Release Notes for Cisco IOS Release 15.8(3)M1

The following release notes support Cisco IOS Releases 15.8(3)M1 and higher releases. These releases support the Cisco 5900 Embedded Services Routers (ESR) platforms. These release notes are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and how to obtain support and documentation.

Contents

This publication consists of the following sections:

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

Image Information and Supported Platforms

Note You must have a Cisco.com account to download the software.

Cisco IOS Release 15.8(3)M1 includes the following Cisco IOS images:

- c5915-adventerprisek9-mz.SPA
- c5915-entbase-mz.SPA
- c5921i86-universalk9-ms.SPA
- c5921i86-entbasek9-ms.SPA
- c5921i86-entbasek9-tar.SPA
- c5921i86-universalk9-tar.SPA
- c5930-adventerprisek9-mz.SPA
- c5940-adventerprisek9-mz.SPA
- c5921i86-universalk9_npe-ms.SPA
- c5921i86-universalk9_npe-tar.SPA

Related Documentation

The following documentation is available:

- Cisco 5900 Embedded Services Routers

  http://www.cisco.com/c/en/us/support/routers/5900-series-embedded-services-routers/tsd-products-support-series-home.html
- IOS Bulletins—You can find bulletins at:

  http://www.cisco.com/cisco/web/psa/default.html?mode=prod&level0=268438303
- Cisco IOS 15.8M cross-platform release notes:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-8m/release/notes/15-8-3-m-rel-notes.html

New Features Supported

This release supports software changes made in IOS that exist on other platforms.

802.1x Support

For the c5915 platform, the 802.1x feature will be supported. The design and implementation are platform independent.

There are some new commands available which are shown below:

To enable AAA:

```
aaa new-model
```

Create Authentication Method, Support:

```
aaa authentication dot1x {default | listname} method1 [method2...]
```

Enable 802.1X port-based authentication:

```
dot1x system-auth-control
```

Enable 802.1X port-based authentication on the interface:

```
access-session port-control {auto | force-authorized | force-unauthorized}
```

IP Device Tracking

For the c5915 platform, IP device tracking API will be implemented using registries and callbacks. IPDT will send and receive various notifications, and there will be registries for features to send commands to IPDT and query the device database.

There is a command to globally enable or disable tracking of IP devices. When disabled, no notifications will be sent and no devices will be learned (as active). If some other feature has caused a detection mechanism to be enabled, detected devices will be added as inactive entries.

Clear Commands

The device tracking database can be cleaned up by using the clear commands. The entries that are cleared will be deleted from the database, and a notification will be sent to registered features, and an ARP probe will immediately be sent to the device.

```
clear ip device tracking ip <ip address>
clear ip device tracking mac <mac address>
clear ip device tracking interface <interface> [untrust]
clear ip device tracking all [untrust]
```

Show Commands

The show commands allow the configuration and contents of the device tracking database to be displayed.

```
show ip device tracking ip <ip address>
show ip device tracking mac <mac address>
show ip device tracking interface <interface>
show ip device tracking all [count]
```

MPLS-VPN Support

For the c5921 platform, the design and implementation are platform independent. Extend MPLS connectivity for private networks that are connected by IP-only path. A dynamic IPsec spoke-spoke tunnel is used to provide this connectivity. The MPLS-VPN is available only for Layer-3 switching.

Use Case

Implement Intranet VPN between the Customer A Site 1 and Customer A Site 2. The customer network consists of the two routers which are CEA-1 and CEA-2, and there are two other loopbacks on PE1-AS1 and PE2-AS1 as part of the VRF Customer A and be redistributed into the MP-BGP routing contexts.

Configuring MPLS forwarding is the first step to provision the service provider's MPLS VPN backbone. This step ensures the service provider's readiness to provide MPLS-related services to prospective customers. At a minimum, the steps to configure MPLS forwarding on PE routers are:

- Enable CEF (Cisco Express Forwarding)
- Configuring IGP Routing Protocol on the PE routers
- Configure MPLS or label forwarding on the PE interfaces connected to the Provider

  VRFs (Virtual Routing and Forwarding Table) on the PE routers, and below are the configuration steps to configure VRF Definitions:
- Configure VRF on PE router

  Configure the VRF Customer A on PE1-AS1 and PE2-AS1 router. This results in the creation of a VRF routing table and a Cisco Express Forwarding (CEF) table for Customer A. Below we see that Customer A VRF being configured on PE1-AS1 router. (Note the VRF name is case sensitive.)

