 A@42 V - Not supported in virtual switch mode - dCEF720 with WS-F6700-DFC3B - Adds 2.70 A@42 V - Not supported in virtual switch mode - dCEF720 with WS-F6700-DFC3A - Adds 3.00 A@42 V - Not supported in virtual switch mode - CEF720 with WS-F6700-CFC (adds 0.75 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	
		Note Review the ROMMON requirements .	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720 and DFC3C or DFC3CXL	12.2(33)SXH
		With Supervisor Engine 720	12.2(17a)SX

WS-X6816-GBIC 16-port Gigabit Ethernet GBIC Switching Module



Note

- Use with Release 12.2(33)SXH or later requires DFC 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_6010.html
- WS-X6816-GBIC requires one of these for use with Supervisor Engine 720-10GE or 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)
- In a [13-slot chassis](#), WS-X6816-GBIC is supported only in slots 9 through 13 and does not power up in other slots.

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6816-GBIC	3.84 A@42 V	16-port Gigabit Ethernet GBIC	
Note Not supported in virtual switch mode.		• 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	
		Note Review the ROMMON requirements .	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX

WS-X6516A-GBIC 16-Port Gigabit Ethernet GBIC Switching Module


Note

- Use with Release 12.2(33)SXH or later requires DFC 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_6010.html

Product ID (append "=" for spares)	Power Required	Product Description	Minimum Software Version
WS-X6516A-GBIC	3.62 A@42 V	16-port Gigabit Ethernet GBIC	
Note Not supported in virtual switch mode.		- CEF256 - 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) 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	
		Note Review the ROMMON requirements .	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

WS-X6516-GBIC 16-Port Gigabit Ethernet GBIC Switching Module



Note

- Use with Release 12.2(33)SXH or later and a DFC requires DFC 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_6010.html
- 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>

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	
Note Not supported in virtual switch mode.		• CEF256 • 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) • 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	
		Note Review the ROMMON requirements .	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

WS-X6416-GBIC 16-port Gigabit Ethernet GBIC Switching Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6416-GBIC	2.81 A@42 V	16-port Gigabit Ethernet GBIC	
Note Not supported in virtual switch mode.		- 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

WS-X6408A-GBIC 8-port Gigabit Ethernet GBIC Switching Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6408A-GBIC	2.00 A@42 V	8-port Gigabit Ethernet GBIC	
Note Not supported in virtual switch mode.		- 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

WS-X6408-GBIC 8-port Gigabit Ethernet GBIC Switching Module

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-X6408-GBIC	2.00 A@42 V	8-port Gigabit Ethernet GBIC	
Note Not supported in virtual switch mode.		- 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
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 WS-X6548-GE-TX, WS-X6148-GE-TX, and WS-X6148A-GE-TX, supports up to 45 ports of ePoE (16.8W).	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(17d)SXB
		With Supervisor Engine 32	12.2(18)SXF
WS-F6K-VPWR-GE	0.42 A @42 V	PoE daughtercard for WS-X6548-GE-TX and WS-X6148-GE-TX	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(17a)SX
		With Supervisor Engine 32	12.2(18)SXF
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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

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 - dCEF720 with WS-F6700-DFC3CXL (adds 2.35 A@42 V) - dCEF720 with WS-F6700-DFC3C (adds 1.65 A@42 V) - dCEF720 with WS-F6700-DFC3BXL - Adds 3.30 A@42 V - Not supported in virtual switch mode - dCEF720 with WS-F6700-DFC3B - Adds 2.70 A@42 V - Not supported in virtual switch mode - dCEF720 with WS-F6700-DFC3A - Adds 3.00 A@42 V - Not supported in virtual switch mode - CEF720 with WS-F6700-CFC (adds 0.75 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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(17a)SX

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

Note

- WS-X6748-GE-TX requires one of the following:
 - [WS-F6700-DFC3CXL](#) (2.35 A@42 V)
 - [WS-F6700-DFC3C](#) (1.65 A@42 V)
 - [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-DFC3CXL](#), [WS-F6700-DFC3C](#), [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	
WS-X6548V-GE-TX	3.40 A@42 V	• RJ-45	
WS-X6548-GE-45AF	3.16 A@42 V	• CEF256	
Note Not supported in virtual switch mode.		• 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 • With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W). • 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	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		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

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:
 - 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	
Note Not supported in virtual switch mode.		- WS-X6148A-GE-TX supports WS-F6K-GE48-AF or WS-F6K-48-AF - WS-X6148A-GE-45AF has WS-F6K-GE48-AF or WS-F6K-48-AF - With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W). - QoS port architecture (Rx/Tx): 1q2t/1p3q8t - Number of ports: 48 Number of port groups: 6 Port ranges per port group: 1–8, 9–16, 17–24, 25–32, 33–40, 41–48 - The aggregate bandwidth of each port group is 1 Gbps.	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
	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	
WS-X6148V-GE-TX	2.89 A@42 V	RJ-45	
WS-X6148-GE-45AF	2.65 A@42 V	- 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 - With WS-F6K-GE48-AF, supports up to 45 ports of ePoE (16.8W). - 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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		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

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	
Note Not supported in virtual switch mode.		• 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) • 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

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	
Note Not supported in virtual switch mode.		- 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
WS-X6524-100FX-MM	1.90 A@42 V	24-port 100FX Ethernet multimode	
Note Not supported in virtual switch mode.		- 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) - 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
WS-X6324-100FX-MM	1.52 A@42 V	24-port 100FX Ethernet	
Note Not supported in virtual switch mode.		- 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

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	
Note Not supported in virtual switch mode.		- 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) - 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
WS-X6548-RJ-21	2.90 A@42 V	48-port 10/100TX RJ-21	
Note Not supported in virtual switch mode.		- 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) - 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXF3
		With Supervisor Engine 32	12.2(18)SXF3

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXF3
		With Supervisor Engine 32	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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF
WS-X6348-RJ-21V	2.39 A@42 V	48-port 10/100TX RJ-21	
Note Not supported in virtual switch mode.		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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXF
		With Supervisor Engine 32	12.2(18)SXF
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 - 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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		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	

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		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	

Shared Port Adapter (SPA) Interface Processors (SIPs)


Note

- SIPs are supported only in images that contain “_wan” in the image name.
- See the “[FPD Image Packages](#)” section on page 4 for information about additional procedures required to support SIPs with Release 12.2(18)SXE and later releases.
- 7600-SIP-400 is and 7600-SIP-600 are not supported in [PFC3A mode](#).

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
7600-SIP-600 Note Not supported in virtual switch mode.	8.14 A@42 V	SPA Interface Processor-600 (not supported in PFC3A mode)	
		Note 7600-SIP-600 has a WS-F6700-DFC3BXL. - Not supported in release 12.2(33)SXH and rebuilds.	
		With Supervisor Engine 720-10GE	12.2(33)SXI
		With Supervisor Engine 720	12.2(18)SXF
Note Supervisor Engine 32 does not support 7600-SIP-600.			
7600-SIP-400 Note Not supported in virtual switch mode.	6.31 A@42 V	SPA Interface Processor-400 (not supported in PFC3A mode)	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 32	12.2(18)SXF
7600-SIP-200 Note Not supported in virtual switch mode.	5.72 A@42 V	SPA Interface Processor-200	
		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXE
		With Supervisor Engine 32	12.2(18)SXF

Shared Port Adapters (SPAs)

These sections describe SPAs:

- [Ethernet SPAs, page 90](#)
- [POS SPAs, page 91](#)
- [ATM SPAs, page 92](#)
- [SFPs for OC3 and OC12 POS and ATM SPAs, page 92](#)
- [Serial SPAs, page 93](#)

Ethernet SPAs

These sections describe Ethernet SPAs:

- [10-Gigabit Ethernet SPAs, page 90](#)
- [Gigabit Ethernet SPAs, page 90](#)

10-Gigabit Ethernet SPAs



Note

Release 12.2(33)SXH and rebuilds do not support [7600-SIP-600](#).

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-1X10GE-L-V2	7600-SIP-400	1-Port 10 Gigabit Ethernet SPA	12.2(33)SXI2
SPA-1XTENGE-XFP	7600-SIP-600	1-port 10-Gigabit Ethernet SPA	12.2(33)SXI
XFP Modules Supported in 10-Gigabit Ethernet SPAs			
XFP-10GLR-OC192LR	10-Gigabit Ethernet LR (10 km)		

Gigabit Ethernet SPAs



Note

Release 12.2(33)SXH and rebuilds do not support [7600-SIP-600](#).

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(33)SXI
SPA-5X1GE	7600-SIP-600	5-port Gigabit Ethernet SPA, SFP Optics	12.2(33)SXI
SPA-2X1GE-V2	7600-SIP-400	2-port Gigabit Ethernet SPA, SFP Optics, version 2	12.2(33)SXI
SPA-2X1GE	7600-SIP-400	2-port Gigabit Ethernet SPA, SFP Optics	12.2(18)SXF

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SFPs Supported in Gigabit Ethernet SPAs			
SFP-GE-S	Extended Temperature	Extended Temperature SX SFP	12.2(18)SXF
SFP-GE-L		Extended Temperature LX/LH SFP	
SFP-GE-Z		Extended Temperature ZX SFP	
SFP-GE-T		Cisco 1000BASE-T SFP (NEBS 3 ESD)	12.2(33)SXH

10/100 Mbps Ethernet SPAs

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-8X1FE-TX-V2	7600-SIP-200	8-port 10/100 Ethernet SPA TX	12.2(33)SXH
SPA-4X1FE-TX-V2	7600-SIP-200	4-port 10/100 Ethernet SPA TX	12.2(33)SXH

POS SPAs



Note

- Release 12.2(33)SXH and rebuilds do not support [7600-SIP-600](#).
- With Release 12.2(33)SXI and later releases where [CSCso97991](#) is not resolved, you must configure an appropriate [burst size](#) when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-OC192POS-VSR	7600-SIP-600	1-port OC-192c/STM-64 POS/RPR SPA, VSR-1	12.2(33)SXI
SPA-OC192POS-LR	7600-SIP-600	1-port OC-192c/STM-64 POS/RPR SPA, SM-LR	12.2(33)SXI
SPA-OC192POS-XFP	7600-SIP-600	1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics	12.2(33)SXI
		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(33)SXI
SPA-2XOC48POS/RPR	7600-SIP-400	2-Port OC-48 POS/RPR SPA	12.2(33)SXI
		Note Requires SFPs .	
SPA-1XOC48POS/RPR	7600-SIP-400	1-Port OC-48 POS/RPR SPA	12.2(18)SXF10
		Note Requires SFPs .	

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

ATM SPAs



Note

- Release 12.2(33)SXH and rebuilds do not support ATM SPAs.
- With Release 12.2(33)SXI and later releases where [CSCso97991](#) is not resolved, you must configure an appropriate [burst size](#) when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.

Product ID (append "=" for spares)	SIP Support	Product Description	Minimum Software Version
SPA-1XOC12-ATM	7600-SIP-400	1-Port OC-12c/STM-4c ATM SPA Note Requires an SFP .	12.2(18)SXE
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-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



Note

With Release 12.2(33)SXI and later releases where [CSCso97991](#) is not resolved, you must configure an appropriate [burst size](#) when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.

Product ID (append “=” for spares)	SIP Support	Product Description	Minimum Software Version
SPA-1xCHSTM1/OC3	7600-SIP-200	1-port Channelized STM1/OC3 to DS0 SPA	12.2(33)SXH
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
SPA-8XCT1/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

Services SPA Carrier (SSC)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SSC-600 Note Not supported in virtual switch mode.	6.54 A @42 V	Services SPA Carrier (SSC)	12.2(33)SXI
		With Supervisor Engine 720-10GE	
		With Supervisor Engine 720	
		With Supervisor Engine 32	

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
7600-SSC-400	5.43 A@42 V	Services SPA Carrier (SSC)	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		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.		

Services SPAs


Note

See the [“FPD Image Packages”](#) section on page 4 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
WS-IPSEC-3	WS-SSC-600	IPsec SPA	12.2(33)SXI
SPA-IPSEC-2G	7600-SSC-400	IPsec SPA	12.2(18)SXE2
Note SPA-IPSEC-2G does not support TACACS+ authentication for IPsec. (CSCee33200)			

Enhanced FlexWAN 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 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(17b)SXA
		With Supervisor Engine 32	12.2(18)SXF

Note

- Not supported in virtual switch mode.
- Supported only in images that contain "_wan" in the image name.
- With Release 12.2(33)SXI and later releases where [CSCso97991](#) is not resolved, you must configure an appropriate [burst size](#) when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.

Enhanced FlexWAN Module Port Adapters

Product ID (append “=” for spares)	Product Description	Minimum Software Version
PA-2FE	2-port Fast Ethernet Port Adapter	12.2(18)SXE
PA-1FE	1-port Fast Ethernet Port Adapter	12.2(18)SXE
PA-POS-10C3	1-port Packet over SONET OC3c/STM1 Port Adapter	12.2(18)SXE
PA-POS-20C3	2-port POS OC3c/STM1	12.2(17b)SXA
SFPs for PA-POS-20C3		
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 service modules that run their own software, see the service module software release notes for information about the minimum required service module software version.
- How you have EtherChannels configured can impact some service modules. In particular, distributed EtherChannels (DECs) can interfere with service module traffic. See this field notice for more information:

<http://www.cisco.com/en/US/ts/fn/610/fn61935.html>

- [Application Control Engine \(ACE\) Module, page 97](#)
- [Anomaly Guard Module\(AGM\), page 97](#)
- [Traffic Anomaly Detector Module \(ADM\), page 97](#)
- [Communication Media Module \(CMM\), page 98](#)
- [Content Switching Module \(CSM\), page 98](#)
- [Content Switching Module with SSL \(CSM-S\), page 99](#)
- [Firewall Services Module \(FWSM\), page 99](#)
- [Intrusion Detection System Modules \(IDSMs\), page 99](#)
- [Network Analysis Modules \(NAMs\), page 100](#)
- [Wireless Services Module \(WiSM\), page 100](#)

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	
Note With releases earlier than Release 12.2(33)SXI, not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(18)SXF4

ACE10-6500-K9 and ACE20-MOD-K9 run their own software—See these publications:

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

See the ACE10-6500-K9 and ACE20-MOD-K9 software release notes for information about the minimum required service module software version.

Note Supervisor Engine 32 does not support ACE10-6500-K9 or ACE20-MOD-K9.

Anomaly Guard Module(AGM)

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 (AGM)	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH1
		With Supervisor Engine 720	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 Supervisor Engine 32 does not support WS-SVC-AGM-1-K9.

Traffic Anomaly Detector Module (ADM)

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 (ADM)	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH1
		With Supervisor Engine 720	12.2(18)SXD3

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

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 Supervisor Engine 32 does not support WS-SVC-ADM-1-K9.

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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX
		With Supervisor Engine 32	12.2(18)SXF

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.

Communication Media Module Port Adapters for WS-SVC-CMM

WS-SVC-CMM-6E1	6-Port E1 Interface Port Adapter	See the WS-SVC-CMM software release notes for information about the minimum required WS-SVC-CMM software version.
WS-SVC-CMM-6T1	6-Port T1 Interface Port Adapter	
WS-SVC-CMM-ACT	Adhoc Conferencing and Transcoding Port Adapter	
WS-SVC-CMM-24FXS	24-Port FXS Interface Port Adapter	

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	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXI2
		With Supervisor Engine 720	12.2(33)SXI2

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.

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)	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXI2
		With Supervisor Engine 720	12.2(33)SXI2

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 Supervisor Engine 32 does not support WS-X6066-SLB-S-K9.

Firewall Services Module (FWSM)

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	
Note With releases earlier than Release 12.2(33)SXI, not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF

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

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

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

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

Intrusion Detection System Modules (IDSMs)

Product ID (append “=” for spares)	Power Required	Product Description	Minimum Software Version
WS-SVC-IDSM2-K9	2.50 A@42 V	Intrusion Detection System Module 2; CEF256	
Note Not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF

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

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.

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	
Note Supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		With Supervisor Engine 720	12.2(14)SX1
		With Supervisor Engine 32	12.2(18)SXF

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

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

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

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)	
Note With releases earlier than Release 12.2(33)SXI, not supported in virtual switch mode.		With Supervisor Engine 720-10GE	12.2(33)SXH
		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_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

- Supervisor Engine 32 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.

Fan Trays



Note

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

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
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

Power Supplies

- [CISCO7606 Power Supplies, page 101](#)
- [WS-C6504-E and CISCO7604 Power Supplies, page 102](#)
- [WS-C6503, WS-C6503-E, and CISCO7603 Power Supplies, page 102](#)
- [All Other Power Supplies, page 102](#)

[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 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 12.2(33)SXH2
	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	

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 or Supervisor Engine 720-10GE in WS-C6509-NEB or OSR7609. - 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, page 105](#)
- [9-Slot Chassis, page 106](#)
- [6-Slot Chassis, page 108](#)
- [4-Slot Chassis, page 109](#)
- [3-Slot Chassis, page 109](#)

13-Slot Chassis

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 720-10GE or Supervisor Engine 720 requires WS-C6K-13SLT-FAN2 • 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 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
CISCO7613	Cisco 7613 chassis: • 13 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720-10GE or Supervisor Engine 720 requires WS-C6K-13SLT-FAN2 • These modules are supported only in slots 9 through 13 and do not power up in other slots: – WS-X6700 series switching modules – WS-X6816-GBIC switching modules – WS-SVC-WISM-1-K9	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF

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	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	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 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF

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 720-10GE, 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 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
WS-C6509-NEB-A	Catalyst 6509-NEB chassis 9 vertical slots 64 chassis MAC addresses - Supports two FAN-MOD-09 modules. - Two FAN-MOD-09 modules required with WS-X6716-10GE or WS-X6708-10GE.	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
WS-C6509-NEB	Catalyst 6509-NEB chassis: 9 vertical slots 1024 chassis MAC addresses - 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
CISCO7609	Cisco 7609 chassis 9 vertical slots 64 chassis MAC addresses	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF

Product ID (append “=” for spare)	Product Description	Minimum Software Version
OSR-7609	Cisco 7609 chassis: 9 vertical slots 1024 chassis MAC addresses - 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

6-Slot Chassis

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6506-E	Catalyst 6506 chassis: 6 slots - Chassis MAC addresses: - Before April 2009—1024 chassis MAC addresses - Starting in April 2009—64 chassis MAC addresses Note Chassis with 64 MAC addresses automatically enable the Extended System ID feature, which is enabled with the spanning-tree extend system-id command. You cannot disable the extended-system ID in chassis that support 64 MAC addresses. The Extended System ID feature might already be enabled in your network, because it is required to support both extended-range VLANs and any chassis with 64 MAC addresses. Enabling the extended system ID feature for the first time updates the bridge IDs of all active STP instances, which might change the spanning tree topology. - Requires WS-C6506-E-FAN - Requires 2,500 W or higher power supply	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
WS-C6506	Catalyst 6506 chassis: 6 slots 1024 chassis MAC addresses - Requires WS-C6K-6SLOT-FAN2 WS-CAC-6000W limited to 4,000 W in WS-C6506	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF

Product ID (append “=” for spare)	Product Description	Minimum Software Version
CISCO7606	Cisco 7606 chassis: • 6 slots • 64 chassis MAC addresses • Requires FAN-MOD-6HS	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF

4-Slot Chassis

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6504-E	Catalyst 6504-E chassis: • 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(18)SXE
	With Supervisor Engine 32	12.2(18)SXF
CISCO7604	Cisco 7604 chassis: • 4 slots • 64 chassis MAC addresses	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	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 • Requires WS-C6503-E-FAN	
	With Supervisor Engine 720-10GE	12.2(33)SXH
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF

Product ID (append “=” for spare)	Product Description	Minimum Software Version
WS-C6503	Catalyst 6503 chassis: • 3 slots • 64 chassis MAC addresses • Requires FAN-MOD-3HS • Does not support WS-X6700 series switching modules and WS-X6816-GBIC switching modules.	
	With Supervisor Engine 720	12.2(14)SX
	With Supervisor Engine 32	12.2(18)SXF
Note Supervisor Engine 720-10GE is not supported in WS-C6503.		
CISCO7603	Cisco 7603 chassis: • 3 slots • 64 chassis MAC addresses • Use with Supervisor Engine 720-10GE or Supervisor Engine 720 requires FAN-MOD-3HS • Does not support WS-X6700 series switching modules and WS-X6816-GBIC switching modules.	
	With Supervisor Engine 720	12.2(14)SX
Note Supervisor Engine 720-10GE and Supervisor Engine 32 are not supported in CISCO7603.		

Unsupported Hardware



Note

- See the “[Supervisor Engine 32 \(CAT6000-SUP32/MSFC2A\)](#)” section on page 42 for information about hardware that is not supported with the Supervisor Engine 32.
- See the *Release Notes for Cisco IOS Release 12.2SXF and Rebuilds* publication for information about support in earlier releases:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html

Release 12.2(33)SXH and later releases do not support the following hardware:

- Supervisor Engine 1 (WS-X6K-S1A-MSFC2, WS-X6K-SUP1A-MSFC)
- Supervisor Engine 2 (WS-X6K-S2U-MSFC2, WS-X6K-S2-MSFC2)
- WS-F6K-DFC distributed forwarding card (DFC)
- Optical Services Modules (OSMs)
- These service modules:
 - WS-X6381-IDS Intrusion Detection System (IDS) Module (WS-SVC-IDSM2-K9 is supported)
 - WS-X6380-NAM Network Analysis Module (NAM; WS-SVC-NAM-2 and WS-SVC-NAM-1 are supported)
 - WS-SVC-AON-1-K9 Application-Oriented Networking (AON) 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
- Release 12.2(33)SXH and rebuilds do not support the 7600-SIP-600 SPA Interface Processor-600 and these SPAs:
 - SPA-10X1GE 10-port Gigabit Ethernet SPA, SFP Optics
 - SPA-5X1GE 5-port Gigabit Ethernet SPA, SFP Optics
 - SPA-1XTENGE-XFP 1-port 10-Gigabit Ethernet SPA, LANPHY XFP Optics
 - SPA-OC192POS-VSR 1-port OC-192c/STM-64 POS/RPR SPA, VSR-1
 - SPA-OC192POS-LR 1-port OC-192c/STM-64 POS/RPR SPA, SM-LR
 - SPA-OC192POS-XFP 1-port OC-192c/STM-64 POS/RPR SPA, XFP Optics
 - SPA-OC192POS-VSR 1-port OC-192c/STM-64 POS/RPR SPA, VSR-1
- WS-X6182-2PA FlexWAN Module
- These Ethernet Switching Modules:
 - WS-X6024-10FL-MT 24-port 10BASE-FL MT-RJ
 - WS-X6248A-TEL 48-port 10/100TX RJ-21
 - WS-X6248-RJ-45 48-port 10/100TX RJ-45
 - WS-X6248-TEL 48-port 10/100TX RJ-21
 - WS-X6324-100FX-SM 24-port 100FX Ethernet
 - WS-X6224-100FX-MT 24-port 100FX Ethernet Multimode MT-RJ
 - WS-X6316-GE-TX 16-port Gigabit Ethernet RJ-45
 - WS-X6416-GE-MT 16-Port Gigabit Ethernet MT-RJ
- WS-CAC-1000W power supply
- WS-CAC-1300W power supply
- WS-CDC-1300W power supply
- These fan trays:
 - FAN-MOD-3
 - FAN-MOD-6
 - WS-C6K-6SLOT-FAN
 - WS-C6509-NEB-FAN
 - WS-C6K-9SLOT-FAN
 - WS-C6K-13SLT-FAN

- 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>

- 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

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, page 113](#)
- [Feature Set Descriptions, page 113](#)

Feature Set Guidelines and Restrictions

These are the feature set guidelines and restrictions:

- The FlexWAN and Enhanced FlexWAN modules and SIPs and SPAs are supported only in images that contain “_wan” in the image name.
- 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
- 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/cgi-bin/Software/Crypto/crypto_main.pl
- Some 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

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.

Feature Name	IP Base	IP Services	Advanced IP Services	Enterprise Services	Advanced Enterprise Services
TCP Intercept					X
IPsec Network Security			X		X
Note • The SPA-IPSEC-2G supports IPsec Network Security in hardware. • Without a SPA-IPSEC-2G, the IPsec Network Security feature (configured with the crypto ipsec command) is supported in software only for administrative connections to Catalyst 6500 series switches.					
MPLS			X		X
IPsec VPNs			X		X
ISO CLNS				X	X

Feature Name	IP Base	IP Services	Advanced IP Services	Enterprise Services	Advanced Enterprise Services
Novell IPX				X	X
IPv6					
With releases earlier than Release 12.2(33)SXI:			X	X	X
With Release 12.2(33)SXI and later releases:	X	X	X	X	X
SLB			X	X	X
IS-IS			X	X	X
VSS					
With releases earlier than Release 12.2(33)SXII:		X	X	X	X
With Release 12.2(33)SXII and later releases:	X	X	X	X	X
BGP4		X	X	X	X
MBGP		X	X	X	X
VRF Lite		X	X	X	X
Bidirectional PIM		X	X	X	X
EIGRP		X	X	X	X
MSDP		X	X	X	X
OSPF		X	X	X	X
PBR		X	X	X	X
NetFlow	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	X	X	X	X	X
Note The SSH k9 images support SSH 3DES access in software on the route processor.					
PIMv1, PIMv2	X	X	X	X	X
RIPv1, RIPv2	X	X	X	X	X

New Features

- [New Features in Release 12.2\(33\)SXI3, page 115](#)
- [New Features in Release 12.2\(33\)SXI2a, page 116](#)
- [New Features in Release 12.2\(33\)SXI2, page 116](#)
- [New Features in Release 12.2\(33\)SXII, page 117](#)
- [New Features in Release 12.2\(33\)SXI, page 118](#)
- [New Features in Release 12.2\(33\)SXH7, page 127](#)
- [New Features in Release 12.2\(33\)SXH6, page 128](#)

- [New Features in Release 12.2\(33\)SXH5, page 128](#)
- [New Features in Release 12.2\(33\)SXH4, page 128](#)
- [New Features in Release 12.2\(33\)SXH3a, page 129](#)
- [New Features in Release 12.2\(33\)SXH3, page 129](#)
- [New Features in Release 12.2\(33\)SXH2a, page 130](#)
- [New Features in Release 12.2\(33\)SXH2, page 130](#)
- [New Features in Release 12.2\(33\)SXH1, page 131](#)
- [New Features in Release 12.2\(33\)SXH, page 132](#)
- [Software Features from Earlier Releases, page 145](#)

**Note**

- See the “[Supervisor Engine 32 \(CAT6000-SUP32/MSFC2A\)](#)” section on page 42 for the list of features not supported with Supervisor Engine 32.
- 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 those releases. When applicable, this section refers to those publications for platform-independent features supported in the Cisco IOS 12.2SX releases.

New Features in Release 12.2(33)SX13

These sections describe the new features in Release 12.2(33)SX13, 04 Nov 2009:

- [New Hardware Features in Release 12.2\(33\)SX13, page 115](#)
- [New Software Features in Release 12.2\(33\)SX13, page 115](#)

New Hardware Features in Release 12.2(33)SX13

None.

New Software Features in Release 12.2(33)SX13

- Deprecation of install mode and patching with Cisco IOS Software Modularity—See this publication:
http://www.cisco.com/en/US/docs/ios/swmod/configuration/guide/sw_mod_instl_cfg.html
- LACP Port-Channel Standalone Disable—See this publication:
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_o1.html#port-channel_standalone-disable

New Features in Release 12.2(33)SX12a

These sections describe the new features in Release 12.2(33)SX12a, 03 Sep 2009:

- [New Hardware Features in Release 12.2\(33\)SX12a, page 116](#)
- [New Software Features in Release 12.2\(33\)SX12a, page 116](#)

New Hardware Features in Release 12.2(33)SX12a

None.

New Software Features in Release 12.2(33)SX12a

None.

New Features in Release 12.2(33)SX12

These sections describe the new features in Release 12.2(33)SX12, 17 Jul 2009:

- [New Hardware Features in Release 12.2\(33\)SX12, page 116](#)
- [New Software Features in Release 12.2\(33\)SX12, page 116](#)

New Hardware Features in Release 12.2(33)SX12

- Content Switching Module (CSM)—See these websites:
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/tsd_products_support_model_home.html
<http://www.cisco.com/en/US/products/hw/modules/ps2706/ps780/index.html>
- Content Switching Module with SSL (CSM-S)—See these websites:
http://www.cisco.com/en/US/products/ps6077/tsd_products_support_model_home.html
<http://www.cisco.com/en/US/products/ps6077/index.html>
- OneX 10G X2 to SFP+ Converter (CVR-X2-SFP10G)
- 1-Port 10 Gigabit Ethernet SPA (SPA-1X10GE-L-V2)—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76intsw.html#SIP,_SSC,_and_SPA_Compatibility

New Software Features in Release 12.2(33)SX12

- 802.1ag - IEEE D8.1 standard Compliant CFM, Y.1731 multicast LBM / AIS / RDI / LCK, IP SLA for Ethernet—See this publication:
http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee.html
- Automated Notification and Detection of LTL/FPOE Problem—The Local Target Logic and Fabric Port Of Exit Static Random Access Memory in various constellation based cards are not protected via Empty Catch Clause. A software based parity table is now maintained and updated in firmware to detect and recover from Static Random Access Memory errors on LAN and Komodo+ cards.

- Filter-ID Based ACL Application—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Filter-ID_ACLS
- Local forwarding on Standby Supervisor Uplinks—See this publication:
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_f1.html#fabric_switching-mode_allow
- SSO - BFD—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bfd.html
- SSO - Etherchannel Traffic Convergence Improvement—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/nsfssso.html#Redundancy_Configuration_Guidelines_and_Restrictions
- 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
- VSS - MPLS/IPv6 Support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Software_Features

New Features in Release 12.2(33)SX11

These sections describe the new features in Release 12.2(33)SX11, 31 Mar 2009:

- [New Hardware Features in Release 12.2\(33\)SX11, page 117](#)
- [New Software Features in Release 12.2\(33\)SX11, page 117](#)

New Hardware Features in Release 12.2(33)SX11

None.

New Software Features in Release 12.2(33)SX11



Note

See the following site for information about supported MIBs:

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

- 6PE Multipath—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mptcl_bgp.html
- 802.1x with user distribution—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_Multiple_VLANs_and_VLAN_User_Distribution_with_VLAN_Assignment

- BGP Support for 4-byte ASN—See these publications:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_basic_net.html
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_overview.html
- CISCO-IP-IF-MIB Support for IP Helper addresses—See this publication:
http://www.cisco.com/en/US/docs/ios/interface/configuration/guide/ir_ipunnelmibs.html
- Modular IOS Usability - ION Installer Usability Enhancements—See this publication:
http://www.cisco.com/en/US/docs/ios/swmod/configuration/guide/12_2SX/sw_mod_12_2SX_book.html
- Trusted boundary with Cisco device verification—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/qos.html#Configuring_Trusted_Boundary_Device_Verification
- VSS Support on IP Base Image—See the “Feature Set Descriptions” section on page 113.

New Features in Release 12.2(33)SXI

These sections describe the new features in Release 12.2(33)SXI, 11 Nov 2008:

- [New Hardware Features in Release 12.2\(33\)SXI, page 118](#)
- [New Software Features in Release 12.2\(33\)SXI, page 119](#)



Note

- These commands, which are present in the Release 12.2(33)SXI CLI, will be tested and supported in a future release:
 - **add prepend** option to **install bind command**
 - **add reload** option to **install activate command**
 - **add pending** option to **show install running command**
 - **mls qos trust device cisco-phone** ([CSCsv53392](#))
- [NAC Layer 3 IP validation](#), called “NAC - Network Admission Control” in Feature Navigator, is supported only in Release 12.2(33)SXH and rebuilds. Release 12.2(33)SXI and later releases do not support NAC Layer 3 IP validation.
- With Release 12.2(33)SXI and later releases where [CSCso97991](#) is not resolved, you must configure an appropriate [burst size](#) when you configure QoS policing on WAN ports. Do not rely on the burst size calculated by QoS.
- Release 12.2(33)SXI and later releases support additional logical interfaces (see the “[Spanning Tree Troubleshooting](#)” section on page 23).

New Hardware Features in Release 12.2(33)SXI

- 10GBASE DWDM X2 Modules—See this publication:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6576/data_sheet_c78_489725.html
- 10GBASE-ZR X2 Module for SMF (X2-10GB-ZR)—See this publication:
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/ps6574/product_data_sheet0900aecd801f92aa_ps5251_Products_Data_Sheet.html

- 2-Port Gigabit Ethernet Shared Port Adapter (SPA-2X1GE-V2)
- ATM SPAs:
 - 1-Port OC-12c/STM-4c ATM SPA (SPA-1XOC12-ATM)
 - 1 port OC-48c/STM-16 ATM SPA (SPA-1XOC48-ATM)
 - 2-Port OC-3c/STM-1c ATM SPA (SPA-2XOC3-ATM, SPA-4XOC3-ATM)
 - 2-Port OC-48 POS/RPR SPA (2xOC48 POS/RPR SPA)
 - See these publications:
 - http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76ovwpos.html
 - http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/6500series/6500sov.html
- 2-GB CompactFlash cards sold by Cisco Systems, Inc., for use in Catalyst 6500 products and ME6500 series products.
- Services SPA Carrier-600 (WS-SSC-600) and VPN Services Port Adapter (WS-IPSEC-3)—See these publications:
 - http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/configuration/guide/ivm_sw_book.html
 - http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/hardware/ivmhw_book.html

New Software Features in Release 12.2(33)SX



Note

See the following site for information about supported MIBs:

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

- Asymmetric Carrier Delay—See this publication:
 - http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgsip.html#Configuring_Asymmetric_Carrier_Delay
- AToM over GRE - Phase 2—See this publication:
 - http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgeth.html#Configuring_AToM_over_GRE
- Backplane Traffic Monitor—See this publication:
 - http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/plat_mon.html
- Bandwidth-Based Call Admission Control (CAC) for IP Multicast—See this publication:
 - http://cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_admission_control.html
- BGP Route-Map Continue Support for Outbound Policy—See this publication:
 - http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_external_sp.html

- Callhome Request—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/callhome.html#Sending_a_Request_for_an_Analysis_and_Report
- CatOS Parity: Port VLAN Granularity for Show Commands—See these publications:
http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_02.html#show_ethernet_oam_status
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s4.html#show_interfaces_counters
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s4.html#show_interfaces_ethernet
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s4.html#show_interfaces_flowcontrol
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s4.html#show_interfaces_status
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s4.html#show_interfaces_trunk
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s5.html#show_l2protocol_tunnel
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_10.html#show_cdp
- CDP Enhancement - Host presence TLV—See these publications:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#802.1X_Host_Modes
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/voip.html#Cisco_IP_Phone_Data_Traffic
- CFM-2—See this publication:
http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm.html
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_metro_ethernet.html
- CNS—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html
- CNS - Configuration Agent—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html
- CNS - Event Agent—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html
- CNS - Image Agent—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html
- CNS - Interactive CLI—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html
- Command Scheduler (Kron)—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services.html

- Config Change Tracking Identifier— The Config Change Tracking Identifier feature assigns a version number to each saved version of the Cisco IOS running-config file and displays details about the versions. When the version number is updated a notification is generated. The Config Logger can also use this feature to determine if there have been any changes to the Cisco IOS running-config file. To enable the Config Change Tracking Identifier feature, enter the **show config id** command.
- Configuration Rollback Confirmed Change—See this publication:
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-rollback.html
- DHCP - DHCPv6 Relay Agent notification for Prefix Delegation—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html>
- DHCPv6 - Relay - Reload persistent Interface ID option—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html>
- DHCPv6 Ethernet Remote ID option—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html>
- Display Admin speed/duplex negotiation status—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/intrface.html#Displaying_the_Speed_and_Duplex_Mode_Configuration
- Dual PQ (Priority Queue)—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfsip.html#Configuring_Dual_Priority_Queueing_on_a_Cisco_7600_SIP-400
- eFSU (Enhanced Fast Software Upgrade)—See these publications:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/issu_efs.html
- Embedded Event Manager (EEM) 2.4—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_overview.html
- Embedded Syslog Manager (ESM)—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_esm_syslog.html
- Ethernet Local Management Interface (LMI) at Provider Edge (PE)—See these publications:
http://www.cisco.com/en/US/docs/ios/ceether/configuration/guide/ce_elmi-pe.html
http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htethlmi.html
- Ethernet OAM-phase2/ELMI-PE—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfgeth.html#Configuring_Ethernet_Operations,_Administration,_and_Maintenance
- FHRP - EOT integration with EEM—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_eot.html
- FHRP - GLBP Client Cache—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_glb.html
- FHRP - GLBP Support for IPv6—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-fhrp.html>
- FHRP - HSRP Group Shutdown—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html

- FHRP - HSRP Multiple Group Optimization—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html
- Flash MIB enhancements—The Flash MIB Enhancements feature allows sorting of flash files according to device, partition, and file indexes. Beginning with Cisco IOS Release 12.2(33)SXI, the Flash MIB Enhancements feature adds the user functionality to sort flash files based on file type. The feature also introduces the **snmp mib flash cache interval** command to set the frequency of the data collection process that enables sorting of data stored in ciscoFlashFileTable. The command also enables the cache for ciscoFlashFileTable to speed up access to data. For more information about setting the data collection interval, see the **snmp mib flash cache interval** command in the Cisco IOS Network Management Command Reference at the following URL:
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html
To locate and download the Cisco Flash MIB for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:
<http://tools.cisco.com/ITDIT/MIBS/servlet/index>
- HSRP for IPv6—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-fhrp.html>
- HSRP Gratuitous ARP—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html
- IEEE 802.1ak - MVRP and MRP—See this publication:
http://www.cisco.com/en/US/docs/ios/lanswitch/configuration/guide/lsw_cfg_mvrp.html
- IEEE 802.1X - Flexible Authentication—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp_ps6017_TSD_Products_Configuration_Guide_Chapter.html
- IEEE 802.1X - Multiple Authentication—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Multiauthentication_Mode
- IEEE 802.1X - Open Authentication—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Pre-Authentication_Open_Access
- IEEE 802.1X - User Port Description—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_Port_Descriptors
- IEEE 802.1X Agentless Audit Support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#NAC_Agentless_Audit_Support
- IEEE 802.1x Fallback support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Understanding_the_Port-based_Authentication_Process
- IEEE 802.1X Multi-Domain Authentication—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Multidomain_Authentication_Mode

- IEEE 802.1x with ACL Assignments—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#Using_802.1X_Authentication_with_ACL_Assignments_and_Redirect_URLs
- IEEE 802.3ah - Link Fault RFI Support—See this publication:
http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_oam.html
- Intrusion Detection Service Module (IDSM) support in VSS mode—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Service_Module_Support
- IP SLAs for Metro-Ethernet—See this publication:
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_metro_ethernet.html
- IP SLAs Random Scheduler—See this publication:
http://www.cisco.com/en/US/docs/ios/ipsla/configuration/guide/sla_multi_scheduler.html
- IPv6 Access Services: DHCPv6 Relay Agent—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-dhcp.html>
- IPv6 ACL Extensions for Mobile IPv6—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mobile.html>
- IPv6 Reformation—IPv6 features are supported in ipbase(k9) and ipservices(k9) images.
- IPv6 Routing - EIGRP Support—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-eigrp.html>
- IPv6 support for VSPA, VPN Services Port Adapter (WS-IPSEC-3)—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/configuration/guide/ivm_vpn3.html
- IPv6 VPN over MPLS (6VPE)—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ov_mpls_6vpe.html
- IPv6: Multicast Address Group Range Support—See this publication:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-multicast.html>
- L2VPN Pseudowire Redundancy—See this publication:
http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/wan_l2vpn_pw_red.html
- LowSpeed SPA support on SIP400—See these publications:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76ovwser.html#Release_History
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/6500series/6500sov.html
- MAC Move Counters—See this publication:
http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_m1.html#mac-address-table_notification_mac-move
- Mini Protocol Analyzer—See this publication:
<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mpa.html>

- MPLS EM - LSP Ping/Trace for LDP & RSVP IPv4 FECs—See this publication:
http://cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_ldp_te_lsp_vccv.html
- MPLS EM - MPLS Multipath (ECMP) LSP Tree Trace—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_em_multipath_tree.html
- MPLS VPN - VRF CLI for IPv4 & IPv6 VPNs—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_ipv4_ipv6.html
- MPLS VPN 6VPE support over IP tunnels—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ov_mpls_6vpe.html
- MPLS VPN VRF Selection using Policy Based Routing—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_vrf_select_rt.html
- MSTP PVST Simulation disabling and Peer Inconsistency Check—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/stp_enha.html#Configuring_PVST_Simulation
- Multicast Address Group Range Support—The Multicast Address Group Range Support feature enhances multicast access control by introducing the capability to define a global range of multicast groups and channels to be permitted or denied using the **ip multicast group-range** command.
- Multicast Enhancement - Egress Replication Performance Improvement for Vlan & PortChannel—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mcastv4.html#wpMulticast_Enhancement
- Multicast Replication Packet Drop Counter—See this publication:
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s5.html#show_platform
- Netconf access for Configuration over BEEP—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_netconf.html
- NETCONF over SSHv2—See this publication:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_netconf.html
- Netflow Accounting for Unicast and Multicast on GRE tunnel interface—See this publication:
http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/cfg_nf_gre_tun.html
- PBF (Policy-Based Forwarding)—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vacl.html#MAC_Policy-Based_Forwarding
- Per Interface Mroute State Limit—See this publication:
http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_admission_control.html
- Per IP Session QoS support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/qos.html#Session-Based_PFC_QoS
- Pre-encryption QOS for VSPA—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/vspa/configuration/guide/ivm_vpn3.html

- QoS Statistics Enhancement—See this publication:
http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_s4.html#show_mls_qos
- Radius Per-VRF Server Group—See this publication:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_per_vrf_aaa.html
- Rapid-PVST+ Dispute Mechanism—See this publication:
<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/spantree.html#Rapid-PVST>
- Reliable Delivery and Filtering for Syslog—See this publication:
http://cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_reliable_del_filter.html
- Role-Based Access Control CLI commands—See this publication:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_role_base_cli.html
- Show Command for Interface Trap Status—Beginning with Cisco IOS Release 12.2(33)SXI, the Show Command for Interface Trap Status feature adds the **show snmp mib ifmib traps** command to display the status of linkUp and linkDown traps. For more information about viewing linkUp and linkDown trap status, see the **show snmp mib ifmib traps** command in the Cisco IOS Network Management Command Reference at the following URL:
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_book.html
For more information about enabling SNMP notification types, see the Cisco IOS Network Management Configuration Guide at the following URL:
http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/12_4t/nm_12_4t_book.html
- Show Diagnostic Health—See this publication:
<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/diags.html>
- SNMP over IPv6—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mng_apps.html
- SNMPv3 - 3DES and AES Encryption Support—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mng_apps.html
- SSO - IPv4 Multicast HA Support for Group-to-RP Mapping—See this publication:
http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_ha_grp_to_rp_mappings.html
- SSO - VRRP—See these publications:
http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-stfl_swovr.html
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_vrrp.html
- Standalone MAB support—See this publication:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/standalone_mab.html
- Static Virtual Tunnel & GRE/TP interface enhancements—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfvpna.html#Configuring_an_IPSec_Virtual_Tunnel_Interface
- STP Bridge Assurance—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/stp_enha.html#Understanding_Bridge_Assurance

- Sub Millisecond Policer Burst Size Support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/qos.html#wppolicer_granularity
- Syslog over IPV6—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mng_apps.html
- System Logging - EAL4 Certification Enhancements:

**Note**

Official EAL4 certification is not claimed by Cisco Systems, Inc. This feature is part of current and planned enhancements which may qualify Cisco IOS Software for future certification.

This feature includes the following enhancements:

- The system logging process will now generate ‘audit start’ and ‘audit stop’ messages.
- The system logging process will now generate messages that include the date and time of an event, the type of event, the subject identity, and the outcome (success or failure) of an event.
- Changes to logging parameters will be logged.
- Further enhancements to minimize lost audit records.
- TACACS+ Per VRF—See this publication:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_vrf_tacas_svrs.html
- VSS - 512 Etherchannels Support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Configuring_Multichassis_EtherChannels
- VSS - ACE 10/20 Support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Service_Module_Support
- VSS - Dual-active detection using L2 Fast Hello detection—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Dual-Active_Detection_Using_Dual-Active_Fast_Hello_Packets
- VSS - Firewall Service Module (FWSM) support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Service_Module_Support
- VSS - PACL support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Software_Features
- VSS - Wireless (WiSM) Support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vss.html#Service_Module_Support
- VTP v3—See this publication:
<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vtp.html>

- Web Authentication with Critical Auth support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/webauth.html#AAA_Fail_Policy
- Webauth Enhancements—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/webauth.html#Customization_of_the_Authentication_Proxy_Web_Pages

New Features in Release 12.2(33)SXH7

These sections describe the new features in Release 12.2(33)SXH7, 15 Mar 2010:

- [New Hardware Features in Release 12.2\(33\)SXH7, page 127](#)
- [New Software Features in Release 12.2\(33\)SXH7, page 127](#)

New Hardware Features in Release 12.2(33)SXH7

None.

New Software Features in Release 12.2(33)SXH7

- VRF-lite aware NAT for non-overlapping IP addresses:



