Features and Important Notes for Cisco IOS Release 15.1(4)M

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 15.1(4)M and contains the following subsections:

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

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(4)M7

There are no new hardware features in Cisco IOS Release 15.1(4)M7.

New Software Features Supported in Cisco IOS Release 15.1(4)M7

There are no new software features in Cisco IOS Release 15.1(4)M7.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M6

There are no new hardware features in Cisco IOS Release 15.1(4)M6.

New Software Features Supported in Cisco IOS Release 15.1(4)M6

There are no new software features in Cisco IOS Release 15.1(4)M6.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M5

There are no new hardware features in Cisco IOS Release 15.1(4)M5.

New Software Features Supported in Cisco IOS Release 15.1(4)M5

There are no new software features in Cisco IOS Release 15.1(4)M5.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M4

This section describes new and changed features in Cisco IOS Release 15.1(4)M4. Some features may be new to Cisco IOS Release 15.1(4)M4 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(4)M4. 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 Connected Grid 2G/3G/4G LTE GRWIC for Verizon Wireless

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

http://www.cisco.com/en/US/docs/routers/connectedgrid/modules/4g/install/CG_2G-3G-4G_Multimode_LTE_GRWIC.html

New Software Features Supported in Cisco IOS Release 15.1(4)M4

There are no new software features in Cisco IOS Release 15.1(4)M4.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M3

There are no new hardware features in Cisco IOS Release 15.1(4)M3.

New Software Features Supported in Cisco IOS Release 15.1(4)M3

There are no new hardware features in Cisco IOS Release 15.1(4)M3.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M2

This section describes new and changed features in Cisco IOS Release 15.1(3)T32. Some features may be new to Cisco IOS Release 15.1(3)T32 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T32. 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 860 Series Integrated Services Routers

The Cisco 860 series integrated services routers (ISRs) combine Internet access, security, and wireless services onto a single, secure device that is simple to use and manage for small businesses. Cisco 860 ISRs are fixed-configuration routers that provide business solutions for secure voice and data communication to small businesses. The Cisco 860 series offers secure broadband services over Gigabit Ethernet and DSL Multi-mode (VDSL2 / ADSL2/2+) WAN links.

Cisco 881-V, Cisco 887VA-V, and Cisco 887VA-V-W

The Cisco 881-V, Cisco 887VA-V, and Cisco 887VA-V-W integrated services routers deliver analog and digital voice support as well as data. For more information on the product, see the following documentation:

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

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

SM-32A Module Support on Cisco 3900/3900E Integrated Services Routers G2 Platforms

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

http://www.cisco.com/en/US/docs/routers/access/interfaces/nm/hardware/installation/guide/sm_32a.html

New Software Features Supported in Cisco IOS Release 15.1(4)M2

There are no new software features in Cisco IOS Release 15.1(4)M2.

New Hardware Features Supported in Cisco IOS Release 15.1(4)M1

This section describes new and changed features in Cisco IOS Release 15.1(3)T31. Some features may be new to Cisco IOS Release 15.1(3)T31 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T31. 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 Cisco IOS Fixed Router

The Cisco 819G and Cisco 819GH integrated services router (ISR) is a compact 3G Cisco IOS fixed router that can operate in outdoor, indoor, and mobile environments. The Cisco 819 ISRs are available in hardened and non-hardened versions. The Cisco 819GH ISR is the hardened version that operates over an extended temperature range. The Cisco 819G ISR is a standard form factor with a commercial operating range. The Cisco 819 integrated services routers support the latest 3G speeds (High-Speed Packet Access Plus [HSPA+] and Evolution Data Optimized [EVDO Rev A]), enabling up to 4G speeds. They are backward-compatible with High-Speed Packet Access (HSPA), Universal Mobile Telecommunications Service (UMTS), Enhanced Data Rates for Global Evolution (EDGE), General Packet Radio Service (GPRS), and EVDO Rev 0/1xRTT. It can also be used as a primary WAN data link. The 3G technology is third-generation wide-area cellular technology that is used in voice telephony and broadband wireless data in a mobile environment.

The Cisco 819 ISR is a desktop form factor with built-in wall-mount features and optional rack-mount features. These routers are powered by an external AC power supply adapter.

