Features and Important Notes for Cisco IOS Release 15.1(1)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(1)T5

There are no new hardware features in Cisco IOS Release 15.1(1)T5.

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(1)T5

There are no new software features in Cisco IOS Release 15.1(1)T5.

New Hardware Features Supported in Cisco IOS Release 15.1(3)T3

There are no new hardware features in Cisco IOS Release 15.1(3)T3.

New Software Features Supported in Cisco IOS Release 15.1(1)T4

This section describes new and changed features in Cisco IOS Release 15.1(1)T4. Some features may be new to Cisco IOS Release 15.1(1)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(1)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(1)T1

This section describes new and changed features in Cisco IOS Release 15.1(1)T1. Some features may be new to Cisco IOS Release 15.1(1)T1 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(1)T1. 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 VWIC3s—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

Cisco Integrated Service Routers Generation 1 C-Series

Cisco IOS Release 15.1(1)T1 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 (CCME)
- Cisco Unified Border Element (CUBE)
- 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)

New Software Features Supported in Cisco IOS Release 15.1(1)T1

This section describes new and changed features in Cisco IOS Release 15.1(1)T1. Some features may be new to Cisco IOS Release 15.1(1)T1 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(1)T1. 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.

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

New Hardware Features Supported in Cisco IOS Release 15.1(1)T

This section describes new and changed features in Cisco IOS Release 15.1(1)T. Some features may be new to Cisco IOS Release 15.1(1)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(1)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.

3G HSPA Enhancement

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

http://www.cisco.com/en/US/products/hw/routers/ps380/products_installation_and_configuration_guides_list.html

Cisco 1905 and Cisco 1921 Integrated Service Routers

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

http://www.cisco.com/en/US/docs/routers/access/1900/hardware/installation/guide/1900_HIG.html

Cisco 3925E and Cisco 3945E Integrated Service Routers

The Cisco 3945E and Cisco 3925E offer new Services Performance Engines (SPEs), that are high-performance modular motherboards with a cryptographic accelerator, 4 onboard GE ports, 2 SFP slots, 3 EHWIC slots, 3 PVDM3 slots, and up to 350Mbps WAN Access with services. The Cisco 3945E and 3925E are shipped with Services Performance Engines (SPEs) pre-installed in the router, or are sold separately. The SPE250 and SPE200 provide a modular approach to system upgrades, because you can easily upgrade the SPE on a Cisco 3945 or Cisco 3925 for improved router performance.

The Cisco 3945E and Cisco 3925E provide highly scalable Security and UC/CUBE services and offer investment protection for customers who purchase a Cisco 3925 or Cisco 3945 today, providing an upgrade option for higher performance levels in the future when increased bandwidth demands require higher performance levels.

Cisco 888E

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

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/partner/docs/routers/access/800/860-880-890/software/configuration/guide/SCG880-860.html

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/oview_ic.html

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

Cisco Connected Grid Router 2000 Series

The Cisco Connected Grid Router 2010 (Cisco CGR 2010) router is a member of the Cisco Connected Grid Router 2000 Series family of routers.It is an especially rugged, high performance router that provides LAN and WAN connectivity, field replaceable parts, and feature upgrades through software licensing. The Cisco CGR 2010 is designed to withstand hostile environments while continuing to deliver the performance, availability, and reliability to scale mission-critical needs.

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

http://www.cisco.com/en/US/products/ps10977/products_installation_and_configuration_guides_list.html

Cisco Unified Communications 500 Series

The Cisco Unified Communications 500 Series is part of the Cisco Smart Business Communications System (SBCS). The Cisco UC 500 series is a unified communications solution for small businesses that provides voice, data, video, and security capabilities.

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

http://www.cisco.com/en/US/products/ps7293/tsd_products_support_series_home.html

Note Cisco UC 500 images are only available via Cisco UC 500 software packs on the Small Business Community Site at www.cisco.com/go/smallbizsupport.

HWIC-1VDSL

The HWIC-1VDSL is used on the Cisco ISR G2 platforms 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 DSL line coming from VDSL2 supported DSLAM.

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

http://www.cisco.com/en/US/products/ps5949/tsd_products_support_series_home.html

HWIC-4SHDSL-E

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

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

New Software Features Supported in Cisco IOS Release 15.1(1)T

This section describes new and changed features in Cisco IOS Release 15.1(1)T. Some features may be new to Cisco IOS Release 15.1(1)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(1)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.

