Features and Important Notes for Cisco IOS Release 15.1(3)T

Contents

These release notes describe the following topics:

New and Changed Information

This section lists the new hardware and software features supported by Cisco IOS Release 15.1M&T and contains the following subsections:

Note A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://www.cisco.com/go/cfn.

New Hardware Features Supported in Cisco IOS Release 15.1(3)T4

There are no new hardware features in Cisco IOS Release 15.1(3)T4.

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

New Software Features Supported in Cisco IOS Release 15.1(3)T4

There are no new software features in Cisco IOS Release 15.1(3)T4.

New Hardware Features Supported in Cisco IOS Release 15.1(3)T2

There are no new hardware features in Cisco IOS Release 15.1(3)T2.

New Software Features Supported in Cisco IOS Release 15.1(3)T2

This section describes new and changed features in Cisco IOS Release 15.1(3)T2. Some features may be new to Cisco IOS Release 15.1(3)T2 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T2. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Right To Use Licensing Support in CLIs and MIBs for Cisco ISR G2 Platforms

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

New Hardware Features Supported in Cisco IOS Release 15.1(3)T

This section describes new and changed features in Cisco IOS Release 15.1(3)T. Some features may be new to Cisco IOS Release 15.1(3)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

EHWIC Multimode VDSL2/ADSL+

The EHWIC-VA-DSL-A, EHWIC-VA-DSL-B, and EHWIC-VA-DSL-M are Multi-mode VDSL/ADSL2+ HWICs.

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/bbdsl/command/reference/bba_02.html#wp1048705

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/dsl_hwic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/inst_ic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/oview_ic.html

http://www.cisco.com/en/US/docs/routers/access/interfaces/rcsi/IOHrcsi.html

VDSL HWIC: HWIC-1VDSL over POTS

The HWIC-1VDSL is used on the Cisco 3945E ISR and the Cisco 3925E ISR to provide VDSL over POTs WAN connectivity. It can be installed on Cisco ISR G2 platforms, and the external RJ-11 port is connected to a DSL line coming from VDSL2 supported DSLAM.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/vdsl2_hwic.html

VWIC3—4MFT-T1/E1

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/customer/docs/routers/access/interfaces/software/feature/guide/vd-t1e1_4p_vwic3.html

New Software Features Supported in Cisco IOS Release 15.1(3)T

This section describes new and changed features in Cisco IOS Release 15.1(3)T. Some features may be new to Cisco IOS Release 15.1(3)T but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T. To determine if a feature is new or changed, see the feature information table at the end of the feature module for that feature. Links to feature modules are included. If a feature does not have a link to a feature module, that feature is documented only in the release notes, and information about whether the feature is new or changed will be available in the feature description provided.

Advanced FXS Analog Gateway Features and SCCP over TLS with Cisco UCM

For detailed information about these features, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/15_1/fxs_15_1_cg_book.html

Cisco CME and SRST Features Enhancement for SCCP and SIP

For detailed information about these features, see the following document:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmeadm.html

Cisco IOS PKI Performance Monitoring Enhancements

For detailed information about this feature, see the following document:

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

Cisco IOS SSL VPN Smart Tunnels Support

For detailed information about this feature, see the following document:

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

Cisco ISR G2 Multi Gigabit Fabric

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/mgfcfg.html

DHCP—Tunnels Support

For detailed information about this feature, see the following document:

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

Embedded Event Manager 3.2

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_eem_3.2.html

Enhancement to Bandwidth QoS-Reference Command

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_a1.html

GETVPN Troubleshooting

For detailed information about this feature, see the following document:

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

IKEv1 Hardening

For detailed information about this feature, see the following document:

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

IKEv2 Remote Access Headend

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

IP Tunneling—IPv6 Rapid Deployment

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-tunnel.html

IPv6—Full Selective Packet Discard Support

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-spd.html

IPv6—Per Interface Neighbor Discovery Cache Limit

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-addrg_bsc_con.html

ISDN Leased Line

The ISDN Leased Line Support for C880 Platforms feature allows the user to configure a dial-up interface to obtain a leased line, which is virtually a permanent connection. After an ISDN BRI interface is configured for access over leased lines, it is no longer a dialer interface, and signaling over the D channel no longer applies.