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

http://cisco.com/en/US/docs/routers/access/800/819/hardware/install/guide/819hwinst.html

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

http://www.cisco.com/en/US/docs/routers/access/800/819/software/configuration/Guide/819_SCG.html

New Software Features Supported in Cisco IOS Release 15.1(4)M1

This section describes new and changed features in Cisco IOS Release 15.1(3)T31. Some features may be new to Cisco IOS Release 15.1(3)T31 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T31. 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 is 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(4)M

This section describes new and changed features in Cisco IOS Release 15.1(3)T3. Some features may be new to Cisco IOS Release 15.1(3)T3 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T3. 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.

China VWIC2-1MFT-G703-C and VWIC2-2MFT-G703-C Modules Support onto Cisco 1906C/K9 Supported Module List

The Cisco 1906C was built on the Cisco 1900 Series Integrated Services Routers (ISRs) based on first-class products. All Cisco 1900 Series ISR products offer embedded hardware encryption acceleration, optional firewall, intrusion prevention, and advanced security services. In addition, the Cisco 1906C ISR has an integrated serial interface module and an EWHIC slot that can support LAN, 3G, or ISDN module options. It can be deployed in a high-speed WAN environment, which provides better service integration capabilities and network flexibility. The Cisco 1906C improves performance and density and will support multiple services. It will also feature multiple independent devices that can be integrated into a compact remote management system. The Cisco second-generation 1- and 2-port T1/E1 Multiflex Trunk Voice/WAN Interface cards (MFT VWIC2s) support data on the Cisco 1906C Series ISRs. The Cisco MFT VWIC2 combines WAN-interface-card (WIC) and voice-interface-card (VIC) functions to provide unparalleled flexibility, versatility, and investment protection through its many uses.

For more information, see the following document:

http://www.cisco.com/en/US/docs/routers/access/1900/hardware/release/notes/Rn_C1906K9.html

Cisco Gigibit Ethernet/SFP Enhanced High-Speed WAN Interface Card

The Cisco Gigabit Ethernet WAN EHWIC (EHWIC-1GE-SFP-CU) is an enhanced high-speed interface card providing copper and optical Gigabit Ethernet ports and connectivity of T1/E1 and T3/E3 over copper for Cisco Integrated Services Routers (ISRs). The Cisco Gigabit Ethernet enhanced high-speed WAN interface card also provides copper and optical Gigabit Ethernet connectivity through a dual-purpose uplink (DPU).

Cisco ISR VE Series

Cisco IOS Release 15.1(4)M supports the Cisco 1841VE and Cisco 2811VE Integrated Services Routers (ISRs). The Cisco 1841VE router offer the following features:

- Embedded hardware-based encryption enabled by an optional Cisco IOS software security image
- Further enhancement of VPN performance with an optional VPN acceleration module
- Firewall functions
- Interfaces for a wide range of connectivity requirements, including support for optional integrated switch ports
- Sufficient performance and slot density for future network expansion and advanced applications
- An integrated real-time clock

The Cisco 2811VE features the ability to deliver multiple high-quality simultaneous services at wire speed up to multiple T1/E1 connections. The routers offer the following features:

- Embedded encryption acceleration and on-the-motherboard voice Digital Signal Processor (DSP) slots
- Intrusion prevention system (IPS) and firewall functions
- High-density interfaces for a wide range of wired and wireless connectivity requirements
- Sufficient performance and slot density for future network expansion requirements and advanced applications

EHWIC Multi-Mode VDSL2/ADSL+ Multicard Support

The HWIC-ADSL-VDSL2 offers multi-mode VDSL2/ADSL2/2+ capabilities on an HWIC form factor for the ISR G2 series.

For more information, see the following documents:

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

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

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

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

Enhanced Cisco 880 Wireless Platforms (C881W-A-K9, C881W-E-K9, C881W-P-K9, C886VA-W-E-K9, C887MVA-W-E-K9, C887VA-W-A-K9, C887VA-W-E-K9)

For more information, see the following document:

http://www.cisco.com/en/US/partner/prod/collateral/routers/ps380/data_sheet_c78_459542_ps380_Products_Data_Sheet.html

New Software Features Supported in Cisco IOS Release 15.1(4)M

This section describes new and changed features in Cisco IOS Release 15.1(3)T3. Some features may be new to Cisco IOS Release 15.1(3)T3 but were released in earlier Cisco IOS software releases. Some features may have been released in earlier Cisco IOS software releases and have been changed in Cisco IOS Release 15.1(3)T3. 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 is available in the feature description provided.