Note

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

The following is an example of the supported configuration:

```
ip nat outside source static real_ip_address nat_ip_address

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

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



Note

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

New Features in Release 12.2(33)SXH6

These sections describe the new features in Release 12.2(33)SXH6, 21 Oct 2009:

- [New Hardware Features in Release 12.2\(33\)SXH6, page 128](#)
- [New Software Features in Release 12.2\(33\)SXH6, page 128](#)

New Hardware Features in Release 12.2(33)SXH6

None.

New Software Features in Release 12.2(33)SXH6

- 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(33)SXH5

These sections describe the new features in Release 12.2(33)SXH5, 20 Apr 2009:

- [New Hardware Features in Release 12.2\(33\)SXH5, page 128](#)
- [New Software Features in Release 12.2\(33\)SXH5, page 128](#)

New Hardware Features in Release 12.2(33)SXH5

None.

New Software Features in Release 12.2(33)SXH5

None.

New Features in Release 12.2(33)SXH4

These sections describe the new features in Release 12.2(33)SXH4, 11 Nov 2008:

- [New Hardware Features in Release 12.2\(33\)SXH4, page 128](#)
- [New Software Features in Release 12.2\(33\)SXH4, page 129](#)

New Hardware Features in Release 12.2(33)SXH4

None.

New Software Features in Release 12.2(33)SXH4

**Note**

See the following site for information about supported MIBs:

<http://www.cisco.com/public/sw-center/netmgt/cmtk/mibs.shtml>

- Radius Per-VRF Server Group—See this publication:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_per_vrf_aaa.html
- TACACS+ Per VRF—See this publication:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_vrf_tacas_svrs.html

New Features in Release 12.2(33)SXH3a

These sections describe the new features in Release 12.2(33)SXH3, 29 Sep 2008:

- [New Hardware Features in Release 12.2\(33\)SXH3a, page 129](#)
- [New Software Features in Release 12.2\(33\)SXH3a, page 129](#)

New Hardware Features in Release 12.2(33)SXH3a

None.

New Software Features in Release 12.2(33)SXH3a

None.

New Features in Release 12.2(33)SXH3

These sections describe the new features in Release 12.2(33)SXH3, 29 Jul 2008:

- [New Hardware Features in Release 12.2\(33\)SXH3, page 129](#)
- [New Software Features in Release 12.2\(33\)SXH3, page 129](#)

New Hardware Features in Release 12.2(33)SXH3

None.

New Software Features in Release 12.2(33)SXH3

**Note**

See the following site for information about supported MIBs:

<http://www.cisco.com/public/sw-center/netmgt/cmtk/mibs.shtml>

SSH Keyboard Interactive Authentication—See this publication:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_secure_shell_v2.html

New Features in Release 12.2(33)SXH2a

These sections describe the new features in Release 12.2(33)SXH2a, 28 Apr 2008:

- [New Hardware Features in Release 12.2\(33\)SXH2a, page 130](#)
- [New Software Features in Release 12.2\(33\)SXH2a, page 130](#)

New Hardware Features in Release 12.2(33)SXH2a

None.

New Software Features in Release 12.2(33)SXH2a

None.



Note

Resolution of [CSCso05127](#) changed the [SPAN syntax and defaults](#).

New Features in Release 12.2(33)SXH2

These sections describe the new features in Release 12.2(33)SXH2, 31 Mar 2008:

- [New Hardware Features in Release 12.2\(33\)SXH2, page 130](#)
- [New Software Features in Release 12.2\(33\)SXH2, page 130](#)

New Hardware Features in Release 12.2(33)SXH2

- 16-port 10-Gigabit Ethernet X2 Switching Module (WS-X6716-10GE)
- 6,000 W DC power supply (PWR-6000-DC)

New Software Features in Release 12.2(33)SXH2



Note

See the following site for information about supported MIBs:

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

- Cisco Enhanced PoE (ePoE) Support—Refer to this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/voip.html#wpCisco_Enhanced_PoE_Support

New Features in Release 12.2(33)SXH1

These sections describe the new features in Release 12.2(33)SXH1, 18 Jan 2008:

- [New Hardware Features in Release 12.2\(33\)SXH1, page 131](#)
- [New Software Features in Release 12.2\(33\)SXH1, page 131](#)

New Hardware Features in Release 12.2(33)SXH1

- Anomaly Guard Module (WS-SVC-AGM-1-K9)—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/anomaly_guard/v4.0/release/note/JaffaAGd.html
- Traffic Anomaly Detector Module (WS-SVC-ADM-1-K9)—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/anomaly_detector/v4.0/release/note/JaffaTAD.html

New Software Features in Release 12.2(33)SXH1



Note

See the following site for information about supported MIBs:

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

- Multi-VRF Selection Using Policy Based Routing (PBR)—See this publication:
http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_mltvrf_slct_pbr.html
- VSS (Virtual Switching System):
 - Supported only with CAT6000-VS-S720-10G/MSFC3 and the hardware listed in the “[Hardware Requirements](#)” section.
 - See these publications:
Cisco IOS Software Configuration Guide, Release 12.2(33)SXH and Later Releases, [Chapter 4](#), “[Configuring Virtual Switching Systems](#).”
The *Cisco IOS Virtual Switch Command Reference* at:
http://www.cisco.com/en/US/docs/ios/vswitch/command/reference/vs_book.html



Note

In releases earlier than Release 12.2(33) SXH2, the VSS feature and the lawful intercept feature cannot be configured together. (CSCsl77715)

- VSS - Fast Link Status Notification—See the “[Virtual Switching System Redundancy](#)” section.
- VSS - GOLD in Virtual Switching System—See the “[Diagnostics](#)” section.

New Features in Release 12.2(33)SXH

These sections describe the new features in Release 12.2(33)SXH, 20 Aug 2007:

- [New Hardware Features in Release 12.2\(33\)SXH, page 132](#)
- [New Software Features in Release 12.2\(33\)SXH, page 132](#)



Note

Release 12.2(33)SXH provides initial support with Cisco IOS software modularity images for these service modules:

- Services SPA Carrier (SSC; 7600-SSC-400) and IPsec SPA (SPA-IPSEC-2G)
- Application Control Engine (ACE) module (ACE10-6500-K9, ACE20-6500-K9)
- Communication Media Module (WS-SVC-CMM)
- BGP Reduction in Transient Memory Usage—Cisco IOS Release 12.2(33)SXH has implemented a reduction in transient memory usage by BGP when BGP updates are built.
- Process MIB Enhancements for Software Modularity—The CISCO-PROCESS-MIB has been enhanced to support Portable Operating System Interface (POSIX) operating systems such as Cisco Software Modularity. Cisco Software Modularity images have been updated to implement the enhanced CISCO-PROCESS-MIB. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

New Hardware Features in Release 12.2(33)SXH

- Catalyst 6509-V-E chassis ([WS-C6509-V-E](#))
- Supervisor Engine 720-10GE (CAT6000-VS-S720-10G/MSFC3)
- Cisco ME 6500 Series Ethernet switches (ME6524)
- 8-port 10/100 Ethernet SPA TX (SPA-8X1FE-TX-V2)
- 4-port 10/100 Ethernet SPA TX (SPA-4X1FE-TX-V2)
- 1-port Channelized STM1/OC3 to DS0 SPA (SPA-1xCHSTM1/OC3)
- Cisco 1000BASE-T NEBS 3 ESD SFP (SFP-GE-T)

New Software Features in Release 12.2(33)SXH



Note

See the following site for information about supported MIBs:

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

- Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: Packed Cell Relay—See this publication:

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

- Any Transport over MPLS (AToM): ATM Cell Relay over MPLS: VP Mode—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html
- Any Transport over MPLS (AToM): Ethernet over MPLS (EoMPLS)—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html



Note With an Cisco ME 6500 Series Ethernet Switch (ME6524), be aware of [CSCsu50427](#).

- Any Transport over MPLS (AToM): Ethernet over MPLS: Port Mode (EoMPLS)—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html
- Any Transport over MPLS (AToM): Graceful Restart—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html
- ATM OAM Emulation—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html
- ATM Port Mode Packed Cell Relay over MPLS—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_any_transport.html
- AutoQoS—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using AutoQoS](#)” chapter.
- AutoSecure—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using AutoSecure](#)” chapter.
- AutoRP Enhancement—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/dmfallsx.html
- BCP Support on MLPPP—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/76cfsip.html#Configuring_PPP_Bridging_Control_Protocol_Support
- BGP Dynamic Neighbors—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sx_bdyn.html
- BGP Multicast Inter-AS (IAS) VPN—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxbmias.html
- BGP Support for BFD—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_adv_features.html
- BGP Support for Dual AS Configuration for Network AS Migrations—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_neighbor.html
- BGP Support for Fast Peering Session Deactivation—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_neighbor.html
- BGP Support for IP Prefix Import from Global Table into a VRF Table—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_bgivt.html
- BGP Support for Named Extended Community Lists—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_external_sp.html

- BGP Support for Next-Hop Address Tracking—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_adv_features.html
- BGP Support for Sequenced Entries in Extended Community Lists—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_external_sp.html
- BGP Support for TCP Path MTU Discovery per Session—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_neighbor.html
- Bidirectional Forwarding Detection (BFD) Standard Implementation—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bfd.html
- Call Admission Control for IKE—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gtcallik.html
- Call Home—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring Call Home” chapter.
- Certificate - ISAKMP Profile Mapping—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gt_isakp.html
- Certificate - Storage Location Specification—See this publication:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_store_pki_cred.html
- Cisco IOS Login Enhancements—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html
- Cisco IOS Scripting w/ Tcl—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_tcl.html
- CLI extension to allow vlan-range for enabling or disabling mac-address learning—See the **mac-address-table learning** command in this publication:
http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_m1.html#mac-address-table_learning
- Config Logger Persistency—See this publication:
<http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/config-logger-6149.html>
- Configurable flow-creation control of acl denied flows—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring Exclude ACL-deny” section in the “Configuring NetFlow” chapter.
- Configuration Change Notification and Logging—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtconlog.html
- Configuration Replace and Configuration Rollback—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtrollbk.html
- Configuration Versioning—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtrollbk.html
- Consolidation of ACL Counter Values in Distributed Environment—See the **show tcam interface** command in this publication:
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s6.html#show_tcam_interface
- Contextual Configuration Diff Utility—See this publication:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_diff.html

- Digital Optical Monitoring (DOM) Phase 2—See the **show interfaces transceiver** command in this publication:

http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s4.html#show_interfaces_transceiver



Note See this publication for additional information about DOM:

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

- Distributed forwarding engines (3C/3CXL) for 67xx line cards—See these sections:
 - [Policy Feature Card Guidelines and Restrictions](#), page 44
 - [Policy Feature Card 3CXL](#), page 46
 - [Policy Feature Card 3C](#), page 46.
- Easy VPN Client RSA - Signature Support—See this publication:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtevcrsa.html
- Easy VPN Phase 5.0—See this publication:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftezvpnr.html
- EasyVPN Phase 6—See this publication:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftezvpnr.html
- EIGRP Support for Route Map Filtering—See this publication:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/gteigrpr.html
- Embedded Event Manager (EEM) 2.3—See this publication:

http://www.cisco.com/en/US/docs/ios/12_4t/netmgmt/configuration/guide/t_eemo.html
- Enhanced hot-standby fabric switchover time—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the enhanced hot-standby fabric switchover time information in the “[Redundancy Configuration Guidelines and Restrictions](#)” section of the “[Configuring NSF with SSO Supervisor Engine Redundancy](#)” chapter.
- Enhanced Tracking Support—See this publication:

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_eot.html
- Enhancing IPv6 Multicast shared-tree performance—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “IPv6 PIM-Sparse Mode (PIM-SM) (S,G) and (*,G) forwarding” item in the “[IPv6 Multicast Guidelines and Restrictions](#)” section in the “[Configuring IPv6 Multicast PFC3 and DFC3 Layer 3 Switching](#)” chapter.
- Ethernet Connectivity Fault Management—See this publication:

http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxh_cfm.html
- Ethernet Operations, Administration, and Maintenance (OAM)—See this publication:

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_oam.html
- Exclusive Configuration Change Access—See this publication:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_exclu.html

- Exclusive Configuration Change Access and Access Session Locking—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_exclu.html
- Extended ACL support for IGMP to support SSM in IPv4—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/hwexmvpn.html
- FHRP - Enhanced Object Tracking of IP SLAs—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxeotsla.html

**Note**

FHRP - Enhanced Object Tracking of IP SLAs is not stateful switchover (SSO)-aware and cannot be used with Hot Standby Routing Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP) in SSO mode.
(CSCtd31237)

- FHRP - Object Tracking List—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_eot.html
- Front Side VRF—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- GLBP MD5 Authentication—See this publication:
http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-stfl_swovr.html
- GRE Tunnel IP Source and Destination VRF Membership—See the “GRE Tunnel IP Source and Destination VRF Membership” sections in this publication:
http://www.cisco.com/en/US/docs/ios/12_4/interface/configuration/guide/inb_tun.html
- Hardware Acceleration for Multicast VPN Extranet Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/hwexmvpn.html
- HQoS Support for Ethernet Over MPLS (EoMPLS) VC on SIP-400—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- HSRP MD5 Authentication—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html
- H-VPLS with MPLS Edge on SIP-400—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- IEEE 802.1ab MED—See this publication:
http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_lldp-med.html
- IEEE 802.1ab, Link Layer Discovery Protocol—See this publication:
http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_lldp-med.html
- IEEE 802.1Q Tagging on a Per-Port Basis—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring the Switch to Tag Native VLAN Traffic Globally” section in the “Configuring IEEE 802.1Q Tunneling” chapter.

- IEEE 802.1x - Auth Fail Open—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “critical ports” information in the “[Using 802.1X Authentication with Inaccessible Authentication Bypass](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x - Voice VLAN—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using 802.1X Authentication with Voice VLAN Ports](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x - Wake on LAN Support—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using 802.1X Authentication with Wake-on-LAN](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x Authenticator—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the information about the role of the switch in the “[Device Roles](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x Guest VLAN—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using 802.1X Authentication with Guest VLAN](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x Private Guest VLAN—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the private VLAN port information in the “[Using 802.1X Authentication with Inaccessible Authentication Bypass](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x Private VLAN Assignment—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring a Guest VLAN](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x RADIUS Accounting—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[802.1X Accounting](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x Radius-Supplied Session Timeout—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Enabling Periodic Reauthentication](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x with DHCP—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using 802.1X Authentication with DHCP Snooping](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IEEE 802.1x with Port Security—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using 802.1X Authentication with Port Security](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- IGMP Filtering—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring IPv4 IGMP Filtering and Router Guard](#)” chapter.
- Ingress / Egress CoS classification with ingress policing per VLAN or EoMPLS VC (L2 & L3 QoS)—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/ipsasw.html
- Inline power IEEE power classification override—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Inline Power Management](#)” section in the “[Configuring Cisco IP Phone Support](#)” chapter.
- Interface Based NDE—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Per-interface NDE](#)” section in the “[Configuring NetFlow](#)” chapter.

- IP 16-way Equal-Cost Multipath—See the **maximum-paths** command in this publication:
http://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_pi1.html#maximum-paths
- IP SLAs - DHCP Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - Distribution of Statistics—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - DNS Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - FTP Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - HTTP Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - ICMP Echo Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - ICMP Path Echo Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - LSP Health Monitor—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxh_hmon.html
IP SLAs - LSP Health Monitor—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxh_hmon.html
- IP SLAs - MPLS VPN Awareness—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - Multi Operation Scheduler—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - One Way Measurement—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - Path Jitter Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - Reaction Threshold—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - Scheduler—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - TCP Connect Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - UDP Based VoIP Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - UDP Echo Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html

- IP SLAs - UDP Jitter Operation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IP SLAs - VoIP Threshold Traps—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsla_c.html
- IPsec Dead Peer Detection (DPD) Periodic Message Option—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtdpmpo.html
- IPSEC Preferred Peer—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_ipspp.html
- IPsec VTI - Virtual Tunnel Interface—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtIPScrm.html
- IPSG (IP Source Guard)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring IP Source Guard” chapter.
- IPv6 Default Router Preferences—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes.html
- IPv6 Multicast: Address Family Support for Multiprotocol BGP—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html
- IPv6 Multicast: Explicit Tracking of Receivers—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_2sx/ipv6_12_2sx_book.html
- IPv6 Multicast: MLD Access Group—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_2sx/ipv6_12_2sx_book.html
- IPv6 Multicast: PIM Accept Register—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_2sx/ipv6_12_2sx_book.html
- IPv6 Multicast: PIM Embedded RP Support—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_2sx/ipv6_12_2sx_book.html
- IPv6 Multicast: Routable Address Hello Option—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_2sx/ipv6_12_2sx_book.html
- IPv6 Multicast: RPF Flooding of Bootstrap Router (BSR) Packets—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_2sx/ipv6_12_2sx_book.html
- IPv6 Multicast: Static Multicast Routing (mroute) for IPv6—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_2sx/ipv6_12_2sx_book.html
- IPv6: Anycast Address—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-stat_routes.html
- L2VPN Interworking—See this publication:
http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_12vpn_intrntwkg.html
- L2VPN Interworking - Ethernet to VLAN Interworking—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsinterw.html
- L2VPN Interworking: Ethernet VLAN to ATM AAL5—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsinterw.html

- L2VPN Interworking: Ethernet VLAN to Frame Relay—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsinterw.html
- L2VPN Interworking: Ethernet VLAN to PPP—See this publication:
http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_l2vpn_intrntwkg.html
- L2VPN Interworking: Frame Relay to ATM AAL5—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsinterw.html
- L2VPN Interworking: Frame Relay to PPP—See this publication:
http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_l2vpn_intrntwkg.html
- LACP 1-1 redundancy with fast switchover—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Understanding LACP 1:1 Redundancy](#)” section in the “[Configuring EtherChannels](#)” chapter.
- Lawful Intercept (LI)—See this publication:
<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/lawful/intercept/book.html>



Note In releases earlier than Release 12.2(33) SXH2, the VSS feature and the lawful intercept feature cannot be configured together. (CSCsl77715)

- Layer 2 Local Switching - ATM to Ethernet—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslocal.html
- Layer 2 Local switching - ATM-FR—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslocal.html
- MAC Address Notification—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring MAC Address Table Notification](#)” section in the “[Configuring LAN Ports for Layer 2 Switching](#)” chapter.
- MAC Authentication Bypass—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using 802.1X Authentication with MAC Authentication Bypass](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- Memory Pool - SNMP Notification Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtmemnot.html
- MPLS - VRF Aware Static Labels—See this publication:
http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_vrf_aware_static.html
- MPLS LDP - Graceful Restart—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsgr29s.html
- MPLS LDP - Session Protection—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fssespro.html
- MPLS over RBE—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- MPLS Static Labels—See this publication:
http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_static_labels.html

- MPLS TE: SSO/NSF aware TE MIB Traps—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fshaov.html
- MPLS Traffic Engineering - AutoTunnel Mesh Groups—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gsamg2.html
- MPLS Traffic Engineering - FRR Scalability Enhancements- do not market—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsatom28.html
- MPLS Traffic Engineering (TE) - AutoTunnel Primary and Backup—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gsautotn.html
- MPLS Traffic Engineering (TE) - Class-based Tunnel Selection—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gscbts.html
- MPLS Traffic Engineering (TE) - Fast Reroute (FRR) Link and Node Protection—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslnph30.html
- MPLS Traffic Engineering (TE) - LSP Attributes—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslspatt.html
- MPLS Traffic Engineering (TE) - RSVP Hello State Timer—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gsrsvpht.html
- MPLS Traffic Engineering (TE): Verbatim Path Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsvbmlsp.html
- MPLS Traffic Engineering: Shared Risk Link Groups (SRLG)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs29srlg.html
- MPLS Traffic Engineering--Inter-AS TE—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gsintast.html
- MPLS VPN - eBGP Multipath support for CSC and InterAS MPLS VPNs—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sbmulti.html
- MPLS VPN - Explicit Null Label Support with BGP IPv4 Label Session—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gsxnlbsp.html
- MPLS VPN - Loadbalancing support for Inter-AS and CSC VPNs—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_load_share_vpn.html
- MPLS VPN - Multi-Path support for Inter-AS VPNs—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsiaseb.html
- MPLS VPN - Route Target Rewrite—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsrtrw4.html
- MPLS VPN - Show Running VRF—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/sb_svr.html
- MSDP compliance with IETF RFC 3618—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxmsdpcp.html
- MSDP MD5 password authentication—See this publication:

http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/smsdpmd5.html

- Multicast Vlan Registration (MVR)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Understanding MVR](#)” section in the “[Configuring IGMP Snooping and MVR for IPv4 Multicast Traffic](#)” chapter.
- Multicast VPN Extranet Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sb/feature/guide/extvpnsb.html
- Multicast VPN Inter-AS Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/iasmcvpn.html
- Multicast VPN MIB—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/mcvpnmib.html
- Multilink Frame Relay (FRF.16.1) - Variable Bandwidth Class—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_mfr.html
- MUX UNI support—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/pfc3mpls.html#Configuring_MUX-UNI_Support_on_LAN_Cards
- Multi-VC to VLAN Scalability—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- NAC - L2 IEEE 802.1x—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using Network Admission Control Layer 2 IEEE 802.1X Validation](#)” section in the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.
- NAC - Network Admission Control—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Network Admission Control](#)” chapter.
- Netflow for IPv6 Unicast traffic—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html
- NetFlow MIB and Top Talkers—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxnfft.html
- NetFlow Multicast Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxonfmc.html
- NetFlow Subinterface Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxonfsi.html
- NSF - OSPF (RFC 3623 OSPF Graceful Restart)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gr_ospf.html
- NSF / SSO - MPLS LDP and LDP Graceful Restart—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fslpgr.html
- NSF/SSO - MPLS TE and RSVP Graceful Restart—See this publication:
http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_te_rsvp_grace.html
- NSF/SSO - MPLS VPN—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsvpngr.html

- OER Border Router Only Functionality—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sx_oerbr.html
- Onboard Failure Logging—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxhobfl.html
- Online Diagnostics for SIP-400—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/ipspasw.html
- OSPF Area Transit Capability—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfatc.html
- PBR Support for Multiple Tracking Options—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtpbtrtk.html
- Per port VTP enable/disable—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring VTP Mode on a Per-Port Basis” section in the “Configuring VTP” chapter.
- Periodic MIB Data Collection and Transfer Mechanism—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/gdatacol.html
- Persistent Self-Signed Certificates—See this publication:
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cert_enroll_pki.html
- Per-VRF Assignment of BGP Router-ID—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/bgp_router_id.html
- PIM Triggered Joins—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxhpimtj.html
- Policy Based Access Control Lists (PBACLs)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Policy-Based ACLs” section in the “Understanding Cisco IOS ACL Support” chapter.
- Port-Based Access Control Lists (PACLs)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring Port ACLs and VLAN ACLs” chapter.
- Private Hosts—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring Private Hosts” chapter.
- QoS Support on Bridging Features—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/ipspasw.html
- Reverse Route Injection (RRI)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_rrie.html
- RFC 1490 Spanning-Tree Interoperability Enhancements—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html
- Router Guard—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Understanding Router Guard” section in the “Configuring IPv4 IGMP Filtering and Router Guard” chapter.

- RSVP Message Authentication—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsrsvpnk.html
- Scalable EoMPLS (SIP-Based)—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- SmartPorts—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Smart Port Macros](#)” chapter.
- SPAN Destination Port Support On Etherchannels—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Local SPAN, RSPAN, and ERSPAN Destinations](#)” section in the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter.
- SPAN Egress Session Increase—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Local SPAN, RSPAN, and ERSPAN Session Limits](#)” section in the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter.
- SSO - GLBP—See this publication:
http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-stfl_swovr.html
- SSO - HSRP—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_hsrp.html
- SSO - NAC—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[NAC and Switchover](#)” section in the “[Configuring Network Admission Control](#)” chapter.
- Support for MPLS-VPN Software Modularity—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/sxmplssm.html
- Support of IPv6 Software Modularity—Cisco IOS Software Modularity images in Release 12.2(33)SXH and later releases support IPv6.
- Suppress BGP Advertisement for Inactive Routes—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_basic_net.html
- Switch Port Analyzer (SPAN) - CPU Source—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Source CPUs](#)” section in the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter.
- Switch Port Analyzer (SPAN) - Distributed Egress SPAN—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Monitored Traffic Direction](#)” section in the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter.
- Switch Port Analyzer (SPAN) - Input Packets with Don't Learn Option—In the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter of the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see these sections:
 - [Local SPAN, RSPAN, and ERSPAN Destinations](#)
 - Information about the **ingress** keyword in these sections:
 - [Configuring Local SPAN](#)
 - [Configuring RSPAN](#)
 - [Configuring ERSPAN](#)
- System Event Archive—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring the System Event Archive](#)” chapter.

- TCP MSS Adjust—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_tcp.html
- Two-Rate Policer—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ft2RTplc.html
- Universal Boot Loader—See the “Universal Boot Loader Image” section on page 4.
- Unknown Unicast Flood Rate-Limiting (UUFRL)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring Unknown Unicast Flood Control” chapter.
- Virtual Private LAN Services (VPLS)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/12_2sxh/feature/guide/vplsstub.html
- VLAN Locking—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “VLAN Locking” section in the “Configuring VLANs” chapter.
- VPLS Multiple VCs per Spoke—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SR_OSM_config/mpls.html
- VRF Aware Multicast Error Messages—The VRF Aware Multicast Error Messages feature improves the troubleshooting of MPLS VPN environments by allowing service providers to track the multicast error messages that are associated with a particular MVPN customer.
- VRF Aware System Message Logging (Syslog)—See this publication:
http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vrf_aware_loggng.html
- WCCP Increased Services—See this publication:
http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_wccp.html
- Web Authentication Proxy—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring Web-Based Authentication” chapter.

Software Features from Earlier Releases

- 4000 ATM VCs per port adapter on the following FlexWAN 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

- 4096 Layer 2 VLANs—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “VLAN Ranges” section in the “Configuring VLANs” chapter.



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

- Any Transport over MPLS (AToM) Features:
 - 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)
 - HDLC over MPLS (HDLC oMPLS)
 - PPP over MPLS (PPPoMPLS)

See this publication:

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

- ATM Cell Loss Priority (CLP) Setting on FlexWAN module ATM interfaces—See this publication: http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html
- ATM OAM ping—See this publication: http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12satmpng.html
- ATM VC access trunk emulation—See this publication: http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- ATM Virtual Circuit (VC) Bundling—See these publications: http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfipaov.html
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsmu26s.html
- Automatic Protection Switching (APS) 1+1—See this publication: http://www.cisco.com/warp/public/127/aps_support_16140.pdf
- 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
- 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
- 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_bgdpdg.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
- BGP multipath load sharing for both eBGP and iBGP in an MPLS-VPN—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/fsxeibmp.html

**Note**

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

For nonMPLS environments, see the Interior Border Gateway Protocol (iBGP) Multipath Load Sharing feature.

- BGP Policy Accounting—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgppa.html
- BGP Restart Session After Max-Prefix Limit—See this publication:
http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_neighbor.html#BGP_Neighbor_Session_Restart_After_the_Max-Prefix_Limit_Is_Reached
- 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 support for TTL security check—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_btsh.html
- Bidirectional Forwarding Detection (BFD) standard implementation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

**Note**

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

Also see “Integrated IS-IS support for BFD over IPv4” and “OSPF support for BFD over IPv4.”

- Bidirectional Protocol Independent Multicast (PIM) in hardware—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Understanding IPv4 Bidirectional PIM](#)” section in the “[Configuring IPv4 Multicast Layer 3 Switching](#)” chapter.
- Boot Protocol (BOOTP) relay—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf012.html
- Bridge Control Protocol (BCP)—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

- Bridging using RFC1483 Routed Encapsulation (BRE)—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/flexwan-config-guide.html
- Certificate Autoenrollment (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftautoen.html
- Certificate Security Attribute-Based Access Control (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftcrtacl.html
- Cisco IOS IP Event Dampening—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftipevdp.html
- IPv6 Switching: Provider Edge Router over MPLS (6PE) (not supported in PFC3A mode)—See this publication:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-over_mpls.html
- Cisco IOS Secure Copy (SCP)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ftscp.html
- Cisco IOS server load balancing:
 - GGSN-SLB Messaging
 - Home Agent Loadbalancing

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 SLB: interface-aware—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.html
- Cisco IOS SLB: stateful failover within single chassis—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.html
- Cisco IP Phone Support—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Cisco IP Phone Support](#)” chapter.
- Cisco Nonstop Forwarding (NSF) with stateful switchover (SSO) supervisor engine redundancy—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring NSF with SSO Supervisor Engine Redundancy](#)” chapter.



Note

-
- 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.

- Clear hardware interface counters—See this publication:
http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- CNS Interactive CLI—Network management applications can use the Cisco Networking Services (CNS) agents to manage network routers. The CNS agent provides the capability to send commands to a router from a programmable source. The CNS Interactive CLI feature introduces a new XML interface that allows you to send interactive commands to a router, such as commands that generate prompts for user input. A benefit of this feature is that interactive commands can be 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/mcl/122sxmcl/12_2sx_mcl_book.html
- Control Plane DSCP Support for RSVP—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/dscprsvp.html
- Crypto Conditional Debug Support (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_dbcry.html
- 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-X6708-10GE
 - 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).

- In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring a Custom IEEE 802.1Q EtherType Field Value](#)” section in the “[Configuring LAN Ports for Layer 2 Switching](#)” chapter.
- Data-link switching plus (DLSw+)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcfdlsw_external_docbase_0900e4b180753b82_4container_external_docbase_0900e4b180771fb6.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 Option 82 on Untrusted Port—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Packet Validation](#)” section in the “[Configuring DHCP Snooping](#)” chapter.
- DHCP Snooping—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring DHCP Snooping](#)” chapter.
- Digital Optical Monitoring (DOM)—See the **show interfaces transceiver** command in this publication:
http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

**Note**

See this publication for additional information about DOM:

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

- Directed broadcasts with the **mls ip directed-broadcast** command supported in hardware—See this publication:
http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- Distinguished Name-Based Crypto Maps (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ftdnacl.html
- Distributed LFI (dLFI) and distributed QoS (dQoS) over Leased Lines on FlexWAN module interfaces—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftdlfi2.html
- Distributed MLPPP (dMLPPP) on FlexWAN module interfaces—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html

**Note**

cRTP is not supported on dMLPPP bundled links.

- Distributed Multilink Frame Relay (FRF.16)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/dmfr.html
- Distributed network-based application recognition (dNBAR) on FlexWAN module interfaces—See this publication:
http://www.cisco.com/en/US/docs/ios/12_4t/qos/configuration/guide/qsnbar1.html

- Dot1q Transparency for EoMPLS on WAN ports—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_Dot1q_Transparency_for_EoMPLS
- Dynamic ARP Inspection (DAI)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Dynamic ARP Inspection](#)” chapter.
- Dynamic Host Configuration Protocol (DHCP)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfdhcp.html
- Dynamic Multipoint VPN (DMVPN) Phase 2 (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftgreips.html
- Easy VPN Server features (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftunity.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_mvsesoo.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)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter.
- Encrypted Multicast over GRE (supported on SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- Encrypted Preshared Key (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_epsk.html
- EtherChannel—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring EtherChannels](#)” chapter.
- EtherChannel Enhancement - 128 EtherChannels Support—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[EtherChannel Feature Overview](#)” section in the “[Configuring EtherChannels](#)” chapter.
- EtherChannel Min-Links—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring the EtherChannel Min-Links Feature” section in the “[Configuring EtherChannels](#)” chapter.
- Ethernet over MPLS (EoMPLS) per VLAN QoS—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#Configuring_EoMPLS_VLAN_Mode_for_SUP720-3BXL-Based_System
- Flex Links—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring Flex Links” chapter.
- 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

- Gateway Load Balancing Protocol (GLBP)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_glb2.html
- Generic Online Diagnostics (GOLD)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Online Diagnostics](#)” chapter and the “[Online Diagnostic Tests](#)” appendix.
- Half-Bridging on FlexWAN ATM interfaces (CSCin27157)
- Hardware Capacity Monitoring—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Determining System Hardware Capacity](#)” section in the “[Power Management and Environmental Monitoring](#)” chapter.
- Hardware Control Plane Interface for Control Plane Policing (CoPP):
 - Release 12.2SX does not support CoPP output rate limiting (policing).
 - Release 12.2SX does not support the CoPP silent operation mode.
 - Release 12.2SX does not support the **match protocol arp** command.
 - Release 12.2SX automatically installs the CoPP service policy on all DFC-equipped switching modules.
 - In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Control Plane Policing](#)” chapter.
- Hardware-supported counters for hardware-supported ACLs, displayed by the **show tcam interface** command (not supported in PFC3A mode). See this publication:
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_s6.html#show_tcam_interface
- 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
- 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
- IDSM-2 EtherChannel load balancing—See this publication:
<http://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/cli/cliguide.html>
- IEEE 802.1Q protocol tunneling—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Layer 2 Protocol Tunneling](#)” chapter.
- IEEE 802.1Q tunneling—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring IEEE 802.1Q Tunneling](#)” chapter.
- IEEE 802.1s - Multiple Spanning Tree (MST) Standard Compliance—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Understanding MST](#)” section in the “[Configuring STP and MST](#)” chapter.
- IEEE 802.1w, rapid reconfiguration of spanning tree; also called Rapid-Per-VLAN-Spanning Tree (Rapid-PVST)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Understanding IEEE 802.1w RSTP](#)” section in the “[Configuring STP and MST](#)” chapter.
- IEEE 802.1X Port-Based Authentication—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring IEEE 802.1X Port-Based Authentication](#)” chapter.

- IEEE 802.3ad, link aggregation control protocol (LACP)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Understanding IEEE 802.3ad LACP EtherChannel Configuration](#)” section in the “[Configuring EtherChannels](#)” chapter.
- IGMP snooping and the IGMP snooping querier—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring IGMP Snooping and MVR for IPv4 Multicast Traffic](#)” chapter.
- IGMP Static Group Range Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/stgrpsxf.html
- IKE: Initiate Aggressive Mode (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ft_ikeag.html
- Integrated IS-IS global default metric—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtisglob.html
- Integrated IS-IS protocol shutdown support maintaining configuration parameters—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtisprot.html
- Integrated IS-IS support for BFD over IPv4—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html



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

- Interior Border Gateway Protocol (iBGP) Multipath Load Sharing—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsbgpls.html



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

- Internet Group Management Protocol Version 3 (IGMPv3) snooping—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[IGMP Version 3 Support Overview](#)” section in the “[Configuring IGMP Snooping and MVR for IPv4 Multicast Traffic](#)” chapter.
- Invalid Special Parameter Index (SPI) Recovery—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gt_ispir.html
- Inverse Multiplexing over ATM (IMA) on FlexWAN module interfaces—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html
- IP-in-IP tunneling and generic routing encapsulation (GRE) tunneling (hardware-assisted)—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, and encryption.
- 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
 - IPsec Anti-Replay Window: Expanding and Disabling—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_iarwe.html
 - IP Security VPN Monitoring (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ipsvm.html
 - IPsec VPN Accounting (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_evpmna.html
 - 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>
 - IP Unnumbered for VLAN-SVI interfaces—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Subinterfaces on Layer 3 Interfaces](#)” section in the “[Configuring Layer 3 Interfaces](#)” chapter.

- IPv6 access services: DHCPv6 prefix delegation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html
- IPv6—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
- IPv6—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
- IPv6—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
- IPv6—Switching support for IPv6:
 - Process
 - CEFv6
 - Distributed CEFv6
- IPv6—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/12_2t/ipv6/ipv6_vgf.html

For command reference information, refer to this publication:

http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_book.html

- IPv6 hardware: multicast assist—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring IPv6 Multicast PFC3 and DFC3 Layer 3 Switching](#)” chapter.
- IPv6 multicast: Bootstrap Router (BSR)—See the BSR information in the *Cisco IOS IPv6 Configuration Library* and the *Cisco IOS IPv6 Command Reference*.
- IPv6 Multicast: HW assisted egress replication—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Displaying the Replication Mode Auto Detection Status](#)” section in the “[Configuring IPv6 Multicast PFC3 and DFC3 Layer 3 Switching](#)” chapter.
- IPv6 multicast RPR support—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring RPR Supervisor Engine Redundancy](#)” chapter.
- IPv6 QoS: (quality of service)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[General Guidelines](#)” section in the “[Configuring PFC QoS](#)” chapter.
- IPv6 Support on WAN Interfaces—See this publication:
http://www.cisco.com/en/US/docs/ios/solutions_docs/ipv6/IPv6dswp.html
- IS-IS caching of redistributed routes—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isredrib.html
- IS-IS Incremental SPF—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/isisispsf.html
- IS-IS Limit on Number of Redistributed Routes—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsiredis.html
- IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsisiadv.html
- IS-IS support for priority-driven IP prefix RIB installation—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fslocrib.html
- IS-IS Support for Route Tags—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t2/feature/guide/gtisitag.html

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

**Caution**

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

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

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

- Key rollover for certificate renewal—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtkyroll.html
- L3 MPLS VPN over GRE on 7600-SIP-400—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- Layer 2 switch ports and VLAN trunks with the Dynamic Trunking Protocol (DTP), including support on Gigabit Ethernet ports for jumbo frames—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring LAN Ports for Layer 2 Switching](#)” chapter.
- Layer 2 traceroute—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using the Layer 2 Traceroute Utility](#)” chapter.
- Link Fragmentation and Interleaving (LFI) for FlexWAN Frame Relay interfaces and ATM Virtual Circuits—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftdlfi2.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.

- Low Latency Queueing (LLQ) and Class-based Weighted Fair Queueing (CBWFQ) on FlexWAN MLPPP links—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html
- MAC address-based traffic blocking—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring MAC Address-Based Traffic Blocking](#)” section in the “[Configuring Network Security](#)” chapter.
- Manual Certificate Enrollment (supported with SPA-IPSEC-2G):
 - Also called TFTP and Cut-and-Paste
 - See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftmancrt.html
- Mapping a subinterface to an EoMPLS VC on 7600-SIP-400—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html

- match cos classification on 7600-SIP-400—See this publication:
http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/6500series/sipspasw.html
- Metro Ethernet Advanced QinQ Service Mapping—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Advanced_QinQ_Service_Mapping
- MLD snooping—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring MLD Snooping for IPv6 Multicast Traffic” chapter.
- MPLS Basic, including Provider (P) and Provider Edge (PE) functionality (MPLS; not supported in PFC3A mode)—See this publication:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/pfc3mpls.html#Basic_MPLS_Load_Balancing
- MPLS Label Distribution Protocol (LDP; not supported in PFC3A mode)—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/mpls.html#MPLS_Support_on_OSMs
- 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
- 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) Fast Reroute (FRR) Link and Node Protection—See these publications:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsfr24.html

**Note**

Also see MPLS Traffic Engineering DiffServ Aware (DS-TE). MPLS TE FRR Link and Node Protection is not supported on these interface types:

- Port channel interfaces
- Switch virtual interfaces (SVIs)
- Multiple link point-to-point protocol (MLPPP) interfaces
- Multilink Frame Relay (MLFR or MFR)

- MPLS Traffic Engineering (TE) Interarea Tunnels—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiarea3.html
- MPLS Virtual Private Networks (MPLS VPN; not supported in PFC3A mode)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsmvpns.html
- MPLS VPN Carrier Supporting Carrier (not supported in PFC3A 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 (not supported in PFC3A mode)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsiaslbl.html
- MPLS VPN—OSPF and Sham-Link Support (not supported in PFC3A mode)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0st/12_0st21/feature/guide/shamlink.html
- MPLS VPN ID (not supported in PFC3A mode)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/vpnid2.html
- MPLS VPN support for EIGRP between Provider Edge (PE) and Customer Edge (CE) —See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/fteipec.html



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

- 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 enhancement - egress replication performance improvement and Multicast Enhancement - Replication Mode Detection—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring the Replication Mode](#)” and “[Enabling Local Egress Replication](#)” sections in the “[Configuring IPv4 Multicast Layer 3 Switching](#)” chapter.
- Multicast-VPN: Multicast Support for MPLS VPN—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring IPv4 Multicast VPN Support](#)” chapter.

**Note**

Support for MVPN also includes support for multicast VRF (MVRP). MVRP is also known as multicast over VRF-lite. MVPN and MVRP are supported in PFC3B or PFC3BXL mode and PFC3C or PFC3CXL mode.

- Multiple-Hot Standby Routing Protocol (MHSRP)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfip.html
- Multiple RSA Key Pair Support (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftmltkey.html
- Multipoint bridging (MPB)—See these publications:
http://www.cisco.com/en/US/docs/routers/7600/install_config/flexwan_config/features.html
http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/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
- NAC - L2 IP; Network Admission Control (NAC) Layer 2 Layer 2 IP validation—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Network Admission Control](#)” chapter.
- NetFlow Aggregation (hardware assisted)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring NetFlow Aggregation](#)” section in the “[Configuring NetFlow](#)” chapter.
- NetFlow - Bridged Flow Statistics—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Enabling NetFlow for Ingress-Bridged IP Traffic](#)” section in the “[Configuring NetFlow](#)” chapter.
- NetFlow Data Export (NDE)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring NDE](#)” chapter.

- NetFlow multicast support:
 - Supported only with NetFlow v9 export format.
 - See this publication:
http://www.cisco.com/en/US/docs/ios/12_3/feature/guide/nfmultic.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.
- NetFlow Multiple Export Destinations:
 - Allows entry of a second **ip flow-export destination** command
 - See In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring the NDE Destination](#)” section in the “[Configuring NDE](#)” chapter.
- NetFlow v9 Export Format, including NetFlow Export of BGP Nexthop Information—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3/feature/gde/nfv9expf.html
- Network Address Translation (NAT) and Port Address Translation (PAT) for IPv4 unicast and multicast traffic (hardware assisted)—Note the following information about hardware-assisted NAT:
 - 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/1cftpadr.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/mcl/122sxmcl/12_2sx_mcl_book.html

(CSCea23296)

- Optimized ACL logging (supported only with PFC3)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Optimized ACL Logging](#)” section in the “[Understanding Cisco IOS ACL Support](#)” chapter.

- OSPF Forwarding Address Suppression in Translated Type-5 LSAs—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ftoadsup.html
- OSPF Inbound Filtering Using Route Maps with a Distribute List—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/routmap.html
- OSPF Incremental Shortest Path First (i-SPF)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospfispf.html
- OSPF Limit on Number of Redistributed Routes—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsoredis.html
- OSPF link-local signaling (LLS) per interface basis—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospflls.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 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 Shortest Path First Throttling—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_spftrl.html
- OSPF support for BFD over IPv4—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

**Note**

Also see “Bidirectional Forwarding Detection (BFD) standard implementation.”

- OSPF Support for Fast Hellos—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fasthelo.html
- OSPF support for forwarding adjacencies over MPLS traffic engineered tunnels—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/ospffa.html
- OSPF Support for Link State Advertisement (LSA) Throttling—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fsolsath.html
- OSPF support for unlimited software VRFs per provider edge (PE) router—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtospfvf.html
- Packet classification based on layer3 packet-length (supported on WAN ports)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftmchpkt.html
- Per Interface Sticky ARP—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “Configuring Sticky ARP” section in the “Configuring Denial of Service Protection” chapter.
- Per port MAC limiting—See the **mac-address-table limit** command in this publication:
http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

- Per VLAN load balancing for advanced QinQ service mapping—See this publication:
http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Per_VLAN_Load_Balancing_for_Advanced_QinQ_Service_Mapping
- 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)SX-E 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.

- PFC QoS—PFC-hardware assisted Quality of Service (QoS)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring PFC QoS](#)” chapter.
- PFC QoS ARP ACLs for QoS Filtering—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring ARP ACLs for QoS Filtering](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS DSCP-based Queue Mapping (supported on WS-X6708-10GE and CAT6000-VS-S720-10G/MSFC3)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring DSCP-Based Queue Mapping](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS DSCP transparency (also called Received ToS byte preservation)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring DSCP Transparency](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS egress ACL support for remarked DSCP—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Enabling Egress ACL Support for Remarked DSCP](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS egress DSCP mutation—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Egress DSCP Mutation](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS egress policing for LAN ports configured as Layer 3 interfaces and for VLAN interfaces—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Attaching a Policy Map to an Interface](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS features on tunnels (not supported in PFC3A mode)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[PFC QoS Configuration Guidelines and Restrictions](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS filtering in MAC ACLs per-VLAN and CoS-based (not supported in PFC3A mode)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring MAC ACLs](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS - Ignore Port Trust—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Enabling Ignore Port Trust](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS Ingress CoS mutation on IEEE 802.1Q tunnel ports—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Ingress CoS Mutation on IEEE 802.1Q Tunnel Ports](#)” section in the “[Configuring PFC QoS](#)” chapter.

- PFC QoS Protocol-Independent MAC ACL Filtering (not supported in PFC3A mode)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Protocol-Independent MAC ACL Filtering](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS SRR (Shaped Round Robin)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Allocating Bandwidth Between Standard Transmit Queues](#)” section in the “[Configuring PFC QoS](#)” chapter.
- PFC QoS user-based microflow policing—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Microflow Policers](#)” section in the “[Configuring PFC QoS](#)” chapter for information about configuring microflow policing based on either source or destination addresses.
- PIM Snooping—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring PIM Snooping](#)” chapter.
- PIM snooping DR flooding enhancement—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Disabling PIM Snooping Designated-Router Flooding](#)” section in the “[Configuring PIM Snooping](#)” chapter.
- PKI AAA authorization using the entire subject name—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t11/feature/guide/gt_dnall.html
- Policy-based routing (PBR) with hardware assist 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/qcftpbr.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. Release 12.2(33)SXH and later releases use the Release 12.2 syntax, which requires **standby preempt** and **standby priority** to be entered as separate commands:
http://www.cisco.com/en/US/docs/ios/ha/command/reference/ha_s3.html#standby_priority
http://www.cisco.com/en/US/docs/ios/ha/command/reference/ha_s3.html#standby_preempt
- 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)
- Port Security, including Port security on 802.1Q tunnel ports, port security on private VLAN ports, port security on trunk ports, port security with 4096 secure MAC addresses, and port security with sticky MAC addresses—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Port Security](#)” chapter.

- Private VLANs—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Private VLANs](#)” chapter.
- Protected private key storage—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gt_ppkey.html
- QoS: Aggregated DSCP / Precedence Values for WRED (supported on for 7600-SIP-400 ATM SPAs)—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 Data Export—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring PFC QoS Statistics Data Export](#)” chapter.
- 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/12_3t/12_3t7/feature/guide/gt_qerym.html
- Query multiple servers during certificate revocation check—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtcertcr.html
- RADIUS Load Balancing (RLB) IMSI sticky—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2sx/feature/guide/slbsxe1.html
- Real-Time Resolution for IPsec Tunnel Peer (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlres.html
- Re-enroll using existing certificate—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gthttpca.html
- Remote SPAN (RSPAN)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter.
- 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
- 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
- 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
- RFC 1889 Compressed Real-Time Protocol (cRTP) on FlexWAN interfaces—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcrtpt.html



Note cRTP is not supported on MLPPP bundled links.

- Route Processor Redundancy (RPR)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring RPR Supervisor Engine Redundancy](#)” chapter.
- Router-Port Group Management Protocol (RGMP)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfrgmp.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/12_2t/12_2t2/feature/guide/rsvpscal.html
- RSVP Scalability Enhancements—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/rsvpscal.html
- SafeNet IPsec VPN client support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gt_scse.html
- SCP health monitoring for enhanced-FlexWAN—The SCP health monitor feature provides improved debugging capabilities for problems that cause WAN module resets because of SCP keepalive failures.
- Secure Shell SSH Version 2 Client Support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ssh2.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/12_1t/12_1t1/feature/guide/sshv1c.html
For information about SSHv1 client support, refer to the following publication:
http://www.cisco.com/en/US/docs/ios/12_1t/12_1t3/feature/guide/sshv1c.html
- Show diagnostic sanity—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Diagnostic Sanity Check](#)” section in the “[Configuring Online Diagnostics](#)” chapter.
- Show Top-N—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Using Top-N Reports](#)” chapter.
- SNMP ifindex persistence—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see in the “[Configuring SNMP IfIndex Persistence](#)” chapter.
- Source Interface Selection for Outgoing Traffic with Certificate Authority (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_asish.html
- 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/12_3t/12_3t2/feature/guide/gtssmma.html

- Source-Specific Multicast with IGMPv3, IGMP v3lite, and URL Rendezvous Directory (URD)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfssm.html
- SPAN—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter.
- SPAN destination port permit list—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Destination Port Permit Lists \(Optional\)](#)” section in the “[Configuring Local SPAN, RSPAN, and ERSPAN](#)” chapter.
- Spanning tree PortFast BPDU filtering, PortFast, UplinkFast, and BackboneFast, and Root Guard Feature—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Optional STP Features](#)” chapter.
- Spanning Tree Protocol (STP)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring STP and MST](#)” chapter.
- SSM mapping for IPv6—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/ipv6_vgf.html
- Standard Domain Naming System (DNS) support—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfipadr.html
- Strict priority low latency queueing (LLQ) on WAN ports—See this publication:
[http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Configuring_Strict_Priority_Low_Latency_Queueing_\(LLQ\)_Support_on_the_OSM-2+4GE-WAN+](http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pwan.html#Configuring_Strict_Priority_Low_Latency_Queueing_(LLQ)_Support_on_the_OSM-2+4GE-WAN+)
http://www.cisco.com/en/US/docs/routers/7600/install_config/12.2SX_OSM_config/pos.html#Configuring_Strict_Priority_LLQ_Support_on_POS_Optical_Service_Modules
- TCP intercept (hardware-assisted)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring TCP Intercept](#)” section in the “[Configuring Network Security](#)” chapter.
- TDR cable diagnostics—TDR is supported on these switching modules:
 - WS-X6148-GE-TX
 - WS-X6148V-GE-TX
 - WS-X6148-GE-45AF
 - WS-X6548-GE-TX
 - WS-X6548V-GE-TX
 - WS-X6548-GE-45AF
 - WS-X6748-GE-TX
 - 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:

- In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Checking the Cable Status Using the TDR](#)” section in the “[Configuring Interfaces](#)” chapter.
- The **test cable-diagnostics** command in the command reference at this URL:
http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- Traffic storm control—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Traffic Storm Control](#)” chapter.
- Trusted Root Certification Authority (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/dtrustrt.html
- Trustpoint CLI (supported with SPA-IPSEC-2G)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/fttrust.html
- UDI - Unique Device Identifier—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtpepudi.html
- Unicast flood blocking (UFB)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Unknown Unicast Flood Control](#)” chapter.
- Unicast Reverse Path Forwarding (Unicast RPF), hardware-assisted, multiple-path—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Unicast Reverse Path Forwarding Check](#)” section in the “[Configuring Network Security](#)” chapter.
- UniDirectional Link Detection—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring UDLD](#)” chapter.
- Uni-Directional Link Routing (UDLR)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring UDE and UDLR](#)” chapter.
- VLAN Access Control Lists (VACLs)—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring Port ACLs and VLAN ACLs](#)” chapter.
- VACL capture—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring a Capture Port](#)” section in the “[Configuring Port ACLs and VLAN ACLs](#)” chapter.



Note VACL capture is not supported on WS-X6708-10GE ports.

- VACL Deny Logging—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring VACL Logging](#)” section in the “[Configuring Port ACLs and VLAN ACLs](#)” chapter.
- Virtual Router Redundancy Protocol (VRRP)—See this publication:
http://www.cisco.com/en/US/docs/ios/12_0st/12_0st18/feature/guide/st_vrrpx.html
- VLANs—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring VLANs](#)” chapter.
- VLANs over IP unnumbered sub-interfaces—See this publication:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtunvlan.html

- VLAN translation—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring VLAN Translation](#)” section in the “[Configuring VLANs](#)” chapter.
- VLAN Trunk Protocol (VTP) and VTP domains—In the *Cisco IOS Software Configuration Guide*, Release 12.2(33)SXH and Later Releases, see the “[Configuring VTP](#)” chapter.
- Voice over Frame Relay (VoFR) FRF.11 and FRF.12 for FlexWAN interfaces—See this publication: http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/vvfvofr.html



Note Because Release 12.2SX does not support voice modules, switches supported in Release 12.2SX can act only as a VoFR tandem switch when FRF.11 or FRF.12 is configured on the FlexWAN module.

- VRF Aware IPsec (supported with SPA-IPSEC-2G)—See this publication: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/hardware/Config_Notes/78_14459_support_TSD_Island_of_Content_Chapter.html
- VRF Lite (Multi-VRF for CE Routers) with IPv4 forwarding between VRFs interfaces, IPv4 ACLs, and IPv4 HSRP (supported on LAN and WAN ports)—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.

- Web Cache Control Protocol (WCCP)—See this publication: http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_wccp.html

Unsupported Features and Commands



Note See also the “[Supervisor Engine 32 Restrictions](#)” section on page 42 and the “[Cisco IOS Software Modularity Unsupported Features](#)” section on page 5.

- Hardware—See the “[Unsupported Hardware](#)” section on page 110.
- In Release 12.2(33)SXH and later releases:
 - DECNet
 - Route Processor Redundancy Plus (RPR+)
 - Network-based application recognition (NBAR) for LAN interfaces (supported in earlier releases only with Supervisor Engine 2)
- These QoS interface commands are not supported on SPA interfaces:
 - **traffic shape**
 - **priority-group**
 - **custom-queue-list**

- **tx-queue-limit**
 - **fair-queue**
 - **random-detect**
 - **rate-limit**
 - **tx-ring-limit**
 - **max-reserved-bandwidth**
- These QoS interface commands are not supported on FlexWAN interfaces:
 - **traffic shape**
 - **priority-group**
 - **custom-queue-list**
 - **tx-queue-limit**
- Control Plane DSCP Support for RSVP
- RSVP Scalability Enhancements
- Random Sampled NetFlow (**flow-sampler** commands)
- In releases earlier than Release 12.2(33)SXH, 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)
- Commands to globally disable EtherChannel or trunking
- **write tech-support** 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)
- Command to display the port MAC address
- System warnings on port counters
- VLAN Management Policy Server (VMPS) client or server
- Cisco IOS MAC-layer access control lists (ACLs)
- Cisco IOS firewall feature set (includes context-based access control; CBAC)
- 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 in Release 12.2(33)SXI and Rebuilds

- [Open Caveats in Release 12.2\(33\)SXI and Rebuilds, page 173](#)
- [Caveats Resolved in Release 12.2\(33\)SXI3, page 175](#)
- [Caveats Resolved in Release 12.2\(33\)SXI2a, page 179](#)
- [Caveats Resolved in Release 12.2\(33\)SXI2, page 179](#)
- [Caveats Resolved in Release 12.2\(33\)SXI1, page 191](#)
- [Caveats Resolved in Release 12.2\(33\)SXI, page 205](#)

Open Caveats in Release 12.2(33)SXI and Rebuilds

Identifier	Technology	Description
CSCtc54248	Management	CDP neighbors aren't seen on sub-intf when it is disabled on main intf
CSCsv62004	MPLS	standby crashes with ipbase image and VRF config
CSCsx28752	MPLS	CPU hog on scaling MPLSoGRE sessions on Modular IOS image
CSCso97991	QoS	policy with bc value less than default(4ms) will cause drops on WAN int
CSCsx51705	QoS	Scalability:HQF not programmed on Enhanced Flexwan after OIR
CSCsu05464	Routing	System out of mem on SSO switchover with more than 32K ipv6 ref-acl flow
CSCsx31739	Routing	Outbound policy changes does not reflect by itself in MTR Code base
CSCsy27228	Routing	Eagle_cnh: Match statement fail to match prefixes
CSCsy27511	Routing	4basn: Issue generating update for pfx w/ 255 as# to old speaker
CSCsv46973	Security	"Change Password" is not properly relyaed
CSCsm75764	Unknown	URL redirect feature is not working properly with s/w switched traffic.
CSCsm96384	Unknown	Routed port is not going to authorized state for webauth fallback
CSCso39162	Unknown	W2: SCHED-7-WATCH: Attempt to monitor... Process= "NAM_Process" & TB's
CSCso79135	Unknown	Wism controller ports 1 state is down after mod shut/unshut
CSCsq48025	Unknown	DACL is not getting programmed untill next Probe interval.
CSCsr22282	Unknown	All the trap entries are cleared on any port flap in the same vlan
CSCsr58151	Unknown	C2W2: EOAM:errdisabled port doesn't recover even if errdisable rcvry en
CSCsr93564	Unknown	AUTHZ success with wrong DACL entry.
CSCsu66341	Unknown	W2: 'MLS MSC' ISSU client needs error buginf, for incompatible case
CSCsu68054	Unknown	Cat6k Platform changes required for BGP 4-bytes AS Numbering
CSCsu82580	Unknown	6VPE : Traffic dropped under stress configuration with more then 3Kvlan
CSCsu95237	Unknown	SSO switchover,clear packet seen on the wire exposing the inner IP pkt
CSCsu99813	Unknown	C2HD1-SI:Span Distributed Stops Traffic - Centralized Duplicates
CSCsv20927	Unknown	Netflow TCAM threshold exceeded syslog in SSO setup with sup acc traffic
CSCsv39496	Unknown	TB@rfsc_issu_negotiate_and_open_server_port on RPR upgarde from W1 to W2
CSCsv40770	Unknown	%ICC_ISSU_NEGO-SP-3-OPEN_PORT_RELIABLE: Can't open reliable port

Identifier	Technology	Description
CSCsv40974	Unknown	"wism mod <mod> controller <l
CSCsv53086	Unknown	ipv6 traffic route-cache switched at ipv6ip tunnel (over mpls)c tail end
CSCsv57305	Unknown	VSS: software forced reload with 100Mbps SFPs in supervisor uplink ports
CSCsv61041	Unknown	VSS: static mac-address-table entries missing in standby running-config
CSCsw38512	Unknown	T/B upon SSO with VSS
CSCsw46893	Unknown	C2HD1-SI - %CHKPT-4-GET_HUGE_BUF: Client (Event Manager) message seen
CSCsw50021	Unknown	After SSO, FIBIDBINCONS1: An internal software error occurred
CSCsw70162	Unknown	C2W21: Span port capture duplicated port-channel packets after SSO
CSCsw93969	Unknown	%ICC_ISSU_NEGO-SP-3-OPEN_PORT_RELIABLE: Can't open reliable port
CSCsx07137	Unknown	Invalid " %FM-4-L2_DYN_TCAM_EXCEPTION" error message for some cases.
CSCsx08647	Unknown	Traceback at bitlist_validbit within vs_ltl_mgr_proc
CSCsx11253	Unknown	Traceback@ip_adm_ha_cf_get_msg_buf during reauthentication with webauth
CSCsx19106	Unknown	Incomp ISSU msg type in PFconfig client on bulk-sync in dual-active cond
CSCsx24934	Unknown	CPU Monitor not heard and ipc TBs on Active VSS switch on issuing Reload
CSCsx27836	Unknown	VS: STP state on standby SP shows DWN sometimes and SSO causes high CPU
CSCsx49071	Unknown	After SSO on Sup4, IPV6 Multicast traffic is not forwarded
CSCsx49326	Unknown	Port-security on TenGig ports doesn't install dynamic mac as secure macs
CSCsx52586	Unknown	Not able to identify ATM Intf and PVC in o/p "sh spanning-tree vlan id"
CSCsx67115	Unknown	VPLS:cos2exp not marked after OIR of Core facing SIP 400 & SIP 600
CSCsx76168	Unknown	ISSU : hqf ipc Tracebacks on ISSU runversion.
CSCsx76244	Unknown	Sup720-Standby continuously reboots on psec mac-move violation with prot
CSCsx95302	Unknown	C2W21: %SYS-SP-2-INTSCHED: 'idle' at level 2 -Process= "Port-Security"
CSCsx96689	Unknown	Bulk sync failed for stp with 802.1x/MDA
CSCsy24099	Unknown	get platform-provided x-matrix table on RP
CSCsy47965	Unknown	FID:for non existent fid ACL on the switch, authz is success
CSCsy53336	Unknown	JQL:VSS:VSLcontrol link failure causes VSS unstability and won't recover
CSCsy75971	Unknown	%CWAN_HA-STBY-4-IFCFG_DFLT_LIST_ERROR messages seen on standby
CSCsy78851	Unknown	Continous message:C6K_MPLS_LC-SP-3-INVALID_TE_IF_NUMBER with atm bundle
CSCsy87276	Unknown	Bridge-Domain: MAC learnt on psuedowire in STP BLK state
CSCsz23445	Unknown	%PORT_SECURITY-SP-6-INVALID_SESSION: Invalid Port-Security ISSU Session
CSCsz28538	Unknown	SPA Timeout for All SPA's on Boot-up.
CSCsz35605	Unknown	LBL sync failure during removal/addition of cts dot1x from a trunk port
CSCsz43938	Unknown	Vacl capture stops working on remove/add of mfr interface.
CSCsz70263	Unknown	CFM on ISL links isn't working correctly.
CSCsz73763	Unknown	misformatted unhelpful error msgs when diag sch cmd fails
CSCsz81520	Unknown	MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC: RP failed allocating IPC buffer
CSCta03464	Unknown	VPLS VC hardware entry lost upon reroute and TE FRR tunnel shutdown

Identifier	Technology	Description
CSCta13870	Unknown	Traffic duplicated on Primary and Backup tunnel after FRR
CSCta30298	Unknown	CHKPT-SP-3-NOMEM: Memory leak seen and later the box crashed
CSCta36799	Unknown	Router Crases @ ppcp_ppm_add_class_to_stored_policy_internal
CSCta36939	Unknown	c2w2b:Crash On ISSU Run Version
CSCta42061	Unknown	traceback on issu from SXI2 to SXI1.fc3 during loadversion on active
CSCta53466	Unknown	ISSU on Sup4 causes IPV6 mcast traffic loss to Rcv in Standby uplink
CSCta75226	Unknown	Mago:ds_isr_cbif ds_num:0 msg on bootup with ip-base image
CSCtb95854	Unknown	%IDBINDEX_SYNC-4-RESERVE: Failed to lookup existing ifindex, on LV & RV

Caveats Resolved in Release 12.2(33)SXI3

- [CSCtc41760](#)—Resolved in 12.2(33)SXI3
Symptom: 6500 may experience redzone crash at UDLD process. Message may appear %SYS-SP-3-OVERRUN: Block overrun at 44456570 (red zone 6D000700) -Traceback= 40291448 402938DC 40D74570 40D763A0
Traceback will vary from code to code.
Conditions: UDLD configured
Workaround: Disable UDLD.
- [CSCsh61458](#)—Resolved in 12.2(33)SXI3
Symptoms: A Cat4k switch may reload after receiving a malformed packet on one specific specific port.
Conditions: This symptom may be observed on a Cat4k switch that enables DNSIX audit trail and recieves crafted IP packets on a specific port.
Workaround: Do not enable the DNSIX audit trail.

Other Resolved Caveats in Release 12.2(33)SXI2

Identifier	Technology	Description
CSCei37916	AAA	Incorrect AAA behavior when both wait-accnt & broadcast acctnt is con
CSCsc97727	AAA	Access Point Crashes When Removing TACACS Server
CSCsq71492	AAA	IOS device crash or tracebacks at tplus_handle_req_timeout
CSCsy55362	AAA	Unresponsive Console/VTYs
CSCse75697	ATM	LOKI: ima clock should default to LINE, backout CSCin90422, CSCsb68536 .
CSCee83031	Infrastructure	test crash, dumping log before command is displayed
CSCsd99763	Infrastructure	Cisco 7200 series reload unexpectedly while configuring BGP acces list
CSCsu65967	Infrastructure	Modular IOS crash at free_lite_internal
CSCsv30540	Infrastructure	Memory corruption in remove_ws when NULL string is passed
CSCsx10028	Infrastructure	Core dump may fail to write
CSCsy31159	Infrastructure	ASR1k 'show history all' is NOT updated properly

Identifier	Technology	Description
CSCsy88640	Infrastructure	nested crash in crashinfo collection.
CSCsz29272	Infrastructure	Crash issuing commands on SP after SCP transfer
CSCta02715	Infrastructure	SXH5: RP crash on each booting time if <logging count> enabled
CSCtb37662	Infrastructure	Deferencing a null ptr in syncNlmLogTableVarbind_callback leads to crash
CSCsi99841	IPServices	vrf-aware trustpoint authentication/enrollment doesn't work
CSCsj19805	IPServices	ip igmp static-group broken after reload on int vlan on a 7600
CSCso06542	IPServices	NAT VRF command gets corrupted in running config
CSCsw65614	IPServices	NAT with route maps doesn't work for TCP application
CSCsz51146	IPServices	TCP bad segment and sequence number in BGP raises CPU on SX11 modular
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
CSCta27331	IPServices	HSRP authentication applied to secondary addresses fails
CSCta77091	IPServices	"socket SO_UDPCHECKSUM option setting failed" when sla responder
CSCta83548	IPServices	NAT Platform: unable to clear an specific nat entry
CSCta89283	IPServices	Add support for NAT redundancy feature in SX releases
CSCtb58282	IPServices	show tcp brief can cause crash
CSCsz05918	Management	CDP neighbors do not come up on vlan interface
CSCsz75221	Management	A local variable in cdp takes up 2k process stack space-prompting crash
CSCej82248	MPLS	%LFD-3-NOOCE: Traceback in lfd_fib_update_mpls_oces
CSCsx82365	MPLS	LDP does not immediately send all IP addresses on new session
CSCsz75180	MPLS	Crash due to mpls subintf being removed
CSCsz92368	MPLS	MDEBUG-2-ACCESSFREED: @tc_handle_dead_peers Enabling/disabling "mpls ip"
CSCta32836	MPLS	Vrf is not getting deleted and stuck in this state (backout CSCsx74883)
CSCsm13783	Multicast	No (*, G) join received from CE1 on PE1 MVPN
CSCsz63723	Multicast	[UNI] MLD entry denied by mCAC isn't deleted.
CSCsz88850	Multicast	Rework CSCsz16580 fix
CSCta26106	QoS	RSVP-3-CONSISTENCY error followed by an unexpected reboot.
CSCsm57831	Routing	EIGRP: admin tags do not propagate between eigrp peers
CSCsm79085	Routing	EIGRP routes flapping due to nexthop changed
CSCsq83006	Routing	Port-channel down makes EIGRP SIA
CSCsu78975	Routing	Crash seen @adj_switch_ipv4_generic_les on 38xx router
CSCsw16157	Routing	Crash following OSPF and MPLS-TE tunnel changes
CSCsw42724	Routing	EIGRP: cant reach SSO terminal state with distribute-list in VRF context
CSCsz31770	Routing	Per-user static route is not installed on LNS after session established
CSCsz43096	Routing	Getting mismatch pkts in show ip cache verbose flow,com. to expected one
CSCsz76701	Routing	Supervisor crash with decodeds pointing to ISIS
CSCsz84906	Routing	isis redistributed route is not removed when interface shutdown

Identifier	Technology	Description
CSCta08632	Routing	ISIS topology broken after Sup force-switchover with ispf
CSCta60119	Routing	non recursive accounting can cause prefixes linked to drop
CSCta93223	Routing	Router crashed upon configuring ip extcommunity and issuing show run
CSCta99162	Routing	Switch reloads when entering the command passive-interface default
CSCtb01505	Routing	Router crashes with ospf_build_net_lsa
CSCtb35914	Routing	nsf command not available in non-modular IPBase image.
CSCtb43448	Routing	EIGRP:interf cmds not removed from Standby conf when deleted from Active
CSCsc49862	Security	IPAddress in Subject Alternative Name is not parsed correctly.
CSCso27236	Security	IOS CA client shows renew date 1 Jan 1970
CSCsv54863	Security	IOS PKI: Not expired Certificate is deleted if autoenrollment fails
CSCsy74318	Security	aaa authentication fail-message not displayed over SSH
CSCsz84055	Security	System crashed unexpected while open ssh2 session
CSCej00344	Unknown	Crash when opening new session from router
CSCek53099	Unknown	SIP200+4xT3/E3:Fail to load cRTP CFG from startup file
CSCsb88996	Unknown	slb traceback spurious memory access after slb statefull switchover
CSCsk88751	Unknown	Kron CLI Process 'show tech-support password
CSCso35876	Unknown	SRB3:New active SP crash at label_entry_get_inlabel
CSCso36150	Unknown	duplicate vlan names causing config-sync failures
CSCso79135	Unknown	Wism controller ports 1 state is down after mod shut/unshut
CSCso79925	Unknown	EC with enhanced hash method (PFC3C) has no knob to use old method (3B)
CSCsr04916	Unknown	PBR dropped the packets after add set vrf vpn1 back to the route-map
CSCsr99518	Unknown	Granikos should not init rekey after receiving new outbound SA at QM3
CSCsu29301	Unknown	C2W21: Ingress SPAN on Sup - ACE module duplicates packets
CSCsu67413	Unknown	RRI - Route disappears after ipsec rekey with multi int scenario
CSCsu84213	Unknown	RPF-MFD hardware entry is missed after doing SSO.
CSCsv27372	Unknown	telnet to a real(directed mode) via GRE tunnel crates SUP crash on SRC2
CSCsw28024	Unknown	Router is getting crashed at crypto_ikmp_cfg_auto_update_parameters
CSCsx13442	Unknown	After shut no shut hub tunnel, spoke cannot trigger isakmp SA
CSCsx81468	Unknown	CWPA2: Drops CLNS Hello packets
CSCsy03587	Unknown	c2w2b: SYS-2-MALLOCFAIL: Memory allocation failed seen with tracebacks
CSCsy07709	Unknown	C2W2: %COMMON_FIB-4-FIBNULLIDB: Missing idb for fibidb Port-channel5A
CSCsy30937	Unknown	Modify dual-active fast-hello function for rapid detection and recovery.
CSCsy34566	Unknown	Disable VLAN mapping on ME6524, 6148A-GE-TX
CSCsy69740	Unknown	SXH: Traffic drop on L2 PO after cleared psecurity on rcving L2 ports
CSCsz01976	Unknown	Need a cli to dump the rommon environment and unset rommon variable
CSCsz04297	Unknown	Cat6k: False Dynamic MAC entry is installed with format 0000.<LTL>.0000
CSCsz23445	Unknown	%PORT_SECURITY-SP-6-INVALID_SESSION: Invalid Port-Security ISSU Session

Identifier	Technology	Description
CSCsz36826	Unknown	6509E fan-tray failed to restore back to HP mode after OIR
CSCsz50968	Unknown	ace interface and vlans up but has no ip connectivity to CAT 6K
CSCsz74896	Unknown	VSS redundancy reload shelf X causes UDLD err-disable
CSCsz76015	Unknown	C2W2: Need cli to set PF_BIAS to ensure lower slot# Sup boots as active
CSCsz81520	Unknown	MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC: RP failed allocating IPC buffer
CSCsz81627	Unknown	spurious memory accesses due to snmp
CSCsz83701	Unknown	W2B: SFP-UTP entPhysicalVendorType cevSFP1000BaseSx to zeroDotZero
CSCsz84544	Unknown	output drops increment on not-connected interface of 6548GE-TX module
CSCsz86787	Unknown	IPV6 mcast and IPV4 EMVPN VRF Lite traffic are not forwarded after SSO
CSCsz87648	Unknown	SP/RP and redundant system handshake broken when the kernel crashes.
CSCsz92137	Unknown	Crash in crypto_destroy_sadb_root() upon unconfiguring tunnel protection
CSCsz92508	Unknown	SPA module reloads when no response to keep-alive polling
CSCsz96469	Unknown	Tracebacks seen @chunk_free_with_pc while unconfiguring
CSCta06175	Unknown	Cat6500/SXH: Deleted configs re-appear on IDSM reset
CSCta06689	Unknown	Rapid PVST:mac address table not flushed after topology change
CSCta10402	Unknown	Tracebacks seen due to BFD PP Process
CSCta10870	Unknown	FPOE takes long time to be programmed on active vss switch
CSCta14457	Unknown	A Cisco device may report alignment errors
CSCta15415	Unknown	DHCP Snooping functionality is not working fine with private vlan
CSCta15851	Unknown	Changing allowed vlan mask causes WiSM LAG member ports to reset
CSCta17587	Unknown	VRF + RHI combination does not work on FWSM
CSCta21771	Unknown	%CONST_DIAG-SP-3-HM_FCI_0-STUCK: Flow control stuck at 0 error on modul
CSCta22749	Unknown	C2W2b: %CONST_DIAG-SW1_SP-3-BOOTUP_TEST_FAIL:LC powercycled during Multip
CSCta27279	Unknown	WCCP s/w switching with Ingress redirection & interface ACL
CSCta30298	Unknown	CHKPT-SP-3-NOMEM: Memory leak seen and later the box crashed
CSCta32922	Unknown	SP crash due to heartbeat failure.
CSCta36799	Unknown	Router Crases @ ppcp_ppm_add_class_to_stored_policy_internal
CSCta36939	Unknown	c2w2b:Crash On ISSU Run Version
CSCta42989	Unknown	"%CSM parser state" configuring CLI when configuring via XML also
CSCta44166	Unknown	Memory leak seen with dynamic crypto map
CSCta48968	Unknown	Modular IOS kernel crashinfo has missing information
CSCta52689	Unknown	cat6k crash in RP due to address error with wccp configuration
CSCta55498	Unknown	[Modular IOS] MIPS CP0 registers save algorithim needs a few improvements
CSCta56676	Unknown	IPsec SA lifetime can go to negative values
CSCta57705	Unknown	C2W2b: reg_invoke_vs_ltl_src_index_changed() needs to be added on stdby.
CSCta57778	Unknown	auth-mgr/eap:: %IDMGR-3-INVALID_ID: bad id in id_get (bad table id)
CSCta60531	Unknown	VSS Preemption causes CAM table updation fails in FWSM env

Identifier	Technology	Description
CSCta67007	Unknown	c2hd1:VRF interfaces not shown and not pinging the CE's
CSCta68053	Unknown	time-period does not take effect in configuration archive
CSCta74242	Unknown	VSS: crash due to snmp get after standby chassis reloads
CSCta74315	Unknown	WS-X6324-100FX-MM May Be Inoperable and Have Status "Other"
CSCta84749	Unknown	Etherchannel should not be allowed if auto qos is enable
CSCta94179	Unknown	Recirculated MPLS packets because of egress service policy are dropped
CSCtb03003	Unknown	VSS: MAC table on standby Supervisor not flushed on link change
CSCtb15569	Unknown	VPN-SPA - traffic failed to decrypt due to SecInfo check failure
CSCtb23289	Unknown	Major temperature alarm has to force system shutdown
CSCtb27643	Unknown	cat6000 Medium buffers leak on SP leading to crash
CSCtb38547	Unknown	Incorrect CP0 values and empty kernel variable section in kernel crashin
CSCtb62523	Unknown	PfR - inside prefixes not learned on cat6k BR
CSCtb63352	Unknown	VSS: With 6KW DC PS, no power to bringup VSL supervisor or linecard
CSCtb66983	Unknown	Nas-port-type is missing in Access-request
CSCtb68478	Unknown	"Illegal nextSsIndex value" message should be removed
CSCtb83677	Unknown	Power Deny for pre-standard power on SXI2 or Later
CSCtb87454	Unknown	DHCP Rogue Server Detection

Caveats Resolved in Release 12.2(33)SXI2a

Identifier	Technology	Description
CSCsu65967	Infrastructure	Modular IOS crash at free_lite_internal
CSCtb15569	Unknown	VPN-SPA - traffic failed to decrypt due to SecInfo check failure
CSCtb27643	Unknown	cat6000 Medium buffers leak on SP leading to crash

Caveats Resolved in Release 12.2(33)SXI2

Resolved Infrastructure Caveats

- [CSCsx49573](#)—Resolved in 12.2(33)SXI2

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/warp/public/707/cisco-sr-20090114-http.shtml>

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

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

Resolved IP Services Caveats

- [CSCsv87997](#)—Resolved in 12.2(33)SXI2

Symptom: DHCPv6 relay process crash on Actice RP.

Conditions: Unknown at this time.

Workaround: Unknown at this time.

- [CSCsw18636](#)—Resolved in 12.2(33)SXI2

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

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

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

- [CSCsx16152](#)—Resolved in 12.2(33)SXI2

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

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

Workaround: No workaround except turning off DHCPv6 relay.

Resolved Routing Caveats

- [CSCsx73770](#)—Resolved in 12.2(33)SXI2

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

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

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

- [CSCsy86021](#)—Resolved in 12.2(33)SXI2

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

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

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

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

Cisco has released free software updates to address these vulnerabilities.

No workarounds are available for the first vulnerability.

A workaround is available for the second vulnerability.

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090729-bgp.shtml>

Resolved Security Caveats

- [CSCsx70889](#)—Resolved in 12.2(33)SX12

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/warp/public/707/cisco-sa-20090923-tunnels.shtml>

Resolved Unknown Caveats

- [CSCsy07555](#)—Resolved in 12.2(33)SX12

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

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml>

- [CSCsy15227](#)—Resolved in 12.2(33)SX12

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/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>

- [CSCsy68923](#)—Resolved in 12.2(33)SX12

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

Workarounds: None

Other Resolved Caveats in Release 12.2(33)SX12

Identifier	Technology	Description
CSCei37916	AAA	Incorrect AAA behavior when both wait-accnt & broadcast acctnt is con
CSCei62358	AAA	Downloading callback-dialstring as part of Tacacs+ author leads to crash
CSCsb34770	AAA	AAA Authentication banner for TACACS behaviour
CSCse12395	AAA	Check keys error for accounting does not cause failover

Identifier	Technology	Description
CSCsl63494	AAA	Issue with session accounting in AAA
CSCsz07569	AAA	Session id changes between interim and stop records
CSCsz43356	AAA	CPUHOG and Traceback after multiple SSH logins
CSCea90968	ATM	Bus error crash after (config-if)# atm pvp 1
CSCsx43905	ATM	Router Crash at dlencia.c on 12.2(33.4.14)SXH
CSCsr27727	Content	Cat6K experiences a reload after %SYS-2-ASSERTION_FAILED: message
CSCsz36400	Content	WCCP router may become confused with incompatible web-cache config
CSCej05426	Infrastructure	HA AutoSAA issuing no rtr react 100001 forces stby into RPR mode
CSCse25551	Infrastructure	IP SLA Group Schedule association with Individual Probes Forgotten .
CSCsj24186	Infrastructure	%SYS-2-NOBLOCK messages from Pool Manager process
CSCsm66896	Infrastructure	IP SLA Monitor strDupOctet memory leak
CSCsq73498	Infrastructure	Dovetail: ciscoipc Crash Followed by RPC Timeout with MultiOS IPC
CSCsq74185	Infrastructure	Image verification not possible on 12.2(33)SRC for the c7200
CSCsr08750	Infrastructure	router is crashing after giving the command memory reserve critical 1
CSCsr94474	Infrastructure	Running-config stuck: nv_csb_semaphore locked during copy run ftp
CSCsu53150	Infrastructure	Tracebacks on ISSU RV xdr_mcast_notify_event
CSCsv54929	Infrastructure	Cannot save banner bigger than 2048 characters
CSCsv90106	Infrastructure	nested crash leads to incomplete crashinfo
CSCsw14433	Infrastructure	at UBR10K ISSU RV, ipc_do_delayed_init() sometimes delay 1 sec
CSCsw61555	Infrastructure	Router Crashes after doing SSO
CSCsw96293	Infrastructure	Reload in SNMP Proxy Forwarder after IOS upgrade
CSCsx42732	Infrastructure	IOS64: IP-SLA configuration fails due to memory alloc failure on stby
CSCsx55240	Infrastructure	Router crashes at html_config_command
CSCsy24676	Infrastructure	IFS returns false success on error conditions
CSCsy45455	Infrastructure	get-next request of rttMonJitterStatsEntry table fails
CSCsy55455	Infrastructure	Crash at saaComponentGet
CSCsy61259	Infrastructure	IFS buff cache goes into infinite loop on driver errors
CSCsy78382	Infrastructure	sending non IP traffic causes IOSD crash
CSCsy86078	Infrastructure	Memory corruption Failure
CSCsz19466	Infrastructure	C2W1: int range command with port-channel load-defer cause router crash
CSCsz21732	Infrastructure	Reload in SNMP at snmpProxyFwderSearchReq
CSCsz52815	Infrastructure	Crash when 'history hours-of-statistics-kept' has value greater than 9
CSCed01880	IPServices	Not able to configure NAT tcp timeouts beyond 4194 sec
CSCef58137	IPServices	Router Crash after high CPU, when IPNAT configured with route-map
CSCsa41736	IPServices	Router crash after enable NAT rate-limit feature
CSCse66643	IPServices	SYS-2-NOBLOCK error when redistributing NAT routes
CSCsg31017	IPServices	parser view (role based cli) not applied when access via RSH

Identifier	Technology	Description
CSCsh49973	IPServices	NAT-ALG corrupts offset value of DNS PTR response
CSCsj76907	IPServices	IPv6 UDP sockets may incorrectly show "--any--" for local address
CSCsm42110	IPServices	IGMPv3 - Multicast router ignores IGMP leave when SSM mapping configured
CSCso50205	IPServices	DNS based SSM mapping creates interface throttles when DNS is not avail
CSCsr69932	IPServices	Stale HSRP packets are being processed instead of discarded
CSCsw51864	IPServices	CHUNKFREE error and crash when changing NAT config
CSCsw52416	IPServices	NAT: dynamic nat entries do not timeout in certain case
CSCsx23602	IPServices	crash after 'clear ip nat trans *'
CSCsx33622	IPServices	Fix MSS calculation issue in TCP
CSCsx58889	IPServices	Call fails under load intermittently with cause 47 no resource avail
CSCsx63640	IPServices	Device gets crash @ tcp_find_conn_info
CSCsx74657	IPServices	Many issues with NAT/Multicast feature
CSCsy26750	IPServices	6k Crash with ipnat_ldap_fixup (Redundancy Checks needed)
CSCsy39623	IPServices	cannot ping local vlan interface ip address with NAT configured
CSCsy39667	IPServices	dhcp-proxy-client incorrectly sends DHCPRELEASE in PPP-agg use-case
CSCsy45371	IPServices	NAT: two static nat entry related issues
CSCsy76195	IPServices	standby delay timer does not take correct effect if set to >254 seconds
CSCsy77298	IPServices	[DHCPD] IOS DHCP server does not send back option 82 in DHCPNAK
CSCsy97506	IPServices	All nat'ed multicast packets punted to software
CSCsz12488	IPServices	LDAP add with malformed BER attributes causes CPUHOG and MALLOCFAIL
CSCsz16580	IPServices	[UNI]Active RP's CPU% spikes by MLD process after reload or longevity
CSCsz89107	IPServices	high cpu due to ip_input process during SNMP trap
CSCsx61048	LegacyProtocols	%SYS-3-TIMERNEG: negative offset -Process= "IPX RIP In"
CSCsw66153	Management	Native vlan not displayed in show cdp neighbor detail
CSCsx30903	Management	parser issues in global config mode
CSCsx46383	Management	No SNMP response on Cat6K for IP-FORWARD-MIB with VRF and SNMP Contexts
CSCsy17342	Management	router reload on removing cns config notify interval
CSCsx74883	MPLS	c2w2b: Standby crash @ vrf_delete_if_ready while unconfiguring vrf inte
CSCsy29604	MPLS	VRF leaking on the same router cause CEF to break
CSCsy60668	MPLS	W1.5:: Toggle "mpls tra router-id" cause router crash
CSCsz11877	MPLS	MPLS-TE Tunnel label re-allocation on mid-point router while RSVP-GR
CSCsz75180	MPLS	Crash due to mpls subintf being removed
CSCsz92368	MPLS	MDEBUG-2-ACCESSFREED: @tc_handle_dead_peers Enabling/disabling "mpls ip"
CSCsm64082	Multicast	AUTORP-4-PAK_ERR may be reported and router crashes
CSCsx15396	Multicast	Mcast IIF stays up while physical interface is down
CSCsx28948	Multicast	I/O Memory leak on 7200
CSCsx34506	Multicast	RPF failure with no PIM neighbor triggers PIM Hello

Identifier	Technology	Description
CSCsx53084	Multicast	Multiple groups fail with autorp
CSCsx58861	Multicast	Crash due to Stack for iGMP process running low
CSCsy72207	Multicast	multicast rate-limit not applied to new (*,G) entries
CSCsy80910	Multicast	Invalid ICMPv6 packet is sent after transmitting MLD reports
CSCsy96184	Multicast	PIM should not reject assert with all zero source if RPT bit is set
CSCsz48668	Multicast	SYS-2-BADSHARE: Bad refcount in datagram_done
CSCsk04590	PPP	tx cpu crash at blt_pak_holdq_peek on shutdown of a member link
CSCsm93088	PPP	MPPP toward DOM Nortel Active but not traffic crossing
CSCsw20267	PPP	MLP APS across SPA does show in the routing table after failover
CSCee63182	QoS	Router crashes while implementing rate-limit
CSCsm97014	QoS	Connectivity breaks for QOS + header compression on virtual templates
CSCsv91699	QoS	"Transmitted pkts/bytes" column showing 0 packets on LSS SIP400
CSCsy26097	QoS	Traceback seen applying Unsupported HFQ Policy
CSCsy28998	QoS	Spurious memory access and tracebacks On Boot
CSCeh66610	Routing	Min hold time from neighbor is not seen in the configuration
CSCsk96581	Routing	BGP sessions fail to establish after int flap due to hold timer expired
CSCsq20928	Routing	CEFv6 dropping IPv6 unicast packets
CSCsq58289	Routing	redistributed connected prefixes not seen as LSA 5 in ospf database.
CSCsr05431	Routing	After SSO, cef removed vrf routes before bgp graceful timers time-out
CSCsr09208	Routing	Memory allocation error of fragmentation when plenty memory available.
CSCsr50704	Routing	dmzlink-bw programs wrong traffic share count in routing table
CSCsr51801	Routing	upon router reload some of the route-maps not permitting the prefixes.
CSCsr72352	Routing	6peinterascrr:Incorrect nexthop advertised between the routereflectors
CSCsu11161	Routing	Neighbor x.x.x.x default-originate issues seen in 12.2 code
CSCsu61953	Routing	Labels not getting allocated for BGP prefixes
CSCsu92300	Routing	"sh ip mroute" shows some routes in pruned state
CSCsu96698	Routing	BGP: /32 route being advertised while 'summary-only' is configured
CSCsv73754	Routing	crash during vrf unconfig - bgp_vpn_impq_add_vrfs_cfg_changes
CSCsv91628	Routing	BGP prefixes not exchanged between Route refectors through MP-EBGP
CSCsw29664	Routing	running and startup config out of sync after iprouting.iosproc restart
CSCsw72680	Routing	IP - Packets loop if running Microsoft NLB in presence of PIM
CSCsw73196	Routing	bgp session flap btw GSR and 7600 due to illegal net(MDT grp addr issue)
CSCsw99768	Routing	BGP malformed update sent
CSCsx03301	Routing	Router crashed @ bgp_reset_reache
CSCsx06457	Routing	BGP may modify routes it does not own
CSCsx08294	Routing	OSPF encounters a bus error crash when running SPF
CSCsx18270	Routing	EIGRP: tags from version 2 peers are not displayed in topology table

Identifier	Technology	Description
CSCsx20177	Routing	"no int loopback" causes stuck prefix in isis level-2 database
CSCsx21482	Routing	Router crashes at ipv6_rip_nvgen_interface when issue wr mem command
CSCsx35205	Routing	Standby ip arp entry is not reinstalled after static arp entry removed
CSCsx39310	Routing	VRRP sends ARP req with Physical MAC if using same virtual IP as int IP
CSCsx47651	Routing	IP LSRR broken with ip unnumbered
CSCsx49358	Routing	Ping fails between the 6CE-6PE over the MPLS cloud
CSCsx51299	Routing	Crash when remove and configure ipv6 ACL via telnet and console
CSCsx75004	Routing	BGP CSC-PE advertises wrong out-label.
CSCsx96069	Routing	OSPFv3 maxage LSA remains after Area-ID change
CSCsx98673	Routing	PE not send extended-community to a peer newly added to peer-group
CSCsx99015	Routing	crash if OSPF redistributes another OSPF and interface bw changes
CSCsy15150	Routing	33SXH5: Traceback @ isis_router when default interface configured
CSCsy27394	Routing	Lawful Intercept Tap visible via show ip interface (sub-interface)
CSCsy27511	Routing	4basn: Issue generating update for pfx w/ 255 as# to old speaker
CSCsy28394	Routing	Tracebacks when attaching 62000 loopback interfaces to OSPF
CSCsy29534	Routing	Bus error crash on removing address-family in router rip config mode
CSCsy45838	Routing	show ip ospf border-router crashing router
CSCsy58115	Routing	Continuous BGP mem increase with non established neighbors
CSCsy73123	Routing	Connected route on port-channel subintf not removed when Po is down
CSCsy76404	Routing	Modular IOS: memory leak in CEF background process
CSCsy77842	Routing	TB isis_process_no_router after isis router process deleted
CSCsy84134	Routing	ARP table is flushed when deleting secondary IP address
CSCsz16724	Routing	BGPv6: default-metric is not being NVGEN'ed and not functioning
CSCsz42043	Routing	OSPF originating orphan TE LSA
CSCsz55293	Routing	wrongly marking IPv4 capability as negotiated, with peer only IPv6 sessi
CSCsz61156	Routing	NH is not stored in BGP table when IPv6 VRF is redistributed
CSCsz78992	Routing	Packet drops due to route insertion failure in EARL
CSCsd91182	Security	crypto pki export pkcs12 hangs when used with SCP
CSCsv20285	Security	Whitney:Authentication to the CA server failed using ION.
CSCsv23797	Security	SSH:Crash seen on 7200 on mcp_dev
CSCsv46973	Security	"Change Password" is not properly relyaed
CSCsw50991	Security	Traceback if underlying interface of 6to4 tunnel goes down.
CSCsy16177	Security	scp:copy to router over sshv2 fails with invalid checksum error
CSCsy17893	Security	Ping to itself doesn't work on IPIP tunnels
CSCsy22311	Security	SCP b/w IOS routers fails while the client is receiving file from server
CSCsz32366	Security	Chunk Memory corruption in SSH Process
CSCsz40612	Security	GRE keepalive retry behavior is wrong

Identifier	Technology	Description
CSCek47612	Unknown	TX cpu stats not displayed in sh hw-module slot proc cpu output
CSCek60142	Unknown	FRR does not work (about 200 ms loss) with E5 SPAs,LC crash on link flap
CSCsd39568	Unknown	stats support for PBR set ip nexthop/set interface
CSCsd45698	Unknown	Cat6K: SLB punted to CPU if src_index is port-channel index
CSCsg35285	Unknown	Slower Cache refresh for int stats when more interfaces up
CSCsh28072	Unknown	ESM may cause rotuer to crash during IPS test attack
CSCsi50091	Unknown	BFD session flaps after executing "undebug all" command.
CSCsj26698	Unknown	Acct-Session-Id in Accounting-Request is different from in Access-Reques
CSCsj89208	Unknown	RP hits TLB exception when SIP-400 OIR with 8k MPBE EFPs
CSCsk62032	Unknown	DHCP snooping support to detect rogue dhcp servers
CSCsl35174	Unknown	Setting Scorpion int MTU < packets injected results in perm 1-way traf .
CSCsm39160	Unknown	TestCFRW shows incorrectly as failed in show diagnostic sanity
CSCsm79995	Unknown	Tracebacks are seen while attaching service-policy in a atm pvc
CSCso39162	Unknown	W2: SCHED-7-WATCH: Attempt to monitor... Process= "NAM_Process" & TB's
CSCso67500	Unknown	mvpn-bidir: Reloading encaps rtr and performing sso causes df index issue
CSCso79135	Unknown	Wism controller ports 1 state is down after mod shut/unshut
CSCsq15198	Unknown	EPC:SRD:RSP720:OSPF/BFD flaps when Gi5/2 (RSP gi link) is no shutted
CSCsq69567	Unknown	SSO Switchover + unicast-routing chg cause MC traffic loss for 2 minutes
CSCsr15448	Unknown	C2W2: E-OAM session not established b/w CE and PE on Port mode EoMPLS
CSCsr43461	Unknown	vrf selection source < > missing under sh_run after router reload
CSCsr58151	Unknown	C2W2: EOAM:errdisabled port doesn't recover even if errdisable rcvry en
CSCsr59237	Unknown	OSPF adj flaps on WS-X6548-GETX, due to LTL / RBH programming mismatch
CSCsr62498	Unknown	C2W2: Span dest port continuously sends some traffic on 6748 cards
CSCsr97387	Unknown	Router crashed at crypto_delete_map_routes during ip address change
CSCsu05721	Unknown	C2W2: %NTI-SP-3-AGENT_ERR and TB was seen after issu runversion
CSCsu40166	Unknown	PBR packets send out to wrong next hop MAC after ACL is changed
CSCsu48241	Unknown	memory leak when removing igmp snooping with acl filtering
CSCsu50413	Unknown	RE: acl merge causes high rp cpu for ~50 min after reload
CSCsu52504	Unknown	%LINEPROTO-5-UPDOWN msg is output when "no cdp enable" is set
CSCsu95857	Unknown	cardDescr (.1.3.6.1.4.1.9.3.6.11.1.3) is returning incorrect value
CSCsu99813	Unknown	C2HD1-SI:Span Distributed Stops Traffic - Centralized Duplicates
CSCsv20768	Unknown	After SSO s/wover, atm clock config changes to line and PTB to UNSTABLE
CSCsv24908	Unknown	L2 Fwd Broken on other modules when SIP-400 int flaps
CSCsv27372	Unknown	telnet to a real(directed mode) via GRE tunnel crates SUP crash on SRC2
CSCsv61458	Unknown	[no] mpls ip propagate-ttl needs no mpls ip - mpls ip to take effect.
CSCsv74822	Unknown	Crash on RPR switchover in the rf_proxy_rp_sync path
CSCsv79673	Unknown	Router MAC learned dynamically after add/remove of xconnect on SVI

Identifier	Technology	Description
CSCsv94560	Unknown	c7600/MPLS: Packet reflection over EoMPLS link when vc going up
CSCsw14147	Unknown	VACL unable to capture traffic from RP
CSCsw21852	Unknown	CSM: memory leak in process "Laminar Icc Event"
CSCsw24172	Unknown	ES20:-%INTR_MGR-DFC2-3-INTR: Parsing Engine (X-Chip) [1]: Inbound Toast
CSCsw28972	Unknown	enh: provide option for port security to not install L2 trap entries
CSCsw31607	Unknown	LTL index incorrect in PI MET table
CSCsw38512	Unknown	T/B upon SSO with VSS
CSCsw40790	Unknown	SNMP Loop on PA-MC-T3+ interfaces (Installed)
CSCsw48824	Unknown	Switchport Block Unicast - prevents RTP on same VLAN
CSCsw49623	Unknown	Router crashes when PfR learn config is displayed on the border
CSCsw59517	Unknown	IGMPv3 snooping drops 'Block Old Sources' report
CSCsw68514	Unknown	SLB probes iin TESTing state while using client cmd in Vserver config
CSCsw69621	Unknown	BR DOWN if inside bgp is only type of learning configured
CSCsw76117	Unknown	TBs seen after redundancy mode change from sso to rpr
CSCsw76910	Unknown	IOS-SLB:Supervisor crashes on configuring/verifying firewallfarm CLIs
CSCsw91858	Unknown	Misleading error when 6716 is configured for VSL
CSCsw92386	Unknown	Not able to delete logging filter and crash at Tcl_NewStringObj
CSCsw96176	Unknown	BFD sessions with version 0 do not come up properly following a reload
CSCsx06578	Unknown	SIERRA:MAGO switch got crashed after reload with SIERRA_INTEG_090106
CSCsx07137	Unknown	Invalid " %FM-4-L2_DYN_TCAM_EXCEPTION" error message for some cases.
CSCsx09110	Unknown	Failed to establish ipsec tunnel with CCM
CSCsx09273	Unknown	WEBAUTH(IP adm) is not INITiating if IPDT entry already exists.
CSCsx10011	Unknown	VSS: IO memory leak from pre_process_vsibc_vsda_pak
CSCsx13050	Unknown	tcl doesn't run or Register event failed messages on Modular IOS
CSCsx19210	Unknown	[show epm session ip 0.0.0.0] crashes supervisor
CSCsx20081	Unknown	Local Web-Auth does NOT work when IP Source-Guard is enabled on port
CSCsx20862	Unknown	Peer RP index unknown messages seen on VSS setup
CSCsx21431	Unknown	Logging Filter CLI gets lost after SSO
CSCsx21886	Unknown	ISSU switchover command sync issue
CSCsx22711	Unknown	router crashes if we unconfigure 1024 GLBPv6 grp on intf and do sh mod
CSCsx27836	Unknown	VS: STP state on standby SP shows DWN sometimes and SSO causes high CPU
CSCsx28532	Unknown	VPN SPA freezes when ip mtu changed on tunnel interface
CSCsx29377	Unknown	1 sec multicast loss on standby sup720-10g
CSCsx29645	Unknown	IPv6 Multicast traffic can not converge after SSO
CSCsx34570	Unknown	VSS:remove port-channel from interface causes other members to go down
CSCsx39263	Unknown	TCAM entries are not installed for TCP intercept after SSO
CSCsx46323	Unknown	C2W21: Standby SUP resets due to monitor session on internal PO

Identifier	Technology	Description
CSCsx49071	Unknown	After SSO on Sup4, IPV6 Multicast traffic is not forwarded
CSCsx49326	Unknown	Port-security on TenGig ports doesn't install dynamic mac as secure macs
CSCsx49420	Unknown	HQoS policy attached to main interface cannot set cos to IPv6 traffic.
CSCsx49718	Unknown	Auth Man Single-host-Guest VLAN doesn't trigger reauth on EAPOL start
CSCsx49889	Unknown	SPA-IPSEC-2G-3-ACEI0TCAMFAILE:SpdSpInstall:cannot install Sp TmInsertSp
CSCsx50407	Unknown	show authenticaiton needs to display policies for a session
CSCsx53964	Unknown	Unable to control traffic-class
CSCsx55152	Unknown	Switch does not send TC trap if it is not a root bridge
CSCsx55698	Unknown	auth_mgr: spurious access @ dot1x_rp_auth_client_deleted
CSCsx58097	Unknown	Tracebacks and crash @ lfd_rewrite_mgr_fill_mfi_out_info observed on SSO
CSCsx58488	Unknown	VSL interfaces are not in restricted mode
CSCsx58786	Unknown	Router crash @ routemap_track_nexthop
CSCsx62912	Unknown	W2: update the PM switch vp limits for MST, PVST and Rapid-PVST
CSCsx64668	Unknown	Config change on port of WS-X6148-FE-SFP will move other ports to down
CSCsx64994	Unknown	Memory leaks in ccm processes after redundancy forced switchover
CSCsx76308	Unknown	HA client crashing attempting to free unassigned memory
CSCsx78789	Unknown	Router crash @ flow_sampler_select with traffic
CSCsx78812	Unknown	MLPPP+LFI over ATM : Inconsistent behavior
CSCsx79379	Unknown	IOS Auth Proxy HTTP may lead to bus error adress 0x0
CSCsx82825	Unknown	Shutdown Loopback interfaces in VSS recovery mode
CSCsx83443	Unknown	crypto debug condition leaks messages which lead to high cpu.
CSCsx93160	Unknown	SXI image shut down linecard ports of WS-X6748-GE-TX
CSCsx98446	Unknown	power consumption of act/stb sup720 has inconsistent behavior
CSCsy01275	Unknown	W15:: SYS-2-MALLOCFAIL: Memory allocation message seen after bootup
CSCsy01763	Unknown	15 - 20 packets leek to DST with PACL after SSO
CSCsy03133	Unknown	TestNonDisruptiveLoopback skipped when run as scheduled test
CSCsy03141	Unknown	Copy of CSCsx06578 - to address the original hang problem in Mago
CSCsy08048	Unknown	CF Buffer Pools need to be scaled by platform
CSCsy08838	Unknown	Zamboni allows clear packet inbound on protected interface
CSCsy12800	Unknown	priv-lvl=15 should NOT be required for Local Web-Auth
CSCsy16220	Unknown	a switch may crash due to deadlock between snmp and eem
CSCsy20589	Unknown	Port diagnostic failures following 'redundancy reload shelf' command
CSCsy21797	Unknown	Cat6k-Unexpected SNMP messages occurred
CSCsy22802	Unknown	MPLS VPN broken, vrf connection (permit missing for internal vlan acl)
CSCsy24522	Unknown	Cannot disable " errdisable detect cause dhcp-rate-limit " 12.2(33)SXI
CSCsy24691	Unknown	entPhysicalTable has power-input 3 Sensor for 6kW DC PS1 and not PS2
CSCsy24895	Unknown	Memory leak in ACE HAPI process

Identifier	Technology	Description
CSCsy26526	Unknown	Router is getting crashed at netconf_sessionQs_set_max_message
CSCsy31098	Unknown	reconfigure pim snooping when configure static mrouter port
CSCsy32202	Unknown	6500 IPSEC SPA SSO 'no crypto connect' cmd causes stdby SUP reload
CSCsy34231	Unknown	EZVPN+VRF:Router reloads while unconfigure crypto map with traffic
CSCsy34566	Unknown	Disable VLAN mapping on ME6524, 6148A-GE-TX
CSCsy37175	Unknown	2FE-PA Subintf lost connection after chassis/Flexwan2 reload
CSCsy37390	Unknown	Need to enable earl interrupt after earl initialization is done
CSCsy37652	Unknown	ws-ipsec-3 VSPA crashed in post frag processing
CSCsy38611	Unknown	Mcast traffic blackhole on uplink recvs after reload of RP switch
CSCsy41526	Unknown	PIM msgs duplicated when MPLS configured and IGMP Snooping Off on xface
CSCsy42216	Unknown	VSL Uptime Counter Reset and other Inaccuracies
CSCsy47281	Unknown	vlan distribution is not working in mago
CSCsy48986	Unknown	VSS: reload shelf shouldn't reload remote service module
CSCsy52376	Unknown	Sup crashes after numerous module resets
CSCsy53060	Unknown	0315 ion image tcp.proc crash during bootup caused switch reloaded
CSCsy53336	Unknown	JQL:VSS:VSLcontrol link failure causes VSS unstability and won't recover
CSCsy54583	Unknown	TTY data process on DFC leaks memory at prot_tty_malloc_named
CSCsy56389	Unknown	SLCP process is impacted by inserting/extracting modules
CSCsy56433	Unknown	Sh rom intermittently fails to display correct region info for standby
CSCsy58553	Unknown	Linecard reset causes traffic onto frt protected tunnel to be dropped
CSCsy61956	Unknown	Crash in ios-base when running 'show ip route' or 'show bgp' commands
CSCsy62160	Unknown	Vlan state unable to recover after shutdown by mac-limit
CSCsy62753	Unknown	MST configured router crashed after receiving PVST BPDU.
CSCsy66794	Unknown	Module Failed SCP dnld observed on ALL WAN CARDS with ISSU.
CSCsy69228	Unknown	Add CLI mls cef tunnel fragment support for non supertycho2
CSCsy69740	Unknown	SXH: Traffic drop on L2 PO after cleared psecurity on rcving L2 ports
CSCsy75971	Unknown	%CWAN_HA-STBY-4-IFCFG_DFLT_LIST_ERROR messages seen on standby
CSCsy76728	Unknown	PfR: Egress BW measured for prefix is incorrect.
CSCsy78851	Unknown	Continous message:C6K_MPLS_LC-SP-3-INVALID_TE_IF_NUMBER with atm bundle
CSCsy78994	Unknown	Memory leak in Service Task
CSCsy81934	Unknown	Non-standard static multicast MAC addresses lose ports after reload
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
CSCsy86050	Unknown	MAC Move Notifications on VSS between active and down ports
CSCsy86252	Unknown	SP Crash printing "supervisor jamming EOBC. It will be disabled."
CSCsy87619	Unknown	VSS port channel going down when powering down active switch

Identifier	Technology	Description
CSCsy94866	Unknown	C2W2B: CSM Config sync causes memory leak
CSCsy95520	Unknown	~500msec Pkt loss after transition to HSRP Active on L3 int
CSCsy96102	Unknown	FM-4-MPLS_RSVD_VLAN_ERROR-failed to remove feature when vrf delete
CSCsz06187	Unknown	VACL capture for ingress software switched packets
CSCsz09329	Unknown	invalid display for show module command firmware version t_whit21@1.0
CSCsz12369	Unknown	FPD support for SPA-8X1FE-TX-V2 is not enabled
CSCsz19246	Unknown	Crash after 'no dot1x port-control auto'
CSCsz22954	Unknown	Supported WS-X6324-100FX-MM is powered down improperly
CSCsz23448	Unknown	SIP 200 not coming up and Router Crashes after applying card type E3 1 1
CSCsz40969	Unknown	Need to add Me_Kr flow-control status registers back into sierra/whitney
CSCsz44520	Unknown	trunk port in UDLD err-disable when native vlan is shutdown
CSCsz44678	Unknown	Tunnel won't forward traffic across global to vrf
CSCsz48086	Unknown	Default violate-action is missing from 3 color policy
CSCsz52069	Unknown	2nd commit DDTS for CSCsz09329
CSCsz53809	Unknown	Configuring vlan name containing space doesnt work across reload.
CSCsz55834	Unknown	GLBP may provided BIA MAC instead of Virtual MAC for mobile users
CSCsz56229	Unknown	Crashing after receiving an IGMP v2 Leave Message.
CSCsz62046	Unknown	Crash at memcpy after CPUHOG in SNMP ENGINE
CSCsz63359	Unknown	c2w2b:"show mls qos ip" displays vslot interface instead switchid and sl
CSCsz63721	Unknown	high cpu utilization when with 1000 policy and 1000 forced target
CSCsz67334	Unknown	ciscoEnvMonTemperatureStatus trap sent sporadically as NotFunctioning
CSCsz71904	Unknown	VSS switch crashed on pm_assert_fail
CSCsz74362	Unknown	Router crash @ af_policer_error_check
CSCsz74896	Unknown	VSS redundancy reload shelf X causes UDLD err-disable
CSCsz75820	Unknown	JQL: VSS hang on SP after RP crashed by software-forced reload
CSCsz83701	Unknown	W2B: SFP-UTP entPhysicalVendorType cevSFP1000BaseSx to zeroDotZero
CSCsz86787	Unknown	IPV6 mcast and IPV4 EMVPN VRF Lite traffic are not forwarded after SSO
CSCsz92137	Unknown	Crash in crypto_destroy_sadb_root() upon unconfiguring tunnel protection
CSCsz96469	Unknown	Tracebacks seen @chunk_free_with_pc while unconfiguring
CSCta06689	Unknown	Rapid PVST:mac address table not flushed after topology change
CSCta10870	Unknown	FPOE takes long time to be programmed on active vss switch
CSCta15415	Unknown	DHCP Snooping functionality is not working fine with private vlan
CSCta22749	Unknown	C2W2b: %CONST_DIAG-SW1_SP-3-BOOTUP_TEST_FAIL:LC powercycled during Multip
CSCta24027	Unknown	See c6k_power_port_mgmt.c:pd_get_sb 98 tracebacks at bootup
CSCta32922	Unknown	SP crash due to heartbeat failure.
CSCta57705	Unknown	C2W2b: reg_invoke_vs_ltl_src_index_changed() needs to be added on stdby.
CSCsi05069	WAN	DCE Sub-interface is not coming up after provisioning

Identifier	Technology	Description
CSCsw31019	WAN	Router crashes while configuring the command "frame-relay be 1"

Caveats Resolved in Release 12.2(33)SX11

Resolved AAA Caveats

- [CSCsv06973](#)—Resolved in 12.2(33)SX11

Symptom:

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

Conditions:

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

Workaround:

Do not use TACACS single-connection option.

- [CSCsv38166](#)—Resolved in 12.2(33)SX11

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

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

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

Cisco has released free software updates that address this vulnerability.

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

This advisory is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml>.

- [CSCef52919](#)—Resolved in 12.2(33)SX11

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

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

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

- [CSCsv73509](#)—Resolved in 12.2(33)SX11

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 IPServices Caveats

- [CSCsr29468](#)—Resolved in 12.2(33)SXII

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/warp/public/707/cisco-sa-20090325-tcp.shtml>

- [CSCsv04836](#)—Resolved in 12.2(33)SXII

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/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

- [CSCsw18636](#)—Resolved in 12.2(33)SXII

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

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

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

Resolved LAN Caveats

- [CSCsv05934](#)—Resolved in 12.2(33)SXII

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/warp/public/707/cisco-sr-20081105-vtp.shtml>

Resolved Multicast Caveats

- [CSCso90058](#)—Resolved in 12.2(33)SX11

Symptoms: MSFC crashes with Red Zone memory corruption.

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

Workaround: There is no workaround.

- [CSCsu79754](#)—Resolved in 12.2(33)SX11

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

Conditions: Unknown at this time.

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

Resolved Routing Caveats

- [CSCsx10140](#)—Resolved in 12.2(33)SX11

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

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

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

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

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

(1) For more information please visit:

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

- [CSCsx73770](#)—Resolved in 12.2(33)SX11

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 Release 12.2(33)SX11

Identifier	Technology	Description
CSCsc78999	AAA	Address Error exception at TPLUS
CSCsk40765	AAA	crash due to AAA/TACACS+ server-private re-configuration
CSCsq37815	AAA	Case sensitive Username authentication is passed with wrong user name
CSCsq94524	AAA	"aaa accounting update newinfo" causes extra "jitter maximum 0" option
CSCsr70963	AAA	Crash when remove DEAD radius server from config
CSCsv02117	AAA	session flapping cause %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs
CSCsw17553	AAA	Radius-server pac keyword is not nvgened when used with automated tester
CSCsw19816	AAA	cat6000: IOS login enhancements not creating logs for telnet with AAA
CSCek78237	ATM	High CPU on ATM PA Helper process on PA-A3-T3
CSCso64050	ATM	HA functionality is not working when policy attached to atm pvc
CSCsr86103	ATM	ATMoMPLS: Traffic stops flowing on applying service-policy on atm pvc
CSCsr27727	Content	Cat6K experiences a reload after %SYS-2-ASSERTION_FAILED: message
CSCsx40747	Content	Router hangs while doing ip casa configurations
CSCef82896	Infrastructure	When removing the user name from auth dialog, http crashes
CSCin79116	Infrastructure	show memory summary could push the CPU util to 100%
CSCsc77704	Infrastructure	region_find_by_addr goes into infinite loop when spurious memory occurs.
CSCsc86307	Infrastructure	c3845 crashed @ show_systat
CSCse41523	Infrastructure	bootldr config caused stbyPRE reset if file does not exist on stby-bootf
CSCse49151	Infrastructure	3800 clock slip over times verified in lab
CSCsh85011	Infrastructure	DSGS7: Router crash at saaEnhancedHistoryFreeTab
CSCsj46707	Infrastructure	ubr7200 G1 hangs during bootup
CSCsj57479	Infrastructure	Traceback found at data_inconsistency_error_with_original_ra
CSCsj87744	Infrastructure	Parser mode change issues
CSCsk80396	Infrastructure	Inconsistant router Crash seen when jitter operation takes place
CSCsl61281	Infrastructure	Show logging command should be a privileged command
CSCsm33221	Infrastructure	IP SLA Probe type DHCP with no relay-agent IP add. on Dhcp disc. packet
CSCsm54810	Infrastructure	router stops producing the auth-proxy login page intermittently
CSCso21611	Infrastructure	Crash at internal idb counter increment function
CSCsq73498	Infrastructure	Dovetail: ciscoipc Crash Followed by RPC Timeout with MultiOS IPC
CSCsr07557	Infrastructure	Memory leak in parser_chunk_malloc after get/set on Auth Framework obj
CSCsr50834	Infrastructure	CPU HOG after changing logging buffered up to 50MB

Identifier	Technology	Description
CSCsr60789	Infrastructure	W1.3: VSL crash after preemptive switchover in ifs_open_file_decrement
CSCsu57889	Infrastructure	banner exec CLI ignoring lines starting with #, !, and ;
CSCsu78906	Infrastructure	Wrong "%SYS-5-CONFIG_I: Configured from x.x.x.x by snmp" messages
CSCsv34988	Infrastructure	Console/Telnet/SSH login banner not properly formatted after upgrade
CSCsv50606	Infrastructure	SNMP: ISSU incompatibility with message type 20
CSCsv80900	Infrastructure	W21:: EARL-SPSTBY-2-SWITCH_BUS_IDLE & PF_ASIC-SPSTBY-3-ASIC_DUMP @boot
CSCsv86766	Infrastructure	Signature fail while copy, causing system:/running-config to be deleted
CSCsw15188	Infrastructure	Router crashes with "debug isdn q931" enabled
CSCsw16658	Infrastructure	Unavailable ipv6 ACL prevent configuring ipv4 ACL
CSCsw35917	Infrastructure	SP syslog messages not sent as SNMP traps by RP's SNMP agent
CSCsw51126	Infrastructure	High CPU on Virtual Exec process after vty session timeout exec setup
CSCsw61555	Infrastructure	Router Crashes after doing SSO
CSCsw76894	Infrastructure	Problems faced with ipv6 SNMP when ipv4 address is not configured
CSCsx32841	Infrastructure	ceImageDescription may exceed 255 characters
CSCek10384	IPServices	7200 NAT dropping Out to In ESP Packets
CSCsl11712	IPServices	Router crashes when DGVPN is configured with VRF . .
CSCsm89795	IPServices	Orbitty repeatedly Crashes - Susceptible to Denial of service attacks
CSCso39062	IPServices	C2W2: %SYS-3-INVMEMINT: Invalid memory action message & TB's with PAT.
CSCso54027	IPServices	Spurious memory access in tcp_rcv_stats
CSCsq14311	IPServices	7200 crash - ipnat_unlock_parent_entry (PPTP)
CSCsq22397	IPServices	DLSw peer connection initiated from interface IP and not local-peer IP
CSCsq81365	IPServices	MFI: UDP forwarded-protocols from VRF are leaked into global table
CSCsu38774	IPServices	FTP'ing a file from a router will fail if the FTP account cannot delete
CSCsu64215	IPServices	ip tcp adjust-mss command results in packet loss for non-TCP traffic
CSCsu67461	IPServices	Router crashes when "show track brief" entered
CSCsu72176	IPServices	Crash:Process Deadlock in Standby while reloading UUT with DHCP configs
CSCsu74400	IPServices	File descriptor leak with FTP of a DHCP database
CSCsu77597	IPServices	Frames with virtual MAC dest address are dropped with bridging enabled
CSCsu95319	IPServices	IGMP report was not sent to helper address.
CSCsv12265	IPServices	HSRP stuck in INIT when learning and if address changed
CSCsv16987	IPServices	nat pool size more than 16 bit long should not be configured
CSCsv27480	IPServices	VRRP MAC aging out due to being stored as dynamic entry after reload
CSCsv54324	IPServices	HSRP stuck in INIT state after a reload on a c3845 gig-eth interface
CSCsv54510	IPServices	Router is not getting pruned after shutting the interface
CSCsv56160	IPServices	BGP session flap due to TCP selective-ack
CSCsv86201	IPServices	Modular IOS : max sockets overflow
CSCsv99443	IPServices	standby delay reload doesn't work on SUP/RSP720

Identifier	Technology	Description
CSCsw16698	IPServices	DHCP database could not be locked DHCPD process could not lock semaphore
CSCsw64000	IPServices	3800: Ethernet controller wrongly programmed when using DHCP and PIM
CSCsw66082	IPServices	Router crash seen at ip_mcast_address_lookup in ssm-map router
CSCsw73391	IPServices	ip igmp limit gets stuck
CSCsw96272	IPServices	nat overload command not translating packets
CSCsx09343	IPServices	Name resolution triggers pager in non-interactive mode.
CSCsx32283	IPServices	Malformed L field in LDAP crashes 6k with NAT
CSCsr04069	LAN	ifOutOctets for vlan subint with GTS/ratelimit is inaccurate
CSCsw81485	LegacyProtocols	Unconfiguring IPX crashes the switch
CSCsb84797	Management	ATM or FR main interface resets when disabling CDP or deleting subint
CSCse29570	Management	router crashes when pulling config from CNS containing no config initial
CSCso35250	Management	unexpected reload while communicating with CNS server
CSCsu10229	Management	The cdpCacheAddress mib not providing GLOBAL_UNICAST Address
CSCsv48296	Management	cns image retrieve command is forcing to router crash
CSCsv93351	Management	CNS ID Change unexpectedly
CSCsq49176	MPLS	7200 Bus error crash on invalid address, charlotte_post_coalesce_rx
CSCsr15969	MPLS	MPLS TE: extended tunnel id may not be 0.0.0.0
CSCsu50374	MPLS	FRR tunnels doesn't go down if TE flooding is disabled on the headend.
CSCsv00773	MPLS	Loose Path Reopt not applied when link costs changed
CSCsv13738	MPLS	slow convergence when use vrf definition instead of ip vrf
CSCsv31126	MPLS	snmpwalk of mplsTunnelTable may not show all MPLS TE Tunnels
CSCsv41456	MPLS	Tracebacks seen at IFMGR-3-DUP_IFINDEXifDescr"Virtual-Access2-mpls layer
CSCsv62004	MPLS	standby crashes with ipbase image and VRF config
CSCsw35638	MPLS	FRR Interoperability issue between Juniper PLR and IOS MP
CSCsw82028	MPLS	BGP graceful restart is not supported on IP service image
CSCsb77148	Multicast	sh ip mpacket x.x.x.x quality output is wrong after counter wraps around
CSCsc52732	Multicast	Enabling PIM on sub-IF causes mcast packet drops on other sub-IF
CSCsl32142	Multicast	crash from memory corruption from malformed auto-rp Multicast
CSCsl52213	Multicast	PIM assert timer mechanism problem
CSCsu86494	Multicast	Assert flag is not cleared after PIM neighbor loss
CSCsv29659	Multicast	RP configured inside the nat not shown on uut outside the nat
CSCsw29463	Multicast	The adjacency/ocf lookup should not be done in mcast fast switching path
CSCsw36940	Multicast	Router crashed at "mrm_manager_sender_commands"
CSCsx15396	Multicast	Mcast IIF stays up while physical interface is down
CSCsf07760	PPP	MLP: Crashes/buffer leaks when large number of sessions come up at once
CSCsr81271	PPP	Invalid VCD error messages upon PVC flap
CSCsu70011	PPP	ipv6 static route pointing to multilink (flexwan) disappears after sso

Identifier	Technology	Description
CSCsh39945	QoS	PRE3:Router crash with 'show int random' with 40k+ pppoeovlan sessions
CSCsh57935	QoS	%RSVP-3-BAD_RSVP_MSG_RCVD_AUTH_WIN after shut/no shut
CSCsl94263	QoS	Router crash at stile_update_fast_flag due to random-detect dscp-base
CSCsm28515	QoS	Marking not happening on FlexWAN interface with SXH after oir/reload
CSCso97991	QoS	policy with bc value less than default(4ms) will cause drops on WAN int
CSCsq55678	QoS	c2w2: Policy on control-plane is not working with acl log option
CSCsr05501	QoS	% NBAR Error: hwidb could not found shows up when reload
CSCsv12372	QoS	Spurious memory access @ fr_queue
CSCsv85791	QoS	Flexwan+/PA-MC-2T3+ introduce 5+ seconds delay on egress
CSCsv91699	QoS	"Transmitted pkts/bytes" column showing 0 packets on LSS SIP400
CSCsw36285	QoS	Incorrect Police rate under calss-default
CSCee30355	Routing	Memory leak at ip_multicast_ctl
CSCef65457	Routing	EIGRP and RIP advertise null0 static routes after they are removed
CSCef67010	Routing	NHRP registrations shouldn't do a routing table lookup
CSCsb15164	Routing	Security holes while configuring a standard ACE with host address
CSCsc98813	Routing	Set metric in route-map effects other RIP routes hop count
CSCsd25753	Routing	BGP Aggregated supernet routes not Advertised properly
CSCse45978	Routing	BGP to RIP redistribution breaks as RIP nexthop moves to alternate path
CSCse68877	Routing	CEF/BGP table MPLS label mismatch YW3 Non Multi-path
