Release Notes for Cisco IOS Release 15.7(3)M2

The following release notes support Cisco IOS Releases 15.7(3)M2 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 15.7(3)M2 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 15.7M cross-platform release notes:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-7m/release/notes/15-7-3-m-rel-notes.html

New Features Supported

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

DLEP Compliance to RFC 8175

The DLEP protocol runs between a router and its attached modem devices, allowing the modem to communicate link characteristics as they change, and convergence events (acquisition and loss of potential routing next-hops). DLEP provides an event driven mechanism instead of a timer-driver one and enables routing protocols to be radio-aware. Support includes a generalized TTL security mechanism for UDP in order to be compliant with RFC 8175.

Generalized TTL Security Mechanism (GTSM) Support

GTSM is designed to protect a router's IP-based control plane from CPU-utilization based attacks. The GTSM mechanism is equally applicable to both TTL (IPv4) and Hop Limit (IPv6).

GTSM in DLEP:

- If a DLEP signal is received with a TTL value that is NOT equal to 255 (254 for IPv4), the receiving implementation MUST ignore the Signal.
- If a DLEP packet in the TCP stream is received with a TTL value other than 255 (254 for IPv4), the receiving implementation MUST immediately transition to the Session Reset state.

Web Services Management Agent (WSMA)

WSMA is a family of embedded agents, used by a point-point management application to fully manage a device. It provide users access to similar capabilities as the CNS agents (CONFIG, EXEC, FILE SYSTEM, DIAGNOSTICS) but via an open standards point-to-point connection. These agents leverage the knowledge and code base of the CNS agents and provide comparable mechanisms in a point-point environment rather than the Event Bus which is the basis of CNS.

CNS agents have proven to be a useful set of management interfaces for scalable management of Cisco devices, but with the following deficiencies:

- Proprietary TIBCO communication bus
- Inflexible protocol interfaces
- Steep application developer learning curve
- Requires a proxy agent (no direct access)

The WSMA addresses these deficiencies. The WSMA is accessible over SSH and HTTP(S) transports. The WSMA transport layer is configurable to be run in both session initiator and listener mode. This allows the WSMA on IOS to run in server mode regardless of how the transport connection is made to the device. The WSMA is accessed directly over the SOAP/SSH or SOAP/HTTP(S) transport.

Additional information can be found in the WSMA Configuration Guide.

Connected Grid Network Agent (CGNA)

The CGNA is a helper to facilitate NMS operations. It is a light-weight process/task in IOS, communicating with NMS via WSMA and HTTPS sessions. The following functions are supported by the CGNA:

- ZTD Support
- Periodic inventory update
- Firmware upload support
- Gzip support

Additional information can be found in the Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide (Cisco IOS)

SCEP Enrollment with Custom Device Credential

The following section describes the use of custom device credential for the SCEP enrollment on the ESR5921.

Changes to the SCEP Enrollment EEM policy

On the ESR5921, there are several changes to the existing SCEP enrollment EEM policy compared to the CGR1K platform. The changes are logged in the header of the policy script tm_ztd_scep.tcl.

New control environment variables:

Variable	Description
ZTD_SCEP_cust_enroll_cred	Controls which credential to use for the enrollment. • Default is "FALSE", which uses the cisco sudi for enrollment credential. • If "TRUE", a custom credential is used for enrollment.
ZTD_SCEP_cust_sudi_url	Location where custom credential files are stored
ZTD_SCEP_cust_sudi_pwd	Password of encrypted custom credential's private key

Requirements

For a custom device credential, there needs to be three parts:

- A device specific certificate (for example: cust_sudi.crt)
- A private key associated with the device certificate (for example: cust_sudi.prv)
- The certificate of the CA server signing the device certificate (for example: cust_sudi.ca)

In the device certificate, it should contain the PID and serial number for this device in its subject name, which can be used on the RA server for authorization through AAA. In order to minimize the compatibility issue, use Cisco CA servers to generate credentials.

