Features and Important Notes for Cisco IOS Release 15.2(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 15.2M&T and contains the following subsections:

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

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

New Hardware Features Supported in Cisco IOS Release 15.2(4)M5

There are no new hardware features supported in Cisco IOS Release 15.2(4)M5.

New Software Features Supported in Cisco IOS Release 15.2(4)M5

There are no new software features supported in Cisco IOS Release 15.2(4)M5.

New Hardware Features Supported in Cisco IOS Release 15.2(4)M4

There are no new hardware features supported in Cisco IOS Release 15.2(4)M4.

New Software Features Supported in Cisco IOS Release 15.2(4)M4

There are no new software features supported in Cisco IOS Release 15.2(4)M4.

New Hardware Features Supported in Cisco IOS Release 15.2(4)M3

This section describes new and changed features in Cisco IOS Release 15.2(4)M3. Some features may be new to Cisco IOS Release 15.2(4)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 15.2(4)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.

SM-X-1T3/E3 (Secure Boot)

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

http://www.cisco.com/en/US/products/ps11746/prod_release_notes_list.html

New Hardware Features Supported in Cisco IOS Release 15.2(4)M2

This section describes new and changed features in Cisco IOS Release 15.2(4)M2. Some features may be new to Cisco IOS Release 15.2(4)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 15.2(4)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.

High Density FXS Module Support on ISR G2

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

http://www.cisco.com/en/US/docs/routers/access/vg350/hardware/installation/guide/vg350hig

New Software Features Supported in Cisco IOS Release 15.2(4)M2

This section describes new and changed features in Cisco IOS Release 15.2(4)M2. Some features may be new to Cisco IOS Release 15.2(4)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 15.2(4)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 VG350 No Payload Encryption (NPE) Image

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

http://www.cisco.com/en/US/docs/routers/access/vg350/software/configuration/guide/vg350scg

Flexible NetFlow: Integration with MQC

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

http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-2mt/fnf-fnf-mqc.html

Flexible NetFlow: IPFIX Export Format

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

http://www.cisco.com/en/US/docs/ios-xml/ios/media_monitoring/configuration/15-2mt/mm-pasv-mon.html

MACE Phase-2 Enhancements

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

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

NBAR2 Custom Protocol

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/configuration/15-2mt/nbar2-custom-protocl.html

Protocol Pack Licensing

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/configuration/15-2mt/NBAR_Protocol_Pack.html

New Hardware Features Supported in Cisco IOS Release 15.2(4)M

This section describes new and changed features in Cisco IOS Release 15.2(4)M. Some features may be new to Cisco IOS Release 15.2(4)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 15.2(4)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.

High Density Analog Gateway

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

http://www.cisco.com/en/US/docs/routers/access/vg350/hardware/installation/guide/vg350hig

Multimode 4G LTE for Cisco 819 ISRs and eHWICs

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

Cisco 819 Hardware Installation Guide:

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

Cisco 819 Software Configuration Guide:

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

Cisco 819 4G LTE Integrated Services Routers Release Notes:

http://www.cisco.com/en/US/docs/routers/access/800/819/release/notes/RN_819.html

4G LTE EHWIC Hardware Installation Guide:

http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/EHWIC-4G-LTEHW.html

4G LTE EHWIC Software Configuration Guide:

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/EHWIC-4G-LTESW.html

4G LTE EHWIC Release Notes:

http://www.cisco.com/en/US/docs/routers/access/interfaces/Release/Notes/RN_MM4G3GWAN.pdf

WLAN Support on 819 Series ISR G2 Routers

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

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

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 15.2(4)M

This section describes new and changed features in Cisco IOS Release 15.2(4)M. Some features may be new to Cisco IOS Release 15.2(4)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 15.2(4)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.

BFD Support for EIGRP IPv6

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2mt/ire-bfd-ipv6.html

BGP: Graceful Shutdown (GSHUT)

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_bgp/configuration/15-2mt/irg-grace-shut.html

Cisco IP Multiplexing

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mob_ntwks/configuration/15-2mt/imo-ip-multiplex.html

CME, SRST Version 9.1

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

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

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

EIGRP Route Tag Enhancements

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-2mt/ire-en-rou-tags.html

GET VPN Support with Suite B

The GET VPN Support with Suite B feature adds support of the Suite B set of ciphers to Cisco Group Encrypted Transport (GET) VPN.

Suite B is a set of cryptographic algorithms that includes AES as well as algorithms for hashing, digital signatures, and key exchange. Suite B for IPsec VPNs is a standard and has been defined in RFC 4869. Suite B provides a comprehensive security enhancement for Cisco IPsec VPNs, and it enables additional security for large-scale deployments. Suite B is the recommended solution for organizations requiring advanced encryption security for the wide-area network (WAN) between remote sites.