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/routers/access/800/software/release/notes/rn880isdn.html

Legacy QoS Command Deprecation: Hidden Commands

For detailed information about this feature, see the following documents:

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

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

MediaTrace 1.0

For detailed information about this feature, see the following document:

lhttp://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/mm_mediatrace.htm

Multicast for Virtual Multipoint Interfaces

For detailed information about this feature, see the following documents:

http://www.cisco.com/en/US/docs/ios/ipmobility/configuration/guide/imo_adhoc_rtr2rd.html

http://www.cisco.com/en/US/products/ps5845/products_installation_and_configuration_guides_list.html

NBAR Static IPv4 IANA Protocols

For detailed information about this feature, see the following document:

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

NSE Capability Negotiations via SDP

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/mgcp/configuration/guide/vm_mgcp_basic_cfg.html

Performance Monitor (Phase 1)

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/mm_pasv_mon.html

Radio Aware Routing RFC 4938bis

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/ipmobility/configuration/guide/imo_adhoc_rtr2rd.html

RSVP Support for Ingress Call Admission Control

For detailed information about this feature, see the following document:

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

Session-Based FPM

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_flex_pack_match.html

Suite-B IPSec Algorithm Support for the On-Board Crypto Engine for Cisco 2951 and Cisco 3900 Series ISRs

The Suite-B IPSec algorithm in the hardware crypto engine is now supported on the Cisco 2951 and 3900 Series Integrated Services Router platforms. Suite-B requirements comprise four user-interface suites of cryptographic algorithms for use with IKE and IPSec that are described in RFC 4869. Each suite consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm.

For detailed information about this feature, see the following documents:

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

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

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

http://www.ciscosystems.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cfg_ikev2.html

Support for Conditional Header Manipulation of SIP Headers

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

Support for Interworking Between CUCM-Controlled RSVP-Capable Networks and RSVP-Incapable Networks

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-h323sip.html

Support for Limiting the Rate of Incoming SIP Calls Processing

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-roadmap.html

Support for Media Flow-Around with SIP Signaling Control on Cisco UBE

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-h323h323.html#wp1318874

Support for Release of Media Flow with Retention of SIP Signaling Control on Cisco UBE for Media Trombone or Media Hairpin Call Is Detected

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-h323h323.html

Support for Reporting End-of-Call Statistics in SIP BYE Message

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

Support for SIP Registration Proxy on Cisco UBE

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

Support for SIP UPDATE Message per RFC 3311

For detailed information about this feature, see the following document:

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-sipsip.html

Switch Image and Configuration Manageability

Smart Install is a plug-and-play configuration and image-management feature that provides zero-touch deployment for new switches. This release supports a new MIB, CISCO-SMART-INSTALL-MIB.my. For information about the new features and the MIB, see the *Smart Install Configuration Guide, Release 12.2(55)SE* at the following URL:

http://cisco.com/en/US/docs/switches/lan/smart_install/release_12.2_55_se/configuration/guide/smart_install3.html

Video Monitoring MIB Support for Medianet Video Monitoring

This feature provides support for the use of the industry-standard Simple Network Management Protocol (SNMP) to monitor media streams. This support is implemented with the addition of the following Cisco proprietary SNMP Management Information Base (MIB) modules:

- CISCO-FLOW-MONITOR-TC-MIB—Defines the textual conventions common to the following MIB modules.
- CISCO-FLOW-MONITOR-MIB—Defines the framework that describes the flow monitors supported by a system, the flows that it has learned, and the flow metrics collected for those flows.
- CISCO-RTP-METRICS-MIB—Defines objects that describe the quality metrics collected for RTP streams, similar to those described by an RTCP Receiver Report packet [RFC 3550].
- CISCO-IP-CBR-METRICS-MIB—Defines objects that describe the quality metrics collected for IP streams that have a Constant Bit Rate (CBR).

For detailed information about these MIBs, and to locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at http://www.cisco.com/go/mibs.