CSCsh54161	Routing	dune, Nov image goes unstable - creates eigrp routing loops
CSCsj42399	Routing	Redistributed static covered by network statement sets metric to 0
CSCsk87526	Routing	T/B ipv6_rib_process_changeQ after shut cmd applied Int. running RIPng
CSCsm63632	Routing	Continuous XDR IPC errors (inability to create an IPC buffer)/Watermark
CSCso56038	Routing	%DUAL-3-INTERNAL traceback at igrp2_packet_community_add_item
CSCso90107	Routing	SNMP: bgpPeertable and cbgpPeertable shows only results for ipv4 peers
CSCsq36206	Routing	MDT tunnels not getting created on 7206 Device
CSCsr01403	Routing	cefswitching2.1:More time taken(12 mts) to converge after Adjacency flap
CSCsr21670	Routing	elected more routes than expected routes as multipath
CSCsr40997	Routing	IPv6 RIP: Unconfiguring RIP from an interface doesn't update RIB on peer
CSCsr67361	Routing	I/O memory leaks when BGP neighbor points to a local address
CSCsr88705	Routing	BGP route getting lost after "shut/no shut" of BGP peering interface
CSCsu01272	Routing	MPLS PE 7600 changes RT when a BGP soft clear is executed
CSCsu05464	Routing	System out of mem on SSO switchover with more than 32K ipv6 ref-acl flow
CSCsu06447	Routing	EIGRP:static route redistribution not working with distribution-list
CSCsu08935	Routing	bgp as-override on 2 byte PE does not overwrite AS 23456 properly
CSCsu32217	Routing	Redistribution from BGP to OSPF vrf fails for high metric prefixes
CSCsu39689	Routing	crash @ipv6_nd_prefix_delete_by_handle with rip 6pe_scaling_performance

Identifier	Technology	Description
CSCsu42077	Routing	next entries didnt function after added new entry on ACL
CSCsu53624	Routing	bgp multicast shows unicast information in show ipv6 protocol
CSCsu62356	Routing	RIPNG 'last gasp' message not seen on Interface down in some IOS branch
CSCsu63996	Routing	OSPF flaps after SSO switchover causes traffic loss after SSO switchover
CSCsu69767	Routing	Global to VRF and VPN import route-map depends on configuration order
CSCsu76993	Routing	EIGRP:Routes not tagged with match source redistribution-source
CSCsu79988	Routing	4BASN: BGP path/bestpath memory usage is 14% higher
CSCsu86338	Routing	<cr> missing in ip extcommunity-list command
CSCsu97177	Routing	switch crashes querying (old) IPv6 MIB
CSCsu97834	Routing	On module reset, 'ip route' statement loses 'name' argument
CSCsv00604	Routing	IPv6 host with static default route still learns ND default router
CSCsv01474	Routing	'ip rip advertise' command lost after interface flap/clear ip route
CSCsv05009	Routing	%OSPF-4-FLOOD_WAR: error during heavy flaps for type-5 and type-7 LSAs
CSCsv17933	Routing	Static route in VRF is not redistributed by RIP after link flap
CSCsv27607	Routing	BGP: Outbound route-map updating withdraw only one member
CSCsv51298	Routing	c3825 faces chunk memory leak @ bgp_do_ipv4redist_callback
CSCsv59334	Routing	Connected nets redistribr from eigrpTObgp when no net 0 is set under eigrp
CSCsv62777	Routing	High CPU process caused by stucked VTY line
CSCsv85052	Routing	Crash observed when "ispf" is issued in vty with ip routing disabled
CSCsv89643	Routing	OSPF: MAC address of next hop unresolved on ptp eth by adjacency bringup
CSCsv97472	Routing	CSCso62166_dcq_issue_rn_walktree_timed_locking is changed
CSCsw24286	Routing	TE tunnel bandwidth command breaks isis topology
CSCsw24611	Routing	Router crashes at bgp_set_path_attr
CSCsw24826	Routing	OSPF crash during type-9 maxage
CSCsw30941	Routing	ospfNbrStateChange trap sent by non-DR
CSCsw65441	Routing	ARP packets drops due to excessive ARP requests sourced from SVI
CSCsw65933	Routing	Prefix not learned from PE to CE
CSCsw79397	Routing	Device crashing at bgp_command_af_specific
CSCsw89080	Routing	changed L1 area address not updated in L2 lsp with multi-area config
CSCsw92379	Routing	Crash seen on releasing snooping bindings after LC OIR
CSCsx11776	Routing	show ip bgp version 1 causes router crash
CSCsx15841	Routing	aggregate-address does not NVGEN upon switchover on cat6k
CSCsx17446	Routing	Tunnel route and a non-tunnel (IGP) route with same metric (TE metric)
CSCsx18270	Routing	EIGRP: tags from version 2 peers are not displayed in topology table
CSCea11368	Security	CRL fetch using ldap fails if vrf configured in trustpoint
CSCeg49153	Security	PKI: crl checking takes too long to timeout if the server is down
CSCeh75136	Security	TACACS+ rem_addr field empty after first SSH authen attempt fails

Identifier	Technology	Description
CSCsc91824	Security	SSH from router disconnects vty session if there is no matching cipher
CSCse80892	Security	isakmp-profiles and VRFs: IPSEC sa fails to come up for the below config
CSCsk22496	Security	Router crashes @ssh_command when remove crypto key
CSCsm70719	Security	Memory allocated @ add_new_cdp_to_list Leaked
CSCsq51052	Security	SSH server on IOS reporting bogus protocol version
CSCsu54801	Security	Cannot get s/w adjacency header information on DFC for IPv6 in v6 tunnel
CSCsu90280	Security	NHRP IPv6 registration not working
CSCsv86113	Security	On modular IOS, SSH on VRF int is allowed irrespective of vrf-also key
CSCeg80842	Unknown	PA-MC-8TE1 controller stuck (similar to CSCdz72292)
CSCek70131	Unknown	SIP1 crash at vip_mlp_fastsend with HEARTBEAT error for mlppp qos
CSCek71010	Unknown	TB seen at bgp_oer_notify_pep bgp_oer_remove_path bgp_bestpath_old
CSCek77516	Unknown	PPC:SUP720:4k:SW-EoMPLS:%SW_MGR-SP-3-CM_ERROR_CLASS: Connection Mana
CSCse82480	Unknown	ip vrf receive cmd adds connected routes to VRF even interface down
CSCsf08092	Unknown	Deprecate tracking 'rtr' cmd in favour of 'ip sla' cmd
CSCsg83756	Unknown	SPA-8XCHT1/E1 after Reload C/A LED green even if no cable plugged
CSCsg87290	Unknown	SIP1-ChOC3: Extra path flap is observed on ChOC3 SPA interfaces
CSCsh22225	Unknown	CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR:
CSCsh54232	Unknown	Remove external loop option for nx1GE SPAs
CSCsi66012	Unknown	2 garbage values in show module csm x ft details
CSCsi78584	Unknown	T3/E3 SPA:Line protocol is not coming up with E3 and framing bypass
CSCsj19308	Unknown	PE and CE ping fails over multilink ppp bundle. .
CSCsj80015	Unknown	Enhance logic for accurately detecting Semaphore Hog
CSCsk30196	Unknown	BADBUFFER error at pak_copy_contiguous_to_contiguous
CSCsk98751	Unknown	Router crash after issue command "mpls tra backup-path tunnel"
CSCsl44170	Unknown	LI tapped PPPoE LCP/PPP control packets originated from router are bogus
CSCsl46159	Unknown	Cost Minimization Feature keeps moving the traffic and doesn't stabilize
CSCsl99156	Unknown	No_Global bit out of syn between IPRM and BGP, when label no change
CSCsm01389	Unknown	Crash after clearing Auto-tunnel backup
CSCsm44147	Unknown	SSO failure due to mismatched command on SRB1
CSCsm72121	Unknown	W2: bad cookie magic was detected after SSO switchover with sh vtp count
CSCsm74948	Unknown	mVPN RP does not send join to directed connected neighbor PE
CSCsm75818	Unknown	Wrong OIL for data-mdt mroutes: multicast traffic loss
CSCsm76792	Unknown	PM HA bulk sync posting RF_DONE before bulk sync has finished
CSCsm83256	Unknown	IDS2 Data port operation status not OK after boot OR SSO
CSCsm96309	Unknown	OIR-SP-4-WARN message displayed when PS1 or FAN removed
CSCso29141	Unknown	DFC installs drop index for MAC-address
CSCso35659	Unknown	L3 traffic rate limited after adding and removing Xcon to a SVI

Identifier	Technology	Description
CSCso36570	Unknown	es20 layer 2 interfaces can be configured with MTU other than jumbomtu
CSCso48665	Unknown	vlan filter can't be removed totally
CSCso51749	Unknown	GRE: policing functionality not working with multicast traffic
CSCso59242	Unknown	sierra: show mem detailed all stat is truncated.
CSCso59974	Unknown	BGP session goes idle after SSO switchover
CSCso88183	Unknown	DOME:dumper.proc crashes on dome when another process crashes
CSCsq07729	Unknown	VSS: flowcontrol incompatible msg when standby switch port add in bundle
CSCsq25028	Unknown	Malloc errors with IPC buffers on a Flex-wan
CSCsq31605	Unknown	auth_mgr:session stuck in Running state if clear auth issued during auth
CSCsq48025	Unknown	DACL is not getting programmed untill next Probe interval.
CSCsq56941	Unknown	6500 - Static MAC cleared from port-channel member ints after reload
CSCsq73122	Unknown	Proxy-ARP returns BIA instead of VMAC with LAM
CSCsq82865	Unknown	Parsing error reading route-map match statements if longer than 254 chrs
CSCsq87496	Unknown	"%OIR-6-INSCARD" syslog not being send from the device
CSCsq96144	Unknown	Netflow v9 Exported Data issue in case of ECMP
CSCsr04190	Unknown	Traceback and standby SUP4 reloads after multiple standby resets
CSCsr09062	Unknown	MLP+QoS - Memory corruption with WRED configured
CSCsr15812	Unknown	Traceback: %SW_MGR-3-CM_ERROR_CLASS: Connection Manager Error: on Congo
CSCsr22282	Unknown	All the trap entries are cleared on any port flap in the same vlan
CSCsr27980	Unknown	%C10K_QOS_GENERAL-3-EREVENT: Error @ ../toaster/c10k_rp/mce_qos.c:mce_qo
CSCsr29559	Unknown	WCCP flap corrupts mcast CEF adjacency
CSCsr37131	Unknown	buginf calls in l2trace when 'debug l2trace' is disabled
CSCsr44036	Unknown	IVFS is not supported, using internal matrix table msgs on router bootup
CSCsr56465	Unknown	With diag Off seeing %CONST_DIAG-SP-3-HM_TEST_FAIL on x6708 LC
CSCsr63098	Unknown	VRF-Aware Smart-Call Home requirement
CSCsr63831	Unknown	show platform hardware capacity fabric - incorrect % and time-SXH3
CSCsr64777	Unknown	EPA crash, Corrupted redzone blk, netflow v5
CSCsr68212	Unknown	MVRF name may get truncated if the VRF name is long
CSCsr88845	Unknown	unicast BootP replies dropped by DHCP snooping
CSCsu01372	Unknown	33SB: Result of boot config command not sync to standby RP after reload
CSCsu04446	Unknown	PfR MC/BR crashes under stress with test traffic
CSCsu05721	Unknown	C2W2: %NTI-SP-3-AGENT_ERR and TB was seen after issu runversion
CSCsu07931	Unknown	cbQosPoliceConformedByte64 counter displays aggregate instead conformed
CSCsu10022	Unknown	L2 traffic is policed when CoPP is enabled
CSCsu10261	Unknown	BFD ISSU peer reload between mcp_dev and sierra image
CSCsu25699	Unknown	OER ICMP Probes using incorrect outbound interface when encrypted
CSCsu36715	Unknown	W2.0 : C2 : ION : Memory Leak in MSDP process

Identifier	Technology	Description
CSCsu36836	Unknown	Conflict when using sockets and files at the same time
CSCsu44534	Unknown	Sup NSF/SSO causes 4 sec traffic loss over EC with uplink ports.
CSCsu45210	Unknown	Upgrade 12.2SXF-> 12.2SXH with Port-Security causes standby boot loop
CSCsu45786	Unknown	Crash on show tcp br after tcp process restart
CSCsu46124	Unknown	SVI ifInMulticastPkts ifOutMulticastPkts are always zero
CSCsu49257	Unknown	Cstn-id timer should be restarted when access-request is seen
CSCsu50611	Unknown	PfR Master Controller crash when shut/no shut
CSCsu67559	Unknown	Copy Run Start does not provide the same functionality as 'wr mem'
CSCsu69660	Unknown	ldcache crashed due to Process Deadlock b/w installer and ldcache proc
CSCsu72026	Unknown	OER MC reports max report limit reach when request all exit links report
CSCsu72496	Unknown	%PM-3-INTERNALERROR: Port Manager Internal Software Error
CSCsu75546	Unknown	C2W21: traffic not span to NAM using span conf mode local-tx source intf
CSCsu77945	Unknown	PfR echo probe shows 0 completes
CSCsu81158	Unknown	Pkt drops on SIP-400 LC due to QoS lock fail for subintfs.
CSCsu81838	Unknown	SA : memory leak @ slb_gtp_echo_response
CSCsu82580	Unknown	6VPE : Traffic dropped under stress configuration with more then 3Kvlan
CSCsu83563	Unknown	MMLS:If rate-lt on when STDBY reloads, doesnt work on swovr:x40/dual RSP
CSCsu84927	Unknown	c2w2:allow DIVC to negotiate red mode when matrix override check is yes
CSCsu85166	Unknown	Crash @ hwidb_get_firstsw after SSO.
CSCsu86524	Unknown	IKMP process leak: check_ipsec_proposal
CSCsu88008	Unknown	c2w2:standby HSRP router crashed @mcast_igmp_process_join
CSCsu88471	Unknown	Err "Insertion of mld_s_g_type in the grp WAVL tree failed" after SSO
CSCsu88557	Unknown	[no] mdix auto" CLI command not present for WS-X6196-RJ21"
CSCsu90369	Unknown	Whitney2: %XDR-DFC4-6-ISSUBADRCVTFM_DUMP Traceback on Switchover
CSCsu91714	Unknown	IGMP-JOIN is lost from SUP to MSFC
CSCsu92395	Unknown	Crash caused by event manager configuration: "action mail"
CSCsu93936	Unknown	PM_SCP-SP-2-LCP_FW_ERR_INFORM for WS-X6548-GETX-45AF
CSCsu95237	Unknown	SSO switchover,clear packet seen on the wire exposing the inner IP pkt
CSCsu95605	Unknown	Route-map with "match route-type local" not functioning properly
CSCsu95662	Unknown	W2: VSL config got error in mixed type with interface range cmd
CSCsu97020	Unknown	policer on flexwan/multilink is dropping even CIR is not reached
CSCsu97418	Unknown	Standby PRE is resetting when doing "write mem"
CSCsv01136	Unknown	Traffic don't get forwarded after iprouting restart then do SSO with PBR
CSCsv04471	Unknown	CDP 2nd port notification traceback
CSCsv07313	Unknown	SPA timeout observed on reload with scalable access-lists config.
CSCsv07858	Unknown	IfIndex for unconfigured VLAN on 7613
CSCsv09249	Unknown	VSS after dual-active recovery MEC on standby chassis UDLD error disable

Identifier	Technology	Description
CSCsv17989	Unknown	interface in SIP200 show "admin down" when it is physical down
CSCsv18681	Unknown	CLI "sh int transceiver properties switch 1" also display switch 2 ports
CSCsv20339	Unknown	MN history table is flooded with multiple (~500) add/delete entries
CSCsv20920	Unknown	telnet from a GRE tunnel to real address for DNS vserver fails
CSCsv21612	Unknown	High CPU on SP due to PM Callback process with VTP pruning enabled
CSCsv21770	Unknown	PAC re-provisioning fails, AAA generates endless number of Prov Requests
CSCsv22779	Unknown	VRF-PBR: Packets dropped with reflexive acl
CSCsv22913	Unknown	igmp snooping querier disabled when static mrouter port is configured
CSCsv24742	Unknown	PfR exit link is OOP when interface counter wraps
CSCsv28564	Unknown	Policy Base Forwarding marks the packets to cos5 on VSS
CSCsv30307	Unknown	ISSU is broken because of CSCsg52337 commit in SRC
CSCsv30679	Unknown	Sup detetes Vlan from Sup IDSM Config on startup / failover
CSCsv32101	Unknown	QoS: memory corruption traceback when using access-list with time range
CSCsv34159	Unknown	Access control based on EAP, not on Radius type, in conflicting messages
CSCsv36306	Unknown	BFD: Removing BGP on the router makes the neigh router crash
CSCsv36698	Unknown	IPC Open Port Errors observed on 7600-SSC-400/VPN-SPA
CSCsv36892	Unknown	New CLI goto tcsh if previous CLI with tcsh terminated abnormally
CSCsv37543	Unknown	GRE/IPsec misconfig is only resovled through module or chassis reload
CSCsv38928	Unknown	IGMP Snooping does not send out Global query on 2nd TCN < 35 seconds
CSCsv39228	Unknown	VSS-The system didn't display SN of SFP correctly
CSCsv39496	Unknown	TB@rfsc_issu_negotiate_and_open_server_port on RPR upgarde from W1 to W2
CSCsv40523	Unknown	WISM: Gig interfaces show as unknown(4)
CSCsv40770	Unknown	%ICC_ISSU_NEGO-SP-3-OPEN_PORT_RELIABLE: Can't open reliable port
CSCsv40974	Unknown	"wism mod <mod> controller <l
CSCsv43991	Unknown	FWSM's internal portchannel on the cat6k side goes down after upgrading
CSCsv44923	Unknown	MAC move behind phone leads to lost connectivity with MAB
CSCsv52426	Unknown	GRE Recirc index is 0x0 in adjacency hence encap operation fails on DFC
CSCsv52941	Unknown	EEM24: snmp-notif ed policies not triggered after removal and add
CSCsv53392	Unknown	"Mls qos trust device cisco-phone" causes instabilty on the system
CSCsv56974	Unknown	OIR WAN Module w/VPN/SPA interfaces. does not take down Vlan/Tunnels
CSCsv57235	Unknown	duplex is changing automatically on WS-X6148-RJ-45
CSCsv57305	Unknown	VSS: software forced reload with 100Mbps SFPs in supervisor uplink ports
CSCsv58013	Unknown	MLPPP policy-map could not be deleted.
CSCsv58279	Unknown	Reload due to Address Error with multicast configuration
CSCsv60643	Unknown	sup4 when toggled 10g mode the config is not synced to standby sup
CSCsv63799	Unknown	PfR MC/BR bus error crash in ip fast flow
CSCsv64079	Unknown	SXF7: Patching fails with WiSM Card on Cat6500

Identifier	Technology	Description
CSCsv66513	Unknown	PBR controlled application not in DEFAULT with exit interface shutdown.
CSCsv66706	Unknown	IDSMP port-channel Allowed-Vlan statements lost on reload
CSCsv66827	Unknown	Clearing the SSH session from a different vty session crashes the box.
CSCsv73299	Unknown	L2 multicast forwarding broken with DHCP snooping & TTL rate-limiter
CSCsv73721	Unknown	ISSU ERP tracebacks on active RP during router bootup
CSCsv76509	Unknown	Cat6k/MSTP in compat mode BPDUs sent in VLAN1 regardless of config
CSCsv80075	Unknown	Pre-release Feature Card VS-F6K-PFC3C (227)
CSCsv86288	Unknown	Sending a hello response with a session-id element causes a crash
CSCsv91278	Unknown	MPLS interface wedged following upgrade to SXI
CSCsv92872	Unknown	10GE link on Sup720-10GE takes more than 30sec to go down during crash
CSCsw17478	Unknown	PVT HOSTS- ports programmed with incorrect rdt index upon bootup
CSCsw18793	Unknown	VRF-PBR: TCAM adjacency not programmed with multiset policy order after
CSCsw32280	Unknown	Diag error on WS-X6148A-45AF card asic with Traffic
CSCsw41168	Unknown	%ALIGN-3-SPURIOUS at sm_get_portEntPhyIndex
CSCsw41439	Unknown	W21,VSL,SNMP,cvsCoreSwitchPreempt,cvsCoreSwitchPriority not SSO aware.
CSCsw41706	Unknown	router reload when registering EEM service diag script
CSCsw43953	Unknown	Card not identified SIP Is OIR'd during Standby SUP bootup
CSCsw45396	Unknown	when STP recovered in uplinkfast,no sent dummy multicast packets
CSCsw48181	Unknown	Unknown Unicast is dropped on Shut/no Shut of a VLAN
CSCsw48824	Unknown	Switchport Block Unicast - prevents RTP on same VLAN
CSCsw51395	Unknown	Proper handling is required for Mac-Filter with Port-security
CSCsw52819	Unknown	Kernel dumper needs a few enhancements.
CSCsw53362	Unknown	c2w2b: Device crashes with NAT stress test
CSCsw73302	Unknown	memory leak in qm_increment_ag_policer_usage on standby-rp
CSCsw75589	Unknown	ip flow-cache mpls label-positions can lead to bus error under load
CSCsw78806	Unknown	Router getting crashed at lat_int_command
CSCsw82732	Unknown	VPN-SPA internal vlan interface wedged in SXH4
CSCsw87352	Unknown	6748's port can not forwarding traffic - port src index wrong
CSCsw87399	Unknown	auth_mgr: crash @ eap_show_context when doing show eap session
CSCsw87563	Unknown	packets with multicast mac and unicast ip are software routed by cat6500
CSCsw90798	Unknown	Bus error crash after configuring vlan name change
CSCsw93969	Unknown	%ICC_ISSU_NEGO-SP-3-OPEN_PORT_RELIABLE: Can't open reliable port
CSCsw98231	Unknown	SDBY stuck @ CEF RRP RF Client(5025) after ISSU RV
CSCsx06578	Unknown	SIERRA:MAGO switch got crashed after reload with SIERRA_INTEG_090106
CSCsx09273	Unknown	WEBAUTH(IP adm) is not INITiating if IPDT entry already exists.
CSCsx10011	Unknown	VSS: IO memory leak from pre_process_vsibc_vsda_pak
CSCsx15038	Unknown	NVgen issue with violate-action commands under policy-map class

Identifier	Technology	Description
CSCsx15138	Unknown	Crash at qos_feature_get_fo
CSCsx16206	Unknown	Traffic loss issue from SFM capable modules to other device through DEC
CSCsx26114	Unknown	IOS tagging certain commands as level 1 in config mode
CSCsx28532	Unknown	VPN SPA freezes when ip mtu changed on tunnel interface
CSCsx29645	Unknown	IPv6 Multicast traffic can not converge after SSO
CSCsx32416	Unknown	BFD session flaps during router/LC bootup after reload
CSCsx34570	Unknown	VSS:remove port-channel from interface causes other members to go down
CSCsx37615	Unknown	VSS: rem comm standby-rp sh plat hardware capacity may reset switch
CSCsx48991	Unknown	Disable LI CLI
CSCsx49718	Unknown	Auth Man Single-host-Guest VLAN doesn't trigger reauth on EAPOL start
CSCsx53257	Unknown	Minor diag error - TestNetflowShortcut failed
CSCsx55543	Unknown	auth_mgr: with vlan assignment reauthentication takes 30sec to start
CSCsx58786	Unknown	Router crash @ routemap_track_nexthop
CSCsx62912	Unknown	W2: update the PM switch vp limits for MST, PVST and Rapid-PVST
CSCsx64668	Unknown	Config change on port of WS-X6148-FE-SFP will move other ports to down
CSCsx76308	Unknown	HA client crashing attempting to free unassigned memory
CSCsy03141	Unknown	Copy of CSCsx06578 - to address the original hang problem in Mago
CSCsv04674	VPDN	Random Vector AVP in ICCN isn't marked as Mandatory
CSCsv04733	VPDN	A LAC might diconnect a tunnel by StopCCN for tunnel-passwords > 31 char
CSCsv68584	VPDN	LAC crashed @sw_mgr_cm_inQ_handler/free
CSCsw78939	VPDN	PDSN(LAC) fails to bring up the VPDN calls after stressing for long time
CSCso62193	WAN	Standby resets due to parser return error "no frame-relay vc-bundle"
CSCsq47900	WAN	OIR operation on POS interfaces with APS result in ALIGN error

Caveats Resolved in Release 12.2(33)SXI

Resolved AAA Caveats

- [CSCsa43465](#)—Resolved in 12.2(33)SXI

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

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

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

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

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

Resolved Infrastructure Caveats

- [CSCse85652](#)—Resolved in 12.2(33)SXI

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/netmgmt/configuration/guide/nm_http_web_ps6350_TSD_Products_Configuration_Guide_Chapter.html

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

- **CSCsr72301**—Resolved in 12.2(33)SXI

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/warp/public/707/cisco-sr-20090114-http.shtml>

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(33)SXI

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/warp/public/707/cisco-sa-20090325-udp.shtml>

- **CSCsm45390**—Resolved in 12.2(33)SXI

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

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

Workaround: None.

- **CSCsm27071**—Resolved in 12.2(33)SXI

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/warp/public/707/cisco-sa-20090325-ip.shtml>

- [CSCek52673](#)—Resolved in 12.2(33)SXI

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

Workaround: None

Resolved Routing Caveats

- [CSCso64422](#)—Resolved in 12.2(33)SXI

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

Workaround: Only allow EIGRP packet from trusted neighbours.

- [CSCsm93548](#)—Resolved in 12.2(33)SXI

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

Workaround: Only allow EIGRP packet from trusted neighbours.

Resolved Security Caveats

- [CSCsi17158](#)—Resolved in 12.2(33)SXI

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

- [CSCsj85065](#)—Resolved in 12.2(33)SXI

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>.

Resolved Unknown Caveats

- [CSCsk93241](#)—Resolved in 12.2(33)SXI

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

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml>

- [CSCsg35077](#)—Resolved in 12.2(33)SXI

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(33)SXI

Identifier	Technology	Description
CSCdu79630	AAA	Username on vty not displayed if accounting is not configured
CSCed69872	AAA	TACACS+ directed request leaves hanging TCP session
CSCed93927	AAA	%RADIUS-3-NOSERVERS: No Radius hosts configured although AAA is up
CSCee42617	AAA	Remove/Re-enter global radius server command causes auth. failure
CSCee66606	AAA	per-group deadtime is nvgen as 60x user input

Identifier	Technology	Description
CSCef27578	AAA	The router crashes when test aaa stop CLI is issued
CSCef97900	AAA	AAAA-3-DROPACCTLOWMEM warning message somewhat misleading
CSCeh84727	AAA	LPIP ARP entries become incompleted after a while
CSCek32177	AAA	TPLUS: Failed to decode AV addr=255.255.255.254
CSCek77360	AAA	Tacacs authentication failed for tcb_clear with pppoe
CSCir01788	AAA	Unable to configure ip tacacs source-interface globally
CSCsc98046	AAA	TACACS Accounting isn't sending stop time in the stop packet.
CSCsd48175	AAA	AAA/TACACS not failing over to second server
CSCse02550	AAA	ip radius source-interface not used in combination with vrf
CSCsg14301	AAA	AAA/TACACS spurious memory accesses in tplus_handle_req_timeout
CSCsg18288	AAA	Enable authentication ignores Tacacs+ configuration in rare situation
CSCsg48725	AAA	TLB exception in tacacs_plus_get_conn
CSCsg82766	AAA	Unexpected crash due to bus error in Cisco 3825
CSCsh23142	AAA	aaa local authentication not happening for authproxy .
CSCsh46990	AAA	Console hangs with enable/line as aaa fall-back methods
CSCsh72214	AAA	Login local denies valid authentication
CSCsi63598	AAA	Bus error crash in tplus_server_key during TACACS+ configuration
CSCsi99473	AAA	TACACS authorization fails with 'request for nonexistent server' msg .
CSCsj90016	AAA	AAA ISSU Client support.
CSCsk06660	AAA	Radius error in AAA blocking mode
CSCsl29214	AAA	AAA server change leads to bus error crash after "show run" is issued
CSCsl47365	AAA	TACACS+ authorization should ignore unknown attribute
CSCsl57645	AAA	tacacs-server directed-request fails for enable authentication on 6500
CSCsl97384	AAA	Command 'show aaa user all' triggers IOS reload due to Bus Error
CSCsm84915	AAA	Nas-port-type is missing in Access-request
CSCso25507	AAA	Modem call with Tacacs failed @ Fail to set vrf socket option
CSCso95426	AAA	Exposure of Radius-Keys in debugs.
CSCsq98160	AAA	No communication between SW and AAA with IPBase image
CSCsr17680	AAA	test aaa group server request failing over
CSCsr26098	AAA	SSH/Telnet failed with IPBase image on Sup32 with AAA server
CSCsi91649	Access	Input packets not cef switched
CSCsj88665	Access	Bus error with PA-MC-2T3+ when deleting channel-group
CSCsl41784	Access	ION: ARP Input memory leak with "mobile ip arp"
CSCeg52354	ATM	Memory leak at pvc_d_enqEvent
CSCei33231	ATM	ATM PVC bundle protected group test failed with bumping exhausted
CSCek40952	ATM	OIR of PA-A3-OC3MM= generates tracebacks on OIR
CSCek74474	ATM	no/default proto ip inarp cmd ineffective until ATM VC bounced.

Identifier	Technology	Description
CSCsd84347	ATM	PVC stops sending OAM loopback if AIS/RDI received
CSCse87275	ATM	CEoP: shaping configuration does not work .
CSCsh34529	ATM	autobahn76: ATM interface config lost on standby RP
CSCsh98378	ATM	Router crashes at atm_create_vp_db
CSCsi72854	ATM	Inconsistent IMA CLI after router reload .
CSCsj71998	ATM	ATM interface lost its ipaddress after graceful stop/start of interface
CSCsj84931	ATM	CEOP: after OIR with atm local switching and ima, router crashes
CSCsk01927	ATM	oam-ac emulation, vc stays UP after shutting CE ATM interface down.
CSCsk72676	ATM	Pvc not coming up after removing vc-class from it
CSCsu03608	ATM	7500 crash at loki_send_phy_config_ll when bringup IMA interface
CSCsj09149	Content	WCCP: no redirection following change in configuration
CSCsl29993	Content	WCCP Should Mark Client 'NOT Usable' with Missing L2 Adjacency
CSCsl65335	Content	WCCP: reload following ACL update
CSCsm12247	Content	WCCP: hash assignment may be lost after service group change
CSCsm32473	Content	WCCP: system reload with path splitting and output redirection
CSCsm35350	Content	WCCP GRE return breaks IPsec traffic AND/OR creates phantom packet count
CSCsm53427	Content	WCCP: multicast + appliance shutdown leads to high CPU
CSCsq31981	Content	WCCP: redirection does not work with CEF and ip accounting
CSCsq64362	Content	running config for wccp has missing and duplicated services
CSCed33145	Infrastructure	line vty exec-timeout not working properly, def causes spur mem acc
CSCeg16786	Infrastructure	Device not loading with the image and SP crashes
CSCeg69540	Infrastructure	10k crash due to a bus error
CSCeh51638	Infrastructure	Calling-Station-Id not send anymore for http admin
CSCeh54177	Infrastructure	Mismatch of the index of ciscoMemoryPoolFree OID to its own value
CSCei86912	Infrastructure	Router reloads unexpectedly while issuing GD commands
CSCek35108	Infrastructure	Rommon truncates boot string to 64 characters
CSCek46087	Infrastructure	IPC ack_pending not updated correctly
CSCek58956	Infrastructure	Need process_ok_to_reschedule check in process_may_suspend
CSCek62770	Infrastructure	bundles need to include CW_ strings
CSCek78644	Infrastructure	SNMP replies do not source VRF interfacaes
CSCir01027	Infrastructure	snmp over ipv6 is broken for cat6k_hi_fi
CSCsa53739	Infrastructure	CISCO-CONFIG-COPY-MIB ccCopyProtocol does not work in 12.0(30)S on 7200
CSCsa57468	Infrastructure	rttmon-mib does not return getnext value when queried via snmp
CSCsa97971	Infrastructure	IOS SLB TCP probe state toggles
CSCsb06920	Infrastructure	SYS-3-MGDTIMER: Running timer -Process= SAA Event Processor
CSCsb98906	Infrastructure	Memory Leak with bgp regexp deterministic configuration
CSCsd23127	Infrastructure	IPC-SP-2-LOCK IPC-SP-2-UNLOCK followed by tracebacks on SSO s/w

Identifier	Technology	Description
CSCsd37499	Infrastructure	%IFS-3-FSMAX: Failed to add ?, maximum filesystems 64 msg with Traceback
CSCsd55059	Infrastructure	polling CISCO-FLASH-MIB slows down GSR
CSCsd81275	Infrastructure	Syncing the private configuration to the standby Router FAILED
CSCse07265	Infrastructure	No syslog message generated for IP SLA timeout condition
CSCse40379	Infrastructure	IP SLA: Increasing the request-data-size via CLI crashes the device.
CSCse40401	Infrastructure	IP SLA Traceback: %SCHED-3-STUCKMTMR: Sleep with expired managed timer
CSCse66080	Infrastructure	Memory leak from MallocLite @ physical_buffer_to_malloc()
CSCse72476	Infrastructure	HTTP authen fails using Local followed by Radius Authorization for EXEC
CSCsg35587	Infrastructure	Latest RTT for jitter calculated as RTT average with timeouts as zero
CSCsg82453	Infrastructure	Syslog over TCP: should try to reconnect to the syslog server
CSCsg99677	Infrastructure	Crashinfo files saved with wrong name CRASHI~1
CSCsh40811	Infrastructure	stbySP crashes with ActNotResp during FSU from SRA to SRB
CSCsh45091	Infrastructure	Port fix for CSCed94684 for ws-c3750-24p
CSCsh47251	Infrastructure	3700 crashes as soon as loading image
CSCsh63508	Infrastructure	disk0:/sys/cpmibit/base is busy, try again later msg on stby SP on SSO.
CSCsh66245	Infrastructure	Lowest memory is too low after reload on Cisco 10000
CSCsh81291	Infrastructure	Exodus Mayflower C10K ISSU fails at loadversion
CSCsh85522	Infrastructure	SNMP-Sever user CLI throwing trace back messages
CSCsh96179	Infrastructure	IPSLA pathEcho probe doesn't complete for all hops
CSCsi22502	Infrastructure	installer imf.tar file not being zipped creates uninstallable image
CSCsi43776	Infrastructure	IPC: Invalid process name pointer; follow-up to CSCsh76558 .
CSCsi49008	Infrastructure	SNMP sends responses to 0.0.0.0 when VRFs configured
CSCsi49890	Infrastructure	SNMP: ciscoFlashFileEntry gives no index on disc with hidden files
CSCsi76486	Infrastructure	ip http source-interface command ignores VRF
CSCsi88974	Infrastructure	LI: Malloc failure on setting MD src interface as Loopback interface
CSCsj06593	Infrastructure	CPU hog msgs for RFSS worker process and Async write process
CSCsj12867	Infrastructure	Restart occurs after executing write memory command
CSCsj27963	Infrastructure	Need graceful handling of full nvram
CSCsj52693	Infrastructure	ospf neighbor flap with fast hellos and 16 neighbors
CSCsj52992	Infrastructure	CPU hogs when configuring snmp-server host
CSCsj54596	Infrastructure	logging userinfo command no longer accepted
CSCsj67434	Infrastructure	The CLI: 'parser config cache interface' does not work
CSCsj80951	Infrastructure	*Neutrino* proc reported memory Freed/Holding is incorrect
CSCsj83417	Infrastructure	BOOM: addto_mempool_pc_array() message seen with show memory command
CSCsk03336	Infrastructure	CEF process is unable to handle timer events when there are lot of Event
CSCsk06492	Infrastructure	snmp-server drop vrf-traffic implementation in 12.2 SRB train
CSCsk09735	Infrastructure	Router crashed on mkdir with 3dots,reload and show file system .

Identifier	Technology	Description
CSCsk10412	Infrastructure	Config Sync: Bulk-sync failure due to BEM mismatch -parser view li-view
CSCsk13725	Infrastructure	GSR: rttmon-mib does not return getnext value when queried via snmp
CSCsk27147	Infrastructure	SNMP stops responding while polling from CISCO-MEMORYPOOL-MIB
CSCsk37278	Infrastructure	BFD clients flaps when boot string is removed from "show running" .
CSCsk41686	Infrastructure	PARSER-3-CFGLOG_NOMEM: constanlty in log
CSCsk42373	Infrastructure	Memory leak in ctid_set_changetime function
CSCsk45467	Infrastructure	Log overruns leaks buffers
CSCsk70446	Infrastructure	NRT: tracebacks @ data_inconsistency_error - 7200 for HTTP config .
CSCsk71670	Infrastructure	New active RP crashed at ipc_issu_process_timer_event()
CSCsk75147	Infrastructure	CBS3120 LightSabre switch crashes during license install while reloading
CSCsk75310	Infrastructure	UDP Echo: control message not sent out of correct interface.
CSCsk82972	Infrastructure	copy running-config to startup-config does not work as expected
CSCsk91176	Infrastructure	PXF crash causes IPC timeout to all linecards in the chassis
CSCsk99687	Infrastructure	crash seen during ISSU runversion in ipc_open_port
CSCsl01595	Infrastructure	c7600: Disable port-channel creation using 'interface range' command.
CSCsl16001	Infrastructure	Booting from dosfs monlib is slow - needs performance improvement
CSCsl23306	Infrastructure	RP crashes at ipc_check_flow_control with sso .
CSCsl33908	Infrastructure	show ver truncates system's running image name to 64 chars
CSCsl39860	Infrastructure	Stdby Sup keeps rebooting w/SSO after running some SNMP CLI cmds
CSCsl52220	Infrastructure	MF: "[no] snmp ifindex persist" enables persistence on other intf.
CSCsl53110	Infrastructure	VSS: Stby rp crashes on boot
CSCsl58963	Infrastructure	Manual OIR of pcmcia flash card crashes dosfs proc in Sup720
CSCsl59629	Infrastructure	Infinite Loop at ciscoFlashFileSize while doing snmpwalk
CSCsl60092	Infrastructure	Active SP crashed @ipc_fragment_cleanup with VSL shut/no shut test
CSCsl64869	Infrastructure	IP SLA: NumOfRTT & PacketLateArrival incremented for same packet
CSCsl70722	Infrastructure	Router crash polling rttmon mib with active IP SLA probes
CSCsl97612	Infrastructure	rttMonStats tables returns NULL values for snmpget
CSCsm01126	Infrastructure	PRE-B crashes while in progress to standby cold-config
CSCsm01334	Infrastructure	%failed to configure the mapping messages are seen on standby SUP.
CSCsm14366	Infrastructure	Empty crash file generated on wan module crash at boot-up
CSCsm27493	Infrastructure	procmib_server port has to send rpc reply only for RPC requests.
CSCsm32392	Infrastructure	memory corruption crash at nv_ifs_open and nv_ifs_close
CSCsm47417	Infrastructure	W2:setting ceExtSysBootImageList cause "wr mem" not working correctly
CSCsm49218	Infrastructure	Missing traceback for jump to zero exceptions
CSCsm77199	Infrastructure	DATACORRUPTION-1-DATAINCONSISTENCY HTTP_FIND_FLASH_FILE
CSCsm89735	Infrastructure	Router crashes on giving show idb after sessions are down in PPPOE-ipv6
CSCso02960	Infrastructure	%RTT-4-DuplicateEvent causes trackbacks after upgrading to 12.2(33)SXH

Identifier	Technology	Description
CSCso29361	Infrastructure	cfg added under interface range vlan not being added in redundant sup
CSCso38185	Infrastructure	IPSLA not handling invalid timestamp properly
CSCso48834	Infrastructure	ip sla config with udp-jitter probe failed due to no connection
CSCso52837	Infrastructure	Error while copying a file to disk0:
CSCso53866	Infrastructure	Accepting interface range commands with or without whitespace is broken
CSCso57001	Infrastructure	RP & SP crash after link flapping for CFM, IP SLA and EVC config
CSCso66862	Infrastructure	ID Manager incorrectly returns ID contexts that are on the free list
CSCsq03621	Infrastructure	Timestamps in "show rmon events" wrap at 2^32-1 milliseconds (7+ weeks)
CSCsq14340	Infrastructure	Stale "snmp community-map" command found in stand-by running config
CSCsq16325	Infrastructure	Incomplete serial interface command creates interface
CSCsq19159	Infrastructure	RP crashes in chassismib_add_sub_card_entry after linecard reload
CSCsq34676	Infrastructure	Modular IOS: show process cpu sorted triggers unexpected reload
CSCsq35093	Infrastructure	XDR-6-XDRIPCNOTIFY: Message not sent to slot 1/0 (1) because of IPC
CSCsq60922	Infrastructure	Modular IOS:Router crashed with SNMP copy and with format in console
CSCsq64663	Infrastructure	SUP32 crashed after deleting LACP etherchannel
CSCsr06282	Infrastructure	DHCP operation and getmany on ciscoRttMonMIB crashes device
CSCsr09033	Infrastructure	SNMP response contains source ip address as a broadcast ip address
CSCsr17757	Infrastructure	IP SLA: Tail-drop with UDP-jitter test with num packets > 1000.
CSCsr18073	Infrastructure	ipslaEtherJitterLatestSum2PosDS sum differs from show ipsla
CSCsr24171	Infrastructure	snmpEngineTime not SSO aware, snmpFrameworkMIB
CSCsr31518	Infrastructure	copy ftp://username:password failed to pass correct value.
CSCsr64361	Infrastructure	Standby continously resetting due to SNMP RF client notification timeout
CSCsr68545	Infrastructure	Error %DATACORRUPTION-1-DATAINCONSISTENCY when running ipsla with rtt
CSCsr84639	Infrastructure	Standby-RP reload while syncing NOTOFICATION-LOG-MIB data
CSCsr97343	Infrastructure	MSDP peer flaps randomly
CSCsu35597	Infrastructure	Renaming a directory/file throws error message
CSCsu37266	Infrastructure	Modular IOS: tcp.proc terminated due to signal SIGSEGV
CSCsu39152	Infrastructure	%IFMGR-4-NOIFINDEX adding interface Multilink [n]
CSCec51750	IPServices	Router reloads do to bus error. and illegal access to low address
CSCec68752	IPServices	crash due to CPUHOG and block overrun on long nat route name string .
CSCec79570	IPServices	UDP port 1985 opens
CSCeh69721	IPServices	%SCHED-3-CORRUPT:Schedulerevent magic corrupted by TFTP Server
CSCek53084	IPServices	ACL/ATOM client inject between REL4/REL3...2
CSCek63433	IPServices	rp crashed when multiple processes exits with shared sockets
CSCek65374	IPServices	PRE3 startup-config parse failed on post sync4 exodus image
CSCek71379	IPServices	%TCP-2-INVALIDTCB: Invalid TCB pointer:-Process= IP Input
CSCsd66215	IPServices	Arp reply not populating the bridge-table on 7200 router

Identifier	Technology	Description
CSCse01124	IPServices	HSRP groups stuck in Init state if dampening cfgd on certain interfaces
CSCse87499	IPServices	RF client timing out in PLATFORM_SYNC that lead to active reset
CSCsg21394	IPServices	Router reload unexpectedly by malformed DNS response packets
CSCsg49882	IPServices	ip ftp source-interface ip address & interface chang after write mem
CSCsg60447	IPServices	7200: BVI stops receiving CLNS/ISIS packets
CSCsh15817	IPServices	UDP socket events are not received by RTR responder process
CSCsi42225	IPServices	We need improvement for ip igmp limit command
CSCsi42717	IPServices	saa_vrf_test_udpe & saa_vrf_test_itter generate an unexpected error mess
CSCsi45840	IPServices	ARP requests for HSRP virtual IP may fail after switchport cmd is used .
CSCsi66366	IPServices	All transport protocols are displayed in running config for VTY
CSCsi66859	IPServices	NSE-100: Router Crash when we send traffic with bridge-group config
CSCsi78892	IPServices	Configuring bridge-group makes CPUHOG message.
CSCsi84742	IPServices	DHCPv6 relay agent can't remove route when RELEASE lease time in nonzero
CSCsj29841	IPServices	Port forwarding breaks NAT-overload on a 6509
CSCsj41479	IPServices	DHCP Services should not be enabled by default in IOS
CSCsj67110	IPServices	HSRP: Stacklow message when unconfiguring interface
CSCsj83854	IPServices	Incorrect static nat entries programmed in nat table
CSCsj93195	IPServices	RP crashes at ipv4fib_les_switch_wrapper on configuring crypto map
CSCsk02920	IPServices	TCP TSecr value invalid - not zero and not last TSval from partner
CSCsk06539	IPServices	bus error while unconfiguring static SSM mappings via TFTP .
CSCsk16821	IPServices	DHCP does not NAK after DHCPREQUEST from unknown client .
CSCsk23972	IPServices	Telnet failed with "No wild listener" error
CSCsk38763	IPServices	Dhcp snooping Ftp'ing of database is failing
CSCsk39022	IPServices	Modular IOS: ip directed-broadcast not working
CSCsk39926	IPServices	Unable to route local FTP traffic over VRF with IOS image
CSCsk47888	IPServices	SRB2:standby keeps reloading due to Bulk-sync failure on PRC mismatch .
CSCsk68320	IPServices	Reload on configuring "no ip routing" with MSDP configured
CSCsk81396	IPServices	NAM process crash in 12.2SXF .
CSCsk83505	IPServices	%L3_MGR-3-REQ_SEND:error packet allocation after Remote HL HW reset
CSCsk96976	IPServices	DHCP Option 66 adds more quotation marks around URL after reload .
CSCsl06431	IPServices	Modular IOS: Memory leak in udp.proc
CSCsl10348	IPServices	Crash writing to or from ftp/tftp server in modular IOS
CSCsl22080	IPServices	12.4.15T: WebVPN stops working with TCP connection queue limit reached
CSCsl23788	IPServices	Dlsw+ peer waits in AB_PENDING or WAIT_WR status with modular IOS
CSCsl31074	IPServices	FA4 line protocol goes up and down when no cable is connected with dhcp
CSCsl43580	IPServices	"standby delay minimum" produces incorrect values while configuring
CSCsl51945	IPServices	HSRPv6: Config Sync and stanby resets with standby 1 ipv6 <>

Identifier	Technology	Description
CSCsl51982	IPServices	nat_sanity:Traceroute test from outside to inside fails
CSCsl67168	IPServices	HSRP should output state change log of both Active/Standby<->any
CSCsl72281	IPServices	Interface-index in DHCP binding database changes after router reload
CSCsl74712	IPServices	VRRP: Config Sync: vrrp 1 track 1 decrement 10
CSCsl96370	IPServices	CPU hog msg during interface reset for scaled hsrp config (debug enbld)
CSCsm34361	IPServices	Required ports [TCP] are not shown in nmap package in PC
CSCsm35794	IPServices	Ignoring Coup after changing HSRP active router's priority
CSCsm36745	IPServices	Warning message for DNS-lookup when no DNS server present
CSCsm59037	IPServices	no service dhcp command causes switch to reload
CSCsm70580	IPServices	c2w2:ciscoFtpClientMIB: ftp_fs.proc extra processes can deadlock & crash
CSCsm71240	IPServices	HSRP not replying to ARP after removing and changing hsrp groups
CSCsm79082	IPServices	RP crash at dispatch_thread_pool when restarting tcp.proc
CSCsm87959	IPServices	HSRP IPv6 becomes :: or unknown after changing interface IP addr
CSCsm92206	IPServices	Router crashes when set the range of interfaces to default configs
CSCso04657	IPServices	SSLVPN service stops accepting any new SSLVPN connections
CSCso17473	IPServices	Stby reload continuously with HSRP: Grp 1 RF Encode data descriptor fail
CSCso30669	IPServices	HA-6-INT_SSO_UNAWARE : While enabling VRRP-SSO onboard GE-interface
CSCso68344	IPServices	Switch acting as DHCP server crashes on issuing no service dhcp command.
CSCso74843	IPServices	stuck in ACTIVE-DRAIN state after 1 day of switchovers
CSCso91230	IPServices	%LINK-2-INTVULN: errors with MLPPP and HWIC-4ESW
CSCso97695	IPServices	backout CSCsm88549 and fix CSCsl48943 with proper fix
CSCsq06813	IPServices	DHCPV6:No multiple RELEASE messages seen on client
CSCsq14698	IPServices	crash when using nat with multicast traffic
CSCsq47043	IPServices	Standby crashes when re-configuring "standby <group> ip" command
CSCsq48201	IPServices	c7300:Bridge IRB-Router crash and traffic flow issue
CSCsq60504	IPServices	Modular IOS Sup720: crashed with tcp timeout logs
CSCsq67478	IPServices	SSH session hangs
CSCsq88779	IPServices	Router fails to boot with overlap address
CSCsq90529	IPServices	Issue with active ftp on the SXH1
CSCsq92440	IPServices	Router Crash with igmp static grp classmap for 10k grps on 10 subints
CSCsq97870	IPServices	Router crash with 'show standby' if group deleted from 2nd terminal
CSCsr08771	IPServices	Crash seen @ dhcpcd_pool_nvgen and dhcpcd_copy_bootfile
CSCsr18589	IPServices	Due to SSO of the Backupswitch, VRRP is flapping
CSCsr27287	IPServices	HSRP group get stuck in Init state after changing IP to secondary
CSCsr55990	IPServices	HSRP mac dynamic on routed pseudowire after reload on active router
CSCsr60108	IPServices	standby delay timer range changed from 0-10000 to 0-300
CSCsr96468	IPServices	Standby config accepted even when MAC reservation failed

Identifier	Technology	Description
CSCsu10108	IPServices	TFTP Server function is not working in 7600 router
CSCsu21716	IPServices	No unsolicited igmp report sent for mroute-proxy
CSCsu27843	IPServices	SW crashed when removed "int vl" on which "ipv6 dhcp client pd" enabled
CSCsu56806	IPServices	HSRPv6 configuration reappears after deleting/configuring SVI
CSCsu93374	IPServices	After SSO standby router, client state doesn't follow master group state
CSCsv06608	IPServices	SXP peering between cat6k with password none option is broken
CSCsg87930	LAN	i82543 driver should not increase input queue drop counter
CSCsl54243	LAN	7600 SIP-400 crash after removing sub-ints; lc_deencap_dot1q_vlan
CSCsm02883	LAN	MFR interfaces do not respond to SNMP after OIR
CSCsr76818	LAN	input queue wedge on SP due to VTP packets
CSCsh33167	LegacyProtocols	Dlsw transparent cache holds MAC address for disconnected circuit
CSCsi09051	LegacyProtocols	Spurious Access seen with ipx routing
CSCsk94676	LegacyProtocols	dls with tbridge, COMMON_FIB-4-FIBIDBMISMATCH
CSCsk98507	LegacyProtocols	Device crash@novell_send_gen_rip_query .
CSCso09152	LegacyProtocols	Slow leak in small buffers caused by CLS_CLOSE_STN
CSCeh97382	Management	Device reset when polling IKE/IPSEC MIB
CSCsk38681	Management	VS2: remote registry call messages ~ cdp2.iosproc:1
CSCsk41552	Management	T/B %SCHED-3-THRASHING of cdp2.iosproc process_wait_for_event
CSCsl64470	Management	router reload with cns config notify
CSCsl68464	Management	SNMP walk on .1.3.6.1.2.1.4.20.1.2 causes CPUHOG clearing tcp session
CSCsq52847	Management	Connection establishment failed with the event agent
CSCsq79032	Management	Excessive remote registry invocation on 'waiting_on_switchover' registry
CSCsq79132	Management	Excessive remote registry invocation on 'proto_on_swidb' registry
CSCsq84595	Management	high # of remote reg. invocation (35 rpc/sec) 'get_unidirectional_mode'
CSCsr93672	Management	Native vlan is not getting displayed in "show cdp neighbors" output
CSCsv08562	Management	IPv6 System crash on bootup with config saved,TB @ dispatch_thread_pool
CSCek72661	MPLS	snmp context doesnt work with new VRF definition CLI.
CSCsd80349	MPLS	Rainier:FRR is not successfully triggered on line prot down event on POS
CSCse23302	MPLS	Staled LDP target session not removed after session flapping
CSCsh97826	MPLS	NRT:6VPE:InterAS entry may not gt installed properly when nxthop is IPv4
CSCsj21066	MPLS	6VPE: adding route-target to IPv6 AF causes IPv4 eBGP session to reset
CSCsj34456	MPLS	LDP change by CSCsi69278 causes inconsistent mplsLdpEntityIndex value .
CSCsj50412	MPLS	Improper handling of remote binding wrt route info
CSCsj98922	MPLS	6VPE - per vrf default route handling broken
CSCsk10104	MPLS	NSE-150, MPLS TE tunnel does not come up after sh/nosh core interface
CSCsk15476	MPLS	MPLS-TE auto-tunnel backup cannot protect primary nhop via L1L2 link
CSCsk42307	MPLS	MPLS-TE CBTS: Sending out OSPF hellos over master tunnel .

Identifier	Technology	Description
CSCsk57114	MPLS	CPUHOG process = SNMP ENGINE, PWMIB, GetNext of cpwVcMplsNonTeMappin
CSCsk62514	MPLS	Parsing Configuration takes longer time on SUP720 with SRB image
CSCsl39233	MPLS	eBGP in VRF-lite not working in images without MPLS .
CSCsl90265	MPLS	CBTS member tunnels are not recovered after SSO switchover
CSCsm10306	MPLS	CBTS master down by member path change causes unexpected traffic loss
CSCsm70668	MPLS	OIR over E3:POS impacting complete Traffic with biscuit tunnel
CSCsm86236	MPLS	Standby reload on reconfiguring address-family ipv4 under vrf definition
CSCso07411	MPLS	Config-sync MCL due to ip ospf interface-retry 0 command getting added
CSCso21506	MPLS	Import Map under vrf blocks bgp aggregate prefix
CSCso23419	MPLS	CBTS master tun reported down for 10 sec after member tun comes up
CSCso51637	MPLS	Crash on removing interface auto-template with 300 active tunnels
CSCso53377	MPLS	All TE Lsps does not recover after SSO switchover
CSCsq02201	MPLS	show run vrf does not display static route with track option
CSCsq46044	MPLS	Error MFI_LABEL_BROKER-3-DELETE_MOI_FAIL and LSD_CLIENT-3-PCHUNK2
CSCsq78822	MPLS	Cannot clear specific LDP neighbor, when router-id not in bound address
CSCsq83958	MPLS	6VPE add remove VRFs crash at avl_balance_right avl_delete_recursive
CSCsq91960	MPLS	failed to delete vrf when it is 32 characters long
CSCsq93004	MPLS	Possible memory corruption with TE auto-tunnel primary and subinterface
CSCsr31401	MPLS	mpls-layer tunnel int not deregistered from snmp when tunnel deleted
CSCsr40433	MPLS	mpls te - explicit path with loose nhops - re-optimization failure
CSCsr43164	MPLS	FRR may not become ready after reoptimize backup tunnel
CSCsr50099	MPLS	show ip explicit-paths command incorrectly displays source route type
CSCsu62667	MPLS	LSP ID change after SSO due to failure in signalling recovered LSP
CSCek75931	Multicast	LNS: %SYS-3-CPUHOG When sessions have multicast
CSCsd14706	Multicast	PIMV2 router send PIMV1 RP-reachable messages loading recieve router CPU
CSCsg95192	Multicast	no ip rp-address <ACL name> causes an address error
CSCsg98535	Multicast	IPv6: clear ipv6 pim topology with (S1,G30K) caused watchdog timeout
CSCsi59438	Multicast	ip multicast limit rpf - fails to stop excessive groups from forming
CSCsj88725	Multicast	Wrong (S,G) RPF after route change, no upstream join
CSCsk26429	Multicast	Router configured for IGMP Proxy may not send IGMP Join
CSCsk45472	Multicast	Bootstrap packets from non-RPF neighbour not dropped on MDT Tunnel
CSCsl10316	Multicast	ipv6 pim join-prune-interval 10 sets the interval to 20 seconds .
CSCsl14450	Multicast	Multicast traffic in Tunnel environments may cause router crash
CSCsl20158	Multicast	SNMP:msdpPeer counters should be able to compare with CLI counters.
CSCsl92316	Multicast	LNS: %SYS-3-CPUHOG when clear l2tp tunnel, sessions have multicast
CSCsm02687	Multicast	3725 router is crashing @oce_base_unlock,ipmulticast_les_fastswitch
CSCsm17426	Multicast	RP-bit not cleared on s,g; traffic outage for 4 minutes

Identifier	Technology	Description
CSCsm26466	Multicast	Standby RP goes down with %MCASTRED-3-BULKACKTIME on active
CSCsm44620	Multicast	Shutdown interface present in PIM interface list
CSCsm48322	Multicast	IPv6 Multicast RP ignores embedded RP register messages
CSCsm53766	Multicast	Reload due to Address Error with multicast configuration
CSCsm73602	Multicast	"ip multicast boundary" makes "VTEMPLATE Backgr" consume much CPU usage
CSCsm77608	Multicast	IP Multicast packets are Process switched.
CSCso67195	Multicast	Memory Corruption Crash with PIM and ACL Logging enabled
CSCsq09962	Multicast	7600 : crash at "pim_proxy_empty_rd"
CSCsq14151	Multicast	RPF of (S,G) is set to NULL, When (S, G, R) entry is converted to (S, G)
CSCsq44925	Multicast	CSCsi47802 need to be modified
CSCsr00815	Multicast	IPv6 PIM Assert winner remains in Incoming interface: Null state
CSCsr09312	Multicast	crash when doing mrm stop
CSCsr15478	Multicast	Input Queue Wedging
CSCsr36971	Multicast	Memory Leak @ PIM process
CSCsr49316	Multicast	Crash ipv6_static_route_find after configured & executed show ipv6 rpf x
CSCsr82895	Multicast	watchdog timeout : RP Crash @ igmp_rejoin_groups during RP Switchover
CSCsu02051	Multicast	S,G expiry timer change is not allowed in Whitney1
CSCsu27888	Multicast	igmpv3 reports are getting discarded
CSCsu71983	Multicast	Memory Leak @ PIM process
CSCsu95080	Multicast	mld_processs block forever in the init_process when parsing config
CSCec08614	platform-12000	Incrementing spurious accesses at srpmib_interface_lookup_long_int
CSCse40966	PPP	MLP links down after SSO switchover if aaa new-model cfiged
CSCsi43652	PPP	PPP: ISSU negotiation should be skipped if standby is incompatible
CSCsl27840	PPP	Router may Crash / Hang, Module Reset @ Shut ATM member + MLPOA
CSCsm41129	PPP	SRB3:140DLFI bundles with qos-Flapping, pkts choke RP as RP does fragmt
CSCso28309	PPP	ping fails while testing pppas feature
CSCsq37078	PPP	Input errors incrementing on Multilink 5 in admin down state
CSCsq55691	PPP	DLFIoATM QoS doesn't work after physical interface shut/no shut
CSCef63607	QoS	Crashes seen during boot if ATM WIC is installed & NAT on int config
CSCek52651	QoS	Traffic shaping broken and drop rate counters are junk
CSCek63203	QoS	CEOP:VH:Ctrl+C while display show policy int cause console freeze
CSCek75808	QoS	MF: Crash observed at qos_show_policymap_interface_all
CSCsg18894	QoS	Queue-limit command should be allowed in conjunction with priority
CSCsh67875	QoS	support for multi-line policer broken
CSCsi73132	QoS	Multicast DSCP value not copied to PIM-SM RP-register packet
CSCsj60212	QoS	sip200: Traceback@reg_invoke_qoscli_inform_features with qos config
CSCsk06872	QoS	SIP-600 QoS : Unsupported configuration is accepted

Identifier	Technology	Description
CSCsk63794	QoS	FlexWAN WS-X6582-2PA + T3+ Serial PA may crash/reload
CSCsl62963	QoS	Router Crashes, Reconfigure a Policy -af_police_remove_coloraware
CSCsm00570	QoS	cwpa2 crashes at hqf_cwpa_pak_enqueue_local
CSCsm38142	QoS	7600 L2WAN SYSTEST: Memory leaking fib_rp_process_feature_classify_stats
CSCsm49062	QoS	cwan2: show queueing interface reports double count for wfq drops
CSCsm87634	QoS	Incorrect burst values seen on policy with multiple policers.
CSCsm93513	QoS	QoS: "queue-limit" config not allowed in dual-level priority queuing
CSCso27913	QoS	Router Crashed, Remove / Modify Conform&Exceed Color class - af_policer_
CSCso50587	QoS	FRR protection is failing after no shutdown backup tunnel
CSCso57695	QoS	policy-map add/removal from interface crashes router.
CSCsq37520	QoS	RP crashes when child-policy added to 1000s of targets
CSCsq43678	QoS	Address error on output policing packet that was not classified
CSCsr44492	QoS	To add user-defined classes restriction at proper place
CSCsu03813	QoS	Upgrading from rockies to w2 deletes the police action from pmap
CSCdy87411	Routing	BGP:Need to delete one list of ip extcommunity-list entries
CSCeg25475	Routing	Distribute-list configured in ipv4 acts in vpnv4 address-family
CSCei25699	Routing	cIpAddressIfIndex of CISCO-IETF-IP-MIB returns 0 value.
CSCek36995	Routing	0.0.0.0 default route increasing on rip DB with object tracking
CSCek51676	Routing	boomclone:deleting SVI crash RP and standby does not take over
CSCek55562	Routing	Tracebacks at topo_db_lookup_by_vrfid due to CPUHOG
CSCek68270	Routing	router crashed at eigrp_ipv4_rib_rdbupdate
CSCek78031	Routing	Tunnel VRF:Rx-rate is 0.Traffic does not reach the destination port
CSCsc40107	Routing	command clear ip bgp vrf VRF_Name flap-statistics not working
CSCsc96014	Routing	EIGRP neighbors from primary add space deleted when sec add removed
CSCsd68016	Routing	ip summary-address rip 0.0.0.0 0.0.0.0 sends out default with metric 16
CSCsd98686	Routing	%XDR-6-CLIENTISSUBADTXTFM: Failed to xmit_transform message .
CSCse00039	Routing	ipv4 prefixes not advertised to EBGp peers
CSCse15634	Routing	neighbor default-originate doesn't work in address-family ipv4 multicast
CSCse26506	Routing	PRE2: BGP CPUHOG when OIR ATM interface -- rt_walktree_cond
CSCse47937	Routing	ICMP unreachable sourced by IOS may contain buffer data
CSCse65277	Routing	MU:default isis metric maximum returns parser error
CSCse97209	Routing	Outbound route-map with continue option sets incorrect std communities
CSCse99913	Routing	Implementation of SYSLOG message for peer reset due to lack of UPDATE
CSCsf06946	Routing	Removing loopback interface causes continuous standby RP reloading
CSCsf11076	Routing	Static route to Null0 with net defined in process not added to topology
CSCsg27697	Routing	router rip AF ipv4 causes standby PRE reset continuously due to BEM erro
CSCsg49166	Routing	EIGRP fails to converge with 1100 neighbors on FR point to point PVCs

Identifier	Technology	Description
CSCsg68717	Routing	A weird behavior in maxpath configuration in ebgp+ibgp case
CSCsg80259	Routing	BGP Routes do not re-populate following reload of Secondary Route Reflect
CSCsg90755	Routing	Standby keeps reloading due to PRC mismatch in IPv4 MDT AF config sync
CSCsg92473	Routing	Switch crashes - IPV6 reflexive acl scalability test
CSCsh12493	Routing	BGP overlapping VRF route not installed in RIB after add/del of VRF
CSCsh20497	Routing	EIGRP IPv6 rtr crashes when config eigrp on serial int (3k/4k port)
CSCsh26706	Routing	ab76:ESM2 TB point to fibidb_decode_update&bitlist_validbit after reload
CSCsh34417	Routing	BGP Distance not updated following failover to a path with a greater dis
CSCsh52567	Routing	MF:Switch Asserts when setting the AS-Path with BGP Route-Map Continue
CSCsh54797	Routing	high CPU in collection process after bringing up pppoe sessions twice .
CSCsh56042	Routing	sham-link goes down when TYPE-5 for SL neighbor address is flushed
CSCsh79933	Routing	BFD does not notify EIGRP of subsequent bfd session failures
CSCsh82722	Routing	RIP routes removed from rip db but stuck in vrf routing table
CSCsh82953	Routing	EIGRP pece routes missing extcomm attrs after redistribution to BGP .
CSCsh86480	Routing	NRT: traceback seen bgp_atf_error
CSCsh92749	Routing	ISIS: ADJ del triggers both LSP and SPF
CSCsh96955	Routing	IPv6 routes learned from eBGP multihop neighbor not installed in RIB
CSCsi07687	Routing	Self ping to SVI fails when vlan configs are removed and re-applied.
CSCsi07822	Routing	6VPE:FIB cannot resolve chain on link flap with eBGP MH Ldsharing in VRF
CSCsi12104	Routing	ipv6_nd_timer:After the shutdown of active router int router is crashing
CSCsi14346	Routing	EIGRP: neighbor command missing in VRF.
CSCsi29163	Routing	BGP: Network statement shows different in the configuration
CSCsi34354	Routing	CET: ATfv4: Assertion tracebacks observed
CSCsi51431	Routing	JQL:SIERRA:SP HighCPU/LCboot up fail with largeACL cfg after sw reload
CSCsi53802	Routing	Change in prefix-list used by vrf import/export map not processed by BGP
CSCsi58867	Routing	CPUHOG After show ip route static or show ip route connected
CSCsi68795	Routing	PE wrongly assigns local label to a vpnv4 confederation prefix
CSCsi70484	Routing	OSPF SPF running constantly if LSID conflicts & prefix filter used.
CSCsi83521	Routing	CLI:Router Crashes after executing sequence of permit commands.
CSCsi87894	Routing	RIP advertise default route after 'no default-information originate'
CSCsi97315	Routing	bfd dereg under peer-grp and peer-session broke
CSCsi98730	Routing	CEF/BGP table MPLS label mismatch in IOS 12.4(6)T5
CSCsj03030	Routing	Chunk memory allocated from the chunk batrr_chunks is not freed
CSCsj13911	Routing	Cat3750:EIGRP does not receive reply for query between some Vlan
CSCsj21785	Routing	TE tunnel does not reoptimize after mtu change
CSCsj34688	Routing	AAA: adding static route cfg does not trigger acct msg to tacacs server
CSCsj37111	Routing	IPv4 inconsistencies & %FIB-4-FIBXDRINV upon reset LC

Identifier	Technology	Description
CSCsj39016	Routing	warn_assert failed: ../fib/fib_table.c:2947 tal_tree_get_item_count_nonf
CSCsj39243	Routing	Issues in IPV4 with summary statement after moving interface to vrf
CSCsj40173	Routing	HSRPv2 Ping IPv6 link-local not recognize the source address
CSCsj45837	Routing	BGP with auto-summary stops advertising classful network if subnet flaps
CSCsj48450	Routing	When configured ICMP code 251-255 on ACL, ACL is not properly configured
CSCsj56281	Routing	BGP inherit peer-policy not working after router reload
CSCsj71764	Routing	incorrect ARP resolution when going through MPLS VPN
CSCsj78403	Routing	clear ip bgp causes crash to RR client with conditional route injection
CSCsj89636	Routing	isis convergance time delay with equal paths
CSCsj94697	Routing	Show ip bgp vpnv4 update-group summ causes high cpu
CSCsk04287	Routing	Spurious memory access at 0x9DA3070 reading 0xC
CSCsk14365	Routing	show command to display recently changed bgp prefixes
CSCsk15805	Routing	static route not removed after TE tunnel shut
CSCsk27077	Routing	router crash observed while clearing virtual access interface
CSCsk34344	Routing	Wrong share-count 1:10 via confed-external BGP peers using dmzlink-bw
CSCsk35688	Routing	Aggregate routes not processed if child routes are deleted pre-maturely
CSCsk37659	Routing	Vrf route table does not get updated once pppox sessions are up.
CSCsk38877	Routing	PE_PUNT_UNRECOGNIZED should be an OUTPUT_FEATURE .
CSCsk48525	Routing	Make ipv4fib global feature message ISSU compliant .
CSCsk54092	Routing	Type 3 LSA's not flushed when network command is removed .
CSCsk56663	Routing	BGP RFC3107 Withdrawn route should have label 0x800000 and had 800001 .
CSCsk63429	Routing	SRB2: High CPU utilization due to MPLS IPRM process after linecard reset
CSCsk65460	Routing	MVPN: mcast-FS fails on decapPE
CSCsk71117	Routing	Traceback with %XDR-6-XDRDISABLEREQUEST: after loadversion
CSCsk78854	Routing	Make ipv6fib global feature message ISSU compliant .
CSCsk79113	Routing	memory leak in VTEMPLATE Background if standby dissappears
CSCsk80250	Routing	BGP has to handle the return value REXP_DONTKNOW of regexec_hybrid
CSCsk82988	Routing	ttl-security next hop inaccessible when peering to loopback
CSCsk83038	Routing	During the ISSU runversion vacl packets switched in SW .
CSCsk84653	Routing	EIGRP variance unequal cost load balance routes get stuck .
CSCsk86150	Routing	w/ BGP auto-summary enabled, networks are lost from BGP after EIGRP flap
CSCsk86476	Routing	OSPF fails in MTU-mismatch setup when mtu-ignore is configured
CSCsk89546	Routing	RIB and FIB not updated after shut TE LB path
CSCsk95829	Routing	TE Tunnel intf is removed from routing table after rapid shut/no shut
CSCsk95969	Routing	mfibv6: Crash in ipv6_pdb_find_ipdb while configuring ipv6 address
CSCsl04835	Routing	BGP conditional route injection not removing routes from iBGP peers
CSCsl06336	Routing	removing 'maximum-paths import 6' causes duplicate paths in VRF table

Identifier	Technology	Description
CSCsI07297	Routing	SXF11: BGP "no neighbor" command caused Address Error exception .
CSCsI13950	Routing	VS2:XDR_LC traceback seen on Standby-RP on bootup .
CSCsI15208	Routing	OSPF DCbitless LSA count goes negative with OSPF flood reduction enabled
CSCsI20133	Routing	PE-CE: remote vpn routes with SoO not advertised to CE
CSCsI20856	Routing	standby HSRP flaps with ospf mib polling/aggressive timers/nostandby sso
CSCsI28278	Routing	OSPF-Route/CEF entry lost after SSO on the neighbor
CSCsI30331	Routing	Prefixes permitted despite the deny action on route-map continue
CSCsI31627	Routing	vrf aware NHRP/mGRE, Crash in rn_walktree_blocking while removingtnl
CSCsI32318	Routing	OSPF: new fix for CSCsk36324 SPF loop
CSCsI33632	Routing	Router crash at vrf_interface_associate when vrf is unconfigured .
CSCsI47915	Routing	Redistribution of ospf in rip with prefix-list not working properly
CSCsI48075	Routing	Floating static route behaves incorrectly in 6vPE
CSCsI49628	Routing	VRF is not getting deleted in 'sh vrf' output
CSCsI50271	Routing	Enhancement is needed in OSPF to avoid suspend
CSCsI51616	Routing	v6-vrf-lite config doesn't sync properly with standby
CSCsI52594	Routing	Cannot ping ipv6 loopback addr (No valid source address for destination)
CSCsI56547	Routing	sh mls cef ipv6 vrf <id> for 6VPE says VRF ids does not exist
CSCsI56914	Routing	OSPFv3 router LSA stuck in retransmit
CSCsI57457	Routing	ISIS NSF switchover failure - similar to CSCsI28278
CSCsI62076	Routing	Router crashed when configuring IPv6 RIP
CSCsI63869	Routing	%DUAL-3-INTERNAL: EIGRP-IPX: PDM Internal Error while processing dndb
CSCsI69845	Routing	VPDN/MPLS : Interface counter not incremented by labeled packets
CSCsI71540	Routing	Router crash after using cmd 'sh ip bgp x.x.x.x [bestpath
CSCsI72774	Routing	Memory leak in CEF consistency checker
CSCsI80887	Routing	Traceback @ rip_sendupdate_subr when update timer set to '0'
CSCsI83415	Routing	Rtr crash in show cmd: new updgrp add enlarges Nbr bitfield size for Tbl
CSCsI84712	Routing	Error- %OSPF-4-FLOOD_WAR: Process 123 re-originates LSA ID 10.55.122.148
CSCsI85391	Routing	TE Tunnel remains down after remove/add IP address
CSCsI92283	Routing	Unable to add into routing table if static route use interface + gateway
CSCsI94410	Routing	Back out the CSCsj17879 for all non ERF branch
CSCsI95609	Routing	Alignment TBs@bgp_ipv6_mpath_statechnng_inprocess on del/add 6VPE vrf
CSCsI96254	Routing	EIGRP distribute-list not checked if intf distribute-list permits route
CSCsm04442	Routing	Router crash at rip_find_sum_idb
CSCsm05082	Routing	BGP Dampening penalty not decaying on frqnt 'sh ip bgp v all' [dampening
CSCsm10603	Routing	L2tp sessions were getting flapped
CSCsm17899	Routing	OSPF routing loop when using Virtual-Link
CSCsm23764	Routing	CEF RF progression error if RRP reloads mid CEF sync

Identifier	Technology	Description
CSCsm26130	Routing	BGP with auto-summary not injecting locally orig. route into BGP table
CSCsm26968	Routing	ipv4 prefix added to routing table in error next hop int ipv4 disabled
CSCsm27958	Routing	Control Plane interface in OSPF interface added preventing SSO oper
CSCsm27979	Routing	router may crash for "address error exception" doing sh ip route vrf
CSCsm30569	Routing	CEF path fragmentation broken for static IPsec VTI
CSCsm36500	Routing	TB@adj_add w/ %ADJ-3-NOFIBIDB: CEF Interface not found msg on SPA OIR
CSCsm39159	Routing	ARP HA cpu hog on stby while bringing up stby with large arp tables
CSCsm39308	Routing	Null Pointer Read condition detected in "clns_find_router_name()"
CSCsm39730	Routing	BGP churn: VRF route version number keeps increasing
CSCsm41873	Routing	MCP: Router crashes while unconfiguring the <ip vrf "vrf name">
CSCsm43938	Routing	stby resets when large config/arp table to sync over to it
CSCsm45634	Routing	BGP VPNv4 route is not activated immediately after receiving update
CSCsm47111	Routing	FIB: Accessing freed memory while dequeuing
CSCsm49143	Routing	6VPE: IPv6 PING is broken in whitney2 SX142 with VRF and source address
CSCsm50741	Routing	Removal of DCbitless LSA causes problems
CSCsm57494	Routing	BGP update is not sent after reloading opposite router
CSCsm64516	Routing	OSPF MD5 Key Does Not Accept Whitespace Character
CSCsm64643	Routing	IPv6 passive interface address not in the isis database
CSCsm72604	Routing	OSPF remaining summary route when dual OSPF process redistributing
CSCsm91801	Routing	ASBR not updating metric in LSA-5 redistributing from 2-nd OSPF process
CSCsm95129	Routing	"no ip next-hop-self eigrp" not working when redistribute from BGP
CSCsm96785	Routing	"nsf cisco" under router ospf config does not work, but "nsf ietf" works
CSCsm96901	Routing	Unable to ping between vrfs through transparent bridge
CSCsm98767	Routing	show ip bgp neighbor does not reflect actual sent/received prefix number
CSCso00383	Routing	MVPN: New style PE doesn't send RD Type 2 MDT update
CSCso07371	Routing	SCHED-7-WATCH: Attempt to set uninitialized watched boolean in pfxlist
CSCso07520	Routing	MCP:OSPFv3 BFD Link-Local peers flap during RP/SSO switchover
CSCso08786	Routing	Standby reloads due to config sync failure on inherit peer-policy cmd.
CSCso09977	Routing	EIGRP IPv6: include-connected option does not work for EIGRP routes.
CSCso12305	Routing	cfc_dev: Missing IPv6 prefixes on unixrp found by full-scan-rib-ios cker
CSCso14177	Routing	EIGRP offset-list with interface modifier does not send correct metric
CSCso14979	Routing	Notify platforms when FIB disables dCEF for a linecard
CSCso15740	Routing	'set metric' clause' in continue route-map sequence does not set metric
CSCso22098	Routing	OSPF down on RPR+ switchover on core router
CSCso22883	Routing	Passive-interface command applied to all address-families
CSCso25823	Routing	Router crashes when mpls ip command is issued on 12.2(32.8.11)SR129 imag
CSCso30199	Routing	ISIS topology broken after a force-switchover when ispf is enabled

Identifier	Technology	Description
CSCso38444	Routing	Change of OSPF network type may break MPLS TE Topology database
CSCso39597	Routing	StbyRP crashed @ bgp_vpnv4_bulk_sync_mpls_lbl_binding during bulk sync
CSCso40442	Routing	BGP sessions Idle after switchover from RPR+ mode
CSCso51519	Routing	Paths with same Nexthop selected as multipaths in some sequence
CSCso52344	Routing	Inconsistent fib entry for 224.0.0.0/4, drop vs multicast oce on RP/LC
CSCso54167	Routing	BGP peer stuck with table version 0
CSCso55151	Routing	ADJ not freeing memory under IPv6 ND stress test
CSCso62166	Routing	Crash @ bgp_netlist_validate when ibgp established with metric
CSCso63693	Routing	ISIS: Maximum circuit limit (255) has reached with passive-interface def
CSCso64274	Routing	0.0.0.0/0 redistributed entry not removed RIP DB after deleting command
CSCso65266	Routing	Memory leak at BGP Router on 12.0(32)Sy4
CSCso67141	Routing	BGP routes are not removed when peer goes down
CSCso67850	Routing	CMTS crashes in ipv6_nd_prefix_get_addr_sb
CSCso73076	Routing	can not delete ACE enties in ACL
CSCso76661	Routing	DHCPv6 PD not working after interface flap
CSCso80951	Routing	BGP peers with same policy fall into different update-group with SOO
CSCso87916	Routing	IPv6 RIP Router crashed,TB @ ipv6_rip_idb_down
CSCso89675	Routing	Device crash @ ip2access_add_pbacl_item with largre PBACL configuration
CSCso93535	Routing	Upon removing a VRF, BGP route timers in other VRF's get reset
CSCso98964	Routing	EIGRP authentication not working for long key-strings
CSCsq02587	Routing	Tunnel not coming up in EoMPLS with mpls TE case
CSCsq05602	Routing	TE tunnels are down but still show in the forwarding table
CSCsq13111	Routing	7609s vlan traffic reporting
CSCsq13938	Routing	reload on 'show ip bgp vpnv4' when import src delinked by BGP deconfig
CSCsq16611	Routing	ipv6 packets are process switched instead of cef-switching.
CSCsq24935	Routing	Switch crash due to unsupported bgp/ipv6 command
CSCsq26684	Routing	ipv6 nd prefix CLI should not update RIB
CSCsq29052	Routing	Ping fails on applying ip unnumbered configs in mpls oam
CSCsq38431	Routing	OSPF "summary address" is executed, even if subnet is becoming small
CSCsq38703	Routing	BGP route still present on remote PE even after deleting the VRF
CSCsq40845	Routing	C2W2: standby reloads while unconfiguring ipv6 access-list with 080521
CSCsq43831	Routing	Stack overflow due to recursion in FIB
CSCsq44052	Routing	ISIS: Unable to configure "is-type level-1"
CSCsq45082	Routing	ip route with associated track/sla gets removed when track is still up
CSCsq49201	Routing	Password in BGP peer-session template not inherited
CSCsq58164	Routing	%IPV6-3-RIB address cannot be deleted when removing address from VRF RIB
CSCsq62703	Routing	Router crashed with TLB (load or instruction fetch) exception

Identifier	Technology	Description
CSCsq75944	Routing	crashes in ipflow_ager, ipflow_sub functions, ipflow_periodic
CSCsq86192	Routing	dmzlink-bw not propagated after inheritance has been configured
CSCsq97517	Routing	C2W2: Mago: CEF on RP is not in sync with SP after reboot.
CSCsq99447	Routing	When BFD/ EIGRP configured in more than 32 vrf BFD does not come up
CSCsr07262	Routing	IPv6 ND response is very slow(>10s) during RP switchover
CSCsr08468	Routing	some external OSPF routes are unable to be installed into Routing Table
CSCsr20566	Routing	interface permanently dampened from routing perspective / STUCKTMR
CSCsr27794	Routing	BGP updates stuck during peer flap
CSCsr30406	Routing	no capability opaque w/o nsf ietf helper disable cause err msg
CSCsr41079	Routing	%CHKPT-4-NOMESSAGE: Message is NULL, (Cannot get data ptr)
CSCsr45653	Routing	Prefixes not deleted by CEF distribution broker
CSCsr55922	Routing	router id is not correctly set in EIGRP ipv6 process
CSCsr67177	Routing	Router with IPv6 OSPF crashes on reloading
CSCsr67562	Routing	Support for running ispf with nodes having overload bit configured
CSCsr67863	Routing	c2w2:TB seen in RPR-->ISSU-3-NOT_FIND_MSG_SES: Can not find message sess
CSCsr74295	Routing	static route to mlppp not in rib
CSCsr83062	Routing	IOSD crash at ipv6_show_interface when doing "show ipv6 interface"
CSCsr83639	Routing	Bus error crash when removing BGP configuration
CSCsr86174	Routing	aggregate-address under address-family does not appear in conf
CSCsr90248	Routing	"aggregate-address advertise-map" not updated dynamically
CSCsr96042	Routing	ASR: IOSD crashes at bgp_vpn_import_walker while unconfiguring vrf
CSCsu03167	Routing	SXF15: IPv4/v6 BGP routes not cleared when source routes is gone
CSCsu12040	Routing	PE with CsC configuration sends wrong labels to SPE
CSCsu24087	Routing	Cisco7609 crashes after "clear ip bgp neighbor x.x.x.x soft in"
CSCsu31954	Routing	Router crash when fragmenting packets with netflow
CSCsu36709	Routing	Unable to boot IOS image on PE (vrf-enabled) router - software fault
CSCsu37200	Routing	%SYS-3-BADTREEPARAM generated while aging DNA lsa type-11
CSCeh98154	Security	High Cpu when using show processes cpu monitor through SSH
CSCin91851	Security	Support keyboard-interactive authentication method
CSCir01449	Security	Sync damage of CSCin74155 fix
CSCsb58633	Security	SCP server gives files with invalid checksum on some router platforms
CSCsb80803	Security	SSH Process: SCHED-3-UNEXPECTEDEVENT error message
CSCsd02612	Security	Failed Secure copy (due to exec privilege) not returning console prompt
CSCsd30932	Security	CLI: router reload on bad refcount error during CA trust point config
CSCsd35474	Security	router crashed during the capf upgrade
CSCsd81870	Security	Teraterm + TTSSH2 does not work in SSH Ver.2
CSCsf15428	Security	Config change before Phase-2 rekeying results in SA lifetime mismatch

Identifier	Technology	Description
CSCsf17406	Security	Large CRLs can cause memory leaks
CSCsg48392	Security	Resuming SSH Session Fails After Disconnecting Another One (Not Console)
CSCsh54862	Security	MPLS TE Tunnel Up by no shut without RSVP signalling completed
CSCsh72664	Security	DMVPN: OSPF neighbor flap and traceback @ tunnel_oqueue. .
CSCsi50499	Security	When aaa cmd author is enabled, SCP fails and tracebacks appear
CSCsi83287	Security	%ALIGN-3-SPURIOUS T/B ipv6fib_gre_ipv6 after packet decap
CSCsj45031	Security	Cat6k unable to SCP files from Tectia ssh server
CSCsk10376	Security	MPLSoGRE EXP to external TOS not copied for locally generated packets
CSCsk43745	Security	IP multicast fast switching flag does not match expected value
CSCsk64898	Security	NAT-PT is broken for ipv6ip tunnel traffic terminated on HSRP IP address
CSCsk75078	Security	rcv client_input_channel_req: channel 0: unknown channel
CSCsl03084	Security	7600 SSH issues with privilege levels
CSCsl13561	Security	Enhanced EzVPN no longer passes traffic
CSCsl43546	Security	6vPEoGRE :- mls cef programming incorrect on SIP600 after reset
CSCsl61311	Security	New SSH sessions with RSA key sometimes fails after changing hostname
CSCsl98498	Security	Tunnel int is going down with mode ipip decapsulate-any
CSCsm55629	Security	Syslog for SSH returns NO username
CSCsm57122	Security	Scp and ssh failing with certain ssh clients
CSCsm70913	Security	UDLR: not able to clear portchannel config from the tunnel after del/add
CSCso48959	Security	user not reported by "login on-success log" feature for SSH logins
CSCso64607	Security	Router Crashes when no ip vrf <vrf>
CSCso67083	Security	IOS crypto ACL does not support pattern matching (discontiguous subnets)
CSCso73533	Security	%ALIGN-3-TRACE traceback seen @ ipv6_init_header
CSCsq14031	Security	Ping fails through crypto tunnel on Full Service Branch testbed
CSCsq58748	Security	IPSEC: IKMP process can get blocked by some PKI OCSP requests
CSCsq60016	Security	Router crashes when entering a long RSA key string
CSCsr55713	Security	DMA Issue:Router crashed while doing ISATAP Tunnel Interoperability test
CSCsr85093	Security	SXF15: SSH session fails withRSA signature verification failed after SSO
CSCdu70318	Unknown	Feature Request: VRF-lite PBR
CSCeb69473	Unknown	connect '/terminal-type' command memory corruption
CSCed88426	Unknown	Extended acl breaks on first switchover (Ctrl-C not synced to stdby)
CSCee25454	Unknown	SADB peering process leaks memory after overnight test
CSCeg35237	Unknown	Watchdog crash after sh crypto session
CSCeh08262	Unknown	Show tech SP output should honor redirect applied
CSCeh42472	Unknown	Standby RSP doesnt boot because of image uncompression failures
CSCeh52674	Unknown	no snmp-server host command will not remove entry from config
CSCeh96798	Unknown	sh mpls forward reporting none for Outgoing interface

Identifier	Technology	Description
CSCei52830	Unknown	Banner command sync is broken by CSCin86483 .
CSCei67734	Unknown	New RF state required for C10K Security ACL/Policy Map compiling
CSCej77184	Unknown	%LSD-4-LABEL_RESOURCE:label exhausted while sso switchover
CSCek35122	Unknown	Wrong statistics on input subinterface vlan counters for EoMPLS
CSCek37984	Unknown	Inconsistent BERT behaviour observed on TE1 SPA
CSCek39284	Unknown	fastethernet0/0/0 intermittently fails after switchover
CSCek40773	Unknown	CE-CE connectivity broken on MPLS VPN with GRE tunnel in VPN core
CSCek50172	Unknown	%SYS-3-TIMERNEG: Cannot start timer with negative set
CSCek63963	Unknown	EEM2.4:Getting the traceback when configuring rate based interfED
CSCek66142	Unknown	%SCHED-3-SEMLOCKED: rf proxy rp agent attempted to lock a semaphore
CSCek66877	Unknown	%XDR_SP-STDBY-6-CLIENTISSU_BLOCKED: XDR client lte broker cannotSync
CSCek67054	Unknown	ISSU Rollback timer should not wait for stdby in Hot if HA mode RPR
CSCek69134	Unknown	AB76:ESM20G MPB-E:RP hangs,CPU at 100% with default int on 8K EVC
CSCek71816	Unknown	CE-CE ping fail after restore ASBR-PE vrf
CSCek73818	Unknown	Router crash when issue mpls oam echo revision command on 7600 HA
CSCek75082	Unknown	Router crashes while unconfiguring channel-group
CSCek75768	Unknown	Ensure EEM policies are registered correctly through ssh.
CSCek76062	Unknown	Router crashed @ validmem_complete_interrupt .
CSCek77996	Unknown	High CPU caused by data traffic with crypto map in crypto connect mode
CSCek78653	Unknown	Cannot bring up PPTP sessions Due to FM Segment initialize failure
CSCek78874	Unknown	KMI:Out of order deletes cause sync issues
CSCin67287	Unknown	NxDS0 BERT capability on PA-MC-8TE1+
CSCir00379	Unknown	NAD supplies old state attribute to ACS while sending new EAPID resp
CSCsa96960	Unknown	ip ttl expired lsp ping pkts shouldn'tt be transited by MFI process sw
CSCsb18498	Unknown	SNMP polling broken in cat6k SXE1 image
CSCsb57042	Unknown	%SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs
CSCsb87956	Unknown	loop in the state IKE_CONFIG_MODE
CSCsb92711	Unknown	HA: %ISSU-3-ERP_AGENT:req_msg is NULL traceback during slave boots up.
CSCsc05894	Unknown	Issue with IP MTU for IPSec VTI
CSCsc21582	Unknown	show crypto isakmp peer shows no output
CSCsc24015	Unknown	Parser loops infinitely for match route-type [ext
CSCsc59190	Unknown	%PM-STDBY-4-INT_FAILUP: fa4/3 failed to come up message after switchover
CSCsc85962	Unknown	Replaying Main Mode packet causing IKE SA deletion
CSCsd02012	Unknown	CEF data mismatch between RIP & VIP
CSCsd04608	Unknown	MQC-IPHC: Router crashed while testing mqc-iphc test
CSCsd08411	Unknown	EEM Tcl policy execution delayed relative to config size
CSCsd09324	Unknown	IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP shown on stby RP when reload rtr

Identifier	Technology	Description
CSCsd47734	Unknown	Additional memory leak fixes by ActiveState
CSCsd48814	Unknown	Unable to start an SSH session from tclsh mode on the router
CSCsd69625	Unknown	EZVPN:IOS C876 Client can't connect to ASA using digi certs and noXauth
CSCsd70321	Unknown	Resetting a line card and an sso right after that - traffic gets dropped
CSCsd76111	Unknown	dot1x:%SM-4-BADEVENT cause by 'authTimeout'
CSCsd82457	Unknown	EOU Policy can't exempt Cisco 7935 Conference Station & Wireless phones
CSCsd87313	Unknown	ip cef load-shar algorithm universal not consistent between stack member
CSCsd98852	Unknown	EEM does not allow read from stdin
CSCse12518	Unknown	MET optimized update can cause blackholing and duplicates
CSCse15947	Unknown	20 seconds of traffic loss after test crash 9 on active SP
CSCse16923	Unknown	5850: IOS upgrade issue in handover split mode
CSCse31572	Unknown	Bus error at crypto_ikmp_config_authenticated
CSCse31818	Unknown	Traceback if_index_open_port_to_speak seen when ISSU with 12.2SG/SGA
CSCse37042	Unknown	BOOM: Adj are not getting resolved for the directly connected vrf en int
CSCse42370	Unknown	BOOM: STNDBY Rest , active crash while applying SP on SIP600 output int
CSCse48657	Unknown	config sync will reset standby when no EEM policy only on active
CSCse53517	Unknown	WiSM: Tracebacks seen after SSO switchover
CSCse57081	Unknown	NACL2IP: Clientless IP Phone triggers authentication to ACS every minute
CSCse63833	Unknown	SNMP bus error while polling cipsStaticCryptomapTable .
CSCse67736	Unknown	Add support for XFP-ZR optics
CSCse69570	Unknown	Leakage of VRF routes in global routing table
CSCse72688	Unknown	In sup720, ingress packet info. of GRE tunnel was not exported to server
CSCse78548	Unknown	LSR adds incorrect label stack (label 1)
CSCse82589	Unknown	LSR mishandles packets with router-alert label
CSCse89636	Unknown	LFD-3-INVINSTALLER LSD-3-LABEL msgs and tracebacks when PRE2 -PRE3 ISU
CSCsf08502	Unknown	event_reqinfo event_pub_sec/event_pub_msec missing for event_none events
CSCsf08803	Unknown	event snmp may wrongly triggered when using type increment
CSCsf22829	Unknown	EEM Interface event detector sets old value to the sample value
CSCsf27677	Unknown	crash on V122_31_SB_THROTTLE image with fix for CSCse89636
CSCsf97859	Unknown	invalid shows in show hw-module subslot with SPA-OC192POS-LR
CSCsg01644	Unknown	EEM debug event manager tcl cli sent to the console, script may crash
CSCsg09654	Unknown	c7304:COMMON_FIB-2-HW_IF_INDEX_ILLEGAL
CSCsg13828	Unknown	fh_fd_timer.proc crashed without any special trigger
CSCsg14063	Unknown	SPA-[2/4]XOC48POS/RPR voltage reading needs parameter checking
CSCsg21809	Unknown	Add bridge asic status collection support .
CSCsg22830	Unknown	Standby not coming up after sso switchover
CSCsg28331	Unknown	AB: SIP600: LC memory leak on PW VC switchover

Identifier	Technology	Description
CSCsg29305	Unknown	hw-module subslot reload crashes the router .
CSCsg41017	Unknown	VSA crashes on tunnel bring up with 1000IKE/1000GRE with pki
CSCsg47039	Unknown	SIP-600/ES20 LC crash following TE-FRR scenario on tunnel recovery
CSCsg57611	Unknown	PBHK id missing in IP and Interface session accounting start records .
CSCsg67551	Unknown	LDP session starts to flap after graceful-restart on switchover
CSCsg75132	Unknown	REDUNDANCY-3-IPC: cannot open standby port session in use
CSCsg86046	Unknown	Unable to monitor traffic in the clear when using the vrf vpn config
CSCsg86567	Unknown	MDT tunnel reuse at stby causing %IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP
CSCsg87235	Unknown	EEM config prevents telnet connection
CSCsg87747	Unknown	RECV_PVID_ERR message received with bringing up etherchannel trunk
CSCsg96495	Unknown	IF--Index: Allow recovery following hwidb->hw_if_index being set to -1
CSCsg98045	Unknown	EEM track event detector missing maxrun option for tcl scripts
CSCsg98612	Unknown	Speed negotiate CLI option missing for SIP-600/ESM-20 eth ports
CSCsg99996	Unknown	on a ERP_CLIENT: Timer event IPC versioning process gets stuck
CSCsh17328	Unknown	WS-SVC-WISM-1-K9 reports 0.0 in entPhysicalVendorType
CSCsh17579	Unknown	Transceiver TX Power displays erroneous TX level
CSCsh17630	Unknown	HA: Standby reset with invalid config
CSCsh28014	Unknown	After unconfig MPLS, seen %SCHED-CFC8-3-UNEXPECTEDEVENT & Traceback
CSCsh30143	Unknown	COMMON_FIB-2-HW_IF_INDEX_ILLEGAL: Attempt to create CEF interface if=0
CSCsh30617	Unknown	EEM software forced crash when unregistering an applet
CSCsh34536	Unknown	CEOP: CEM group config lost on standby RP
CSCsh35451	Unknown	stbySP crash after LV-RV-RVSO-RV w/ MDR SM blockin RF in RF_PROG_ACTIVE
CSCsh42678	Unknown	C2W2:SWITCH_BUS_IDLE on standby SP after RV
CSCsh56121	Unknown	Losing RSA keys on Standby Supervisor after switchover or reload
CSCsh57238	Unknown	SXF6:sh int cmd on 6148 cards display zero o/p drops even with qos drops
CSCsh61002	Unknown	SPA-5X1GE: GE-port not transmitting after 'shut/no shut' and vica versa
CSCsh64820	Unknown	ISSU Abort imme after RunV cause act/stby with new/old image
CSCsh74385	Unknown	EEM fails to register with the redundancy framework (RF)
CSCsh74417	Unknown	crash in c10k_remote_crash_interrupt
CSCsh74962	Unknown	Interface Bounce holding CAC limit unable to accept IKE session.
CSCsh83272	Unknown	We need to have consistency-check type rp-sp by default
CSCsh83362	Unknown	Xconnect down as L2TPv2 to PPP-AC switching not enabled after reload
CSCsh84657	Unknown	STP Loopguard: Ability to disable loopguard for Po270 and higher for FWM
CSCsh96342	Unknown	PVID inconsistency handled incorrectly when running MST
CSCsh97395	Unknown	IDSM: Monitor config was removed after RPR switchover
CSCsh97848	Unknown	Sierra: LACP pdus should be untagged .
CSCsi00377	Unknown	Exit Mismatch when application & prefix with common dst have diff policy

Identifier	Technology	Description
CSCsi05265	Unknown	SYS-2-GETBUF: Bad getbuffer -Process= LSDp Input Proc
CSCsi05515	Unknown	Entrance Load and Range on by default
CSCsi05566	Unknown	Configured ACL not formatted correctly when controlling applicaton
CSCsi09699	Unknown	OER -Inside prefixes not learned rom BGP for egress optimization
CSCsi22093	Unknown	Standby resets more than once, w red mode change + write mem
CSCsi28462	Unknown	Unable to initialize the SASL client on the peer router.
CSCsi31755	Unknown	BEEP IO handler hogs cpu and memory
CSCsi32646	Unknown	%UTIL-3-IDTREE_TRACE: PW freelist DB:Duplicate ID free for 14463433
CSCsi43654	Unknown	SIP-600: EXCEEDGUAR msg appears when boot with interface bandwidth
CSCsi46510	Unknown	Gig port goes down on switchover, TB @ process_unlock_semaphore
CSCsi49150	Unknown	%PM-SP-4-PORT_BOUNCED: Port Gi9/3 was bounced by Consistency Check IDBS
CSCsi52382	Unknown	radius attribute 5 nas-port not sent in access-request for RA VPN users
CSCsi55428	Unknown	FRU Trap sequence incorrect when " hw-module subslot shutdown unpowered"
CSCsi58211	Unknown	Link flap under load with XENPAK-10GB-LW
CSCsi63649	Unknown	%SYS-3-TIMERNEG:Cannot start timer with negative offset,TTY Background
CSCsi70224	Unknown	NRT: STANDBY BOOT VAR disappears after HA switchover
CSCsi80642	Unknown	EzVPN ISAKMP rekey fails due to invalid proposal
CSCsi82166	Unknown	BEEP Router crashes at user_pw_lookup with 12.4(13.13)T1 image
CSCsi84417	Unknown	router hang/crash and cpuhog msgs seen when attaching service-policy
CSCsi85453	Unknown	cfg-sync failed if switchport config is pasted on active & stby restart
CSCsi85532	Unknown	c851 crash w/o specifying pw-class in pseudowire
CSCsi92079	Unknown	OER system disabled fatal error . .
CSCsi94738	Unknown	8xCHT1/E1 SPA modules not in entAliasMappingIdentifier
CSCsi96685	Unknown	Crash in chunk free called by sss_free_switch
CSCsi97434	Unknown	A router may crash when ipsec is established
CSCsi99875	Unknown	BOOM: spa_eeprom_read_bit on BOOTUP
CSCsj00870	Unknown	CAT6000: ICC client shall use ipc_return_message under error conditions
CSCsj01961	Unknown	ifindex table size from nvram sould be validated before malloc
CSCsj03212	Unknown	blade get into bad b2b state if it is not b2b ready
CSCsj04201	Unknown	%MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC: RP failed allocating IPC buffer
CSCsj06641	Unknown	LI: Traceback found in creating entry in cTap2StreamTable
CSCsj08713	Unknown	Disable bfd on SVI interfaces
CSCsj12034	Unknown	fabric switching-mode allow dcef-only- config makes stby stuck at rommon
CSCsj14565	Unknown	ACL = deny; sa request ignored when crypto local-address is dynamic
CSCsj19316	Unknown	Standby resets while booting up due to %FILESYS-4-RCSF error
CSCsj20130	Unknown	%QM-2-TCAM_ERROR: TCAM programming error 20
CSCsj21464	Unknown	EPM dACL enhancements and EPM SSO support

Identifier	Technology	Description
CSCsj25470	Unknown	EEM hostnames over 20 characters causes CLI actions to hang
CSCsj27436	Unknown	c7600 duplicate and INVALID mls mpls label entries in FIB
CSCsj32493	Unknown	IPSEC: Incorrect IPSec connection info in InvalidSPI testing
CSCsj36327	Unknown	SPA-4XOC48POS/RPR won't come up after reload
CSCsj37398	Unknown	Properly initialize the Tycho register AC_QOS_DEFAULT_EGRESS (0x334)
CSCsj38796	Unknown	LC/SP crash @ label_entry_get_inlabel
CSCsj40695	Unknown	EEM: Incorrect TCL event registration string can hang or crash device
CSCsj42098	Unknown	SupV drops big packets destined to a GRE Tunnel when frag. needed .
CSCsj43677	Unknown	Active Sup720 crash when removing Standby supervisor
CSCsj43962	Unknown	ISG interface responds to ARP for GLBP VIP with own MAC
CSCsj48453	Unknown	AW: CAT6k does not forward multicast traffic to WISM in L3 mode
CSCsj49293	Unknown	POS Interface Output Rate (200 mbps) > Line rate (155 Mbps)
CSCsj53663	Unknown	EEM: RP crashed at fh_fd_syslog_event_match
CSCsj57351	Unknown	SU07 ME-C3750 crashed during elmi test
CSCsj58287	Unknown	7600-SSC-400 crashes on reload
CSCsj58538	Unknown	Lots of prowler/patriot interface go down for few second during sso swov
CSCsj59997	Unknown	VTI tunnel: Arp for tunnel destination instead next hop.
CSCsj60006	Unknown	QoS: 'match ip rtp 65530 5' though accepted is not showing up in sh run
CSCsj60182	Unknown	IPSEC Tunnels not coming up in transport adjacency mode
CSCsj65189	Unknown	Traffic stops over EOM ckt after SSO and followed by TE FRR cutover
CSCsj65755	Unknown	Packet loss with SPI NOT Available message during rekey .
CSCsj70303	Unknown	BOOM :Alignment error found @ ha_send_cfg_change_internal.
CSCsj74617	Unknown	MFI static-label configuration does not sync to slave RP
CSCsj77885	Unknown	%HA_EM-7-FMS_POLICY_MAX_ENTRIES message because of teminal length limit
CSCsj78751	Unknown	ES20: shut & no shut on ZR XFP causes the port to stay down
CSCsj78820	Unknown	MEM leak in Crypto IKMP process(crypto_ikmp_author_get_attributes)
CSCsj80655	Unknown	timer value overflows when the specified val is larger than a long val
CSCsj85897	Unknown	SPA-TE1-Linkrec's out of sync between SPA and LC
CSCsj86153	Unknown	Modular IOS CPU load oscillates even under constant load
CSCsj87687	Unknown	Crash during startup with mpls configured
CSCsj89905	Unknown	EEM applet hangs if system prompt is changed
CSCsj90252	Unknown	SYS-3-CPUHOG IP RIB Update seen on Active RP
CSCsj90758	Unknown	UUT with BGP/DMVPN crashes after restarting iprouting.iosproc
CSCsj91961	Unknown	Ifnums of channels for E3 dont match on active and stdby
CSCsj94539	Unknown	Spurious Alarms in PA-MC-8TE1+ may cause router crash
CSCsj98198	Unknown	When we have only 1 flow in TT, flows are not exported to MC
CSCsj98492	Unknown	Pak subblock handlers need to be part of packet library

Identifier	Technology	Description
CSCsk02456	Unknown	TBs found @ pm_assert_fail. .
CSCsk04241	Unknown	XFP occasionally goes into module not-ready state after enabling laser
CSCsk07255	Unknown	Sip-600 crash on SSO
CSCsk08329	Unknown	inbound service-policy traffic incorrectly seen in default-class
CSCsk16240	Unknown	C2W1: active not responding msgs seen om reload with 41patches
CSCsk16706	Unknown	AB76:Unable to configure cwan int in SSO- standby doesnt support cmd
CSCsk17449	Unknown	GLBP debug is shown for non-GLBP addresses
CSCsk19817	Unknown	shut/no shut causes pm failed get pm mp semaphore
CSCsk19866	Unknown	Unable to boot boomerang image on sup720
CSCsk21354	Unknown	PAT : Missing second Netflow shortcut after route change.
CSCsk26456	Unknown	SPA-4XOC3-ATM does not pass traffic after SPI4 source FIFO overflow err
CSCsk27081	Unknown	ifHCInOctets and ifHCOctets on GE-WAN interfaces wrap up at 2^32
CSCsk32872	Unknown	Wrong API usage, can lead to crash .
CSCsk33045	Unknown	MST BPDU *must* be sent untagged, even when the switch is configured wit
CSCsk37675	Unknown	IKE stuck after several hours of IKE SA rekey .
CSCsk38937	Unknown	Loss of traffic for more than 15 seconds when PRE2 failover to standby
CSCsk39340	Unknown	IPRM process runs at 100% CPU for more than 30 mts
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
CSCsk44233	Unknown	While raising the interrupt level, bgp_route_map_inform tries to suspend
CSCsk45585	Unknown	Heathland: On bootup MPLS not supported on platform message
CSCsk48089	Unknown	Enhance "ip policy route-map" command for backward compatibility
CSCsk49151	Unknown	Vlan policy-map rejected upon reloading.
CSCsk58040	Unknown	WS-X6148A-GE-45AF retains previous modules MACs after OIR
CSCsk60112	Unknown	NRT:NSE-150 is not initializing the memory to zero before assign a value
CSCsk60912	Unknown	MPLS forwarding table empty on standby RP .
CSCsk63657	Unknown	Not able to sync up to loopback line on SPA-1XOC12-POS
CSCsk64543	Unknown	PoE Power Calculations Incorrect
CSCsk64625	Unknown	VPLS pkt drops in xchip when TE tunnel path changes to alternate path
CSCsk67417	Unknown	Crash while two or more users displays: show ip arp inspection log
CSCsk67457	Unknown	BCP-MLP:Traffic stops flowing making one link shut on multilink
CSCsk67578	Unknown	Flow End sysUpTime higher value than the Router sysUpTime
CSCsk70628	Unknown	MST : Not subtracting remaining hop count of agreement BPDU
CSCsk73627	Unknown	WS-X6548-GE-TX powered down due to keep alive polling feature
CSCsk73838	Unknown	After fabric tiemout is seen, line card did not recover using earl patch
CSCsk77282	Unknown	EEM RPC file descriptor leak
CSCsk77462	Unknown	IETF Class attribute is missing in radius accounting record

Identifier	Technology	Description
CSCsk77648	Unknown	HA: issu image-version compatibility en/dis not function properly.
CSCsk78390	Unknown	Naxos crashes while trying to fpd upgrade granikos
CSCsk80552	Unknown	Shut and no shut of interface causes the delay in forming rp mapping
CSCsk82191	Unknown	Multicast groups sometimes not populated on switchover.
CSCsk82370	Unknown	RP crash and tracebacks in crypto related process
CSCsk83089	Unknown	Increase maximum aggregate policer > 10Gbps
CSCsk83683	Unknown	VRF-Lite aware PBR feature does not work after reload/SSO swover
CSCsk83954	Unknown	Traceback on wan linecards on bootup if mpls access-list configured
CSCsk84443	Unknown	cempMemPoolEntry return worng value
CSCsk84498	Unknown	EVERGLADES:archive,write-mem feature broken
CSCsk86114	Unknown	SRB2:spa-atm: SIP200 crashes at checkheaps_process on atm shut noshut .
CSCsk86381	Unknown	KMI memory leak in 'IPSEC key engine' when delete p2 failed
CSCsk86510	Unknown	DSCP in outer IP copied from MPLS EXP on MPLS->GRE path
CSCsk88273	Unknown	Traceback seen @edisms on clearing counter on Active SP
CSCsk89091	Unknown	HWIF-QOS-ERR: Failure installing Port QoS TX/Rx setting
CSCsk89852	Unknown	VS2: MEC (LACP) members flap when native subinterface is configured
CSCsk89970	Unknown	SPA-IPsec-2G: Don't add Vlan 1 to Wmac & HMAC trunk interface by default
CSCsk93354	Unknown	High CPU on stby PRE due to BEM VERIFY .
CSCsk93366	Unknown	lte_rp_get_lte_update_xdr_size/fib_upd_consume_rec_meets_upd_rec crash
CSCsk94870	Unknown	VS2: TB @ ether_extract_addr
CSCsk97144	Unknown	wait for remote process DiagCard7/-1creation times out with 1018 ION
CSCsl02190	Unknown	ICMPv6 to all node multicast address fail .
CSCsl04500	Unknown	OBFL process causing 6708 high CPU
CSCsl05874	Unknown	MPLS-MFI: mpls fragmentation not working in particle-based routers
CSCsl06059	Unknown	Router crash at route_map_vrf_af_change_nh
CSCsl06577	Unknown	Linking bootflash to bootdisk failed after pcmcia_driver.proc restart
CSCsl07575	Unknown	If VC comes up after policy is applied, VC traffic goes to class-default
CSCsl08596	Unknown	C2W1B: portType and entPhysicalVendorType of 10GBase-LRM is incorrect
CSCsl08912	Unknown	Vlan access list not working when have "xconnect vfi #" under the SVI
CSCsl10489	Unknown	OER ignores MOS score of jitter probe when INPOLICY timer expires
CSCsl11335	Unknown	MVPN-MIB:Entries obtained from "ciscoMvpnBgpMdtUpdateTable" is incorrect
CSCsl11868	Unknown	With IP CEF enabled ACL is not denying packets as intended. .
CSCsl12121	Unknown	Sierra: TB(Spurious memory access) when get ciscoPortSecurityMIB
CSCsl12827	Unknown	Handling Transit IpSec in VRF mode
CSCsl12836	Unknown	CPUHOG in OBFL VOLT bootflash process
CSCsl13477	Unknown	SSO not working with crypto maps terminating at same peer address .
CSCsl16353	Unknown	Problem in SIP400 Vpls Frr Link Protection

Identifier	Technology	Description
CSCsI17798	Unknown	Etherchannel state inconsistent between active and standby
CSCsI18525	Unknown	Standby-SP doesn't have mfib table
CSCsI18765	Unknown	6500-7600 : SPAN of EoMPLS port causes packet reflection or loop
CSCsI18918	Unknown	12.2SRA: Disable Cell Packing .
CSCsI19708	Unknown	Naxos : Disable Telesto Internal TERMINATION For Reference Clock, PB RAM
CSCsI20701	Unknown	EEM RPC memory leak in fh_fd_rpc_get_filename and ifs_simple_open_common
CSCsI21171	Unknown	Crypto syslog messages span multiple packets
CSCsI26033	Unknown	Modifying the BFG doesn't re-create the SA's
CSCsI26998	Unknown	Switch crashes on applying PBR with next-hop verify-availability
CSCsI27236	Unknown	%SYS-3-CPUHOG: Task is running for (126000)msecs, causes RP crash .
CSCsI27957	Unknown	%EC-SP-5-CANNOT_BUNDLE2 is seen after inserting WS-SVC-FWM-1
CSCsI28371	Unknown	SPA-IPsec-2G VRF: L2 loop and broadcast storm may occur on default vlans
CSCsI30308	Unknown	PIM snooping corrupts PIM RPF Proxy packet
CSCsI32940	Unknown	Router crashes while reloading Naxos
CSCsI34481	Unknown	IPV6-MCAST:router crashes while unconfiguring ipv6 mcast routing
CSCsI34515	Unknown	VS2:after SSO with preemption, port security is broken
CSCsI34612	Unknown	RP faced a Modular IOS kernel crash in mem_vmem_free
CSCsI34717	Unknown	TMS_PI1:Syslog missing consumer device-id
CSCsI35325	Unknown	MRIB client remains after a linecard removal
CSCsI39691	Unknown	Config Sync:Bulk-sync failure due to Servicing Incompatibility after SSO
CSCsI40528	Unknown	VS2: Port-channel fails to forward unicast packets after switchover .
CSCsI41230	Unknown	IPSec SPA breaks IPSec if interesting traffic uses TCP ports
CSCsI43540	Unknown	VS2:snmp mac notification for port channel on DFC linecard doesn't work
CSCsI51380	Unknown	Sup720 and Sup32 TCAM & SSRAM Consistency Checkers refinement
CSCsI51395	Unknown	slot_earl_icc_shim_addr:device crash with hw-module reset
CSCsI52092	Unknown	DHCP db agent considers port-channel interface (poX) as invalid
CSCsI53037	Unknown	Mail action does not separate headers from body
CSCsI53279	Unknown	Physical interfaces on Cat6k set to 10 usec regardless of line speed
CSCsI53727	Unknown	Add UDLD interface counters for debugging purpose
CSCsI53845	Unknown	sup720/SXH: dummy packet send over inband when sw netflow is used
CSCsI54630	Unknown	Memory leak after create-apply-remove-delete policies on QM Process RP
CSCsI57993	Unknown	Everglades: MC crash on executing 'sh oer mas traffic-class learned'
CSCsI58673	Unknown	EEM Prevents VTY telnet to MCP router
CSCsI58924	Unknown	Standby SP crashed due to TestAclDeny failure on bootup/switchover
CSCsI59553	Unknown	SIP-400: bursty traffic causes packet drop even in low rates
CSCsI61164	Unknown	Router may crash @ipflow_fill_data_in_flowset when changing flow version
CSCsI62341	Unknown	ip rip summary address cannot be applied to VAI

Identifier	Technology	Description
CSCsl62344	Unknown	Call-home:parser error and profiles are deleted after reload
CSCsl63311	Unknown	6500 May Experience High CPU due to NAT traffic
CSCsl69123	Unknown	SIP-400:QoS:Police drops MPLSCP, CDPCP negotiation packets - SRA,SRB
CSCsl70016	Unknown	WS-X6516A-GBIC card in switch 2 goes down frequently in vs1
CSCsl70148	Unknown	PIM enabled p2p Crypto GRE Tunnels not installed in Hardware
CSCsl70408	Unknown	Standby PRE fails to reach SSO due to BEM CPU hog
CSCsl70667	Unknown	12.2(33)SRB2: LC crash at fib_fib_feature_space_xdr_decode
CSCsl71704	Unknown	VS2:RACL not applied on MEC after disabling netflow & chng flowmask
CSCsl72332	Unknown	cat6k crash with 'no mobility network-id 4'
CSCsl72752	Unknown	VS2: after preempted switchover, interface states are out of sync
CSCsl72826	Unknown	Router Crash @ ipfib_policy_forward
CSCsl72912	Unknown	VS2: WS-X6708 DFC crash in local_cb1(Segment violation)
CSCsl74456	Unknown	VPN-SPA : TCAM not programmed on POS sub-interface after a reload
CSCsl74976	Unknown	Punted MPLS-tagged traffic causes control plane instabilities
CSCsl75136	Unknown	Cat6k with Sup32 failed to boot up after power cycle.
CSCsl75164	Unknown	Router crash when 'clear cry session'
CSCsl75719	Unknown	sxf13 show int tunnel with blank display
CSCsl75836	Unknown	VS2: MCAST LTL T/B's observed, when removing VLAN / SVI used for mcast
CSCsl76647	Unknown	VPN SPA Cannot clear SA using conn-id with CLI
CSCsl78582	Unknown	12.2SRC:SSO :%COMMON_FIB-3-FIB_PATH_LIST_DB:Attempt to add empty path
CSCsl79141	Unknown	Vlan mode EoMPLS new VC does not come up after SIP-600 reload
CSCsl79195	Unknown	XDR issu negotiation failed for standby SP after switchover
CSCsl79219	Unknown	mvpn : bidir shadow entries not installed
CSCsl79781	Unknown	EEM config causes config-sync PRC mismatch error with "do" command
CSCsl80682	Unknown	SPA crashes if crypto acl changed
CSCsl83211	Unknown	Sup32 running ION image fails to bootup after a power-cycle.
CSCsl83212	Unknown	Traceback logs are seen when deleting auto-template interface
CSCsl84317	Unknown	Active crashes on applying acl to EoMPLS subif on SIP-600
CSCsl87677	Unknown	changing the access vlan doesn't reflect the vlan of the secure configur
CSCsl87843	Unknown	GLBP: AVF flaps on changing to lower interface address
CSCsl89069	Unknown	Zamboni crashed at illegal event/state combinationin CfgMonInd, clear sa
CSCsl89176	Unknown	Cat6k may crash when vlanTrunkPortEntry is polled via snmp
CSCsl89425	Unknown	BFD sessions dont scale
CSCsl89890	Unknown	VS2: crash in psecure-process_timer
CSCsl91085	Unknown	system/iprouting.iosproc crash after activate 39 dummy/restart patches
CSCsl92286	Unknown	60 second multicast traffic loss as VSS standby chassis initializes
CSCsl92475	Unknown	CAM entries not removed after EtherChannel down

Identifier	Technology	Description
CSCsI93559	Unknown	Unsupported ISL encap CLI option should be disabled on 6716
CSCsI94301	Unknown	VS2: Mac learning in linecard gets disabled by pre-emption switchover.
CSCsI98238	Unknown	QoS statistics-export only exports to directly-connected destinations
CSCsm01399	Unknown	Bus idle recovery may cause 10GE interface to remain down
CSCsm04256	Unknown	CPUHOG and crash after 'show memory detailed all statistics' issued
CSCsm04824	Unknown	OER Top Talker Functionality broken on s3223
CSCsm05486	Unknown	mtu mis program in adj thru tunnel interface after b2b failover
CSCsm08087	Unknown	Arp unresolved after sh/nosh of egress int ;route-map applied at ingress
CSCsm08830	Unknown	Config-Sync: BadCode fix for CSCed88426
CSCsm08971	Unknown	SEA:Soft reload occurs everytime after issue show cmd's and T/B with mz
CSCsm11717	Unknown	VS2:On reloading standby chassis T/Bs on SP console for 1 minute
CSCsm11898	Unknown	IOS:SLB: Incorrect NAT Translation when Nat client is enabled
CSCsm12692	Unknown	6VPE:RP switchover need for about 10 minutes to resume IPv6 traffic
CSCsm13389	Unknown	RRI is not called be if QM rekey timer expiry forces SA deletion
CSCsm14915	Unknown	Stack overwrite crash with large No of GLBP IPv6 groups on interface
CSCsm15350	Unknown	vpnspace crashed at assert failure in l2-mcpu.c on line
CSCsm15687	Unknown	SIP-600 GE subints fail with crypto connect & VPN SPA
CSCsm16309	Unknown	Fastpath thread crash in BFD code after all BFD sessions went down
CSCsm17066	Unknown	GLBP forwarders flap on SSO
CSCsm17983	Unknown	Memory corruption by l3_mgr_e7_fmask_init_platform
CSCsm19550	Unknown	sup720 rx intr should check tx descriptor exhaustion
CSCsm20994	Unknown	kron job daily reoccurences fail after new year
CSCsm21126	Unknown	C7600-SSC-400: Resync fabric interface on fabric error
CSCsm22385	Unknown	V4 VPN traffic stops after toggling agg. label between vpn-cam and tcam
CSCsm23160	Unknown	RFS: rf task attempted to unlock semaphore owned by interrupt
CSCsm24904	Unknown	Bridge-mib timing out dot1dBasePortIfIndex
CSCsm24906	Unknown	IPV6 neighbour discovery not working on SVI intf under VRF
CSCsm25061	Unknown	ike fragments dropped by vpnspace
CSCsm26063	Unknown	C2W2:Active RP Crash on sh/no sh of intf with ipv6 address configured
CSCsm26415	Unknown	Traceback seen when show platform cfm issued for fwd_vlan 0
CSCsm27017	Unknown	VS2: power configuration is not synced to standby
CSCsm28287	Unknown	Active RP crash on shutdown of GRE tunnel followed by switchover
CSCsm30584	Unknown	cwpa2 card crashes after attaching and removing service policy
CSCsm30858	Unknown	PIM register packets upmarked to TOS 6 by PTcam redirection
CSCsm31178	Unknown	policy-map stops working on a good int if wrongly applied on another int
CSCsm32363	Unknown	Netflow SLB sw-installed entries not aging out
CSCsm32493	Unknown	Backout of CSCsh94882

Identifier	Technology	Description
CSCsm33528	Unknown	Rekey packet loss for pure ipsec
CSCsm35364	Unknown	SPA-IPSEC-2G get reload automatically by RP
CSCsm37673	Unknown	Traffic from SSLM service module not going over multi-module etherchanne
CSCsm38962	Unknown	LLDP Port-ID and Port-Description TLVs are interchanged
CSCsm40606	Unknown	WS-X6724 SFP get's reboots again and again with TestSynchedFab Failed
CSCsm43962	Unknown	Cat6k L2TP packet looped through blocked port
CSCsm44309	Unknown	L2 Po - new member was not included in mapped ucast flood &mcast indices
CSCsm44413	Unknown	RP not added into LTL index when bridge-group is configured
CSCsm46017	Unknown	Process switching of ISL frame is not correct in sierra dueto CSCsl63311
CSCsm46607	Unknown	dot1q subinterface and mac-address limits on same vlan cause stadby relo
CSCsm48287	Unknown	Drop counters for VPLS VC not incrementing
CSCsm48357	Unknown	crash at line by line config sync failure while unconfig FR xconnect
CSCsm49103	Unknown	I/O Memory Leak when running show mls cef command
CSCsm49440	Unknown	RRI: Need to support remote-peer option when source proxy == peer
CSCsm50309	Unknown	Crash due to ipflow aggregation when configuring OER in border router
CSCsm51299	Unknown	Code divergence caused a need for a second fix for CSCsl27236.
CSCsm54873	Unknown	EEM some time are not triggered properly
CSCsm56279	Unknown	C2W2: Important enhancements to "test swi vir ltl index" CLI
CSCsm56293	Unknown	Sup4:DFC only mode, create bus stall condition-the switch still crash
CSCsm59384	Unknown	DPD not deleting IKE SA's
CSCsm59488	Unknown	Fix backwards compatibility for multicast egress netflow cli
CSCsm59926	Unknown	RP receives 2 copies of each PIM register with MVPN
CSCsm59949	Unknown	vtp3:with 4k vlan HA reload/sso causes the standby to reload continuously
CSCsm62179	Unknown	C2W2: MPLS pseudowire ping for SVI mode EoMPLSoGRE fails
CSCsm64424	Unknown	C2W1: Copy command generates spurious authorization requests
CSCsm66023	Unknown	IPv6 VTI RP crashed ace_reverse_map when changing tnlsrsrc from v4 to v6
CSCsm66280	Unknown	TIDP: Router crashes at tidp_find_or_add_peer
CSCsm66602	Unknown	SIP 400 loses VPLS VC entry on shutting down the MPLS TE tunnel
CSCsm66678	Unknown	Policing not working in MPLS cloud
CSCsm69112	Unknown	Multicast output drop w/ IGMP snooping @ near line rate 1Gbps
CSCsm69827	Unknown	%SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3
CSCsm70349	Unknown	BPDU traffic over Eompls is not switched on 3C system
CSCsm70707	Unknown	WS-X6748-SFP shutdown(Could not set appropriate Switching mode)
CSCsm70774	Unknown	Router crashes at cfg_kron_pley_sbmd_cmd.
CSCsm71537	Unknown	divide by 0 crash in oer_br_update_iface_counters
CSCsm72807	Unknown	DHCP packets can get corrupted in an SSO environment
CSCsm73395	Unknown	Per-User ACL install error

Identifier	Technology	Description
CSCsm73592	Unknown	Crash when removing tunnel interface.
CSCsm75020	Unknown	EARL7 Additional ECC Error Handling enhancements
CSCsm75286	Unknown	bgp route-map doesn't work correctly when deleted part of sequences
CSCsm76172	Unknown	Memory held by "mls-hal-agent" process in standby-sp
CSCsm77171	Unknown	Router crash when "ip flow" enabled.
CSCsm79344	Unknown	Bogus "TCAM MASK entry capacity exceeded" message
CSCsm81399	Unknown	No Such Instance error from many SNMP objs for 1xOC48 POS/RPR SPA
CSCsm82169	Unknown	VSS: heathland interfaces are err-disabled on standby chassis
CSCsm82264	Unknown	VS2: Entire VSS system goes down after restarting call-home process
CSCsm82382	Unknown	7600 standby RP memory leaking cause CEF disable
CSCsm82472	Unknown	DAI: L2-Portchannel formed for member's DAI trust mismatch
CSCsm82958	Unknown	radius sticky entry deleted even if the idle timer is not 0
CSCsm83893	Unknown	W2: "sh mls cef adj mpls detail" after SSO freeze RP cause T/B , reboot
CSCsm83948	Unknown	CISCO7609 returns sysObjectId as ciscoProducts.402 (which is cisco7606)
CSCsm84257	Unknown	crash in ipflow_periodic context due to watchdog timeout
CSCsm84267	Unknown	Tracebacks & %CPU_MONITOR-SP-6-NOT_HEARD: messages with NAT.
CSCsm85936	Unknown	UUT cpu at 40% with bi-dir traffic across a single tunnel
CSCsm86027	Unknown	B2B failover,ace_tunnel_compare:Invalid address_type, router crashed
CSCsm92183	Unknown	c2w1: Heathland card is not coming up due to diag failure
CSCsm92365	Unknown	c76 router loses its vlan database after configuring VTPv3
CSCsm93047	Unknown	IPSec uses incorrect SA lifetime during rekey
CSCsm93648	Unknown	C2W2:080226 Rtr crashed when moving tunnels from VTI to GRE/TP
CSCsm94421	Unknown	Configuring STP cost in an etherchannel to the default has no effect
CSCsm95456	Unknown	Duplicate L3 packets with 6708 and DEC
CSCsm96243	Unknown	Switch crashes on executing sh tcam interface acl with include option
CSCsm96610	Unknown	OOB-MAC-SYNC is on, need to change internally the cam aging to 480 Sec
CSCsm97669	Unknown	Cat6K with NAT-T through PAT: IKE packets with src_port != 4500 dropped
CSCsm97836	Unknown	Memory leak VSL Manager
CSCsm98000	Unknown	ISSU upgrade procedure takes switch into RPR instead of SSO
CSCsm98256	Unknown	Berytos got power down due to TestMacNotification and TestFabricCh0Healt
CSCsm98671	Unknown	TestTrafficStress fails with certain configuration
CSCsm99079	Unknown	kron causes CPU HOG
CSCsm99690	Unknown	Netflow: Crash with aggregation caches and export to MPLS VPN
CSCso00104	Unknown	Router crashes on aggregation-type prefix-length and ACL changes to OER
CSCso00793	Unknown	ITP-76: Flexwan Memory version "VI4DP647228EBK-MD" causes reload
CSCso00864	Unknown	Standby sup crashed on configuring local-address command for cry map
CSCso02208	Unknown	VS2: crash when provisioning LI stream

Identifier	Technology	Description
CSCso03419	Unknown	VRF_Lite aware PBR: Set ip vrf clause changes on Reload/SSO with SIERRA.
CSCso05127	Unknown	WS-X6708-10GE crashes following upgrade to 12.2(33)SXH1 and 12.2(33)SXH2
CSCso05889	Unknown	Pak Subblock creation fails from CEF in ION
CSCso05920	Unknown	cpmCPUMemoryFree incorrect for Posix memory
CSCso11489	Unknown	%SYS-SP-3-INVMEMINT while collecting ION crashinfo
CSCso11822	Unknown	LACP PC switchport, on OIR, "channel group 112 active" config gets lost
CSCso12405	Unknown	ViF multicast packets are process switched. IO mem middle buffer leak
CSCso12903	Unknown	RE MET address check missing while running MET patch on IO bus timeout
CSCso13950	Unknown	implementation of cmasModuleActionNotif in CSICO-MODULE-AUTO-SHUTDOWN-M
CSCso16532	Unknown	Entries missing from cam table with sh mac- multicast igmp-snooping cmd
CSCso18683	Unknown	IP DSCP Re-circulation not working as expected after issu runversion.
CSCso20519	Unknown	Cheronia: Fix SMB drive strength programming.
CSCso22987	Unknown	PBR requirement not met even if BRs are one-hop away through another BR.
CSCso28275	Unknown	Traffic polarization within a MEC on VSS.
CSCso28295	Unknown	MVPN Tunnel-sourced non-rpf traffic constantly dropped in software
CSCso28791	Unknown	MAC_MOVE-SP-4-NOTIF seen for L2TP packets over dot1q tunnel
CSCso29226	Unknown	IP source guard is not supported on ether channel member
CSCso30038	Unknown	A OIL is not registered properly in mroute table with static igmp group
CSCso30598	Unknown	GLBP - SSO : Stby reload continuously after switchover on c7304
CSCso30649	Unknown	vtp3:pvlans are not updated correctly on converting from off to server
CSCso31506	Unknown	IPv6 AH Extension Headers Punted to Software on PFC-3B & 3C
CSCso32193	Unknown	IPv6 software switched in Egress replication mode
CSCso37640	Unknown	DHCP snooping ACL's are not getting programmed after switchover.
CSCso38151	Unknown	Error/Traceback after power fail. %SPA-3-SW_ERROR: spa_get_card_info:
CSCso38671	Unknown	VS specific message seen on Sup32 image when "erase startup-config"
CSCso39444	Unknown	The new Active supervisor will crash after SSO @ fib_path_list_lock_memo
CSCso39518	Unknown	fh_policy_dir.proc process crash when activate 0E patch
CSCso39818	Unknown	Ingress Marking not working on SIP-600 on linecard reset/ toggle mlsqos
CSCso40891	Unknown	Stb rp reloaded during every bootup, process = FM, fm_free_platform_data
CSCso43539	Unknown	power converter failure reported before power was on
CSCso44072	Unknown	High CPU due to multicast traffic getting punted to software
CSCso45104	Unknown	PfR: Incoming Optimization BGP not working for connected routes on BR
CSCso46210	Unknown	VS: NAM on Standby switch not able to configure SPAN session
CSCso46337	Unknown	%MFI-SP-3-MFICOMM: un-matched frr_cutover_cnt after SSO switchover
CSCso49344	Unknown	Egress policing policy not programmed in SIP-600 after system reload.
CSCso50175	Unknown	% ENT_API-4-NOPORT: Traceback seen after switchover
CSCso50383	Unknown	Packet drops at TE/FRR tunnel disposition after node failure

Identifier	Technology	Description
CSCso50779	Unknown	The interface does not linkup if "speed nonegotiate" is configured
CSCso52097	Unknown	IPV6 :Missing second Netflow shortcut after route change
CSCso53557	Unknown	linecard crash @ lc_remove_vc_policy when removing and reapplying wred
CSCso53741	Unknown	VPNSPA does not handle duplicate IPSec SA correctly in nested tunnel
CSCso54131	Unknown	After SSO BPDU are being dropped
CSCso55072	Unknown	Crash occurs during execution of TCL code in ESM handler
CSCso57020	Unknown	VSS: After sso, the RBH values on orphan PO flips w/o link/po flapping
CSCso57886	Unknown	unrestricted while loop when looking for EOS flag in the packet
CSCso59288	Unknown	On enabling oob, aging is changed to 3 times is not shown in cli output
CSCso60063	Unknown	Router crash @ dot1x_credential_deconfig_password
CSCso60528	Unknown	C2W2: FWSM - Standby FWSM PO shows down and links go down eventually
CSCso62526	Unknown	c7600 RSP720: stdby RSP relods upon no flow-sampler interface commad
CSCso63263	Unknown	Bogus IPC-5-WATERMARK: 988 messages pending in xmt for the port
CSCso65821	Unknown	wrr-queue map configuration propagates to all ports on a 6408
CSCso66357	Unknown	Classification on nbar fails on removing pmap from other pvc on ATM M2P
CSCso68840	Unknown	eou inactivity timer over rides reauth timer from ACS
CSCso69601	Unknown	Dynamic MAC address added for port in port security violation
CSCso71355	Unknown	PVLAN - 6500 - Multicast flood broken from pvlan port to promiscuous
CSCso71955	Unknown	Alignment errors with netflow on Interface, crash on 7600/6500
CSCso72178	Unknown	W2:TestCapture,TestTrap & TestIPv6FibShortcut diag failed ondemand&boot
CSCso72250	Unknown	Incorrect color for SYSTEM led of Active and Standby sup in VS mode
CSCso72541	Unknown	%MFIB_STATS-DFC2-2-MFIB_STATS_LC_FAILED_GET_COUNTERS for Sip 600
CSCso74559	Unknown	C2W2: Mago IOS "test Crash" create crashinfo file on bootflash only
CSCso74909	Unknown	Router crashes when show ip access-list <access-list-name> expand
CSCso81632	Unknown	Manipulating Service Module span session causes high cpu
CSCso82039	Unknown	C2W2: Active console is getting locked for 2.5 mins during sso.
CSCso84567	Unknown	6500 with WCCP and CoPP punts non-TCP packets into CoPP policy.
CSCso85133	Unknown	DOM tranceiver "voltage" values are always Zero in SUP4
CSCso85859	Unknown	RP crashes when using 'show memory detailed'
CSCso85908	Unknown	Windows client behind nat using ipsec over l2tp failed at rekey
CSCso86544	Unknown	Afer SSO, new active SP crashes @ pm_vlan_get_portlist
CSCso87083	Unknown	vtp3:crash @vlanmgr_db_get_vlist_ptr on 'test sw-vlan show nvfile'
CSCso87348	Unknown	Corruption in subflow code
CSCso87838	Unknown	HSRP: with aggressive timers HSRP peer flaps when "wr mem"
CSCso88042	Unknown	Wism module Allowed-Vlan statements lost on reload
CSCso88772	Unknown	sp-inband tx capture causes primary SUP to hang
CSCso89823	Unknown	Pos interface "rxload" and "input bytes" counters incorrectly increment

Identifier	Technology	Description
CSCso97593	Unknown	MCP:qos config loss after MCP reload
CSCso98143	Unknown	Router crash at pm_platform_private_alloc_and_reserve_vlan
CSCsq00884	Unknown	"mls qos trust" cmd lost under port-channel interface when upgrading IOS
CSCsq01879	Unknown	7600 EoMPLS mls cef entry for imposition is programmed mtu 0
CSCsq03475	Unknown	W2: Memory corruption caused by env object after being freed.
CSCsq04075	Unknown	C2W2:DHCP Snooping entries not cleared after removing IP Source Guard
CSCsq04274	Unknown	Memory leak observed on l2_vlan_stat_mem_allocate during vlans creation
CSCsq04355	Unknown	Fix in CSCso81632 is not complete
CSCsq04673	Unknown	SIGSEGV in ios-base and syslog_pubinfo_enqueue
CSCsq06208	Unknown	HM gold policy should not trigger again after crossing the threshold
CSCsq09228	Unknown	CHSTM1 SPA: Linkup/down traps not generated and snmp set not working
CSCsq14726	Unknown	SIP200_MP-4-TIMEOUT: Master CPU request timed out
CSCsq15308	Unknown	timer not stopped properly for eem policy scripts
CSCsq17712	Unknown	In RPR, ISSU rollback feature is broken in SRC throttle.
CSCsq19146	Unknown	FPD creation for new pegasus rx (1.6) FPA image for Sip-1 CR
CSCsq20970	Unknown	ATM option missing, while configuring T1 controller for mode atm
CSCsq21051	Unknown	W2: Heathland mode change doesn't work after the second SSO switchover
CSCsq31935	Unknown	6500 - L3 port channel - CDP packet sent tagged in internal vlan
CSCsq33458	Unknown	IOS new IKE sa uses DOI of zero when ipsec sa already exists
CSCsq34245	Unknown	IPC Open Port Errors observed with SIP-400
CSCsq36972	Unknown	Portchannel does not form. Log messages indicate misconfig.
CSCsq37376	Unknown	Packet Buffer Capture May Crash a 6500 in IOS
CSCsq39079	Unknown	SPA-IPSEC-2G Crash under load due to IKE session establishment
CSCsq39254	Unknown	Call-home: Standby sup reloaded after removing and adding profile
CSCsq41048	Unknown	Dot1x crashed at eap_peer during dot1x authentication of 350 hosts
CSCsq44850	Unknown	c2w2 : TB seen at %PM-3-INTERNALERROR: Port Manager Internal Software Er
CSCsq46327	Unknown	Ca6k SXH : 2 crypto maps in same redundant standby grp: RRI not deleted
CSCsq46590	Unknown	Packet loss during SSO failover on ECMP supervisor uplinks
CSCsq46854	Unknown	EEM applet patterns do not properly handle escape sequences
CSCsq47140	Unknown	67xx module may not come online
CSCsq47305	Unknown	High CPU on SP when both VSL PO are source interface
CSCsq47774	Unknown	CDP send on internal vlan over L3 Etherchannel after reload
CSCsq48271	Unknown	adding redundant CSM causes config sync to indicate in sync when not
CSCsq51231	Unknown	ALIGN-3-SPURIOUS: Spurious memory access made @ idbman_get_port_swidb
CSCsq51378	Unknown	ATM PA Interface shows up/up after force redundancy, no cables connected
CSCsq52836	Unknown	vtp3:VLAN db is lost upon TLB(translational bridge) config
CSCsq53085	Unknown	VS: 15 seconds down time upon module reset

Identifier	Technology	Description
CSCsq53822	Unknown	Monitor session removal may affect traffic through WS-X6148A-RJ-45
CSCsq56747	Unknown	Active SP CPU 100% after SSO switchover with 080527 Modular IOS image
CSCsq59297	Unknown	port-channel IDB gets mixed up
CSCsq60553	Unknown	Create cwslc-rommon3.bin for cwp2 to accomodate release Rommon (1.8)
CSCsq61089	Unknown	VS2: physical OIR of 6708 causes 16 seconds interruption
CSCsq62351	Unknown	C2W2:SUPW: GOLD EEM cannot crash switch immediately as recovery action
CSCsq62537	Unknown	W2: Span destination with MEC port sends duplicated traffic
CSCsq63041	Unknown	Unable to configure xconnect in FE interface - command rejected
CSCsq63681	Unknown	c7600 Router crashing due to freed pointer in cfib invoked by Netflow
CSCsq64011	Unknown	VSS: Traffic from standby switch to active with RBH = 0x0 dropped
CSCsq67001	Unknown	Standby switch reloaded by auto qos on MEC standby member port
CSCsq73317	Unknown	MAB authorization failed with port-security
CSCsq74300	Unknown	Set interface change for CSCsk63775 needs to be backed out
CSCsq75704	Unknown	FW2 FE PA Interface stays up/down with no conn and goes up/up after sso
CSCsq77043	Unknown	EEM long hostname prevents tcl cli_open from functioning
CSCsq77381	Unknown	W2: Diag - TestL3Capture2 failed after LV-SSO
CSCsq77464	Unknown	mls rate-limit unicast cef receive value re-written upon TCAM exception
CSCsq78513	Unknown	VSS: Etherchannel counters incorrect
CSCsq78538	Unknown	ISSU: runversion/commitversion fails when specifying sup-bootdisk:
CSCsq78956	Unknown	strcpy of binary can cause mem corruption
CSCsq79253	Unknown	Pinnacle interrupts not re-enabled after memory inconsistency detected
CSCsq80270	Unknown	Cat 6k crashes randomly after IPSec SPA module is inserted.
CSCsq80891	Unknown	VSS switches reload at the same time after VSL link failure
CSCsq81116	Unknown	c2w2:Device crash @ oer_cc_free_message while unconfiguring
CSCsq81235	Unknown	Cannot configure a vrf again when deleted using 'no ip vrf' command
CSCsq81576	Unknown	Outcome of 'exception switch' commands may be unexpected.
CSCsq82663	Unknown	SLB router CPU usage is high with GE interface
CSCsq82991	Unknown	IPSG Pacl entry appears after the ISSU RV or SSO
CSCsq83789	Unknown	LTL for unknow unicast is wrongly programmed for some L3 interfaces
CSCsq84116	Unknown	Cisco 7604 with OC3, Flexwan crashes into ROMMON
CSCsq84757	Unknown	(ha cfg-sync issue)ERSPAN config gets disabled after RP switchover
CSCsq85139	Unknown	VS2: Can not establish session to standby NAM
CSCsq89415	Unknown	"no bert" indicates "abort request" instead of "stopped"
CSCsq90487	Unknown	ME6524 running modular IOS images require 512 MB DRAM in SP in SXH3
CSCsq91258	Unknown	L2 entry purged from hardware when in use by L3 shortcut
CSCsq91788	Unknown	Router crashes while loading configs (from TFTP) thro' VTY.
CSCsq94036	Unknown	Packets are hardware switched after applying ip precedence

Identifier	Technology	Description
CSCsq94068	Unknown	Archive Configuration gets out of sync when files are manually deleted
CSCsq94136	Unknown	Burst of traffic cause anti-replay check to fail
CSCsq94150	Unknown	VSS system crash on show command during the initial conversion
CSCsq94366	Unknown	Mem leak in rrp_update_peer_info_on_rp
CSCsq96843	Unknown	SIP-400 ISSU crash after inserting SPA
CSCsq97640	Unknown	Resetting Standby Sup4 multiple times causes lincecard switchbus timeout
CSCsq98887	Unknown	Packet drop on applying and removing ACL on tunnel interface with pim
CSCsr02723	Unknown	MDEBUB:Spurious memory access detected at env_sensor_get_update
CSCsr02816	Unknown	ISSU tracebacks seen on SP during runversion at MsgReceive.S:14
CSCsr06037	Unknown	the monitor session source is removed by deleting sub-interface
CSCsr06914	Unknown	fm_slb_inbad_send():Invalid Flowmask errors upgrading to 12.2(33)SXH2a
CSCsr08482	Unknown	PM support to program ethertype to all ports when port-group in mux mode
CSCsr08985	Unknown	CMM ports going to shutdown state on reload in Whitney 1
CSCsr09554	Unknown	Move SIBYTE SB_RMON_OVRFL messages under debug
CSCsr12976	Unknown	High CPU in ION ios-base process
CSCsr13633	Unknown	%PM-3-INTERNALERROR: Port Manager Internal Software E
CSCsr17564	Unknown	Traceback errors seen when applying 2-level policy on a ATM VC
CSCsr18924	Unknown	kernel idle hook thread in IOS-Base taking 50% CPU
CSCsr20679	Unknown	VSL PO as SPAN source and Orphan PO as SPAN destination not allowed
CSCsr26663	Unknown	C2W2: GLBP 800 peers with default timers flap after SSO
CSCsr27735	Unknown	Tracking feature not monitor IP SLA state after boot up
CSCsr28305	Unknown	Packet drops on L2 portchannel on WS-X6708-10G
CSCsr39272	Unknown	%DATACORRUPTION-1 due to spa sensor temp overrunning buffer
CSCsr44005	Unknown	network-rf should count virtual interfaces when calculating expected sw
CSCsr44967	Unknown	EEM multi-event Tcl policies fail to register
CSCsr45495	Unknown	PBR with deny statements : TCAM running out of masks
CSCsr45851	Unknown	ifOperStatus for Control Plane Interface is always down
CSCsr45961	Unknown	PRE2: GE ARP issue following a PRE switchover
CSCsr46367	Unknown	EEM mutli-event Tcl policies with all track trigger confuses EEM
CSCsr48938	Unknown	UNBL:bootldr image can't boot on SupW
CSCsr49669	Unknown	Match protcol arp doesnt work in whitney1 earlier it was working for Roc
CSCsr51799	Unknown	pa-mc-8t1 interface down after stopping BERT prematurely
CSCsr55523	Unknown	WCCP service group ID is zero in ACL TCAM Adjacency
CSCsr57615	Unknown	Need to add a config command to turn off/on FEFI for IOS
CSCsr58773	Unknown	VS2: After SSO, VSL member stuck in "w" state, and MEC errors
CSCsr66588	Unknown	Netflow SLB aging parameter values are not synced to SP after reload
CSCsr72427	Unknown	WS-X6148-45AF/WS-F6K-FE48-AF %ILPOWER-5-ILPOWER_MISCONFIG after reload

Identifier	Technology	Description
CSCsr72674	Unknown	RP crash seen @ ipmulticast_tunnel_load_split_tdp_send_hello_packet
CSCsr75094	Unknown	MDEBUG: Spurious Memory Access on SSO
CSCsr78910	Unknown	time not updated in 'System returned to ROM by reload' in show version
CSCsr80601	Unknown	ISAKMP SA not deleted as Expected UUT
CSCsr81962	Unknown	C2W1: Monitor session servicemodule causes internal loop on SUP720-10GE
CSCsr91190	Unknown	IP multicast SSO compatibility required in images with no PIM SSO subsys
CSCsr93467	Unknown	c2w2:Traceback seen while doing "switch accept mode virtual "
CSCsr94563	Unknown	EEM: Policy fails to unregister with unkown event ID error
CSCsr96283	Unknown	High CPU due to add/del SPAN configs
CSCsr97097	Unknown	VS: RP IPC-5-WATERMARK msgs due to CARD_RESET, after SSO
CSCsr99560	Unknown	cos2exp policy not working for VPLS SVI after OIR
CSCsr99933	Unknown	FWLB: High purge rate causes CPU to increase by 15%
CSCsu00487	Unknown	Cat4500 MAB failure on random stack ports
CSCsu03297	Unknown	RE: Fabric force bus-mode does not work anymore
CSCsu03772	Unknown	Dot1q native vlan tagging is not working with "switchpot nonegotiate"
CSCsu05800	Unknown	C2W2: need to extend the wait time for bus sync after sso
CSCsu24825	Unknown	SUP32 unstable to communicate with all neighbors after reload
CSCsu27109	Unknown	When SSO is performed on 7600, mpls label allocation fails.
CSCsu27660	Unknown	CDP packet sent tagged in internal vlan
CSCsu29117	Unknown	PE send traffic back to EoMPLS tunnel after lsp path changed
CSCsu31444	Unknown	OER Fails to create active Jitter Probes due to IP SLA Error
CSCsu31651	Unknown	VSS: Traffic dropped on non-bundled port if RBH=0
CSCsu33707	Unknown	Multicast traffic will not stop after PIM prune
CSCsu37481	Unknown	Netflow Incorrect Octet value with packet-based sampling
CSCsu39704	Unknown	Command "pseudowire" rejected at Virtual-PPP interface
CSCsu48150	Unknown	Enhancement to Me_Kr register dumps from CSCsg21809
CSCsu49002	Unknown	ciscoIpMRouteBps sometimes indicates wrongful value
CSCsu51875	Unknown	c2w2: Router crashes at fib_upd_record_deleting
CSCsu55145	Unknown	ASR Crash Due To Memory Corruption
CSCsu57958	Unknown	DHCP-Snooping not intercepting DHCP messages from the Server
CSCsu59556	Unknown	Traceback seen @ fibidb_init
CSCsu63335	Unknown	"Failed to find process pid" error message on 12.2(33)SXH3
CSCsu64581	Unknown	Last port of T3/E3 SPA connected back to back does not ping
CSCsu68698	Unknown	No syslogs and stack on console when SP crashes due RP boot timeout
CSCsu69177	Unknown	C2W2: Traffic drop after SSO on SUP4 P router w/ IP and MPLS traffic
CSCsu72884	Unknown	Modifying match criteria frm v6 to v4 doesnt change team label state
CSCsu73128	Unknown	C2W2-ION-080922: Crash on Plain IPSec tunnel setup

Identifier	Technology	Description
CSCsu76070	Unknown	duplicate packets when lawful intercept is enabled
CSCsu78109	Unknown	Intermittent HM test failures showing in SEA log
CSCsu94350	Unknown	C2w2:Not able to change the replication mode with latest sierra image
CSCsu94880	Unknown	Bus error crash at fm_format_inband_adj_data
CSCsu99270	Unknown	CPUHOG observed when configuring more vlan interfaces
CSCsv30359	Unknown	HSRP: CPU hog when no failover bound to crypto
CSCsv34415	Unknown	Diag failure on power-cycle puts VSS switches in rommon
CSCsv43802	Unknown	High CPU utilization triggers crash in diags.
CSCsj89931	Voice	Standby router resets due to parser return error
CSCso89692	Voice	tcl via EEM crashes IOS
CSCsg84658	VPDN	CISCO-VPDN-MGMT-EXT-MIB Bad Month and Day Timestamp
CSCsh93436	VPDN	L2TP in ION image may not work properly
CSCsi25578	VPDN	LNS rejects L2TP ICRQ with same session ID as existing session
CSCsj12579	VPDN	LAC crashes when configured with l2tp ignore tx-speed
CSCsj47108	VPDN	l2tp tunnel password 7 is always in the vpdn-group config
CSCsk26165	VPDN	A router may crash when configured for L2TP
CSCsl87404	VPDN	L2TP tunnels are not getting established with PPPoE Relay
CSCsm62033	VPDN	Call Serial Number AVP is not RFC complaint and is marked as mandatory
CSCso12748	VPDN	Mandatory of Message Type AVP for SCCRQ is FALSE
CSCso56185	VPDN	SCCRQ has M-bit set to 0 in Receiving Window Size AVP
CSCsq52048	VPDN	Router crash with traceback decode: l2tp_l2x_cc_get_clear_cntrs
CSCeg65084	WAN	FR DLCI with ppp virtual-template config is lost after reboot
CSCek71844	WAN	VTEMPLATE: Cloning from vprofile fails
CSCsb88464	WAN	FR IF-MIB: ifLastChange not updated on FR/MFR encap sub Intfs (SPA/PLIM)
CSCsc67488	WAN	ARP Req from Frame Relay causes %IP-4-ZERO_ADDR: Zero MAC address Error
CSCsg32308	WAN	copy/paste of ntp-authentication-key statement is not possible
CSCsh92709	WAN	Wrong mode being output in show users command
CSCsi56413	WAN	PA-POS-OC3SMI interface output stuck .
CSCsj68446	WAN	NTP will not sync - NTP packets received but ignored by NTP process .
CSCsl90285	WAN	POS-APS: CWPA-3-NODISPATCH messages seen when configuring APS
CSCsq18856	WAN	FR SVCs cannot be setup

Caveats in Release 12.2(33)SXH and Rebuilds

- [Open Caveats in Release 12.2\(33\)SXH and Rebuilds](#), page 247
- [Caveats Resolved in Release 12.2\(33\)SXH7](#), page 247
- [Caveats Resolved in Release 12.2\(33\)SXH6](#), page 259
- [Caveats Resolved in Release 12.2\(33\)SXH5](#), page 265
- [Caveats Resolved in Release 12.2\(33\)SXH4](#), page 276
- [Caveats Resolved in Release 12.2\(33\)SXH3a](#), page 286
- [Caveats Resolved in Release 12.2\(33\)SXH3](#), page 288
- [Caveats Resolved in Release 12.2\(33\)SXH2a](#), page 295
- [Caveats Resolved in Release 12.2\(33\)SXH2](#), page 296
- [Caveats Resolved in Release 12.2\(33\)SXH1](#), page 301



Note

- The caveat information is updated frequently.
- If you have a Cisco.com account that supports access to the Bug Toolkit, you can search for the most current Release 12.2SX caveat information at this URL:

<http://tools.cisco.com/Support/BugToolkit/action.do?hdnAction=searchBugs>

Open Caveats in Release 12.2(33)SXH and Rebuilds

Identifier	Technology	Description
CSCtb69049	Unknown	Modular IOS "exception kernel filepath ..." options are ambiguous.

Caveats Resolved in Release 12.2(33)SXH7

Resolved AAA Caveats

- [CSCsg21398](#)—Resolved in 12.2(33)SXH7

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

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

Workaround: There is no workaround.

Resolved Multicast Caveats

- [CSCsl32142](#)—Resolved in 12.2(33)SXH7

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

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

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

- [CSCtc68037](#)—Resolved in 12.2(33)SXH7

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

Conditions:

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

Resolved Security Caveats

- [CSCsz32366](#)—Resolved in 12.2(33)SXH7

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

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

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

“crypto key zeroize rsa”

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

- [CSCsg65318](#)—Resolved in 12.2(33)SXH7

Symptoms: Malformed SSH version 2 packets may cause a memory leak.

Conditions: This symptom is observed on a Cisco platform configured for SSH version 2 after it has received malformed SSHv2 packets. The impact of this flaw is that the affected platform may operate in a degraded condition. Under rare circumstances it may reload to recover itself.

Workarounds: Options consist of using SSH version 1 in the interim until the affected platform can be upgraded to a fixed release or permitting only known trusted hosts/networks that can connect to the router by using a VTY access list.

Following are examples of the workarounds:

Configure SSH version 1