Call Home

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

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/callhome_asr1k.html

Call Restriction Regulations

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

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

Cisco Unified Border Element Support for Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure

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#wpxref97945

CME (Communications Manager Express) 8.0/SRST (Survivable Remote Site Telephony) 8.0

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/Cisco_Unified_IPPhones_69xx_Series.html#wp1072892

CME CSTA CTI Protocol Suite

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

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/open/source/sdkgnusl.html

Compliance-Mode Cipher and Hash Selection for GET VPN Group Member

This feature allows Federal Information Processing Standards (FIPS) compliance and Common Criteria (CC) compliance by enabling Cisco Group Encrypted Transport VPN (GET VPN) group members to specify locally-acceptable cipher and hash algorithms for the key encryption keys (KEKs) and traffic encryption keys (TEKs) that they download from the key server. This feature is configured with the following commands:

client rekey encryption

client rekey hash

client transform-sets

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

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

DHCP Zero Touch

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

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

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cns_services_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Direct Download from CCO Capability in Cisco IOS IPS

The Direct Download from CCO Capability in Cisco IOS IPS feature was introduced to allow an administrator to use the CLI to specify, download and upgrade new signatures posted for Cisco IOS directly from Cisco.com. An administrator can also configure the router through the CLI to receive future periodic signature downloads automatically to eliminate the manual maintenance efforts and costs of changing or tuning IPS signatures whenever a new IPS signature update is posted.

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

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_ips5_sig_fs_ue.html

DoD MLPP PBX1 Certification for CME

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

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

DoD Secure Device Support for CME: Support STU/STE/IP STE with CME

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

EnergyWise Branch Routers

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

http://www.cisco.com/en/US/products/ps10538/tsd_products_support_configure.html

Enhanced Music on Hold

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmemoh.html#wp1022363

G.SHDSL Auto Pair Detect

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

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/shdslfm.html#wp1054629

IEEE 802.1ag—D8.1 Standard Compliant CFM, Y.1731 Multicast LBM/AIS/RDI/LCK, IP SLA for Ethernet

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

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee.html

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_cfm-ieee_y1731.html

IKEv2 Site-to-Site

IKEv2 is the supporting protocol for IP Security Protocol (IPsec) and is used for performing mutual authentication and establishing and maintaining security associations (SAs). IKEv2 supports crypto-map and tunnel protection based IKEv2 solutions and features such as Dynamic Multipoint VPN (DMVPN), IPsec Static Virtual Tunnel Interface (sVTI), and IPsec Dynamic Virtual Tunnel Interface (dVTI).

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 SLAs Engine 3.0

The Auto IP SLAs feature in Cisco IOS IP Service Level Agreements (SLAs) Engine 3.0 enables you to define a single probe definition that can be combined with different collections of endpoints to create multiple operations, including operations for proactive threshold monitoring, and allows a source to auto-discover the endpoints of an IP SLAs Responder. IP SLAs Engine 3.0 also enables the active measurement of Quality of Service (QoS) performance.

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-1mt/sla-15-1mt-book.html

iSAC Codec Support

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

Key Replacement for Digitally Signed Cisco Software

The Key Replacement for Digitally Signed Cisco Software feature provides a mechanism to replace public keys on a Cisco router or switch that are used to verify the authenticity of the software image.

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

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_dgtly_sgnd_sw.html

Layer 2 Switch Port Manageability MIBs

The Layer 2 Ethernet Switching Interface BRIDGE-MIB is supported in the Cisco 1861 platform. The BRIDGE-MIB enables the user to know the Media Access Control (MAC) addresses and spanning tree information of the Ethernet switch modules. The user can query the MIB agent using the SNMP protocol and get the details of Ethernet switch modules such as MAC addresses of each interfaces and spanning protocol information.

The Bridge-MIB uses the following approaches to get the Layer 2 BRIDGE-MIB information:

- Community string based approach
- Context based approach

In the community string based approach, one community string is created for each VLAN. Based on the query, the respective VLAN MIB is displayed.

In the context based approach, the SNMP context mapping commands are used to display the values for the L2 interfaces information. Each VLAN is mapped to a context. When the user queries with a context, the MIB displays the data for that specific VLAN which is mapped to the context. In this approach, each VLAN is manually mapped to a context.

