



Features and Important Notes for Cisco IOS Release 15.1(2)T

Contents

These release notes describe the following topics:

- [New and Changed Information, page 47](#)
- [Important Notes, page 56](#)
- [Limitations and Restrictions, page 62](#)

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:

- [New Hardware Features Supported in Cisco IOS Release 15.1\(2\)T4, page 47](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(2\)T4, page 48](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(2\)T2, page 48](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(2\)T2, page 48](#)
- [New Hardware Features Supported in Cisco IOS Release 15.1\(2\)T, page 48](#)
- [New Software Features Supported in Cisco IOS Release 15.1\(2\)T, page 50](#)



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(2)T4

There are no new hardware features in Cisco IOS Release 15.1(2)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(2)T4

This section describes new and changed features in Cisco IOS Release 15.1(2)T4. Some features may be new to Cisco IOS Release 15.1(2)T4 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(2)T4. 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(2)T2

There are no new hardware features in Cisco IOS Release 15.1(2)T2.

New Software Features Supported in Cisco IOS Release 15.1(2)T2

This section describes new and changed features in Cisco IOS Release 15.1(2)T2. Some features may be new to Cisco IOS Release 15.1(2)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(2)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.

WAAS Express

This feature introduces WAN optimization technology as a software offering on Cisco IOS based platforms. This technology will interoperate with WAN optimization head-end appliances from Cisco.

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

http://www.cisco.com/en/US/docs/ios/wan/configuration/guide/cfg_waas_exp.html

New Hardware Features Supported in Cisco IOS Release 15.1(2)T

This section describes new and changed features in Cisco IOS Release 15.1(2)T. Some features may be new to Cisco IOS Release 15.1(2)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(2)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.

1-Port and 2-Port VVIC3s—Voice WAN Interface Cards

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

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/vd-t1e1_vwic3.html

4-Port and 8-Port Cisco Gigabit EtherSwitch EHWIC Modules for the Integrated Service Routers Generation 2 (ISR G2) Platform

Cisco Gigabit EtherSwitch enhanced high-speed WAN interface cards (EHWICs) are 10/100/1000 BaseT Layer 2 Gigabit Ethernet (GE) switches with an optional power over Ethernet (PoE) module that provides inline power for IP telephones.

Cisco Integrated Service Routers Generation 1 C-Series

Cisco IOS Release 15.1(2)T supports the Cisco 1841C, Cisco 2801C, Cisco 2811C, Cisco 2821C, Cisco 3825C, and Cisco 3845C integrated service routers generation 1 C-series. The following features are not supported on these routers:

- Cisco Communications Manager Express (CME)
- Cisco Unified Border Element (UBE)
- Dynamic Multipoint Virtual Private Network (DMVPN)
- Group Encrypted Transport Virtual Private Network (GET-VPN)
- Hierarchical quality of service (HQoS)
- Multicast features:
 - PIM SSM
 - IGMPv3
 - MVPN
 - MSDP
- NetFlow v9
- Optimized Edge Routing (OER)
- Performance Routing (PFR)
- Power over Ethernet (PoE)
- Survivable Remote Site Telephony (SRST)

Digital Subscriber Line (DSL)—Multimode (VDSL2 and ADSL2/2+)

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

<http://www.cisco.com/en/US/partner/docs/routers/access/800/860-880-890/software/configuration/guide/SCG880-860.html>

<http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/hardware/installation/guide/860-880-890HIG.html>

http://www.cisco.com/en/US/docs/ios/bbds1/command/reference/bba_book.html

STM1 Support for Cisco 3900 Series of Platforms

The SM-1-STM1 is a high-speed, single-port multichannel STM-1 port adapter, which serves as a multichannel E1 STM-1 port on Cisco 3900 series integrated services routers (ISR).

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

<http://www.cisco.com/en/US/docs/routers/access/interfaces/adapt/STM1PA/STM1.html>

New Software Features Supported in Cisco IOS Release 15.1(2)T

This section describes new and changed features in Cisco IOS Release 15.1(2)T. Some features may be new to Cisco IOS Release 15.1(2)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(2)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.