Deployment

On the RA Server:

- Install the custom CA server's certificate (For example: cust_sudi.ca) into the CA trustpoint (for example: CUST_CA).
- Configure the RA server to grant requests authenticated by custom CA.
- Configure the AAA to use a custom PID and serial number for authorization, which is the same as with the CGR1K.

On the ESR5921:

- Deploy the device credential files into nvram, flash or another location.
- Configure the EEM environmental variables to use a custom credential.
- Trigger the enrollment.

Example Installation

Custom credentials are presented as cust_sudi (.crt .prv .ca) in PEM format. Other setups and configurations are identical to the CGR1K SCEP enrollment. The following section describes the differences.

On the RA Server

Import a custom CA certificate:

```
esr_ra#config t
Enter configuration commands, one per line.  End with CNTL/Z.
esr_ra(config)#cry pki trustpoint CUST_CA
esr_ra(ca-trustpoint)#
Jan 25 23:23:07.592: CRYPTO_PKI: Creating trustpoint CUST_CA
esr_ra(ca-trustpoint)#enrollment terminal
esr_ra(config)#cry pki authenticate CUST_CA

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIDAjCCAeqgAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRAwDgYDVQQDDAdjdXN0
X2NhMB4XDTE4MDExNjIxMTIyMloXDTIxMDExNTIxMTIyMlowEjEQMA4GA1UEAwwH
Y3VzdF9jYTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJti8mgKvIIv
f53VuRwb4hRaFI8Om4ytM3MeSQZGMz3jeQnoVcf89xUHQ/J44kI4UHEqdIojmb87
teuMoszFbhTBfBo5qaGT/VH59fB1R+NlP+aTfXczxasz7F3BReVuRBpqkUizofJi
sTitPChtdWU+A9mf/5gGRg0XAkKFk3SFmoMUlqx+1z6W1NRVrpp1VF2NSDI85Mwp
3mY+IUA4P30wVA0VHc8B4Z1MFGj/1gndOfajSe46Sb0BX175kiymElOO8QqmXm5n
JBE5plFdHg/QU3z/56UC6p1vv9fCAoxVk0dUm1dpfA1c6WebF3kkBH6TyVphmZt1
qJ0b2e2mzEECAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMC
AYYwHwYDVR0jBBgwFoAUsyUTzlY0/tJmYTt7rTMVxTK+mPswHQYDVR0OBBYEFLMl
E85WNP7SZmE7e60zFcUyvpj7MA0GCSqGSIb3DQEBBAUAA4IBAQBqNJAHH95ZUz75
MHp0oQe3sPm904WB4qsvONQTx36AUss92tK74wBL25h2mq+EdXgTpCuaT1s4eIKV
wpC9JDmeoS0DX3snJj7F+kzF04aoLZ440FOWxGcGsMvdupq0VJvrGau1SseJqKFA
xet9NPonDtPnewLzXelC+KgVFxpAguWGwb0G0GcAn6tUYJIXUGpphAjLZj2pHxbq
Yy2/MANkq+Cn4bo8jaYNmQSK9UNtgLztKXMHJJoeKsBjfc/DOHLMKqLeSA8atlfH
5ggncLqMoOC/xUsH2GguSNmS210nd1ZbQ5dLfxbgu2O/xeCPkGGn+o+PbH0BNaN2
y85OBDVC
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
      Fingerprint MD5: 2676D4CD 25A4E2E9 BACC55DE CB04B2F6
      Fingerprint SHA1: AEF90CBD F4CC3F77 7474FCA6 D0C706E1 038A9516

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
esr_ra(config)#
```

Configure RA server:

```
!
crypto pki server myra
 no database archive
 issuer-name cn=ioscs RA,ou=ioscs RA
 grant auto trustpoint CUST_CA
 grant auto rollover ra-cert
 hash sha1
 mode ra
!
```

