

New and Changed Information

This section lists the new hardware and software features that are supported in Cisco IOS Release 15.0M and contains the following sections:

- [New Software Features Supported in Cisco IOS Release 15.0\(1\)M6, page 57](#)
- [New Hardware Features Supported in Cisco IOS Release 15.0\(1\)M3, page 57](#)
- [New Software Features Supported in Cisco IOS Release 15.0\(1\)M3, page 58](#)
- [New Hardware Features Supported in Cisco IOS Release 15.0\(1\)M2, page 59](#)
- [New Software Features Supported in Cisco IOS Release 15.0\(1\)M2, page 59](#)
- [New Hardware Features Supported in Cisco IOS Release 15.0\(1\)M, page 60](#)
- [New Software Features Supported in Cisco IOS Release 15.0\(1\)M, page 63](#)



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>.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://www.cisco.com/go/mibs>

New Software Features Supported in Cisco IOS Release 15.0(1)M6

This section describes new and changed features in Cisco IOS Release 15.0(1)M6. Some features may be new to Cisco IOS Release 15.0(1)M6 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 15.0(1)M6. 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

This feature enhances Cisco IOS licensing CLIs and MIBs to track Right To Use (RTU) licenses 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 15.0(1)M3

This section describes new and changed features in Cisco IOS Release 15.0(1)M3. Some features may be new to Cisco IOS Release 15.0(1)M3 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 15.0(1)M3. 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 15.0(1)M3 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
- Cisco Unified Border Element
- 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 15.0(1)M3

This section describes new and changed features in Cisco IOS Release 15.0(1)M3. Some features may be new to Cisco IOS Release 15.0(1)M3 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 15.0(1)M3. 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 15.0(1)M2

This section describes new and changed features in Cisco IOS Release 15.0(1)M2. Some features may be new to Cisco IOS Release 15.0(1)M2 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 15.0(1)M2. 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.

Cisco 1905 and Cisco 1921 Integrated Services Routers Generation 2

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

**Note**

The Cisco 1905 ISR with 256MB RAM does not support the netboot or warm upgrade features. This is a limitation due to memory constraints. Customers need to purchase an extended memory license to upgrade to 512MB RAM if they want to use the netboot or warm upgrade features.

New Software Features Supported in Cisco IOS Release 15.0(1)M2

This section describes new and changed features in Cisco IOS Release 15.0(1)M2. Some features may be new to Cisco IOS Release 15.0(1)M2 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 15.0(1)M2. 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.

EnergyWise Branch Routers

Cisco EnergyWise is a technology that measures, monitors, and manages the power usage of powered devices, Cisco devices in a domain, and the endpoints connected to them. The endpoints communicate with the power management station through Cisco devices, such as the Cisco 1900 series routers, Cisco 2900 series routers, and Cisco 3900 series routers.

Key Replacement for Digitally Signed Cisco Software

Key replacement for Digitally Signed Cisco Software 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

Reuse MAC for ATM RBE

The Configurable MAC for ATM point-to-point subinterfaces for Route-Bridge Encapsulation (RBE) feature enables the user to configure the MAC address for the ATM point-to-point subinterfaces using the **atm ether-mac-address** command. This configured MAC address will then be used for the RBE feature, which enables packets from the hosts to be bridged across the ATM connection with unique MAC address per host or connection.

New Hardware Features Supported in Cisco IOS Release 15.0(1)M

This section describes new and changed features in Cisco IOS Release 15.0(1)M. Some features may be new to Cisco IOS Release 15.0(1)M 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 15.0(1)M. 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 HWIC Enhancements

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

<http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/mrwlsgsm.html>

887V 3G, WLAN, and SRST Models

The Cisco 887V integrated services router offers broadband speeds and simplified management to small businesses, enterprise small branches, and teleworkers. Cisco 887V supports the following options:

- 3G backup
- 802.11n wireless LAN access point
- Survivable Remote Site Telephony
- Advanced security, including intrusion prevention, GET VPN, and dynamic multipoint VPN (DMVPN)
- Power over Ethernet (PoE) on two switch ports

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

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

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

C3825-NOVPN and C3845-NOVPN

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

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4_22_yb/rn3800yb.html

Cisco 800 Broadband Series Routers

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

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

Cisco 867, 886, and 887 Series

The Cisco 867, Cisco 886, and Cisco 887 integrated services routers deliver ADSL over POTS (ADSLoPOTS) interface and ADSL over ISDN (ADSLoISDN) interface as the major WAN connection.

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

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

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

Cisco Integrated Services Routers Generation 2

Cisco 1900 Series Integrated Services Routers

The Cisco 1900 series integrated services routers are future-enabled with multicore CPUs, new optional 802.11n capabilities, and new energy monitoring and control capabilities while enhancing overall system performance. Additionally, a new Cisco IOS Software Universal image and Services Ready Engine module enables you to decouple the deployment of hardware and software, providing a stable technology foundation that can quickly adapt to evolving network requirements. The Cisco 1900 series integrated services routers offer embedded hardware encryption acceleration, optional firewall, intrusion prevention, and the industry's widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, and Copper and Fiber GE.