Call Escalation from Voice to Video

For more information, see the following document:

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

Cisco IOS NAM PA for WAAS Express

For more information, see the following document:

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

Cisco IOS Shell

For more information, see the following document:

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

Cisco ISR G2 Multi Gigabit Fabric Phase 2

For more information, see the following document:

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

Cisco Unified CME 8.6

For more information, see the following document:

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

Cisco V.150.1 Minimum Essential Requirements

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html

CUBE Lite on Cisco 800 Series ISR

CUBE features like SIP-to-SIP Delayed-Offer/Early-Offer calls, SRTP calls in pass-through mode, and basic SIP to H.323 calls are supported on CUBE Lite platform (Cisco 880 and Cisco 890 platforms).

DHCP User Auth CLI for FORCERENEW

For more information, see the following document:

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

DMVPN Event Tracing

For more information, see the following document:

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

EIGRP IPv6 VRF-Lite

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/iproute_eigrp/configuration/guide/ire_cfg_eigrp.html

Flexible NetFlow—32-Bit AS Number Support

With Cisco IOS Release 15.1(4)M, Flexible NetFlow supports 32-bit autonomous system (AS) numbers. Flexible NetFlow can capture and export 32-bit numbers as well as 16-bit numbers. If you specify the 4-octet keyword in the collect routing or match routing command, you configure the 32-bit autonomous system number as a nonkey or key field; otherwise, you configure the 16-bit version. If you configure both a 32-bit version and a 16-bit version within a record, only the 32-bit version applies. The 32-bit AS numbers have a different v9 export type than that used for 16-bit AS numbers. Your collector and analysis infrastructure should be able to process values for 32-bit AS numbers.

The following commands have been added in this release to support this feature:

[match | collect] **routing destination as** [*4-octet*]

[match | collect] **routing destination as peer** [*4-octet*]

[match | collect] **routing source as** [*4-octet*]

[match | collect] **routing source as peer** [*4-octet*]

For more information on export types, see the *NetFlow Layer 2 and Security Monitoring Exports* document:

http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/nf_lay2_sec_mon_exp.html

IPv4 MIB Support (RFC 4293)

Cisco IOS Release 15.1(4)M includes support for the IPv4 MIB as described in RFC 4293, Management Information Base for the Internet Protocol (IP). As part of this support, the **clear ip traffic** command and the **show ip traffic** command were modified. For more information about these commands and their modifications, see the *IP Application Services Command Reference* and the *IP Switching Command Reference.*

http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html

http://www.cisco.com/en/US/docs/ios/ipapp/command/reference/iap_book.html

IPv6 Multicast VRF Lite

For more information, see the following document:

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

IPv6 Support for IPSec and IKEv2

Cisco IOS Release 15.1(4)M provides IPv6 support for IKEv2 and IPSec protocols. This is in accordance with the US Government's IPv6 certification requirements. This release implements IPv6 support for crypto maps and tunnel protection.

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

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

LISP Locator/ID Separation Protocol

For more information, see the following document:

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

MAC Authentication Bypass (MAB)

For more information, see the following document:

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

MVPN—Data MDT Enhancements

Multicast distribution tree (MDT) groups were selected at random when the traffic passed the threshold and there was a limit of 255 MDTs before they were reused. The MVPN—Data MDT Enhancements feature provides the ability to deterministically map the groups from inside the VPN routing and forwarding (S,G) entry to particular data MDT groups, through an access control list (ACL). The user can now map a set of VPN routing and forwarding (S,G) to a data MDT group in one of the following ways:

- 1:1 mapping (1 permit in ACL)
- Many-to-1 mapping (many permits in ACL)
- Many-to-many mapping (multiple permits in ACL and a nonzero mask data MDT)

Because the total number of configurable data MDTs is 1024, the user can use this maximum number of mappings in any of the described combinations.

OSPF—Demand Circuit Disable

For more information, see the following document:

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

PPPoE—Max-Payload Support on Client

For more information, see the following document:

http://www.cisco.com/en/US/docs/ios/bbdsl/configuration/guide/bba_ppoe_client.html

Product Security Baseline—Password Encryption and Complexity Restrictions

This feature introduces the aaa password restriction command, which enforces that passwords be subject to the following restrictions:

- The new password must contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters
- The new password should not have a character repeated more than three times consecutively
- The new password should not be the same as the associated username. A password obtained by capitalization of the username or username reversed is not accepted
- The new password should not be "cisco," "ocsic," or any variant obtained by changing the capitalization of letters therein, or by substituting "1" "|" or "!" for i, or by substituting "0" for "o", or substituting "$" for "s."