  Note While removing the VRF From the router, the all-existing IP Addresses which are associated with Customer A VRF will be removed as shown above.

- Configure the RD

  The RD creates routing and forwarding tables. The RD is added to the beginning of the customer's IPv4 prefixes to convert them into globally unique VPNv4 prefixes. Next we see the configuration for defining the RD under the VRF.

  The RD can be used in either of these formats:

  – 16-bit AS number: Your 32-bit number (for example, 1:100)

  – 32-bit IP address: Your 16-bit number (for example, 10.10.10.101:1)
- Configure the import and export policy

  Configure the import and export policy for the MP-BGP extended communities. The policy is used for filtering routes for that particular RT. below it shows the relevant configuration for defining import and export policy.

  Note You can simply write use the same value for both (import and export) and we can verify that in our running-configuration we see that the values are same for both Export and Import.

- Associate VRF with the interface

Associate virtual routing/forwarding instance (VRF) with an interface or sub-interface in this Customer A. (Associating the VRF to an interface results in removal of the IP address from that interface. This is only if VRF was associated to an interface that had the IP address already configured. This means that the IP address will have to be reconfigured after the VRF is associated with that interface.)

Note The above steps are also followed in PE2-AS1, as they both require same configurations.

You are also required to add Interface Loopback 1 under VRF Customer A.

You can verify the above configuration with the Below Commands:

```
show ip vrf
show ip vrf interfaces
```

Configuration of BGP PE-PE Routing on PE Routers

Configuring BGP PE-PE routing between the PE routers is the next step in an MPLS VPN deployment. The purpose of this step is to ensure that VPNv4 routes can be transported across the service provider backbone using MP-iBGP. The P router is transparent to this entire process and, therefore, does not carry any customer routes.

- Configure BGP routing on PE routers

  Enable BGP routing and identify the AS on the PE1-AS1 and PE2-AS1 routers as below:

- Configure the MP-iBGP neighbors

  Configure the remote MP-iBGP neighbor and use the loopback interface as the source of BGP messages and updates. Note that you have to use the update-source command only when the neighbor is peering to your loopback address. This is irrespective of whether it is an iBGP or eBGP neighbor.

- Configure the VPNv4 address family

  Configure the address family for VPNv4 under the BGP configuration process. This step allows you to enter the VPNv4 address family to activate the VPNv4 neighbors. Activate the iBGP neighbor, which is essential for transporting VPNv4 prefixes across the service provider backbone. Using next-hop-self is optional and is primarily used when the service provider has an eBGP PE-CE routing with the customers, because internal BGP (iBGP) sessions preserve the next-hop attribute learned from eBGP peers, which is why it is important to have an internal route to the next hop. Otherwise, the BGP route is unreachable. To make sure you can reach the eBGP next hop, include the network that the next hop belongs to in the IGP or use the next-hop-self neighbor command to force the router to advertise itself, rather than the external peer, as the next hop.

  In addition, configure the propagation of the extended communities with BGP routes so as to enable RT propagation, which identifies the VPNs that the routes have to be imported into.

- Configure the IPv4 address family

  Configure the peer VRF IPv4 address family under the BGP configuration process. This step allows you to enter the IPv4 networks that will be converted to VPNv4 routes in MP-BGP updates. For simplicity, redistribution of all connected networks is configured into the MP-BGP process.

  After configuring BGP PE-PE routing between the PE routers, you can verify that the MP-iBGP neighbors are operational by issuing any of the following commands:

```
show ip bgp vpnv4 all summary
show IP bgp vpnv4 all
```

```
show ip bgp summary
show ip bgp neighbor ip-address
```

No special configurations need to be performed on the P routers P1-AS1 and P1-AS2 for MPLS VPN support. Because the P routers only participate in MPLS labeled packet forwarding, the only requirements are those of an LSR in an MPLS network, namely, IGP for NLRI exchange and LDP for label assignment and distribution. As always, CEF needs to be enabled on all interfaces configured for MPLS forwarding.