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

www.cisco.com/go/isrg2

Cisco 2900 Series Integrated Services Routers

The Cisco 2900 series integrated services routers platforms are future-enabled with multicore CPUs and support for high-capacity Digital Signal Processors (DSPs) for future enhanced video capabilities, high-powered service modules with improved availability, Gigabit Ethernet switching with enhanced POE, and new energy monitoring and control capabilities while enhancing overall system performance.

Additionally, a new Cisco IOS Software Universal image and Services Ready Engine module enable you to decouple the deployment of hardware and software, providing a flexible technology foundation that can quickly adapt to evolving network requirements.

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

www.cisco.com/go/isrg2

Cisco 3900 Series Integrated Services Routers

The Cisco 3900 series integrated services routers are future-enabled with support for new high-capacity DSPs for future enhanced video capabilities, high-powered service modules with improved availability, multicore CPUs, Gigabit Ethernet switching with enhanced POE, and new energy visibility and control capabilities while enhancing overall system performance. Additionally, a new Cisco IOS Software Universal image and Services Ready Engine module enable you to decouple the deployment of hardware and software, providing a flexible technology foundation that can quickly adapt to evolving network requirements. The Cisco 3900 series integrated services routers offer embedded hardware encryption acceleration, voice- and video-capable DSP slots, optional firewall, intrusion prevention, call processing, voice mail, and application services. In addition, the platform supports the industry's widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, and Copper and Fiber GE.

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

www.cisco.com/go/isrg2

Enhanced EtherSwitch Service Modules

The Cisco enhanced EtherSwitch service modules (SM-ES2-16-P, SM-ES3-16-P, SM-ES3G-16-P, SM-ES2-24, SM-ES2-24-P, SM-ES3-24-P, and SM-ES3G-24-P) provide Cisco 2900 series routers and Cisco 3900 series routers the ability to use Cisco enhanced EtherSwitch service modules as independent Layer 2 and Layer 3 switches when running Cisco IOS software.

Internal Service Modules

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

http://www.cisco.com/en/US/products/ps10598/tsd_products_support_series_home.html

Next Generation Advanced Integration Module

AIM2-CUE

The AIM2-CUE provides support for Cisco Unity Express voice mail, auto attendant, and interactive voice response (IVR) features. The AIM2-CUE is the next generation of the AIM-CUE. The AIM2-CUE provides higher scalability than the AIM-CUE.

The AIM2-CUE is supported on the Cisco 890, Cisco 1841, Cisco 2801, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, and Cisco 3845 series routers on an AIM form factor. For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/products/sw/voicesw/ps5520/>

AIM2-APPRE-104-K9

The AIM2-APPRE-104-K9 is an Application eXtension Platform (AXP). Cisco AXP allows third parties such as system integrators, managed service providers, and large enterprise customers to extend the functionality of Cisco ISRs by providing their own value-added integrated services. On the service

module, Cisco AXP hosts applications in a separate runtime environment with dedicated resources. In addition, Cisco AXP provides application programming interfaces (APIs) that enable functions such as packet analysis, event notification, and network management to be utilized by hosted applications.

The AIM2-APPRE-104-K9 is supported on the Cisco 890, Cisco 1841, Cisco 2801, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, and Cisco 3845 series routers on an AIM form factor. For detailed information about this feature, see the following document:

<http://www.cisco.com/en/US/products/ps9701/index.html>

Next Generation High-Density PVDM3 Modules

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

http://www.cisco.com/en/US/docs/routers/access/1900/software/configuration/guide/pvdm3_config_ps10538_TSD_Products_Configuration_Guide_Chapter.html

Service Module

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

<http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/ism-sm-sre.html>

Services Ready Engine

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

<http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/ism-sm-sre.html>

New Software Features Supported in Cisco IOS Release 15.0(1)M

This section describes new and changed features in Cisco IOS Release 15.0(1)M. Some features may be new to Cisco IOS Release 15.0(1)M 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 15.0(1)M. 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.

802.1P CoS Bit Set for PPP and PPPoE Control Frames

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

http://www.cisco.com/en/US/docs/ios/bbds1/configuration/guide/bba_cos_ppp_pppoe.html

AAA Authorization and Authentication Cache

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

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

AAA per-User Scalability

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.html

AAA Support for Greater than 8 Login and Exec Auth

The maximum size for the following AAA method lists has been enhanced from 8 to 250. Before the maximum size was 8, where 7 named lists could be configured, plus 1 default list. Now, the user can configure 250 (249 named lists plus 1 default list).