The restrictions can be applied to the passwords configured using the following commands: **aaa pod server, enable password, enable secret, radius-server key, radius-server host key, server-key,** and **tacacs-server key**.

Radius Statistics VIA SNMP

For more information, see the following document:

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

Secure Tone Support on MGCP TDM GW

For more information, see the following document:

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

SIP Loopback Support

For more information, see the following document:

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

USB Enable/Disable for Cisco ISR Routers

Feature Introduction

The USB Disable feature provides Cisco IOS administrators with the ability to disable all USB ports on the router.

Default Setting

Cisco IOS enables USB ports by default, which preserves existing USB functionality such as the following:

- Booting the Cisco IOS from a USB port
- Saving configuration files to a router for Cisco IOS reloads

Note Using the USB Disable feature (to disable or re-enable the USB ports) requires a router reboot. When USB ports are disabled from within Cisco IOS, USB functionality remains unavailable until re-enabled.

For more information, see the following document:

http://www.cisco.com/en/US/docs/solutions/GGSG-Engineering/15_1_4M/USB_Disable.html

Video Conferencing Services on Cisco Integrated Services Router G2

This release enhances the existing audio conferencing and transcoding feature set by adding support for video conferencing on Cisco Integrated Services Router Generation 2 (ISR G2). This ISR G2 uses on-board Digital Signal Processor (DSP) resources (Packet Voice Video Digital Signal Processor Module PVDM3) combined with Cisco IOS software to switch a scalable number of ad hoc or MeetMe video conference calls for Cisco Unified Communications Manager or Cisco Unified Communications Manager Express.

For more information, see the following document:

http://www.cisco.com/en/US/products/sw/voicesw/ps4952/products_installation_and_configuration_guides_list.html

ZBFW Support for MSRPC

For more information, 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(4)M:

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(4)M6

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M5:

- BGP processing of the removal of private AS numbers from the AS path.

  Old Behavior: When the **neighbor remove-private-as** command is configured and a route-map without a continue clause is configured, the processing order is:

  - neighbor remove-private-as processing
  - set as-path prepend or set as-path prepend last-as

  However, if the route-map contains a continue clause, the processing order is reversed.

  New Behavior: When the **neighbor remove-private-as** command is configured and a route-map is configured (whether it has a continue clause or not), the processing order is always:

  - neighbor remove-private-as processing
  - set as-path prepend or set as-path prepend last-as

- RTP signal processing is disabled by default.

  Old Behavior: RTP packets of payload type ?123? can cause errors on Cisco AS5350 and AS5400 series platforms.

  New Behavior: RTP signal processing is disabled by default to prevent errors caused by RTP packets of payload type “123” and can be enabled when necessary using the **voice-fastpath voice-rtp-signalling enable** command.

  Additional Information:
  http://www.cisco.com/en/US/tech/tk652/tk653/technologies_tech_note09186a00800a96c1.shtml

- Improper tunnel MTU value.

  Old Behavior: The IPsec encapsulation bytes are calculated based on the source interface.

  New Behavior: The IPsec encapsulation bytes are calculated based on the outgoing physical interface.

Additional Information:
http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/ip_inspect_through_ip_security_strip.html#GUID-6BED3794-8050-4464-9A17-8D8C8C02EF88

- Setting of factory defaults.

  Old Behavior: When the push button is pressed, configuration and image recovery takes place at WLAN AP running on 2nd core of next generation c8xx platforms.

  New Behavior: When the push button is pressed, ONLY configuration recovery takes place at WLAN AP running on 2nd core of next generation c8xx platforms.

- A new keyword is added to the **timers** command.

  Old Behavior: The **dns** keyword is not available with the **timers** command.

  New Behavior: The **timers** command can use the **dns** keyword.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr5/vcr-t2.html

Cisco IOS Release 15.1(4)M5

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M5:

- Change to how IPv6 paths are advertised.

  Old Behavior: An IPv6 path is advertised without a label when the label has not been negotiated

  New Behavior: IPv6 paths are not advertised if the label has not been negotiated

- The SIP call hold/resume scenario has been enhanced so that the RTP sequence number is continuous from the origin of the call until 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/voi-sipsip-sbc.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/cube_sip/configuration/15-2mt/voi-sipsip-sbc.html

- The prompt command is made available on the Cisco 860 series, 860VAE series, and 880 series routers.