For more details to configure and retrieve the BRIDGE-MIB details, see the Release Notes and Technical Notes at:

http://www.cisco.com/en/US/docs/ios/15_0/15_0x/15_01_XA/rn1800xa.html#wp422468

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a9b.shtml#brgmib

LDAP Integration with Active Directory

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

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_accountg.html

LDAP/AD Support for Authproxy

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

http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authentifcn_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1001230

MLPP Support for Supplementary Services on SCCP Controlled Analog Endpoints

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

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

MPLS MTU Command for GRE Tunnels

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mp_l2_vpns/configuration/15-1mt/mp-any-transport.html

Parser Concurrency and Locking Improvements

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

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_config-lock.html

QoS Policing Support on Switched Virtual Interfaces (SVIs)

The **police** command was modified to include support for policing on Switched Virtual Interfaces (SVIs) for the Cisco1800, 2800, and 3800 series integrated services routers.

Reuse MAC for ATM RBE

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

http://www.cisco.com/en/US/docs/ios/atm/configuration/guide/atm_reuse_MAC_for_ATM_RBE.html

RFC4040 Based Clear Channel Codec Signaling with SIP

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

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

RSA 4096-Bit Key Generation in SW Crypto Engine Support

The range value for **the modulus** keyword value for the **crypto key generate rsa** command is extended from 360 to 2048 bits to 360 to 4096 bits.

This change impacts the following Cisco documents:

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

In the following document the **crypto key generate rsa** command was updated:

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

Serviceability Support for SIP Dialer and Call Progress Analysis

Cisco IOS Release 15.1(1)T adds two command line interface (CLI) commands for Call Progress Analysis (CPA) monitoring and diagnostics:

test dsp cpa *slot dsp* **message**

This command enables or disables printing of CPA messages to the console or/and the syslog.

test dsp cpa *slot dsp* **parameter**

This command displays or resets CPA parameters.

SG3 Fax Support

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

http://www.cisco.com/en/US/docs/ios/voice/fax/configuration/guide/vf_cfg_t38_fxrly.html

SIP—TLS/TCP and SRTP with SRST

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/firmware/8_5_3/english/release/notes/7900_853.html

SIP IPv6—ANAT Support

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

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

SSL VPN Phase-4 Features

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.html

SSLVPN DVTI 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_ssl_vpn.html

Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP to SIP Calls

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

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb_10022.html

Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

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 Interworking Between RSVP Capable 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_10021.html

Support for MGCP 1.0 Call Control for SRTP on Cisco IOS Gateways

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

http://www.cisco.com/en/US/docs/ios/voice/mgcp/configuration/guide/15_0/vm_15_0_book.html

Support for MIB to Report Call Volume and Call Rate Related Statistics 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-gw-roadmap.html

Support for Multiple Registrars on SIP Trunks on a Cisco Unified Border Element, on Cisco IOS SIP TDM Gateways, and on Cisco Unified Communications Manager Express

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

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

Support for PAI, PPI and Privacy Headers on the SIP Trunk of CUCME with Either SIP or SCCP Line-Side

Support for PAI, PPI, and Privacy Headers on the Cisco Unified CME SIP trunk. When enabled, Calling Number, Calling Name, and Privacy information is sent using PAI, PPI, and Privacy headers over the SIP trunk of Cisco Unified CME. This feature also enables interworking between the Remote-Party-ID (RPID) information contained in SIP line-side messages to PAI, PPI, and Privacy header information on the SIP trunk.

Support for SIP 181 Call is Being Forwarded Message

Support for SIP 181 Call is Being Forwarded message was added to Cisco IOS SIP TDM gateways and Cisco Unified Border Elements (Cisco UBEs). This feature is enabled by default. To disable this feature for all SIP 181 messages or for SIP 181 message either with or without SDP, see the **block** and **voice-class sip block** commands in the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html.

On the Cisco UBE, this feature also adds the ability to receive SIP 181 messages on one leg and send out SIP 183 messages on the other leg. For details about enabling this feature on a Cisco UBE, see the **map resp-code** and **voice-class sip map resp-code** commands in the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html.

Support for Stripping Off Progress Indication from Incoming ISDN Messages on SIP and H323 TDM Gateways

Support for stripping off progress indicator (PI) from incoming Q.931 CALL-PROCEEDING message on Cisco IOS SIP and H.323 gateways and on Cisco UBEs. Configuration of this feature determines whether an incoming Q.931 CALL-PROCEEDING message with a PI value results in a SIP 183 message or H.323 Progress message. This behavior allows interworking with third-party SIP and H.323 servers. For details about enabling this feature, see the **progress_ind** command in the *Cisco IOS Voice Command Reference* at http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html.

Tcl UDP and VRF Support

The Tcl UDP and VRF feature provides support for UDP sockets. This feature also provides VRF support for all Tcl sockets, including both UDP and TCP sockets.