1. Login Authentication (**aaa authentication login...**)
2. Exec Authorization (**aaa authorization exec...**)
3. Exec Accounting (**aaa accounting exec...**)

AppleTalk Support Discontinuation

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

http://www.cisco.com/en/US/docs/ios/at/configuration/guide/appletalk_support_discontinuation.html

ATM Conditional Debug Support

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

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

ATM OAM Loopback Mode Detection

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

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

ATM OAM Traffic Reduction

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

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

ATM PVC F5 OAM Recovery Traps

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

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

ATM PVC Trap Enhancements for Segment and End AIS/RDI Failures

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

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

ATM QoS MIB

The Cisco ATM QoS MIB (CISCO-ATM-QOS-MIB) and its defined objects support quality of service (QoS) parameters configured for a virtual channel (VC) over an ATM interface using the following features:

- Shaping traffic on a per-VC basis
- Shaping traffic on a per-virtual path (VP) basis
- Configuring Weighted Random Early Detection (WRED) parameters per VC

**Note**

This MIB is a read-only MIB.

For details, see the CISCO-ATM-QOS-MIB.my file, available through the Cisco MIB FTP site at the following location: <http://tools.cisco.com/ITDIT/MIBS/servlet/index>.

ATM VP Average Traffic Rate

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

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

BFD—Static Route Support

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

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

BFD—VRF Support

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

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

BFD—WAN Interface Support (ATM, FR, POS, and Serial)

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

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

BGP Event-Based VPN Import

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

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

BGP Per Neighbor Graceful Restart Configuration

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

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

BGP RT Changes Without PE-CE Neighbor Impact

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

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

Calling Station ID Attribute 31

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

http://www.cisco.com/en/US/docs/ios/isg/command/reference/isg_m1.html#wp1303641

Cisco IOS Firewall Support for TRP—Phase 2

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

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

Cisco IOS IPS with Lightweight Signatures

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

Cisco Services for IPS on Cisco IOS

The Cisco Services for IPS on Cisco IOS feature enforces the presence of a valid IPS subscription license when signatures are loaded on a router where the Cisco IOS IPS feature is turned on.

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

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

Cisco Unified Border Element Support for Configurable Pass-Through of SIP INVITE Parameters

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#wp1376226>

Cisco Unified Border Element Support for Generating Out-of-Dialog SIP OPTIONS Ping Messages to Monitor SIP Servers

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#wp1345256>

Cisco Unified Border Element Support for SRTP-RTP Internetworking

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_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Configurable SIP Parameters via DHCP

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#wp1344896>

DHCP Client FORCERENEW Message

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

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

DHCP Client Option 121

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

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

Digitally Signed Cisco Software

The Digitally Signed Cisco Software feature introduces technology to verify and validate the software origin and integrity for system software that is loaded into Cisco products. Newer products are being outfitted with software verification technology, and software is being digitally signed using secure asymmetrical (public-key) cryptography. Such software is referred to as digitally signed software.

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

DMVPN—Tunnel Health Monitoring and Recovery

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

DMVPN—Tunnel Health Monitoring and Recovery (Interface Line Control)

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

DMVPN—Tunnel Health Monitoring and Recovery (Syslog)

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

Embedded Event Manager (EEM) 3.1

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

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

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

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

Extended NAS-Port-Type and NAS-Port Support

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

http://www.cisco.com/en/US/docs/ios/bbdsi/configuration/guide/bba_extd_nas_port.html

Flexible NetFlow—Ingress VRF Support

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

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon.html

Flexible NetFlow—NBAR Application Recognition

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

http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/cust_fnflow_rec_mon.html

Forced Update to SIP Parameters via DHCP

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#wp1391051>

FPM—Packaging, eTCDF, and Full Packet Search Enhancements

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

G.722 Codec Support with SRST

Support is provided for the G.722 codec in Cisco Unified SRST mode. To enable this capability, enter the **codec g722-64k** command in call-manager-fallback configuration mode.

When this command is entered, the G.722 codec is considered to be the SRST codec, provided the phone supports that codec capability. For phones that do not support the G.722 codec, the phones will fall back to the G.711 codec.

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

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/command/reference/srsa_a_m.html#wp1323319

GET VPN VRF-Aware GDOI on GM

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

H.323 Calling Without a Calling Number

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

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_n1.html#wp1024844

IGMP Static Group Range Support

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

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_igmp_static_rng.html

iLBC Codec on SCCP Analog FXS Gateway, Transcoding, and Conferencing; G.722-64K for H.323 & SIP

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

http://www.cisco.com/en/US/docs/ios/voice/cminterop/configuration/guide/vc_enh_confr_vgr.html

IP Multicast Load Splitting—Equal Cost Multipath Using S, G, and Next-Hop

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

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_load_splt_ecmp.html

IPv6: Multicast Address Group Range Support

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

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

IS-IS MIB

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

http://www.cisco.com/en/US/docs/ios/iproute_isis/configuration/guide/irs_mib.html

IS-IS—MPLS LDP Autoconfiguration

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

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

IS-IS—MPLS LDP Synchronization

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

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

IS-IS Support for an IS-IS Instance per VRF for IP

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

http://www.cisco.com/en/US/docs/ios/iproute_isis/configuration/guide/irs_instance_vrf.html

Lawful Intercept

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

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

Licensing Support for Cisco IOS SSLVPNs

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

MLP LFI over ATM Configuration Scaling

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

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

MPLS VPN—BGP Local Convergence

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

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

MPLS VPN—Inter-AS Option AB

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

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

MTR Support for Multicast

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

http://www.cisco.com/en/US/docs/ios/mtr/configuration/guide/multi-top_rtng.html

Multicast Address Group Range Support

The Multicast Address Group Range Support feature enhances multicast access control by introducing the capability to define a global range of multicast groups and channels to be permitted or denied using the **ip multicast group-range** command.