On the ESR5921

This procedure assumes the custom sudi files are available on nvram:

```
esr-e1#dir nvram:
Directory of nvram:/

  245  -rw-        2684                    <no date>  startup-config
  246  ----        7101                    <no date>  private-config
    1  ----         427                    <no date>  persistent-data
    2  -rw-          17                    <no date>  ecfm_ieee_mib
    3  -rw-         805                    <no date>  CiscoLicensi#1CA.cer
    4  -rw-          14                    <no date>  myra.ser
    5  -rw-        1103                    <no date>  cust_sudi.ca
    7  -rw-        1743                    <no date>  cust_sudi.prv
    9  -rw-        1176                    <no date>  cust_sudi.crt

262144 bytes total (242067 bytes free)

esr-e1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
esr-e1(config)#event manager environment ZTD_SCEP_CGNA_Profile CGNA_Profile
esr-e1(config)#event manager environment ZTD_SCEP_cust_enroll_cred TRUE
esr-e1(config)#event manager environment ZTD_SCEP_cust_sudi_url nvram:
esr-e1(config)#event manager environment ZTD_SCEP_cust_sudi_pwd cisco123
esr-e1(config)#event manager environment ZTD_SCEP_IDevID_trustpoint_name cust_sudi
esr-e1(config)#event manager environment ZTD_SCEP_Enabled TRUE
esr-e1(config)#event manager policy tm_ztd_scep.tcl type system authorization bypass
esr-e1(config)#end
esr-e1#
```

Run the policy manually:

```
esr-e1#event manager run tm_ztd_scep.tcl

Jan 26 06:45:47.471: %HA_EM-4-LOG: tm_ztd_scep.tcl: WARNING: Environment variable
ZTD_SCEP_LDevID_trustpoint_name has not been set. LDevID is assumed.
Jan 26 06:45:47.472: %HA_EM-4-LOG: tm_ztd_scep.tcl: WARNING: Environment variable
ZTD_SCEP_enrollment_retry_count has not been set. Will use default value of 4.
Jan 26 06:45:47.473: %HA_EM-4-LOG: tm_ztd_scep.tcl: WARNING: Environment variable
ZTD_SCEP_enrollment_retry_period has not been set. Will use a default value of 2mn.
```

```
Jan 26 06:45:50.826: %SYS-5-CONFIG_I: Configured from console by  on vty0
(EEM:tm_ztd_scep.tcl)
Jan 26 06:45:54.878: %SYS-5-CONFIG_I: Configured from console by  on vty0
(EEM:tm_ztd_scep.tcl)
Jan 26 06:45:55.406: %HA_EM-4-LOG: tm_ztd_scep.tcl: WARNING: Default IDEVID trustpoint
name overridden by environment variable ZTD_SCEP_IDevID_trustpoint_name with cust_sudi.
Jan 26 06:45:58.829: %SYS-5-CONFIG_I: Configured from console by  on vty0
(EEM:tm_ztd_scep.tcl)
Jan 26 06:46:03.348: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 26CF4621 A2F95AFC
A2655309 C1F1F553
Jan 26 06:46:03.348: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 96D56639 CA0417E2
4482FCB9 5E34BF6F 8E7FAC54
esr-e1#
Jan 26 06:46:03.460: %SYS-5-CONFIG_I: Configured from console by  on vty0
(EEM:tm_ztd_scep.tcl)
esr-e1#
Jan 26 06:46:04.091: %HA_EM-6-LOG: tm_ztd_scep.tcl: INFO: Waiting for SCEP enrollment to
complete.
esr-e1#
Jan 26 06:48:03.515: %PKI-6-CERTRET: Certificate received from Certificate Authority
esr-e1#
```

Additional Notes

For compatibility issues with the enrollment credential on the ESR5921, you may test it on the ESR5921 to make sure it can be accepted by Cisco IOS. Use these steps:

1. Make sure the credential files are named as previously stated. (.ca . prv and .crt respectively)
2. Issue the following command, assuming the credential files are cust_sudi.ca, cust_sudi.prv and cust_sudi.crt:

```
esr-e1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
esr-e1(config)#crypto pki import cust_sudi pem url flash: password cisco123
% Importing CA certificate...
Source filename [cust_sudi.ca]? <enter>
Reading file from flash:cust_sudi.ca
% Importing private General Purpose key PEM file...
Source filename [cust_sudi.prv]? <enter>
Reading file from flash:cust_sudi.prv
% Importing General Purpose certificate PEM file...
Source filename [cust_sudi.crt]? <enter>
Reading file from flash:cust_sudi.crt
% PEM files import succeeded.
esr-e1(config)#
```

Virtual WPAN (VWPAN) Interface and Mesh-security

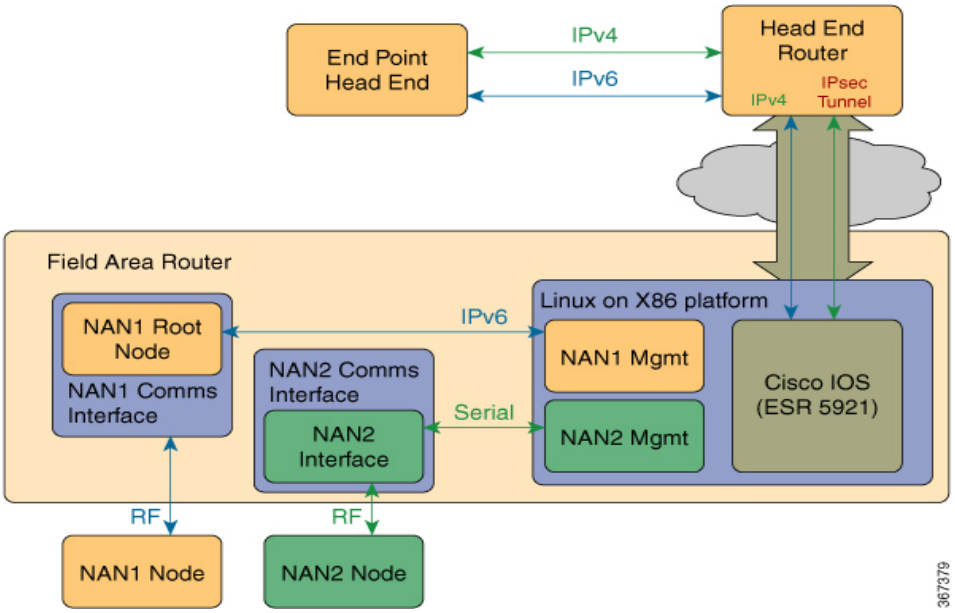
Virtual WPAN interface

A new Virtual WPAN interface is included in Cisco IOS release 15.7(3)M1 or higher to provide 802.1X and Mesh-security services on the ESR C5921 running on field area routers. This interface serves as the anchor to the Port Access Entity (PAE) for the partner module and the end-points. It also provides configuration and monitoring of CLI commands.

The VWPAN interface has three main subsystems:

- Partner Module
  The module connects directly to Linux using USB. The partner module must have an embedded 802.1X supplicant.
- Extensible Authentication Protocol (EAP) relay application
  A partner-developed GOS application that functions as an EAP relay between the module and IOS. EAP packets received from the module are forwarded to Cisco IOS and are processed in the reverse direction. The application uses an API library (libvwpan) that Cisco provides to communicate with Cisco IOS.
- Cisco IOS Virtual WPAN interface
  Provides the 802.1X and Mesh-security services for partner module and mesh endpoints.

The following graphic illustrates the high level architecture:



IEEE802.1x

IEEE802.1x is an essential component to support WPAN and mesh security. This feature is ported in the ESR5921.

