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)SXJ6

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXJ6:

- Route Processor software for NetFlow

  Old Behavior: Route Processor (RP) export values (byte/packet counts per flow) are independent of the configured platform NetFlow sampling ratio.

  New Behavior: The RP software divides the exported packet/byte counts for V5 and V9 export by the configured platform sampling ratio. To enable this behavior, use the platform netflow rp sampling scale command.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_02.html#platform_netflow_rp_sampling_scale

- New CLI: **mls ipv6 acl pbr svi hardware**

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-i5.html

Cisco IOS Release 12.2(33)SXJ5

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXJ5:

- Minimum value raised for **port-channel min-links**

  Old Behavior: The minimum value for the **port-channel min-links** command was 1.

  New Behavior: The minimum value for the **port-channel min-links** command is 2.

- WS-X6066-SLB-APC CSM, WS-X6066-SLB-S-K9 CSM-S, WS-SVC-SSL-1 SSL service module support

  Old Behavior: Release 12.2(33)SXJ and rebuilds do not support these services modules, but they power up in the chassis:

  - WS-X6066-SLB-APC Content Switching Module (CSM)
  - WS-X6066-SLB-S-K9 Content Switching Module with SSL (CSM-S)
  - WS-SVC-SSL-1 Secure Sockets Layer (SSL) Services Module

  New Behavior: With Release 12.2(33)SXJ5 and later releases, the modules do not power up in the chassis.

- WiSM QoS untrusted mode

  Old Behavior: By default, WiSM portchannel interface ports are configured toS trust CoS. Other QoS trust modes can be configured, but there is no option to set the mode to "untrusted".

  New Behavior: There is an option to configure the untrusted mode:

```
Router(config)# wism module 4 con 1 qos trust ?
  cos            Trust CoS
  dscp           Trust DSCP
  ip-precedence  Trust IP precedence
  none           UnTrust
```

Cisco IOS Release 12.2(33)SXJ4

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXJ4:

- Command accounting and command authorization to be sent in asplain notation

  Old Behavior: Command accounting and command authorization that include a 4-byte ASN number are sent in the same format that is used on the command-line interface.

  New Behavior: Command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

  Additional information:

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp3.html

  http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp4.html

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_10.html

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_11.html

- Fast Network Time Protocol (NTP) synchronization

  Old Behavior: The burst and initial burst (iburst) modes are enabled manually.

  New Behavior: The burst and iburst modes are enabled by default.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr-n1.html#GUID-CC69EFC5-68A3-4C5D-90CD-67DE45D4A370

Cisco IOS Release 12.2(33)SXJ3

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXJ3:

- Output changes for the **show ip igmp interface vlan** command

  Old Behavior: The "IGMP snooping query interval" line from the **show ip igmp interface vlan** command displays the IGMP snooping query interval configured on the switch where you enter the CLI.

  Any redundant IGMP snooping queriers do not use the query interval of the active IGMP snooping querier and instead use the locally configured query interval (or the default). You cannot display the active interval On a switch where a redundant IGMP snooping querier is configured.

  New Behavior: The `IGMP snooping query interval` line from the **show ip igmp interface vlan** command displays the IGMP snooping query interval learned from the active IGMP snooping querier or the IGMP Query Interval learned from the active IGMP querier if the IGMP querier is operating in IGMP v3 mode. The **show ip igmp interface vlan** command displays the IGMP snooping query interval configured on the switch where you enter the CLI.

  The `IGMP configured snooping query interval` line from the **show ip igmp interface vlan** command displays the IGMP snooping query interval configured on the switch where you enter the CLI.

  Any redundant IGMP Snooping Queriers learn the active IGMP snooping querier interval. If a redundant IGMP snooping querier becomes active, the newly elected active IGMP snooping querier uses the locally configured IGMP snooping query interval (or the default).

- Default 8q4t DSCP-based queue mapping change

  Old behavior:

  queue 1, threshold 1: 0-9, 11, 13, 15-17, 19, 21, 23, 25, 27, 29, 31, 33, 39, 41-45, 47

  queue 2, threshold 1: 14

  queue 2, threshold 2: 12

  queue 2, threshold 3: 10

  queue 3, threshold 1: 22

  queue 3, threshold 2: 20

  queue 3, threshold 3: 18

  queue 4, threshold 1: 24, 30

  queue 4, threshold 2: 28

  queue 4, threshold 3: 26

  queue 5, threshold 1: 32, 34-38

  queue 6, threshold 1: 48-63

queue 8, threshold 1: 40, 46

New behavior:

queue 1, threshold 1: 0-9, 11, 13-17, 19, 21-25, 27, 29-39, 48-63

queue 1, threshold 2: 12, 20, 28

queue 1, threshold 3: 10, 18, 26

queue 8, threshold 1: 40-47

Additional Information:

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

- Number of login retries for user authentication is configurable

  Old behavior: If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple login retries.