Multicast MIB VRF Support

The Multicast MIB VRF Support feature is an enhancement to help manage Cisco devices in a multicast VPN (MVPN) environment using SNMP. This feature enhances the Cisco suite of supported multicast MIBs by making the following multicast MIBs VRF aware:

- CISCO-IPMROUTE-MIB
- CISCO-PIM-MIB
- IGMP-STD-MIB
- IPMROUTE-STD-MIB
- MSDP-MIB
- PIM-MIB

Multicast VRF (MVRF) awareness enables the MIB objects associated with these multicast MIBs to be queried and set for the individual MVRFs configured. In addition, MVRF awareness provides the capability to detect conditions for a trap inside of an MVRF and look up the correct information for that MVRF; the traps would then be sent to the SNMP manager that is configured for that MVRF.

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>.

Multicast VPN Extranet Support

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

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_mc_vpn_extranet.html

Multicast VPN Extranet VRF Select

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

http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_mc_vpn_extranet.html

Multipart SDP Support for NAT/FPG

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

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

NAS-Port ID Format C Enhancement:

This feature introduces the **nas-port-id format c** command for Broadband Access Group (BBA group) configuration. This command defines a specific broadband subscriber access line identification (NAS-Port-ID) coding format. When this command is configured, the original value of the NAS-Port-ID tag is overwritten. For more details, see the *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*.

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

http://www.cisco.com/en/US/docs/ios/bbdsi/configuration/guide/bba_nas_id_c.html

NAT Static and Dynamic Route-Map Name-Sharing

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

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

NSSA-Only

The NSSA-Only feature can be used to restrict the scope of routes that are imported into NSSA areas. The following commands were modified by this feature: **area nssa**, **redistribute (IP)**, **set level**, **show ip opsf**, and **summary-address**.

For more information about configuring this feature, see these commands in the *Cisco IOS IP Routing: Protocol Independent Command Reference*:

http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_book.html

Option to Disable Volume-Based IPsec Lifetime Rekey

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_vpn_ipsec.html

OSPF Graceful Shutdown

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

http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_ttl.html

OSPF TTL Security Check

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

http://www.cisco.com/en/US/docs/ios/iproute_ospf/configuration/guide/iro_ttl.html

OSPFv3 Fast Convergence—LSA and SPF Throttling

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

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

OSPFv3 Graceful Restart

For detailed information about this feature, see the following document:
<http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf.html>

PfR EIGRP mGRE DMVPN Hub-and-Spoke Support

For detailed information about this feature, see the following document:
<http://www.cisco.com/en/US/docs/ios/oer/configuration/guide/pfr-eigrp.html>

PIM Stub

For detailed information about this feature, see the following document:
http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_stub_routing.html

PIM Triggered Joins

For detailed information about this feature, see the following document:
http://www.cisco.com/en/US/docs/ios/ipmulti/configuration/guide/imc_pim_triggered_joins.html

PKI High Availability

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_auth_rev_cert.html

PPP CLI Enhancement for L2CP Phase III

The **show ppp interface** command is enhanced to display all the sessions under a particular Ethernet or ATM interface. If there are multiple sessions under an interface, this command displays detailed PPP information for all the sessions. For detailed information about this command, see the *Cisco IOS Broadband Access Aggregation and DSL Command Reference*.

The **show caller user** command is enhanced to display additional information on virtual access interfaces and VCD information if the session is bound to an ATM interface. For detailed information about this command, see the *Cisco IOS Dial Technologies Command Reference*.

PPP-Max-Payload and IWF PPPoE Tag Support

For detailed information about this feature, see the following document:
http://www.cisco.com/en/US/docs/ios/bbdsi/configuration/guide/bba_ppp_mx_payld.html

PPPoE Agent Remote ID and DSL Line Characteristics Enhancement

For detailed information about this feature, see the following document:
http://www.cisco.com/en/US/docs/ios/bbdsi/configuration/guide/bba_rmtid_dsl.html

PPPoE—Session Limiting on Inner QinQ VLAN

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

http://www.cisco.com/en/US/docs/ios/bbds1/configuration/guide/bba_qinq_vlan_limt.html

PPPoE Smart Server Selection

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

http://www.cisco.com/en/US/docs/ios/bbds1/configuration/guide/bba_pppoe_sss.html

Preloaded Routes for Outgoing INVITE on a Cisco Unified Border Element Using a Path Header in REGISTER, Service-Route in 200 OK Response to REGISTER and Outbound Proxy

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_ps6441_TSD_Products_Configuration_Guide_Chapter.html

RSVP Fast Local Repair

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

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

RSVP Interface-Based Receiver Proxy

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

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

RSVP—VRF Lite Admission Control

The RSVP—VRF Lite Admission Control feature introduces support for Resource Reservation Protocol (RSVP) call admission control (CAC) in an IP session within the context of a virtual routing and forwarding (VRF) instance.