```
Configure SSH version 1
+-----
!-- configure from global config mode
!
config t
!
ip ssh version 1
end

VTY access-list
+-----
!-- 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
```

More information about configuring VTY access lists is available in Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T Controlling Access to a Virtual Terminal Line:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cntrl_acc_vtl_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1049991

More information about SSH on IOS is available in the Configuring Secure Shell on Routers and Switches Running Cisco IOS guide:

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

Resolved Unknown Caveats

- [CSCtc41760](#)—Resolved in 12.2(33)SXH7

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

Traceback will vary from code to code.

Conditions: UDLD configured

Workaround: Disable UDLD.

- [CSCtc49782](#)—Resolved in 12.2(33)SXH7

Symptoms: Upgrade from 12.2(18)SXF6 to 12.2(33)SXH5 introduced additional vty lines to the running-configuration (vtp line 5 - 15). These new lines do not inherit the security ACL or transports configured by the customer on the old lines (0-4). Switch upgrade caused device to be non-compliant with network security policy defined by customer.

Condition: Software upgrade from 12.2(18)SXF6 to 12.2(33)SXH5.

Workaround: We have to manually configure the ACL for those newly introduced vty lines.

- [CSCtc71597](#)—Resolved in 12.2(33)SXH7

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

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

Workaround: No Workaround

- [CSCtc83104](#)—Resolved in 12.2(33)SXH7

Conditions: When an ipv6 RACL is configured on an interface. All packets containing ipv6 optional headers are punted to RP. But if any packets that are sent with no L4 header are also hitting this punt entry present at the top of tcam.

Workaround: No Workaround:

- [CSCsh61458](#)—Resolved in 12.2(33)SXH7

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

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

Workaround: Do not enable the DNSIX audit trail.

Resolved WAN Caveats

- **CSCtd75033**—Resolved in 12.2(33)SXH7

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
router#
```

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 Reference Guide” at the following link:

<http://www.cisco.com/warp/public/620/1.html>

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

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

- NTP Access Group

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

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

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

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

- Infrastructure Access Control Lists

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

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

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

```
!---
!--- Feature: Network Time Protocol (NTP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
```

```

INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!--- via the interface command "ntp broadcast client"
!--- then broadcast and directed broadcasts must be
!--- filtered as well. The following example covers
!--- an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!--- via the interface command "ntp multicast client"
!--- then multicast IP packets to the mutlicast group must
!--- be filtered as well. The following example covers
!--- a NTP multicast group of 239.0.0.1 (Default is
!--- 224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.

access-list 150 deny udp any
INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations. Permit all other traffic to transit the
!--- device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example
!--- shown)

interface fastEthernet 2/0
    ip access-group 150 in

```

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

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

– Control Plane Policing

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

—Filtering untrusted sources to the device.