This feature also includes two new command-line interface (CLI) commands and one modified CLI command. The commands are as follows:

- **snmp-server host**—Enables the delivery of flow monitoring SNMP notifications to a recipient.
- **snmp-server enable traps flowmon**—Enables flow monitoring SNMP notifications. By default, flow monitoring SNMP notifications are disabled.
- **snmp mib flowmon alarm history**—Sets the maximum number of entries maintained by the flow monitor alarm history log.

For more information about these commands, see the *Cisco IOS Master Command List*.

Important Notes

The following information applies to all releases of Cisco IOS Release 15.1T.

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 this section.

Behavior changes are provided for the following releases:

Cisco IOS Release 15.1(3)T4

The following behavior changes are introduced in Cisco IOS Release 15.1(3)T4:

- SIP call hold/resume scenario has been enhanced so that the RTP sequence number is continuous from the origin of the call till the end.

  Old Behavior: The RTP sequence number is not continuous from the origin until the end of a SIP call, including the time when the call is on hold.

  New Behavior: The RTP sequence number is now continuous from the origin until the end of a SIP call.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_sip/configuration/15-1mt/sip-to-sip_supplementary_services_for_session_border_controller.html

- The new keywords **standard** and **system** are added to the existing **dtmf-interworking** CLI under voice service and dial-peer configuration modes.

  Old Behavior: SIP INFO dtmf digit to RFC4733 DTMF interworking was not supported.

  New Behavior: The newly added keyword **standard** generates RTP NTE packets that are RFC 4733-compliant.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr2/vcr-d2.html#GUID-ED049ED0-50B0-4C38-B3EE-7DDE625389F4

- PfR syslog levels are added to minimize number of messages.

  Old Behavior: There are too many PfR syslog messages.

  New Behavior: PfR syslog levels are added to minimize the number of messages displayed, and a syslog notice is added to display when 30 percent of the traffic classes are out-of-policy.

Additional Information:
http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-1mt/pfr-15-1mt-book.html

Cisco IOS Release 15.1(3)T3

The following behavior changes are introduced in Cisco IOS Release 15.1(3)T3:

- The lease time for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client.

  Old Behavior: DHCP server was sending infinite lease time to manual binding clients.

  New Behavior: The DHCP server sends a finite lease (the value configured using the **lease** command in DHCP pool configuration mode) to the clients for which manual bindings are configured.

- New keywords are added to the **ip access-list** command.

  Old Behavior: There is no filtering capability on packets with IP helper-address destinations.

  New Behavior: Filtering capability is supported for packets with IP helper-address destinations.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_i1.html

- The **all** keyword was added to the **ipv6 nd ra suppress** command.

  Old Behavior: The **all** keyword was not part of command syntax.

  New Behavior: Use of the **all** keyword with the **ipv6 nd ra suppress** command suppresses all IPv6 router advertisements, periodic multicast and solicited, on an interface.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/command/ipv6-i3.html#GUID-1C8D6870-C7DC-4C4B-A6F1-00FA21506E1E

- BGP scan time range is changed.

  Old Behavior: The **bgp scan-time** command has a scanner-interval range of 15 to 60 seconds. The **bgp scan-time** command cannot be configured (it remains at the default value of 60 seconds) if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).

  New Behavior: The **bgp scan-time** command has a scanner-interval range of 5 to 60 seconds. The **bgp scan-time** command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).

- An ADSL interface fails to retrain when the **dsl enable-training-log** command is configured.

  Old Behavior: When the **dsl enable-training-log** command is configured and a cable is disconnected from an asymmetric digital subscriber line (ADSL) card and then reconnected, the ADSL interface fails to retrain.

  New Behavior: To prevent this from happening, disable the retrieval of the DSL training log using the **no dsl enable-training-log** command. The DSL will now train up to the DSLAM.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/bbdsl/command/bba-a1.html

- Change in BGP next-hop for redistributed recursive static routes.

  Old Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next hop to be itself. The local next-hop (equal to next-hop-self) is kept.

  New Behavior: A router advertising a locally originated route (from a static route with recursive next-hop) advertises the next-hop to be the recursive next-hop of the static route.