  Old Behavior: The Cisco 860 series, 860VAE series, and 880 series routers do not support the prompt command.

  New Behavior: The prompt command is available on these routers.

- PfR syslog levels have been added to minimize the number of messages.

  Old Behavior: Too many PfR syslog messages are generated.

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

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

- In the IPsec SVTI configuration with HA, existing security associations are not affected.

Old Behavior: When configuring IPsec SVTI with HA, the standby router reload interrupts the existing security associations.

New Behavior: When configuring IPsec SVTI with HA, the standby router reload does not affect the existing security associations.

Additional Information:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-2mt/sec-ipsec-virt-tunnl.html#GUID-D4B2DE6B-A9B1-4F68-AF39-995CDAFFDEB9

- An early warning is displayed on the CPU for over temperature case.

  Old Behavior: There is no early warning displayed on the CPU for over temperature case.

  New Behavior: There is an early warning displayed on the CPU for over temperature case.

- The **clear call threshold interface** command can be used for a Gigabit Ethernet interface.

  Old Behavior: Unable to the **clear call threshold interface** command for a Gigabit Ethernet interface.

  New Behavior: Gigabit Ethernet interface is a valid interface type.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr1/vcr-c5.html#GUID-63581F18-D001-4975-A04E-9A0807CAB08E

- HQF shape timer can replenish the shape tokens at 1 ms or 4 ms intervals.

  Old Behavior: The Hierarchical Queuing Framework (HQF) shaper timer replenishes the shape tokens at 4-millisecond (ms) intervals.

  New Behavior: The **qos shape-timer** command allows you to configure the HQF shaper timer to replenish the shape tokens at 1-ms or 4-ms intervals.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/qos/command/Q_through_R.html

Cisco IOS Release 15.1(4)M4

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M4:

- Connected number and Connected name are sent in an ISDN CONNECT message as Connected Number IE and Connected Name (display IE).

  Old Behavior: Connected number and Connected name that are signaled to the Cisco IOS software from a SIP 200 OK message are not sent in an ISDN CONNECT message.

  New Behavior: Connected number and Connected name that are signaled to the Cisco IOS software from a SIP 200 OK message are sent as Connected Number IE and Display IE (Connected Name) in the ISDN CONNECT message. Passing the Connected number and the Connected name is enabled by configuring the following commands in interface configuration mode: **isdn outgoing ie connected-number**, **isdn outgoing ie display**.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/dial/command/reference/dia_i2.html

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

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

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

- A new keyword is added to the **supplementary-service sip** command.

  Old Behavior: The *handle-replaces* keyword is not available in the **supplementary-service sip** command.

  New Behavior: The *handle-replaces* keyword is available for the **supplementary-service sip** command.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr4/vcr-s12.html#GUID-98E8D5E4-A18F-49D4-ACC7-8104E01A0C1A

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

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

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

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

- Added analogue vm-integration in SIP line

  Old Behavior: vm-integration only applies to SCCP line.

  New Behavior: vm-integration also applies to SIP line.

  Additional Information:
  http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/srst_voicemail.html

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

  Old Behavior: There are too many PfR syslog messages.

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

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

- Connected number and Connected name are sent in an ISDN CONNECT message as Connected Number IE and Connected Name (display IE).

  Old Behavior: Connected number and Connected name that are signaled to Cisco IOS software from a SIP 200 OK message are not sent in an ISDN CONNECT message.

  New Behavior: Connected number and Connected name that are signaled to Cisco IOS software from a SIP 200 OK message are sent as Connected Number IE and Display IE (Connected Name) in the ISDN CONNECT message. Passing the Connected number and the Connected name is enabled by configuring the following commands in interface configuration mode: **isdn outgoing ie connected-number**, **isdn outgoing ie display**.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/dial/command/reference/dia_i2.html

- Answer (ANS) tone treatment is enabled for modem and fax answer tone.

  Old Behavior: There is no ANS tone treatment enabled for modem and fax answer tone.

  New Behavior: The ANS tone treatment can be enabled for modem and fax answer tone by using the *ans-treatment* keyword in the **fax-relay** command.

Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr2/vcr-f1.html

- Fast Network Time Protocol (NTP) synchronization is achieved.