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

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

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    any eq 123

!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 123

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
    match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
    class drop-udp-class
        drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
    service-policy input drop-udp-traffic
```

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

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

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

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
    match access-group 150
```

```

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
!--- appropriate traffic rates

policy-map rate-udp-traffic
  class rate-udp-class
    police 10000 1500 1500 conform-action transmit
    exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
  service-policy input drop-udp-traffic

```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlmt.html

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

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

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

Other Resolved Caveats in Release 12.2(33)SXH7

Identifier	Technology	Description
CSCsi54201	AAA	IDMGR-3-INVALID_ID error message
CSCsq71492	AAA	IOS device crash or tracebacks at tplus_handle_req_timeout
CSCsx15897	AAA	Cisco 3800 shows symptoms of memory leak in AAA component
CSCsy55362	AAA	Unresponsive Console/VTYs
CSCtc27153	ATM	Shaping configuration does not work in SXH
CSCei86912	Infrastructure	Router reloads unexpectedly while issuing GD commands
CSCin66315	Infrastructure	Inconsistency with sysuptime and rttMonLatestRttOperTime
CSCsj27963	Infrastructure	Need graceful handling of full nvram
CSCsk85192	Infrastructure	copy command with : after attribute is not checked against ACS. .
CSCsl52962	Infrastructure	interface range Port-channel command causes RP crash
CSCsm80522	Infrastructure	Zero size crash file generated with "test crash" on Sip 600 module
CSCso40612	Infrastructure	7600 HA router crashed @ parser_syntax_cleanup on
CSCso48834	Infrastructure	ip sla config with udp-jitter probe failed due to no connection

Identifier	Technology	Description
CSCso56916	Infrastructure	persistent variable "snmpboot" don't get incremented after reload
CSCse59109	IPServices	high CPU usage when IP SLA is enabled
CSCsi99841	IPServices	vrf-aware trustpoint authentication/enrollment doesn't work
CSCsm52759	IPServices	% Internal software error: 22 seen on telnetting to ipv6 hosts
CSCsz72591	IPServices	Router configured as a DHCP client crashes with crafted DHCP packet.
CSCsz97239	IPServices	PmtuAger Expiration and MSS value
CSCtc55616	IPServices	RSA key generation from SSH session disables SSH service in ION
CSCtd13820	IPServices	Show Standby causes unexpected exception to CPU: crash at standby_show
CSCtd32285	IPServices	No nat translation with PAT applied on VRF interfaces
CSCsc62963	LAN	Have configurable MTU Range 1500 -1530 on PA-1FE and PA-2FE
CSCsz05918	Management	CDP neighbors do not come up on vlan interface
CSCsz75221	Management	A local variable in cdp takes up 2k process stack space-prompting crash
CSCtc40711	Management	next-hop verify-availability still forwards traffic with no CDP neighbor
CSCtd43540	Management	Memory leak at cdp_handle_version_info
CSCtb76828	Multicast	%SYS-2-BADSHARE: Bad refcount in datagram_done for MSDP process
CSCsm42477	QoS	Sierra:Standby reloaded on QOS configuration.
CSCso29025	QoS	Sip-400: Traceback msgs at process_ok_to_reschedule
CSCsq11897	Routing	Spurious memory seen at idb_get_ip_addrs and idb_get_ip_unnum
CSCsq13111	Routing	7609s vlan traffic reporting
CSCsq99447	Routing	When BFD/ EIGRP configured in more than 32 vrf BFD does not come up
CSCsr05431	Routing	After SSO, cef removed vrf routes before bgp graceful timers time-out
CSCsr67177	Routing	Router with IPv6 OSPF crashes on reloading
CSCsr84530	Routing	Static route not properly redistributed into BGP -- backout CSCsl92283
CSCsr88705	Routing	BGP route getting lost after "shut/no shut" of BGP peering interface
CSCsw30941	Routing	ospfNbrStateChange trap sent by non-DR
CSCsw99768	Routing	BGP malformed update sent
CSCsy58115	Routing	Continuous BGP mem increase with non established neighbors
CSCsz61156	Routing	NH is not stored in BGP table when IPv6 VRF is redistributed
CSCta07104	Routing	Config-Sync & Traffic failure in VPN SSO scripts
CSCta08632	Routing	ISIS topology broken after Sup force-switchover with ispf
CSCtb82674	Routing	IS-IS adjacency stays down after switchover
CSCtc45716	Routing	SNMPWALK of ipRouteEntry.7 with a view configured triggers high CPU
CSCtd73256	Routing	a catalyst switch may reload unexpectedly during 'show ip ospf int'
CSCte10790	Routing	c6500: device crashing on "no 250" on access-list
CSCse31829	Security	Memory leak in Crypto IKMP process
CSCsz83570	Security	SSH Sessions disconnect when viewing logs w/ pagers
CSCtc12312	Security	PKI may get stuck after 32678 CRL fetches

Identifier	Technology	Description
CSCsb95192	Unknown	RRI with HA doesnt populate the routes correctly - static keyword
CSCsk18794	Unknown	speed and negotiation configuration issue on FE-TX-V2 SPA
CSCsk49041	Unknown	crypto_ikmp_utils.c: possible Invalid Pointer Read
CSCsk66851	Unknown	*,G/m entry does not have OIF programmed in HW sometimes
CSCsk86410	Unknown	Abnormal ISAKMP traffic caused an alignment error and traceback.
CSCsl30308	Unknown	PIM snooping corrupts PIM RPF Proxy packet
CSCsl70542	Unknown	OBFL:high cpu during interrupt coalesce
CSCsl87677	Unknown	changing the access vlan doesn't reflect the vlan of the secure configur
CSCsm40013	Unknown	Multiple LC crash after shutting down TE tunnel interface
CSCsm63524	Unknown	SUP32 crashes due to SP hang when it recovers from errdisable
CSCsm96309	Unknown	OIR-SP-4-WARN message displayed when PS1 or FAN removed
CSCsq01879	Unknown	7600 EoMPLS mls cef entry for imposition is programmed mtu 0
CSCsq63621	Unknown	SPD classifies OSPF IP Precedence 0 as priority
CSCsr09586	Unknown	Remarks not appearing correctly in Policy Based ACL
CSCsr50134	Unknown	Router or Linecard may reload at cv6_6pe_frr_stats
CSCsr74002	Unknown	7600 - VPLS - QinQ- UDLD packet received on qinq flooded to vpls
CSCsu31088	Unknown	Not able to execute any commands under intf after running SPA FPGA bert
CSCsu72935	Unknown	C2W2B: memory corruption on 122-32.8.11.XIW20 (w2_x_pi) image
CSCsu84213	Unknown	RPF-MFD hardware entry is missed after doing SSO.
CSCsu99813	Unknown	C2HD1-SI:Span Distributed Stops Traffic - Centralized Duplicates
CSCsv13243	Unknown	BFD config causing BGP session to go down
CSCsv40523	Unknown	WISM: Gig interfaces show as unknown(4)
CSCsv43187	Unknown	120seconds after SSO, Some multicast traffic drops
CSCsw40790	Unknown	SNMP Loop on PA-MC-T3+ interfaces (Installed)
CSCsx65705	Unknown	router crash on no route-map with match ipv6 address access-list
CSCsx74064	Unknown	On modular IOS, SSH on VRF int is allowed irrespective of vrf-also key
CSCsx79379	Unknown	IOS Auth Proxy HTTP may lead to bus error adress 0x0
CSCsy04594	Unknown	Vlan interfaces flap when a root guard port receive superior bpdu
CSCsy37236	Unknown	High CPU at Filesys process on DFC LC and crash at btree_map_search
CSCsy54583	Unknown	TTY data process on DFC leaks memory at prot_tty_malloc_named
CSCsy56433	Unknown	Sh rom intermittently fails to display correct region info for standby
CSCsy58553	Unknown	Linecard reset causes traffic onto frr protected tunnel to be dropped
CSCsy66446	Unknown	%BIT-SP-4-OUTOFRANGE ltl_fpoef_defer_notify_with_pri on port-channel flap
CSCsy66678	Unknown	stp_helper_manipulate_queue: standby SP CPUHOG
CSCsy81934	Unknown	Non-standard static multicast MAC addresses lose ports after reload
CSCsy86252	Unknown	SP Crash printing "supervisor jamming EOBC. It will be disabled."
CSCsz04297	Unknown	Cat6k: False Dynamic MAC entry is installed with format 0000.<LTL>.0000

Identifier	Technology	Description
CSCsz19246	Unknown	Crash after 'no dot1x port-control auto'
CSCsz36826	Unknown	6509E fan-tray failed to restore back to HP mode after OIR
CSCsz38798	Unknown	On SSO, Sup engine/DFC module get reset when MET set deleted
CSCsz53124	Unknown	IPSEC VPN interoperability issue when IPCOMP compression enabled
CSCsz53809	Unknown	Configuring vlan name containing space doesnt work across reload.
CSCsz69993	Unknown	Pause frames on WS-X6708-10GE sent to cpu with flow-control disabled
CSCsz96469	Unknown	Tracebacks seen @chunk_free_with_pc while unconfiguring
CSCta06428	Unknown	VSS: Active Crash at iccp_test_get_first_mcast_resp_data
CSCta06451	Unknown	PfR:BR Memory leak in export path on 7600
CSCta15851	Unknown	Changing allowed vlan mask causes WiSM LAG member ports to reset
CSCta29818	Unknown	Enhanced-Flexwan Module Power Down after Code Upgrade from SXF to SXH
CSCta42669	Unknown	C2W1: segv exception after portchannel configuration
CSCta45976	Unknown	BFD adj not formed if NBR IPaddr is on the same RTR but w diff VRFintf
CSCta56676	Unknown	IPsec SA lifetime can go to negative values
CSCta56890	Unknown	WiSM LAG and Data Ports flaps on SSO Switchover
CSCta71873	Unknown	Mcast traffic stops flowing across fabric to required fpoes
CSCta95295	Unknown	IOMEM depleted when PKI servers unavailable for CRL checking
CSCta98108	Unknown	With NAT, on Netflow database cleanup timer expiry, CPU spikes on 7600
CSCtb04231	Unknown	Imprecise parity error crash due to mistral timeout
CSCtb31400	Unknown	BGP sends Route-Refresh request on entering route-map configuration
CSCtb45475	Unknown	sh plat hard capacity cpu report system memory usage incorrectly
CSCtb62031	Unknown	cat6k: High cpu and high inband when reflexive ACL is used with WCCP
CSCtb70578	Unknown	L2PT incorrectly decapsulates STP PDU for RSPAN causing PVID mismatch
CSCtb72638	Unknown	Ezvpn server not sending split tunneling access-list to client
CSCtb78973	Unknown	PM-SP-3-INTERNALERROR: Port Manager Internal Software Error with dot1x
CSCtb84298	Unknown	Shadow state of wism PO line protocol down on stdby After OIR of WiSM
CSCtb87149	Unknown	NF is disabled on L3 sub-intf with per interface NF enabled
CSCtc11691	Unknown	VSS: Switch crashes after loading the sierra 090920 image
CSCtc15386	Unknown	IOS tags VLAN name configuration command as level 1
CSCtc16740	Unknown	Global BPDUGuard does not work on MVAP ports
CSCtc17058	Unknown	VC stops sending traffic due to duplicate vpn id in port based EoMPLS
CSCtc22217	Unknown	SPA-8X1FE-TX-V2 negotiation auto and duplex mode issue
CSCtc24864	Unknown	Enable cdp - removed on shut/ no shut dot1q-tunnel interface
CSCtc27745	Unknown	LLDP packets go out tagged if native vlan (not Vlan1) is configured
CSCtc30691	Unknown	Crash/Spurious memory access on privilege ipaddr-object-group/port-objec
CSCtc38716	Unknown	ME6524 may reset due to single power supply failure
CSCtc38771	Unknown	12.2SXH: Intermittent BPDU drop over Dot1Q tunnel.

Identifier	Technology	Description
CSCtc40724	Unknown	Multicast packets may get dropped on 6500 when member join mcast group
CSCtc40851	Unknown	traceback on applying port acl to interface.
CSCtc49542	Unknown	VSS: output drops on VS-720 port due to CoS mapping mismatch
CSCtc52807	Unknown	C2HD1-SI: L3 Portchannel's FPOE mask incorrect after SSO
CSCtc53958	Unknown	"sh run" on Cat6k results in tunnel flapping on non-modular IOS
CSCtc79335	Unknown	Sup Crash on several locations with IP SEC config
CSCtc81772	Unknown	High cpu utilization with IPv6 ACL
CSCtc90469	Unknown	Sup32 crash just after boot up with ACL Deny Test Failure
CSCtd01483	Unknown	With fm platform debug on when private-host is config'd the switch crash
CSCtd13853	Unknown	Linecard interfaces going into UDLD errdisable state on reload
CSCtd16863	Unknown	6500 PoE issues with 1120 line of APs when using dot1x
CSCtd18947	Unknown	Port-based EoMPLS stops passing tagged traffic
CSCtd21153	Unknown	Packets are not netflow switched for wccp-L2-redirect(inbound)with hash
CSCtd31143	Unknown	SPA in CC mode with SSO breaks connectivity when other sup comes online
CSCtd35521	Unknown	MVPN PIM neighborship is not formed within vrfs
CSCtd45736	Unknown	EOAM:LB functionality is broken from 11/17 due to CSCtb70578
CSCtd58314	Unknown	memory corruption crash with sh ip arp inspect log
CSCtd59572	Unknown	Spurious memory access errors seen after fpd upgrade of T3/E3 on SIP200
CSCtd59664	Unknown	%ERROR: Standby doesn't support this on configuring speed on SIP-400 int
CSCtd72437	Unknown	Packets punted to software forwarding when route-map is used for NAT
CSCtd78587	Unknown	Crash when recovering a port which was err-disabled twice
CSCtd92043	Unknown	Ph2 rekey use wrong proxy-id's on cat6k ezvpn ipsec-spa-2g
CSCte08785	Unknown	mac notification change history log not seen for deleted mac entries.
CSCte20914	Unknown	SPAN Reflector not enabled for WS-SVC-ADM-1-K9 : 2nd Commit
CSCte56366	Unknown	DSCP values are not mapped to RX priority queue
CSCte87347	Unknown	FPGA upgrade of CHT1E1 to 2.8 is not successful
CSCtf03547	Unknown	VSS: Switch went down coz %EARL-SW1_SP-4-EBUS_SEQ_ERROR: with SXH7 image
CSCtf06477	Unknown	VSS: changing switching mode powers down service modules in SXH
CSCtf16330	Unknown	DHCP Rogue Server Detection : Multiple DHCPDISCOVER's issue
CSCtf53433	Unknown	Knob 'platform ipv6 acl punt extension-header' default should be false
CSCsi05069	WAN	DCE Sub-interface is not coming up after provisioning
CSCsw31019	WAN	Router crashes while configuring the command "frame-relay be 1"

Caveats Resolved in Release 12.2(33)SXH6

Resolved Security Caveats

- [CSCsx70889](#)—Resolved in 12.2(33)SXH6

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/warp/public/707/cisco-sa-20090923-tunnels.shtml>

Resolved Unknown Caveats

- [CSCsy07555](#)—Resolved in 12.2(33)SXH6

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

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml>

- [CSCsy15227](#)—Resolved in 12.2(33)SXH6

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/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>

Other Resolved Caveats in Release 12.2(33)SXH6

Identifier	Technology	Description
CSCin67182	AAA	Crash in aaa_sg_v2_get_next_server on trying unconfigured radius ser
CSCsc97727	AAA	Access Point Crashes When Removing TACACS Server
CSCse12395	AAA	Check keys error for accounting does not cause failover
CSCsh34529	ATM	autobahn76: ATM interface config lost on standby RP
CSCsx43905	ATM	Router Crash at dlencia.c on 12.2(33.4.14)SXH
CSCee83031	Infrastructure	test crash, dumping log before command is displayed
CSCsc77704	Infrastructure	region_find_by_addr goes into infinite loop when spurious memory occurs.
CSCsc88003	Infrastructure	Issuing banner exec commnad under interface range crash switch
CSCsd99763	Infrastructure	Cisco 7200 series reload unexpectedly while configuring BGP acces list
CSCse40379	Infrastructure	IP SLA: Increasing the request-data-size via CLI crashes the device.
CSCsk41686	Infrastructure	PARSER-3-CFGLOG_NOMEM: constanlty in log
CSCsm66896	Infrastructure	IP SLA Monitor strDupOctet memory leak
CSCsq74185	Infrastructure	Image verification not possible on 12.2(33)SRC for the c7200
CSCsr08750	Infrastructure	router is crashing after giving the command memory reserve critical 1

Identifier	Technology	Description
CSCsr94474	Infrastructure	Running-config stuck: nv_csb_semaphore locked during copy run ftp
CSCsu65967	Infrastructure	Modular IOS crash at free_lite_internal
CSCsv90106	Infrastructure	nested crash leads to incomplete crashinfo
CSCsx10028	Infrastructure	Core dump may fail to write
CSCsy86078	Infrastructure	Memory corruption Failure
CSCsz19466	Infrastructure	C2W1: int range command with port-channel load-defer cause router crash
CSCsz52815	Infrastructure	Crash when 'history hours-of-statistics-kept' has value greater than 9
CSCta02715	Infrastructure	SXH5: RP crash on each booting time if <logging count> enabled
CSCed01880	IPServices	Not able to configure NAT tcp timeouts beyond 4194 sec
CSCsa41736	IPServices	Router crash after enable NAT rate-limit feature
CSCsa47672	IPServices	NAT refcount counter maximum value of 65536 (64K)
CSCse01431	IPServices	NAT-CCE : NAT SBC : outside sip call not go through
CSCse66643	IPServices	SYS-2-NOBLOCK error when redistributing NAT routes
CSCsj19805	IPServices	ip igmp static-group broken after reload on int vlan on a 7600
CSCsk23972	IPServices	Telnet failed with "No wild listener" error
CSCsw52416	IPServices	NAT: dynamic nat entries do not timeout in certain case
CSCsw65614	IPServices	NAT with route maps doesn't work for TCP application
CSCsx33622	IPServices	Fix MSS calculation issue in TCP
CSCsx34372	IPServices	c2w21/C2W2b:OSPF is not working with udldr/ude
CSCsy39623	IPServices	cannot ping local vlan interface ip address with NAT configured
CSCsy39667	IPServices	dhcp-proxy-client incorrectly sends DHCPRELEASE in PPP-agg use-case
CSCsy97506	IPServices	All nat'ed multicast packets punted to software
CSCsz12488	IPServices	LDAP add with malformed BER attributes causes CPUHOG and MALLOCFAIL
CSCsz56393	IPServices	Modular IOS - SUP720 - Sends malformed syslog packet
CSCsz89107	IPServices	high cpu due to ip_input process during SNMP trap
CSCsz91851	IPServices	NAT : ESP packets not translated with static NAT outside translation
CSCta24043	IPServices	"%IPNAT-4-ADDR_ALLOC_FAIL" message seen when all ports are not allocated
CSCta83548	IPServices	NAT Platform: unable to clear an specific nat entry
CSCta89283	IPServices	Add support for NAT redundancy feature in SX releases
CSCtb58282	IPServices	show tcp brief can cause crash
CSCej82248	MPLS	%LFD-3-NOOCE: Traceback in lfd_fib_update_mpls_oces
CSCsy60668	MPLS	W1.5:: Toggle "mpls tra router-id" cause router crash
CSCsz11877	MPLS	MPLS-TE Tunnel label re-allocation on mid-point router while RSVP-GR
CSCsz75180	MPLS	Crash due to mpls subintf being removed
CSCsz92368	MPLS	MDEBUG-2-ACCESSFREED: @tc_handle_dead_peers Enabling/disabling "mpls ip"
CSCsx34506	Multicast	RPF failure with no PIM neighbor triggers PIM Hello
CSCta26106	QoS	RSVP-3-CONSISTENCY error followed by an unexpected reboot.

Identifier	Technology	Description
CSCse15634	Routing	neighbor default-originate doesn't work in address-family ipv4 multicast
CSCse45978	Routing	BGP to RIP redistribution breaks as RIP nexthop moves to alternate path
CSCsg92473	Routing	Switch crashes - IPV6 reflexive acl scalability test
CSCsl90028	Routing	CEF low mem crash after pumping more than 1Lac OSPF routes
CSCsm05082	Routing	BGP Dampening penalty not decaying on frqnt 'sh ip bgp v all' [dampening
CSCsm79085	Routing	EIGRP routes flapping due to nexthop changed
CSCso07371	Routing	SCHED-7-WATCH: Attempt to set uninitialized watched boolean in pfxlist
CSCsq20928	Routing	CEFv6 dropping IPv6 unicast packets
CSCsq45082	Routing	ip route with associated track/sla gets removed when track is still up
CSCsq83006	Routing	Port-channel down makes EIGRP SIA
CSCsr27794	Routing	BGP updates stuck during peer flap
CSCsu96698	Routing	BGP: /32 route being advertised while 'summary-only' is configured
CSCsv17933	Routing	Static route in VRF is not redistributed by RIP after link flap
CSCsv59334	Routing	Connected nets redistr from eigrpTObgp when no net 0 is set under eigrp
CSCsv73754	Routing	crash during vrf unconfig - bgp_vpn_impq_add_vrfs_cfg_changes
CSCsx08294	Routing	OSPF encounters a bus error crash when running SPF
CSCsx51299	Routing	Crash when remove and configure ipv6 ACL via telnet and console
CSCsx98673	Routing	PE not send extended-community to a peer newly added to peer-group
CSCsy29534	Routing	Bus error crash on removing address-family in router rip config mode
CSCsy73123	Routing	Connected route on port-channel subintf not removed when Po is down
CSCsy76404	Routing	Modular IOS: memory leak in CEF background process
CSCsy77842	Routing	TB isis_process_no_router after isis router process deleted
CSCsy84134	Routing	ARP table is flushed when deleting secondary IP address
CSCsz16724	Routing	BGPv6: default-metric is not being NVGEN'ed and not functioning
CSCta60119	Routing	non recursive accounting can cause prefixes linked to drop
CSCsc49862	Security	IPAddress in Subject Alternative Name is not parsed correctly.
CSCso27236	Security	IOS CA client shows renew date 1 Jan 1970
CSCsv23797	Security	SSH:Crash seen on 7200 on mcp_dev
CSCsv54863	Security	IOS PKI: Not expired Certificate is deleted if autoenrollment fails
CSCsz84055	Security	System crashed unexpected while open ssh2 session
CSCtb36521	Security	PKI get stuck in pager when requesting to fetch SCEP capabilities
CSCee25454	Unknown	SADB peering process leaks memory after overnight test
CSCek53099	Unknown	SIP200+4xT3/E3:Fail to load cRTP CFG from startup file
CSCsd39568	Unknown	stats support for PBR set ip nexthop/set interface
CSCsg35285	Unknown	Slower Cache refresh for int stats when more interfaces up
CSCsi46897	Unknown	PRE crash after snmpwalk on mib cbQosSetStatsTable
CSCsj26698	Unknown	Acct-Session-Id in Accounting-Request is different from in Access-Reques

Identifier	Technology	Description
CSCsk25046	Unknown	Not all ifIndex'es are in cbQoSServicePolicyTable
CSCsk29975	Unknown	Tunnel not up, invalid local address after modify the local address .
CSCsk62407	Unknown	CPU HOG@fm_format_addr_to_compare on applying large IPv6 ACL
CSCsl61273	Unknown	Standby crash after autoqos config
CSCsl72962	Unknown	Mask the debug message error in multicast throttle logic
CSCsm39160	Unknown	TestCFRW shows incorrectly as failed in show diagnostic sanity
CSCsm45254	Unknown	OBFL ENV app in infinite-loop causing high CPU
CSCsm84073	Unknown	c2w2:vrf ping fails after toggle mls mpls recir, sso,remove/add ip vrf
CSCsm84163	Unknown	Memory leak for IKE/IPSEC after hsrp failover, router crashed w/ no mem
CSCso35876	Unknown	SRB3:New active SP crash at label_entry_get_inlabel
CSCso36150	Unknown	duplicate vlan names causing config-sync failures
CSCso59242	Unknown	sierra: show mem detailed all stat is truncated.
CSCso79925	Unknown	EC with enhanced hash method (PFC3C) has no knob to use old method (3B)
CSCsq31935	Unknown	6500 - L3 port channel - CDP packet sent tagged in internal vlan
CSCsq55506	Unknown	Inter community PVLAN traffic is software switched
CSCsq69567	Unknown	SSO Switchover + unicast-routing chg cause MC traffic loss for 2 minutes
CSCsq78343	Unknown	Tidy up the netflow sub flow code
CSCsq96144	Unknown	Netflow v9 Exported Data issue in case of ECMP
CSCsr04916	Unknown	PBR dropped the packets after add set vrf vpn1 back to the route-map
CSCsr99518	Unknown	Granikos should not init rekey after recieving new outbound SA at QM3
CSCsu11487	Unknown	pm_fec_is_mec() returns FALSE when 1 of 5 local MEC members is shutdown
CSCsu27660	Unknown	CDP packet sent tagged in internal vlan
CSCsu29301	Unknown	C2W21: Ingress SPAN on Sup - ACE module duplicates packets
CSCsu36715	Unknown	W2.0 : C2 : ION : Memory Leak in MSDP process
CSCsu67413	Unknown	RRI - Route disappears after ipsec rekey with multi int scenario
CSCsu92395	Unknown	Crash caused by event manager configuration: "action mail"
CSCsv12378	Unknown	c2w2:Memory leak in Crypto IKMP process on IOS EzVPN server
CSCsv24908	Unknown	L2 Fwd Broken on other modules when SIP-400 int flaps
CSCsv27372	Unknown	telnet to a real(directed mode) via GRE tunnel crates SUP crash on SRC2
CSCsv27548	Unknown	Cat6k/sip200: PPP packets punted sip200 multilink interface
CSCsv27617	Unknown	Flow creation disabled in netflow table after reload for WAN main ints
CSCsv52025	Unknown	call-home: Port numbers cannot be added to URLs with IP addresses
CSCsv63799	Unknown	PfR MC/BR bus error crash in ip fast flow
CSCsw14147	Unknown	VACL unable to capture traffic from RP
CSCsw32280	Unknown	Diag error on WS-X6148A-45AF card asic with Traffic
CSCsw41706	Unknown	router reload when registering EEM service diag script
CSCsw48181	Unknown	Unknown Unicast is dropped on Shut/no Shut of a VLAN

Identifier	Technology	Description
CSCsw52819	Unknown	Kernel dumper needs a few enhancements.
CSCsw68514	Unknown	SLB probes iin TESTING state while using client cmd in Vserver config
CSCsw76117	Unknown	TBs seen after redundancy mode change from sso to rpr
CSCsw78413	Unknown	BFD over ATM subinterfaces is broken in recent SR images
CSCsw83488	Unknown	Negative value seen for counters in vpn session
CSCsx09110	Unknown	Failed to establish ipsec tunnel with CCM
CSCsx20862	Unknown	Peer RP index unknown messages seen on VSS setup
CSCsx21886	Unknown	ISSU switchover command sync issue
CSCsx29377	Unknown	1 sec multicast loss on standby sup720-10g
CSCsx49889	Unknown	SPA-IPSEC-2G-3-ACEI0TCAMFAILE:SpdSpInstall:cannot install Sp TmInsertSp
CSCsx55152	Unknown	Switch does not send TC trap if it is not a root bridge
CSCsx58786	Unknown	Router crash @ routemap_track_nexthop
CSCsx82825	Unknown	Shutdown Loopback interfaces in VSS recovery mode
CSCsy01275	Unknown	W15:: SYS-2-MALLOCFAIL: Memory allocation message seen after bootup
CSCsy01763	Unknown	15 - 20 packets leak to DST with PACL after SSO
CSCsy03587	Unknown	c2w2b: SYS-2-MALLOCFAIL: Memory allocation failed seen with tracebacks
CSCsy08838	Unknown	Zamboni allows clear packet inbound on protected interface
CSCsy16220	Unknown	a switch may crash due to deadlock between snmp and eem
CSCsy21797	Unknown	Cat6k-Unexpected SNMP messages occurred
CSCsy24895	Unknown	Memory leak in ACE HAPI process
CSCsy26526	Unknown	Router is getting crashed at netconf_sessionQs_set_max_message
CSCsy26979	Unknown	33SXH5: Traceback seen @satvs_assert_class3
CSCsy34566	Unknown	Disable VLAN mapping on ME6524, 6148A-GE-TX
CSCsy37175	Unknown	2FE-PA Subintf lost connection after chassis/Flexwan2 reload
CSCsy41526	Unknown	PIM msgs duplicated when MPLS configured and IGMP Snooping Off on xface
CSCsy54365	Unknown	frequent datapath recovery and traffic loss on WS-X6704 with DFC
CSCsy58886	Unknown	NGN:Active crashes when standby booting up on SRC2->SRC3 ISSU
CSCsy61956	Unknown	Crash in ios-base when running 'show ip route' or 'show bgp' commands
CSCsy62753	Unknown	MST configured router crashed after receiving PVST BPDU.
CSCsy69228	Unknown	Add CLI mls cef tunnel fragment support for non supertycho2
CSCsy69740	Unknown	SXH: Traffic drop on L2 PO after cleared psecurity on rcving L2 ports
CSCsy78994	Unknown	Memory leak in Service Task
CSCsy82121	Unknown	IGMP Source only not working due to MC_CAP not set
CSCsy85171	Unknown	CDL2 Read Error: Time out
CSCsy86050	Unknown	MAC Move Notifications on VSS between active and down ports
CSCsy87619	Unknown	VSS port channel going down when powering down active switch
CSCsy95520	Unknown	~500msec Pkt loss after transition to HSRP Active on L3 int

Identifier	Technology	Description
CSCsz01976	Unknown	Need a cli to dump the rommon environment and unset rommon variable
CSCsz06187	Unknown	VACL capture for ingress software switched packets
CSCsz07068	Unknown	VSS: Output Drops on a VSL port due to small Tx Queue limit
CSCsz12369	Unknown	FPD support for SPA-8X1FE-TX-V2 is not enabled
CSCsz14072	Unknown	Memory leak at "MAB Framework" process when dot1x is enabled
CSCsz20625	Unknown	Error message seen if SIP Is OIR'd during Standby SUP bootup
CSCsz22954	Unknown	Supported WS-X6324-100FX-MM is powered down improperly
CSCsz23448	Unknown	SIP 200 not coming up and Router Crashes after applying card type E3 1 1
CSCsz40969	Unknown	Need to add Me_Kr flow-control status registers back into sierra/whitney
CSCsz42143	Unknown	WS-X6148A-GE-TX module fails keepalives when excessive errors on port.
CSCsz44678	Unknown	Tunnel won't forward traffic across global to vrf
CSCsz47077	Unknown	SWITCH_NUMBER rommon variable set on its own and by "wr erase" command
CSCsz55834	Unknown	GLBP may provided BIA MAC instead of Virtual MAC for mobile users
CSCsz62046	Unknown	Crash at memcpy after CPUHOG in SNMP ENGINE
CSCsz63359	Unknown	c2w2b:"show mls qos ip" displays vslot interface instead switchid and sl
CSCsz67334	Unknown	ciscoEnvMonTemperatureStatus trap sent sporadically as NotFunctioning
CSCsz71970	Unknown	c2w2b: Freed Memory being Accessed by lldp_med_free_local_annex
CSCsz75820	Unknown	JQL: VSS hang on SP after RP crashed by software-forced reload
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
CSCta01121	Unknown	c2w1:MDEBUG traceback is seen while unconfiguring qos feature in FM.
CSCta05502	Unknown	Spurious memory access made at psecure_port_del_addr_by_mac_imp
CSCta06175	Unknown	Cat6500/SXH: Deleted configs re-appear on IDSM reset
CSCta10870	Unknown	FPOE takes long time to be programmed on active vss switch
CSCta21771	Unknown	%CONST_DIAG-SP-3-HM_FCI_0_STUCK: Flow control stuck at 0 error on modul
CSCta27279	Unknown	WCCP s/w switching with Ingress redirection & interface ACL
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 algorithim needs a few improvements
CSCta74315	Unknown	WS-X6324-100FX-MM May Be Inoperable and Have Status "Other"
CSCta76808	Unknown	add CLI command for medium buffer pool
CSCta94179	Unknown	Recirculated MPLS packets becasue of egress service policy are dropped
CSCtb23289	Unknown	Major temperature alarm has to force system shutdown
CSCtb28032	Unknown	Changing module corrupts Flex Link

Identifier	Technology	Description
CSCtb28712	Unknown	SPAN Reflector not enabled for WS-SVC-ADM-1-K9
CSCtb38547	Unknown	Incorrect CP0 values and empty kernel variable section in kernel crashin
CSCtb60330	Unknown	VTI: Missed DPD ACK on phase 1 expiry causing phase 2 deletion.
CSCtb63352	Unknown	VSS: With 6KW DC PS, no power to bringup VSL supervisor or linecard
CSCtb66983	Unknown	Nas-port-type is missing in Access-request
CSCtb68478	Unknown	"Illegal nextSsIndex value" message should be removed
CSCtb87454	Unknown	DHCP Rogue Server Detection
CSCsi56413	WAN	PA-POS-OC3SMI interface output stuck .

Caveats Resolved in Release 12.2(33)SXH5

Resolved AAA Caveats

- [CSCsv73509](#)—Resolved in 12.2(33)SXH5

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

- [CSCsr72301](#)—Resolved in 12.2(33)SXH5

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/warp/public/707/cisco-sr-20090114-http.shtml>

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

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

- [CSCsx49573](#)—Resolved in 12.2(33)SXH5

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/warp/public/707/cisco-sr-20090114-http.shtml>

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(33)SXH5

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/warp/public/707/cisco-sa-20090325-udp.shtml>

- [CSCsm27071](#)—Resolved in 12.2(33)SXH5

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/warp/public/707/cisco-sa-20090325-ip.shtml>

- [CSCsm45390](#)—Resolved in 12.2(33)SXH5

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

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

Workaround: None.

- [CSCsv04836](#)—Resolved in 12.2(33)SXH5

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/warp/public/707/cisco-sa-20090908-tcp24.shtml>.

- [CSCsw18636](#)—Resolved in 12.2(33)SXH5

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(33)SXH5

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/warp/public/707/cisco-sa-20090325-tcp.shtml>

Resolved LAN Caveats

- [CSCsv05934](#)—Resolved in 12.2(33)SXH5

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/warp/public/707/cisco-sr-20081105-vtp.shtml>

Resolved Multicast Caveats

- [CSCso90058](#)—Resolved in 12.2(33)SXH5

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.

- [CSCsu79754](#)—Resolved in 12.2(33)SXH5

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

Conditions: Unknown at this time.

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

Resolved Routing Caveats

- [CSCsx73770](#)—Resolved in 12.2(33)SXH5

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 Release 12.2(33)SXH5

Identifier	Technology	Description
CSCec82106	AAA	Router crashes with a bus error when removing AAA comands
CSCei62358	AAA	Downloading callback-dialstring as part of Tacacs+ author leads to crash
CSCin40015	AAA	telnet to NAS fails when user profile has access-profile
CSCsc78999	AAA	Address Error exception at TPLUS
CSCse02550	AAA	ip radius source-interface not used in combination with vrf
CSCsl63494	AAA	Issue with session accounting in AAA
CSCsq37815	AAA	Case sensitive Username authentication is passed with wrong user name
CSCsq94524	AAA	"aaa accounting update newinfo" causes extra "jitter maximum 0" option
CSCsv06973	AAA	Router Crashes at tplus_shutdown_single_connection
CSCsw19816	AAA	cat6000: IOS login enhancements not creating logs for telnet with AAA
CSCsy00716	AAA	Accounting record has sensitive information in clear text structure
CSCso64050	ATM	HA functionality is not working when policy attached to atm pvc
CSCsr27727	Content	Cat6K experiences a reload after %SYS-2-ASSERTION_FAILED: message
CSCsx40747	Content	Router hangs while doing ip casa configurations
CSCed33145	Infrastructure	line vty exec-timeout not working properly, def causes spur mem acc
CSCef82896	Infrastructure	When removing the user name from auth dialog, http crashes
CSCek62770	Infrastructure	bundles need to include CW_ strings
CSCin79116	Infrastructure	show memory summary could push the CPU util to 100%
CSCsb98906	Infrastructure	Memory Leak with bgp regexp deterministic configuration
CSCsc86307	Infrastructure	c3845 crashed @ show_systat
CSCsd55059	Infrastructure	polling CISCO-FLASH-MIB slows down GSR
CSCse41523	Infrastructure	bootldr config caused stbyPRE reset if file does not exist on stby-bootf
CSCse49151	Infrastructure	3800 clock slip over times verified in lab
CSCsh66245	Infrastructure	Lowest memory is too low after reload on Cisco 10000

Identifier	Technology	Description
CSCsj24186	Infrastructure	%SYS-2-NOBLOCK messages from Pool Manager process
CSCsj67434	Infrastructure	The CLI: 'parser config cache interface' does not work
CSCsm27493	Infrastructure	procmib_server port has to send rpc reply only for RPC requests.
CSCso29361	Infrastructure	cfg added under interface range vlan not being added in redundant sup
CSCsq19159	Infrastructure	RP crashes in chassismib_add_sub_card_entry after linecard reload
CSCsv80900	Infrastructure	W21:: EARL-SPSTBY-2-SWITCH_BUS_IDLE & PF_ASIC-SPSTBY-3-ASIC_DUMP @boot
CSCsv86766	Infrastructure	Signature fail while copy, causing system:/running-config to be deleted
CSCsw35917	Infrastructure	SP syslog messages not sent as SNMP traps by RP's SNMP agent
CSCsw61555	Infrastructure	Router Crashes after doing SSO
CSCsx32841	Infrastructure	ceImageDescription may exceed 255 characters
CSCsx95675	Infrastructure	interface config disappear after "wr mem"
CSCsy55455	Infrastructure	Crash at saaComponentGet
CSCec72958	IPServices	Software forced crash when translating LDAP packet
CSCef58137	IPServices	Router Crash after high CPU, when IPNAT configured with route-map
CSCek10384	IPServices	7200 NAT dropping Out to In ESP Packets
CSCsh49973	IPServices	NAT-ALG corrupts offset value of DNS PTR response
CSCsj41479	IPServices	DHCP Services should not be enabled by default in IOS
CSCsj76907	IPServices	IPv6 UDP sockets may incorrectly show "--any--" for local address
CSCsk16821	IPServices	DHCP does not NAK after DHCPREQUEST from unknown client .
CSCsm89795	IPServices	Orbitty repeatedly Crashes - Succetible to Denial of service attacks
CSCso02053	IPServices	NAT does not add dynamic aliases after reload.
CSCso04657	IPServices	SSLVPN service stops accepting any new SSLVPN connections
CSCso39062	IPServices	C2W2: %SYS-3-INVMEMINT: Invalid memory action message & TB's with PAT.
CSCso54027	IPServices	Spurious memory access in ttcp_rcv_stats
CSCsq14311	IPServices	7200 crash - ipnat_unlock_parent_entry (PPTP)
CSCsq81365	IPServices	MFI: UDP forwarded-protocols from VRF are leaked into global table
CSCsq92440	IPServices	Router Crash with igmp static grp classmap for 10k grps on 10 subints
CSCsu10108	IPServices	TFTP Server function is not working in 7600 router
CSCsu64215	IPServices	ip tcp adjust-mss command results in packet loss for non-TCP traffic
CSCsu72176	IPServices	Crash:Process Deadlock in Standby while reloading UUT with DHCP configs
CSCsu95319	IPServices	IGMP report was not sent to helper address.
CSCsv16987	IPServices	nat pool size more than 16 bit long should not be configured
CSCsv86201	IPServices	Modular IOS : max sockets overflow
CSCsw16698	IPServices	DHCP database could not be locked DHCPD process could not lock semaphore
CSCsw51864	IPServices	CHUNKFREE error and crash when changing NAT config
CSCsw68135	IPServices	Removing static nat with route-map cause Address Error
CSCsw73391	IPServices	ip igmp limit gets stuck

Identifier	Technology	Description
CSCsx09343	IPServices	Name resolution triggers pager in non-interactive mode.
CSCsx23602	IPServices	crash after 'clear ip nat trans *'
CSCsx32283	IPServices	Malformed L field in LDAP crashes 6k with NAT
CSCsx74657	IPServices	Many issues with NAT/Multicast feature
CSCsy26750	IPServices	6k Crash with ipnat_ldap_fixup (Redundancy Checks needed)
CSCsy45371	IPServices	NAT: two static nat entry related issues
CSCsw81485	LegacyProtocols	Unconfiguring IPX crashes the switch
CSCsu10229	Management	The cdpCacheAddress mib not providing GLOBAL_UNICAST Address
CSCsw66153	Management	Native vlan not displayed in show cdp neighbor detail
CSCsr50099	MPLS	show ip explicit-paths command incorrectly displays source route type
CSCsv00773	MPLS	Loose Path Reopt not applied when link costs changed
CSCsv41456	MPLS	Tracebacks seen at IFMGR-3-DUP_IFINDEXifDescr"Virtual-Access2-mpls layer
CSCsw35638	MPLS	FRR Interoperability issue between Juniper PLR and IOS MP
CSCsb77148	Multicast	sh ip mpacket x.x.x.x quality output is wrong after counter wraps around
CSCsr82895	Multicast	watchdog timeout : RP Crash @ igmp_rejoin_groups during RP Switchover
CSCsu86494	Multicast	Assert flag is not cleared after PIM neighbor loss
CSCsu95080	Multicast	mld_processs block forever in the init_process when parsing config
CSCsv29659	Multicast	RP configured inside the nat not shown on uut outside the nat
CSCsx15396	Multicast	Mcast IIF stays up while physical interface is down
CSCsx28948	Multicast	I/O Memory leak on 7200
CSCsx58861	Multicast	Crash due to Stack for iGMP process running low
CSCsf07760	PPP	MLP: Crashes/buffer leaks when large number of sessions come up at once
CSCsr81271	PPP	Invalid VCD error messages upon PVC flap
CSCsu70011	PPP	ipv6 static route pointing to multilink (flexwan) disappears after sso
CSCee63182	QoS	Router crashes while implementing rate-limit
CSCek75808	QoS	MF: Crash observed at qos_show_policymap_interface_all
CSCsl94263	QoS	Router crash at stile_update_fast_flag due to random-detect dscp-base
CSCsm97014	QoS	Connectivity breaks for QOS + header compression on virtual templates
CSCsr05501	QoS	% NBAR Error: hwidb could not found shows up when reload
CSCsv85791	QoS	Flexwan+/PA-MC-2T3+ introduce 5+ seconds delay on egress
CSCed71294	Routing	Multicast multipath does not work in the vrf context
CSCee30355	Routing	Memory leak at ip_multicast_ctl
CSCef65457	Routing	EIGRP and RIP advertise null0 static routes after they are removed
CSCej49366	Routing	Removing default-metric under EIGRP deletes routes erroneously
CSCsb15164	Routing	Security holes while configuring a standard ACE with host address
CSCsd25753	Routing	BGP Aggregated supernet routes not Advertised properly
CSCse68877	Routing	CEF/BGP table MPLS label mismatch YW3 Non Multi-path

Identifier	Technology	Description
CSCsg68717	Routing	A weird behavior in maxpath configuration in ebgp+ibgp case
CSCsh34417	Routing	BGP Distance not updated following failover to a path with a greater dis
CSCsh54161	Routing	dune, Nov image goes unstable - creates eigrp routing loops
CSCsi70484	Routing	OSPF SPF running constantly if LSID conflicts & prefix filter used.
CSCsj13911	Routing	Cat3750:EIGRP does not receive reply for query between some Vlan
CSCsj42399	Routing	Redistributed static covered by network statement sets metric to 0
CSCsk11930	Routing	Not able to reconfigure the numbered ip extcommunity-list
CSCsk35688	Routing	Aggregate routes not processed if child routes are deleted pre-maturely
CSCsk80250	Routing	BGP has to handle the return value REXP_DONTKNOW of regexec_hybrid
CSCsk87526	Routing	T/B ipv6_rib_process_changeQ after shut cmd applied Int. running RIPng
CSCsl32318	Routing	OSPF: new fix for CSCsk36324 SPF loop
CSCsl48075	Routing	Floating static route behaves incorrectly in 6vPE
CSCsl49628	Routing	VRF is not getting deleted in 'sh vrf' output
CSCsl51616	Routing	v6-vrf-lite config doesn't sync properly with standby
CSCsm57494	Routing	BGP update is not sent after reloading opposite router
CSCsm91959	Routing	Code review: aggregation child routes can miss aggregation logic
CSCsm95129	Routing	"no ip next-hop-self eigrp" not working when redistribute from BGP
CSCsm96901	Routing	Unable to ping between vrfs through transparent bridge
CSCso39597	Routing	StbyRP crashed @ bgp_vpnv4_bulk_sync_mpls_lbl_binding during bulk sync
CSCso51519	Routing	Paths with same Nexthop selected as multipaths in some sequence
CSCso55151	Routing	ADJ not freeing memory under IPv6 ND stress test
CSCso90107	Routing	SNMP: bgpPeertable and cbgpPeertable shows only results for ipv4 peers
CSCsq24935	Routing	Switch crash due to unsupported bgp/ipv6 command
CSCsq43831	Routing	Stack overflow due to recursion in FIB
CSCsq97517	Routing	C2W2: Mago: CEF on RP is not in sync with SP after reboot.
CSCsr01403	Routing	cefswitching2.1:More time taken(12 mts) to converge after Adjacency flap
CSCsr11662	Routing	EIGRP active routes never go to SIA, queries not sent
CSCsr50704	Routing	dmzlink-bw programs wrong traffic share count in routing table
CSCsr51801	Routing	upon router reload some of the route-maps not permitting the prefixes.
CSCsr67361	Routing	I/O memory leaks when BGP neighbor points to a local address
CSCsr86174	Routing	aggregate-address under address-family does not appear in conf
CSCsr90248	Routing	"aggregate-address advertise-map" not updated dynamically
CSCsu06447	Routing	EIGRP:static route redistribution not working with distribution-list
CSCsu11161	Routing	Neighbor x.x.x.x default-originate issues seen in 12.2 code
CSCsu12040	Routing	PE with CsC configuration sends wrong labels to SPE
CSCsu63996	Routing	OSPF flaps after SSO switchover causes traffic loss after SSO switchover
CSCsu76993	Routing	EIGRP:Routes not tagged with match source redistribution-source

Identifier	Technology	Description
CSCsv01474	Routing	'ip rip advertise' command lost after interface flap/clear ip route
CSCsv05009	Routing	%OSPF-4-FLOOD_WAR: error during heavy flaps for type-5 and type-7 LSAs
CSCsv27607	Routing	BGP: Outbound route-map updating withdraw only one member
CSCsv85052	Routing	Crash observed when "ispf" is issued in vty with ip routing disabled
CSCsv89643	Routing	OSPF: MAC address of next hop unresolved on ptp eth by adjacency bringup
CSCsv97472	Routing	CSCso62166_dcq_issue_rn_walktree_timed_locking is changed
CSCsw24286	Routing	TE tunnel bandwidth command breaks isis topology
CSCsw24826	Routing	OSPF crash during type-9 maxage
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
CSCsw65933	Routing	Prefix not learned from PE to CE
CSCsw79397	Routing	Device crashing at bgp_command_af_specific
CSCsx06457	Routing	BGP may modify routes it does not own
CSCsx15841	Routing	aggregate-address does not NVGEN upon switchover on cat6k
CSCsx17446	Routing	Tunnel route and a non-tunnel (IGP) route with same metric (TE metric)
CSCsx51596	Routing	TCAM ACL entry not correct after removing IP accounting
CSCsx99015	Routing	crash if OSPF redistributes another OSPF and interface bw changes
CSCsy15150	Routing	33SXH5: Traceback @ isis_router when default interface configured
CSCsy45838	Routing	show ip ospf border-router crashing router
CSCea11368	Security	CRL fetch using ldap fails if vrf configured in trustpoint
CSCeh75136	Security	TACACS+ rem_addr field empty after first SSH authen attempt fails
CSCsc91824	Security	SSH from router disconnects vty session if there is no matching cipher
CSCsv20285	Security	Whitney:Authentication to the CA server failed using ION.
CSCsx15430	Security	Verbose name lookup calls in IP context causes PKI to block due to pager
CSCsx17447	Security	IOS not including HOST header in HTTP CRL request
CSCsy16177	Security	scp:copy to router over sshv2 fails with invalid checksum error
CSCsy22311	Security	SCP b/w IOS routers fails while the client is receiving file from server
CSCeg35237	Unknown	Watchdog crash after sh crypto session
CSCeg80842	Unknown	PA-MC-8TE1 controller stuck (similar to CSCdz72292)
CSCek70131	Unknown	SIP1 crash at vip_mlp_fastsend with HEARTBEAT error for mlppp qos
CSCek77996	Unknown	High CPU caused by data traffic with crypto map in crypto connect mode
CSCsd04608	Unknown	MQC-IPHC: Router crashed while testing mqc-iphc test
CSCsd45698	Unknown	Cat6K: SLB punted to CPU if src_index is port-channel index
CSCse63833	Unknown	SNMP bus error while polling cipsStaticCryptomapTable .
CSCsg14926	Unknown	Standby can not boot because of insufficient memory with 32K interfaces
CSCsg83756	Unknown	SPA-8XCHT1/E1 after Reload C/A LED green even if no cable plugged
CSCsg87290	Unknown	SIP1-ChOC3: Extra path flap is observed on ChOC3 SPA interfaces

Identifier	Technology	Description
CSCsh22225	Unknown	CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR:
CSCsi55428	Unknown	FRU Trap sequence incorrect when " hw-module subslot shutdown unpowered"
CSCsi78584	Unknown	T3/E3 SPA:Line protocol is not comin up with E3 and framing bypass
CSCsj19308	Unknown	PE and CE ping fails over multilink ppp bundle. .
CSCsk30196	Unknown	BADBUFFER error at pak_copy_contiguous_to_contiguous
CSCsk33045	Unknown	MST BPDU *must* be sent untagged, even when the switch is configured wit
CSCsk49151	Unknown	Vlan policy-map rejected upon reloading.
CSCsk67417	Unknown	Crash while two or more users displays: show ip arp inspection log
CSCsk84498	Unknown	EVERGLADES:archive,write-mem feature broken
CSCsk89091	Unknown	HWIF-QOS-ERR: Failure installing Port QoS TX/Rx setting
CSCsl44170	Unknown	LI tapped PPPoE LCP/PPP control packets originated from router are bogus
CSCsl53279	Unknown	Physical interfaces on Cat6k set to 10 usec regardless of line speed
CSCsl72332	Unknown	cat6k crash with 'no mobility network-id 4'
CSCsm44147	Unknown	SSO failure due to mismatched command on SRB1
CSCsm66678	Unknown	Policing not working in MPLS cloud
CSCsm72121	Unknown	W2: bad cookie magic was detected after SSO switchover with sh vtp count
CSCsm74948	Unknown	mVPN RP does not send join to directed connected neighbor PE
CSCsm76792	Unknown	PM HA bulk sync posting RF_DONE before bulk sync has finished
CSCsm79995	Unknown	Tracebacks are seen while attaching service-policy in a atm pvc
CSCsm83256	Unknown	IDSM2 Data port operation status not OK after boot OR SSO
CSCsm98671	Unknown	TestTrafficStress fails with certain configuration
CSCso03419	Unknown	VRF_Lite aware PBR: Set ip vrf clause changes on Reload/SSO with SIERRA.
CSCso05889	Unknown	Pak Subblock creation fails from CEF in ION
CSCso11489	Unknown	%SYS-SP-3-INVMEMINT while collecting ION crashinfo
CSCso11822	Unknown	LACP PC switchport, on OIR, "channel group 112 active" config gets lost
CSCso35659	Unknown	L3 traffic rate limited after adding and removing Xcon to a SVI
CSCso38671	Unknown	VS specific message seen on Sup32 image when "erase startup-config"
CSCso40891	Unknown	Stb rp reloaded during every bootup, process = FM, fm_free_platform_data
CSCso72250	Unknown	Incorrect color for SYSTEM led of Active and Standby sup in VS mode
CSCso88183	Unknown	DOME:dumper.proc crashes on dome when another process crashes
CSCso93350	Unknown	Boot string fails to set in rommon but no error message
CSCsq22383	Unknown	SP crash due to CPU hog by online diags
CSCsq56941	Unknown	6500 - Static MAC cleared from port-channel member ints after reload
CSCsq73122	Unknown	Proxy-ARP returns BIA instead of VMAC with LAM
CSCsq82865	Unknown	Parsing error reading route-map match statements if longer than 254 chrs
CSCsq87496	Unknown	"%OIR-6-INSCARD" syslog not being send from the device
CSCsr06037	Unknown	the monitor session source is removed by deleting sub-interface

Identifier	Technology	Description
CSCsr08482	Unknown	PM support to program ethertype to all ports when port-group in mux mode
CSCsr09062	Unknown	MLP+QoS - Memory corruption due to Change BW and flap int
CSCsr24647	Unknown	MSFC autostate don't up svcle Vlan int after two SSO switchover
CSCsr29559	Unknown	WCCP flap corrupts mcast CEF adjacency
CSCsr39272	Unknown	%DATACORRUPTION-1 due to spa sensor temp overrunning buffer
CSCsr88845	Unknown	unicast BootP replies dropped by DHCP snooping
CSCsu01372	Unknown	33SB: Result of boot config command not sync to standby RP after reload
CSCsu10022	Unknown	L2 traffic is policed when CoPP is enabled
CSCsu33707	Unknown	Multicast traffic will not stop after PIM prune
CSCsu40077	Unknown	MAB + Dot1x + aggressive timers leave port unauthorized but forwarding
CSCsu40166	Unknown	PBR packets send out to wrong next hop MAC after ACL is changed
CSCsu48241	Unknown	memory leak when removing igmp snooping with acl filtering
CSCsu49257	Unknown	Cstn-id timer should be restarted when access-request is seen
CSCsu50413	Unknown	RE: acl merge causes high rp cpu for ~50 min after reload
CSCsu67559	Unknown	Copy Run Start does not provide the same functionality as 'wr mem'
CSCsu75546	Unknown	C2W21: traffic not span to NAM using span conf mode local-tx source intf
CSCsu81158	Unknown	Pkt drops on SIP-400 LC due to QoS lock fail for subintfs.
CSCsu83563	Unknown	MMLS:If rate-lt on when STDBY reloads, doesnt work on swovr:x40/dual RSP
CSCsu86524	Unknown	IKMP process leak: check_ipsec_proposal
CSCsu88557	Unknown	[no] mdix auto" CLI command not present for WS-X6196-RJ21"
CSCsu91725	Unknown	Bus crash problem due to cipSecGlobalStats MIB query
CSCsu95237	Unknown	SSO switchover,clear packet seen on the wire exposing the inner IP pkt
CSCsu97020	Unknown	policer on flexwan/multilink is dropping even CIR is not reached
CSCsu99270	Unknown	CPUHOG observed when configuring more vlan interfaces
CSCsv05263	Unknown	Sup32 crashes when dumping r2d2 registers
CSCsv07858	Unknown	IfIndex for unconfigured VLAN on 7613
CSCsv09249	Unknown	VSS after dual-active recovery MEC on standby chassis UDLD error disable
CSCsv14886	Unknown	Failure to send RADIUS state attribute
CSCsv17989	Unknown	interface in SIP200 show "admin down" when it is physical down
CSCsv20339	Unknown	MN history table is flooded with multiple (~500) add/delete entries
CSCsv20768	Unknown	After SSO s/wover, atm clock config changes to line and PTB to UNSTABLE
CSCsv20920	Unknown	telnet from a GRE tunnel to real address for DNS vserver fails
CSCsv22779	Unknown	VRF-PBR: Packets dropped with reflexive acl
CSCsv24742	Unknown	PfR exit link is OOP when interface counter wraps
CSCsv30679	Unknown	Sup detetes Vlans from Sup IDSM Config on startup / failover
CSCsv32101	Unknown	QoS: memory corruption traceback when using access-list with time range
CSCsv37543	Unknown	GRE/IPsec misconfig is only resovled through module or chassis reload

Identifier	Technology	Description
CSCsv38928	Unknown	IGMP Snooping does not send out Global query on 2nd TCN < 35 seconds
CSCsv43991	Unknown	FWSM's internal portchannel on the cat6k side goes down after upgrading
CSCsv44923	Unknown	MAC move behind phone leads to lost connectivity with MAB
CSCsv52426	Unknown	GRE Recirc index is 0x0 in adjacency hence encap operation fails on DFC
CSCsv57235	Unknown	duplex is changing automatically on WS-X6148-RJ-45
CSCsv57305	Unknown	VSS: software forced reload with 100Mbps SFPs in supervisor uplink ports
CSCsv58279	Unknown	Reload due to Address Error with multicast configuration
CSCsv60643	Unknown	sup4 when toggled 10g mode the config is not synced to standby sup
CSCsv64079	Unknown	SXF7: Patching fails with WiSM Card on Cat6500
CSCsv66706	Unknown	IDSM port-channel Allowed-Vlan statements lost on reload
CSCsv66827	Unknown	Clearing the SSH session from a different vty session crashes the box.
CSCsv73299	Unknown	L2 multicast forwarding broken with DHCP snooping & TTL rate-limiter
CSCsv74607	Unknown	Pid 21: Process "IPC Seat Manager" stack 0x4732A474 savedsp 0x5002AE98
CSCsv75511	Unknown	VSS:NAM on standby switch can't reach netwk after unconfig re-config ...
CSCsv76509	Unknown	Cat6k/MSTP in compat mode BPDUs sent in VLAN1 regardless of config
CSCsv85551	Unknown	SP crash due to consume all scp triggered by OIR loop when PS go off
CSCsv86288	Unknown	Sending a hello response with a session-id element causes a crash
CSCsv92872	Unknown	10GE link on Sup720-10GE takes more than 30sec to go down during crash
CSCsw17478	Unknown	PVT HOSTS- ports programmed with incorrect rdt index upon bootup
CSCsw18793	Unknown	VRF-PBR: TCAM adjacency not programmed with multiset policy order after
CSCsw25255	Unknown	Rapid PVST : Slow convergence unless debug spanning event is turned on
CSCsw31607	Unknown	LTL index incorrect in PI MET table
CSCsw39798	Unknown	Sup32 failover causes line protocol down to IP phone with dot1x config
CSCsw41168	Unknown	%ALIGN-3-SPURIOUS at sm_get_portEntPhyIndex
CSCsw41439	Unknown	W21,VSL,SNMP,cvsCoreSwitchPreempt,cvsCoreSwitchPriority not SSO aware.
CSCsw43953	Unknown	Card not identified SIP Is OIR'd during Standby SUP bootup
CSCsw45396	Unknown	when STP recovered in uplinkfast,no sent dummy multicast packets
CSCsw48824	Unknown	Switchport Block Unicast - prevents RTP on same VLAN
CSCsw51395	Unknown	Proper handling is required for Mac-Filter with Port-security
CSCsw53362	Unknown	c2w2b: Device crashes with NAT stress test
CSCsw59517	Unknown	IGMPv3 snooping drops 'Block Old Sources' report
CSCsw73302	Unknown	memory leak in qm_increment_ag_policer_usage on standby-rp
CSCsw82732	Unknown	VPN-SPA internal vlan interface wedged in SXH4
CSCsw87352	Unknown	6748's port can not forwarding traffic - port src index wrong
CSCsw87563	Unknown	packets with multicast mac and unicast ip are software routed by cat6500
CSCsw90798	Unknown	Bus error crash after configuring vlan name change
CSCsw98231	Unknown	SDBY stuck @ CEF RRP RF Client(5025) after ISSU RV

Identifier	Technology	Description
CSCsx16206	Unknown	Traffic loss issue from SFM capable modules to other device through DEC
CSCsx37615	Unknown	VSS: rem comm standby-rp sh plat hardware capacity may reset switch
CSCsx39263	Unknown	TCAM entries are not installed for TCP intercept after SSO
CSCsx70229	Unknown	Add the symbols back in SXH throttle which were removed by CSCsw82732
CSCsx76308	Unknown	HA client crashing attempting to free unassigned memory
CSCsx83443	Unknown	crypto debug condition leaks messages which lead to high cpu.
CSCsy22802	Unknown	MPLS VPN broken, vrf connection (permit missing for internal vlan acl)
CSCsy24691	Unknown	entPhysicalTable has power-input 3 Sensor for 6kW DC PS1 and not PS2
CSCsy79691	Unknown	RP crash with dot1x critical authentication configured
CSCsy83830	Unknown	IOS-RLB crashes while deleting the username sticky
CSCsy96102	Unknown	FM-4-MPLS_RSVD_VLAN_ERROR-failed to remove feature when vrf delete
CSCsc67488	WAN	ARP Req from Frame Relay causes %IP-4-ZERO_ADDR: Zero MAC address Error
CSCso62193	WAN	Standby resets due to parser return error "no frame-relay vc-bundle"

Caveats Resolved in Release 12.2(33)SXH4

Resolved Infrastructure Caveats

- [CSCse85652](#)—Resolved in 12.2(33)SXH4

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/netmgmt/configuration/guide/nm_http_web_ps6350_TSD_Products_Configuration_Guide_Chapter.html

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

Other Resolved Caveats in Release 12.2(33)SXH4

Identifier	Technology	Description
CSCef97900	AAA	AAAA-3-DROPACCTLOWMEM warning message somewhat misleading
CSCsl29214	AAA	AAA server change leads to bus error crash after "show run" is issued
CSCsu42152	AAA	authorization fails if fallback method is "if-authenticated"
CSCsu21040	AAA	Enable authentication prompts for username/password instead of just pass
CSCin45879	AAA	Router reloaded with radius reorder & dead server & server-private
CSCsl47365	AAA	TACACS+ authorization should ignore unknown attribute
CSCsq31981	Content	WCCP: redirection does not work with CEF and ip accounting
CSCsr60789	Infrastructure	W1.3: VSL crash after preemptive switchover in ifs_open_file_decrement
CSCsr50834	Infrastructure	CPU HOG after changing logging buffered up to 50MB
CSCsj06593	Infrastructure	CPU hog msgs for RFSS worker process and Async write process
CSCsj52992	Infrastructure	CPU hogs when configuring snmp-server host
CSCso21611	Infrastructure	Crash at internal idb counter increment function
CSCsq16325	Infrastructure	Incomplete serial interface command creates interface
CSCsi88974	Infrastructure	LI: Malloc failure on setting MD src interface as Loopback interface
CSCsm32392	Infrastructure	memory corruption crash at nv_ifs_open and nv_ifs_close
CSCsq34676	Infrastructure	Modular IOS: show process cpu sorted triggers unexpected reload
CSCsu37266	Infrastructure	Modular IOS: tcp.proc terminated due to signal SIGSEGV
CSCsh45091	Infrastructure	Port fix for CSCed94684 for ws-c3750-24p
CSCsm01126	Infrastructure	PRE-B crashes while in progress to standby cold-config
CSCsr64361	Infrastructure	Standby continuously resetting due to SNMP RF client notification timeout
CSCsq03621	Infrastructure	Timestamps in "show rmon events" wrap at 2^32-1 milliseconds (7+ weeks)

Identifier	Technology	Description
CSCsq35093	Infrastructure	XDR-6-XDRIPCNOTIFY: Message not sent to slot 1/0 (1) because of IPC
CSCsk91176	Infrastructure	PXF crash causes IPC timeout to all linecards in the chassis
CSCsh63508	Infrastructure	disk0:/sys/cpmbit/base is busy, try again later msg on stby SP on SSO.
CSCsm14366	Infrastructure	Empty crash file generated on wan module crash at boot-up
CSCsj54606	Infrastructure	end of summer-time can be set earlier than start of summer time
CSCsq60922	Infrastructure	Modular IOS:Router crashed with SNMP copy and with format in console
CSCsm78184	Infrastructure	Switchover failed with %C10KISSU-3-GET_MSG_MTU messages
CSCsm47417	Infrastructure	W2:setting ceExtSysBootImageList cause "wr mem" not working correctly
CSCsr55990	IPServices	HSRP mac dynamic on routed pseudowire after reload on active router
CSCsm35794	IPServices	Ignoring Coup after changing HSRP active router's priority
CSCsq90529	IPServices	Issue with active ftp on the SXH1
CSCsq60504	IPServices	Modular IOS Sup720: crashed with tcp timeout logs
CSCsu21716	IPServices	No unsolicited igmp report sent for mroute-proxy
CSCsq97870	IPServices	Router crash with 'show standby' if group deleted from 2nd terminal
CSCsm79082	IPServices	RP crash at dispatch_thread_pool when restarting tcp.proc
CSCsi66366	IPServices	All transport protocols are displayed in running config for VTY
CSCsr08771	IPServices	Crash seen @ dhcpd_pool_nvgen and dhcpd_copy_bootfile
CSCsj83854	IPServices	Incorrect static nat entries programmed in nat table
CSCsg87930	LAN	i82543 driver should not increase input queue drop counter
CSCsr76818	LAN	input queue wedge on SP due to VTP packets
CSCsh33167	LegacyProtocols	Dlsw transparent cache holds MAC address for disconnected circuit
CSCsr93672	Management	Native vlan is not getting displayed in "show cdp neighbors" output
CSCuk57502	Management	CDP does not report IPv6 addresses for Modular IOS.
CSCsq79032	Management	Excessive remote registry invocation on 'waiting_on_switchover' registry
CSCsq84595	Management	high # of remote reg. invocation (35 rpc/sec) 'get_unidirectional_mode'
CSCsq78822	MPLS	Cannot clear specific LDP neighbor, when router-id not in bound address
CSCsq46044	MPLS	Error MFI_LABEL_BROKER-3-DELETE_MOI_FAIL and LSD_CLIENT-3-PCHUNK2
CSCsq91960	MPLS	failed to delete vrf when it is 32 characters long
CSCso21506	MPLS	Import Map under vrf blocks bgp aggregate prefix
CSCsr40433	MPLS	mpls te - explicit path with loose nhops - re-optimization failure
CSCsu62667	MPLS	LSP ID change after SSO due to failure in signalling recovered LSP
CSCsm70668	MPLS	OIR over E3:POS impacting complete Traffic with biscuit tunnel
CSCsq93004	MPLS	Possible memory corruption with TE auto-tunnel primary and subinterface
CSCsr09312	Multicast	crash when doing mrm stop
CSCsm77608	Multicast	IP Multicast packets are Process switched.
CSCsu02051	Multicast	S,G expiry timer change is not allowed in Whitney1
CSCsr49316	Multicast	Crash ipv6_static_route_find after configured & executed show ipv6 rpf x

Identifier	Technology	Description
CSCsr36971	Multicast	Memory Leak @ PIM process
CSCsu71983	Multicast	Memory Leak @ PIM process
CSCsq37078	PPP	Input errors incrementing on Multilink 5 in admin down state
CSCsm28515	QoS	Marking not happening on FlexWAN interface with SXH after oir/reload
CSCsl62963	QoS	Router Crashes, Reconfigure a Policy -af_police_remove_coloraware
CSCsu03813	QoS	Upgrading from rockies to w2 deletes the police action from pmap
CSCsm00570	QoS	cwpa2 crashes at hqf_cwpa_pak_enqueue_local
CSCsg18894	QoS	Queue-limit command should be allowed in conjunction with priority
CSCso54167	Routing	BGP peer stuck with table version 0
CSCso80951	Routing	BGP peers with same policy fall into different update-group with SOO
CSCsm26130	Routing	BGP with auto-summary not injecting locally orig. route into BGP table
CSCsr83639	Routing	Bus error crash when removing BGP configuration
CSCsu24087	Routing	Cisco7609 crashes after "clear ip bgp neighbor x.x.x.x soft in"
CSCsj78403	Routing	clear ip bgp causes crash to RR client with conditional route injection
CSCsq36206	Routing	MDT tunnels not getting created on 7206 Device
CSCsk86476	Routing	OSPF fails in MTU-mismatch setup when mtu-ignore is configured
CSCsm72604	Routing	OSPF remaining summary route when dual OSPF process redistributing
CSCsq38431	Routing	OSPF "summary address" is executed, even if subnet is becoming small
CSCsq49201	Routing	Password in BGP peer-session template not inherited
CSCsi68795	Routing	PE wrongly assigns local label to a vpnv4 confederation prefix
CSCsq13938	Routing	reload on 'show ip bgp vpnv4' when import src delinked by BGP deconfig
CSCsu40881	Routing	Secondary EIGRP address on VRF not added/deleted properly to EIGRP topo
CSCsg90755	Routing	Standby keeps reloading due to PRC mismatch in IPv4 MDT AF config sync
CSCsr67562	Routing	Support for running ispf with nodes having overload bit configured
CSCsu03167	Routing	SXF15: IPv4/v6 BGP routes not cleared when source routes is gone
CSCso93535	Routing	Upon removing a VRF, BGP route timers in other VRF's get reset
CSCsk86150	Routing	w/ BGP auto-summary enabled, networks are lost from BGP after EIGRP flap
CSCsm30569	Routing	CEF path fragmentation broken for static IPsec VTI
CSCsq05602	Routing	TE tunnels are down but still show in the forwarding table
CSCso08786	Routing	Standby reloads due to config sync failure on inherit peer-policy cmd.
CSCsj39016	Routing	warn_assert failed: ../fib/fib_table.c:2947 tal_tree_get_item_count_nonf
CSCsm50741	Routing	Removal of DCbitless LSA causes problems
CSCsr96042	Routing	ASR: IOSD crashes at bgp_vpn_import_walker while unconfiguring vrf
CSCsu36709	Routing	Unable to boot IOS image on PE (vrf-enabled) router - software fault
CSCsr86489	Security	C6k: SCP file copy causes RP crash during authorization of user
CSCsq58748	Security	IPSEC: IKMP process can get blocked by some PKI OCSP requests
CSCsf17406	Security	Large CRLs can cause memory leaks

Identifier	Technology	Description
CSCeg49153	Security	PKI: crl checking takes too long to timeout if the server is down
CSCsg48392	Security	Resuming SSH Session Fails After Disconnecting Another One (Not Console)
CSCsq60016	Security	Router crashes when entering a long RSA key string
CSCsd81870	Security	Teraterm + TTSSH2 does not work in SSH Ver.2
CSCso48959	Security	user not reported by "login on-success log" feature for SSH logins
CSCsr85093	Security	SXF15: SSH session fails withRSA signature verification failed after SSO
CSCsm82472	Unknown	DAI: L2-Portchannel formed for member's DAI trust mismatch
CSCsq98887	Unknown	Packet drop on applying and removing ACL on tunnel interface with pim
CSCsj51113	Unknown	crash in ether_cfm_tm_send
CSCsu48150	Unknown	Enhancement to Me_Kr register dumps from CSCsg21809
CSCsu22349	Unknown	Removing ACL or service policy from vrf interface drops traffic
CSCso27956	Unknown	TCAM ASSERT FAILURE on LI stress with add/removal of lots of streams
CSCsu81785	Unknown	6500 can no longer receive the ACL as filter ID from
CSCso71955	Unknown	Alignment errors with netflow on Interface, crash on 7600/6500
CSCso30038	Unknown	A OIL is not registerd properly in mroute table with static igmp group
CSCsm08087	Unknown	Arp unresolved after sh/nosh of egress int ;route-map applied at ingress
CSCsq51378	Unknown	ATM PA Interface shows up/up after force redundancy, no cables connected
CSCsm75286	Unknown	bgp route-map doesn't work correctly when deleted part of sequences
CSCsr18656	Unknown	BPDU bit is over written when 2nd PCL lookup is enabled.
CSCsr37131	Unknown	buginf calls in l2trace when 'debug l2trace' is disabled
CSCsq94136	Unknown	Burst of traffic cause anti-replay check to fail
CSCsu94880	Unknown	Bus error crash at fm_format_inband_adj_data
CSCsm64424	Unknown	C2W1: Copy command generates spurious authorization requests
CSCsr81962	Unknown	C2W1: Monitor session servicemodule causes internal loop on SUP720-10GE
CSCsm26063	Unknown	C2W2:Active RP Crash on sh/no sh of intf with ipv6 address configured
CSCso60528	Unknown	C2W2: FWSM - Standby FWSM PO shows down and links go down eventually
CSCso74559	Unknown	C2W2: Mago IOS "test Crash" create crashinfo file on bootflash only
CSCsu05800	Unknown	C2W2: need to extend the wait time for bus sync after sso
CSCsq44850	Unknown	c2w2 : TB seen at %PM-3-INTERNALERROR: Port Manager Internal Software Er
CSCsr93467	Unknown	c2w2:Traceback seen while doing "switch accept mode virtual "
CSCsq80270	Unknown	Cat 6k crashes randomly after IPSec SPA module is inserted.
CSCsm43962	Unknown	Cat6k L2TP packet looped through blocked port
CSCsq84116	Unknown	Cisco 7604 with OC3, Flexwan crashes into ROMMON
CSCsu49002	Unknown	ciscoIpMRouteBps sometimes indicates wrongful value
CSCsr08985	Unknown	CMM ports going to shutdown state on reload in Whitney 1
CSCso05920	Unknown	cpmCPUMemoryFree incorrect for Posix memory
CSCso29141	Unknown	DFC installs drop index for MAC-address