Additional PDL Support for NBAR

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

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

Assisted RTCP Packet Generation

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

http://www.cisco.com/en/US/partner/docs/ios-xml/ios/voice/config_library/12-4t/cube-12-4t-library.html

BFD IPv6 Encapsulation Support

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

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

BGP—Remove/Replace Private AS Filter

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

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

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_remove_as.html

BGP Dynamic Neighbors

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

http://www.cisco.com/en/US/docs/ios/iproute_bgp/configuration/guide/irg_neighbor.html

Bidirectional Forwarding Detection MIB version 2

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

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

Box to Box (Interchassis) Redundancy for the Cisco Unified Border Element

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

http://www.cisco.com/en/US/docs/ios/ios_xe/voice_cube_-_ent/configuration/guide/cube_ent/vb_book_xe.html

Cisco CME and SRST Features Enhancement

New features for Cisco Unified CME 8.1:

- Toll Fraud Prevention Enhancement
- Enhancements to SIP Phone Configuration
- Support for Cisco Unified 6901 and 6911 SCCP IP Phones

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

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

Cisco IOS PKI RA Server Interoperate Support with the Microsoft CA Server

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_mng_cert_serv.html

Cisco IOS ZBFW SCCP Video Support

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

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

Cisco IOS Zone-based Firewall

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

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

Cisco Unified Border Element—Per-Call Debugging

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

http://www.cisco.com/en/US/docs/ios/ios_xe/voice_cube_-_ent/configuration/guide/cube_ent/vb_book_xe.html

Cisco Unified Communications Trusted Firewall Control— Version 3

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/TrustedFW.html

DHCP VRF Exclude Support

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

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

DMVPN Configuration Using FQDN

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_conf_using_fqdn.html

DMVPN—Tunnel Health Monitoring and Recovery (Backup NHS)

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_tun_mon.html

DTLS Support for Cisco IOS SSL VPN

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

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn.htm

FPM Packaging Feature

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

Healthcare Router System

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

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

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

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

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html

IPv6 Support on BVI Interfaces

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

Layer 2 Switch Port Manageability MIBs for MAC Notification

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

<http://www.cisco.com/en/US/partner/docs/routers/access/800/860-880-890/software/configuration/guide/SCG880-860.html>

MLD Proxy

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

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

MPLS VPN over mGRE

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

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

OSPFv3 BFD

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

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

Preserve 802.1q with 802.1p Marking over ATM PVCs for xDSL Uplinks

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

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_trans_vlan-tags_dsl_links.html

RSVP for Flexible BW Interface

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

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

RSVP over DMVPN

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

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

SDP Solution for iPhone Deployment

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

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

Serviceability Enhancement for PCM Capture

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

http://www.cisco.com/en/US/docs/ios/ios_xe/voice_cube_-_ent/configuration/guide/cube_ent/vb_book_xe.html

Static Route Support for BFD over IPv6

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

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

Suite-B Support in IOS SW Crypto

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

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_cert_enroll_pk_i.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 Ability to Configure Source IP Address for Signaling and Media per SIP Trunk

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

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-bind.html

Support for Call Routing Logic on the Cisco Unified Border Element Based on the Information Embedded in the History-info Header

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

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for Hiding the Internal Topology Information Embedded Within the History-info Header at the Cisco Unified Border Element

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

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for Inclusion of the Authorization Header in the Initial REGISTER Request

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

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for Monitoring Utilization of Critical Resources on Gateway Router, Cisco Unified Border Element and Cisco Unified CME and Reporting Over SIP Trunks

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

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-res_utlzn_monitoring.html

Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-SIP Call on the Cisco Unified Border Element

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

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb_book/vb_book.html

Support for Pass-Through of STUN and DTLS Packets

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

http://www.cisco.com/en/US/partner/docs/ios-xml/ios/voice/config_library/12-4t/cube-12-4t-library.html

Support for Populating the Route Header Based on the Proxy Server IP Address and Port, and the Service-Route Header Present in the Register Response

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

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html

Support for VMWI over SIP on Cisco IOS Gateways

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

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-mwi.html

Support Inbound Dial-peer Match Based on the Remote IP Address on SIP Trunks

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

http://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/gt_url.html

Voice Support on 1-Port and 2-Port HWICs

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

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_11xw/fmt1e1ic_voice.html

Important Notes

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

- [Cisco IOS Behavior Changes, page 56](#)
- [Important Notes for Cisco IOS Release 15.1\(2\)T, page 61](#)