Cisco IOS Release 15.1(3)T2

The following behavior changes are introduced in Cisco IOS Release 15.1(3)T2:

- BGP no longer activates IPv6 peers in the 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/iproute_bgp/configuration/guide/irg_basic_net.html

  http://www.cisco.com/en/US/partner/docs/ios/ios_xe/iproute_bgp/configuration/guide/irg_basic_net_xe_ps11174_TSD_Products_Configuration_Guide_Chapter.html

- A change has been made in the **neighbor prefix-length-size** command.

  Old Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, if that neighbor has a peer policy or route map that is removed, the **neighbor prefix-length-size** command setting is also removed.

  New Behavior: When the **neighbor prefix-length-size** command is configured in the L2VPN VPLS address family, the value of that command overrides the value set for the peer-group. If the command is locally configured for the peer, it will not be inherited from the peer-group.

- A change has been made in the **show bgp ipv4 unicast summary** command.

  Old Behavior: The **show bgp ipv4 unicast summary** command displays an incorrect number of dynamically created neighbors per address family if a peer-group has been removed from the configuration.

  New Behavior: The **show bgp ipv4 unicast summary** command displays the correct number of dynamically created neighbors, even if a peer-group has been removed. The output displays the number of dynamically created neighbors per address family, and at the end of the output, displays the total number of dynamically created neighbors on the router.

- If there is cause for an IKE registration security association to be deleted on a GDOI group member, it will also be deleted for all groups that share it.

  Old Behavior: When an IKE registration SA is shared among multiple GDOI groups, it is not consistently cleared on members of all groups.

  New Behavior: If there is cause for an IKE registration SA to be deleted on a group member (even if another group is still running and has previously registered through it), it will be deleted for all groups.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_vpn.html

- The hold-alert notification period is not adjustable after first timeout.

  Old Behavior: The hold-alert notification period is not adjustable after first timeout.

New Behavior: The hold-alert notification period is adjustable after first timeout. The recurrence <recurrence-timeout> parameter has been added.

Additional Information:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_h1ht.html#wp1021169

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmering.html#wp1013688

- A CERM license is reserved only after the user logs in.

  Old Behavior: A Crypto Export Restrictions Manager (CERM) license is reserved for every SSL or Transport Layer Security (TLS) session.

  New Behavior: A CERM license is reserved only after the user logs in.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_sslvpn/configuration/15-1mt/sec-conn-sslvpn-ssl-vpn.html

- Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints.

  Old Behavior: Analog (FXS) phones connected to Cisco IAD2430 are not recognized as SCCP endpoints.

  New Behavior: Analog (FXS) phones connected to Cisco IAD2430 are recognized as SCCP endpoints.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/fxssccpsplmft.html

- The **ntp panic update** command is introduced.

  Old Behavior: There is no command to configure Network Time Protocol (NTP) to reject time updates greater than the panic threshold of 1000 seconds.

  New Behavior: A new command, **ntp panic update**, is introduced to configure NTP to reject time updates greater than the panic threshold of 1000 seconds. If the **ntp panic update** command is configured and the received time updates are greater than the panic threshold of 1000 seconds, the time update is ignored and the following console message is displayed:

  ```
  NTP Core (ERROR): time correction of -22842. seconds exceeds sanity limit 1000.
  seconds; set clock manually to the correct UTC time.
  ```

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_10.html

- The **cable-detect** command does not support analog FXO ground-start voice port.

  Old Behavior: The **cable-detect** command can be configured on analog FXO loop-start, ground-start, and cama voice port.

  New Behavior: The **cable-detect** command cannot be configured on analog FXO ground-start voice port. This command is supported only for analog FXO loop-start and cama voice port.

Cisco IOS Release 15.1(3)T1

The following behavior changes are introduced in Cisco IOS Release 15.1(3)T1:

- The **show ip multicast rpf tracked** command is no longer supported.

  Old Behavior: The **show ip multicast rpf tracked** command is available for use. However, it is not recommended that customers use this command.

New Behavior: The **show ip multicast rpf tracked** command is removed.