The GET VPN Support with Suite B feature introduces or modifies the following commands: **client rekey hash**, **group size**, **identifier**, **rekey sig-hash algorithm**, and **show crypto gdoi**.

IKEv2 Load Balancer Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg-clb-supp.html

IPSLA Multicast Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipsla/configuration/15-2mt/sla_mcast_suppt.html

IS-IS IPv6 Administrative Tag

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-2mt/ip6-route-isis-adm-tag.html

IS-IS IPv6 Advertise Passive Only

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_isis/configuration/15-2mt/ip6-route-isis-adv-pass-onl.html

Metadata NBAR Integration

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mdata/configuration/15-2mt/mdata-nbar-intgrtn.html

Multiple Destination Pattern Support on Voice Dial Peer

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

http://www.cisco.com/en/US/docs/ios-xml/ios/voice/dialpeer/configuration/15-2mt/vd-dp-overview.html

Multiple PPPoE Clients Support on PVC with Configurable MAC Address

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

http://www.cisco.com/en/US/docs/ios-xml/ios/bbdsl/command/bba-m1.html#GUID-CC326925-AD9D-4EE9-8A2A-2C4688B96DCF

NTPv4 MIB

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

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/configuration/15-2mt/bsm-ntp4-mib.html

OSPFv3 MIB

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

http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_ospf/configuration/15-2mt/iro-ospfv3-mib.html

OSPFv3 VRF-Lite/PE-CE

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

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

Proxy Mobile IPv6 Support for MAG Functionality

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

http://www.cisco.com/en/US/docs/ios-xml/ios/mob_pmipv6/configuration/15-2mt/imo-pmipv6-mag-support.html

Raw Socket Transport

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

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

Routed Pseudowire and Routed VPLS

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

http://www.cisco.com/en/US/docs/routers/access/ISRG2/software/feature/guide/RoutedPW.pdf

RSVP over UDP

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

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/15-2mt/config_rsvp.html

ScanSafe Web Security

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

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/15-2mt/scansafe-web-sec.html

Note The ISR Web Security with Cisco ScanSafe feature in this IOS release is under controlled availability. If you intend to use this feature please contact your Cisco representative. He or she will provide you the necessary guidance in implementing this feature into your network. For additional information please contact us at ss-isr-connector-sales@cisco.com.

Support for Algorithms in the Suite B Specification for IPSec by the On-Board Crypto Engine in Cisco Integrated Services Routers Generation 2: 800 Series, 1900 Series, 2901, 2911, 2921, 2935R, 3925E, and 3945E.

The IPSec algorithms required by Suite B are now supported by the hardware crypto engine on the Cisco Integrated Services Routers Generation 2: 800 Series, 1900 Series, 2901, 2911, 2921, 2935R, 3925E, and 3945E, each of which has embedded hardware-accelerated VPN encryption.

Suite B requirements comprise four user-interface suites of cryptographic algorithms for use with IKE and IPsec, which are described in RFC 6379 and RFC 6380. Each suite consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm.

Suite B provides a comprehensive security enhancement for Cisco IPsec VPNs, and it allows additional security for large-scale deployments. Suite B is the recommended solution for organizations requiring advanced encryption security for the wide-area network (WAN) between remote sites.

For detailed information about Cisco IOS IPsec features in 15.2(4)M that support Suite B, see the following documents:

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_pki/configuration/15-2mt/sec-cert-enroll-pki.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-2mt/sec-cfg-vpn-ipsec.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ikevpn/configuration/15-2mt/sec-key-exch-ipsec.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg-ikev2-flex.html

http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-2mt/sec-get-vpn-suiteb.html

TCP—Configurable Keepalive Timer

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/15-2mt/iap-tcp.html

UCS-E Series Server

The Cisco UCS E-Series Server Modules (E-Series Servers) are the next generation of Cisco UCS Express servers. E-Series Servers are a family of size, weight, and power efficient blade servers that are housed within the Generation 2 Cisco Integrated Services Routers (ISR G2). E-Series Servers provide the following:

- A general purpose compute platform for branch-office applications deployed either on the Microsoft Windows or Linux operating systems, or deployed as virtual machines on hypervisors, such as VMware vSphere or Microsoft Hyper-V.
- A hosting platform for virtualized Cisco branch-office services, such as Cisco Virtual Wide Area Application Services (vWAAS), Cisco Unified Communications Manager (Unified CM), and Cisco Enterprise Content Delivery System (ECDS).