Identifier	Technology	Description
CSCsv34415	Unknown	Diag failure on power-cycle puts VSS switches in rommon
CSCsu76070	Unknown	duplicate packets when lawful intercept is enabled
CSCsl27957	Unknown	%EC-SP-5-CANNOT_BUNDLE2 is seen after inserting WS-SVC-FWM-1
CSCsq77043	Unknown	EEM long hostname prevents tcl cli_open from functioning
CSCsu63335	Unknown	"Failed to find process pid" error message on 12.2(33)SXH3
CSCsu33221	Unknown	"Flood in diag inband driver" messages followed by silent reload.
CSCsr06914	Unknown	fm_slb_inbad_send():Invalid Flowmask errors upgrading to 12.2(33)SXH2a
CSCsr99933	Unknown	FWLB: High purge rate causes CPU to increase by 15%
CSCsl02190	Unknown	ICMPv6 to all node multicast address fail .
CSCsr45851	Unknown	ifOperStatus for Control Plane Interface is always down
CSCsu91714	Unknown	IGMP-JOIN is lost from SUP to MSFC
CSCek37984	Unknown	Inconsistent BERT behaviour observed on TE1 SPA
CSCsm11898	Unknown	IOS:SLB: Incorrect NAT Translation when Nat client is enabled
CSCso93708	Unknown	IPsec-HA:RFclient timingout on7200 running 12.4(15)Tx, AdvSecurity fse
CSCsr18924	Unknown	kernel idle hook thread in IOS-Base taking 50% CPU
CSCsq83789	Unknown	LTL for unknow unicast is wrongly programmed for some L3 interfaces
CSCsq94366	Unknown	Mem leak in rrp_update_peer_info_on_rp
CSCsk34832	Unknown	Memory leak in HTTP CORE PID 174
CSCse12518	Unknown	MET optimized update can cause blackholing and duplicates
CSCsq51249	Unknown	Monitor session removal may affect traffic through WS-X6148A-RJ-45
CSCsr09554	Unknown	Move SIBYTE SB_RMON_OVRFL messages under debug
CSCsu37481	Unknown	Netflow Incorrect Octet value with packet-based sampling
CSCsr66588	Unknown	Netflow SLB aging parameter values are not synced to SP after reload
CSCsq89415	Unknown	"no bert" indicates "abort request" instead of "stopped"
CSCsu68698	Unknown	No syslogs and stack on console when SP crashes due RP boot timeout
CSCsq85850	Unknown	Opnext GLC-LH-SM :remote port stays up when local RX cable is removed
CSCsq37376	Unknown	Packet Buffer Capture May Crash a 6500 in IOS
CSCsq46590	Unknown	Packet loss during SSO failover on ECMP supervisor uplinks
CSCsr51799	Unknown	pa-mc-8t1 interface down after stopping BERT prematurely
CSCsr45495	Unknown	PBR with deny statements : TCAM running out of masks
CSCsu29117	Unknown	PE send traffic back to EoMPLS tunnel after lsp path changed
CSCsq79253	Unknown	Pinnacle interrupts not re-enabled after memory inconsistency detected
CSCsu72496	Unknown	%PM-3-INTERNALERROR: Port Manager Internal Software Error
CSCsq36972	Unknown	Portchannel does not form. Log messages indicate misconfig.
CSCsq59297	Unknown	port-channel IDB gets mixed up
CSCsu03297	Unknown	RE: Fabric force bus-mode does not work anymore
CSCsq97640	Unknown	Resetting Standby Sup4 multiple times causes lincocard switchbus timeout

Identifier	Technology	Description
CSCsu95605	Unknown	Route-map with "match route-type local" not functioning properly
CSCso98143	Unknown	Router crash at pm_platform_private_alloc_and_reserve_vlan
CSCsr63831	Unknown	show platform hardware capacity fabric - incorrect % and time-SXH3
CSCso88772	Unknown	sp-inband tx capture causes primary SUP to hang
CSCsu24825	Unknown	SUP32 unstable to communicate with all neighbors after reload
CSCsu44534	Unknown	Sup NSF/SSO causes 4 sec traffic loss over EC with uplink ports.
CSCsu46124	Unknown	SVI ifInMulticastPkts ifOutMulticastPkts are always zero
CSCsh57238	Unknown	SXF6:sh int cmd on 6148 cards display zero o/p drops even with qos drops
CSCsl37513	Unknown	SYS-2-MOD_TEMPSENSORFAIL:Module w/ X6148A-GE-45AF and CatOS
CSCsr78910	Unknown	time not updated in 'System returned to ROM by reload' in show version
CSCsq15308	Unknown	timer not stopped properly for eem policy scripts
CSCso28275	Unknown	Traffic polarization within a MEC on VSS.
CSCsq14259	Unknown	TX Flowcontrol goes on when link negotiation is disabled
CSCso35250	Unknown	unexpected reload while communicating with CNS server
CSCso57886	Unknown	unrestricted while loop when looking for EOS flag in the packet
CSCsu45210	Unknown	Upgrade 12.2SXF-> 12.2SXH with Port-Security causes standby boot loop
CSCso48665	Unknown	vlan filter can't be removed totally
CSCsq53085	Unknown	VS: 15 seconds down time upon module reset
CSCsq61089	Unknown	VS2: physical OIR of 6708 causes 16 seconds interruption
CSCsk94870	Unknown	VS2: TB @ ether_extract_addr
CSCsq80891	Unknown	VSS switches reload at the same time after VSL link failure
CSCsu31651	Unknown	VSS: Traffic dropped on non-bundled port if RBH=0
CSCsr55523	Unknown	WCCP service group ID is zero in ACL TCAM Adjacency
CSCso88042	Unknown	Wism module Allowed-Vlan statements lost on reload
CSCsr72427	Unknown	WS-X6148-45AF/WS-F6K-FE48-AF %ILPOWER-5-ILPOWER_MISCONFIG after reload
CSCsq63727	Unknown	WS-X6748-GE-TX - input and output errors seen during auto negotiation
CSCsr82501	Unknown	Change global function to static breaks install patch feature in SXH
CSCsq91258	Unknown	L2 entry purged from hardware when in use by L3 shortcut
CSCsu55635	Unknown	Load values of PO members with Fixed algo get 0 during bootup on Standby
CSCsm28287	Unknown	Active RP crash on shutdown of GRE tunnel followed by switchover
CSCsq56747	Unknown	Active SP CPU 100% after SSO switchover with 080527 ION image
CSCso86544	Unknown	Afer SSO, new active SP crashes @ pm_vlan_get_portlist
CSCsk73838	Unknown	After fabric tiemout is seen, line card did not recover using earl patch
CSCsq51231	Unknown	ALIGN-3-SPURIOUS: Spurious memory access made @ idbman_get_port_swidb
CSCsm79344	Unknown	Bogus "TCAM MASK entry capacity exceeded" message
CSCsq04075	Unknown	C2W2:DHCP Snooping entries not cleared after removing IP Source Guard
CSCsu73128	Unknown	C2W2-ION-080922: Crash on Plain IPSec tunnel setup

Identifier	Technology	Description
CSCsq81235	Unknown	Cannot configure a vrf again when deleted using 'no ip vrf' command
CSCso66357	Unknown	Classification on nbar fails on removing pmap from other pvc on ATM M2P
CSCsl39691	Unknown	Config Sync: Bulk-sync failure due to Servicing Incompatibility after SSO
CSCsu82768	Unknown	Crash at pclc_g2_fw_offline_notification after SSO
CSCso85133	Unknown	DOM tranceiver "voltage" values are always Zero in SUP4
CSCsu03772	Unknown	Dot1q native vlan tagging is not working with "switchpot nonegotiate"
CSCsm48287	Unknown	Drop counters for VPLS VC not incrementing
CSCso49344	Unknown	Egress policing policy not programmed in SIP-600 after system reload.
CSCsr96283	Unknown	High CPU due to add/del SPAN configs
CSCso39818	Unknown	Ingress Marking not working on SIP-600 on linecard reset/ toggle mlsqos
CSCso18683	Unknown	IP DSCP Re-circulation not working as expected after issu runversion.
CSCsq82991	Unknown	IPSG Pacl entry appears after the ISSU RV or SSO
CSCso32193	Unknown	IPv6 software switched in Egress replication mode
CSCsq73317	Unknown	MAB authorization failed with port-security
CSCsr02723	Unknown	MDEBUB: Spurious memory access detected at env_sensor_get_update
CSCsr75094	Unknown	MDEBUB: Spurious Memory Access on SSO
CSCso72541	Unknown	%MFIB_STATS-DFC2-2-MFIB_STATS_LC_FAILED_GET_COUNTERS for Sip 600
CSCsu72884	Unknown	Modifying match criteria frm v6 to v4 doesnt change tcam label state
CSCsj04201	Unknown	%MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC: RP failed allocating IPC buffer
CSCsk78390	Unknown	Naxos crashes while trying to fpd upgrade granikos
CSCsr13633	Unknown	%PM-3-INTERNALERROR: Port Manager Internal Software E
CSCsl32940	Unknown	Router crashes while reloading Naxos
CSCsm08971	Unknown	SEA: Soft reload occurs everytime after issue show cmd's and T/B with mz
CSCsm66602	Unknown	SIP 400 loses VPLS VC entry on shutting down the MPLS TE tunnel
CSCsq83219	Unknown	Standby SP crashed at sp_reset_slcp after "redundancy reload peer"
CSCso00864	Unknown	Standby sup crashed on configuring local-address command for cry map
CSCsq67001	Unknown	Standby switch reloaded by auto qos on MEC standby member port
CSCsm19550	Unknown	sup720 rx intr should check tx descriptor exhaustion
CSCsr07565	Unknown	TCAM didn't reprogram after removing dynamic ACE
CSCsm84267	Unknown	Tracebacks & %CPU_MONITOR-SP-6-NOT_HEARD: messages with NAT.
CSCsk19866	Unknown	Unable to boot boomerang image on sup720
CSCsr48938	Unknown	UNBL: bootldr image can't boot on SupW
CSCsm85936	Unknown	UUT cpu at 40% with bi-dir traffic across a single tunnel
CSCsm22385	Unknown	V4 VPN traffic stops after toggling agg. label between vpn-cam and tcam
CSCsr58773	Unknown	VS2: After SSO, VSL member stuck in "w" state, and MEC errors
CSCsk89852	Unknown	VS2: MEC (LACP) members flap when native subinterface is configured
CSCsr20679	Unknown	VSL PO as SPAN source and Orphan PO as SPAN destination not allowed

Identifier	Technology	Description
CSCso57020	Unknown	VSS: After sso, the RBH values on orphan PO flips w/o link/po flapping
CSCsq78513	Unknown	VSS: Etherchannel counters incorrect
CSCsq77381	Unknown	W2: Diag - TestL3Capture2 failed after LV-SSO
CSCsq21051	Unknown	W2: Heathland mode change doesn't work after the second SSO switchover
CSCso72178	Unknown	W2:TestCapture,TestTrap & TestIPv6FibShortcut diag failed ondemand&boot
CSCsq26223	Unknown	WS-X6348-RJ-45 Blackholing traffic/reset continuously
CSCsm65386	Unknown	WS-X6516A-GBIC card resets on SSO.
CSCsm40606	Unknown	WS-X6724 SFP get's reboots again and again with TestSynchedFab Failed
CSCsv30359	Unknown	HSRP: CPU hog when no failover bound to crypto
CSCsu57958	Unknown	DHCP-Snooping not intercepting DHCP messages from the Server
CSCsr49669	Unknown	Match protocol arp doesnt work in whitney1 earlier it was working for Roc
CSCsl18525	Unknown	Standby-SP doesn't have mfib table
CSCsv43802	Unknown	High CPU utilization triggers crash in diags.
CSCsq82663	Unknown	SLB router CPU usage is high with GE interface
CSCsl71704	Unknown	VS2:RACL not applied on MEC after disabling netflow & chng flowmask
CSCsq81116	Unknown	c2w2:Device crash @ oer_cc_free_message while unconfiguring
CSCek40773	Unknown	CE-CE connectivity broken on MPLS VPN with GRE tunnel in VPN core
CSCsk32209	Unknown	Crash seen on a stand-alone router while generating RSA keys
CSCsj32493	Unknown	IPSEC: Incorrect IPsec connection info in InvalidSPI testing
CSCek71010	Unknown	TB seen at bgp_oer_notify_pep bgp_oer_remove_path bgp_bestpath_old
CSCsu59556	Unknown	Traceback seen @ fibidb_init
CSCsq85139	Unknown	VS2: Can not establish session to standby NAM
CSCsq78956	Unknown	strepv of binary can cause mem corruption
CSCsr26663	Unknown	C2W2: GLBP 800 peers with default timers flap after SSO
CSCsu69177	Unknown	C2W2: Traffic drop after SSO on SUP4 P router w/ IP and MPLS traffic
CSCso29226	Unknown	IP source guard is not supported on ether channel member
CSCsr02816	Unknown	ISSU tracebacks seen on SP during runversion at MsgReceive.S:14
CSCsj06641	Unknown	LI: Traceback found in creating entry in cTap2StreamTable
CSCso28791	Unknown	MAC_MOVE-SP-4-NOTIF seen for L2TP packets over dot1q tunnel
CSCsq04274	Unknown	Memory leak observed on l2_vlan_stat_mem_allocate during vlans creation
CSCsj90758	Unknown	UUT with BGP/DMVPN crashes after restarting iprouting.iosproc
CSCsu64581	Unknown	Last port of T3/E3 SPA connected back to back does not ping
CSCsg32308	WAN	copy/paste of ntp-authentication-key statement is not possible
CSCsq47900	WAN	OIR operation on POS interfaces with APS result in ALIGN error
CSCsq18856	WAN	FR SVCs cannot be setup

Caveats Resolved in Release 12.2(33)SXH3a

Resolved Infrastructure Caveats

- [CSCse85652](#)—Resolved in 12.2(33)SXH3a

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/netmgmt/configuration/guide/nm_http_web_ps6350_TSD_Products_Configuration_Guide_Chapter.html

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

Other Resolved Caveats in Release 12.2(33)SXH3a

Identifier	Technology	Description
CSCsu03167	Routing	SXF15: IPv4/v6 BGP routes not cleared when source routes is gone

Caveats Resolved in Release 12.2(33)SXH3

Resolved IPServices Caveats

- [CSCek52673](#)—Resolved in 12.2(33)SXH3

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

Workaround: None

Resolved Security Caveats

- [CSCsi17158](#)—Resolved in 12.2(33)SXH3

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

- [CSCsk93241](#)—Resolved in 12.2(33)SXH3

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

Cisco has released free software updates that address this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20080924-mfi.shtml>

Other Resolved Caveats in Release 12.2(33)SXH3

Identifier	Technology	Description
CSCdu79630	AAA	Username on vty not displayed if accounting is not configured
CSCsg18288	AAA	Enable authentication ignores Tacacs+ configuration in rare situation
CSCsl10068	AAA	AAA api migration in login.c, exec.c .
CSCsl45701	AAA	TACACS+ per VRF authen failing: Address already in use
CSCsl57645	AAA	tacacs-server directed-request fails for enable authentication on 6500
CSCso87641	AAA	Tacacs unable to connect to server
CSCso95426	AAA	Exposure of Radius-Keys in debugs.
CSCsq98160	AAA	No communication between SW and AAA with IPBase image
CSCsr26098	AAA	SSH/Telnet failed with IPBase image on Sup32 with AAA server
CSCei33231	ATM	ATM PVC bundle protected group test failed with bumping exhausted
CSCek74474	ATM	no/default proto ip inarp cmd ineffective until ATM VC bounced.
CSCsh98378	ATM	Router crashes at atm_create_vp_db
CSCsi72854	ATM	Inconsistent IMA CLI after router reload .
CSCsk72676	ATM	Pvc not coming up after removing vc-class from it
CSCek58956	Infrastructure	Need process_ok_to_reschedule check in process_may_suspend
CSCsa97971	Infrastructure	IOS SLB TCP probe state toggles
CSCsb06920	Infrastructure	SYS-3-MGDTIMER: Running timer -Process= SAA Event Processor
CSCsd37499	Infrastructure	%IFS-3-FSMAX: Failed to add ?, maximum filesystems 64 msg with Traceback
CSCsh96179	Infrastructure	IPSLA pathEcho probe doesn't complete for all hops
CSCsj52693	Infrastructure	ospf neighbor flap with fast hellos and 16 neighbors
CSCsk70446	Infrastructure	NRT: tracebacks @ data_inconsistency_error - 7200 for HTTP config .
CSCsk99687	Infrastructure	crash seen during ISSU runversion in ipc_open_port
CSCsl60092	Infrastructure	Active SP crashed @ipc_fragment_cleanup with VSL shut/no shut test
CSCsm49218	Infrastructure	Missing traceback for jump to zero exceptions
CSCsm77199	Infrastructure	DATA CORRUPTION-1-DATAINCONSISTENCY HTTP_FIND_FLASH_FILE
CSCsm89735	Infrastructure	Router crashes on giving show idb after sessions are down in PPPOE-ipv6
CSCso02960	Infrastructure	%RTT-4-DuplicateEvent causes tracebacks after upgrading to 12.2(33)SXH
CSCec51750	IPServices	Router reloads do to bus error. and illegal access to low address
CSCeh69721	IPServices	%SCHED-3-CORRUPT:Schedulerevent magic corrupted by TFTP Server
CSCsb85982	IPServices	Router reloads@ add_or_create_more_soc_buckets
CSCsi42225	IPServices	We need improvement for ip igmp limit command
CSCsk83505	IPServices	%L3_MGR-3-REQ_SEND:error packet allocation after Remote HL HW reset
CSCsk96976	IPServices	DHCP Option 66 adds more quotation marks around URL after reload .
CSCsl51945	IPServices	HSRPv6: Config Sync and standby resets with standby 1 ipv6 <>
CSCsm59037	IPServices	no service dhcp command causes switch to reload
CSCsm70580	IPServices	c2w2:ciscoFtpClientMIB: ftp_fs.proc extra processes can deadlock & crash

Identifier	Technology	Description
CSCsm92206	IPServices	Router crashes when set the range of interfaces to default configs
CSCso68344	IPServices	Switch acting as DHCP server crashes on issuing no service dhcp command.
CSCso91230	IPServices	%LINK-2-INTVULN: errors with MLPPP and HWIC-4ESW
CSCsq14698	IPServices	crash when using nat with multicast traffic
CSCsq48201	IPServices	c7300:Bridge IRB-Router crash and traffic flow issue
CSCsq67478	IPServices	SSH session hangs
CSCsl54243	LAN	7600 SIP-400 crash after removing sub-ints; lc_deencap_dot1q_vlan
CSCeh97382	Management	Device reset when polling IKE/IPSEC MIB
CSCsk38681	Management	VS2: remote registry call messages ~ cdp2.iosproc:1
CSCsq79132	Management	Excessive remote registry invocation on 'proto_on_swidb' registry
CSCsj50412	MPLS	Improper handling of remote binding wrt route info
CSCsk42307	MPLS	MPLS-TE CBTS: Sending out OSPF hellos over master tunnel .
CSCso53377	MPLS	All TE Lsps does not recover after SSO switchover
CSCek75931	Multicast	LNS: %SYS-3-CPUHOG When sessions have multicast
CSCsk26429	Multicast	Router configured for IGMP Proxy may not send IGMP Join
CSCsl10316	Multicast	ipv6 pim join-prune-interval 10 sets the interval to 20 seconds .
CSCsl20158	Multicast	SNMP:msdpPeer counters should be able to compare with CLI counters.
CSCsl92316	Multicast	LNS: %SYS-3-CPUHOG when clear l2tp tunnel, sessions have multicast
CSCsm17426	Multicast	RP-bit not cleared on s,g; traffic outage for 4 minutes
CSCsm44620	Multicast	Shutdown interface present in PIM interface list
CSCsm48322	Multicast	IPv6 Multicast RP ignores embedded RP register messages
CSCsm53766	Multicast	Reload due to Address Error with multicast configuration
CSCsq09962	Multicast	7600 : crash at "pim_proxy_empty_rd"
CSCsq14151	Multicast	RPF of (S,G) is set to NULL, When (S, G, R) entry is convered to (S, G)
CSCse40966	PPP	MLP links down after SSO switchover if aaa new-model cfged
CSCek63203	QoS	CEOP:VH:Ctrl+C while display show policy int cause console freeze
CSCsm29181	QoS	Crash when NBAR applied to sub-interface
CSCsm49062	QoS	cwan2: show queueing interface reports double count for wfq drops
CSCek36995	Routing	0.0.0.0 default route increasing on rip DB with object tracking
CSCse65277	Routing	MU:default isis metric maximum returns parser error
CSCsf06946	Routing	Removing loopback interface causes continuous standby RP reloading
CSCsi87894	Routing	RIP advertise default route after 'no default-information originate'
CSCsi98730	Routing	CEF/BGP table MPLS label mismatch in IOS 12.4(6)T5
CSCsj21785	Routing	TE tunnel does not reoptimize after mtu change
CSCsj56281	Routing	BGP inherit peer-policy not working after router reload
CSCsk37659	Routing	Vrf route table does not get updated once pppox sessions are up.
CSCsl04835	Routing	BGP conditional route injection not removing routes from iBGP peers

Identifier	Technology	Description
CSCsl06336	Routing	removing 'maximum-paths import 6' causes duplicate paths in VRF table
CSCsl20856	Routing	standby HSRP flaps with ospf mib polling/aggressive timers/nostandby sso
CSCsl30331	Routing	Prefixes permitted despite the deny action on route-map continue
CSCsl72774	Routing	Memory leak in CEF consistency checker
CSCsl84712	Routing	Error- %OSPF-4-FLOOD_WAR: Process 123 re-originates LSA ID 10.55.122.148
CSCsl92283	Routing	Unable to add into routing table if static route use interface + gateway
CSCsm04442	Routing	Router crash at rip_find_sum_idb
CSCsm39159	Routing	ARP HA cpu hog on stby while bringing up stby with large arp tables
CSCsm43938	Routing	stby resets when large config/arp table to sync over to it
CSCsm45634	Routing	BGP VPNv4 route is not actived immediately after receving update
CSCsm47111	Routing	FIB: Accessing freed memory while dequeuing
CSCsm91801	Routing	ASBR not updating metric in LSA-5 redistributing from 2-nd OSPF process
CSCsm96785	Routing	"nsf cisco" under router ospf config does not work, but "nsf ietf" works
CSCso00383	Routing	MVPN: New style PE doesn't send RD Type 2 MDT update
CSCso27510	Routing	Removing SVI with IPv6 address with 'no int vlan' crashes the router
CSCso30199	Routing	ISIS topology broken after a force-switchover when ispf is enabled
CSCso62166	Routing	Crash @ bgp_netlist_validate when ibgp established with metric
CSCso63693	Routing	ISIS: Maximum circuit limit (255) has reached with passive-interface def
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
CSCso89675	Routing	Device crash @ ip2access_add_pbacl_item with largre PBACL configuration
CSCsq62703	Routing	Router crashed with TLB (load or instruction fetch) exception
CSCsq75944	Routing	crashes in ipflow_ager, ipflow_sub functions, ipflow_periodic
CSCeh48777	Security	tunnel interface fluctuates between UP/DOWN state during ipsec rekey
CSCir01449	Security	Sync damage of CSCin74155 fix
CSCsb58633	Security	SCP server gives files with invalid checksum on some router platforms
CSCsb80803	Security	SSH Process: SCHED-3-UNEXPECTEDEVENT error message
CSCse12154	Security	Bus error crash after executing secure copy (scp)
CSCsk75078	Security	rcv client_input_channel_req: channel 0: unknown channel
CSCsl61311	Security	New SSH sessions with RSA key sometimes fails after changing hostname
CSCsm57122	Security	Scp and ssh failing with certain ssh clients
CSCin67287	Unknown	NxDS0 BERT capability on PA-MC-8TE1+
CSCsc24015	Unknown	Parser loops infinitely for match route-type [ext
CSCsc85962	Unknown	Replaying Main Mode packet causing IKE SA deletion
CSCsd69625	Unknown	EZVPN:IOS C876 Client can't connect to ASA using digi certs and noXauth
CSCse31572	Unknown	Bus error at crypto_ikmp_config_authenticated
CSCse53517	Unknown	WiSM: Tracebacks seen after SSO switchover

Identifier	Technology	Description
CSCsg22830	Unknown	Standby not coming up after sso switchover
CSCsg87747	Unknown	RECV_PVID_ERR message received with bringing up etherchannel trunk
CSCsh61002	Unknown	SPA-5X1GE: GE-port not transmitting after 'shut/no shut' and vica versa
CSCsi49150	Unknown	%PM-SP-4-PORT_BOUNCED: Port Gi9/3 was bounced by Consistency Check IDBS
CSCsi63649	Unknown	%SYS-3-TIMERNEG:Cannot start timer with negative offset,TTY Background
CSCsi85453	Unknown	cfg-sync failed if switchport config is pasted on active & stby restart
CSCsi94738	Unknown	8xCHT1/E1 SPA modules not in entAliasMappingIdentifier
CSCsj37398	Unknown	Properly initialize the Tycho register AC_QOS_DEFAULT_EGRESS (0x334)
CSCsj43677	Unknown	Active Sup720 crash when removing Standby supervisor
CSCsj49293	Unknown	POS Interface Output Rate (200 mbps) > Line rate (155 Mbps)
CSCsj78820	Unknown	MEM leak in Crypto IKMP process(crypto_ikmp_author_get_attributes)
CSCsj85897	Unknown	SPA-TE1-Linkrec's out of sync between SPA and LC
CSCsj86153	Unknown	Modular IOS CPU load oscillates even under constant load
CSCsj91738	Unknown	Non-ip packet with mcast-mac addr cause high CPU with VPN-SPA VRF mode.
CSCsj94539	Unknown	Spurious Alarms in PA-MC-8TE1+ may cause router crash
CSCsj98198	Unknown	When we have only 1 flow in TT, flows are not exported to MC
CSCsj98492	Unknown	Pak subblock handlers need to be part of packet library
CSCsk19817	Unknown	shut/no shut causes pm failed get pm mp semaphore
CSCsk67457	Unknown	BCP-MLP:Traffic stops flowing making one link shut on multilink
CSCsk77462	Unknown	IETF Class attribute is missing in radius accounting record
CSCsk88273	Unknown	Traceback seen @edisms on clearing counter on Active SP
CSCsk93366	Unknown	lte_rp_get_lte_update_xdr_size/fib_upd_consume_rec_meets_upd_rec crash
CSCsl04386	Unknown	%BIT-STDBY-4-OUTOFRANGE : Traceback on Bootup .
CSCsl06059	Unknown	Router crash at route_map_vrf_af_change_nh
CSCsl11335	Unknown	MVPN-MIB:Entries obtained from "ciscoMvpnBgpMdtUpdateTable" is incorrect
CSCsl11868	Unknown	With IP CEF enabled ACL is not denying packets as intended. .
CSCsl17798	Unknown	Etherchannel state inconsistent between active and standby
CSCsl28371	Unknown	SPA-IPsec-2G VRF: L2 loop and broadcast storm may occur on default vlans
CSCsl34481	Unknown	IPV6-MCAST:router crashes while unconfiguring ipv6 mcast routing
CSCsl35325	Unknown	MRIB client remains after a linecard removal
CSCsl39710	Unknown	cat6000 mac-address-table does not add entries for local fwsm mac . .
CSCsl40528	Unknown	VS2: Port-channel fails to forward unicast packets after switchover .
CSCsl53494	Unknown	C7600-SSC-400: Error message display incorrect product name
CSCsl53727	Unknown	Add UDLD interface counters for debugging purpose
CSCsl61164	Unknown	Router may crash @ipflow_fill_data_in_flowset when changing flow version
CSCsl69123	Unknown	SIP-400:QoS:Police drops MPLSCP, CDPCP negotiation packets - SRA,SRB
CSCsl70667	Unknown	12.2(33)SRB2: LC crash at fib_fib_feature_space_xdr_decode

Identifier	Technology	Description
CSCsl72912	Unknown	VS2: WS-X6708 DFC crash in local_cb1(Segment violation)
CSCsl80682	Unknown	SPA crashes if crypto acl changed
CSCsl89890	Unknown	VS2: crash in psecure-process_timer
CSCsl93559	Unknown	Unsupported ISL encap CLI option should be disabled on 6716
CSCsl94393	Unknown	OPNEXT / Sup32 uplink port stays up when far-end port down.
CSCsl98238	Unknown	QoS statistics-export only exports to directly-connected destinations
CSCsm04256	Unknown	CPUHOG and crash after 'show memory detailed all statistics' issued
CSCsm24906	Unknown	IPv6 neighbour discovery not working on SVI intf under VRF
CSCsm32363	Unknown	Netflow SLB sw-installed entries not aging out
CSCsm37673	Unknown	Traffic from SSLM service module not going over multi-module etherchanne
CSCsm54873	Unknown	EEM some time are not triggered properly
CSCsm56279	Unknown	C2W2: Important enhancements to "test swi vir ltl index" CLI
CSCsm59039	Unknown	Message "ME_AR#0 WARNING: Cannot FLUSH Dic#0" seen for WS-X6708A-10 LC
CSCsm59384	Unknown	DPD not deleting IKE SA's
CSCsm59926	Unknown	RP receives 2 copies of each PIM register with MVPN
CSCsm59949	Unknown	vtp3:with 4k vlan HA reload/sso causes the standby to reload continuously
CSCsm69112	Unknown	Multicast output drop w/ IGMP snooping @ near line rate 1Gbps
CSCsm69827	Unknown	%SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3
CSCsm70707	Unknown	WS-X6748-SFP shutdown(Could not set appropriate Switching mode)
CSCsm70774	Unknown	Router crashes at cfg_kron_plcy_sbmd_cmd.
CSCsm71537	Unknown	divide by 0 crash in oer_br_update_iface_counters
CSCsm72807	Unknown	DHCP packets can get corrupted in an SSO environment
CSCsm75020	Unknown	EARL7 Additional ECC Error Handling enhancements
CSCsm76111	Unknown	10G ports generate CRC errors when using CISCO-FINISAR transceivers
CSCsm77171	Unknown	Router crash when "ip flow" enabled.
CSCsm77923	Unknown	C6k: Invalid vlan iface order in config after new vlan iface addition
CSCsm82264	Unknown	VS2: Entire VSS system goes down after restarting call-home process
CSCsm82958	Unknown	radius sticky entry deleted even if the idle timer is not 0
CSCsm84257	Unknown	crash in ipflow_periodic context due to watchdog timeout
CSCsm86027	Unknown	B2B failover,ace_tunnel_compare:Invalid address_type, router crashed
CSCsm94421	Unknown	Configuring STP cost in an etherchannel to the default has no effect
CSCsm99170	Unknown	Memory Leak seen in fw_lcp process
CSCsm99690	Unknown	Netflow: Crash with aggregation caches and export to MPLS VPN
CSCso00793	Unknown	ITP-76: Flexwan Memory version "VI4DP647228EBK-MD" causes reload
CSCso05127	Unknown	WS-X6708-10GE crashes following upgrade to 12.2(33)SXH1 and 12.2(33)SXH2
CSCso08224	Unknown	WS-X6148-45AF port link takes 8 or more seconds to come up
CSCso13950	Unknown	implementation of cmasModuleActionNotif in CSICO-MODULE-AUTO-SHUTDOWN-M

Identifier	Technology	Description
CSCso16973	Unknown	VC in PE2 stays UP even after disabling ip cef globally
CSCso17569	Unknown	VPN-SPA: WAN interface mtu incorrectly programmed on the SPA
CSCso19924	Unknown	VPN SPA Module: Performance degradation on none-fragmented packets
CSCso20519	Unknown	Cheronia: Fix SMB drive strength programming.
CSCso20978	Unknown	EEM cron timer events save internal timer names to the config
CSCso22754	Unknown	MAB/802.1X interop busted
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.
CSCso38151	Unknown	Error/Traceback after power fail. %SPA-3-SW_ERROR: spa_get_card_info:
CSCso39444	Unknown	The new Active supervisor will crash after SSO @ fib_path_list_lock_memo
CSCso39518	Unknown	fh_policy_dir.proc process crash when activate 0E patch
CSCso43539	Unknown	power converter failure reported before power was on
CSCso44072	Unknown	High CPU due to multicast traffic getting punted to software
CSCso46210	Unknown	VS: NAM on Standby switch not able to configure SPAN session
CSCso50175	Unknown	% ENT_API-4-NOPORT: Traceback seen after switchover
CSCso51417	Unknown	Enabling Gigabit ports on RSP720 cause send/receive of BFD packets fail
CSCso52097	Unknown	IPV6 :Missing second Netflow shortcut after route change
CSCso53741	Unknown	VPNSPA does not handle duplicate IPSec SA correctly in nested tunnel
CSCso54131	Unknown	After SSO BPDU are being dropped
CSCso55072	Unknown	Crash occurs during execution of TCL code in ESM handler
CSCso56644	Unknown	EEM2.3::%SYS-3-CPUHOG: EEM ED Interface
CSCso59288	Unknown	On enabling oob, aging is changed to 3 times is not shown in cli output
CSCso62526	Unknown	c7600 RSP720: stdby RSP relods upon no flow-sampler interface commad
CSCso65821	Unknown	wrr-queue map configuration propagates to all ports on a 6408
CSCso68840	Unknown	eou inactivity timer over rides reauth timer from ACS
CSCso71355	Unknown	PVLAN - 6500 - Multicast flood broken from pvlan port to promiscuous
CSCso75657	Unknown	Unable to configure cwan int in SSO - standby doesn't support cmd
CSCso82039	Unknown	C2W2: Active console is getting locked for 2.5 mins during sso.
CSCso84567	Unknown	6500 with WCCP and CoPP punts non-TCP packets into CoPP policy.
CSCso85859	Unknown	RP crashes when using 'show memory detailed'
CSCso87348	Unknown	Corruption in subflow code
CSCso87838	Unknown	HSRP: with aggressive timers HSRP peer flaps when "wr mem"
CSCso89823	Unknown	Pos interface "rxload" and "input bytes" counters incorrectly increment
CSCsq00884	Unknown	"mls qos trust" cmd lost under port-channel interface when upgrading IOS
CSCsq03475	Unknown	W2: Memory corruption caused by env object after being freed.
CSCsq04355	Unknown	Fix in CSCso81632 is not complete
CSCsq04673	Unknown	SIGSEGV in ios-base and syslog_pubinfo_enqueue

Identifier	Technology	Description
CSCsq09228	Unknown	CHSTM1 SPA: Linkup/down traps not generated and snmp set not working
CSCsq19146	Unknown	FPD creation for new pegasus rx (1.6) FPA image for Sip-1 CR
CSCsq20970	Unknown	ATM option missing, while configuring T1 controller for mode atm
CSCsq33790	Unknown	Switch crashes when authenticating a user with Filter-Id attribute
CSCsq34245	Unknown	IPC Open Port Errors observed with SIP-400
CSCsq39079	Unknown	SPA-IPSEC-2G Crash under load due to IKE session establishment
CSCsq46327	Unknown	Ca6k SXH : 2 crypto maps in same redundant standby grp: RRI not deleted
CSCsq47140	Unknown	67xx module may not come online
CSCsq47305	Unknown	High CPU on SP when both VSL PO are source interface
CSCsq51286	Unknown	Memory Leak Occuring in QM Process on RP when a port is shut/no shut
CSCsq53822	Unknown	Monitor session removal may affect traffic through WS-X6148A-RJ-45
CSCsq60553	Unknown	Create cwslc-rommon3.bin for cwpa2 to accomodate release Rommon (1.8)
CSCsq62351	Unknown	C2W2:SUPW: GOLD EEM cannot crash switch immediately as recovery action
CSCsq63019	Unknown	Router Crash when "Clear Crypto Sessions" is issued on EzVPN server
CSCsq63681	Unknown	c7600 Router crashing due to freed pointer in cfib invoked by Netflow
CSCsq74300	Unknown	Set interface change for CSCsk63775 needs to be backed out
CSCsq75704	Unknown	FW2 FE PA Interface stays up/down with no conn and goes up/up after sso
CSCsq76749	Unknown	System Crash when inserting 10G Cards
CSCsq77464	Unknown	mls rate-limit unicast cef receive value re-written upon TCAM exception
CSCsq87431	Unknown	tracebacks seen on issuing sh mls qos ip command
CSCsq87833	Unknown	platform ipv6 acl ahp command rejected during bootup
CSCsq90487	Unknown	ME6524 running modular IOS images require 512 MB DRAM in SP in SXH3
CSCsq94150	Unknown	VSS system crash on show command during the initial conversion
CSCsr12976	Unknown	High CPU in ION ios-base process
CSCsr28305	Unknown	Packet drops on L2 portchannel on WS-X6708-10G
CSCsl90285	WAN	POS-APS: CWPA-3-NODISPATCH messages seen when configuring APS

Caveats Resolved in Release 12.2(33)SXH2a

Identifier	Technology	Description
CSCsl45701	AAA	TACACS+ per VRF authen failing: Address already in use
CSCso87641	AAA	Tacacs unable to connect to server
CSCsh61002	Unknown	SPA-5X1GE: GE-port not transmitting after 'shut/no shut' and vica versa
CSCsm69827	Unknown	%SYS-2-MALLOCFAIL:Process= "GraphIt" in SXH1_fc3
CSCso05127	Unknown	WS-X6708-10GE crashes following upgrade to 12.2(33)SXH1 and 12.2(33)SXH2

Identifier	Technology	Description
CSCso53516	Unknown	VSS: Incorrect fpoe programming causing unicast traffic blackhole

Caveats Resolved in Release 12.2(33)SXH2

Resolved Security Caveats

- [CSCsj85065](#)—Resolved in 12.2(33)SXH2

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

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

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080924-ssl.shtml>.

Resolved Unknown Caveats

- [CSCsg35077](#)—Resolved in 12.2(33)SXH2

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(33)SXH2

Identifier	Technology	Description
CSCee66606	AAA	per-group deadtime is nvgend as 60x user input
CSCee89849	AAA	Router reloaded at vtemplate_build_command_strings
CSCsc98046	AAA	TACACS Accounting isn't sending stop time in the stop packet.
CSCsd48175	AAA	AAA/TACACS not failing over to second server
CSCsg14301	AAA	AAA/TACACS spurious memory accesses in tplus_handle_req_timeout

Identifier	Technology	Description
CSCsj88665	Access	Bus error with PA-MC-2T3+ when deleting channel-group
CSCsl41784	Access	ION: ARP Input memory leak with "mobile ip arp"
CSCsd84347	ATM	PVC stops sending OAM loopback if AIS/RDI received
CSCsj84931	ATM	CEOP: after OIR with atm local switching and ima, router crashes
CSCsl29993	Content	WCCP Should Mark Client 'NOT Usable' with Missing L2 Adjacency
CSCsl65335	Content	WCCP: reload following ACL update
CSCsm12247	Content	WCCP: hash assignment may be lost after service group change
CSCsm32473	Content	WCCP: system reload with path splitting and output redirection
CSCsm35350	Content	WCCP GRE return breaks IPsec traffic AND/OR creates phantom packet count
CSCsm53427	Content	WCCP: multicast + appliance shutdown leads to high CPU
CSCsa57468	Infrastructure	rttmon-mib does not return getnext value when queried via snmp
CSCse07265	Infrastructure	No syslog message generated for IP SLA timeout condition
CSCsj54596	Infrastructure	logging userinfo command no longer accepted
CSCsj83417	Infrastructure	BOOM: addto_mempool_pc_array() message seen with show memory command
CSCsk06492	Infrastructure	snmp-server drop vrf-traffic implementation in 12.2 SRB train
CSCsk13725	Infrastructure	GSR: rttmon-mib does not return getnext value when queried via snmp
CSCsk37278	Infrastructure	BFD clients flaps when boot string is removed from "show running" .
CSCsk75310	Infrastructure	UDP Echo: control message not sent out of correct interface.
CSCsl33908	Infrastructure	show ver truncates system's running image name to 64 chars
CSCsl58963	Infrastructure	Manual OIR of pcmcia flash card crashes dosfs proc in Sup720
CSCsl70722	Infrastructure	Router crash polling rttmon mib with active IP SLA probes
CSCsg60447	IPServices	7200: BVI stops receiving CLNS/ISIS packets
CSCsi78892	IPServices	Configuring bridge-group makes CPUHOG message.
CSCsj29841	IPServices	Port forwarding breaks NAT-overload on a 6509
CSCsj93195	IPServices	RP crashes at ipv4fib_les_switch_wrapper on configuring crypto map
CSCsk06539	IPServices	bus error while unconfiguring static SSM mappings via TFTP .
CSCsk39022	IPServices	Modular IOS: ip directed-broadcast not working
CSCsk39926	IPServices	Unable to route local FTP traffic over VRF with IOS image
CSCsl10348	IPServices	Crash writing to or from ftp/tftp server in modular IOS
CSCsl23788	IPServices	Dlsw+ peer waits in AB_PENDING or WAIT_WR status with modular IOS
CSCsk94676	LegacyProtocols	dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH
CSCsk41552	Management	T/B %SCHED-3-THRASHING of cdp2.iosproc process_wait_for_event
CSCsj34456	MPLS	LDP change by CSCsi69278 causes inconsistent mplsLdpEntityIndex value .
CSCsk57114	MPLS	CPUHOG process = SNMP ENGINE, PWMIB, GetNext of cpwVcMplsNonTeMappin
CSCsl39233	MPLS	eBGP in VRF-lite not working in images without MPLS .
CSCsd14706	Multicast	PIMV2 router send PIMV1 RP-reachable messages loading recieve router CPU
CSCsg95192	Multicast	no ip rp-address <ACL name> causes an address error

Identifier	Technology	Description
CSCsj88725	Multicast	Wrong (S,G) RPF after route change, no upstream join
CSCsl27840	PPP	Router may Crash / Hang, Module Reset @ Shut ATM member + MLPOA
CSCsi73132	QoS	Multicast DSCP value not copied to PIM-SM RP-register packet
CSCsk63794	QoS	FlexWAN WS-X6582-2PA + T3+ Serial PA may crash/reload
CSCea90941	Routing	IOS Ignores EIGRP Stub Command In Startup-Config at Initial Power On
CSCeg25475	Routing	Distribute-list configured in ipv4 acts in vpv4 address-family
CSCse53019	Routing	redistribution not triggered when BGP as-path/community changes
CSCsg80259	Routing	BGP Routes do not re-populate following reload of Secondary Route Reflect
CSCsh12493	Routing	BGP overlapping VRF route not installed in RIB after add/del of VRF
CSCsh92749	Routing	ISIS: ADJ del triggers both LSP and SPF
CSCsi51431	Routing	JQL:SIERRA:SP HighCPU/LCboot up fail with largeACL cfg after sw reload
CSCsk34344	Routing	Wrong share-count 1:10 via confed-external BGP peers using dmzlink-bw
CSCsl07297	Routing	SXF11: BGP "no neighbor" command caused Address Error exception .
CSCsl47915	Routing	Redistribution of ospf in rip with prefix-list not working properly
CSCsl57457	Routing	ISIS NSF switchover failure - similar to CSCsl28278
CSCsl83415	Routing	Rtr crash in show cmd: new updgrp add enlarges Nbr bitfield size for Tbl
CSCsl94410	Routing	Back out the CSCsj17879 for all non ERF branch
CSCsm23764	Routing	CEF RF progression error if RRP reloads mid CEF sync
CSCsm27979	Routing	router may crash for "address error exception" doing sh ip route vrf
CSCsm64516	Routing	OSPF MD5 Key Does Not Accept Whitespace Character
CSCso22098	Routing	OSPF down on RPR+ switchover on core router
CSCin91851	Security	Support keyboard-interactive authentication method
CSCsj45031	Security	Cat6k unable to SCP files from Tectia ssh server
CSCsl98498	Security	Tunnel int is going down with mode ipip decapsulate-any
CSCeb69473	Unknown	connect '/terminal-type' command memory corruption
CSCeh08262	Unknown	Show tech SP output should honor redirect applied
CSCek53174	Unknown	dhep snooping cannot scale beyond 225 bindings
CSCek66116	Unknown	B2B: IKEa trans 0x17; opcode 0x53; param 0x41 msg displayed forever
CSCek71816	Unknown	CE-CE ping fail after restore ASBR-PE vrf
CSCek78874	Unknown	KMI:Out of order deletes cause sync issues
CSCsb87956	Unknown	loop in the state IKE_CONFIG_MODE
CSCsh17328	Unknown	WS-SVC-WISM-1-K9 reports 0.0 in entPhysicalVendorType
CSCsh84657	Unknown	STP Loopguard: Ability to disable loopguard for Po270 and higher for FWM
CSCsh97395	Unknown	IDSM: Monitor config was removed after RPR switchover
CSCsi52382	Unknown	radius attribute 5 nas-port not sent in access-request for RA VPN users
CSCsi97434	Unknown	A router may crash when ipsec is established
CSCsj48453	Unknown	AW: CAT6k does not forward multicast traffic to WISM in L3 mode

Identifier	Technology	Description
CSCsj68951	Unknown	Diag Minor Error: TestVslStatus by shut down one side Sup4 uplink
CSCsj87584	Unknown	call-home inventory full needs show ipdrom switch all for VSS
CSCsj91961	Unknown	Ifnums of channels for E3 dont match on active and stdby
CSCsk16240	Unknown	C2W1: active not responding msgs seen om reload with 41patches
CSCsk21354	Unknown	PAT : Missing second Netflow shortcut after route change.
CSCsk27081	Unknown	ifHCInOctets and ifHCOctets on GE-WAN interfaces wrap up at 2^32
CSCsk32872	Unknown	Wrong API usage, can lead to crash .
CSCsk33740	Unknown	replay window size of 1024 causes IPSec Policy Check and Replay Failure
CSCsk41134	Unknown	ISAKMP SA neg not successful for in tunnel mode w/ RSA-SIG
CSCsk44233	Unknown	While raising the interrupt level, bgp_route_map_inform tries to suspend
CSCsk58040	Unknown	WS-X6148A-GE-45AF retains previous modules MACs after OIR
CSCsk80552	Unknown	Shut and no shut of interface causes the delay in forming rp mapping
CSCsk82370	Unknown	RP crash and tracebacks in crypto related process
CSCsk83089	Unknown	Increase maximum aggregate policer > 10Gbps
CSCsk84925	Unknown	ipv4:SSM mroute not created due to ip mr-cache on IIF, traffic hits MSFC
CSCsk97144	Unknown	wait for remote process DiagCard7/-1creation times out with 1018 ION
CSCsl06577	Unknown	Linking bootflash to bootdisk failed after pcmcia_driver.proc restart
CSCsl12827	Unknown	Handling Transit IpSec in VRF mode
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
CSCsl27236	Unknown	%SYS-3-CPUHOG: Task is running for (126000)msecs, causes RP crash .
CSCsl32344	Unknown	Group of 4 ports on 6708 stops passing traffic
CSCsl34515	Unknown	VS2:after SSO with preemption, port security is broken
CSCsl43540	Unknown	VS2:snmp mac notification for port channel on DFC linecard doesn't work
CSCsl51380	Unknown	Sup720 and Sup32 TCAM & SSRAM Consistency Checkers refinement
CSCsl51395	Unknown	slot_earl_icc_shim_addr:device crash with hw-module reset
CSCsl52092	Unknown	DHCP db agent considers port-channel interface (poX) as invalid
CSCsl53037	Unknown	Mail action does not separate headers from body
CSCsl53845	Unknown	sup720/SXH: dummy packet send over inband when sw netflow is used
CSCsl58673	Unknown	EEM Prevents VTY telnet to MCP router
CSCsl58924	Unknown	Standby SP crashed due to TestAclDeny failure on bootup/switchover
CSCsl59553	Unknown	SIP-400: bursty traffic causes packet drop even in low rates
CSCsl63311	Unknown	6500 May Experience High CPU due to NAT traffic
CSCsl70016	Unknown	WS-X6516A-GBIC card in switch 2 goes down frequently in vsl
CSCsl70404	Unknown	Memory leak on SUP - CMFI Process
CSCsl71339	Unknown	Prevent ssa interrupts from corrupting sfp i2c accesses
CSCsl72752	Unknown	VS2: after preempted switchover, interface states are out of sync

Identifier	Technology	Description
CSCsl74456	Unknown	VPN-SPA : TCAM not programmed on POS sub-interface after a reload
CSCsl74976	Unknown	Punted MPLS-tagged traffic causes control plane instabilities
CSCsl75136	Unknown	Cat6k with Sup32 failed to boot up after power cycle.
CSCsl75719	Unknown	sxf13 show int tunnel with blank display
CSCsl75836	Unknown	VS2: MCAST LTL T/B's observed, when removing VLAN / SVI used for mcast
CSCsl76647	Unknown	VPN SPA Cannot clear SA using conn-id with CLI
CSCsl79219	Unknown	mvpn : bidir shadow entries not installed
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 combination in CfgMonInd, clear sa
CSCsl89176	Unknown	Cat6k may crash when vlanTrunkPortEntry is polled via snmp
CSCsl89425	Unknown	BFD sessions dont scale
CSCsl91085	Unknown	system/iprouting.iosproc crash after activate 39 dummy/restart patches
CSCsl92286	Unknown	60 second multicast traffic loss as VSS standby chassis initializes
CSCsl94301	Unknown	VS2: Mac learning in linecard gets disabled by pre-emption switchover.
CSCsl97653	Unknown	bcm2_5421_isr bcm2_num: 1 messages seen in the log
CSCsm01399	Unknown	Bus idle recovery may cause 10GE interface to remain down
CSCsm04824	Unknown	OER Top Talker Functionality broken on s3223
CSCsm05486	Unknown	mtu mis probram in adj thru tunnel interface after b2b failover
CSCsm08419	Unknown	debounce timer issue on sup32 10GE uplink and 6708
CSCsm11717	Unknown	VS2:On reloading standby chassis T/Bs on SP console for 1 minute
CSCsm13389	Unknown	RRI is not called be if QM rekey timer expiry forces SA deletion
CSCsm15350	Unknown	vpnspace crashed at assert failure in l2-mcpu.c on line
CSCsm20994	Unknown	kron job daily reoccurences fail after new year
CSCsm21126	Unknown	C7600-SSC-400: Resync fabric interface on fabric error
CSCsm22935	Unknown	Problem in c6k_power_get_ilpower_daughterboard_used_pwr
CSCsm24904	Unknown	Bridge-mib timing out dot1dBasePortIfIndex
CSCsm26415	Unknown	Traceback seen when show platform cfm issued for fwd_vlan 0
CSCsm27017	Unknown	VS2: power configuration is not synced to standby
CSCsm30858	Unknown	PIM register packets upmarked to TOS 6 by PTeam redirection
CSCsm32493	Unknown	Backout of CSCsh94882
CSCsm33528	Unknown	Rekey packet loss for pure ipsec
CSCsm34871	Unknown	Need to support enhanced PoE feature
CSCsm35364	Unknown	SPA-IPSEC-2G get reload automatically by RP
CSCsm44309	Unknown	L2 Po - new member was not included in mapped ucast flood &mcast indices
CSCsm44413	Unknown	RP not added into LTL index when bridge-group is configured
CSCsm46682	Unknown	HL: VACL capture functionality not working with the latest sierra

Identifier	Technology	Description
CSCsm48564	Unknown	Need to exclude RxErrors from being monitored by LinkErrorMonitoring HM
CSCsm49103	Unknown	I/O Memory Leak when running show mls cef command
CSCsm49440	Unknown	RRI: Need to support remote-peer option when source proxy == peer
CSCsm51299	Unknown	Code divergence caused a need for a second fix for CSCsl27236.
CSCsm56293	Unknown	Sup4:DFC only mode, create bus stall condition-the switch still crash
CSCsm59488	Unknown	Fix backwards compatibility for multicast egress netflow cli
CSCsm70349	Unknown	BPDU traffic over Eompls is not switched on 3C system
CSCsm81399	Unknown	No Such Instance error from many SNMP objs for 1xOC48 POS/RPR SPA
CSCsm82169	Unknown	VSS: heathland interfaces are err-disabled on standby chassis
CSCsm82382	Unknown	7600 standby RP memory leaking cause CEF disable
CSCsm83893	Unknown	W2: "sh mls cef adj mpls detai"l after SSO freeze RP causeT/B , reboot
CSCsm83948	Unknown	CISCO7609 returns sysObjectId as ciscoProducts.402 (which is cisco7606)
CSCsm92183	Unknown	c2w1: Heathland card is not coming up due to diag failure
CSCsm95456	Unknown	Duplicate L3 packets with 6708 and DEC
CSCsm96243	Unknown	Switch crashes on executing sh tcam interface acl with include option
CSCsm96610	Unknown	OOB-MAC-SYNC is on, need to change internally the cam aging to 480 Sec
CSCsm97836	Unknown	Memory leak VSL Manager
CSCsm98256	Unknown	Berytos got power down due to TestMacNotification and TestFabricCh0Healt
CSCso02208	Unknown	VS2: crash when provisioning LI stream
CSCso12903	Unknown	RE MET address check missing while running MET patch on IO bus timeout
CSCso25489	Unknown	CSCsg03804 - Time Based ACL Issue not fixed
CSCsj68446	WAN	NTP will not sync - NTP packets received but ignored by NTP process .

Caveats Resolved in Release 12.2(33)SXH1

Resolved AAA Caveats

- [CSCsj91123](#)—Resolved in 12.2(33)SXH1

Symptoms: Router reloads after authentication attempt fails on console.

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

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

Resolved Infrastructure Caveats

- [CSCsk14633](#)—Resolved in 12.2(33)SXH1

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/warp/public/707/cisco-sr-20070912-regexp.shtml>

- [CSCsk33054](#)—Resolved in 12.2(33)SXH1

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/warp/public/707/cisco-sr-20070912-regexp.shtml>

- [CSCsk61790](#)—Resolved in 12.2(33)SXH1

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

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

Workaround: There is no workaround.

Resolved Routing Caveats

- [CSCsi84089](#)—Resolved in 12.2(33)SXH1

Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

Workaround: Add area 0 in the OSPF VRF processes.

Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

Resolved Unknown Caveats

- [CSCsi99869](#)—Resolved in 12.2(33)SXH1

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.

Other Resolved Caveats in Release 12.2(33)SXH1

Identifier	Technology	Description
CSCek58496	AAA	Mem alloc at aaa_test_setup_auth_req/aaa_test_setup_acct_req leaked
CSCsh59019	AAA	Avoiding AAA client hangs, if a protocol subsystem is not present.
CSCsi99473	AAA	TACACS authorization fails with 'request for nonexistent server' msg .
CSCsj34688	AAA	AAA: adding static route cfg does not trigger acct msg to tacacs server
CSCsj89305	AAA	RADIUS/NAS-IP address is sent out as 0.0.0.0
CSCsj97165	AAA	%AAA-3-BADMETHODERROR: Router crash @ aaa_get_new_acct_reg_type .
CSCsl33966	AAA	C6509 : attribute 32 nas-Id not sent for Auth (missed by CSCsf30451) .
CSCsm06740	AAA	Memory Leak in AAA accounting and Virtual Exec
CSCef67942	Access	AS leaking memory under IP input - regcomp
CSCsi00099	Access	Spurious Memory Access Error @ ct3sw_check_freedm_fifo
CSCsj37071	Access	PA-MC-E3 will not recover after workload stress
CSCek61180	ATM	crash @ write_to_url, doprintc_core, atm_remove_vc
CSCin90065	ATM	ATM pvc trap may not always be generated or generated continously
CSCsb67229	ATM	Ip add config on p2p interface tries to reflect it on all p2p int .
CSCse13374	ATM	IMA ports on 7600 always initialized to default clocking on bootup .
CSCse98383	ATM	Bandwidth not changed on IMA group when one member link is made down .
CSCsj57084	ATM	Voice packets in LLQ experience latency
CSCsi05906	Content	WCCP:appliance failover does not update TCAM adjacency
CSCsi10700	Content	WCCP:copy TOS value from inner to outer GRE packet

Identifier	Technology	Description
CSCsi91658	Content	Wccp stops layer 2 redirection when dscp is present in the redirect acl
CSCsj09149	Content	WCCP: no redirection following change in configuration
CSCsj48440	Content	WCCP: L2 return traffic is software switched
CSCsk14208	Content	WCCP does not work after OIR or Reboot
CSCsl04908	Content	WCCP: shutdown of appliance i/f leads to c6k reload
CSCsb95806	Infrastructure	Incorrect 64bit counter on 1Gb MPLS interface via SNMP .
CSCsc33389	Infrastructure	When snmp-server host is deleted, the trap is not sent to other hosts
CSCsc84077	Infrastructure	IOS CLI will stop accepting octal by default
CSCsd52019	Infrastructure	cieIfStateChangeReason and locIfReason support broken.
CSCsf30779	Infrastructure	Add CLI for section keyword in show run output modifiers
CSCsh25151	Infrastructure	memory leak seen with reflexive ACL and NAT/PAT
CSCsh48919	Infrastructure	Embedded spaces in DOSFS dirs/file names cause crash in some platforms
CSCsh81291	Infrastructure	Exodus Mayflower C10K ISSU fails at loadversion
CSCsj37635	Infrastructure	Incorrect source IP address is used for IP SLA icmp-echo with VRF
CSCsj58223	Infrastructure	Bus Error after 'show memory' .
CSCsj80951	Infrastructure	*Neutrino* proc reported memory Freed/Holding is incorrect
CSCsj83924	Infrastructure	Porting command show history all to mainlines
CSCsj83966	Infrastructure	Syslog traps cause CPUHOG when lot of interface come up at same time. .
CSCsk10335	Infrastructure	Traceback @ ipc_send_message_blocked during bootup .
CSCsk27147	Infrastructure	SNMP stops responding while polling from CISCO-MEMORYPOOL-MIB
CSCsk38461	Infrastructure	Show platform hardware command getting rejected .
CSCsk67272	Infrastructure	CPU HOG while polling ciscoFrameRelayMIB .
CSCsl09867	Infrastructure	Exec-timeout not working at more prompt when using Modular IOS
CSCsl13216	Infrastructure	warm upgrade is not working .
CSCsl53110	Infrastructure	VSS: Stby rp crashes on boot
CSCeh56158	IPServices	NAT outside source translation fails for GRE packets .
CSCsg97662	IPServices	Cant disable skinny (tcp 2000) .
CSCsh92986	IPServices	Very long latency for RSH traffic going through FWSM .
CSCsi16903	IPServices	IGMPv3 mode 4 group report with { } source list gets translated to mode 6
CSCsi28444	IPServices	DHCP server has parse problems with x in bootfile
CSCsi42717	IPServices	saa_vrf_test_udpe & saa_vrf_test_itter generate an unexpected error mess
CSCsi57927	IPServices	FTP session hangs TCP in closewait after CLI times out . .
CSCsj07951	IPServices	Memory Corruption when Autoinstall over FR
CSCsj62846	IPServices	Need to differentiate IPv4 and IPv6 . .
CSCsj89544	IPServices	TCP retransmissions get dropped below IP layer. .
CSCsk07170	IPServices	MD5 validation error shows IPv4 address but should IPv6 address
CSCsk10604	IPServices	Syn pkts destined to VRF fail to match the default TCB in table

Identifier	Technology	Description
CSCsk29013	IPServices	IGMP groups in the vrf not rejoined after executing a cle ip mr vrf
CSCsk80935	IPServices	SXF12, SNMP response being broadcast .
CSCsk81396	IPServices	NAM process crash in 12.2SXF .
CSCsk82821	IPServices	The UUT not able to receive the Large ICMP message.
CSCsl00350	IPServices	ARP entry not created for nat translated IP .
CSCsl06431	IPServices	Modular IOS: Memory leak in udp.proc
CSCsc77148	LegacyProtocols	Router crash while issuing show ipx cache command. Cleanup SA warnings.
CSCsh34949	LegacyProtocols	DLSW router crash with Bus Error
CSCsj98895	LegacyProtocols	v2-single-tcp peer connection is established on a non config/prom peer
CSCsg05873	Management	Buffer leak with SNA Focalpoint PU consuming middle buffers with NMVTs
CSCsk36618	Management	Device crash with cdp traffic @ 200 pkts/sec and clear cdp table
CSCsi75566	MPLS	Packets dropped on FRR backup tunnel if protected intf is dot1q
CSCsi99825	MPLS	7613 crashed on SNMP ENgine
CSCsj55865	MPLS	Traceback seen @ lsd_rewrite_create and lsd_frr_co_req
CSCsk14113	MPLS	LDP change in advertise-tag for access list stop advertising some prefix
CSCsk57589	MPLS	TB:%LFD-3-INVINSTALLER & %BGP_MPLS-3-VPN_REWRITE(seen on bootup)
CSCec55244	Multicast	PIMv6: Spurious access at pim_ipv6_hello_addr_adv_size
CSCek26940	Multicast	Need to unhide interval for send-rp-discovery
CSCsh56720	Multicast	CPUHOG/Watchdog timeout when using igmp static group class-map cmd
CSCsi01481	Multicast	%PIM_PROT-3-SHUTDOWN_ERR seen at unconfig ipv6 pim rp-addr .
CSCsi97586	Multicast	MGX-RPM-XF-512 reset after customer deleted multicast vpn and vpn vrf
CSCsj16861	Multicast	Dynamically overwritten bidir RP doesn't get removed from HW
CSCsj64230	Multicast	bidir DF election should not be restarted on a downstream interface
CSCsk49073	Multicast	%DUMPER-3-PROCINFO ... SIGSEGV when running Extranet MVPN
CSCef54653	PPP	Members inactive in a multilink bundle except the first member. .
CSCse28421	PPP	%AAAA-3-BADSTR error when Multilink interface goes down .
CSCek49107	QoS	Router crashes @ traffic_shape_dequeue_shim .
CSCek78675	QoS	SIP200 crash at hqf_cwpa_pak_enqueue_local during qos test .
CSCse18146	QoS	SIP1-CT3: SIP1 crashed after switchover @giant_node_process .
CSCsg98040	QoS	QoS applied to int with dot1q trunk does not match MPLS EXP on 12.2S
CSCsk09651	QoS	Router may reload with shaping policy on MLPPPoFR . .
CSCec43841	Routing	EIGRP: IP next-hop incorrect on spokes when using no next-hop-self
CSCek33384	Routing	Tunnels stay down after cutover at MPLS head test cases
CSCek75079	Routing	Problem in type7 to type5 translation if summary-addr configured
CSCek76776	Routing	ip interface settings persistent after deleting/adding sub-interface
CSCek78315	Routing	Access to NULL ptr with debug ip ospf hello .
CSCek79264	Routing	static route tracked by track-object not installed into routing tabl .

Identifier	Technology	Description
CSCsa73179	Routing	Memory corruption/crash when 'no default-information orig' under RIP
CSCsc73725	Routing	EIGRP packet pacing should have lower minimum value
CSCsd34114	Routing	IPv6 Localpools allows more than one prefix per user
CSCse42362	Routing	EIGRP next hop not updated on spoke, in a dual hub/dual path dmvpn topo
CSCsf27220	Routing	Router crashes on traffic with NHRP
CSCsg12385	Routing	No IPv6 uRPF subblock control decode function
CSCsg16778	Routing	router may crash at bgp_update_nbrsoo after deleting BGP neighbor .
CSCsg25995	Routing	N/w configured are not seen in mbgp table with nbr nlri unicast multi
CSCsg63932	Routing	IPv6 Static issue with same path from two clients
CSCsg72029	Routing	setting M bit in RA supresses autoconfig bit
CSCsg94088	Routing	OSPF route map not matching community-list / ipv6 redistributing bgp
CSCsh20656	Routing	TCP header compression elicits upstream retransmissions from Fritz
CSCsh38140	Routing	CEF drops when using CEF LB paths and active link recovers from failure
CSCsh54797	Routing	high CPU in collection process after bringing up pppoe sessions twice .
CSCsh57509	Routing	RIPv2 does not delete redundant paths with different next hops .
CSCsh80008	Routing	BGP: soft reconfiguration inbound and neighbor weight has no effect
CSCsh82953	Routing	EIGRP pece routes missing extcomm attrs after redistribution to BGP .
CSCsh87744	Routing	IPv6 mcast: RPF fails even while MBGP has default route
CSCsh88825	Routing	bgp: advertisement-interval not nvgened for peer-groups
CSCsi09698	Routing	BGP adv connected prefixes suppressed by IP Event Dampening after reload
CSCsi15183	Routing	change MTU value causes %DUAL-3-INTERNAL in ipigrp2_add_item_dest
CSCsi17002	Routing	IPv6 PBR policy routes to non-attached destination
CSCsi25729	Routing	ISIS doesn't enable BFD except after micro reload
CSCsi27696	Routing	oldest ebgp bestpath not retained in eibgp multipath cases
CSCsi33147	Routing	OSPFv3: prefix lsa does not re-originate after interface comes up .
CSCsi41109	Routing	Traffic loss and High RP CPU with SPA OIR with a large configuration
CSCsi47635	Routing	deleted sub-interface shows up on next config sub-interface
CSCsi48304	Routing	Multi-source redistributing makes ospfv3 external db corrupt
CSCsi53353	Routing	BGP TTL Hack breaks ipv6 neighbor
CSCsi58303	Routing	eigrp resync peer graceful-restart repeatedly after reload .
CSCsi58867	Routing	CPUHOG After show ip route static or show ip route connected
CSCsi62017	Routing	%XDR-DFC3-6-XDRLCDISABLEREQUEST: Client XDR Interrupt Priority Client
CSCsi80057	Routing	RIP default-information originate with route-map not working correctly .
CSCsj00161	Routing	IPv6 may load balance between summary discard and reachability paths .
CSCsj04761	Routing	No space between 'any' and 'eq' after configuring ipv6 acl
CSCsj06265	Routing	Switch crashes when doing clear ip ospf process
CSCsj09838	Routing	RR some prefix might not be sent after bgp neighbor flaps .

Identifier	Technology	Description
CSCsj10185	Routing	CPU hog in ospfv3_clean_partial_spfQ and ospf_clean_partial_spfQ
CSCsj17820	Routing	Hub crashes during unconfiguration due to program counter error
CSCsj17950	Routing	ISIS redistributed static routes might not be advertised
CSCsj25841	Routing	default not sent using neighbor default-originate conditionally w/route
CSCsj25940	Routing	%SYS-2-NOTQ: unqueue didn't find 6433F698 in queue .
CSCsj32013	Routing	GSR crashing with bgp_vpnv4_purge_one_import .
CSCsj36133	Routing	Invalid header length BGP notification when sending withdraw
CSCsj37111	Routing	IPv4 inconsistencies & %FIB-4-FIBXDRINV upon reset LC
CSCsj53361	Routing	ISIS flaps after NSF/SSO of peer with 16 neighbor,5k routes and traffic.
CSCsj54395	Routing	router crash when iphc configured with SLIP encap
CSCsj64154	Routing	c7600 - %SIP200_MP-4-PAUSE: Non-master CPU is suspended for too long
CSCsj71306	Routing	mfibv4: HA: BGP MDT update is injected into standby . .
CSCsj72039	Routing	Prefix not in ISIS database if serial interface and passive
CSCsj80615	Routing	BGP not sending prefix with expected next hop to the peers . .
CSCsj85485	Routing	EIGRP NSF - MSFC switchover causes hello's to be sent over passive intf
CSCsj89636	Routing	isis convergance time delay with equal paths
CSCsj97484	Routing	32kEVC: ESM LC OIR crash causes RP to crash when LC comes up.
CSCsj99269	Routing	BGP: VPNv4 general scanner runtime close to 1 hour at boot time .
CSCsk21328	Routing	6504 crashes in IPV6
CSCsk26719	Routing	show ip access crash with per-user acl
CSCsk27077	Routing	router crash observed while clearing virtual access interface
CSCsk29853	Routing	ospf takes almost 10 minutes to flash Stale, self-originated LSAs
CSCsk33115	Routing	OSPF virtual-link fails to come up during IETF GR & RIB entries deleted
CSCsk35970	Routing	BGP Router/Scanner causes high CPU utilization when using BGP multipath
CSCsk35985	Routing	OSPFv3: router crashes for "show ipv6 ospf lsdb" after redist of routes
CSCsk36324	Routing	OSPF: spf calculation goes into loop causing high CPU .
CSCsk38877	Routing	PE_PUNT_UNRECOGNIZED should be an OUTPUT_FEATURE .
CSCsk46195	Routing	Arp entry does not age out with private vlans and no ip sticky-arp
CSCsk48182	Routing	BGP: Router crashes @ bgp_netlist_validate
CSCsk66339	Routing	ISIS fails remove native path from local RIB / del path from global RIB
CSCsk89546	Routing	RIB and FIB not updated after shut TE LB path
CSCsl13950	Routing	VS2:XDR_LC traceback seen on Standby-RP on bootup .
CSCsl18176	Routing	OSPF SPF calculation with TE metric absolute picks wrong egress .
CSCsl28278	Routing	OSPF-Route/CEF entry lost after SSO on the neighbor
CSCsl71540	Routing	Router crash after using cmd 'sh ip bgp x.x.x.x [bestpath
CSCsh72664	Security	DMVPN: OSPF neighbor flap and traceback @ tunnel_oqueue. .
CSCsj60938	Security	SCP with redirect option locks up console or VTY line .

Identifier	Technology	Description
CSCsj78065	Security	tunnel_trace CPUHOG in Net Background process
CSCsk00054	Security	mGRE fragmentation into tunnel broken
CSCdu70318	Unknown	Feature Request: VRF-lite PBR
CSCdz55178	Unknown	QoS profile name of more then 32 chars will crash the router .
CSCek34097	Unknown	with about 100 subints configd rtr crashes at ipv6 multicast-rout
CSCek36017	Unknown	Need show mac abbreviated equivalent command in IOS
CSCek52381	Unknown	Killing tcp.proc leads to no thread information in LC
CSCek75082	Unknown	Router crashes while unconfiguring channel-group
CSCek76062	Unknown	Router crashed @ validmem_complete_interrupt .
CSCek78066	Unknown	Whitney:CLI & MIB mismatch for aux-1 temperature Sensor SUP32
CSCek78633	Unknown	SSO:ESM20:TB at %MFI-3-REDISTMGR: Redistribution Manager
CSCek79138	Unknown	VLAN policy not applied to bridged pkts if SVI shutdown .
CSCin99430	Unknown	snmp-server sparse is not working correctly for IF-MIB
CSCsa79984	Unknown	CTRLC_ENBL should be cleared when line is reset
CSCsb29131	Unknown	show crypto ipsec sa identity detail causes system to reload
CSCsc24830	Unknown	Far end router reload causing traceback at dmlp_update_hw_stats
CSCsc98471	Unknown	show diagnostic sanity fails to check software modularity boot string .
CSCsd88768	Unknown	%SYS-2-BADSHARE: Bad refcount in datagram_done fix for PA-MCX-8TE1
CSCse45684	Unknown	multicast (hsrp/ospf) coming from service modules is blackholed by vacl.
CSCse67736	Unknown	Add support for XFP-ZR optics
CSCsf01190	Unknown	Netflow export destination command dissapears from running config .
CSCsf97859	Unknown	invalid shows in show hw-module subslot with SPA-OC192POS-LR
CSCsg09423	Unknown	IPSEC SAs dont recover after rekey with 3000 IKE SAs and PKI (RSA-Sig) .
CSCsg15159	Unknown	Traffic to Null0 accounted with Null as dest IF
CSCsg16417	Unknown	show ip slb connections firewall cmd accepts not configured FW farm name
CSCsg19793	Unknown	Psecure absolute aging on DFC causes MAC inconsistency w/ Central EARL
CSCsg21809	Unknown	Add bridge asic status collection support .
CSCsg23226	Unknown	service counters max age does not function correctly for value 6-9 sec
CSCsg29305	Unknown	hw-module subslot reload crashes the router .
CSCsg36532	Unknown	DMVPN Phase 2: Black hole traffic when spoke-spoke tunnel fails
CSCsg99914	Unknown	sip-200 power-cycles after BGP flap (not responding to keepalive)
CSCsh17579	Unknown	Transceiver TX Power displays erroneous TX level
CSCsh24450	Unknown	Memory leak from IF-MGR DB elem chunk @ im_if_db_init
CSCsh24460	Unknown	ipv6 ISIS ping through doesnt return 100% success rate
CSCsh31782	Unknown	Bus error crash - show crypto isakmp sa
CSCsh34467	Unknown	Standby constanly reset due to RF request with large configuration .
CSCsh49239	Unknown	After redundancy failover Mcast packets drop for 60-90sec on SUP uplink

Identifier	Technology	Description
CSCsh64639	Unknown	VS2: [dead threads] process takes a large chunk of CPU util
CSCsh69341	Unknown	SLB: Incorrect feature execution in ssv
CSCsh80130	Unknown	Add warning/comments to interfaces when Auto Lag is used for interface
CSCsh82046	Unknown	SIERRA: sup4 standby crashes at sstrncpy during bootup.
CSCsh85531	Unknown	E1 channels down after PE reload
CSCsh88532	Unknown	Auto-LAG EtherChannel not configurable; doesn't trust QoS. .
CSCsh91974	Unknown	PIM CLI causes RP crash when issued under control-plane subconfig prompt
CSCsh97848	Unknown	Sierra: LACP pdus should be untagged .
CSCsh99583	Unknown	VTP's Local updater ID uses EOBC though up state SVIs exist
CSCsi00136	Unknown	IKE does not process more than 2 NAT-D payload
CSCsi05265	Unknown	SYS-2-GETBUF: Bad getbuffer -Process= LSDp Input Proc
CSCsi06759	Unknown	SIP 200: SNMP-3-DVR_DUP_REGN_ERR
CSCsi09942	Unknown	VTP3: Print warning message when the vlan name exceeds 20 characters
CSCsi11874	Unknown	Sup720 DFC forwarding some packets to MSFC instead of hw switching
CSCsi12416	Unknown	Native vlan traffic disruption in etherchannel standalone (I) mode
CSCsi23021	Unknown	WiSM in Slot 13 cause Duplicate IP message and loss of access
CSCsi24069	Unknown	Collect additional debug info for Modular IOS kernel crashes
CSCsi39631	Unknown	Show mpls l2transport vc detail using incorrect packet counters
CSCsi42270	Unknown	IOS-SLB Radius Server LB may not mark a real as failed
CSCsi48280	Unknown	PRE3 Mcast: Switchover not shown from default to data MDT
CSCsi49436	Unknown	Netflow API needs to be extended to provide peer AS information
CSCsi50028	Unknown	dot1x port moves authorize->guest, radius attributes and zombie MAC held
CSCsi65363	Unknown	Not able to run to t1 loopback when using a PA-MC-T3 with flexwan
CSCsi70426	Unknown	Traceback seen when router received a craft EAP id-response frame
CSCsi71940	Unknown	System crashed with auto-qos negative test with traffic .
CSCsi74194	Unknown	18SXF: Egress SPAN may cause high CPU
CSCsi76842	Unknown	Line protocol remains down on changing from frame-relay to hdlc/ppp.
CSCsi79991	Unknown	VACL capture not supported for the GE-WAN or GigabitEthernet on SIP-400
CSCsi81885	Unknown	Trunk negotiation fails when Po is configured with Min_links . .
CSCsi82337	Unknown	Policy routing punts incoming packets to process with VRF select enabled
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
CSCsi98587	Unknown	Excessive MET refs and memleak after ipv4 stress, crash follows .
CSCsi99234	Unknown	RP crash at validblock with %SYS-6-BLKINFO: Corrupted redzone blk
CSCsi99875	Unknown	BOOM: spa_eeeprom_read_bit on BOOTUP

Identifier	Technology	Description
CSCsi99991	Unknown	When CMM is rebooted, FE goes into ErrDisabled state
CSCsj00385	Unknown	logging event link-status default negates existing interface config
CSCsj01961	Unknown	ifindex table size from nvram could be validated before malloc
CSCsj02971	Unknown	12.2SRB - signed/unsigned error in code for 'show ip cache aggregation a
CSCsj03212	Unknown	blade get into bad b2b state if it is not b2b ready
CSCsj04905	Unknown	IOS-SLB: FWLB sticky config not get removed
CSCsj05519	Unknown	Standby NSE crashed IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP
CSCsj08713	Unknown	Disable bfd on SVI interfaces
CSCsj10375	Unknown	802.1X: VLAN Changing on port causes link to go down
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
CSCsj11771	Unknown	VS2: transceiver_rp_oir_online takes ~6s during reg_invoke_oir_online
CSCsj13444	Unknown	rsp720-10ge: PBR next-hop information lost on RPR switchover .
CSCsj14557	Unknown	Bogus Port channel 345 is created on simultaneous boot sometimes
CSCsj14847	Unknown	crypto connect command dropped after reload on unchannelized 2CT3+ .
CSCsj16292	Unknown	DATA CORRUPTION-1-DATA INCONSISTENCY: copy error
CSCsj17048	Unknown	WS-X6708: show flow control shows send admin/oper state as desired
CSCsj17485	Unknown	Router crashed on doing a show cry isa pro while deleting them
CSCsj18494	Unknown	Leak +MN to pfc to avoid flooding due to tx span .
CSCsj27352	Unknown	RX Priority q-limit is set to default after reload
CSCsj28026	Unknown	WhitneyVS: Unable to mibwalk clcFdbVlanInfoTable . .
CSCsj28753	Unknown	IF-MIB::ifHCOutUcastPkts is incorrect on ESM20G
CSCsj29657	Unknown	Degradation in TPS - Whitney IOS image .
CSCsj32493	Unknown	IPSEC: Incorrect IPSec connection info in InvalidSPI testing
CSCsj34267	Unknown	SP crashes due to segmentation violation with 400 igmp groups/vrf
CSCsj34552	Unknown	ip address of vlan interface not programmed into spa-ipsec-2g
CSCsj35776	Unknown	Some of the VCs are INACTIVE after SPA OIR
CSCsj36689	Unknown	Corruption in block allocated by svcld_config
CSCsj38796	Unknown	LC/SP crash @ label_entry_get_inlabel
CSCsj42303	Unknown	6K installs ffff.ffff.ffff in CAM table under very specific conditions
CSCsj48589	Unknown	BGP route (injected by OER) remains in Routing table after path is clear
CSCsj51666	Unknown	ip ssh ver 2 command missing in 12.2(25)EWA
CSCsj56703	Unknown	SSO failover causes RSTP forwarding and physical interfaces blocking .
CSCsj58538	Unknown	Lots of prowler/patriot interface go down for few second during sso swov
CSCsj61811	Unknown	process restart pcmcia_driver.proc on SP crashes the SP
CSCsj64453	Unknown	HSRP support in protocol policing
CSCsj66829	Unknown	Switch crash with clear ip igmp snoop stat and show ip igmp snoop st

Identifier	Technology	Description
CSCsj66987	Unknown	ifAlias for Subintf Reports the Previous Value if Description Deleted
CSCsj67096	Unknown	Issue w/NATed traffic on PortChannel (WS-X6408 and WS-X6516) on Sup720
CSCsj72251	Unknown	BOOTP replies dropped if DHCP snooping is enabled
CSCsj72438	Unknown	Control plane instability and %EARL-DFC3-2-SWITCH_BUS_IDLE: Switching bu
CSCsj75636	Unknown	Crash in SP observed when per-port igmp statistics cleared
CSCsj77885	Unknown	%HA_EM-7-FMS_POLICY_MAX_ENTRIES message because of teminal length limit
CSCsj78751	Unknown	ES20: shut & no shut on ZR XFP causes the port to stay down
CSCsj80655	Unknown	timer value overflows when the specified val is larger than a long val
CSCsj81067	Unknown	IPSec VPN SPA: OLD-CISCO-CHASSIS-MIB does not return cardType
CSCsj81502	Unknown	show pagp clis are not displaying the correct information .
CSCsj83102	Unknown	crash upon card type configuration on WS-X6582-2PA / PA-MC-8TE1+
CSCsj84641	Unknown	some patches failed to commit during install commit of 41 patches.
CSCsj85930	Unknown	t/b slot_earl_icc_shim_addr tm_send_message on changing to rpr
CSCsj86854	Unknown	SPAN does not reset FPOE (to SP) when converting to distributed
CSCsj87584	Unknown	call-home inventory full needs show ipdrom switch all for VSS
CSCsj88208	Unknown	DOM not working for LR+ and ER+ Xenpaks
CSCsj88221	Unknown	class-default should not police BPDUs
CSCsj89470	Unknown	Bus Error crash in Netflow on 7200 running netflow and L2TP
CSCsj89905	Unknown	EEM applet hangs if system prompt is changed
CSCsj90252	Unknown	SYS-3-CPUHOG IP RIB Update seen on Active RP
CSCsj91795	Unknown	Appl TCs are not monitored when 12.2SRB BR is used with 12.4(15)T1 MC .
CSCsj95733	Unknown	Packet loss between sup4 uplink to 65xx modules
CSCsk02456	Unknown	TBs found @ pm_assert_fail. .
CSCsk02962	Unknown	Supervisor Reload after SSO switchover on Multicast MET reconstruction .
CSCsk03679	Unknown	VS2: show mls nde intermittently causes ALIGN-3-SPURIOUS T/B's
CSCsk06769	Unknown	shut on L2 int cause packets to loop back on T1 int causing traffic loss
CSCsk09155	Unknown	spa-ipsec-2g remains in Initialization state
CSCsk18206	Unknown	TCAM adjacency hardware programming problem with PBR and NAT .
CSCsk20346	Unknown	P router crash due to no EOBC buffer and illegal access to low address
CSCsk23521	Unknown	EARL-SPSTBY-2-SWITCH_BUS_IDLE is seen with SW switched traffic
CSCsk24272	Unknown	SUP720-3B RP Crash due to I/O Buffer Leak by NDE w/ NAM 127.0.0.x Addr
CSCsk26973	Unknown	Memory leak in nhrrp_cache_delete for incomplete cache entries
CSCsk30146	Unknown	Router crashed %DUMPER-3-PROCINFO: pid = 12315: (sbin/ios-base) SIGBUS
CSCsk33661	Unknown	show platform hardware capacity should include LTL usage .
CSCsk33724	Unknown	DOM does not work anymore for cwdm gbic/sfp
CSCsk33740	Unknown	replay window size of 1024 causes IPSec Policy Check and Replay Failure
CSCsk34237	Unknown	Egress multicast replication broken due to wccp .