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

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

RTSP Live Streaming and Max Time for Cisco IOS VoiceXML Browser

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

- *Cisco IOS Tcl IVR and VoiceXML Application Guide* at http://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/tcl_c.html
- *Cisco VoiceXML Programmer's Guide* at <http://www.cisco.com/en/US/docs/ios/voice/vxml/developer/guide/vxmlprg.html>

Service Advertisement Framework

The Cisco Service Advertisement Framework feature provides a service-discovery framework that allows applications to discover the existence, location, and configuration of networked resources within networks. Cisco SAF allows a timely and reliable awareness of the services within networks when applications advertise and discover services on networks.

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

- *Cisco Service Advertisement Framework* feature module at http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/saf_cg.html
- *Cisco IOS Service Advertisement Framework Command Reference* feature module at http://www.cisco.com/en/US/docs/ios/saf/command/reference/saf_book.html

SSHv2 Enhancements for RSA Keys

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

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

SSLVPN Client Side Certificate-Based Authentication

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 Adjustable Timers for REGISTRATION Refresh and Retries

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#wpxref66062>

Support for Distinctive Ringing on SCCP IOS Gateways

The Support for Distinctive Ringing on SCCP IOS Gateways feature enables setting of a distinct ring tone to alert the user whether an incoming call is from an internal or external phone. For more information, see the **ring cadence** command in the *Cisco IOS Voice Command Reference*.

Support for FAC and Speed Dial to Voice Mail Using Three Numerical Digits

In Cisco IOS Release 15.0(1)M and later releases, you can configure all-numeric three- or four-digit flexible feature access codes so that users are not required to dial a prefix or special characters. For example, if you configure a feature code of 788 for Call Forward Cancel, the phone user dials just the feature code (788) to access that feature. For more information, see the following document:

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

Support for PAI, PPI, Privacy, P-Called-Party-ID, and P-Associated-URI Headers on 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-sipsip_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Support for Selectively Using SIP: URI or Tel: URI Formats on Individual 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#wpxref16579>

Support on Cisco Unified Border Element for Selective Filtering of Outgoing Provisional Responses

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#wp1393468>

Suppress BGP Advertisement for Inactive Routes

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

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

Unified Communications Trusted Firewall Control Version II

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

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

Voice Quality Enhancements on Cisco Unified Border Element Platforms

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

VRF Aware RSVP Agent and Gateway

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

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

WCCP: VRF Support

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

http://www.cisco.com/en/US/docs/ios/ipapp/configuration/guide/ipapp_wccp.html

Zone-Based Firewall 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_policy_firew.html

MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

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

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

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

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

Limitations and Restrictions

If the routed port on an NM-16ESW is used in a topology that has physical loop, the unknown multicast packets (such as HSRP and OSPF multicast hello packets) will be flooded and will form a loop. Instead, use switchports of NM-16ESW and don't use the routed port for this environment.

Important Notes

The following information applies to all releases of Cisco IOS Release 15.0M.

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 standalone 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 15.0\(1\)M7, page 78](#)
- [Cisco IOS Release 15.0\(1\)M6, page 78](#)
- [Cisco IOS Release 15.0\(1\)M5, page 79](#)
- [Cisco IOS Release 15.0\(1\)M4, page 80](#)

- [Cisco IOS Release 15.0\(1\)M3, page 81](#)
- [Cisco IOS Release 15.0\(1\)M2, page 85](#)
- [Cisco IOS Release 15.0\(1\)M1, page 87](#)

Cisco IOS Release 15.0(1)M7

The following behavior changes are introduced in Cisco IOS Release 15.0(1)M7:

- 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-ssl-vpn-ssl-vpn.html#GUID-33399B8A-875B-42E9-BA7F-375F68B64208

Cisco IOS Release 15.0(1)M6

The following behavior changes are introduced in Cisco IOS Release 15.0(1)M6:

- 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.
- Added New Commands.
 Old Behavior: N/A
 New Behavior: These new commands are used to revert the IPHC format of compression and decompression to the non-RFC-compliant format.
 The latest command pages are available at:
ip header-compression old-iphc-comp:
http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_i1.html#wp1065764
ip header-compression old-iphc-decomp:
http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_i1.html#wp1066790
- **Background save interval** command allows user to turn off auto save feature.
 Old Behavior: Telephony feature causes frequent CPU spikes when large configurations are present and when auto save is enabled. Calls may experience performance issues or fail to initiate.
 New Behavior: New configuration CLI allows user to turn off auto save feature.
 Additional Information:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/command/reference/cme_b1ht.html#wp1030564
- 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

Cisco IOS Release 15.0(1)M5

The following behavior changes are introduced in Cisco IOS Release 15.0(1)M5:

- Default Maximum 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/partner/docs/ios/qos/command/reference/qos_q1.html#wp1075320

- Prevent ARP packet drop by setting ARP packet priority.