  New behavior: The number of login retries is configurable. The default number of retries is 5.

  Additional information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_auth/configuration/15-2mt/sec-cfg-authen-prxy.html#GUID-ED4C668A-3E5F-44BE-83CF-A3B490E5AEDF

- IOS Server Load Balancing (SLB) CLI removal

  Old behavior: Release 12.2(33)SXI and rebuilds and earlier releases support IOS SLB.

  New behavior: IOS SLB is not supported in Release 12.2(33)SXJ and later releases. The IOS SLB CLI is not present in Release 12.2(33)SXJ3 and later releases.

  Additional information: Release 12.2(33)SXJ and later releases support server load balancing (SLB) as implemented on the Application Control Engine (ACE) module (ACE20-MOD-K9).

Cisco IOS Release 12.2(33)SXI12

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXI12.

Cisco IOS Release 12.2(33)SXI11

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXI11.

Cisco IOS Release 12.2(33)SXI10

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXI10.

Cisco IOS Release 12.2(33)SXI9

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI9:

- Uncorrectable adjacency table ECC error response

  Old Behavior: When an uncorrectable adjacency table ECC error occurs, a message was generated.

New Behavior: You can configure the reponse to an uncorrectable adjacency table ECC error as either a message (default) or module reset and a message.

Additional Information: Enter the **mls cef error adjacency ecc-uncorrectable action reset** global configuration mode command to configure module reset as the reponse to an uncorrectable adjacency table ECC error. Enter the **no mls cef error adjacency ecc-uncorrectable action reset** global configuration mode command to revert to the default behavior (generate a message as the reponse to an uncorrectable adjacency table ECC error).

- Number of login retries for user authentication is configurable.

  Old Behavior: If the authentication fails, the authentication proxy reports the failure to the user and prompts the user with multiple login retries.

  New Behavior: The number of login retries is configurable. The default number of retries is 5.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_auth/configuration/15-2mt/sec-cfg-authen-prxy.html#GUID-ED4C668A-3E5F-44BE-83CF-A3B490E5AEDF

Cisco IOS Release 12.2(33)SXI8a

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXI8a.

Cisco IOS Release 12.2(33)SXI8

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI8:

- CSM module configuration synchronization

  Old Behavior: In releases where CSCtj44456 is not resolved, the **hw-module csm slot_number standby config-sync** command can be entered even if the CSM configuration is being modified in another administrative session.

  New Behavior: In releases where CSCtj44456 is resolved, a message is displayed and the **hw-module csm slot_number standby config-sync** command does not take effect if the CSM configuration is being modified in another administrative session.

  Additional Information: None.

Cisco IOS Release 12.2(33)SXI7

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI7:

- BGP No Longer Activates IPv6 Peers in IPv4 Address Family Automatically

  Old Behavior: By default, both IPv6 and IPv4 capability is exchanged with a BGP peer that has an IPv6 address. When an IPv6 peer is configured, that neighbor is automatically activated under the IPv4 unicast address family.

  New Behavior: Starting with new peers being configured, an IPv6 neighbor is no longer automatically activated under the IPv4 address family. You can manually activate the IPv6 neighbor under the IPv4 address family if you want. If you do not want an existing IPv6 peer activated under

the IPv4 address family, you can manually deactivate the peer with the no neighbor ipv6-address activate command. Until then, existing configurations that activate an IPv6 neighbor under the IPv4 unicast address family will continue to try to establish a session.

Additional Information:

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

- Change in transceiver detail show command output

  Old Behavior: The **show interfaces tengigabitethernet** *slot*/*port* **transceiver detail** command voltage fields display **0.00** for all outputs.

  New Behavior: The voltage fields display **N/A** for all outputs.

  Additional Information: None.

- IEEE 802.1X Enhancement

  Old Behavior: Not applicable

  New Behavior: Addition of the optional **delay** *delay_interval* keyword and argument:

  ```
  Router(config)# ip device tracking [probe {count count | delay delay_interval | interval interval}]
  ```

  Configures these parameters for the IP device tracking table:

  count—Number of times that the switch sends the ARP probe. The range is 1 to 5. The default is 3.

  delay_interval (implemented in releases where CSCtn27420 is resolved)—Number of seconds that the switch delays sending an ARP probe, triggered by link-up and ARP probe generation by the tracked device. The range is 1 to 120 seconds. The default is 0 seconds.

  interval—Number of seconds that the switch waits for a response before resending the ARP probe. The range is 30 to 300 seconds. The default is 30 seconds.