Identifier	Technology	Description
CSCsk37675	Unknown	IKE stuck after several hours of IKE SA rekey .
CSCsk38024	Unknown	VS2: EtherChannel state on standby is incorrect due to out of order FEC
CSCsk41374	Unknown	device crash seen when auth-proxy enabled on the LPIP vlan .
CSCsk43058	Unknown	Port channel to WiSM controller suspended after upgrading to 12.2(33)SXH
CSCsk43673	Unknown	C2W1: Network RF client takes too long to process switchover . .
CSCsk45585	Unknown	Heathland: On bootup MPLS not supported on platform message
CSCsk55012	Unknown	setting portDuplex from 'full' to 'full' may cause standby reset .
CSCsk55423	Unknown	7600's SPD implementation allow COS 5 or above in Extended headroom
CSCsk58810	Unknown	should NOT allow enable port-security on negotiating trunk interface .
CSCsk60874	Unknown	show tech needs 'show diagnostic results' and 'show diagnostic events' .
CSCsk60912	Unknown	MPLS forwarding table empty on standby RP .
CSCsk62017	Unknown	multicast (hsrp/ospf) coming from service modules is blackholed by vACL.
CSCsk64860	Unknown	Config rollback to data file causes system to stuck at delete file mode.
CSCsk65482	Unknown	clear ip slb CLI is defined with wrong privilege level
CSCsk65860	Unknown	IOS-SLB:Security ACL breaks Client traffic
CSCsk67801	Unknown	WiSM:WiSM interfaces in manual LAG get shutdown at reload
CSCsk68656	Unknown	AB76: MFI push issu client msg type 5020 V1 MTU differ btwn SRB1/SRC
CSCsk70087	Unknown	Sup720 TLB exception created by fill_earl_vlan_stats_hdr .
CSCsk73627	Unknown	WS-X6548-GE-TX powered down due to keep alive polling feature
CSCsk78396	Unknown	Router may crash if SNMP walk on cefcModuleTable .
CSCsk80934	Unknown	Add errmsg to clearly indicate if lc reset due to power convertor failur
CSCsk82459	Unknown	VS2: continuous msg - Flooding detected in diag inband driver caused SSO
CSCsk82877	Unknown	METROPOLIS #0 cnt=1 reg:[1B0]kic_kic_int 02
CSCsk83524	Unknown	L3 physical interface input drop counter is incorrect .
CSCsk83646	Unknown	BX10 ports don't link-up after Centaurus resets . .
CSCsk83683	Unknown	VRF-Lite aware PBR feature does not work after reload/SSO swover
CSCsk84944	Unknown	unidirectional Ethernet UDE is broken on WS-6704 after SW upgrade
CSCsk85987	Unknown	VS2: After 2 x SSO, SVI was down and multicast join didn't work
CSCsk86381	Unknown	KMI memory leak in 'IPSEC key engine' when delete p2 failed
CSCsk87262	Unknown	Switch crashes when polling port security MIB for SIP or Flexwan
CSCsk88173	Unknown	mac-address-table static with disable-snooping break on reboot
CSCsk88760	Unknown	122SR:Routers crashes on unconfiguring vlan in the LACP mode
CSCsk89100	Unknown	6196-RJ-21 Dropping all ingress frames with CRC counter incremented.
CSCsk89335	Unknown	After SSO switchover, see 6K DC power supplies mismatched .
CSCsk91267	Unknown	Module fails to come up with (FRU-power failed)
CSCsk93587	Unknown	TestFabricCh0Health test failure with unidir traffic via Ch1 on Berytos
CSCsl04500	Unknown	OBFL process causing 6708 high CPU

Identifier	Technology	Description
CSCsl04687	Unknown	DFC3C pps counter does not work
CSCsl06110	Unknown	DHCP snooping agent: parse failures when importing the DB
CSCsl08912	Unknown	Vlan access list not working when have "xconnect vfi #" under the SVI
CSCsl13477	Unknown	SSO not working with crypto maps terminating at same peer address .
CSCsl23758	Unknown	WS-X6548-RJ-45: Wrong value of the output counter on show interface
CSCsl26981	Unknown	PBACL config causes hostname change when you downgrade to Rockies image
CSCsl26998	Unknown	Switch crashes on applying PBR with next-hop verify-availability
CSCsl41230	Unknown	IPSec SPA breaks IPSec if interesting traffic uses TCP ports
CSCsl70148	Unknown	PIM enabled p2p Crypto GRE Tunnels not installed in Hardware
CSCsl70634	Unknown	67xx EC tx/rx traffic dependency resulting in low throughput
CSCsl94488	Unknown	Smartports CLI missing in sup32 ipbase image
CSCsm17983	Unknown	Memory corruption by l3_mgr_e7_fmask_init_platform
CSCei22295	WAN	Traceback is seen at fr_svc_tearardown_calls
CSCsc38968	WAN	Frame-relay EEK failure does not keep subinterface down
CSCsi70599	WAN	Standby reloads due to Config Sync: Line-by-Line sync verifying failure



Caveats Resolved in Release 12.2(33)SXH

Resolved AAA Caveats

- [CSCsg88561](#)—Resolved in 12.2(33)SXH

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

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

Limited to C7600 ONLY.

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

Resolved Content Caveats

- [CSCsi46028](#)—Resolved in 12.2(33)SXH

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

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

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

Resolved Infrastructure Caveats

- [CSCsc64976](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20051201-http.shtml>

- [CSCsi13344](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sr-20090114-http.shtml>

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

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

- [CSCsf04754](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20080610-snmpv3.shtml>

Resolved IPServices Caveats

- [CSCsh04686](#)—Resolved in 12.2(33)SXH

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(33)SXH

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.

- [CSCse56501](#)—Resolved in 12.2(33)SXH

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://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>

- [CSCek37177](#)—Resolved in 12.2(33)SXH

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

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

This issue is documented as Cisco bug ID [CSCek37177](#)

There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>

Resolved LAN Caveats

- [CSCsd34759](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sr-20060913-vtp.shtml>

Resolved Legacy Protocols Caveats

- [CSCsf28840](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20070110-dlsw.shtml>

Resolved Management Caveats

- [CSCsf07847](#)—Resolved in 12.2(33)SXH

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 MPLS Caveats

- [CSCsa52940](#)—Resolved in 12.2(33)SXH

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 Multicast Caveats

- [CSCse15770](#)—Resolved in 12.2(33)SXH

Symptom: IOS device may reload unexpectedly

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

Workarounds: Disable the MRM feature,

Resolved Routing Caveats

- [CSCec12299](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20080924-vpn.shtml>

- [CSCed40933](#)—Resolved in 12.2(33)SXH

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://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6.shtml>.

- [CSCef67682](#)—Resolved in 12.2(33)SXH

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/products_security_advisory09186a00807cb0fd.shtml

contain fixes for this issue.

- [CSCsd58381](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml>

Resolved Security Caveats

- [CSCsg40567](#)—Resolved in 12.2(33)SXH

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.

- [CSCsc19259](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20070808-scp.shtml>.

- [CSCse50135](#)—Resolved in 12.2(33)SXH

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

Conditions: AAA is configured

Workarounds: None

- [CSCsd85587](#)—Resolved in 12.2(33)SXH

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/products_security_advisory09186a00809bb300.shtml .

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://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml> 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/products_security_advisory09186a0080847c49.shtml

- [CSCse24889](#)—Resolved in 12.2(33)SXH

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 Unknown Caveats

- [CSCek49649](#)—Resolved in 12.2(33)SXH

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

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

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

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

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

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

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

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

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

Control Plane Policing (CoPP) can be used to block traffic with a destination IP address in the 127.0.0.0/8 address range sent to the device. Cisco IOS Software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the

management and control planes to minimize the risk and effectiveness of direct infrastructure attacks. CoPP protects the management and control planes by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations.

```
!-- Permit all traffic with a destination IP
!-- addresses in the 127.0.0.0/8 address range sent to
!-- the affected device so that it will be policed and
!-- dropped by the CoPP feature
!
access-list 111 permit icmp any 127.0.0.0 0.255.255.255
access-list 111 permit udp any 127.0.0.0 0.255.255.255
access-list 111 permit tcp any 127.0.0.0 0.255.255.255
access-list 111 permit ip any 127.0.0.0 0.255.255.255
!
!-- Permit (Police or Drop)/Deny (Allow) all other Layer3
!-- and Layer4 traffic in accordance with existing security
!-- policies and configurations for traffic that is authorized
!-- to be sent to infrastructure devices
!
!-- Create a Class-Map for traffic to be policed by the
!-- CoPP feature
!
class-map match-all drop-127/8-netblock-class
  match access-group 111
!
!-- Create a Policy-Map that will be applied to the
!-- Control-Plane of the device.
!
policy-map drop-127/8-netblock-traffic
  class drop-127/8-netblock-class
    police 32000 1500 1500 conform-action drop exceed-action drop
!
!-- Apply the Policy-Map to the Control-Plane of the
!-- device
!
control-plane
  service-policy input drop-127/8-netblock-traffic
!
```

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

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

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/grtrtlmt.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

- **CSCsd68605**—Resolved in 12.2(33)SXH

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(33)SXH

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/products_security_advisory09186a00807f4139.shtml

- **CSCsf12082**—Resolved in 12.2(33)SXH

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://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml>

- **CSCsg53589**—Resolved in 12.2(33)SXH

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

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

Workaround: Disable DHCP Snooping

- **CSCsi01470**—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20080326-mvpn.shtml>.

- [CSCsi86396](#)—Resolved in 12.2(33)SXH

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(33)SXH

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(33)SXH

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.

- [CSCek36513](#)—Resolved in 12.2(33)SXH

Symptom: When allocating buffers for the initial creation of a Crypto Key an error may occur that could cause the Crypto engine to generate an incorrectly sized key.

Conditions: None

Workaround: None

- [CSCse52951](#)—Resolved in 12.2(33)SXH

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/products_security_advisory09186a00807f4139.shtml

- [CSCsh73972](#)—Resolved in 12.2(33)SXH

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

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

Workaround: None

- [CSCsg70474](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

Resolved Voice Caveats

- [CSCsd81407](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

- [CSCsc60249](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

- [CSCsi60004](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

- [CSCeb21064](#)—Resolved in 12.2(33)SXH

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/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>.

Other Resolved Caveats in Release 12.2(33)SXH

Identifier	Technology	Description
CSCdp33836	AAA	unhide aaa authorization console and warn user
CSCef27578	AAA	The router crashes when test aaa stop CLI is issued
CSCek46627	AAA	Accounting method list update failed .
CSCsa40461	AAA	VRF-aware TACACS+ not working with enable authentication
CSCsb11698	AAA	Input Queue Wedge with TACACs
CSCsd49317	AAA	no tacacs-server administration causes router hang .
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
CSCse69002	AAA	Accounting of auth failure doesn't work with some switches
CSCsf30451	AAA	radius-server attrib 32 include-in-access-req/accounting-req not sent
CSCsg43322	AAA	AAA: No free authorization/accounting lists for network
CSCsh23142	AAA	aaa local authentication not happening for authproxy .
CSCsh43536	AAA	aaa group server config lost after reboot
CSCsh46990	AAA	Console hangs with enable/line as aaa fall-back methods
CSCef35417	Access	7200:Frame-relay LMI messages are not being handled correctly
CSCef81197	Access	Rx-error throttling disabled on VIP after OIR
CSCeg55131	Access	Spurious access @mip_unchain_idb while configuring t1 controller
CSCeh01287	Access	FR/WAN over IP: Required sessions are not establised. keeps flaping
CSCei05246	Access	CE3 interface output frozen after OIR VIP6-80
CSCin88048	Access	unchannelized interface line -protocol not coming up
CSCsa64102	Access	Spurious accesses and Badshare with PA-MC-T3
CSCsa83881	Access	PA-T3+: interface port remains up during unavailable seconds
CSCsa83897	Access	PA-MC-T3: T3 port does not enter UAS during high P and C-bit error rates
CSCsa93523	Access	7200 PA-E3 incrementing carrier transitions and packet drops
CSCsb07696	Access	HYPERION-4-HYP_RESET: Hyperion Error Interrupt
CSCsb21867	Access	PA-MC-8TE1+ in Flexwan: ctrlr detects LOS after restart does not recover
CSCsb23106	Access	7206vrx with NPE-G1 bus error crash when OIR PA-2T3+
CSCsb27358	Access	PA-T3+ goes down when seeing two bursts of AIS less than 1 second each

Identifier	Technology	Description
CSCsb29894	Access	Frame relay input errors and CRC errors with reload and rpr+ switchover
CSCsb83876	Access	Interface counters stop incrementing on serial interface counter
CSCsc48543	Access	shot down E3 controller via SNMP crash the c7200 device
CSCsc66658	Access	Interfaces starts toggling when loopback local configured
CSCsc85029	Access	AIS led on pa-mc-2t3+ remains on if t3 connected after reload
CSCsc91995	Access	Spurious memory access T3 Flexwan
CSCsd41989	Access	ct3 pa: t3 controller stays down for local loopback in flexwan
CSCse06752	Access	LAM /32 cef entry shows unresolved
CSCdy11156	ATM	13E:12E:RP crashed while applying config on ATM-PA,mgd_timer_stop .
CSCea26450	ATM	PVC may stay down when interface cable is pulled out/put back rapidly
CSCef62324	ATM	router may crash upon removal of ATM subinterface with PVCs
CSCeg03837	ATM	ALIGN-3-SPURIOUS traceback in Standby RP when subinterface is configured
CSCeh71960	ATM	alignment traceback on standby RP
CSCei39688	ATM	ATM subinterface fails to pass traffic due to CEF initialization failure
CSCei45749	ATM	PVCs go inactive when clear interface atm3/ima0 command is issued
CSCek39364	ATM	CLI: HA Standby router reloads while unconfiguring atm bundle .
CSCek39946	ATM	Local Switching connectivity not recovering after switchover
CSCin94072	ATM	Bundle master should have length zero and adj complete
CSCin95455	ATM	Duplicate options displayed in connect command output .
CSCsa85850	ATM	PA-A3 allows to configure CBR at 155000 kbps .
CSCsb12329	ATM	ifAdminStatus of ATM sub-interface is down without shutdown command
CSCsc49134	ATM	Router crashes while creating ATM subinterface - ATM pvc discovery
CSCsd73881	ATM	Router gets reloaded at process_ok_to_reschedule .
CSCsd88636	ATM	Continuous RP CPUHOG by ATM OAM Input process
CSCsh39541	ATM	CEF adjacency shows incomplete on ATM int with SUP4 .
CSCsh74025	ATM	clns packets not being punted by an enhanced flexwan .
CSCsb89463	Content	WCCP doesn't redirect packets with 'ip cef' enabled
CSCsc72066	Content	MNLB - incorrect affinities installed
CSCsc94191	Content	WCCP does not GRE Redirect TCP FIN packet that would fragment
CSCsd20327	Content	WCCP going up/down
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
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
CSCuk60755	Content	WCCP redirection broken in process switch path

Identifier	Technology	Description
CSCuk61396	Content	WCCP does not interop with NAT/Inspection
CSCuk61773	Content	WCCP: ignore redirect assignment messages with identical content
CSCdx62060	Infrastructure	Interface names made to display full while show int summary done
CSCdy11174	Infrastructure	ciscoFlashCopyTable/ciscoFlashMiscOpTable obj unreadable @ creation
CSCee23195	Infrastructure	Spurious memory access in show ipc queue .
CSCee72249	Infrastructure	snmp-server host only supports 1 host and trap not shown in config
CSCef64439	Infrastructure	PRE takes long time to become STANDBY HOT after switch-over. .
CSCef77951	Infrastructure	excessive processor memory held by IRB/CRB rxtypes
CSCeg12652	Infrastructure	Vrf aware LDP traps fail
CSCeg41564	Infrastructure	Unable to delete snmp-server enable traps sonet from sh run
CSCeg62070	Infrastructure	Tracebacks noticed with Radius configs through HTTP Post
CSCeh12411	Infrastructure	router hangs while executing show runn-
CSCeh62781	Infrastructure	%IPC-5-WATERMARK FAST.control.RIL(2070000.E) seat 2070000
CSCeh74715	Infrastructure	SNMPv1 should not send traps with counter64
CSCeh88425	Infrastructure	ip http client password does not survive reload
CSCei16552	Infrastructure	cannot remove snmp-server engineID from running-config
CSCei32102	Infrastructure	Need an option to disable snmp traps for link during switch failover
CSCei87744	Infrastructure	System doesnt count milli-seconds
CSCej57779	Infrastructure	BGP: some vrf instances are not up on bgp-bpn setup after sys-reload .
CSCek32390	Infrastructure	IP SLA: CPUHOG seen in SAA Event Processor
CSCek42751	Infrastructure	%Error opening system:/running-config (No such file or directory)
CSCek46087	Infrastructure	IPC ack_pending not updated correctly
CSCek48739	Infrastructure	ION config checkpoint SNMP/HTTP handle for sierra branch
CSCek55001	Infrastructure	Dir /recursively with many directories crashes the router
CSCek56630	Infrastructure	race condition in process_sleep_on_timer code
CSCek64188	Infrastructure	Fragmentation fix of CSCek64051 is incomplete
CSCek72874	Infrastructure	Initiator crashes with 500 fvr and ivrf for BGP protocol
CSCek74114	Infrastructure	ASL: Rollback was NOT able to remove ASL configuration
CSCek77066	Infrastructure	SNMP query returns incorrect flash name
CSCin96568	Infrastructure	FTS-7514-1: CISCO-PROCESS-MIB support for modular IOS
CSCin97208	Infrastructure	Standby does not come up during switchover with slavenvram in access
CSCin99048	Infrastructure	Crash seen when "class-map type inspect" or "sh class-map type inspect
CSCir00786	Infrastructure	AAA authorization shouldnt be invoked when updating Boot Variables .
CSCsa58550	Infrastructure	Alignment correction at ipc_process_raw_pak
CSCsa78886	Infrastructure	v-access leak with ppoe session even though SSS requests v-access .
CSCsb14936	Infrastructure	SNMPv3 EngineID (default value) not established correctly
CSCsb80841	Infrastructure	router crashes when configuring interface range on HWIC-4ESW

Identifier	Technology	Description
CSCsb85983	Infrastructure	bootflash corruption seen even with CSCei17174 fix
CSCsb92309	Infrastructure	reimplementation of cache_interface_state under CSCdw09607
CSCsc04397	Infrastructure	Spurious memory access made at Fcheck_interface_state
CSCsc06891	Infrastructure	no traps are sent when CF is inserted or removed.
CSCsc13652	Infrastructure	SNMP: value of _LargestFree is greater than total amount of memory.
CSCsc13670	Infrastructure	Rollback: backups generated are truncated at times in archive feature .
CSCsc33350	Infrastructure	snmp trap link-status compulsorily becomes disable in dot1Qsubinterface
CSCsc44237	Infrastructure	memory leak in client applications iterating over an empty idb list
CSCsc53414	Infrastructure	IOS Low Memory Caused by SSH
CSCsd13491	Infrastructure	show memory statistics history displays wrong values in processor pool
CSCsd23127	Infrastructure	IPC-SP-2-LOCK IPC-SP-2-UNLOCK followed by tracebacks on SSO s/w
CSCsd24224	Infrastructure	SSO: standby reloads due to config sync error atno exception crashinfo
CSCsd29469	Infrastructure	Cat6000 SNMP stops responding while polling from ciscoEnhancedMemPoolMIB
CSCsd32923	Infrastructure	Bus Error in Exec attempting command completion in a full command buffer
CSCsd36608	Infrastructure	Multiple IPC Versioning Process instances causing memory leak
CSCsd37284	Infrastructure	SP06: Unexpected exception to CPUvector 2000, PC = 0 when copy rmon cfg
CSCsd38693	Infrastructure	Renaming ATA/CF file to a name ending with ... corrupts DOS File System
CSCsd49133	Infrastructure	Alarms are not pouplated in ceAlarmTable - ceAlarmList is empty.
CSCsd59610	Infrastructure	%SYS-4-REGEXP: new engine: regexp compilation had failed.
CSCsd62013	Infrastructure	Traceback on Standby RP@add_lpmapping_entry_private+74
CSCsd65958	Infrastructure	Incorrect value for ifHCInOctets, ifHCOutOctets, ifHCInUcastPkts
CSCsd70700	Infrastructure	rsp crashed with TB pointing to ralib_event_card_inserted()
CSCsd72511	Infrastructure	SNMPv3 community strings are sent in the clear (TACACS+ accounting)
CSCsd77560	Infrastructure	snmp auth/priv users are not persisted across reload
CSCsd77751	Infrastructure	IOS - SUP720 - sends empty/blank syslog messages
CSCsd80252	Infrastructure	verify /md5 returns error msg %Error computing MD5
CSCsd90876	Infrastructure	Rainier:memory corruption when a '
CSCse10074	Infrastructure	MF: any traps sent to a host specified to V3 user will crash active .
CSCse19199	Infrastructure	C2C1: config snmp traps and host will casue SNMP entity no access 2 mins
CSCse22016	Infrastructure	MLPoATM config gets truncated and link goes down after router reload
CSCse42502	Infrastructure	snmp-queue length incorrect
CSCse56676	Infrastructure	Some SNMP notifications go to the wrong host
CSCse80032	Infrastructure	Mediation Device cannot resync SNMP engine time after 7600 reload .
CSCse82855	Infrastructure	show monitor event-trace error message prints to syslog not terminal
CSCse95758	Infrastructure	Access Lists support for all CONFIG-COPY-MIB protocols under snmp-server
CSCse98807	Infrastructure	Traceback, Process=SNMP Timers, %SCHED-3-STUCKMTMR during regression .
CSCsf00284	Infrastructure	Event trace timestamps should be datetime no uptime by default

Identifier	Technology	Description
CSCsf03710	Infrastructure	ION - Process and Mempool MIB - collapse of ion_mibs_all branch
CSCsf04921	Infrastructure	18SXF6: getnext loop condition detected on ciscoFlashFileTable .
CSCsf27228	Infrastructure	Coredump is not working properly in NativeIOS
CSCsf32784	Infrastructure	Need a mechanism to tell if a CF disk is bootable
CSCsg00673	Infrastructure	SNMP query on Transient memory shows wrong values .
CSCsg04840	Infrastructure	Fix the list of SA warnings
CSCsg06724	Infrastructure	Box crashes with 100 VRF Lite Config with PIM & BGP
CSCsg15939	Infrastructure	Switches crash after remove/plug in compact flash
CSCsg25826	Infrastructure	CiscoFlashMib ciscoFlashPartitionName is truncating the flash name
CSCsg28584	Infrastructure	show list does not display all entries; list corrupted
CSCsg32222	Infrastructure	Need the support for 64 bit bit/second OID on Cat6k/7600
CSCsg40016	Infrastructure	show tech causes various system problems
CSCsg42072	Infrastructure	Virtual Exec sessions not freeing memory
CSCsg43466	Infrastructure	%IPC-5-INVALID: Invalid Dest Port w/ TB @ ipc_xmt_account after SSO
CSCsg61640	Infrastructure	System repeatedly crashes with/without no ip address command
CSCsg70355	Infrastructure	adopt new default summer-time rules from Energy Policy Act of 2005.
CSCsg71381	Infrastructure	Disabling cisco-specific lsa and tty, removea all ospf trapa from conf
CSCsg80228	Infrastructure	Additional byte appended to ifIndex causes SNMP trap misalignment
CSCsh23981	Infrastructure	IPC ISSU: First message to seat 0x2070000 not found .
CSCsh28948	Infrastructure	High CPU for sh run/wr mem with PTA sessions up
CSCsh46540	Infrastructure	Router hangs with simultaneous format and copy operations
CSCsh64335	Infrastructure	Snmp query on a directory with more than 127 char causes crash
CSCsh70638	Infrastructure	Spurious memory access @ top_proc_hist_entry
CSCsh79371	Infrastructure	SNMP memory leak for Modular IOS on 12.2(18)SXF6 .
CSCsh93041	Infrastructure	PRE2: ifLastChange OID is increasing slightly over the time
CSCsh93638	Infrastructure	High PacketLossSD values when gathering SAA data
CSCsi04892	Infrastructure	unconfigure no ip sla schedule 2 gives error message
CSCsi11056	Infrastructure	Cannot configure http probe
CSCsi15080	Infrastructure	RP crash when listing files by using the context-sensitive help
CSCsi17590	Infrastructure	CPUHOG at process check heaps with 600 vrf configured on PE router .
CSCsi22502	Infrastructure	installer imf.tar file not being zipped creates uninstallable image
CSCsi48665	Infrastructure	Specify exact or prefix for SNMPv3 group to context name assoc. from CLI
CSCsi51014	Infrastructure	disk access CLI freeze the router after running fsck .
CSCsi73444	Infrastructure	IPC: %SIP200_MP-4-PAUSE: Non-master CPU is suspended for too long, from
CSCsj55691	Infrastructure	HTTPS: crash at http_ssl_read when https url is not ready
CSCdy14140	IPServices	bus error at tcp_outputpending caused by sh run and format slot att
CSCed28542	IPServices	%SYS-2-INTSCHED: may_suspend at level 3 in IP NAT Ager

Identifier	Technology	Description
CSCed93425	IPServices	DHCP Database fails to write to local flash.
CSCed95187	IPServices	IP ID field is predictable for connectionless RST packets .
CSCee30364	IPServices	ip ftp username not used after username was previously used in URI .
CSCee32814	IPServices	Source port selection is predictable, should be harder to guess
CSCee73956	IPServices	BTSH: TCP filtering support .
CSCef09586	IPServices	CMs stuck in init(d) if DHCP ser. ip addr. overlaps with diff VRF
CSCef59415	IPServices	routes still exists even after clear ip dhcp binding
CSCeh11675	IPServices	NAT failures with port allocation
CSCeh35980	IPServices	after unconfig & config of BGP, seeing a crash in TCP .
CSCeh83666	IPServices	ip/ipnat_db.c: dereferenced pointer prev_block might be null
CSCeh86935	IPServices	Multiple TCP services (incl. TACACS+) use incorrect source address .
CSCei27084	IPServices	CLI on Discontiguous pools broken : hides later pools
CSCei93982	IPServices	Modified ALG classification base on src & dst port
CSCek12203	IPServices	File system issues after unsuccessful FTP operation. .
CSCek25582	IPServices	continuous Spurious Accesses at igmp_process_timers
CSCek66164	IPServices	show command pipeline redirect into rcp crashes the router
CSCek68118	IPServices	window scale option(03030001) occurs in debug ip tcp packet output .
CSCin78000	IPServices	LDP session in xmit state if MPLS flapped at high traffic on L2 SUP3
CSCsb27868	IPServices	DHCP Relay should unicast offer/ack on unnum ethernet sub- int
CSCsc12899	IPServices	SSM Mapping configuration inside a VRF broken
CSCsc47919	IPServices	VRRP does not correctly interoperate with Proxy ARP
CSCsc61309	IPServices	Buffer leak in dhcpv6.
CSCsc78813	IPServices	DNS reply payload does not get translated in the NAT router.
CSCsd23056	IPServices	reverse telnet (tty daemon) broken by TCL feature
CSCsd33013	IPServices	FHRPs fail to clear ARP entry after Duplicate IP event
CSCsd42600	IPServices	%SYS-3-BAD_RESET alongwith SegV exception crash
CSCsd43344	IPServices	isis-nsf info doesnt sync with standby in SSO mode .
CSCsd50113	IPServices	HSRP State Change Logging Level Incorrect
CSCsd51530	IPServices	autocommand-options nohangup is removed on line vty 0-4
CSCsd52667	IPServices	CLI: ip nat pool config causes cpuhog and router crash .
CSCsd61092	IPServices	SSM-Mapping enabled in the vrf but not NVGEN'd
CSCsd69052	IPServices	Netbios/NAT optimization
CSCsd80754	IPServices	HSRP Active-Router not respond to ARP request about VIP
CSCsd87810	IPServices	IOS tftp server should not differentiate between / and backslash in path
CSCse01124	IPServices	HSRP groups stuck in Init state if dampening cfgd on certain interfaces
CSCse02028	IPServices	Some commands fail in APPEND of FTP which uses KRON.
CSCse04560	IPServices	tftp-server allows for information disclosure .

Identifier	Technology	Description
CSCse05106	IPServices	sh mls netflow ip sw-installed does not show any flow with NAT config.
CSCse05736	IPServices	A router running RCP can be reloaded with a specific packet .
CSCse23548	IPServices	modular ios (ION) : logging source-interface command ignored
CSCse51263	IPServices	RP side console Exec process hangs deadly sometimes
CSCsf16715	IPServices	TCP will leak TCBS if app closes in notification callback context
CSCsf27218	IPServices	Router does not reply to TCP ECHO request
CSCsf33034	IPServices	T/B tcb_isvalid+7C during bootup and when EOMPLS vc is configured.
CSCsg00846	IPServices	Crash of RP blob due to a missed inetd_service_mutex unlock
CSCsg19598	IPServices	SSH session hangs intermittently
CSCsg38013	IPServices	ssh ipv6 client not working with ION image .
CSCsg39837	IPServices	Add Transport Port Agent to allow reserving/randomly generating ports
CSCsg49882	IPServices	ip ftp source-interface ip address & interface chang after write mem
CSCsg56926	IPServices	no logging console not working in ION for tcp debugs
CSCsg59059	IPServices	sup720 crashes when delete ip nat pool after clearing nat translations
CSCsg78218	IPServices	can not remote ip rcmd mwam 0.0.0.0 mwan enable on 12.2(18)sxd7a
CSCsg99331	IPServices	Show host doesn't display hostname fully for Unknown, temp entries .
CSCsg99600	IPServices	Modular IOS : ip helper address 1.1.1.255 not work
CSCsh21505	IPServices	ip helper address on vrf interface in ION, dhcp routed with global table
CSCsh24843	IPServices	DHCP Relay-Agent forwarding out incorrect VLAN using IP-Unnumbered
CSCsh25210	IPServices	'ip dhcp database' may fail by running 'config replace'
CSCsh31939	IPServices	c2w1:ciscoFtpClientMIB:Get & Set operation cause process deadlock & crash
CSCsh33430	IPServices	Crash in hsrp_addr_hash_lookup or hsrp_addr_hash_lookup_interface
CSCsh36234	IPServices	install commands fails with SCP as source .
CSCsh56081	IPServices	Spanning tree of vlan-bridge is operated incorrectly
CSCsh58099	IPServices	ftp process should call a registry cleanup- Message Could not register..
CSCsh59375	IPServices	Relay_vrf:dhcp ip addr not switched after smart-relay enabled .
CSCsh59439	IPServices	Unable to configure same HSRP virtual MAC address on several interfaces
CSCsh75069	IPServices	Input Queue Wedge with UDP Echo packets .
CSCsh75240	IPServices	nat log translations syslog does not work
CSCsi10974	IPServices	Error configuring dhcp option 67
CSCsi29875	IPServices	3/27: SP: oir_rf_reload_self: icc_req_imm failed, node not booting
CSCsi33626	IPServices	Tracebacks in qde_start in transport_port_agent, semaphore uninitialized
CSCsi40766	IPServices	H323 calls fail after router processes total of 54535 calls
CSCsi45840	IPServices	ARP requests for HSRP virtual IP may fail after switchport cmd is used .
CSCsi51178	IPServices	Switch crashes due to ssh session at pak_client_set_pid .
CSCsi77774	IPServices	On modular IOS,Telnet on VRF int is allowed irrespective of vrf-also key
CSCsj07297	IPServices	Config Sync: in no vrrp 1 preempt and standby resets

Identifier	Technology	Description
CSCsj09846	IPServices	crash during bootup with ALIGN-1-FATAL:Illegal access to a low address
CSCsj22472	IPServices	BGP forced deleting vrf ARP entry if BGP session is not up
CSCsj38828	IPServices	Sierra:Memory Leak on HTTP Core Task during Webauth/http access
CSCdz80245	LAN	SNMP: Need ifDescr output without description
CSCek46996	LAN	Cwan FA-PA port need to be in promiscuous mode if IP address not conf
CSCek65222	LAN	vlan config produces inconsistent results
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
CSCse25462	LAN	VTP password configuration should follow IOS conventions
CSCse40078	LAN	VTP integer wrap
CSCsf25728	LAN	Unable to session to FWSM when source-bridge ring-group is configured
CSCsd55300	LegacyProtocols	DLSw ER LLC session fails to connect with SUP720 or SUP32
CSCse13882	LegacyProtocols	Show dlsw peer caused router to crash
CSCse17611	LegacyProtocols	DLSw Circuits Connect outside of DLSW ER to switch with passive mapping
CSCei29821	Management	cns config initial is not getting removed from startup configuration
CSCek36010	Management	Need show cdp port <module> option in IOS
CSCse95996	Management	PRC: config.failure recvd when attr is verbose=all, legacy CLI
CSCsg05873	Management	Buffer leak with SNA Focalpoint PU consuming middle buffers with NMVTs
CSCsg88433	Management	IP Telephone issues seen with Dhcp snooping and NAC posture validation
CSCsh79171	Management	SNMP GetNext on cdpGlobalLastChange.0 returns error
CSCdy83805	MPLS	%MPLS_TE-3-CONSISTENCY: consider replacing errmsg with buginf
CSCdz08851	MPLS	FRR doesnt trigger on ethernet using RSVP HELLO
CSCec56047	MPLS	TE:gtag-rrr: TSP Tunnel not up (Destination IP address not found)
CSCed21063	MPLS	TE Tunnel Destination Label Missing
CSCed71976	MPLS	MPLS error messages are incomplete and need improvement (TE)
CSCef02056	MPLS	Inter-AS TE lsp keeps on re-signal when RSVP Policy rejects on ASBR
CSCef59507	MPLS	Dead LDP session still shows up after new session established
CSCef87449	MPLS	RRR LM: Admin shut handler does not preempt LSPs
CSCeg11894	MPLS	MPLS VPN: Forwarding failure between CSC-PE and PE to CSC-CE link
CSCeg74562	MPLS	LDP Scalability Problem with high neighbor count
CSCeg83614	MPLS	Crash while signalling FRR BW-P LSP
CSCeh18195	MPLS	MPLS-TE: packet loss when switching to tunnel intf after OL clears
CSCeh29183	MPLS	Tracebacks and FIB messages on auto-tunnel mesh bringup
CSCeh32706	MPLS	Inter-AS LSP is fail to signal after rebooting headend as ASBR box
CSCeh51720	MPLS	TE LM floods link in wrong area after links area is changed in ospf
CSCeh53373	MPLS	MPLS TE Inter-Area Node Protection Broken

Identifier	Technology	Description
CSCeh54615	MPLS	LDP Label Mapping msg optimization problems
CSCeh55186	MPLS	MPLS-TE: Pasive i/f command on broadcast links does not work properl
CSCeh72672	MPLS	rainier: duplicate per-vrf aggregate labels in LFIB after SSO swtove
CSCei83160	MPLS	PIM neighbor not recognised with multicast vrf tunnel.
CSCej00319	MPLS	RP Crash for E2 E3 E4 E4P interaction
CSCej01615	MPLS	LDP Scaling Problem with Release and Withdraw Messages
CSCej10404	MPLS	BN: 10GE - remote P fails to FRR - loss >50ms
CSCek28918	MPLS	BGP Peer route is NOT re-installed after clear ip route *
CSCek30891	MPLS	Traffic loss during reopt for zero bw TE LSPs
CSCek35484	MPLS	FRR: MP tears down protected lsp if local protection des flag rese
CSCsa65819	MPLS	BGP IPv4+Labels: Make send-label unconfigurable on non MPLS images
CSCsa77411	MPLS	RP crash at rrr_lm_unlock_bandwidth
CSCsb29168	MPLS	FRR-MIB: protected option is not properly displayed
CSCsb29326	MPLS	FRR-MIB:snmpwalk fails with cmplsFrrFacObjects
CSCsb52900	MPLS	mpls forwarding table label inconsistency after switchover
CSCsb85903	MPLS	R3.1 :Stdby RP Crashed @netsuper_lookup while becoming Active on SSO
CSCsb99035	MPLS	MPLS-TE Tailend does not reflect Path MTU into max pkt size
CSCsc02825	MPLS	12.3 Bus Error crash due to MPLS TDP process
CSCsc14208	MPLS	7600: Automesh tunnels went down after changing loopback IP address
CSCsc40236	MPLS	NRT: Multipath for IPv4+labels is broken when mpls ip is toggled
CSCsc94359	MPLS	BGP table and CEF forwarding table have mismatched labels
CSCsd21449	MPLS	MPLS-TE:No protection to primary LSP whilst reoptimising to optimal path
CSCsd33867	MPLS	MPLS TE Auto-Tunnel: Primary Tunnel missing protection from N-NHOP
CSCsd40153	MPLS	Rainier: label is not advertise to downstream ldp neighbor after reload
CSCsd43514	MPLS	CPU stuck in 99% after clear auto-tunnel backup or shut & no shut int
CSCsd55004	MPLS	FRR path gets reoptimized while in Active state
CSCsd87844	MPLS	change RD cause standby PRE reset
CSCsd87915	MPLS	TE tunnel goes down after SSO when refresh interval is 5000msec
CSCse09498	MPLS	Primary Tunnels not being established when using Auto-Tunnel mesh
CSCse38446	MPLS	NRT:snmp requests hangs when doing TE_MIB - mplsTunnelResourcePointer
CSCse75429	MPLS	Sierra: LDP neighbour doesnt come UP when LDP-GR is enabled
CSCse93633	MPLS	Auto-tunnel primary tunnels created to id 0.0.0.0
CSCsf14018	MPLS	sierra IOU/ION crash at vrf_sub_destroy() on config/unconfig of VRFs
CSCsf19418	MPLS	sh mpls ldp graceful-restart can cause router restart
CSCsf98345	MPLS	vrf-interface down cause LDP peer reset
CSCsg11718	MPLS	vrf stuck in delete pending state
CSCsg17790	MPLS	Large traffic drops intermittently observed on PRE3 switchover

Identifier	Technology	Description
CSCsg22369	MPLS	FRR in Ready state when bak tun is down after te config toggled in IGP
CSCsg44555	MPLS	7600 MPLS TE mid-point stuck at up/down and Juniper headend up/up
CSCsg96651	MPLS	%TDP-3-PTCLREAD: peer 6.6.6.6:0, read failure seen w/ VCs going down
CSCsh23227	MPLS	Packets dropped on FRR backup tunnel with FA
CSCsh35249	MPLS	targeted LDP convergence improvements
CSCsh38086	MPLS	TE tunnels can have maximum uptime 49 days, 17 hours, 2 minutes
CSCsi14211	MPLS	LDP process should optimize its cleanup of a down session
CSCec73297	Multicast	PIMv6: Unicasted PIM messages dropped if arriving over a non-PIM int
CSCee03081	Multicast	PIMv6: Source address for the register tunnel should be configurable
CSCef60452	Multicast	possible blackout when receiving Join on RPF interface (iif)
CSCeh67947	Multicast	Auto-RP group 224.0.1.40 Pruned after Assert.
CSCej10551	Multicast	MIB: ciscoPimInvalidRegister trap should return src of register
CSCej32303	Multicast	need to remove ip pim message-interval
CSCej78303	Multicast	RP crash @ pim_tt_grange_first after CMD: no ipv6 unicast-routing
CSCek31478	Multicast	ip multicast boundry cmd does not take effect after modify ACL
CSCek36056	Multicast	BSRv6: CLI failure on [ipv6 pim bsr candidate bsr] + BSR is broken .
CSCek42421	Multicast	One prune not processed on receiving batched join/prune message
CSCek46450	Multicast	consolidate CSCek33784 and CSCdv53060
CSCek66440	Multicast	iprouting crash at reg_attempt_remote_call with BGP
CSCsa64481	Multicast	RPF error when route is bound to serial interface
CSCsb85290	Multicast	IPv6 BSR: BSM forwarding breaks with ipv6 vrf implementation
CSCsc29555	Multicast	Memory Leak at pimv2_build_assert
CSCsc72515	Multicast	Bidir: On becoming non-DF, downstream int not deleted from olist
CSCsc98828	Multicast	PIMV6: SR flag set on RP acting as first hop
CSCsd13124	Multicast	Candidate BSR does not failover immediately when bsr interface is shut .
CSCsd16043	Multicast	Auto-RP for multicast may prematurely expire the group to RP mappings .
CSCsd17747	Multicast	Leftover ip pim vrf register-source command cause standby RP keep reset.
CSCsd39528	Multicast	Sync Damage: PIM Reg tunnels with duplicate ifindex values.
CSCsd42929	Multicast	Router does not ignore MLDv1 Leave group in SSM range
CSCsd49955	Multicast	RPF info created by (S,G) RPT-bit prune does not change by (S,G) join
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
CSCse03637	Multicast	PIM Dense Mode - Prune sent in error after assert is won .
CSCse05960	Multicast	PIM leaking memory used for xdr messages
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
CSCse34768	Multicast	VRF PIM neighbor lost if existing vrf mroutes exceeds route-limit value.

Identifier	Technology	Description
CSCse34938	Multicast	ipv6 pim bsr border command not available on LAN sub-interfaces
CSCse44079	Multicast	Multicast UDL - High CPU in IGMP Input when UDL interface down .
CSCse92050	Multicast	With mis-configuration, router may reload at twheel_running
CSCsg24505	Multicast	PIM-DM Assert winner does not always send prune
CSCsg58641	Multicast	Traceback: SCHED-2-MESSAGE: Key (PIM Process)
CSCsg71344	Multicast	PIM Join is not sent when shut/no shut is done
CSCsg94099	Multicast	PIM Register not sent to RP when mcast source is connected PPPoE client
CSCsh58021	Multicast	InetAddress objects in CISCO-PIM-MIB returned as strings instead of hex
CSCsh78277	Multicast	Sierra: mwheel CPUhog on RPF link failure causing crash .
CSCsh83214	Multicast	Named access-lists (with no matches) created when used with PIM commands
CSCsi03359	Multicast	Sending extra PIM hello if the first one does not go through
CSCeh71577	platform-72xx	Traceback found while loading image
CSCeg77503	platform-76xx	SAA Packets do not hit the outbound service policer
CSCeh32595	platform-76xx	Ping fails across atm interface after configuring routing protocols
CSCsa47099	platform-76xx	IPX broke on wan link of OSM-2OC12-ATM
CSCsa53708	platform-76xx	OSM crashes under stress when having to pad packets
CSCsa95421	platform-76xx	OSM-1OC48-POS-SS+ drops packets
CSCsb64975	platform-76xx	Rate counters are erratic for a bi-dir traffic more than 2 Gig
CSCsc25557	platform-76xx	PORT3: Router crashed in CWAN OIR Handler in attempt to lock a semaphore
CSCsc73288	platform-76xx	OSM asic error:SRIC packet data CRC error
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+
CSCse05336	platform-76xx	Packet drop on OSM-2+4GE-WAN+ if sub-if is created or deleted
CSCse26606	platform-76xx	packet drop occur when issuing shut/no shut on other sub-if /w OSPF
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
CSCei76630	PPP	PP:R3:FW2+ATM:MLPPPoA+dLFI: I/O Pool MALLOCFAIL after PORT DOWN/UP
CSCek26657	PPP	Rainier:STD RP showing IPV6-STDBY-4-IDB: state mismatch messages .
CSCek49202	PPP	MLP: interface in invalid state when changing group fails .
CSCin44386	PPP	Multilink interface flaps after a router reload
CSCin86885	PPP	vip crashes due to memory corruption on freeing mlp bundle
CSCsb42241	PPP	VIP crash in ct3sw_rx_interrupt with PA-MC-2T3+ PA
CSCsb97950	PPP	dLFioATM: Packets with CLP set, get punted to RP.
CSCsc33562	PPP	SNMP ifInOctets shows negative value for MLP interface

Identifier	Technology	Description
CSCsc37902	PPP	Standby MSFC may experience bus error after RP_MLP-4-MISCONFIGLINK.
CSCsc45771	PPP	7500 VIP4-80 Crash with Unexpected exception, decode vip_mlp_periodic
CSCsc69804	PPP	SIP1-ChOC3:Initial packets fail with SW-MLP on SIP-200
CSCsd21567	PPP	Distributed counter statistics for UUT is incorrect
CSCsd30719	PPP	A2A: Stdby sup crashes @ mlp_remove_link .
CSCsd35268	PPP	MLP: Bundle line prot down after sh/no sh with min-links config
CSCsd43211	PPP	Rainier: dLFIoLL with oversubscription crashes SIP-200 on HA switchover
CSCsd72854	PPP	ISIS over MLPPP fails after reboot .
CSCse11678	PPP	SIP: Ping fails after removal of primary link from multilink bundle.
CSCse20150	PPP	SIP1-CT3:SW-MLP: all intf are going down w/46 byte pkt size @LR traffic
CSCse91675	PPP	SWMLP: all intf are going down w/46 byte pkt size 8links/bundles@LR trfc
CSCsf10497	PPP	MLPPP bundle across the SPAs are not configurable
CSCsf25712	PPP	Sip-200 CPU1 crash @ blt_pak_holdq_peek
CSCsg02881	PPP	MLP: Bandwidth of down MLP group should be sum of member bandwidths
CSCsg11708	PPP	Receive adjacency & process switching of pkts on mlp if after switchover
CSCsg25664	PPP	dLIFoMLPPPoATM PA: Corrupted PC crash PR
CSCsg35429	PPP	CLI:Spurious Memory access at ppp_ncp_cstate .
CSCsi48550	PPP	dMLP: account lost_frags& rx discards as bundle intf input error
CSCec26696	QoS	RSVP shows wrong allocated bw in show ip rsvp interface
CSCec80902	QoS	Router crashes with Bus Error at 0xFD011147
CSCec85835	QoS	RSVP treats compressed flows as non-conformant
CSCed54330	QoS	WFQ on virtual-template causes allocation error and tracebacks
CSCed79634	QoS	police percent conversions are incorrect in 2nd and 3rd lvl policies
CSCee13430	QoS	Crash observed when reconfiguring channel-group
CSCee36050	QoS	VIP crash when re-use channel group with set service policy
CSCee47275	QoS	card resets due to [no] fair-queue cleanup loops
CSCee56112	QoS	Show Policy interface input/output should not display all.
CSCee66909	QoS	ct3 spa: qos configs should be blocked on multilink member links
CSCee68344	QoS	GE-WAN card crashes in /enqueue/process-policymap_msg/policymap_hash
CSCee69260	QoS	FIFO queueing with QoS service-policy
CSCef21601	QoS	ResvConfirm dropped when non-RSVP hops exist along a calls path
CSCef25953	QoS	dwred statistics are not updated in show policy-map int output
CSCef44588	QoS	Info: Illegal normal burst size seen with default config
CSCef46134	QoS	CPUHOG at CEF MQC IPC Background on SIP-600 on remove/apply qos
CSCef63607	QoS	Crashes seen during boot if ATM WIC is installed & NAT on int config
CSCef66517	QoS	packet drop on flexwan when traffic shaping
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
CSCeg30179	QoS	NRT: crash @ hqflayer_update()
CSCeg33229	QoS	VIP crash when service policy removed from MFR int with traffic
CSCeh31441	QoS	Flexwan module powercycles with shaping+dLFIoATM
CSCeh54083	QoS	random-detect aggregate cmd not working for virtual-template
CSCeh82893	QoS	PP:R3:SIP400:QOS: LLQ+police drop rate counters are broken
CSCeh84740	QoS	VIP crash on RPR+ switchover with qos config and high load traffic
CSCei09171	QoS	PP:R3:SIP-200: %C7600_SIP200_MP-4-PAUSE @ fibidb_handle_delete
CSCei10181	QoS	PP:R3:FW+MLP+MLFR:MALLOCFAIL for LLQ+CBWFQ to hit the LC crash
CSCei16615	QoS	Neighbor 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
CSCei67700	QoS	frde failed to match control packets on fr over ATOM
CSCej09368	QoS	Abnormal queue depth for time and byte based WRED on ETH over ATOM
CSCej77367	QoS	RP crash at hqf_check_vc_layertype during qos testing
CSCek05730	QoS	Bus error crash at mlp_fastswitch_les.
CSCek25851	QoS	Rainier:PWAN2: Router crash @hqf_police_update on attaching qos poli
CSCek29478	QoS	MPLS TE tunnel fails with path option Loose as first hop
CSCek34117	QoS	SIP1+ATM(OC3 SPA): Crashed at hqf_walk_and_police_inline() .
CSCek37011	QoS	Rainier:SIP-200:LC crash @hqf_dp_fifo_cleanup on rem HQoS child pol
CSCek43669	QoS	defaultclass input policy not work for non-queue class for sip1 atm
CSCek44025	QoS	Hierarchy is not collapsed when FRF.12 is configured
CSCek63384	QoS	Service-Policy is Lost When the Multilink Interface is Reset .
CSCin72437	QoS	MQC: Concurrent access crashes the Flexwan during switchover
CSCin86096	QoS	Classification matching on IPv6 acl fails
CSCin96590	QoS	RSP: VIP crash @free_wred_stats on rpr+ s/o w/ traffic w/mlp-qos
CSCin96938	QoS	Spurious access at no_vc_backpressure
CSCsa68661	QoS	LC crashes when service-policy is configured on channelized interface
CSCsa80132	QoS	RSVP reservation across secondary link torn down after 1 minute
CSCsb25607	QoS	dLFIoFR: all lp pkts dropped on oversubscribed mixed traffic
CSCsb32141	QoS	Router reloads when admitting an RSVP flow
CSCsb36818	QoS	Service policies lost on interface bw reconfiguration
CSCsb40118	QoS	Unable to reserve more than 99% of bandwidth
CSCsc00993	QoS	Lower tx-ring-limit for ATM VCs with higher SCR when QoS is enabled
CSCsc35609	QoS	Crash in rvsp tail-end while shutting down egress interface on mid
CSCsc39917	QoS	show policy-map interface shows default bandwidth for class-default
CSCsc43751	QoS	RR & Auth interop issue: test for Integrity obj in bundle msg too strict

Identifier	Technology	Description
CSCsc62327	QoS	Bad RSVP MD5 Authentication Messages when many topology changes
CSCsc90843	QoS	Crash in HQF when deleting service-policy
CSCsc93633	QoS	Software bus error crash on 7206VXR w/12.3(14)T3 w/ NBAR configured
CSCsc95511	QoS	Bus error crash at hqf_scheduler_info_init
CSCsc98510	QoS	Enhanced Flexwan reloads with VRF/MLPPP/QoS
CSCsd09892	QoS	no fair-queue causing VIP crash .
CSCsd17641	QoS	SIP-400 QoS: after changing hier. policy, the policy no longer attaches
CSCsd37025	QoS	CPUHOG and crash when removing nbar policy-map
CSCsd47863	QoS	Refresh are not sent downstream after change in path with RR+policy
CSCsd56696	QoS	A2A: FR Adaptive shaping is not accurate .
CSCsd68445	QoS	Unable to attach the new hierarchical service policy onto the sub-intf .
CSCsd71119	QoS	ALL ATM PVC DOWN IN FLEXWAN WITH PA-A3-OC3 AND OAM
CSCsd71131	QoS	dLFIoLL + QoS : service policy is suspended after clear int mul1
CSCsd76528	QoS	Queues not released after deletion of mch vlan for HQoS policies .
CSCsd95712	QoS	VIP4-80 with local switching and QoS crashing
CSCse02510	QoS	Crash with ALIGN-1-FATAL at hqf_process_wfq_command
CSCse17960	QoS	Address Error crash with tcp retransmit to ATM VC with qos
CSCse22161	QoS	RP pool Memory corruption SXF4 - checkheaps_process/validblock crash
CSCse94388	QoS	SIP200 crash at dlfi_do_fragment on HQF with priority .
CSCsf11353	QoS	Autobahn:FW2 kept crash at hqf_dp_set_blt_quantum and dlfi_inform_config
CSCsf20194	QoS	SIP-200 crashes after OIR when both input and out policy attached to MFR
CSCsf27085	QoS	SIP200 CPU1 crash@hqf_sip1_work_with_callback on removing priorit class
CSCsh46565	QoS	PWAN2 HQoS(LLQ): shape ave rate is not applied .
CSCsh65322	QoS	ATM output packet drops on 7600 with Enhanced FlexWAN and PA-A3-OC3SMI .
CSCsh76895	QoS	Multiple conform and voilet action allowed under single classmap .
CSCsi01422	QoS	Hierarchical Frame-Relay QoS does not work .
CSCsi05251	QoS	bus error crash at get_rateinterval_from_service_policy at subint delete
CSCea46927	Routing	ISIS-NSF: Cautiously refresh neighbor adjacency on RR reception
CSCed06329	Routing	BGP-v6: Version number churns when multipath configured on BGP-v6
CSCed17879	Routing	advertise ipv4 routes across ipv6 BGP peers not working
CSCed23406	Routing	Redistributed routes stuck in RIP database permanently
CSCed84633	Routing	support for intf option in distribute-list under address-family. .
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
CSCee35050	Routing	%OSPF-4-NORTRID not correct with multiple vrfs using same IP
CSCee40207	Routing	Memory leak in BGP Open Process After SSO RP Switchover
CSCee43724	Routing	CsC BGP ipv4+label not consistent with e-bgp next-hop change

Identifier	Technology	Description
CSCee50452	Routing	RRI: static routes removed from config when peer disconnects
CSCef50427	Routing	System crashed when show ip bgp XX.
CSCef59924	Routing	ISIS: rtr. crash at isis_free_next_hop_parent_list
CSCef70161	Routing	vrf peers with same policy fall into different update-group .
CSCef93058	Routing	ARP req was send with delay when each VRF uses same dest IP
CSCef97738	Routing	BGP/MVPN: incorrect update-source is passed from BGP to MVPN
CSCeg03019	Routing	cef not working between different tunnels .
CSCeg13748	Routing	Ping loss to HSRP vip address of a VRF interface on sup720
CSCeg16631	Routing	CSCee32557 breaks RIP distribute-list w/ VRF interface
CSCeg52659	Routing	BGP route may not get withdrawn under rare condition
CSCeg57155	Routing	BGP: network statement prefix is not originated when auto-summary on .
CSCeg58039	Routing	BGP: changing the max-paths value may cause a crash .
CSCeg85719	Routing	IPHC: UDP frames from MWR1900 or RPM-XF may be discarded
CSCeh09588	Routing	300 second traffic loss with 100 OSPF neighbor after SSO switchover
CSCeh31691	Routing	CWAN-MFI: Pos interfaces do not work with PPP encap
CSCeh35659	Routing	4 port gig per-interface ip bgp fast-external-fallover permit .
CSCeh41328	Routing	Multi-topology transition deletes IPv6 routes from RT
CSCeh41598	Routing	Router reload on rip_process_mgd_timers
CSCeh62512	Routing	all ping failed after SSO switchover on all the vrf interfaces
CSCeh66944	Routing	mdt safi with NSF is not working
CSCeh80535	Routing	IPv6 PING packet dropped at 6PE router
CSCeh92012	Routing	OSPF did not redistribute route expectedly
CSCei04409	Routing	Crash in CBTS while using show adjacency int filter command on vip
CSCei04683	Routing	PP:R3:IPv6:Default ISIS Route Generated from L1/L2 to L2 Router
CSCei06089	Routing	Conditional default-originate with route-map does not work in 28S3
CSCei12603	Routing	30ms traffic loss on reoptimization while BW change over TE tunnel
CSCei25214	Routing	router crash @registry fastcase_expection w/ ip cef dist command
CSCei25442	Routing	BGP MVPN - sanitise notification to PIM database
CSCei25454	Routing	BGP: The BGP IPv4 MDT table may receive RD type 2 prefixes
CSCei29944	Routing	RP crashes at bgp_get_msg_count while sho ip bgp summ
CSCei32930	Routing	EBGP+label : soft-reconfig inbound broken
CSCei45669	Routing	OSPF router may fail to flush its self-originated LSA
CSCei53226	Routing	BGP: fix updgrps for non private-as peers with remove-private-as
CSCei58655	Routing	ISIS not aging version of LSP in isis local rib
CSCei59309	Routing	Crash in iprouting_set_ndb_last_rdb()
CSCei60544	Routing	BGP: redistribute connected routes missing from bgp after removing IGP
CSCei62049	Routing	SPD classification removed from fast path

Identifier	Technology	Description
CSCei65252	Routing	IOS forwarding packets for non-routable addresses in the 0.0.0.0/7
CSCei65553	Routing	OSPF must accept LSID with a mix of 0/1s in the host portion
CSCei67996	Routing	Unbalanced load-sharing tsp tunnel when morethan 1 tunnel is applied
CSCei75828	Routing	CPUHOG when 4000 IPv6 VLANs
CSCei83720	Routing	DMVPN:NHRP hold timer refreshed every 5000msec on Spoke router
CSCei93768	Routing	check heaps CHUNKBADMAGIC crash at BGP Router when remove dmzlink ba .
CSCej00946	Routing	mVPN: remote PE tunnel interface wont show up when SSM configed .
CSCej31343	Routing	Active RP crash at fib_upd_record_is_delete when no ip vrf vpn1
CSCej35288	Routing	Null IDB in ipsendnet -process traceback when failover from PRE2A-B
CSCej36831	Routing	VRF-lite/leaking;50% loss to local IP
CSCej42345	Routing	Creating SVI Triggers ARP for the Static NAT IP addresses.
CSCej48262	Routing	The session exceeded MTU counter has NOT incremented correctly for
CSCej76134	Routing	spurious memory access in isis_area_address_match
CSCek24782	Routing	5400XM reloads unexpectedly with stress with AAA holding excess mem
CSCek32139	Routing	SSO : Spurious access at ip_spd_fib_punt_feature_check
CSCek32244	Routing	Not all routes locally generated with auto-summary enabled
CSCek35039	Routing	next-hop isnt matched in the route-map .
CSCek35061	Routing	Disassociate VRF from a MPLS interface crashes the router
CSCek36037	Routing	BGP: Initial keepalive algorithm should be more aggressive
CSCek38025	Routing	MDT interoperability with old image is not working .
CSCek38584	Routing	ISIS IP route is del/add/del when interface shutdown
CSCek39048	Routing	Modular IOS: default distribute-list route-map crash router .
CSCek39701	Routing	ospf adj is not maintained over p2p after swithover
CSCek41338	Routing	CLI: rsp router reloads while configuring under template conf mode
CSCek42585	Routing	BGP Does not establish with Third Party boxes after Link Flap
CSCek45564	Routing	iprouting crash with corrupted block on mpath config change
CSCek47667	Routing	clear bgp ipv6 unicast * does not work .
CSCek47888	Routing	TE LSPs torn down and resigalled after ISIS process restart
CSCek48274	Routing	clear ip bgp soft in may not delete all the BGP prefix
CSCek58880	Routing	RP crashed in ospf_rrr_find_telink/ospf_intfc_command
CSCek62005	Routing	ip prefix list deletes lists before sending notif (causing rtr crash
CSCek62848	Routing	BGP does not notify PIM of RD type 1 mdt safi updates
CSCek65928	Routing	redundancy config-sync failures prc for router isis ipv6 cmd
CSCek69969	Routing	router crash when show ip bgp internal
CSCek76093	Routing	CLNS neighbor is still formed on router after isis protocol disabled
CSCek77849	Routing	bgp aggregate-address results in high BGP Router process utilization
CSCin85894	Routing	Reflexive acl when used as ext. acl gives T/bks & crashes with std.

Identifier	Technology	Description
CSCsa55567	Routing	Crash during show xdr multicast-group (xdr_mcast_display_all)
CSCsa68864	Routing	Loadsharing over 2 equal cost sham-links is not working
CSCsa69518	Routing	MVPN : MDT update is sent with RD 0:0
CSCsa72510	Routing	%COMMON_FIB-DFC1-4-CHAIN_REMOVE_INCONS1 seen on reset of mod 2
CSCsa78050	Routing	Alignment errors in internet_enqueue
CSCsa82134	Routing	router reload when there are over 64 equal cost next-hops for IPv6
CSCsa82564	Routing	MVPN: Repeated Bus Error on 30S1
CSCsa86801	Routing	Traceback messages seen at ipigrp2_route_map_inform.
CSCsa87034	Routing	clear bgp ipv4 unicast command does not clear Routing table
CSCsa87473	Routing	BGP:MPLS/VPN: After reload PE missing prefixes from RR.
CSCsa88766	Routing	PRP crash due to BGP
CSCsa90843	Routing	ARP is not resolved properly
CSCsa91499	Routing	Suprious Access seen from fib_table_flush
CSCsa97101	Routing	FIBNULLIDB in create path due to race condition
CSCsb01157	Routing	CEF Scanner runs when new vaccess interface is created
CSCsb06829	Routing	Loadinfo freed without unregistering dependency if path weight >127
CSCsb08994	Routing	test ip command returns ambiguous command error.
CSCsb09709	Routing	removing bgp with ipv6 address family causes crash (watchdog timeout)
CSCsb09852	Routing	BGP: pathless nets not freed when updgrp members are out of sync
CSCsb12089	Routing	CEF: RF proceeds to standby hot before standby is fully synced
CSCsb12896	Routing	SSO:routes in a vrf is not synced in CEF between active and standby
CSCsb24535	Routing	clear ip bgp update-group [ip address] clears all the bgp peers
CSCsb28300	Routing	Standby stuck in stanby cold bulk after loadversion
CSCsb36755	Routing	BGP does not delete multi-path route when receiving worse metric UPDATE
CSCsb40115	Routing	BGP: Failed to find expected # of multipath entries
CSCsb44220	Routing	ipfast needs to retry opening the ipc port in the background
CSCsb47281	Routing	Stdby stuck in cold bulk after LV
CSCsb50606	Routing	Leak in dead process due to TCBs from BGP active connections
CSCsb54823	Routing	BGP: prefixes temp advertised despite prefix-list ORF .
CSCsb63652	Routing	bgp aggregate-address results in high BGP Router process utilization .
CSCsb64858	Routing	reset during icmp redirect packet generation/determination
CSCsb66121	Routing	MPLS TE tunnel: export netflow pak wth IP TTL=0
CSCsb75669	Routing	BGP: restore next-hop-self command for eBGP peers
CSCsb77733	Routing	Failed to ping the IPv6 loopback interface due to IPv6-CEF-Drop
CSCsb79895	Routing	RIP protocol with MD5 authentication fails
CSCsb83521	Routing	%SCHED-3-STUCKMTMR - Process= IPC LC Port Opener after SSO
CSCsb86987	Routing	Traceback from bgp_ipv4_mcast_lookup() after reload

Identifier	Technology	Description
CSCsb89043	Routing	%ALIGN-3-SPURIOUS access made at adj_ios_update_fixup_and_macstr.
CSCsb89900	Routing	ISIS: tracebacks %SYS-3-MGDTIMER: Parent is a leaf, set_exptime_internal
CSCsb92705	Routing	password command not displayed in show bgp template peer-session command
CSCsb96034	Routing	Traffic down for too long after SSO switchover .
CSCsc00378	Routing	export map is not taking affect dynamically when PE-CE runs ospf
CSCsc16611	Routing	7304 router crashes due to watchdog timeout
CSCsc30197	Routing	Router crashes at Config command router isis with traceback
CSCsc37212	Routing	ISIS: Redistributed routes might not be advertised if interface flaps
CSCsc41457	Routing	NHRP: Registration cache entries do not override no-socket mappings
CSCsc41694	Routing	router hangs while unconfiguring the CLI no router bgp <No>
CSCsc43989	Routing	CEF adjacency inconsistent with NHRP cache entry
CSCsc49231	Routing	Traceback seen with SYS-3-MGDTIMER Running timer, init, NHRP
CSCsc59027	Routing	mem leak in CEF IPC Background process
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
CSCsc72090	Routing	EIGRP doesn't honor interface IP MTU when sending packets
CSCsc74229	Routing	VPN routes get deleted from the BGP table though counter shows otherwise
CSCsc75426	Routing	Crash when BGP sends update with bad attribute .
CSCsc76327	Routing	EIGRP PE-CE: Constant route-flap with a redistributed VRF-static-route
CSCsc83742	Routing	BGP MAXPFX Sylog message does not include VRF tableid info
CSCsc83821	Routing	ISIS: TLV 237 not found in database when isis metric is configured
CSCsc98835	Routing	CPUHOG when access-list is modified causes OSPF and BGP session drops .
CSCsd00028	Routing	OSPF: spurious access in ospf_generate_trap
CSCsd03021	Routing	360K internal routes will produce CPUHOG messages and tracebacks .
CSCsd04128	Routing	Packets drop after reloading master switch and getting back to a stack
CSCsd04810	Routing	Route pointing towards an interface where IP is not enabled but ISIS is.
CSCsd11019	Routing	Rainier:After RPR-Plus switchover standby RP crashes
CSCsd12046	Routing	Receiving foreign packets from the network
CSCsd15749	Routing	SoO-tagged prefixes sent when SoO configured on peer group .
CSCsd28214	Routing	RIP watchdog timeout crash on flapping links
CSCsd32373	Routing	BGP does not flag multipath correctly, causing loadbalancing issues .
CSCsd33445	Routing	SYS-3-MGDTIMER: Running timer message for NHRP
CSCsd41237	Routing	vrf import map is not working .
CSCsd50101	Routing	NRT: Intermittent crashes going to issu loadversion
CSCsd51309	Routing	SUP720 crashes every time after disabling auto-tunnel mesh feature
CSCsd52225	Routing	BGP soft-reconfiguration keeps the old next-hop
CSCsd53402	Routing	ABR deletes OSPF summary route for 5sec after DR is changed

Identifier	Technology	Description
CSCsd59023	Routing	RP Arping for adjacent next-hop bringing up PTA sessions with AAA .
CSCsd60687	Routing	T/B untyped_dqueue_match_its seen during RPR switchover
CSCsd63038	Routing	MVPN: BGP session for IPv4 MDT between any two PEs never comes up
CSCsd64173	Routing	Bus error crash IPV6 due to OSPF summary prefix command
CSCsd66372	Routing	BGP: router crashes at bgp_scan_walker
CSCsd67591	Routing	OSPF: crash while modifying route-map .
CSCsd67768	Routing	1200 BGP peer sessions with 10/30 keepalive/holdtime values flap often.
CSCsd72747	Routing	nssa summary to null0 disappears after 'clear ip ro *'
CSCsd73245	Routing	IPRT-3-PATHIDX: Bad path pointer of 0 message is reported.
CSCsd74189	Routing	show ip bgp vpnv4 vrf NAME community-list NAME gives error mesg.
CSCsd74396	Routing	eigrp authenticaion fails with md5 enabled
CSCsd75574	Routing	VIP crashed with IOBUS Error Interrupt Status register 0x4
CSCsd76419	Routing	IPv6 ND and CEF do not match
CSCsd76832	Routing	NRT: Output interface not available with ip_route_and_transmit traceback
CSCsd81600	Routing	OSPF Stub-links should advertise LSInfinity when max-metric configured
CSCsd82809	Routing	Can't add a static ipv6 route on an interface with ipv6 unnumbered
CSCsd84489	Routing	Crash in ospf_add_all_stub_routes on topology change
CSCsd88685	Routing	ISIS overload-bit on startup does not work with RPR+/SSO fail-over
CSCsd89569	Routing	sh ip int brief output - Any interface listed with OK? msg
CSCsd94133	Routing	sh ip cef exact route for vrf and 6PE ipv6 shows no oce
CSCsd98686	Routing	%XDR-6-CLIENTISSUBADTXTFM: Failed to xmit_transform message .
CSCsd98763	Routing	MRAI between PE and CE defaults to 30 seconds
CSCsd99760	Routing	After iprouting.iosproc Process Restart Routing table not updated
CSCse04220	Routing	Clearing IPv6 BGP sessions can cause crash .
CSCse05031	Routing	BGP conditional default-originate with route-map doesnot work correctly
CSCse07118	Routing	OSPF: crash while using the transmit-interface command .
CSCse10102	Routing	BGP Update-group: inconsistent error mesg. when EIGRP is PE-CE
CSCse10683	Routing	BGP Route-refresh double-counted
CSCse18445	Routing	BGP4-MIB should not send trap for IPv6 BGP peer.
CSCse19783	Routing	ip cef load-sharing configuration can't be removed
CSCse26515	Routing	DR does not flood back LSA on receipt of LSA from DROTHER router
CSCse26682	Routing	Ping failure with isatap configuration
CSCse26921	Routing	BGP route is not updated with newly configured route-target
CSCse26941	Routing	Bus error configuring cef table output-chain build favor convergence-spe
CSCse29589	Routing	c18xx tracebacks when trying to send NHRP registration
CSCse30000	Routing	ATT-bit control for dual-homed L1 ISIS
CSCse34050	Routing	ISIS keep advertizing passive interface, even after doing shutdown

Identifier	Technology	Description
CSCse40346	Routing	NRT:Router Crashed with tracebacks while testing isis_ldp
CSCse41174	Routing	NRT: GSR router crashed at ospf_send_one_paced_update during l2tun test
CSCse41484	Routing	DMVPN / VPN-SPA / few GRE packets not encrypted when negotiating the SAs
CSCse44052	Routing	Crash when config IPv6 interface distribute list
CSCse49697	Routing	can not disable bgp nexthop trigger tracking NHAT
CSCse51804	Routing	DMVPN tunnels not stable; keeps flapping
CSCse54241	Routing	ISIS - LSP purge not sent for DIS removal
CSCse57232	Routing	Display lsa throttle timer in sh ip ospf by default
CSCse61025	Routing	ip http auth aaa is not needed for Authproxy to work
CSCse64565	Routing	OSPF passive-interface default pb when converting switchport to L3
CSCse66181	Routing	BGP PMTUD cannot be turned off for peer group
CSCse67487	Routing	Autobhan76: Router Crashed in the unconfig section.
CSCse69162	Routing	Multi-topology ISIS breaks CLNS routing
CSCse72792	Routing	OSPF: neighbor cmd rejected if VL configured
CSCse74643	Routing	ISIS metric maximum is missing under sub-interface
CSCse77758	Routing	No IPv6 unicast-routing command disables ipv6 cef .
CSCse78454	Routing	ipv6 ospfv3 cfg lost from interface on restart iprouting.iosproc .
CSCse82584	Routing	OSPF does not remove MAXAGE LSAs
CSCse85383	Routing	OSPFv3: Restructure link-state request list (CSCsd03021)
CSCse86806	Routing	'clear ip bgp soft out' failed to send default-originate
CSCse87859	Routing	no service udp-small-server does not block IPv6 udp port 7 (echo)
CSCse89119	Routing	OSPF discard route (Null0) is disappeared from RIB when AD is changed
CSCse90843	Routing	Fib entries not freed - remain in deleted state
CSCse91962	Routing	prefix stays in BGP table with RD 0:0 even after vrf's RD is configured
CSCse97513	Routing	BGP session to a Third Party router does not come up after reload
CSCsf00171	Routing	summary route not flushed from ospf database
CSCsf02935	Routing	Router Crash due to Ospf Sham link and BGP redistribution
CSCsf05579	Routing	ISIS passive-interface default problem in IOS 12.2(18)SXF
CSCsf11980	Routing	NHRP: Crash w/ OSPF, DMVPN @ max_proto_mtu nhrp_send_resolution_request
CSCsf15429	Routing	7304 Router Crash @ fr_bq_proc continuous loop FR Broadcast Output
CSCsf20947	Routing	BGP 'neighbor default-originate' advertisement ignored after link flap.
CSCsf26043	Routing	Cat6k Selective Packet Discard not classify ISIS at high-priority
CSCsf32449	Routing	Sup720 MVPN PE - Tunnel does not come back up after reload .
CSCsf99057	Routing	JQL: OSPF Stub-router should work with SSO/RPR-Plus if NSF is disabled
CSCsg02387	Routing	Timeout response with SNMP over IPV6 phase II
CSCsg03483	Routing	FIB-4-FIBCBK: Missing cef table for tableid 1 during route update XDR e
CSCsg07742	Routing	ip vrf sitemap soo requires bounce when removing/re-adding

Identifier	Technology	Description
CSCsg14026	Routing	Routers/Switches forward traffic destined to Class E Addresses
CSCsg16748	Routing	ABR deletes OSPF type 3 LSA after it received max-aged type 2 LSA
CSCsg17977	Routing	Non-master CPU is suspended for too long @ mtrie_leaf_insert
CSCsg21418	Routing	Bus error related to CLNS fast switching
CSCsg26492	Routing	Error: can not find acl. Abort - msg when removing permit entry in ACL .
CSCsg28497	Routing	MT isis adj flaps during GSR RP FO causing prolonged traffic loss
CSCsg29248	Routing	OSPF: summary-address cmd can create stale LSA .
CSCsg29498	Routing	adj trace stores pointer not value = Segmentation Fault
CSCsg33571	Routing	Add prefix option under router xxx vrf process distribute-list options
CSCsg34030	Routing	show bgp ipv6 unicast longer-prefixes not showing expected output
CSCsg40507	Routing	SIERRA:ISIS/BFD session doesnt come up after changing ip-addr of interf
CSCsg42246	Routing	CPUHOG in IP Background, and router reload .
CSCsg42488	Routing	Juniper - Cisco PE incorrect extended community for OSPF
CSCsg43140	Routing	Switch may crash due to bgp over vpn .
CSCsg45637	Routing	Traceback occurs while accessing bgp_vpnv4_lookup_prefix .
CSCsg46366	Routing	OSPF NSSA LSA forwarding address set even when P bit will be clear.
CSCsg46638	Routing	BGP does not send withdraw when distribute-list is configured
CSCsg49166	Routing	EIGRP fails to converge with 1100 neighbors on FR point to point PVCs
CSCsg52336	Routing	Crash at ospf_flush_area_summary_lsa after 'no ip vrf' of unassigned vrf
CSCsg52887	Routing	SegV at ctunnel_oqueue when 'no ctunnel destination' on one side
CSCsg55209	Routing	BGP paths increase, with same prefix and next-hop under soft-reconfig .
CSCsg55591	Routing	MPLS VPN Local label not allocated/programmed for sourced BGP network
CSCsg59699	Routing	OSPFv3 autocost gives interfaces the wrong cost sometimes .
CSCsg65298	Routing	OSPF: connected network learnt via ospf after interface shutdown #2
CSCsg65625	Routing	flo_isp: Assertion failed: fib_instance_can_be_used
CSCsg66635	Routing	TE metric becomes invalid after reboot .
CSCsg71797	Routing	bgp bestpath as-path multipath-relax - command crashes Supervisor card
CSCsg74898	Routing	IPHC: Juniper interop: Timestamp on the RTP Packet not to update
CSCsg78246	Routing	ISIS Wide redistribution metric shows incorrectly on local table
CSCsg83723	Routing	%COMMON_FIB-3-DEPENDENCY_WALK: error message seen
CSCsg84690	Routing	ospf: default route with a bad mask may not get installed .
CSCsg85846	Routing	PE does not flush VPN Summary LSAs when redistrib is cleared
CSCsg95101	Routing	ALIGN-3-SPURIOUS: Spurious memory access
CSCsh02161	Routing	BGP vpnv4 route reflector not withdrawn redistributing prefix .
CSCsh11482	Routing	incorrect link-local next-hop for prefixes from update-group 'leader'
CSCsh13291	Routing	Traceback@xdr_rp_disable_slot due to XDR keepalive timeout
CSCsh13542	Routing	LOOPPAK detected for UDP ECHO Back packets