Old Behavior: Network congestion causes ARP packets to drop because the ARP packet priority is not enabled.

New Behavior: A new command, **arp packet-priority enable**, was added. Use the **arp packet-priority enable** command when network congestion causes ARP packets to drop. Enabling ARP packet priority significantly reduces the number of ARP packet drops.

Additional Information:

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

- 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.

- 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>
- 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."
```
- Voice register pool description containing spaces gets lost after reload
 Old Behavior: In Cisco IOS Releases 15.0(1)M2 and 12.4(22)T, when a description for a Register Pool contained a space, i.e., "John Doe," the description would disappear after the configuration was reloaded.
 New Behavior: Any descriptors containing spaces are now preserved after router reboot. Quotation marks are not mandatory, but can be used if desired.
- 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

Cisco IOS Release 15.0(1)M4

The following behavior changes are introduced in Cisco IOS Release 15.0(1)M4:

- 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 is 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
- Numeric hostname support is added to the CLI.
 Old Behavior: If a hostname with all numerals is specified, an error is returned and the hostname is not saved.
 New Behavior: If an all-numeric hostname is specified, an error will be returned but the numeric hostname will still be saved.

Additional Information:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html

- CLI is changed to remove the **log** entry from the **permit ip any any log** command.

Old Behavior: To remove the **log** option from the **permit ip any any log** command, use the **no permit ip any any log** and the **permit ip any any** commands.

New Behavior: To remove the **log** entry and the user-defined cookie, use the **permit ip any any [word]** command.

Additional Information:
http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_p1.html#wp1077059
- An error message is displayed when you try applying the tunnel interface to a crypto map.

Old Behavior: An 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
- 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 CLI is changed to disable pipelining for URLF requests to the Trend Server.

Old Behavior: The Trend Router Provisioning Server (TRPS) does not provide the functionality to turn on or off the TRPS pipeline requests.

New Behavior: The 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
- Right to Use license is added for Cisco 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

Cisco IOS Release 15.0(1)M3

The following behavior changes are introduced in Cisco IOS Release 15.0(1)M3:

- The **right-to-left** keyword is added to the **domain** (AAA) command.

Old Behavior: Using the **domain** command and the **stripping** keyword in dynamic authorization local server configuration mode, a string can be terminated at the first delimiter going from left to right only in order to configure username domain options for the RADIUS application.

New Behavior: In addition to using the **domain** command and the **stripping** keyword to terminate at the first delimiter going from left to right only in order to configure username domain options for the RADIUS application, the **right-to-left** keyword can be added after the **domain** command and **stripping** keyword in dynamic authorization local server configuration mode to allow a string to be terminated at the first delimiter going from right to left in order to configure username domain options for the RADIUS application.

Additional Information: The following documents were updated to reflect this change to the **domain** command:

Cisco IOS Security Configuration Guide:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_d2.html#wp1037886

Lawful Intercept:

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

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

The Define Interface Policy-Map AV Pairs AAA Feature:

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

Configuring Authentication:

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

- The **error throttling** command is supported on E1 controllers.

Old Behavior: The **error throttling** command can be enabled only on T1 controllers.

New Behavior: The **error throttling** command can also be enabled on E1 controllers of a channelized E3 port adapter.

Additional Information:

http://www.cisco.com/en/US/docs/ios/interface/command/reference/ir_d1.html#wp1015132

- 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 because 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

- 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_ps10592_TSD_Products_Configuration_Guide_Chapter.html#wp1155880