VPN ISM IPv6 Support

The VPN ISM IPv6 Support feature enables IPv6 capability on Reventon so that IPsec IPv6 traffic is offloaded along with IPsec IPv4 traffic to the Integrated Services Module (ISM). Reventon is an ISM that delivers a peak rate of 600 Mbps IPsec encryption and decryption on Integrated Services Routers Generation 2 (ISR G2) devices.

Note Note: The VPN ISM IPv6 Support feature does not support high availability (HA) and IPv6 dynamic crypto maps.

VRRPv3 Protocol Support

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

http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/15-2mt/fhp-vrrp.html

Zero Touch Recovery

Compact flash cards can help you configure new or replacement routers, and to recover the configuration of a failed router. For example, if the Connected Grid Swap Drive feature is enabled, you can transfer the same system configuration information from one router to another by using a compact flash memory card (or compact flash card) while the routers are operating. This is done by inserting an optional compact flash card in slot CF1 and copying all contents of CF0. After the copy operation is completed, you can remove and insert this compact flash card unit in slot CF0 of either a new router or a replacement router for a failed unit. When the new or replacement router is rebooted, it uses the configuration from the compact flash card as the running and startup configuration. This functionality enables you to quickly configure new or replacement routers with a standard configuration with little or no manual configuration required.

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

http://www.cisco.com/en/US/docs/routers/connectedgrid/modules/switch/gsg/intro.html#wp1154774

Important Notes

The following information applies to all releases of Cisco IOS Release 15.2(4)M.

Important Notes for Cisco IOS Release 15.2(4)M

This section describes important issues that you should be aware of for Cisco IOS Release 15.2(4)M and later releases.

Images Deferred Because of Caveat CSCub34396

In Cisco IOS Release 15.2(4)M, images for all platforms have been deferred because of a severe defect. This defect has been assigned Cisco caveat ID CSCub34396; Headline: traffic flow in dmvpn is flowing unencrypted.

The software solution for these deferred images is Cisco IOS Release 15.2(4)M1.

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

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

ScanSafe Web Security

The ISR Web Security with Cisco ScanSafe feature is under controlled availability in Cisco IOS Release 15.2(4)M and later releases. If you intend to use this feature please contact your Cisco representative. He or she will provide you the necessary guidance in implementing this feature into your network. For additional information please contact us at ss-isr-connector-sales@cisco.com.

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 15.2(4)M4

The following behavior changes are introduced in Cisco IOS Release 15.2(4)M4:

- The **radius-server attribute 66 include-in-access-req** and **radius-server attribute 67 include-in-access-req** commands are added to identify the PPTP tunnel-specific information.

  Old Behavior: The RADIUS server does not have Point-to-Point Tunneling Protocol (PPTP) tunnel-specific information because the tunnel-client endpoint and tunnel-server endpoint attributes are missing in the access-request packets sent to the RADIUS server.

  New Behavior: The following commands are introduced to identify the hostname or address of the network access server (NAS) at the initiator and server end of the Point-to-Point Tunneling Protocol (PPTP) tunnel by sending the Tunnel-Client-Endpoint attribute and the Tunnel-Server-Endpoint attribute in access-request packets to the RADIUS server.

  - **radius-server attribute 66 include-in-access-req**
  - **radius-server attribute 67 include-in-access-req**

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sec-cr-r1.html#GUID-3020A932-7C95-4231-8B6C-396289F361CC

  http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sec-cr-r1.html#GUID-4E9E50BE-B625-4B4A-B7CA-DAC0B9DF57A6

- Installing simultaneous QoS policies on both ATM subinterface and ATM PVC, or on different Frame Relay subinterface and Frame Relay DLCI, results in a SIP 200 crash.

  Old Behavior: Installing simultaneous QoS policies on both ATM subinterface and ATM PVC, or on different Frame Relay subinterface and Frame Relay DLCI is allowed.

  New Behavior: Installing simultaneous QoS policies on both ATM subinterface and ATM PVC, or on different Frame Relay subinterface and Frame Relay DLCI is not allowed.

  Additional Information:

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfgsip.html#wp1233460

Cisco IOS Release 15.2(4)M3

The following behavior changes are introduced in Cisco IOS Release 15.2(4)M3:

- The “aaa accounting delay-start extended-time” command is introduced to add Framed-IP-Address to the accounting start packets in the dual stack scenario.

  Old Behavior: The RADIUS attribute 8 (Framed-IP-Address) is not included in the accounting start packets in the following two scenarios:

  - The user is a dual-stack (IPv4 or IPv6) subscriber.
  - The IP address is from a local pool and not from the RADIUS server.