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\(2\)T5, page 56](#)
- [Cisco IOS Release 15.1\(2\)T4, page 57](#)
- [Cisco IOS Release 15.1\(2\)T3, page 58](#)
- [Cisco IOS Release 15.1\(2\)T2, page 60](#)

Cisco IOS Release 15.1(2)T5

The following behavior changes are introduced in Cisco IOS Release 15.1(2)T5:

- BGP scan time range is changed.
 Old Behavior: The **bgp scan-time** command has a scanner-interval range of 15-60 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 5-60 seconds. The **bgp scan-time** command can be configured, even if BGP Next Hop Tracking (NHT) is configured (by the **bgp nexthop** command).
- 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.
- Multicast updates are passed by zone-based firewall with IP multicast traffic.
 Old Behavior: If you use the **drop** (zone-based policy) command to configure a zone-based firewall with IP multicast traffic, all multicast updates are dropped by the zone-based firewall.

New Behavior: All multicast updates are passed by the zone-based firewall even if the zone-based policy configuration includes the **drop** command.

Additional information:

http://cisco.com/en/US/docs/ios-xml/ios/security/d1/dnsix-dmdp_retries_through_dynamic.html#GUID-FC5653D0-8DD9-4ADB-8C03-34A028AEE954

- 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/fxsccpsplmft.html>

- New keywords “standard” and “system” are added to 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(2)T4

The following behavior changes are introduced in Cisco IOS Release 15.1(2)T4:

- 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 output, displays the total number of dynamically created neighbors on the router.

- 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

- 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-ssl-vpn-ssl-vpn.html

Cisco IOS Release 15.1(2)T3

The following behavior changes are introduced in Cisco IOS Release 15.1(2)T3:

- By default, the TCP SIP NAT ALG functionality is disabled.

Old Behavior: In the **ip nat service** command, the **tcp** keyword used along with the **sip** keyword was used to enable the TCP SIP NAT ALG functionality.

New Behavior: The **tcp** keyword used along with the **sip** keyword in the **ip nat service** command is removed. The TCP SIP NAT ALG functionality is disabled by default.

Additional Information:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_nat.html#wp1049948

- 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 is removed for subinterface queue-limit.

Old Behavior: The default maximum queue-limit on a subinterface was 512 if no hold-queue was 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/docs/ios/qos/command/reference/qos_q1.html#wp1075320

- BGP address families 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 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 backoff (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 was 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
 “%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 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.

- The line coding and loss of sync information is changed in the output for the **show controller shdsl** command.

Old Behavior: The output for the **show controller shdsl** command for the HWIC- 4SHDSL-E shows the line coding as AUTO-TCPAM when Annex F and G are selected, and loss of sync as LOSWAS.

New Behavior: The output for the **show controller shdsl** command for the HWIC- 4SHDSL-E shows the line coding as 16-TCPAM or 32-TCPAM depending on which TCPAM is used to train lines when Annex F and G are selected, and loss of sync as LOSW.

Additional Information:

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

- Behavior change type: New keyword added to **ignore crc** command.

Old Behavior: The **always** keyword was 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/bbds/command/reference/bba_book.html

Cisco IOS Release 15.1(2)T2

The following behavior changes are introduced in Cisco IOS Release 15.1(2)T2:

- Specific BGP **show** commands display dampening information on an individual VRF basis.

Old Behavior: The following commands display flap-statistics, dampened-paths, and dampening parameters of VRFs under the VPNv4 or VPNv6 address family identifier:

- **show ip bgp all dampening**
- **show ip bgp vpnv4 all dampening**
- **show ip bgp vpnv6 unicast all dampening**

New Behavior: Because VRFs can have dampening enabled independently of other VRFs and the global VPNv4 and VPNv6 topologies, the following commands display flap-statistics, dampened-paths, and dampening parameters of individual VRFs under that VRF name:

- **show ip bgp all dampening**
- **show ip bgp vpnv4 all dampening**
- **show ip bgp vpnv6 unicast all dampening**

If dampening is not enabled for a VRF, that is stated under the VRF name.

For more information, see the [Cisco IOS IP Routing: BGP Command Reference](#).