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

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

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

Cisco IOS Release 15.1(4)M3

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M3:

- CLI introduced to ignore S1 SONET overhead byte set to 0xF

  Old Behavior: A packet received with an S1 SONET overhead byte set to 0xF causes the router to switch the clock source to internal.

  New Behavior: A CLI **atm sonet ignore s1** has been introduced, which when set directs the router to ignore an S1 overhead byte set to 0xF, which in turn ensures that the clock does not change.

  Additional Information:

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

  This CLI is currently applicable only on ASR1K. This CLI will be visible but not enabled on other platforms.

- The **do** configuration command has been reactivated for Cisco IOS Release 15.x.

  Old Behavior: The **do** command had been removed temporarily.

  New Behavior: The **do** command is now reactivated.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/D_through_E.html#GUID-7E54B6C8-BA6F-4B0E-8A7B-19B50E66042A

- BGP scan time range is changed

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

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

- Increase in autonomous system number or community prepending in BGP Inbound Optimization using PfR.

  Old Behavior: In both the “BGP Autonomous System Number Prepend” and “BGP Autonomous System Number Community Prepend” methods of controlling inside prefixes using PfR, the number is increased one by one up to the maximum of six ASes in unreachable, loss, and delay OOP cases.

  New Behavior: In both the “BGP Autonomous System Number Prepend” and “BGP Autonomous System Number Community Prepend” methods of controlling inside prefixes using PfR, the new behavior increases the AS number or community to the maximum of six immediately, for unreachable and loss OOP cases.

  In the delay OOP case, the behavior is the same as the old behavior.

Additional Information: See the "PfR Entrance Link Selection" section under Information About in:

http://www.cisco.com/en/US/docs/ios-xml/ios/pfr/configuration/15-2mt/pfr-bgp-inbound.html

- Increased maximum number of traffic classes (prefixes) to be learned in a PfR learn list.

  Old Behavior: Using the Cisco IOS CLI, **count** (PfR) command, the maximum number of traffic classes to be learned in a PfR learn list was 100, with a default of 50.

  New Behavior: Using the Cisco IOS CLI, **count** (PfR) command, the maximum number of traffic classes to be learned in a PfR learn list is 1000, with a default of 1000.

  Additional Information: The command is documented in the Performance Routing Command Reference at:

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

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

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

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

  Additional information:

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

- Netmask should be specified while configuring the svc address pool under policy group.

  Old Behavior: Netmask was optional while configuring the svc address pool under policy group.

  New Behavior: Netmask keyword is made mandatory while configuring the svc address pool.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-s6.html
  #GUID-4AB61E8E-4D2E-4A5B-9943-6AD1F90FF572

Cisco IOS Release 15.1(4)M2

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M2:

- The **logging source-interface** command needs new VRF information for customer ease of use.

  Old Behavior: Users could not configure VRF information when using the **logging source-interface** command.

  New Behavior: The **vrf** keyword and *vrf-name* argument are supported in the Cisco IOS Releases 12.2(33)SXJ1 and 15.1(3)S.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/ipv6/command/reference/ipv6_09.html

- Change to **neighbor prefix-length-size** command

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

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

- Change in **show bgp ipv4 unicast summary** command

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

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

- **Batch** command available under interface mode.

  Old Behavior: **batch** command was not available under interface.

  New Behavior: **batch** command is available under interface

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/routconf.html

- The **cable-detect** command does not support analog FXO ground-start voice port. The command must be documented with this information.

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

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

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr1/vcr1-cr-book.html

- Tunnel transport MTU now accounts for IPsec encryption with GRE

  Old Behavior: The tunnel transport maximum transmission unit (MTU) did not account for IPsec encryption overhead with generic routing encapsulation (GRE). The tunnel transport MTU is used to fragment the packet. Since the transport MTU reduces, some packets that were previously fragmented post encryption are fragmented at the tunnel interface.

  New Behavior: The tunnel transport MTU now accounts for IPsec encryption overhead with GRE. Use the **show interfaces tunnel** command to see updated command output for a tunnel interface.

- Power down time for the SRE module.

  Old Behavior: SRE module takes two minutes to power down.

  New Behavior: If the SRE module is not running an application, the time-out interval is less than two minutes. If the SRE module is running an application, it requires a 2-minute time-out interval to reflect the actual change in Cisco EnergyWise level.