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

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

Transport 802.1q and 802.1p Tags over ATM PVCs

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

Web Services Management Agent with TLS

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

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

Zone Based Firewall (ZBFW) Usability and Manageability Features

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

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

Important Notes

The following information applies to all releases of Cisco IOS Release 15.1(1)T.

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(1)T5

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T5:

- The 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

Cisco IOS Release 15.1(1)T4

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T4:

- 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 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/15-2mt/sec-conn-sslvpn-ssl-vpn.html#GUID-33399B8A-875B-42E9-BA7F-375F68B64208

Cisco IOS Release 15.1(1)T3

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T3:

- 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.

- TCP keepalive sessions are terminated when a host behind a zone-based policy firewall disconnects ungracefully.

  Old Behavior: When a host behind a zone-based policy firewall disconnectes ungracefully and loses the TCP connection information, TCP keepalive sessions are terminated on the other endpoint after the TCP keepalive times out.

New Behavior: When a zone-based policy firewall is enabled for TCP keepalive traffic and the host behind the firewall is undergoing an ungraceful disconnect, TCP keepalive works only when the configured TCP timeout is complete. On receiving an out of window reset (RST) packet, the firewall sends an empty acknowledge (ACK) packet to the initiator of the RST packet. This ACK will have the current sequence (SEQ) and ACK number from the firewall session. On receiving this ACK, the client sends an RST packet with the SEQ number that is equal to the ACK number in ACK packet. The firewall processes this RST packet, clears the firewall session, and passes the RST packet.

Additional Information:

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

- 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

- 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/bbdsl/command/reference/bba_book.html

- New command, **ntp panic update,** 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

Cisco IOS Release 15.1(1)T2

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T2:

- New CLI 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

- 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

Cisco IOS Release 15.1(1)T1

The following behavior changes are introduced in Cisco IOS Release 15.1(1)T1:

- DHCP server sends infinite lease time to the clients.

  Old Behavior: DHCP server does not send infinite lease time to the clients for which manual bindings are configured.

  New Behavior: DHCP server sends infinite lease time to the clients for which manual bindings are configured.

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

- Keyword removed from the **ip nat service** command.

  Old Behavior: The **ip nat service** CLI included the **enable-mib** keyword

  New Behavior: The **enable-mib** keyword has been deprecated from the **ip nat service** CLI.

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

- The **cns config notify** command is not supported.

  Old Behavior: The **cns config notify** command was supported.

New Behavior: The **cns config notify** command will be hidden and not supported effective with Cisco IOS Release 15.1(1)T1.

Additional Information:
http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_04.html#wp1083435

- Change to BGP path selection.

  Old Behavior: BGP selects paths which are not the oldest paths for multipath. This causes BGP to unnecessarily flap from multipath to non-multipath as a result of route flaps

  New Behavior: BGP uses the best-path selection algorithm to find a set of equally good routes. These routes are the potential multipaths. In Cisco IOS Release 12.2(33)SRD and later releases, when there are more equally good multipaths available than the maximum permitted number, then the oldest paths are selected as multipaths.

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

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

- Behavior change for auto-summary (BGP) command.

  Old Behavior: When a connected route is automatically summarized by the auto-summary (BGP) command, the route is not deleted from the BGP routing table if the interface assigned that address is shut down.

  New Behavior: When a connected route is automatically summarized by the auto-summary (BGP) command, the route is properly deleted from the BGP routing table if the interface assigned that address is shut down.

  For more information, see the auto-summary (BGP) command:
  http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp1.html

- 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

- The **no** form of the **ip nhrp map multicast dyn** command clears all dynamic entries in the multicast table.

  Old Behavior: Dynamic entries in the multicast table are not cleared even though the hold time has expired and the **ip nhrp map multicast dyn** command is disabled, which disables the automatic addition of routers to the multicast mappings by NHRP.

  New Behavior: All dynamic entries in the multicast table are now cleared when the hold time has expired and the **ip nhrp map multicast dyn** command is disabled.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_nhrp.html#wp1011428

- Input error counter is the sum of all error types.

  Old Behavior: Each errored packet in the input error counter can report multiple errors, such as CRC, framing, and abort.

  New Behavior: Each errored packet in the input error counter reports only one specific error.