Identifier	Technology	Description
CSCsh14457	Routing	SIERRA: supw crashes @ ospf_nbr_find_retrans_block with OSPF/BFD
CSCsh15066	Routing	VRF has 2 ospf process, when one process is removed the router crashed
CSCsh15489	Routing	OSM-1CHOC12 FR tcp header-compression needs reload to take effect
CSCsh19852	Routing	ospfv3: stale network LSA after DR interface goes down ; also v2 problem
CSCsh20140	Routing	OSPF: ispf traceback in chunk_destroy .
CSCsh23176	Routing	Router crashes @ rip_timer_process .
CSCsh27931	Routing	Switch crash when tunnels are shut
CSCsh38228	Routing	uRPF w/exception ACL not logging deny log ACEs in interrupt path
CSCsh41234	Routing	Standby router keeps reloading with SRA image
CSCsh42565	Routing	TE tunnel does not come up on ospf non-broadcast network type .
CSCsh51559	Routing	Spurious access made at bgp_vpn_afmodify_walker
CSCsh53926	Routing	Bus error crash at add_path - ispf .
CSCsh55768	Routing	Catalyst 3550 SVI packet buffers leaked .
CSCsh57652	Routing	RIP accepts update before hold down timer expires.
CSCsh57795	Routing	Removing 1 RIP neighbor removes all neighbors
CSCsh59495	Routing	BGP non-exist-map statement incorrectly stored as exist-map.
CSCsh61119	Routing	High CPU due to ARP refresh triggered by Serial interface flap
CSCsh63785	Routing	NRT:MPLS-TE tunnel down after switchover
CSCsh66406	Routing	BGP VPN4 has stale routes after executing maximum routes 50 80 in vrf .
CSCsh67160	Routing	CEF consistency checkers go offline after sso switchover
CSCsh67709	Routing	BGP: 'redistribute connected' triggered only by shut/no shut local intf
CSCsh68376	Routing	Routes learned from CBB route reflector didn't get refreshed .
CSCsh80008	Routing	BGP: soft reconfiguration inbound and neighbor weight has no effect
CSCsh81289	Routing	DFC earl adj vlan incorrect, sceompls vcs disposition fails after bootup
CSCsh87119	Routing	Suppress OSPF-6-ZERO_BANDWIDTH, when interface is down
CSCsh92854	Routing	output bytes not incrementing correctly in 122.SB3.
CSCsi03434	Routing	Memory leak @ ospf_redist_work_enqueue
CSCsi06948	Routing	Bus error when issuing BGP dampening related commands .
CSCsi11438	Routing	OSPF does not remove maxage LSAs and age goes to bigger than 16 bit
CSCsi14346	Routing	EIGRP: neighbor command missing in VRF.
CSCsi23719	Routing	'no isis protocol shutdown' on a sub-interface enables 'clns routing'
CSCsi35541	Routing	CPUHOG and T/B seen after clearing ospf routes
CSCsi41944	Routing	Virtual Exec CPUHOG
CSCsi45422	Routing	iprouting.iosproc process reloads when making changes to static routes
CSCsi49948	Routing	MDT prefixes are not installed and sent out on iprouting restart .
CSCsi57971	Routing	ISIS does not advertise prefix of passive interface
CSCsi58867	Routing	CPUHOG After show ip route static or show ip route connected

Identifier	Technology	Description
CSCsi60103	Routing	IPv6 OIR PA Name Clash enhancements
CSCsi60240	Routing	prefix-list change not processed for redistribute route-map correctly.
CSCsi62559	Routing	SPD classifies OSPF IP Precedence 0 as priority .
CSCsi65922	Routing	Cannot unshut BGP neighbor once it is shutdown
CSCsi68819	Routing	Prefixes are moved to non-fwd tree after delete when RPR is configured
CSCsi68882	Routing	Crash@ network_redist after executing no router eigrp . .
CSCsi86386	Routing	clear ip bgp * soft in does not work for inbound route-map for ip4 label
CSCuk49694	Routing	6PE: Ignoring label update from peer
CSCuk52253	Routing	IPv6 static route missing tag argument
CSCuk54191	Routing	MP-iBGP routes not installed in VRF RIB
CSCuk54781	Routing	ICMPv6 Packet too big does not account for label stack
CSCuk55579	Routing	CEFv6 inconsistencies found after a HA Switchover
CSCuk58462	Routing	Routes are not filtered even when route-map rule sets deny the rule
CSCuk58481	Routing	Crash in fib_path_list_ifnums_compare()
CSCuk60585	Routing	ISO-IGRP: Crash may occur when nv-gening redistribution into iso-igr
CSCuk60910	Routing	IPHC:invalid TCP header may cause memory corruption & reload
CSCdu83050	Security	ssh needs source-address
CSCdz34708	Security	GRE : tunnel path-mtu-discovery doesnt copy DF bit to GRE+IP header
CSCed68627	Security	Dynamic spoke to spoke tunnel fails to come up with dual-DMVPN
CSCed73942	Security	IDBs for tunnel interfaces are not reused
CSCei70222	Security	VAM2+: epa_get_blk_buffer FAILED after overnight stress test
CSCei85164	Security	OCSP fails when timezone is configured
CSCej43220	Security	7200 Dynamic VTI tunnels take 10 seconds to come up
CSCek30711	Security	te-mib caseMIB_TE_cli_get_set_get fail due to CLI return nullset
CSCek30748	Security	Router reloads when config tunnel protection ipsec profile vpnprof
CSCek56735	Security	IPV6IP tunnel with VRF does not switch data packets. .
CSCek73041	Security	SSH:Connection closed message not seen after the retry prompts
CSCin48676	Security	Quatro:SSH V2:Switch reloads @ checkSurrender due to V2 session
CSCsb47257	Security	bus error crash @ pki_add_to_obj_list
CSCsb54378	Security	watchdog timeout crash when starting ssh session from the router .
CSCsb62045	Security	scp connection fails with error: unexpected filename:
CSCsb74409	Security	IOS ssh client blocks Virtual Exec / SSH Process
CSCsc23816	Security	clear crpto sa peer A.B.C.D command does not reset the tunnel
CSCsc30451	Security	Some VTI interfaces remain down despite ike & ipsec sa created
CSCsc72722	Security	CBAC - firewall resets TCP idle timer upon receiving invalid TCP packets
CSCsd00341	Security	GRE tunnel CEF switches via invaild adj when sequence-datagrams configd
CSCsd30932	Security	CLI: router reload on bad refcount error during CA trust point config

Identifier	Technology	Description
CSCsd38247	Security	CLI: default keepalive command causes router crash .
CSCsd76601	Security	Resuming SSH Session Fails After Other Session Has Been Disconnected .
CSCsd77758	Security	packet loss from tag2ip with double GRE encapsulation using tunnel vrf
CSCsd80510	Security	Default tunnel bandwidth and delay are not reasonable values. step 1
CSCsd92405	Security	router crashed by repeated SSL connection with malformed finished messag
CSCse03277	Security	VTI: VTI tunnel does not come up after remove/add tunnel configuration
CSCse11457	Security	show crypto ca timers shows static output
CSCse12154	Security	Bus error crash after executing secure copy (scp)
CSCse22153	Security	Rainier:%COMMON_FIB-STDBY-2-IF_NUMBER_ILLEGAL message on stby. .
CSCse29545	Security	Crypto pki trustpoint loses ip-address command upon reload
CSCse40423	Security	With ATM, tunnel interfaces do not ping until a shut-noshut is done .
CSCse62462	Security	MFI - VRF Tunnel packet is sent unlabeled
CSCse69736	Security	Update tunnel default bandwidth and delay
CSCse79611	Security	SSH source-interface command not working
CSCse93597	Security	RSA keys not replicated via SSO redundancy to standby
CSCsf25722	Security	software forced reload after executing secure copy (scp)
CSCsf30150	Security	GRE: Tunnel interface should go down when tunnel source interface up/dwn
CSCsf96592	Security	midchain loop restart requires input_if swap and all-encap bytecount
CSCsg10671	Security	No message when CA re-enrollment fails
CSCsg47462	Security	Address error crash at tunnel_ep_addr_compare
CSCsg62226	Security	IPSEC: crash@ ace_reverse_map while checking the traffic flow with ipsec
CSCsh25172	Security	scp can't be used to copy large files
CSCsh26382	Security	Ipssec SAs getting deleted for AH+ESP Transform set
CSCsh41459	Security	The router crashes, when removing/adding VRFs
CSCsh56320	Security	Memory Leak when executing sh crypto ipsec or sh crypto session
CSCsh66935	Security	Crash in avl_get_next_threaded on deconfiging 100 tunnels/vrfs
CSCsh75224	Security	RP crashes due to stack overflow with ssh
CSCsi21930	Security	mplsTunnelPerfHCPackets value mismatch CLI ouput
CSCdx54940	Unknown	CPU utilization in 3660 is 98% with aal2 calls
CSCea16744	Unknown	GBIC optical 7500 router crash on attach queueing output policy
CSCea24341	Unknown	SLB real to real ICMP traffic broken with FWLB
CSCeb77318	Unknown	IOS SLB: Incorrect checksum of forwarded icmp unreachable
CSCed15183	Unknown	Verify ATA is supported but msg says it is not
CSCed26241	Unknown	BootP Requests Modified in 12.2(15)BC1
CSCed94829	Unknown	IOS reloads due to malformed IKE messages
CSCee66208	Unknown	Not able to remove port config using no port under DFP
CSCee79634	Unknown	Avert: IP phone is not statically authenticated on 831 using CDP

Identifier	Technology	Description
CSCee84918	Unknown	DHCP snooping on 3550 drops DHCPNAKs recieved when renewing old IP
CSCef82820	Unknown	Loadbalancing with >= 3 links in AToM cause VC to be down or crash
CSCeg02918	Unknown	Bus Error at auth_proxy_proc_profile
CSCeg41161	Unknown	Implementation of RM aging feature for EARL7 systems
CSCeg76039	Unknown	Show archive log config: conf terminal, exit, ctrl+z logged
CSCeh06200	Unknown	No HTTP access via TACACS if idle time configured on TACACS server
CSCeh12640	Unknown	show diag # performs show diagbus # instead of amb. command msg
CSCeh21210	Unknown	MF: DHCP Snooping crash when server send invalid option 82
CSCeh35237	Unknown	7600: 6748GE LC OIR causes spurious mem access and traceback
CSCeh42348	Unknown	PP:CWAN-QOS:DWRED is broken
CSCeh42472	Unknown	Standby RSP doesnt boot because of image uncompression failures
CSCeh51550	Unknown	SCP Health:LCs not responding to SCP keepalives after rpr+ for long
CSCeh56402	Unknown	Shutting peer FR link crashes router
CSCeh63002	Unknown	id_alloc_util_free should check for already freed ids
CSCeh78028	Unknown	7600 Port-Sec: traffic fails to recover after reload
CSCeh78345	Unknown	Ensure EEM policies close tty session properly upon exit.
CSCei00856	Unknown	CWAN-QOS:oc-3:col2 crash with external memory address
CSCei08288	Unknown	show run misses no errdisable detect cause udd command
CSCei09247	Unknown	Local serial link goes up/down when remote link is admin down
CSCei27448	Unknown	Router crashes while displaying sh ip pim mdt bgp
CSCei37672	Unknown	chevys/c2lc take ~ 180s before resetting following a mandatory proc exit
CSCei38036	Unknown	layer 2 entry not removed when no int vlan
CSCei41088	Unknown	MVPN Tunnel interface not created with BGP Confederation
CSCei46182	Unknown	c6msfc2a/sup32 DEC MOP packet internally looping
CSCei48635	Unknown	ChOC3/STM-1 SPA: many MFR interfaces remain down following microcode
CSCei51175	Unknown	PP:R3:SIP-200:1490 bridging - CPU1 crash with egress pol on main int
CSCei52830	Unknown	Banner command sync is broken by CSCin86483 .
CSCei55605	Unknown	Getting Traceback on the router while scheduling Kron
CSCei58681	Unknown	port channel does not form after minlinks added and removed
CSCei59601	Unknown	router crashes at ac_switching_validate_fibidb
CSCei68902	Unknown	Maverick: MFR interfaces could be down after SPA/router reload
CSCei72033	Unknown	1xcSTM-1 SPA goes OOS upon adding 12 serial links to MFR bundle
CSCei73829	Unknown	Phase 2 Rekeying with VPN Client results in volume lifetime of 0
CSCei74749	Unknown	port is suspended on the standby due to flowcontrol parameters
CSCei79969	Unknown	Traceback at issu_rcv_transform found on PE after VPN SSO
CSCei80699	Unknown	multicast tunnel if_number numbers being duplicated
CSCei86192	Unknown	PP:R3:FlexWAN+PA-8xT1/E1: RP crashed MALLOCFail due to loveletter

Identifier	Technology	Description
CSCei86256	Unknown	Crash when typing show lacp neighbors
CSCei86313	Unknown	PP:R3:FW+8xT1/E1:Stuck in LOS state after card type E1 provisioned
CSCei90238	Unknown	Rainier:SIP-200: %C7600_SIP200_MP-4-PAUSE @tal_tree_item_delete
CSCei92291	Unknown	Message on reload:Error in setting Reload Reason
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
CSCej02181	Unknown	SLB: cannot configure weight 0
CSCej08637	Unknown	Inline power sensors needed on standby to support entity mib SSO.
CSCej13660	Unknown	mem leak from MallocLite allocated by crypto_kmi_add_data_to_pyld
CSCej16004	Unknown	ML MTU cfg from CLI does not change the MTU operation
CSCej21515	Unknown	ATM SPA DLL tuning may miss valid lock points
CSCej21520	Unknown	ATM SPA: Removing APS on Protect interface causes locked console
CSCej27397	Unknown	CT3 SPA: add firmware support to allow host to set overflow threshol
CSCej37803	Unknown	cT3 SPA:Upgrade to IOFPGA rev2.1
CSCej63166	Unknown	%LSD-4-LABEL_RESOURCE: label range is not freed
CSCej70453	Unknown	Unable to control application: OER Route Map Failure
CSCej83531	Unknown	isakmp sa is not up in change_hostname_ip
CSCej86188	Unknown	MLS packet error syslogs should be configurable and no service int
CSCek03772	Unknown	zamboni: crashes for double fragmentaion
CSCek22536	Unknown	SLB high cpu with second VIP inservice and user->real traffic
CSCek22595	Unknown	SLB vserver access commands break user->real traffic
CSCek22782	Unknown	CSM: Configuration sync check does not work in all cases
CSCek24053	Unknown	Sup720_rp: spurious memory accesses in cardifmib_get_card_index
CSCek25660	Unknown	tarceback found at l2_modify_one_entry(0x207b9614)+0x48 .
CSCek26158	Unknown	IOS TCL leaks memory when EEM policy triggered.
CSCek26296	Unknown	PR+:p-map with a single band+shape class doesnot guarantee bandwidth .
CSCek26742	Unknown	Rainier:SPA-8XCHT1/E1: All T1/E1s in DOWN after RPR+ switchover
CSCek28110	Unknown	TB @ xdr_lc_check_sequence %XDR-SP-3-XDROOS rcvd after multipile SSO
CSCek28561	Unknown	SIP1/ChOC3: T1/E1 BERT unusable after first run
CSCek30152	Unknown	Error in calculation subrate bandwidth for Kentrox mode .
CSCek31059	Unknown	mvpn:duplicate pkts are seen while crossing multiple PEs
CSCek31610	Unknown	IOS changes to support sticky replication in CSM
CSCek31960	Unknown	ping failed when core configured with GRE tunnel
CSCek32555	Unknown	MFR i/f lineprotocol takes too long to come up after RPR+ switch
CSCek35321	Unknown	ifStackTable has 2 lower layers for 4chstm1 e1 ds1 layer
CSCek35767	Unknown	Need show mls statistics protocol equivalent in IOS
CSCek35770	Unknown	Need show module power equivalent in IOS

Identifier	Technology	Description
CSCek35773	Unknown	Need show mls multicast router equivalent options in IOS
CSCek35951	Unknown	Priority queue with policing configured doesnt work
CSCek36014	Unknown	Need show version epld equivalent in IOS
CSCek37181	Unknown	Loopback on controller for online diagn of wism card
CSCek37494	Unknown	mls acl tcam share-global should not be NVGENed
CSCek37963	Unknown	1st level WRED faild with Policer in 1st & 2nd level .
CSCek39186	Unknown	MAC-address for HSRPs VIP not in FVRF vlan if tunnel redirected .
CSCek39392	Unknown	Crash @ registry_add_list when loading IOU/unix-p-ms image
CSCek42027	Unknown	SPA FPD upgrade fails with sip1-CR
CSCek43497	Unknown	IBM/JDSU type SFP not work with latest rainier image
CSCek44502	Unknown	6vpe:QoS classify counter not working .
CSCek45036	Unknown	Interuppt throttling to be implemented for Sibyte Modular IOS images.
CSCek45862	Unknown	set mpls exp impositon not working with 6PE IPv6 traffic on SIP-200
CSCek47083	Unknown	B2B:ad erros on active blade when both blades are reloaded .
CSCek47205	Unknown	B2B:PKI:Crash at bitlist_validbit
CSCek47574	Unknown	SIP 400 drop mpls packets and cause traceroute fails
CSCek48252	Unknown	RRI current peer not set specifically in case of QM retrans fail
CSCek50172	Unknown	%SYS-3-TIMERNEG: Cannot start timer with negative set
CSCek50720	Unknown	Improve error handling for DLL centering algorithm
CSCek53756	Unknown	%SYS-3-INTPRINT: Illegal printing attempt from interrupt level on LC
CSCek54572	Unknown	crash at ace_create_cm_head_node .
CSCek54959	Unknown	%MFI-3-REDISTMGR %LFD-3-BADEXEC %LFD-3-SM upon SSO Switchover
CSCek55639	Unknown	Failed to assert Physical Port Administrative State Down alarm
CSCek55870	Unknown	fabric buffer-reserve queue default issues
CSCek57760	Unknown	IP MTU of GRE tunnel not used by SPA-IPSEC
CSCek58678	Unknown	%SYS-3-INTPRINT: Illegal printing attempt from interrupt level on LC
CSCek60775	Unknown	Router crashed at ace_clear_local_address after change to VIP addres .
CSCek61974	Unknown	Minimum configurable rx timers should be greater than 1
CSCek63611	Unknown	rekey fails after crypto card is rebooted .
CSCek65022	Unknown	7600-SSC-400: SPA-IPSEC-2g EFC clock hardware issue .
CSCek65087	Unknown	Traceback see at unqueue while running cef_tunnel_vrf script
CSCek66277	Unknown	Diagnostics test 18 TestAclDeny should be marked Disruptive .
CSCek66294	Unknown	TCP adjust mss on egress direction
CSCek66590	Unknown	C7600-SSC-400: Crash in show hw-m subslot x status volt
CSCek66842	Unknown	12.2SRB: OER netflow enabling broken .
CSCek66877	Unknown	%XDR_SP-STDBY-6-CLIENTISSU_BLOCKED: XDR client lte broker cannotSync
CSCek67100	Unknown	Cheronia: Crashinfo write fails

Identifier	Technology	Description
CSCek67622	Unknown	BFD should not be configurable on etherchannel intf
CSCek67701	Unknown	SPA-IPSEC-2G: Crashdump not getting saved on NMI .
CSCek68108	Unknown	Router crashed at ace_policyloader_util.c after remove crypto map .
CSCek68218	Unknown	sip-600 crashing with diagnostics error online_wan_diag_rp_request
CSCek68265	Unknown	Major alarm on active caused syst. shutdown instead of swover to stdby
CSCek68281	Unknown	Syslog instead of crashing on correctable FIB SSRAM ECC errors
CSCek68800	Unknown	mls error action freeze default to change from freeze to reset
CSCek68890	Unknown	After reload 2 Zamboni, routing adj not come up over some tunnels .
CSCek70014	Unknown	Need a way to clear diagnostic event log
CSCek72777	Unknown	%CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR for 7600 SIP card .
CSCek73332	Unknown	Bidir shadow entry is missing some interfaces in oif
CSCek74858	Unknown	glbp weighting track config sync failure
CSCek75768	Unknown	Ensure EEM policies are registered correctly through ssh.
CSCek78219	Unknown	SIERRA: Active Sierra Stnby Boomerang -- stdby crashes in IPC on bootup
CSCin78110	Unknown	Some E1 controller does not come up if a large config on other LC
CSCin89551	Unknown	VIP crash at dmfr_fastsend when pumping traffic via dMFR bundles.
CSCin97815	Unknown	FRF.16 - blt counters not updated to RP after reload of router
CSCin97912	Unknown	FESPA-SIP1:After LC reset, Intf comes as up-up even if peer is down
CSCin98448	Unknown	controller shut throws up error msg and remote end is not going down
CSCir01217	Unknown	name_svr.proc[64]: Could not register interest
CSCsa54688	Unknown	%IDBINDEX_SYNC-3-UNKNOWN_TYPE: IDB type is unknown after switchover
CSCsa56229	Unknown	Traceback mesg seen when standby SUP comes online on Port security
CSCsa57524	Unknown	Incorrect SPA GE-WAN main interface IF-MIB Counter Support
CSCsa58703	Unknown	Not all ATM ACs indicated up via show mpls l2tr sum using PW redundancy
CSCsa61687	Unknown	c12000 crashes by issuing show sss cmd.
CSCsa66683	Unknown	Enhance bridged flow stats to support l2 vlans
CSCsa71295	Unknown	show mod indicates Unknown diag status for SIP cards after switchover
CSCsa75094	Unknown	po based eompls pkst not hitting eom adj until po shut/unshut
CSCsa76016	Unknown	NAT netflow entyr created without reason
CSCsa76801	Unknown	Major bootup failure on Sup720 causing other linecards to PwrDown
CSCsa77785	Unknown	Router crashes when L2 redirection is configured with HTTP traffic
CSCsa79561	Unknown	Any type 6 key with arbit length crashes the router
CSCsa79630	Unknown	Cat6500 Netflow does not export all flows
CSCsa80358	Unknown	Connectivity lost on native vlan on etherchannel trunk betn 2 cat6ks
CSCsa80620	Unknown	ct3 spa: serial interface efc queue stuck on deleting/adding mlp bundle
CSCsa87316	Unknown	Issuing interface ATM/IMA may result in an unexpected reload.
CSCsa91478	Unknown	L2TPV3: SW_MGR-3-CM_ERROR:Connection Manager Error - unprovision segment

Identifier	Technology	Description
CSCsa94234	Unknown	GTP SLB : Sticky timer should be atleast greater than Session Timer
CSCsa95306	Unknown	SNMPWALK does not get all CSG user group information
CSCsa96960	Unknown	ip ttl expired lsp ping pkts shouldn'tt be transited by MFI process sw
CSCsa97042	Unknown	Secured port dropping traffic after applying & removing mac-filter
CSCsa99158	Unknown	Unexpected START records triggered by IPSec - unreliable AAA records
CSCsa99983	Unknown	FR VC is up but not passing traffic with L2TPv3
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
CSCsb13358	Unknown	failaction gtp purge doesnt delete some gtp stickies when probe fail
CSCsb14516	Unknown	SYS-3-INTPRINT errors seen when ACL used as route-map match criteria
CSCsb14543	Unknown	t/b pm_port_counters_lock on module reset of active supervisor
CSCsb18498	Unknown	SNMP polling broken in cat6k SXE1 image
CSCsb26172	Unknown	Rollback: Timed Rollback option is not available.
CSCsb29028	Unknown	Processor Memory leak in Crypto IKMP process
CSCsb31368	Unknown	ATM Multipoint bridging on c65xx is broken after SW upgrade
CSCsb33258	Unknown	RP crash while mvpn come up - MDFS buildup
CSCsb36463	Unknown	RF-bit not set in the DBUS hdr for the FS switched+RTD port snooped pkt
CSCsb40858	Unknown	IP packets with ip options sourced from TE head fails for 1 hop tunnels.
CSCsb41923	Unknown	isakmp key ending in backslash will be lost after device reboot
CSCsb42176	Unknown	PA-POS-2OC3: router hang upon neighbor reload
CSCsb48739	Unknown	GTP SLB:Session reassigned even when sticky entry exists
CSCsb53810	Unknown	sup720 outbound acl not denying traffic, hitting incorrect team entry
CSCsb54233	Unknown	ISIS hello not recvd on dot1q sub interface on a WS-X6582-2PA
CSCsb56931	Unknown	The SWIDB subblock named QM was not removed, on PPP to FR encaps change
CSCsb57042	Unknown	%SYS-SP-3-OVERRUN at test_hm_diag_scratch_regs
CSCsb59349	Unknown	Standby RP crashed on applying policy to 1k SVI
CSCsb60453	Unknown	Need improved logs for severe fabric errors which triggers fab swover
CSCsb61021	Unknown	IP Spoofed packets from CE are not hw switched with egress WCCP
CSCsb62773	Unknown	Guaranteed bandwidth not consistent with hier shaping configured
CSCsb63267	Unknown	Error locating default vpn
CSCsb65595	Unknown	TCAM LOU expansion doesnt work properly for IPv6 .
CSCsb67152	Unknown	MET inconsistent on DFC, multicast traffic is blackholed for an OIF
CSCsb68178	Unknown	Traceback Seen @ %MPLS_IPRM-3-DB_PATH on 6VPE
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
CSCsb71242	Unknown	MMLS NSF/SSO: Mcast Failover time very high for the first switchover
CSCsb74212	Unknown	Logical & Phy Port run Configs lost on toggling no sw / sw frm VTY
CSCsb76401	Unknown	config mode locks out when u boot active and standby with differ images
CSCsb77716	Unknown	dot1x:SP crash at sm_destroy_instance on OIR or link flap
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
CSCsb84998	Unknown	MLS-MSC ASSERTION FAILED with T/Bs after hw-module reset
CSCsb85030	Unknown	lost connectivity after port security disabled/removed - packets drop
CSCsb85049	Unknown	cwpa2 bridged/routed ATM PDUs lost between Flexwan2 and SUP720
CSCsb85927	Unknown	Routes not deleted on the EzVPN Vi server
CSCsb86198	Unknown	show port-sec int <int-name> add not sync with stdby after SO
CSCsb89241	Unknown	BRE LTL is not populated properly after reload for flexwan2
CSCsb89847	Unknown	Source and destination BGP AS not being exported correctly with Netflow
CSCsb89891	Unknown	dhcp snooping traceback on sup720
CSCsb91644	Unknown	IPv6 MFIB entry is updated on RP and delayed to update MFIB on SP & DFC
CSCsb94412	Unknown	SIP1: RBE: OAM Packets being accounted as input errors
CSCsb94859	Unknown	ATOM_TRANS-3-CONSISTENCY observed Pseudowire Reundancy
CSCsb95563	Unknown	cat6k crashes while releasing mem blocks after unconfig regd. EM Policy
CSCsb95851	Unknown	Cat6K crashing by bus error at msc_sc2vdb_unlink
CSCsb98702	Unknown	Breakpoint (signal 5 exception) when ltl profiling .
CSCsc01223	Unknown	E5 L2TPv3 SCALE: Not all sessions are coming up on router reload
CSCsc02537	Unknown	Add error message when sh frame-relay frag executed for hw mfr/frf.1
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
CSCsc08498	Unknown	SCHED-3-THRASHING traceback from MWAM_CONSOLE Background Process
CSCsc08602	Unknown	RLB errors with code 50 and access messages without username
CSCsc08947	Unknown	6k IOS Autostate: L3 int up/up if last L2 port disabled while L3 is shut
CSCsc09557	Unknown	Dot1x authenticated ports loosing states after SSO
CSCsc13720	Unknown	llq functionality with _match input vlan_ broken
CSCsc16508	Unknown	dmfr: VIP may crash @mfr_print on enabling debug dmfr packets
CSCsc18551	Unknown	Spurious Access on OSM line card
CSCsc18728	Unknown	Sup720 HW PAT (NAT overload) punts frames with valid MTU
CSCsc18986	Unknown	IOS SLB causes high CPU
CSCsc21417	Unknown	OER does not work with NAT
CSCsc21446	Unknown	Multiple IKE SAs created
CSCsc24102	Unknown	Fabric sync errors if WS-X6704-10GE is on slot 4 on 7606
CSCsc25952	Unknown	Need to print out error message for unsupported marking on OSM

Identifier	Technology	Description
CSCsc26048	Unknown	Cat6k: CPUHOG in PIM Snooping Process
CSCsc26490	Unknown	wrong static mac address entry in case of GLBP virtual mac
CSCsc28781	Unknown	%PM-SP-STDBY-3-INTERNALERROR: Port Manager Internal Software Error (pd !
CSCsc29022	Unknown	c7500 -- Broken policy on MFR causing wrong SNMP counters
CSCsc29320	Unknown	Ezvpn server doesn't show number of connections in show crypto session
CSCsc30268	Unknown	linecards crash @ free_qos_set_if_sub_structures
CSCsc30532	Unknown	PIM snooping not populating mac-address table properly on auto rp group
CSCsc32189	Unknown	ISAKMP does not check multiple transform payloads in one proposal .
CSCsc32248	Unknown	Multiple IKE SAs if packets destined to unreachable addresses
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
CSCsc37514	Unknown	Pseudowire: LSP ping output
CSCsc43862	Unknown	SPA ping failure caused by SIP-200 serial primary channel sync failure
CSCsc46301	Unknown	Crash in GTP SLB imsi sticky
CSCsc46922	Unknown	Memory leak - SSM segments
CSCsc48715	Unknown	LFIB does not install both adjacency with Load balancing
CSCsc48986	Unknown	WS-X6148-FE-SFP boards may fail to bootup in Supervisor IOS
CSCsc52306	Unknown	IDSMD: span tree not blocking when two IDSMD in inline mode
CSCsc52645	Unknown	SIP1-CT3: Whole T1 goes down while doing timeslot BERT on CT3 SPA
CSCsc54584	Unknown	Ingress standard ACL for transit traffic broken with MFR bundle
CSCsc55229	Unknown	FWSM rebooting continously
CSCsc55949	Unknown	C2 Frequent fabric channel sync errors and rxErrors
CSCsc55951	Unknown	SPA-4XOC3-ATM has compatibility issue with 3rd vendor device
CSCsc56179	Unknown	mac-address is not purge when interface is shutdown .
CSCsc57156	Unknown	Hardware fault on FWSM ports not causing FWSM redundancy failover
CSCsc58025	Unknown	Out of Service
CSCsc59025	Unknown	UDLD config on 2nd uplinki of act/sby sup change after switchover
CSCsc59190	Unknown	%PM-STDBY-4-INT_FAILUP: fa4/3 failed to come up message after switchover
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.
CSCsc61809	Unknown	Min-links feature doesn't work intermittently even just on shut/no shut
CSCsc61899	Unknown	SIP1-ChOC3: HDLC Controller Device driver Failure (linkrec error)
CSCsc64718	Unknown	persistent-store command not available on SUP32 Images
CSCsc65256	Unknown	Connection Count incorrect after ungraceful disconnect/reconnect
CSCsc65787	Unknown	Enhance (or remove) the automatic intf MTU changing logic in CSCsa73817
CSCsc68250	Unknown	Packet flow halt on 7600-SIP-400
CSCsc68615	Unknown	Router Crash %CPU_MONITOR-3-PEER_EXCEPTION IPv6 IP Tunnel

Identifier	Technology	Description
CSCsc69076	Unknown	SIP1-ChOC3: Spurious access at swsb_delete on unconfig of T1 chnl group
CSCsc69851	Unknown	Port Security does not show offending MAC address in syslog
CSCsc71051	Unknown	VIP4-80 crashed with multilink frame relay configure and L2TPv3
CSCsc71245	Unknown	sup720:High CPU and traceback in ipsec_db_get_ipsec_sa_list with VPNSM
CSCsc75397	Unknown	sup32 enables fix for CSCeb49514 with cross-module etherchannel
CSCsc77287	Unknown	SIERRA: Telnet/console: freeze by remote command module slot
CSCsc77455	Unknown	Fabric counters are inconsistent
CSCsc78707	Unknown	xconnect: l2transport option not valid on dot1q interfaces
CSCsc80303	Unknown	%IPC-SP-5-WATERMARK: 7167 messages pending in rcv for the port Card7/0:
CSCsc80822	Unknown	VPN-SPA - Router fails to decrypt certificate payload during IKE negotia
CSCsc81495	Unknown	PWAN2 HQoS packets dropped with on-the-fly policymap modification
CSCsc81834	Unknown	Netflow uses incorrect source ip address if its within MPLS vrf
CSCsc83961	Unknown	Both APS protect & working ports forwarding traffic
CSCsc84768	Unknown	FESPA-SIP1:BFD session parameter configuration lost on SPA s/w OIR
CSCsc86600	Unknown	SNMP:subinterface aal5 layer: Ifindex counter for ATM SPA not updated
CSCsc89044	Unknown	IO memory leak with big buffers and EOBC0/0
CSCsc89229	Unknown	Traceback & crash at pm_get_standby_vlan on Sup720
CSCsc89932	Unknown	Switch crash after running show diagnostic sanity command
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
CSCsc91075	Unknown	IPSEC Connection Count incorrect after unsuccesfull connection attempt
CSCsc93283	Unknown	R2.5: no mls qos mpls trust exp CLI not effective after reload
CSCsc94402	Unknown	DHCP snooping error msg dispalyed continuously on console
CSCsc96158	Unknown	VPNSM / VPNSPA: IKE SA not deleted even after IPSEC SA idles out.
CSCsc98850	Unknown	ZAMBONI:Could not send pmtu information vlan 65535 pmtu 0 Error
CSCsd00258	Unknown	ENH - Syslog msg - exceeding broadcast suppression threshold
CSCsd00694	Unknown	Need to use L2 port mac for pagp bpdu's to work with cat5000
CSCsd01719	Unknown	SIP-600: SPA OIR with DOT1Q tunnel on port-channel can crash RP
CSCsd01885	Unknown	Flexwan module, when pvc is down, mac-address are not flushed
CSCsd03220	Unknown	OER NFC: stats for default route not aggregated.
CSCsd03416	Unknown	Active RP Crashed after doing rerouting in PIM SM Stress Test
CSCsd03960	Unknown	OSM shaping parameter not programmed correct
CSCsd04808	Unknown	ROOT_Inc message is not show up for all mst instance
CSCsd05513	Unknown	7600 CBQOS-MIB is missing info which is present in CLI
CSCsd08411	Unknown	EEM Tcl policy execution delayed relative to config size
CSCsd09324	Unknown	IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP shown on stby RP when reload rtr
CSCsd13448	Unknown	IOS SLB custom udp probes don't support faildetect

Identifier	Technology	Description
CSCsd15625	Unknown	CEF Adjacencies not established with sub-interfaces configured
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
CSCsd18278	Unknown	Host backpressure is not handled by SPA IPC firmware code
CSCsd18296	Unknown	Bdwt guarantee not met in cbwfq when cfged with llq in child in MIV .
CSCsd19181	Unknown	Crypto connect command is dropped from serial interface after reload .
CSCsd19203	Unknown	SIP400:ATM:new LLQ traffic stop flowing on dynamic changes to Policy
CSCsd22834	Unknown	SIP1-ChOC3: Tx CPU suspended for too long @tal_tree_item_insert
CSCsd23454	Unknown	NPE-G2 VAM2+ : Mem increase at crypto_ipsec_sa_lookup_insert key eng
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
CSCsd25653	Unknown	vrf-also in named ACL for VTY line not saved in running configuration
CSCsd28910	Unknown	Port put in err-disable due to link flaps while other end reloads
CSCsd29911	Unknown	IPSLA : Issues with tracking command threshold weight up xx down xx
CSCsd29927	Unknown	6500 BIT-SP-4-OUTOFRANGE error with voice vlan dot1p and monitor session
CSCsd30533	Unknown	Duplicate ipsec flows at the hub created when spoke is behind nat device
CSCsd32192	Unknown	GRE Tunnel With Checksum Enabled Does Not Transmit Multicast Packets
CSCsd32634	Unknown	R3.2:IOS:Sup32 crashed after range of vlans 1-4094 has been configured .
CSCsd33992	Unknown	%PM-SP-STDBY-3-INTERNALERROR: when boot up
CSCsd35622	Unknown	session timeout TCL causes CPU hog/crash
CSCsd36670	Unknown	Can not enable cdp globally from SNMP
CSCsd38305	Unknown	crash Ethchnl assert (group>=1)switch_private.c:38 after EC remote chang
CSCsd40211	Unknown	Sup720 : Delay in arp result after interface shut/no shut
CSCsd42319	Unknown	SIP400 crashes during bootup with current pikespeak image
CSCsd43481	Unknown	EoMPLS drops OSPF multicast packets with mls ip verify length minimum
CSCsd45167	Unknown	Memory leak in Crypto IKMP Process
CSCsd45932	Unknown	Rainier: On an idle SIP-200 with any chann SPA, CPU util is 10% per SPA
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
CSCsd47734	Unknown	Additional memory leak fixes by ActiveState
CSCsd48741	Unknown	DFC does not see sampled netflow vlans after reload
CSCsd49280	Unknown	show idprom should work with non-cisco xenpaks
CSCsd49374	Unknown	CT3 SPA:%SPA_CHOC_DSX-3-SPA_CMD_SEND_ERR:, all intf stay down
CSCsd49862	Unknown	BFD session stays down after doing shu/unshut on vlan-bundle interface
CSCsd50828	Unknown	AS-path based redistribution fails
CSCsd51577	Unknown	bfd echo to no echo switch removes bfd monitoring
CSCsd52633	Unknown	VPN-Spa stop forwarding traffic if any changes on ATM traffic shaping

Identifier	Technology	Description
CSCsd53513	Unknown	%ALIGN-3-SPURIOUS_SO: Spurious memory access seen with tracebacks
CSCsd56549	Unknown	GRE doesnt get the same port that it req, PPTP change Call ID wrongly
CSCsd58181	Unknown	VIP4-80 Crash with ch-STM1 PA
CSCsd58422	Unknown	%IXP_MAP-3-QOS_CONFIG: error detected: Can't download policymap
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
CSCsd63951	Unknown	sup720 ION: active crashes when slot 2 is reset
CSCsd64103	Unknown	'mls qos trust dscp' not working for traffic coming from FWSM
CSCsd64224	Unknown	Memory leak in Crypto IKMP process when using certificate authentication
CSCsd64533	Unknown	Memory leak in Crypto IKMP process when using certificate authentication
CSCsd64640	Unknown	Memory leak in IPSEC key engine process with isakmp profiles
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
CSCsd66276	Unknown	IDSM: monitor session dest config removed after two sso switchovers .
CSCsd66406	Unknown	SP error msg is not printed part of syslog levels
CSCsd67456	Unknown	VPN-SPA: IPsec SA comes up with wrong lifetime in KB
CSCsd68266	Unknown	input errors increment on 10/half port
CSCsd69480	Unknown	%HYPERION-4-HYP_RESET on flexwan2 chSTM1 card
CSCsd69842	Unknown	Memory leak in Crypto IKMP process on ezvpn server
CSCsd70321	Unknown	Resetting a line card and an sso right after that - traffic gets dropped
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
CSCsd73598	Unknown	Rainier: TB points to mgd_timer_complain_uninit when remove bfd interval
CSCsd74729	Unknown	crypto map in vrf mode failed to create ipsec sa if fvrf != ivrf
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)
CSCsd75836	Unknown	netflow removed from config at bootup due to CSCuk50395
CSCsd75929	Unknown	Sup32 fails to get DHCP snooping binding table on switchover
CSCsd77207	Unknown	Bidir traffic changed from HW to SW switch after add 200 sub-inf quickly
CSCsd78210	Unknown	FPD upgrade file search failed although the file is present.
CSCsd79536	Unknown	Standby RP crashes once at reload after installing set of patches .
CSCsd79558	Unknown	DMVPN:IPSEC SAs fail to get established with fvrf configured on tu
CSCsd80745	Unknown	bus error or alignment err at crypto_isakmp_profile_contain_xauth_info.
CSCsd80770	Unknown	Netflow exports UDP packets with source port 0
CSCsd83402	Unknown	Large packets dropped when service policy applied

Identifier	Technology	Description
CSCsd84497	Unknown	auth-proxy requests stuck in init state
CSCsd86340	Unknown	After unplugging PC from back of phone into new port - error disable
CSCsd87313	Unknown	ip cef load-shar algorithm universal not consistent between stack member
CSCsd88586	Unknown	PBR : Wrong behaviour when first next-hop falls under a route to Null0
CSCsd89949	Unknown	locIfReason is wrongly reporting admin down in an linkDown trap .
CSCsd90173	Unknown	TestIPSecEncrypDecrypPkt HM test config init error reporting is needed
CSCsd92208	Unknown	vlan map ocpu is wrong in the active vpnspa after sso+b2b failover .
CSCsd93294	Unknown	%SYS-STDBY-2-CHUNKFREE err and crash, points to chunk_free_with_pc
CSCsd94127	Unknown	COS aligned to IPP for routed multicast traffic
CSCsd94439	Unknown	I/O mem corruption on SP with mld snooping report-suppression enabled
CSCsd94541	Unknown	Multiple T3 controllers bounce on the SPA
CSCsd94936	Unknown	all interfaces are up/down after physical oir cable
CSCsd95575	Unknown	RP-Crash @ draco2_pa_eobc_intr
CSCsd95701	Unknown	CLI : sh mls qos ip <intf> shows intf disabled on vlan-based switchport
CSCsd95877	Unknown	%MLS_ACL_COMMON-SP-4-MLS_ACL_CONSIST appears on active SP on sso.
CSCsd96121	Unknown	Mac's don't get purged when the port is blocking during topology change
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.
CSCsd98852	Unknown	EEM does not allow read from stdin
CSCsd98887	Unknown	SP Memory Leak In mls-msc Process
CSCse00115	Unknown	mcast egress replication -- Wrong output interface index for msc
CSCse00135	Unknown	Initial few sweep ping packets fail for MLPoMPLS
CSCse00284	Unknown	ION Code crashes active sup under heavy stress and show proc cpu cmd
CSCse01998	Unknown	All vlans in FWSM gets removed after doing no fire mod 9 vlan-gr 11
CSCse08044	Unknown	Netflow Export produced wrong flow record on cache expiration .
CSCse09852	Unknown	Low PPPoEoQ Call Rates with Netflow config on VT intf
CSCse11333	Unknown	Native IOS does not syslog thermal warnings from IDSM-2 Cat6k card.
CSCse11794	Unknown	MPB+QoS: Observe SIP crash with scaled atm bridged vc .
CSCse12195	Unknown	6816: Interface 3/4 flapping when interface 3/1 is not connected
CSCse12314	Unknown	Synguard rate limits tcp probes syn packets
CSCse14269	Unknown	Failed to obtain ident counters for stats update
CSCse14548	Unknown	DHCP SNOOPING support for receiving giaddr nonzero in untrusted port
CSCse15728	Unknown	VPNSM does not perform invalid spi recovery in vrf mode
CSCse15947	Unknown	20 seconds of traffic loss after test crash 9 on active SP
CSCse16512	Unknown	Egress Queuing on WS-6148-21AF broken
CSCse16923	Unknown	5850: IOS upgrade issue in handover split mode
CSCse17175	Unknown	Line down on some serilal interfaces for Chann STM-1 SMI PA

Identifier	Technology	Description
CSCse19351	Unknown	VTI-FVRF:table_id shuld only be consumed when crypto VRF is configured .
CSCse19732	Unknown	Not able to apply policy on a port -which is earlier part of I3 port-cha
CSCse19848	Unknown	Multicast / Broadcast SNMP counters aren't populated for some interfaces
CSCse27836	Unknown	LACP MiniLink Portchannel flaps though hotstandby ports exist
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'
CSCse30293	Unknown	Inbound SA not setup correctly
CSCse31973	Unknown	NF double counts packets when span is configured.
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
CSCse33420	Unknown	LACP: config for some other port-channel gets removed on bundling ports
CSCse33488	Unknown	DS1: Back to back connectivity not successful between T1/E1 SPA-PA
CSCse33543	Unknown	VSEC: IKE SAs stays in MM_KEYEXCH state -RSA signature
CSCse34615	Unknown	Radius Acct on-off messages are dropped by Vserver
CSCse34697	Unknown	crypto injected route points to wrong interface .
CSCse35278	Unknown	VPNSM drops transit NAT-T packets
CSCse37364	Unknown	traceback @ hal_get_dist_job on toggling mmls
CSCse37587	Unknown	DHCP snooping in conjunction with VRF breaks DHCP
CSCse39956	Unknown	VPLS:UCODE:Replication broken when CW followed by NO_CW VC
CSCse41480	Unknown	cos vlan priority is not preserved for MPLS traffic over EoMPLS tunnel
CSCse43709	Unknown	supw nmi support
CSCse47430	Unknown	Need boundry check in heartbeat_create_recv_info
CSCse47638	Unknown	SP and linecard CPUHOG tracebacks at earl7_read_adj_entry when flap link
CSCse47732	Unknown	No support for DS3-MIB for channelized STM1 SPA .
CSCse47811	Unknown	Guard output does not reach GRE tunnels on SUP-720
CSCse48657	Unknown	config sync will reset standby when no EEM policy only on active
CSCse49072	Unknown	sierra: Online diag status for SIP spa modules Unknown / Not Applicable
CSCse49388	Unknown	Tunnel int fails to receive traffic when links of a diff tunnel shut .
CSCse49846	Unknown	Sierra: Convergence issues; avoid snding RPF-chg followed by sc-delete .
CSCse51577	Unknown	Sup2/MSFC2: Memory leak at Dead/FM VMR chunk when pasting in NAT config
CSCse53002	Unknown	Memory leak in IPSEC key engine process at kmi_malloc_num_sas
CSCse53090	Unknown	After console timeout, access can be done to standby console.
CSCse54768	Unknown	CASA traffic not CEF switched
CSCse56921	Unknown	GTP SLB Reloads at the time of session/sticky creation in multiple vserv
CSCse59209	Unknown	Seeing spurious mem trace back when change etherchannel mode to pagp
CSCse59363	Unknown	Crash with an inband/out-of-band channel deadlock detection
CSCse59777	Unknown	WLSM: CPUHOG on L3mm process

Identifier	Technology	Description
CSCse59865	Unknown	ESM20G/SIP600:Router crashes at vlan_if_get_data on bootup w/ 100 subf
CSCse60601	Unknown	Standby Sup crash due to ACLDeny bug in TYCHO
CSCse60667	Unknown	mfiSlaBasic-bat regression cores on show ip cef with feature lfd summary
CSCse61252	Unknown	ION : reset reason displayed incorrectly in show version
CSCse61387	Unknown	After LC is removed, show policy-map control-plane still show LC counter
CSCse65726	Unknown	command no tacacs-server admin resets router
CSCse66269	Unknown	ION free memory dropping during mcast failovers but no process leaking
CSCse69360	Unknown	CLI output from show running-config <spa module number> is broken
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
CSCse70423	Unknown	change WS-X6708-10GE default behavior for non-E chassis
CSCse72235	Unknown	LAC crash when fragmenting ingress PPPoA and labelled in egress
CSCse73539	Unknown	c7600 - crash of active sup720 after inserting a second one
CSCse75904	Unknown	VPNSM: periodic accounting is still sent for disconnected vpn users
CSCse77196	Unknown	Parser truncates pre-shared keys in keyring when line length > 256 bytes
CSCse77427	Unknown	7600 H-VPLS performance issues using SIP-600 and 10G SPA
CSCse77768	Unknown	Mac learning missing some MAC when traffic sent from MPBE to VPLS core
CSCse78548	Unknown	LSR adds incorrect label stack (label 1)
CSCse81638	Unknown	Output stuck on WS-X6524-100FX-MM module
CSCse82589	Unknown	LSR mishandles packets with router-alert label
CSCse83031	Unknown	memory leak reported with Eompls cfg with EFP xconnect child trees
CSCse84226	Unknown	AToM: vc state UP under sh connection when MTU is mismatched
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
CSCse86602	Unknown	Cat6500 IOS does not set correct portAdminSpeed
CSCse87210	Unknown	Enable service cards to operate in crossbar mode with Dist Etherchannels
CSCse87417	Unknown	FlexLink : ARP frames w/ known opcodes cause interop issues.
CSCse87618	Unknown	cRTP and Interleave doesnt work together on Virtual-Template Interface.
CSCse88171	Unknown	PA-MC-8TE1+: cRTP compression failure
CSCse88708	Unknown	Early stop of Bert test on OSM-1CHOC12/T1-SI produces error
CSCse89636	Unknown	LFD-3-INVINSTALLER LSD-3-LABEL msgs and tracebacks when PRE2 -PRE3 ISU
CSCse90572	Unknown	FIB TCAM exception related enhancements
CSCse90586	Unknown	upon low mem crypto kmi crashed with double-free pyld .
CSCse91987	Unknown	slbConnectionTable objects are not getting populated on snmp query
CSCse95888	Unknown	E5 FE SPA interface bandwidth changes when the remote interface is shut
CSCse98354	Unknown	SIP-200: SYNC FAILED not initialized. Interfaces up/down.
CSCse98369	Unknown	class-default bandwidth percent 100% - SPA ATM fails

Identifier	Technology	Description
CSCse98570	Unknown	802.1q subinterfaces have no ifIndex on SUP32
CSCse98692	Unknown	12.2SX code not showing int trust state in sh mls qos cmd
CSCse98795	Unknown	bus error while printing access-list
CSCsf03566	Unknown	Memory corruption crash trying to free unassigned block
CSCsf03730	Unknown	interface remains down even after E1 level local loopback on STM1
CSCsf04112	Unknown	Getting ifPhysAddress changes mac-address of SPA-2X1GE
CSCsf05390	Unknown	CPU HOG @ hwi_db_if_type_unlist followed by router crash.
CSCsf07232	Unknown	tcsh stdio operations do not output to current terminal
CSCsf08368	Unknown	Prevent NBAR configuration on non-FlexWAN interfaces
CSCsf08419	Unknown	EIGRP memory leak in registry_ion.c when neighbor flaps.
CSCsf08502	Unknown	event_reqinfo event_pub_sec/event_pub_msec missing for event_none events
CSCsf08803	Unknown	event snmp may wrongly triggered when using type increment
CSCsf09219	Unknown	SYS-2-NULCHUNK messages/Traceback @ipflow_create_template in netflow
CSCsf10116	Unknown	Reflexive ACL not getting Sw Installed.
CSCsf10203	Unknown	MLD gces not freed even after MLD leaves and L3 traffic stopped
CSCsf10605	Unknown	crypto session count incorrect after ungraceful disconnect
CSCsf11098	Unknown	12.2(SRA) releases report errors trying to FPD upgrade SPA-2X1GE-V2 SPA
CSCsf11639	Unknown	WS-X6148-FE-SFP interface counter increments even if the link is down
CSCsf11787	Unknown	EARL bus idle error occurs when the switching bus stall occurs
CSCsf13044	Unknown	MVPN: Bidir mroute OIF missing - pim joins not received from MDT tunnel
CSCsf14994	Unknown	SIP1-ChOC3:Some of the MLP links wont ping, if deleted & configred again
CSCsf15527	Unknown	ION: Reset Reason Does Not Change on Normal Reload
CSCsf17163	Unknown	TCAM mask/entry resource not released after conf/unconf pacl
CSCsf17739	Unknown	Sup720 SVI does not show multicast traffic rate
CSCsf18752	Unknown	mls ip slb search wildcard rp breaks gtp slb if 2 sfarms are configd
CSCsf20751	Unknown	FlowControl inconsistency between Po and gig interfaces after SW upgrade
CSCsf21629	Unknown	physical links on neighboring switch flap after first SSO
CSCsf22364	Unknown	PortLoopbackTest failed for OC-12 POS SPA on bootup with 26th Aug Image
CSCsf22829	Unknown	EEM Interface event detector sets old value to the sample value
CSCsf23115	Unknown	SUP720 does not recognize FAN2 after one of fans failed. .
CSCsf25240	Unknown	Qos queue-limit warning message on bootup
CSCsf26400	Unknown	Cat6000 may not power up all POE devices after reload
CSCsf27493	Unknown	Ports on WS-6724-SFP with GLC-T adapters don't come up
CSCsf28708	Unknown	TestQos failed on SIP-600 on 12.2SRA
CSCsf31458	Unknown	R3Vail: SupW image - entPhysicalTable is not SSO aware. .
CSCsf32012	Unknown	Fix CSCsc77521 for 6748/DFC
CSCsf96390	Unknown	C7600:subinterface ifIndex is disappearing after reload for PA-STM1

Identifier	Technology	Description
CSCsf96476	Unknown	Router Crash when enabling BFD on ISIS- bfd_intf_addr_change_walker
CSCsf96980	Unknown	No ipv mrib clients established after second SSO switchover, no HW swite
CSCsf97682	Unknown	Last port of T3/E3 SPA connected back to back does not ping
CSCsf98341	Unknown	UDLD failed to receive PDU when linked to L3 port.
CSCsf98713	Unknown	PVST/MST compabitility fix for TELUS
CSCsf98858	Unknown	AB76: BFD echo mode fail detection time is much longer than async mode
CSCsf99460	Unknown	SUP720 cannot disable link-status traps for EOBC0/0 interfaces
CSCsg00173	Unknown	v4 Sparse/SSM traffic when src is in PVLAN src port/DFC is not routed
CSCsg00845	Unknown	'no logging event link-status' is lost after reload
CSCsg01644	Unknown	EEM debug event manager tcl cli sent to the console, script may crash
CSCsg02241	Unknown	SUP720/SUP32 NAT translates incorrectly
CSCsg02391	Unknown	PORT_SECURITY-SP-2-INELIGIBLE error after module reset
CSCsg02605	Unknown	Rapid reboot does not work
CSCsg03739	Unknown	cat6k with vpnsm several possible crypto ikmp leaks .
CSCsg04681	Unknown	MPLS tunnel recir failed after tunnel is taken over by vpnspace
CSCsg06577	Unknown	'Desc ord internal vlan allocation' brings up sup with major diag error
CSCsg07525	Unknown	Periodic (30sec) traffic loss/dup over dis port-cha due to wrong RBH
CSCsg07765	Unknown	Sierra: scp_fpoe_req: memory allocation error, subopcode=10, count=9
CSCsg07870	Unknown	crash seen on switchover at pf_redun_sync_port_asic_on_swover .
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 .
CSCsg09757	Unknown	MP(Maintenance Pack) information missing in the MIB .
CSCsg10075	Unknown	'show policy-map i/f' on --more-- prompt blocks MQC database updates
CSCsg10159	Unknown	Successive Default route ctrl fails on different link but on same router
CSCsg10531	Unknown	Packet loss ratio is more than tolerance under dynamic stress
CSCsg11616	Unknown	iprouting restart crashes Sup due to Block overrun at 5E64940 (red zone
CSCsg12887	Unknown	mcast over gre - tunnel key crashes the box even at low rate traffic(20p
CSCsg13828	Unknown	fh_fd_timer.proc crashed without any special trigger
CSCsg16272	Unknown	Catalyst6500 LinkDown snmp trap does not generate while performing OIR .
CSCsg16425	Unknown	show ip slb reals command displays huge connections value
CSCsg16964	Unknown	Sup32 crashes with 23rd image tb@_shmwin_error
CSCsg18080	Unknown	Router crashes on trying to get snmp counters
CSCsg23979	Unknown	Crashes in iprouting.iosproc produce no tracebacks
CSCsg24215	Unknown	SNMP linkdown traps not generated
CSCsg24609	Unknown	Whitney: snmp CISCO-L2-CONTROL-MIB getmany errors .
CSCsg24971	Unknown	IPC Failure message on WS-X6816-GBIC while displaying netflow entries
CSCsg25416	Unknown	flash information is missing from show hardware output in ION

Identifier	Technology	Description
CSCsg27123	Unknown	Learning not disabled on SPAN dest without learning option
CSCsg27783	Unknown	DFC team wrongly progged when policy map is appld with VACL,Reflex. acl
CSCsg28959	Unknown	rwinde = 0xFFFF on the non PI causing all mcast traffic to be dropped
CSCsg30355	Unknown	OIR of redundant sup w/ CatOS crash the Cat6500 System running IOS
CSCsg32319	Unknown	Probe connections not cleaned up when access/vrf is configured .
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 .
CSCsg36726	Unknown	Bonham parity errors may cause packet loss on a 7600-SIP-400 module.
CSCsg37435	Unknown	ifIndex missing for 802.1Q vLAN subif after GigEth card OIR .
CSCsg37484	Unknown	Bus Error in crypto_map
CSCsg37644	Unknown	IOS SLB does not work on 7600 if Client is behind MPLS cloud
CSCsg38231	Unknown	'crypto eng gre vpnblade' cmd does make the tunnels to be accelerated by
CSCsg38618	Unknown	Session to a 24 bit address fails on WiSM
CSCsg38930	Unknown	7600 SPA-IPSEC-2G - Multicast data is not forwarded through GRE Tunnel
CSCsg39665	Unknown	CPP: Add MIB support for Control-Plane interface
CSCsg39754	Unknown	DHCP snooping redirect ACL permits more than just bootpc and bootps port
CSCsg40267	Unknown	SPA-OC192POS-XFP reports voltage outside of nominal range
CSCsg40391	Unknown	Dot1x: Port config on authenticated port changed after linecard reset
CSCsg40401	Unknown	SUP32 unstable to communicate with all neighbors after reload.
CSCsg41552	Unknown	Module fails to come online first time after reset
CSCsg42860	Unknown	ACE-R6: Back Plane Link RESET to 8 GIG after SUP Switchover
CSCsg43284	Unknown	ISAKMP non-first frag doesn't reach RP from VPNSPA
CSCsg46087	Unknown	Packet dropped at ocpu for packet size greater than 1461
CSCsg49395	Unknown	%BIT-SP-4-OUTOFRANGE: bit is not in the expected range
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
CSCsg51811	Unknown	OER BGP Inbound advert incorrectly modifies all inside prefix adverts .
CSCsg52355	Unknown	RHI Injected routes lost after SUP switchover
CSCsg53461	Unknown	Service Internal incorrectly required for Purge Interface Command
CSCsg53526	Unknown	Some packets to vip are denied by inbound acl after server nat
CSCsg53550	Unknown	EOU commands cannot be enabled on sub-interface
CSCsg55237	Unknown	L2 flooding stops when new MAC address entries are learnt
CSCsg55315	Unknown	Packets duplicated out of Gig1/1 when SPAN Monitor session enabled
CSCsg56625	Unknown	E3 LC continues crash by receive corrupt tag packets ttl=1
CSCsg58587	Unknown	On 7604 snmp output counters for vlan are counted twice
CSCsg58854	Unknown	SPA Ethernet HC 64-bit SNMP counters wrap after reaching 2^32
CSCsg61773	Unknown	MMLS: Egress mode, OIF inconsistent between SP/RP, traffic blackholed

Identifier	Technology	Description
CSCsg61795	Unknown	RLB should not re-use a session when no session-id has been set
CSCsg62154	Unknown	18SXF7: ltl_alloc_index_at: T/Bs are seen after multiple switchover
CSCsg64170	Unknown	SSO switchover causes service module to appear down for 10-30 secs .
CSCsg64306	Unknown	%MCAST-SP-6-L2_HASH_BUCKET_COLLISION
CSCsg64327	Unknown	Tunnels go down with multicast traffic in global vrf mode.
CSCsg66543	Unknown	CISCO-SWITCH-ENGINE-MIB, inconsistent L3 stats between CLI and SNMP.
CSCsg67551	Unknown	LDP session starts to flap after graceful-restart on switchover
CSCsg68740	Unknown	FRR is not triggered when cable is removed from a POS SPA/OSM LC
CSCsg68783	Unknown	ATM SAR hangs when MPLS TE auto-tunnel mesh is cleared
CSCsg69081	Unknown	show crypto ipsec sa should indicate if pfs in use
CSCsg69605	Unknown	Need to reword SYSTEM_CONTROLLER-3-EXCESSIVE_RESET syslog
CSCsg69646	Unknown	'timer wheel' not running for the tunnel .
CSCsg70932	Unknown	ESCORT: router crashes with QoS on and traffic running
CSCsg72398	Unknown	SLB: Packets getting process switched w/ multiple UDP Vservers
CSCsg72678	Unknown	TCAM entries not displayed for DFC card after OIR .
CSCsg73179	Unknown	bi-dir mls rp doesnt get updated after a change in topology .
CSCsg73688	Unknown	Whitney,SNMP,CBQOS,enhance cbQosPoliceCfgRate64 to support 10G int.
CSCsg75132	Unknown	REDUNDANCY-3-IPC: cannot open standby port session in use
CSCsg77142	Unknown	Memory leak in Cat6k SNMP Trap process
CSCsg77629	Unknown	Need to add a command to turn off/on FEFI
CSCsg79810	Unknown	The MPLS MTU is overruled by the ip mtu on ATM interface
CSCsg80948	Unknown	Uneven load-sharing for 4-path ECMP case
CSCsg85046	Unknown	7600 router with SPA-4XOC48POS/RPR on SIP-600 crashes on bootup
CSCsg85415	Unknown	heartbeat_fatal crash, CPU HOG tracebacks point to SEA
CSCsg87228	Unknown	Serial interface (T1 or E1) NOT working with Crypto Connect
CSCsg87235	Unknown	EEM config prevents telnet connection
CSCsg90190	Unknown	Software does not limit 96 Ports LC inline Power based on HW Limitation
CSCsg91545	Unknown	ACL TCAM inconsistency seen if ipv6 acl with 2k mask is used .
CSCsg92393	Unknown	SUP720 CEF loadshare algorithm simple mode does not work for IPv4
CSCsg92950	Unknown	memory corruption overrunning oce counter stack
CSCsg92954	Unknown	Poor Voice Quality over congested Links
CSCsg94023	Unknown	show int status does not show routed port correctly
CSCsg94565	Unknown	PreFrag not works with tun mtu > secure mtu, packet size just > tun mtu
CSCsg97755	Unknown	CMFI Background process produces %SYS-SP-3-CPUHOG
CSCsg98045	Unknown	EEM track event detector missing maxrun option for tcl scripts
CSCsg99084	Unknown	mago: ME-C6524 Tx CRC errors on uplink ports with 100FX SFP .
CSCsg99369	Unknown	Isakmp processes TV attributes as TLV

Identifier	Technology	Description
CSCsg99872	Unknown	VPNSM: IPSEC accounting (start/stop) not sent under some conditions
CSCsg99877	Unknown	AToM: load balancing not happening on the core links
CSCsg99914	Unknown	sip-200 power-cycles after BGP flap (not responding to keepalive)
CSCsh02514	Unknown	MCAST: rpf null for (S,G), process switched on shared tree
CSCsh05800	Unknown	Mcast egress replication - VDB is not updated on L3 PO subinterfaces
CSCsh06605	Unknown	Modular IOS Kernel Release
CSCsh11498	Unknown	%SM-4-BADEVENT: Event rt_reg_ok is invalid for the current state wait
CSCsh13947	Unknown	EoMPLS: Router crashes @ ipv4fib_pas_frag_pak
CSCsh15366	Unknown	Ether SFP/XFP SPAs : Peer link up incorrectly
CSCsh15864	Unknown	Interfaces follow no logical order in sh mls qos ip output
CSCsh16213	Unknown	Disabling MLDsnooping does not clean special MACs 3333.0000.0016, 3333.0
CSCsh17979	Unknown	Ports PWR_DENY not enough system PWR/chassis BackPlane PWR (Not Real)
CSCsh20211	Unknown	'Complete' diags fail TestNetflowInlineRewrite test on Service Modules
CSCsh20354	Unknown	client does not receive mode config data
CSCsh20950	Unknown	18SXF8: PRBS support needs to be disabled on the Malabar8 module
CSCsh21371	Unknown	Catalyst 6500 msfc last reload date not reset properly after reload
CSCsh22835	Unknown	Major Error is seen with module 6 after switchover in rpr mode. .
CSCsh23961	Unknown	Multicast netflow not working for Vlan interface (SVI)
CSCsh25976	Unknown	C2W1: SSO sync issue with PSFANINCOMPAT & PSFANFAIL sensor .
CSCsh27094	Unknown	SSO: VPN Spa got reset twice when subslot x/1 present
CSCsh27234	Unknown	Packet drop occurs at the moment uRPF applied
CSCsh28014	Unknown	After unconfig MPLS, seen %SCHED-CFC8-3-UNEXPECTEDEVENT & Traceback
CSCsh29863	Unknown	New active crashes after switchover in rpr mode .
CSCsh30617	Unknown	EEM software forced crash when unregistering an applet
CSCsh31287	Unknown	tunnel mcast adj shows src mac is all zeros
CSCsh31306	Unknown	T1 serial o/p drops / no QOS drops - flexwan - T1 multichannel PA.
CSCsh33128	Unknown	MMLS/MVPN: Partial SC internal vlan not included in (*,G)
CSCsh33518	Unknown	STP information is not in sync with Active .
CSCsh33770	Unknown	contrl vlan not set; zamboni remains in initializing state .
CSCsh34872	Unknown	With mls mpls recirc configd primary internal vlan has vpn-num .
CSCsh35311	Unknown	Proxyacl downloaded from the ACS cause spurious memory access
CSCsh35600	Unknown	Change CSCsc81300 behavior for deny log ACEs
CSCsh36377	Unknown	crypto connect cmd not updated in standby RP for ATM subif .
CSCsh37008	Unknown	Need to enable Malabar8 in WS-C6509-NEB-A chassis with one fan .
CSCsh37272	Unknown	BFD cpu pegs, invalid element for addition, possible crash
CSCsh37276	Unknown	Switch crashed @ fm_ipv4_intf_nde_req_process
CSCsh38443	Unknown	Removing associated vlan would trigger the mac-add to get purge every 5m

Identifier	Technology	Description
CSCsh38737	Unknown	Flexwan with PA shows incorrect serial int count on sh ver after reload.
CSCsh39318	Unknown	10K / PRE-2 crashes at %MROUTE-4-ROUTELIMIT
CSCsh42857	Unknown	MPLS-TE: After tunnel reoptimization the tunnel label is not updated
CSCsh45258	Unknown	delay execution of redundancy force switchover in case stdby nrd .
CSCsh45949	Unknown	SA's are created by the crypto engine in the wrong subslot
CSCsh48439	Unknown	Sup4:Jagger is not supported
CSCsh48947	Unknown	PWR_DENY Port 47/48 on each LC max PWR support Backplane per LC or VDB
CSCsh49043	Unknown	Output drops in Queue3 after changes in cos-map config on 6148A-GETX .
CSCsh49239	Unknown	After redundancy failover Mcast packets drop for 60-90sec on SUP uplink
CSCsh52941	Unknown	AUTHPROXY:CLI to increase the number of HTTP Proxy process
CSCsh53141	Unknown	IKE SA not getting deleted after clear crypto session
CSCsh54325	Unknown	SIP600/ES20 PXF punt path broken when sup slot is 1 or 2
CSCsh54516	Unknown	JQL:ModularIOS ~80% ARP Proccess performance degradation compared to IOS
CSCsh54951	Unknown	PBR: TCAM incorrectly programmed when match statement is NOT used
CSCsh56121	Unknown	Losing RSA keys on Standby Supervisor after switchover or reload
CSCsh59346	Unknown	allowed number for port-chan interface is not correct for config cli
CSCsh61396	Unknown	R3.8: Hydra module resets during to excessive LCP_FW_ERR Qchip msgs
CSCsh61946	Unknown	Second 6kW DC power supply is shutdown after SSO switch over.
CSCsh62565	Unknown	SSH keys regenerated every hour cause route flaps due to high CPU load
CSCsh68327	Unknown	C6k: rxOversizedPkts counter counts up when link flaps
CSCsh68976	Unknown	memory leak at xcvr_idprom when executing show hw-module all tranceiver
CSCsh69601	Unknown	SNMP poll output byte counters are inaccurate in 12.2(33)SRA1
CSCsh70393	Unknown	no output from sh env voltage command
CSCsh72111	Unknown	mls rate-limit layer2 ip-admission shouldn't be enabled by default
CSCsh73935	Unknown	RP crash with SNMP get to ciscoMvpnMrouteMdtEntry
CSCsh74322	Unknown	rp fails bootup when reload installed image with 42 patch in 1 tar ball
CSCsh74385	Unknown	EEM fails to register with the redundancy framework (RF)
CSCsh74417	Unknown	crash in c10k_remote_crash_interrupt
CSCsh76923	Unknown	Memory Corruption or bus error crash on cat6k running NAT .
CSCsh77220	Unknown	SSO failover causes certain configs being removed .
CSCsh80993	Unknown	VTP Domain Name is not updated on show cdp neighbor detail after rpr sw
CSCsh83109	Unknown	HapiEchoTest fails on SPA-IPSEC-2G when reset.
CSCsh83559	Unknown	Modular IOS: memory leak in xdr_reference
CSCsh85833	Unknown	VACL display sequence does not match between show run and show start
CSCsh87819	Unknown	Traffic-class passive thruput not measured correctly
CSCsh92031	Unknown	Sierra: Standby RP crashed at auth_proxy_posture_clear_nacl
CSCsh94105	Unknown	force supervisor to rommon in a cleaner way

Identifier	Technology	Description
CSCsh94882	Unknown	Unity client not initiating mode config should be rejected
CSCsh94940	Unknown	Supervisor crash by memory corruption (BADFREEMAGIC) in free block .
CSCsh95304	Unknown	unequal weight on multiple paths is not correctly calculated
CSCsh98208	Unknown	PIM Snooping strips out Prune List in a (*,g) Join (s,g) RPT prune msg .
CSCsh98849	Unknown	SIERRA: Active and stby SP and active RP crashed@rf_proxy_fatal_error
CSCsi00136	Unknown	IKE does not process more than 2 NAT-D payload
CSCsi00173	Unknown	Bus error at crypto_ipsec_unlock_peer .
CSCsi00377	Unknown	Exit Mismatch when application & prefix with common dst have diff policy
CSCsi00706	Unknown	Sierra: upon fib tcam exception to use ratelimiter and not reload
CSCsi00712	Unknown	Connected ipv4 routes for WAN interfaces missing on reload
CSCsi02033	Unknown	7600 - creating a new dot1q subinterface breaks eompls vc
CSCsi04335	Unknown	Web Auth performance numbers are not as expected.
CSCsi09388	Unknown	VPNSM SA deleted by idle timeout
CSCsi10219	Unknown	receive side sip1 crashes when rtp traffic is sent for hw MLP + CRTP .
CSCsi10945	Unknown	Http Auth-proxy with OTP does not display token/SNK challange
CSCsi11382	Unknown	Diags failing for NAM module. Module powered down
CSCsi12289	Unknown	FWSM Does Not Display Correct Timezone for DST
CSCsi14145	Unknown	runt counter not implemented correctly
CSCsi14965	Unknown	Need to remove compression cli from cwpw/cwtlc if not supported
CSCsi15191	Unknown	BOM messages observed while activation of rollback on stndby supervisor
CSCsi26184	Unknown	possible fix for CSCsh71274 - improper pak subblock free in ttlexp path
CSCsi32436	Unknown	SNMP set in CISCO-VLAN-MEMBERSHIP-MIB does not mark config changed
CSCsi40628	Unknown	Dual RSPAN session causes loop between 2 6500 chassis .
CSCsi42517	Unknown	SRB Crashes when upgrading from SXF to SRB with SLB stateful config
CSCsi42769	Unknown	VPNPA crashes with large certificates (PKI) .
CSCsi45454	Unknown	ENH to allow traffic to be forwarded with packet-buffer action ignore
CSCsi46469	Unknown	SNMP:loop in cbqosmib on 7609 12.2(33)SRA2
CSCsi46861	Unknown	%MFI-3-REDISTMGR: Redistribution Manager: tracebacks following SSO
CSCsi48975	Unknown	system crash due to Invalid memory action (malloc) at interrupt level
CSCsi49520	Unknown	After SSO, no EOBC buffer available., system cannot recover .
CSCsi51649	Unknown	RP crashes@fm_send_inband_install_message+21C in many cases with NAT
CSCsi52209	Unknown	7600-sip-600 crash at PXF-DFC1-2-FAULT: T0 OHB Exception: SLIP FIFO full
CSCsi54333	Unknown	RP Inlet & Outlet temperatures displayed as N/A on Sup32
CSCsi55626	Unknown	SP hung/RP crashed after mld hosts left from 200-vlan
CSCsi56793	Unknown	Tracebacks seen and Unexpected call: sp_power_mgmt_led() on DFC wan card
CSCsi60125	Unknown	Hosts receive TCP RST due to incorrect NAT translation on cat6k .
CSCsi60472	Unknown	Change default packet-based NF sampling rate to 16 seconds

Identifier	Technology	Description
CSCsi64204	Unknown	SXF:SIP400:ATMSPA Noticeable delay in output of show int atm command
CSCsi69234	Unknown	BFD SM: transition state from Init to Up if recv bfd init packet
CSCsi70920	Unknown	Return traffic doesn't trigger EOU when ip admission on two interfaces
CSCsi72758	Unknown	clear multicast traffic not get to vpnspa in crypto connect mode .
CSCsi74360	Unknown	packet loops between icpu and ocpu while sending clear mcast traffic
CSCsi74923	Unknown	Traceback on changing netflow flowmask
CSCsi76192	Unknown	r3:show wism status not populated until standby up after SSO
CSCsi76936	Unknown	Crash in GLBP if debug is enabled and it rcvs pkt from unknown group
CSCsi77983	Unknown	RP crashed ipflow_pak_pre_check on shutdown the trunk port
CSCsi86691	Unknown	IOS: BR crashes when it learns OER prefixes via dynamic PBR
CSCsi88920	Unknown	MLD rcvr in SVI stops receiving v6 mcast trffc if another rcvr leaves
CSCsi90011	Unknown	User Auth after Machine Auth causes dot1x security violation
CSCsi93683	Unknown	BFD sessions cannot be removed after creating the maximum number allowed
CSCsi94863	Unknown	New xenpak background task .
CSCsi97311	Unknown	subinterfaces are down in OER even if they are actually up .
CSCsi98993	Unknown	Block FPD for Intel SPROM based ATM SPAs
CSCsj01310	Unknown	Modular-IOS: TCP probes are not working with VRF
CSCsj04905	Unknown	IOS-SLB: FWLB sticky config not get removed
CSCsj07935	Unknown	%CONST_DIAG-SP-2-HM_MOD_RESET:Failed TestFabricCh0Health .
CSCsj09249	Unknown	OER PFR MC crash: divide by 0 crash in oer_br_update_iface_counters
CSCsj16292	Unknown	DATACORRUPTION-1-DATAINCONSISTENCY: copy error
CSCsj18014	Unknown	Caller ID string received with extra characters
CSCsj19019	Unknown	Netflow entries not installed for wccp GRE
CSCsj25470	Unknown	EEM hostnames over 20 characters causes CLI actions to hang
CSCsj27811	Unknown	EOBC buffer leak caused by CMM module .
CSCsj40695	Unknown	EEM: Incorrect TCL event registration string can hang or crash device
CSCsj46607	Unknown	RPF showing up on enabled and disabled check
CSCsj53663	Unknown	EEM: RP crashed at fh_fd_syslog_event_match
CSCsj58287	Unknown	7600-SSC-400 crashes on reload
CSCsj59997	Unknown	VTI tunnel: Arp for tunnel destination instead next hop.
CSCsj60182	Unknown	IPSEC Tunnels not coming up in transport adjacency mode
CSCsj65189	Unknown	Traffic stops over EOM ckt after SSO and followed by TE FRR cutover
CSCsj65755	Unknown	Packet loss with SPI NOT Available message during rekey .
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
CSCso08224	Unknown	WS-X6148-45AF port link takes 8 or more seconds to come up
CSCuk56305	Unknown	no mpls ip propagate-ttl forwarded is configured by default

Identifier	Technology	Description
CSCuk57037	Unknown	IGMP: crash at at ../ipmulticast/igmp.c:3162
CSCsb46223	Voice	Bus error crash at Tcl_DStringAppend
CSCek31227	VPDN	Router Crashed while testing Voluntary L2TP Tunneling
CSCef71011	WAN	Trans/Bridging: All pings fail when serial(atm-dxi) in use.
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.
CSCek27504	WAN	NTP crash during show runn after deletion of NTP ref-peer
CSCek42041	WAN	Inconsistent DTR pulsing
CSCek45604	WAN	All OSM modules on the router crashes with FR qos configs .
CSCsa72748	WAN	router crash due to watchdog timeout on frame relay broadcast
CSCsb44267	WAN	bus error crash when forwarding IPX over GRE
CSCsb86675	WAN	Multicast Packets are forwarded out on down PVC on ATM Bundle
CSCsc50986	WAN	NTP unsynchronizes when packets out of order at STEP
CSCsc66187	WAN	%CWPA-3-IPCSENDERFAIL: Failed to send IPC message for loveletter .
CSCsd19880	WAN	ATM pvc does not come up with new style legacy command
CSCsd59878	WAN	Packet switching on FlexWAN stops for 15 secs during an SSO switchover .
CSCse55004	WAN	NTP clients wont associate
CSCse87862	WAN	SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe regn with SNMP IM by driver
CSCse95146	WAN	Sup720 with cross module etherchannel duplicates all packets
CSCsi33554	WAN	Connected net for virtual-template is not created in vrf routing table
CSCsi70727	WAN	LFI Not Working with Cisco<-->Cisco Encapsulation on Frame-Relay