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

- Documentation changes to support Optimized Edge Routing (OER) CLI hidden in Cisco IOS Release 15.0(1)SY

  Old Behavior: OER border router functionality was supported on the Catalyst 6500 Switch.

  New Behavior: OER is no longer supported on the Catalyst 6500 Switch, and the OER CLI is hidden in Cisco IOS Release 15.0(1)SY.

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

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

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

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

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

Cisco IOS Release 15.1(4)M1

The following behavior changes are introduced in Cisco IOS Release 15.1(4)M1:

- PPPoA SSO for forwarded sessions is not supported.

  Old Behavior: PPPoA SSO for forwarded sessions on LAC is not supported.

  New Behavior: PPPoA SSO for forwarded session is supported. The output of the show pppatm redundancy command is modified to display the number of PPPoA sessions that are forwarded and synced to the standby Route Processor (on the active RP) and forwarded and re-created on the standby RP.

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

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

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

- BGP no longer activates IPv6 peers in IPv4 address family automatically.

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

  New Behavior: Starting with new peers being configured, an IPv6 neighbor is no longer automatically activated under the IPv4 address family. You can manually activate the IPv6 neighbor under the IPv4 address family if you want. If you do not want an existing IPv6 peer activated under the IPv4 address family, you can manually deactivate the peer with the no neighbor ipv6-address activate command. Until then, existing configurations that activate an IPv6 neighbor under the IPv4 unicast address family will continue to try to establish a session.

  Additional Information:
  http://www.cisco.com/en/US/partner/docs/ios-xml/ios/iproute_bgp/configuration/15-1mt/irg-basic-net.html

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

- The **ip header-compression old-iphc-comp** and **ip header-compression old-iphc-decomp** commands are added to configure the IPHC format of compression and decompression to the non-RFC-compliant format.

  Old Behavior: The header compression decodes RTP timestamp incorrectly. This issue occurs mainly with IPHC format compression interacting with older IOS releases.

New Behavior: The **ip header-compression old-iphc-comp** and **ip header-compression old-iphc-decomp** commands are used to revert the IPHC format of compression and decompression to the non-RFC-compliant format.

Additional Information:
http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_i1.html#wp1065764

http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_i1.html#wp1066790

- Routing protocols purge routes when an interface goes down.

  Old Behavior: Routing protocols do not purge routes when an interface goes down. This is the default behavior.

  New Behavior: Routing protocols purge routes when an interface goes down. This is the default behavior.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios/iproute_pi/command/reference/iri_pi1.html#wp1013065

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

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

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

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

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

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

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

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

- A change has been made to the CLI command output.

  Old Behavior: The command output does not display the bundled WLAN AP bootloader version.

  New Behavior: The command output displays the bundled WLAN AP bootloader version.

- A new command, **cdma ddtm**, is added.

  Old Behavior: On CDMA modems, data transmission is disrupted by incoming voice calls if data dedicated transmission mode (DDTM) is disabled.

  New Behavior: The **cdma ddtm** command enables DDTM.

  Additional Information:
  http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/mrwlcdma.html

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

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

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

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

- The flow direction field can now be exported by Cisco Performance Monitor.

  Old Behavior: The flow direction field was not exported by Cisco Performance Monitor.

  New Behavior: The **collect flow direction** command can now be used to export the flow direction field along with the other performance data being monitored.

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

  and

  http://www.cisco.com/en/US/docs/ios/media_monitoring/configuration/guide/15_1m_and_t/mm_15_1m_and_t.html

- There is a change in the CLI output.

  Old Behavior: When the netflow cache size is other than the default (64K), netflow needs to be reenabled at all applicable interfaces to take effect.

  New Behavior: After every reboot the configured netflow cache size is applied from the startup configuration. There is a change of configuration order for “ip flow-cache entries xxxxx” and “ip flow-egress input-interface”; the **show running configuration** command now reflects this change.

Important Notes for Cisco IOS Release 15.1(4)M3

This section describes important issues that you should be aware of for Cisco IOS Release 15.1(4)M3 and later releases.