  New Behavior: The “aaa accounting delay-start extended-time” command is introduced to delay the accounting start records for the configured time (in seconds) after the IPCPv6 address is sent to the RADIUS server. During this configured delay time, the IPCPv4 address is sent and the Framed-IPv4-Address is added to the accounting start record. If the IPCPv4 address is not sent in the configured delay time, the accounting start record is sent without the Framed-IPv4-Address.

  Additional Information:

http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html

- The NHRP syslog error message includes the IP address of the node where the error originates

  Old Behavior: The NHRP syslog error message does not include the IP address of the node where the error originates, the source NBMA, and the destination address

  New Behavior: The NHRP syslog error message includes the IP address of the node where the error originates, the source NBMA, and the destination address.

  Additional Information:

  http://cisco.com/en/US/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-s/sec-conn-dmvpn-tun-mon.html

- Initial INVITE with 0.0.0.0 call flow is supported.

  Old Behavior: Initial INVITE with 0.0.0.0 is not supported unless ACK contains valid IP address.

  New Behavior: This call flow is supported.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/sip/configuration/15-mt/voi-sip-rfc.html#GUID-B6E5879A-D5DC-4E2C-BC97-AC927985E10E

- Transmission of IPsec Dummy Packets per RFC 4303

  Old Behavior: IOS devices does not conform to RFC 4303.

  New Behavior: IOS devices conforms to RFC 4303 to enable transmitting dummy packets.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html

- IPv6 support is added for legacy Control Plane Policing (CoPP) on Cisco Express forwarding interfaces.

  Old Behavior: IPv6 support is not available for CoPP, resulting in a failure of policing and rate limiting.

  New Behavior: IPv6 support is added for legacy CoPP on Cisco Express forwarding interfaces that support aggregate-scope policing and rate limiting.

- The **extended** keyword is added to the **show waas status** command.

  Old Behavior: The show waas status command displays the status of Wide Area Application Services (WAAS) Express.

  New Behavior: The extended keyword is added to the show waas status command. The extended keyword provides complete information for WAAS Express.

  Additional Information:

  http://www.cisco.com/en/US/docs/ios/wan/command/reference/wan_s2.html#wp1101997

Cisco IOS Release 15.2(4)M2

The following behavior changes are introduced in Cisco IOS Release 15.2(4)M2:

- The **show aaa servers** command output displays estimated outstanding/throttled access/accounting transactions.

  Old Behavior: Outstanding access transactions are left unprocessed on RADIUS server.

New Behavior: The **show aaa servers** command output displays the number of access, authorization, and accounting requests and estimated outstanding/throttled access/accounting transactions that are being processed. The **clear aaa counters** servers all command clears all counters except estimated outstanding/throttled access/accounting transactions. These values will automatically reduce.

Additional Information:
http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-s2.html#GUID-971F25CD-9424-4B5C-8B64-C344CBA0977D

http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-c1.html#GUID-68BC9DC6-282E-4192-A4D1-B9DE80AD26A7

- Up to ten classless static routes are supported using option 121 on dhcp client.

  Old Behavior: Only two classless static routes were supported using option 121 on the dhcp client.

  New behavior: Up to ten classless static routes are supported using option 121 on dhcp client.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-2mt/config-dhcp-client.html

- The advanced protocol pack is provided as the base protocol pack version with a licensed Cisco image.

  Old Behavior: A default protocol pack was is provided as the base protocol pack version with a Cisco image.

  New Behavior: Default protocol packs are no longer supported. The advanced protocol pack is provided as the base protocol pack with a licensed Cisco image on a device. The advanced protocol pack has the complete set of Protocol Description Language files (PDLs) available for a release. The standard protocol pack is provided as the base protocol pack with an unlicensed Cisco image.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/configuration/15-2mt/NBAR_Protocol_Pack.html

- On an Advanced Protocol Pack, only a Packet Description Language Module (PDLM) with “Advanced Protocol Pack” in the NAME field can be loaded. On a Standard Protocol Pack, only a PDLM with “Standard Protocol Pack” in the NAME field can be loaded.

  Old Behavior: No restriction on the NAME field for loading an Advanced or Standard Protocol Pack.

  New Behavior: On an Advanced Protocol Pack, only a Packet Description Language Module (PDLM) with “Advanced Protocol Pack” in the NAME field can be loaded. On a Standard Protocol Pack, only a PDLM with “Standard Protocol Pack” in the NAME field can be loaded.