  Additional Information: The following modules are affected:

  WIC-1T,

  WIC-2T,

  WIC-2A/S,

  HWIC-1T,

  HWIC-2T,

  HWIC-2A/S,

  VWIC-xMFT-T1 (or E1),

  VWIC2-xMFT-T1/E1,

  WIC-1DSU-T1-V2,

  HWIC-1DSU-T1,

  WIC-1B-U-V2,

  WIC-1B-S/T-V3,

  HWIC-1B-U (12.4 mainline only),

  WIC-xAM,

  WIC-xAM-V2

  The HWIC and WIC slots in the following platforms are affected:

  Cisco 1841

  Cisco 2691

  Cisco 2801

  Cisco 2811, Cisco c2821,Cisco c2851

  Cisco 3725, Cisco 3745

- The primary Key Server (KS) now displays a registered Group Encrypted Transport VPN Mode (GM) that is properly encrypting traffic.

  Old Behavior: When cooperative key server key distribution occurs, one KS declares itself as the primary KS, creates a policy, and sends out the policy to the other secondary KS. The secondary KS continues to wait before declaring the primary KS as the primary KS and continues to stay in election mode, but since both the primary and secondary KS have a policy, the GM registration succeeds.

  New Behavior: When cooperative key server key distribution occurs, one KS declares itself as primary, creates a policy, and sends the policy to the other secondary KS. The secondary KS declares the primary KS as primary KS when it gets the policy and ends the election mode. The secondary KS now also blocks GM registration while the cooperative key server key distribution is in progress. This change allows the cooperative key server distribution to become more efficient because it saves time. For example, the following syslog warning message is displayed:

  ```
  00:00:16: %GDOI-5-COOP_KS_BLOCK_NEW_GM_REGISTER_ELECTION: This KS temporarily blocks
  GM with ip-addr 10.0.4.1 from registering in group diffint as the KS election is
  underway
  ```

Additional Information: The Cooperative Key Server section in the Cisco Group Encrypted Transport VPN feature document was updated to reflect this change:

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

- The auto configuration options are added to the DSL group.

  Old Behavior: DSL group did not have auto configuration options. Only manual configuration was allowed.

  New Behavior: DSL group provides auto configuration options such as default, exit, no, and shdsl.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_d1.html#wp1039345

- The SIP-KPML option is added to the **dtmf-relay** command in voice register pool mode.

  Old Behavior: Only three types of audio relay methods were supported in the **dtmf-relay** command under voice register pool.

  New Behavior: SIP-KPML option is added as the fourth type of audio relay method in the **dtmf-relay** command under voice register pool in Cisco Unified CME and Cisco Unified SRST.

  Additional information:
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_d1ht.html#wp1048382

- Error message is displayed when you try applying the tunnel interface to a crypto map.

  Old Behavior: Error message is not displayed when you try applying the tunnel interface to a crypto map using the **crypto map** (interface IPSec) command.

  New Behavior: An error message is displayed when you try applying the tunnel interface to a crypto map using the **crypto map** (interface IPSec) command.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c4.html#wp1060970

- 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(1)T

This section describes important issue that you should be aware of for Cisco IOS Release 15.1(1)T and later releases.

CISCO-RTTMON-MIB.oid Is Not Supported in the Universal IP Base IOS Technology Package

The Cisco IP Service Letter Agreements (SLAs) responder on a Cisco 2900 series Integrated Service Router (ISR) with the universal ipbasek9 technology package operates as expected. However, any attempt to utilize snmpset or snmpget to retrieve the CiscoRttMonMIB (.1.3.6.1.4.1.9.9.42) module instance identifiers (OIDs) will fail (issuing the **show snmp mib | include rttMonApplResponder** command displays an empty list).

To provide support for snmpset or snmpget and the CISCO-RTTMON-MIB on a Cisco ISR Generation 2 (G2), activate an evaluation license for one of the following technology packages on the Cisco ISR G2: datak9, securityk9, or uck9. Note that evaluation licenses automatically become Right to Use licenses after the initial evaluation period.

Additional Information:

Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2

Class Calculated Percentage Rate Value

Cisco IOS software ensures that a class's calculated percentage rate value is valid before associating it with an interface.

Old Behavior: When a class with bandwidth, priority, or shape is associated with an interface, Cisco IOS software does not check the class's calculated percentage rate value.

New Behavior: When a class with bandwidth or priority is associated with an interface, Cisco IOS software checks the class's calculated percentage rate value. The value must be between 8 and 2,000,000 kbps. When a class with shape is associated with an interface, Cisco IOS software checks the class's calculated percentage rate value. The value must be between 8,000 and 1,000,000,000 bps. If the values are outside of these ranges, Cisco IOS software does not allow the class to be associated with the interface.

Additional Information:

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_a1.html#wp1011774

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_n1.html#wp1048842

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_s1.html#wp1060033