  Additional Information:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.html#CSCtn27420

- IP DHCP snooping enhancements

  Old Behavior: not applicable

  New Behavior: Release 12.(33)SXI7 has these IP DHCP snooping CLI changes.

  ```
  Router(config)# ip dhcp snooping information option replace
  ```

  Or:

  ```
  Router(config-if)# ip dhcp snooping information option replace
  ```

  Replaces the DHCP relay information option received in snooped packets with the switch's option-82 data. Available in releases where CSCto29645 is resolved and when DHCP option-82 data insertion is enabled.

  ```
  Router(config-if)# ip dhcp snooping information option allow-untrusted
  ```

  Available in interface configuration mode in releases where CSCto29645 is resolved.

  Additional Information:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snoodhcp.html#CSCto29645

Cisco IOS Release 12.2(33)SXI6

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI6:

- BFD CPU Utilization

  Old Behavior: CPU Hog is reported by BFD PP process and initial research shows it could be an issue with process's hog detection and bailout. There were no macros supporting the process hog detection and bailout.

  New Behavior: Two new macros have been added to the support process hog detection and bailout.

- Persistence for SNMP Engine ID

  Old Behavior: SNMP Engine ID persistence is not available

  New Behavior: SNMP Engine ID persistence is available. The Engine ID is stored in the NVRAM, the first time when it is generated. The Engine ID is written to a file called snmpid-file in the NVRAM. This file is created in active Route Processor(RP) when you use the write memory command or the copy running startup command. The file will be created in the standby RP when the Engine ID is synced to the standby RP.

  If the file exists in NVRAM, the Engine ID persistence is guarenteed. If this file is removed for some reason and device is reloaded, the following message is displayed on the console on bootup- 00:01:37: % SNMP ID Persistence Error : Unable to open file : No such file or directory

  The persistence is only for the default SNMP Engine ID. If you have configured the Engine ID using the snmp-server engineID local command, then that Engine ID will have precedence over the persisted Engine ID.

- The summary address is not advertised to the peer

  Old Behavior: The summary address is advertised to the peer if the administrative distance is configured as 255.

  New Behavior: The summary address is not advertised to the peer if the administrative distance is configured as 255.

- Fan tray messages for failure and absence

  Old Behavior: Except for E-series chassis, the message displayed for either a fan tray failure or for removal reported only failure or absence (different causes were reported in different releases).

  New Behavior: Except for E-series chassis, the message displayed for either a fan tray failure or for removal reports that the cause might be either a failure or absence.

Cisco IOS Release 12.2(33)SXI5

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXI5:

- Source IP address sent in prune echo messages is now set to the source IP address of the prune echoer

  Old Behavior: The source IP address of prune echo messages is not set to the source IP address of the router that is echoing the prune message (prune echoer). This behavior is not in accordance with RFC 4601 and could potentially cause interoperability issues in certain IPTV deployment scenarios, for example, in VPLS deployments with a mix of Cisco and third-party routers.

  New Behavior: The source IP address that is sent in prune echo messages is now set to the source IP address of the prune echoer.

  Additional Information: None.

- New CLI option is added to view the running configuration without the ACL information.

  Old Behavior: The ACL information is displayed in the running configuration .

  New Behavior: The show running command is modified to provide an option to view the running configuration without the ACL information.

  Additional information:

  http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_s5.html#show_running-config

- SPAN restrictions in PFC3B modes with **xconnect encapsulation mpls**

  Old Behavior: In PFC3B mode or PFC3BXL mode, the **xconnect encapsulation mpls** command might cause traffic to loop continuously with these SPAN configurations:

  – To avoid the problem, if the **xconnect encapsulation mpls** command is configured on a physical interface, the CLI prevents configuration of that port as part of a SPAN session.

  – To avoid the problem, if a SPAN session is configured on a physical port and you attempt to configure the **xconnect encapsulation mpls** command, the CLI prints a warning that recommends against the configuration.

  – If the **xconnect encapsulation mpls** command is configured on a physical interface, you should not configure **source cpu** {**rp** | **sp**} in any SPAN session, but the CLI does not enforce any restriction.

  – If a SPAN session is configured with **source cpu** {**rp** | **sp**} and you attempt to configure the **xconnect encapsulation mpls** command, the CLI does not enforce any restriction.

  New Behavior: In releases where CSCth62957 is resolved, to avoid a configuration that might cause traffic to loop continuously, the CLI enforces these restrictions in PFC3B mode or PFC3BXL mode:

  – If the **xconnect encapsulation mpls** command is configured on a physical interface, the CLI prevents configuration of that port as part of a SPAN session.