- Keyword removed from the **ip nat service** command.

Old Behavior: The **ip nat service** command includes the **enable-mib** keyword.

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

Important Information:

http://www.cisco.com/en/US/docs/ios/ipaddr/command/reference/iad_nat.html#wp1049948
- The **cns config notify** command is not supported. A note has been added with this information.

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

New Behavior: The **cns config notify** command is hidden and not supported.

Additional Information:

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_04.html#wp1083435
- Long filenames are now truncated differently.

Old Behavior: A filename longer than six characters is truncated to the first six characters and suffixed with “~1.”

New Behavior: Long filenames are now truncated to the first six characters and suffixed with “~” followed by a numeral. The numeral changes incrementally if a naming conflict is identified.
- BGP selects oldest paths as multipaths.

Old Behavior: BGP selects paths that are not the oldest paths for multipaths. This causes BGP to flap unnecessarily from multipaths to nonmultipaths 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. When there are more equally good multipaths available than the maximum permitted number, 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.

Additional Information:

http://www.cisco.com/en/US/docs/ios/iproute_bgp/command/reference/irg_bgp1.html

- Command accounting and command authorization is 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:

- HWIC-1B-U (12.4 mainline only)
- HWIC-1DSU-T1
- HWIC-1T
- HWIC-2A/S
- HWIC-2T
- WIC-1T
- WIC-2A/S
- WIC-2T
- VWIC-xMFT-T1 (or E1)
- VWIC2-xMFT-T1/E1
- WIC-1B-U-V2
- WIC-1B-S/T-V3
- WIC-1DSU-T1-V2

- 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 2821
 - Cisco 2851
 - Cisco 3725
 - Cisco 3745
- Support was removed from ATM and inverse multiplexing over ATM (IMA) interfaces.
Old Behavior: The **bfd echo** and **bfd interval** commands support ATM and IMA interfaces.
New Behavior: The **bfd echo** and **bfd interval** commands do not support ATM and IMA interfaces.
Additional Information:
http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#wp1036236
http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#wp1036357
 - Upper limit MTU value for POS interfaces is changed across all Cisco 7200 branches.
Old Behavior: The maximum MTU size that can be configured on POS interfaces is 117,994.
New Behavior: The maximum MTU size that can be configured on POS interfaces is 9216.
Additional Information:
http://www.cisco.com/en/US/docs/interfaces_modules/port_adapters/install_upgrade/multichannel_serial/pa-pos-1oc3_install_config/6514conf.html#wp1041110
http://www.cisco.com/en/US/docs/interfaces_modules/port_adapters/install_upgrade/multichannel_serial/pa-pos-2oc3_install_config/3028conf.html#wp1028535

Cisco IOS Release 15.0(1)M2

The following behavior changes are introduced in Cisco IOS Release 15.0(1)M2:

- Added the **atm ether-mac-address** command to the ATM command reference.
Old Behavior: The **atm ether-mac-address** command was not available.
New Behavior: The **atm ether-mac-address** command is available.
Additional Information:
http://www.cisco.com/en/US/docs/ios/atm/command/reference/atm_a1.html#wp1046973
- Added **ip header-compression special-vj** and **special-vj** commands.
Old Behavior: The TCP special Van Jacobson (VJ) format for header compression is not supported.
New Behavior: Functionality is extended to support the TCP special Van Jacobson (VJ) format for header compression.
- Addition of IVR media prompt function for Cisco IAD 2435.

Old Behavior: Cisco IAD 2435 fails to play IVR media prompts.

New Behavior: Cisco IAD 2435 will play IVR media prompts when running Cisco IOS Release 15.0(1)M.

Additional Information:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/admin/configuration/guide/cmehbasic.html#wp1182120

- CLI change

Old Behavior: Entries in the NAT table cannot be cleared on SNAT backup router for H.323 RAS traffic. This can happen when the NAT table of the primary router is out of sync with the NAT table of the secondary router as an unintended consequence of the asymmetric queuing feature being enabled. This problem does not occur if the asymmetric queuing feature is disabled. Asymmetric routing for SNAT will work properly regardless of whether as-queuing is enabled or disabled.

New Behavior: The **as-queuing** keyword for the **ip nat stateful** command has been removed so that the asymmetric queuing cannot be enabled. Any out of sync condition between the NAT table of the primary router and the secondary router caused by network latency will resolve itself in a short amount of time.

- CLI change

Old Behavior: An individual entry in the NAT table cannot be cleared. When you enter the **clear ip nat translation** command you get the following error message:

```
%Translation in use, cannot remove
```

New Behavior: NAT entries can be deleted using any of following three CLI changes:

1. Use the **clear ip nat translation *** command to delete all entries in the NAT table.
2. Use the **clear ip nat translation inside global-ip local-ip** command and press Enter to delete all flow entries associated with that half entry.
3. Use the **clear ip nat translation inside global-ip local-ip forced** command to delete all flow entries associated with that particular half entry.

- CLI change

Old Behavior: A breakpoint exception reload occurs when you configure SNMP traps using Cisco Works and the following errors are displayed:

```
%SNMP-5-WARMSTART: SNMP agent on host is undergoing a warm start
%SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk #####, data #####.
-Process= "NAT MIB Helper", ipl= 0, pid= 277 -Traceback=
```

This symptom is observed after the SNMP server is unconfigured and then configured again. The commands used for this configuration could include **snmp-server enable traps** or **snmp-server community**.

New Behavior: The breakpoint does not occur if NAT MIB support is disabled, which is the default setting. If NAT MIB support is enabled by entering the new **enable-mib** keyword for the **ip nat service** command, breakpoint exception reloads might occur.

- GETVPN:KS when “rekey address ipv4” is not configured.

Old Behavior: If rekey address is not configured in the GDOI group, the **show crypto gdoi ks rekey** command reloads trying to access a null pointer.

New Behavior: If the rekey address is not configured in the GDOI group, the **show crypto gdoi ks rekey** command will show the multicast destination address as “Not Found.”

- H245 address-check command introduced.
 Old Behavior: The gateway automatically closes the gateway TCP connection when the remote side TCP connection attempts to overwrite the data on the existing gateway TCP connection.
 New Behavior: The gateway uses IP addresses to determine which endpoint to close when TCP connections are opened simultaneously. The gateway TCP connection is closed only if the IP address is smaller.
 Additional information:
http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_h1.html
- Increase in object group-based Access Control Entries (ACEs) in Access Control List (ACL) from 256 to 2048.
 Old Behavior: The highest number of object group-based ACEs supported in an ACL is 256.
 New Behavior: The highest number of object group-based ACEs supported in an ACL is 2048.
- The **reason** keyword added to **reload** command.
 Old Behavior: Everything after the **reload** command is treated as the reason string by the parser and if it does not recognize the first word it will be rejected.
 New Behavior: The **reason** keyword was added after the **reload** command to allow the parser to recognize the reason string.
 Additional Information:
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_r1.html#wp1056246
- The transcode feature on Cisco IAD880 series integrated access devices (IADs).
 Old Behavior: The transcoding feature is not available on Cisco IAD880 series IADs.
 New Behavior: Transcoding feature is supported on Cisco IAD880 series IADs. A maximum of two transcoding sessions are supported.
 Additional Information:
<http://www.cisco.com/en/US/docs/routers/access/iad880/software/configuration/guide/IAD880SCG.html>
- Warning messages added to **dspfarm profile** command regarding transcoding and conferencing.
 Old Behavior: No explicit messages display in response to attempts to configure conferencing or transcoding on Cisco VG 20x platforms or to configure conferencing on Cisco IAD 243x platforms.
 New Behavior: These platforms display explicit warning messages if attempts are made to configure services that are not available.
 Additional Information:
http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_d2.html#wp1457890

Cisco IOS Release 15.0(1)M1

The following behavior changes are introduced in Cisco IOS Release 15.0(1)M1:

- Implementing IPv6 mobile configuration file and several commands were modified.
 Old Behavior: The “Enabling and Configuring NEMO on the IPv6 Mobile Router” task in the “Implementing IPv6 Mobile” configuration guide was incorrect, as were several commands within this task.

New Behavior: The task and commands were reworked so that the configuration information is now correct.

Additional Information:

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

- Implementing the **show nextport mm** command output as new example in the **show nextport** command.

Old Behavior: Command is without the **show nextport mm** command output as example.

New Behavior: The command output example was changed so that the configuration information is now correct.

Additional Information:

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_s07.html#wp1275793

- In Cisco IOS Release 15.0(1)M1, you can configure the interface MTU on PA-1FE and PA-2FE port adapters (PAs). Before this enhancement, the MTU of those interfaces was not configurable. When you attempted to configure the interface MTU, the following message was printed:

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

Additional Information:

http://www.cisco.com/en/US/docs/ios/mps/configuration/guide/mp_mtu_cmd_changes.html

- **mgcp behavior g729-variants static-pt** command is enabled by default

Old Behavior: The Real-time Transport Protocol (RTP) payload type on G.729 voice codecs was set as dynamic by default.

New Behavior: The Real-time Transport Protocol (RTP) payload type on G.729 voice codecs is set to static by default, and the **mgcp behavior g729-variants static-pt** command is enabled by default.

Additional Information:

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_m1.html#wp1429063

- Old Behavior: PADO delay per circuit id does not work properly with substring match.

New Behavior: PADO delay configurations using circuit ID have been enhanced.

Eight examples and scenarios were added to the **pppoe server circuit-id delay** command page.

Additional Information:

http://www.cisco.com/en/US/docs/ios/bbds/command/reference/bba_02.html

- The snmp-object Ed type supports “oid” and “counter64.”

Old Behavior: The snmp-object ED does not support types “oid” and “counter64.” This makes it impossible to match on objects such as sysObjectID or ifHCInOctets.

New Behavior: The event snmp-object CLI and the event_register_snmp_object event detector have been reworked to support types “oid” and “counter64.” You can now match objects such as sysObjectID or ifHCInOctets.

Additional Information:

http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm_06.html

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

Field Notices and Software-Related Tools and Information

We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. You can find Field Notices at

http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html

Visit the Software Center/Download Software page on Cisco.com to subscribe to Cisco software notifications, locate MIBs, access the Software Advisor, and find other Cisco software-related information and tools. Access the Software Center/Download Software page at

<http://www.cisco.com/cisco/web/download/index.html>, or by logging into Cisco.com and selecting **Support > Download Software**.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*
http://www.cisco.com/en/US/products/hw/routers/ps214/products_tech_note09186a008012fb88.shtml
- *Troubleshooting Bus Error Exceptions*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml
- *Why Does My Router Lose Its Configuration During Reboot?*
http://www.cisco.com/en/US/products/hw/routers/ps233/products_tech_note09186a00800a65a5.shtml
- *Troubleshooting Router Hangs*
http://www.cisco.com/en/US/products/hw/routers/ps359/products_tech_note09186a0080106fd7.shtml
- *Troubleshooting Memory Problems*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6f3a.shtml
- *Troubleshooting High CPU Utilization on Cisco Routers*
http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a00800a70f2.shtml
- *Troubleshooting Router Crashes*
http://www.cisco.com/en/US/products/hw/iad/ps397/products_tech_note09186a00800b4447.shtml
- *Using CAR During DOS Attacks*
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_tech_note09186a00800fb50a.shtml