You can configure a default route on Customer Site pointing to it's respective PE Routers and initiate a Ping to see the result.

SSMS Server Support

For c5921 platform, we support smart licensing. The smart agent version needs to be upgraded and in turn, the registration server needs to be upgraded. For these smart agent upgrades, the SSMS server needs to be upgraded. Once SSMS server is setup the platform smart agent license version need to be upgraded in sync with the new SSMS server.

Support has been added for seven types of license throughputs available from "level zero to level six" for registration. They are as follows:

- c5921-x86-level0 5 Mbps
- c5921-x86-level1 10 Mbps
- c5921-x86-level2 25 Mbps
- c5921-x86-level3 50 Mbps
- c5921-x86-level4 100 Mbps
- c5921-x86-level5 200 Mbps
- c5921-x86-level6 500 Mbps

Note Default throughput is c5921-x86-default @ 8 Kbps

The user may register for any one of the throughput levels where default throughput 8 Kbps is already configured by default.

Once the user registered for Evaluation mode they can configure up to 500 Mbps. Once the Evaluation mode is completed with the specific throughput level the throughput will return to default throughput level i.e. 8 Kbps.

For required throughput the user need to register with respective token.

On the router, please follow below commands:

Commands to Register

```
Router# configure terminal
Router(config) # license smart enable
Router# end
Router# license smart register id <registration token>
```

Upon successful registration, you can confirm the configuration by enabling smart license debuging. You can then see the debug message as follows;

"SMART_LIC-6-AGENT_REG_SUCCESS: Smart Agent for Licensing Registration with Cisco licensing cloud successful"

In order to verify the license registration please use the following show command:

```
Router# show platform software license
Packet forwarding: Enabled
Current enforcement forwarding rate: 8 Kbps
Unique Device Identifier: CISCO5921-K9:9UY3149NYMF
License features supported:
       Feature              Rate     Status
  ---------------------   ---------  ------
  c5921-x86-default       8 Kbps      In Use
  c5921-x86-evaluation    50 Mbps     -
  c5921-x86-level0        5 Mbps      -
  c5921-x86-level1        10 Mbps     -
  c5921-x86-level2        25 Mbps     -
  c5921-x86-level3        50 Mbps     -
  c5921-x86-level4        100 Mbps    -
  c5921-x86-level5        200 Mbps    -
  c5921-x86-level6        500 Mbps    -
```

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or closed (resolved).

Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Cisco IOS Release 15.8(3)M1

The following sections list caveats for Cisco IOS Release 15.8(3)M1:

Open Caveats

There are no open caveats with this release.

Closed Caveats

The following caveats are fixed with this release:

- **CSCvj20285**

  Stack corruption crash on ESR.

  Symptoms:

  ESR 5921 crashes due to stack corruption. Crashinfo has messages like the following example:

  ```
  %SYS-3-OVERRUN: Block overrun at A32C4C30 (red zone 00000000)
  ```

```
%SYS-6-BLKINFO: Corrupted redzone blk A32C4C30, words 64, alloc CB34368, InUse,
dealloc 0, rfcnt 1
```

Conditions:

Hardware or software error conditions can lead to this.

Workaround:

There is no workaround.

- **CSCvj46903**

  On the c5921: License enforcement to default 8kbps does not happen, even after evaluation period has expired.

  Symptoms:

  License enforcement to 8kbps after evaluation period expired.

  Conditions:

  When evaluation period expires.

  Workaround:

  There is no workaround.

- **CSCvj85142**

  On the c5921: Throughput Level getting configured even after the evaluation license has expired.

  Symptoms:

  Able to configure the Throughput Level once the Evaluation license got expired.

  Conditions:

  Once the Evaluation license got Expired the throughput license level should not be able to configure.

  Workaround:

  There is no workaround.

- **CSCvm55010**

  USB support needs to be added

  Symptoms:

  The 5921 does not support any devices connected to its USB port.

  After unplugging and then plugging in devices from USB port, the device was not able to send/receive traffic to/from USB port.

  Conditions:

  After unplugging and then plugging in devices from USB port.

  Workaround:

  Resolved in this release.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