  – If a SPAN session is configured on a physical port and you attempt to configure the **xconnect encapsulation mpls** command on that port, the CLI prints a warning that recommends against the configuration.

  – If the **xconnect encapsulation mpls** command is configured on a physical interface, you cannot configure **source cpu** {**rp** | **sp**} in any SPAN session.

  – If a SPAN session is configured with **source cpu** {**rp** | **sp**} and you attempt to configure the **xconnect encapsulation mpls** command, the CLI prints a warning that recommends against the configuration.

  Additional Information: None.

- Support for the **exception switch kernel** command

  Old Behavior: Releases 12.2(33)SXI4 and 12.2(33)SXI4a support the **exception switch kernel** command.

  New Behavior: Release 12.2(33)SXI5 and later releases do not support the **exception switch kernel** command.

  Additional Information: None.

Cisco IOS Release 12.2(33)SXH8b

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXH8b.

Cisco IOS Release 12.2(33)SXH8a

No behavior changes are introduced in Cisco IOS Release 12.2(33)SXH8a.

Cisco IOS Release 12.2(33)SXH8

The following behavior changes are introduced in Cisco IOS Release 12.2(33)SXH8:

- TM_DATA_PARITY_ERROR error, ASIC reset, and supervisor engine reload

  Old Behavior: The response to an TM_DATA_PARITY_ERROR error was an ASIC reset and interrupted inband traffic.

  New Behavior: The response to an TM_DATA_PARITY_ERROR error is a supervisor engine reload.

  Additional Information:

  http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCtf51541

- Option to automatically unconfigure the FTP, TFTP, an RCP source interface configuration.

  Old Behavior: The FTP, TFTP, an RCP source interface configuration needs to be manually unconfigured.

  New Behavior: The FTP, TFTP, an RCP source interface configuration is now automatically unconfigured. This helps to prevent any router crash if the source interface configurations are utilised further unknowingly.

  Additional Information:

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

- Duplicate remark statements can no longer be configured from the IPv6 access control list.

  Old Behavior: Duplicate remark statements could be configured from the IPv6 access control list.

  New Behavior: Duplicate remark statements can no longer be configured from the IPv6 access control list. Because each remark statement is a separate entity, each one is required to be unique.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_05.html

- TestAclFpgaMonitor Diagnostic

  Old Behavior: The TestAclFpgaMonitor diagnostic was not supported.

  New Behavior: The TestAclFpgaMonitor diagnostic is supported.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-41A39BF2-A0F6-434D-A49C-BFDE3285D01E

- Supervisor engine response to a major alarm

  Old Behavior: With redundant supervisor engines, the redundant supervisor engine becomes active and the active supervisor engine drops to ROMMON. With a single supervisor engine, if the cause of the major alarm is not corrected, after 5 minutes the supervisor engine drops to ROMMON.

  New Behavior: With redundant supervisor engines, the redundant supervisor engine becomes active and the active supervisor engine drops to ROMMON. In releases where CSCtf54909 is resolved, if the fan tray is faulty or absent, the active supervisor engine shuts down. With a single supervisor

engine, if the cause of the major alarm is not corrected, after 5 minutes the supervisor engine drops to ROMMON. In releases where CSCtf54909 is resolved, if the fan tray is faulty or absent, the supervisor engine shuts down.

- TestScratchRegister Added to Online Diagnostics

  Old Behavior: Online diagnostics did not test the scratch register for SPAs in 7600-SIP-200 or 7600-SIP-400.

  New Behavior: The "TestScratchRegister" test is implemented in online diagnostics for SPAs in 7600-SIP-200 and 7600-SIP-400.

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-xml/ios/interface/command/ir-o1.html#GUID-464753DB-036E-4225-9AF9-2580245E747E

- 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 DHCPOFFER, 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-xml/ios/ipaddr_dhcp/configuration/12-2sx/config-dhcp-server.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-2sx/config-dhcp-client.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-r1.html#GUID-1516B259-AA28-4839-B968-8DDBF0B382F6

- 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-xml/ios/ipaddr_dhcp/configuration/15-mt/config-dhcp-accounting-security.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr-r1.html#GUID-1516B259-AA28-4839-B968-8DDBF0B382F6

- **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-xml/ios/iproute_bfd/configuration/12-2sx/irb-12-2sx-book.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_s4.html#show_tech-support

- **ip-sec 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)

- 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_pi/command/reference/iri_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-xml/ios/interface/command/ir-cr-book_chapter_010001.html#wp2089533070

  http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir-o1.html#GUID-13F4C686-1A5A-4689-B33C-1FDDC4B1D932

- 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