- Command is changed to disable pipelining for URLF requests to Trend Server.
 Old Behavior: Trend Router Provisioning Server (TRPS) does not provide the functionality to turn on or off the TRPS pipeline requests.
 New Behavior: TRPS enables you to turn on or off the TRPS pipeline requests.
 The **pipeline**, **on**, and **off** keywords are added to the **parameter-map type trend-global** command.
 Additional Information:
http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_p1.html#wp1059633
- New command is introduced to configure polarity detection for 10-Mbps full-duplex links.
 Old Behavior: By default, polarity detection is enabled for 10-Mbps full-duplex links on Integrated Services Router Generation 2 (ISR G2) platforms. With connection to some network equipment over a 10-Mbps full-duplex link, the polarity detection feature can cause cyclic redundancy check (CRC) errors. There is no CLI command to disable this feature.
 New Behavior: By default, the polarity detection feature is disabled for 10-Mbps full-duplex links on ISR G2 platforms. Use the **rj45-auto-detect-polarity {enable | disable}** command to enable or disable polarity detection.
 Additional Information:
http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_o1.html#wp1067169
- The default state for the Cisco Gigabit EtherSwitch EHWIC when the interface is not connected to an active port is changed.
 Old Behavior: GigabitEthernet0/3/0 is up, line protocol is down.
 New Behavior: GigabitEthernet0/3/0 is down, line protocol is down.
- Right to Use license is added for ISR G2 platforms.
 Old Behavior: The Right to Use license is not available for technology packages and all features on Cisco ISR G2 platforms.
 New Behavior: The Right to Use license is available for technology packages and all features on Cisco ISR G2 platforms, except for the HSEC feature. Use the license accept end user agreement command in global configuration mode to configure a one-time acceptance of the Cisco End User License Agreement (EULA) for all Cisco IOS software packages and features.
 Additional Information:
http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

Important Notes for Cisco IOS Release 15.1(2)T

The following information applies to all releases of Cisco IOS Release 15.1(2)T:

Images Deferred Because of Caveat CSCti18193

In Cisco IOS Release 15.1(2)T, images for all platforms have been deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCti18193. With caveat CSCti18193, Cisco IOS Release 15.1(2)T is affected by denial of service (DoS) vulnerability during TCP establishment phase. The software solution for these deferred images is Cisco IOS Release 15.1(2)T0a.



Note

Failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco with respect to the deferred images will apply to the replacement images.

Toll Fraud Prevention

In Cisco IOS Release 15.1(2)T, the Toll Fraud Prevention feature is supported as below:

- Source IP address authentication is enabled on incoming IPv4 H323/ or SIP trunk calls. The source IP address of any incoming IPv4 H323 or SIP trunk calls will be authenticated based on:
 - Manually configured IP address trusted list.
 - VoIP dial-peer session target (the state of a VoIP dial-peer must be in “Operation State = UP”)

Incoming IPv4 H323 or SIP trunk calls will be rejected if the authentication fails and the default **cause-code call-reject (21)** disconnects the call.

Execute the **show ip address trusted list** command to display IP address trusted data and a list of valid source IP addresses. The default behavior can be disabled as shown in the example below:

```
voice service voip
no ip address trusted authenticate
```

- Secondary dial-tone is disabled for a call initiated from a FXO port. No secondary dial-tone causes the outgoing call setup to fail if the called number is NULL. The default behavior can be disabled as shown below:

```
voice-port <fxo-port>
secondary dialtone
```

- Direct-inward-dial is enabled to prevent the toll fraud for incoming ISDN calls. Two-stage dialing is disabled for incoming ISDN calls by default. The incoming called number will then be used for outgoing call setup. The default behavior can be disabled as shown in the example below:

```
voice service pots
no direct-inward-dial isdn
```

For more information, see the *Cisco Unified Communications Manager Express System Administrator Guide* at the following URL:

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

Limitations and Restrictions

Any limitations and restrictions that apply to Cisco IOS Release 15.1M&T will be documented here.

Limitations and Restrictions in Cisco IOS Release 15.1(2)T2a

This section describes limitations and restrictions in Cisco IOS Release 15.1(2)T2a and later releases.

FIPS Certification

Cisco IOS Release 15.1(2)T2a is only to provide FIPS certification for the Cisco ISR Generation 2 platforms.