Cisco Images Deferred

In Cisco IOS Release 15.1(4)M3, 24 images have been deferred. This defect has been assigned Cisco caveat ID CSCtx06747. The affected images are as follows:

c5350-ik9s-mz

c5350-ik9su2-mz

c5350-jk9s-mz

c5350-jk9su2_ivs-mz

c5400-ik9s-mz

c5400-ik9su2-mz

c5400-jk9s-mz

c5400-jk9su2_ivs-mz

c7200-adventerprisek9-mz

c7200-adventerprisek9_sna-mz

c7200-advipservicesk9-mz

c7200-advipservicesk9_li-mz

c7200-advsecurityk9-mz

c7200-ipbasek9-mz

c7200-spservicesk9-mz

c7200p-adventerprisek9-mz

c7200p-adventerprisek9_sna-mz

c7200p-advipservicesk9-mz

c7200p-advipservicesk9_li-mz

c7200p-advsecurityk9-mz

c7200p-ipbasek9-mz

c7200p-spservicesk9-mz

vgd-jk9s-mz

vgd-jk9su2_ivs-mz

The software solution for these deferred images is Cisco IOS Release 15.1(4)M3a. The DDTS Solution is CSCtx06747 (Headline: Boot failure due to TLB (Store) Exception with ASSERTION FAILED logged.

To increase network availability, Cisco recommends that you upgrade affected Cisco IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected Cisco IOS images. Any pending order will be substituted by the replacement software images.

Note Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

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

Important Notes for Cisco IOS Release 15.1(4)M1

This section describes important issues that you should be aware of for Cisco IOS Release 15.1(4)M1 and later releases.

Cisco Security Manager

The Cisco Connected Grid 2010 router supports Cisco Security Manager. For more information, see the *Cisco Security Manager Configuration Guides*:

http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html

Gateway Crash When SIP-KPML Signaling Is Configured in SIP Gateway Dial Peers (CSCtq56727)

There is a defect in Cisco IOS Release 15.1(4)M when the configuration in Unified Communications Manager that is pointing to a SIP gateway is set with DTMF signaling type as “no preference” and the SIP gateway is configured with DTMF relay as sip-kpml.

Bulk call failures are seen during heavy loads of traffic and are followed by a gateway crash. The crash report indicates mallocfail tracebacks on CCSIP_SPI_CONTROL, AFW, VTSP and other processes.

The show processes memory sorted command shows a continuous increase in memory held by the CCSIP_SPI_CONTROL process even when the average number of calls at the gateway is constant.

There are two workarounds:

1. Set the DTMF signaling type as “OOB and RFC 2833” in Unified Communications Manager SIP trunk configuration that is pointing to the SIP gateway.
2. Configure “dtmf-relay rtp-nte” at the SIP gateway dial-peer configuration, instead of “sip-kpml.” The Unified Communications Manager is configured with “no preference.”

In order to recover from the crash, the gateway router must be reloaded.

Important Notes for Cisco IOS Release 15.1(4)M

This section describes important issues that you should be aware of for Cisco IOS Release 15.1(4)M and later releases.

Video Conferencing Services on the Cisco Integrated Services Router G2

The following section describes some important information about the video conferencing and transcoding feature.

- For a Cisco Unified IP Phone 7985 that is registered with Cisco Unified CME to participate in a video conference, the phone requires a DSP farm profile that is configured with the H.263 codec. Cisco Unified IP Phones 7985 connected to Cisco Unified Communications Manager can support both H.263 and H.264.
- Cisco Unified IP Phones 9951 and 9971 hav the following interoperability issues:
  - Cisco Unified IP Phones 9951 and 9971 require a DSP farm profile that is configured with the H.264 codec.
  - When you enable the lecture mode option on Cisco Unified CME, a conferee on Cisco Unified IP Phones 9951 and 9971 cannot become a lecturer. Users on the phone can only participate in the video conference as conferees.
  - Cisco Unified IP Phones 9951 and 9971 use the Real-Time Transport Protocol (RTP) payload value of 97. This value is often reserved for cisco-codec-fax-ack. You must reconfigure your RTP payload for cisco-codec-fax-ack and for cisco-codec-video-h264 by adding the following commands to the appropriate dial-peer profile:

    rtp payload-type cisco-codec-fax-ack 111

    rtp payload-type cisco-codec-video-h264 97
- Lifesize endpoints using 4cif resolution display a blank screen when a conferee on a Cisco Unified IP Phone 9951 or 9971 with qcif resolution becomes the active speaker. The display correctly displays all other conferees.

- Ad hoc conferences on endpoints that are connected through a SIP trunk are currently not supported. However, endpoints that are connected through a SIP trunk can connect to MeetMe video conferences.