Additional Information:\

http://www.cisco.com/en/US/docs/ios/ipmulti/command/reference/imc_06.html

- Default maximum removed for subinterface queue-limit.

  Old Behavior: The default maximum queue-limit on a subinterface is 512 if no hold-queue is configured on the main interface.

  New Behavior: As part of HQF, this restriction has been removed. Now, the maximum queue-limit can be set as high as the hold-queue size on the main interface.

  Additional Information:
  http://www.cisco.com/en/US/partner/docs/ios/qos/command/reference/qos_q1.html#wp1075320

- Input service policies are not implemented for PPPoE client traffic.

  Old Behavior: Input service policies attached to a main interface or a subinterface are not implemented for PPPoE client traffic. Only input service policies attached to a dialer interface are implemented.

  New Behavior: Input service policies attached to a main interface or a subinterface are implemented for PPPoE client traffic but only if an input service policy is not configured for a dialer interface. If an input service policy is configured for a dialer interface, the old behavior is retained. Only the quality of service (QoS) counters for packet classification are supported. Counters for packet dropping, packet marking, and policing actions are not supported and are ignored.

- BGP address families are no longer stuck in NoNeg or idle state after reload.

  Old Behavior: After a reload of a router, some or all of the BGP address families do not come up. This is because the router is receiving messages from a neighbor that the AFI or SAFI is not supported, and the router does not retry those AFIs. The output of **show ip bgp all summary** command shows the address family in NoNeg or idle state, and it will never leave that state. Typical output looks like:

  ```
  Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
  x.x.x.x 4 1 0 0 1 0 0 never (NoNeg)
  ```

  New Behavior: When the router receives a message that the AFI or SAFI is not supported, the router does not simply drop the rejected AFIs or SAFIs from subsequent OPEN messages. Instead, the router retries the AFI/SAFI within the existing OPEN message retry timing sequence, but with an exponential back off (stopping at 10 minutes) applied to decisions about whether to include a particular AFI/SAFI in an OPEN message. The timing of OPEN messages is not changed. Successful negotiation of the AFI results in a reset of the backoff sequence for future attempts. Also, when a BGP connection collision occurs with a session in the ESTABLISHED state, BGP sends a CEASE notification on the newly opened connection, and a keepalive message on the old connection. The new connection is closed. If the old session is stale, the keepalive causes it to be closed. The neighbor will retry its OPEN message after receiving the CEASE message and waiting a few seconds.

- New BGP error message

  Old Behavior: No error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels (via the **neighbor send-label** command or via a template). Sending MPLS labels to IPv6 peers is not supported.

  New Behavior: An error message is generated when BGP neighbors are configured with both an IPv6 address and MPLS send labels. An example of the error message is as follows:

  ```
  %BGP-4-BGP_LABELS_NOT_SUPPORTED: BGP neighbor 2001:DB8:1::2 does not support sending
  labels.
  ```

- 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.

- Two new keywords, **protocol** and **pbr**, are added to the **mode route** command.

  Old Behavior: Destination-only traffic classes cannot be controlled when more than one protocol is operating at the border routers.

  New Behavior: Destination-only traffic classes can be controlled when more than one protocol is operating at the border routers using dynamic PBR.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/command/pfr-cr-book.html

- On the Cisco 860, 880, 890, 2900, and 3900 series ISRs, the default behavior changes when the interface is not connected to an active port.

  Old Behavior: GigabitEthernet0/3/0 is up, line protocol is down.

  New Behavior: GigabitEthernet0/3/0 is down, line protocol is down.

- A new keyword is added to the **ignore crc** command.

  Old Behavior: The **always** keyword is not available for the **ignore crc** command.

  New Behavior: The **ignore crc** command can use the **always** keyword to always ignore CRC errors.

  Additional information:
  http://www.cisco.com/en/US/docs/ios/bbdsl/command/reference/bba_book.html

- A new keyword is added to the **bind interface** command

  Old Behavior: The **dynamic** keyword is not available for the **bind interface** command.

  New Behavior: The **bind interface** command can use the **dynamic** keyword.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_b1.html#wp1545540