  Additional information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/configuration/15-2mt/NBAR_Protocol_Pack.html

- BGP Processing of the Removal of Private AS Numbers from 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:

  1. **neighbor remove-private-as** processing.
  2. **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:

1. **neighbor remove-private-as** processing.
2. **set as-path prepend** or **set as-path prepend last-as**.

- Metadata service functionality is added to the SAF feature.

  Old Behavior: Metadata service functionality is not available.

  New Behavior: The Cisco SAF Forwarder can send service metadata to its neighbor SAF nodes. Metadata is XML information, and service data is information that a server communicates to a client about itself. The service metadata does not propagate in mixed 15.1(3)S) and 15.2(1)S environments until such time that the version of EIGRP and SAF is upgraded.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/saf/configuration/15-2s/saf-15-2s-book.html

- Default change.

  Old Behavior: Earlier, the 7600 platform, on GRE tunnels protected with IPsec and static VTI tunnels, required the configuration of lesser “ip mtu” explicitly on the tunnel interface to prevent fragmentation post encryption.

  New Behavior: By default, all overheads including GRE and IPsec are accounted beforehand and the resultant value (i.e. Transport MTU - overhead [GRE+IPsec]) is programmed as ip mtu on these tunnels.

  Additional Information:
  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/7600series/76cfvpn1.html#wp2518134

- The default mode for the default transform set is changed to tunnel.

  Old Behavior: The default mode for all transform sets, including the default transform set, is tunnel.

  New Behavior: The default mode for the default transform set is transport; the default mode for all other transform sets is tunnel.

  Additional Information:
  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2s/sec-cfg-ikev2-flex.html#GUID-F936D366-EEE2-4016-A8CA-DE4EF6C1B205

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-2mt/sec-cfg-ikev2-flex.html#GUID-F936D366-EEE2-4016-A8CA-DE4EF6C1B205

  http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-sy/sec-cfg-ikev2-flex.html#GUID-F936D366-EEE2-4016-A8CA-DE4EF6C1B205

- Cable detection is extended to analog FXSLS, FXSGS, and FXOGS voice ports.

  Old Behavior: Cable detection existed on analog FXOLS voice port only.

  New Behavior: Cable detection is extended to analog FXSLS, FXSGS, and FXOGS voice ports, and a new CLI cable-detect-poll-timer is introduced to configure the cable polling timer value for background polling processes.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr1/vcr-c1.html

  http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr4/vcr-s9.html#GUID-DDA37612-EDAE-42A4-B84E-1D1D345183B5

- IKEv2 default max in-negotiation CAC counter has been modified to 40.

  Old Behavior: IKEv2 default max in-neg CAC counter was 1000.

New Behavior: IKEv2 default max in-neg CAC counter has been modified to 40 and is true for all platforms.

Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-s3.html

- Missing threshold for logout calls in the queue display.

  Old Behavior: The threshold is missing for logout calls in the queue display. The CLI is **hunt-group logout** [**DND | HLog**].

  New Behavior: The **notify** keyword and **threshold-number** argument are added in the **hunt-group logout** command to enable the indication of the calls in queue for logout agents using the Hlog Programmable Line Key:

  hunt-group logout [**DND | HLog | notify | threshold-number**]

- Unable to lock out the background settings using the xml append file. Users cannot configure commonProfile xml content and comprise it with the callLogBlfEnabled enabled by “presence call-list”.

  Old Behavior: Users cannot configure the commonProfile xml content.

  New Behavior: Introduced the following new CLI to set parameters under commonProfile section in IP phone SEP*.cnf.xml configuration files:

  service profile [**phonePassword password | callLogBlfEnabled | backgroundImageAccess false**]

- **Monitor pcm-trace profile** CLI extended to include analog and BRI voice ports.

  Old Behavior: Configuring **monitor pcm-trace profile** to perform ds0 dumps for analog and BRI voice ports was not possible.

  New Behavior: **Monitor pcm-trace profile** CLI extended to allow dsO dumps to be configured for analog and BRI voice ports.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/monitor_event-trace_through_Q.html

- WebEx data, streaming, video, and voice application types are not supported.

  Old Behavior: The **webex-data**, **webex-streaming**, **webex-video**, and **webex-voice** keywords are available in the **match application** command.

  New Behavior: The **webex-data**, **webex-streaming**, **webex-video**, and **webex-voice** keywords are not available in the **match application** command.

  Additional Information: http://www.cisco.com/en/US/docs/ios-xml/ios/qos/command/match_access-group_through_mls_ip_pbr.html#GUID-05DC6228-60F5-428A-AEE0-2C4FE9FC848E

- Setting of factory defaults.

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

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