Mesh-Security

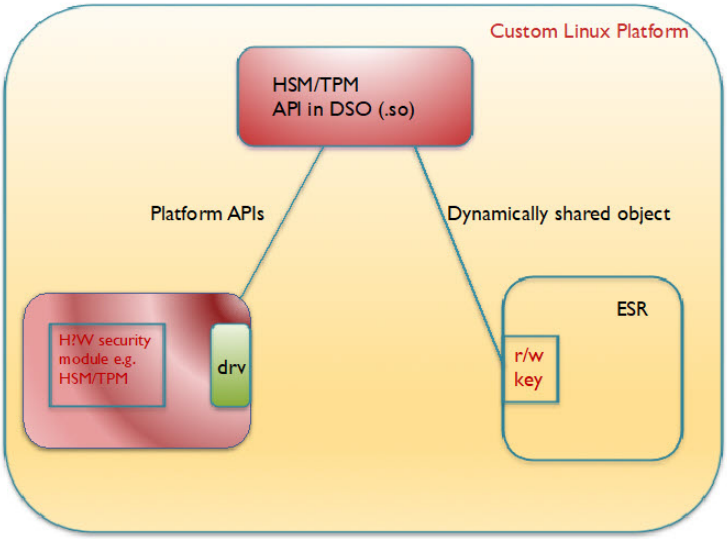
802.11i based mesh security module monitors and manages the PTKs and GTKs in the wireless mesh networks. Porting this feature to ESR is also required.

For the mesh network keys' storage, the integration partner provides an ACT2 equivalent module secure storage with related APIs. Use this interface for the mesh security master key access, which encrypts the clients' session keys and stores them on the flash.

On ESR 5921, there is no real security storage feature, which is a mandatory requirement for VWPAN and mesh security feature of storing sessions. On Cisco platforms, it is usually implemented through ACT. But for ESR running on customer's platform, it needs to integrate with the platform's HSM (hardware security module).

The approach is explained in the following: (Library Name: libesrhsm.so)

- A set of public APIs for store/retrieve securities (such as AES keys) are defined.
- APIs should be implemented by customers according to their specific requirement with DSO (dynamic shared object).
- ESR will dynamically load the library and use these sets of APIs to store and retrieve securities as needed.



To use this library provided by the integration partner, copy the library to the ESR flash and setup the emulation.conf file. The mesh-security feature uses it as the secure key storage without any additional configurations.

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 15.7(3)M2

The following sections list caveats for Cisco IOS Release 15.7(3)M2:

Open Caveats

- **CSCvh66062**

  While using DLEP, heartbeat is not sent by the router, and the radio is closing the TCP connection.

  For discovery and non-discovery cases, the client session is established. After a period of time, the heartbeat is not send by the router and radio waits for the heartbeat and closes the TCP connection.

  Workaround:

  There is no workaround.

- **CSCvi07896**

  SNMP is sending two packets per trap, one of which has the SNMP version set to 0.

  Whenever an SNMP trap is generated, the additional one trap is generated with the name **?enterprisespecific?** of which the version is 0. FND processes and ignores this trap.

  Workaround:

  There is no workaround.

- **CSCvi68368**

  TLS negotiation fails for DLEP when RFC 8175 is used between the radio and the router to establish the session.

  Workaround:

  Use normal TCP session for the connection between the radio and the router for DLEP RFC 8175.

- **CSCvi24602**

  ZTD script needs to improve Subject field parsing for custom sudi certs from different CA issuers.

  Different signing CA issuers may re-arrange the order of elements in the Subject field of a signed custom SUDI certificate.

Closed Caveats

The following caveats are fixed with this release:

- **CSCvg54074**

  3rd Party SIP Phones not registering from CME 11.6

- **CSCvi52003**

  In a KVM setup, when the C5921 is accessed via swrvcon (virtual console) application and issued any CLI (example, show version) in swrvcon then the CPU spikes up around 40% in IOS thread and 20% in FP thread.

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.
