Release Notes for Cisco IOS Release 15.5(2)T

First Published: March 30, 2015
Last Updated: April 3, 2015

These release notes contain the latest information about using Cisco IOS software with the Cisco 1000 Series Connected Grid Routers (CGR 1000 or routers) for Release 15.5(2)T.

This release includes support for the Cisco 500 Series WPAN Industrial Routers (IR500). The IR500 series includes:

- IR509 WPAN Gateway, a distribution automation (DA) gateway that provides secure IPv4/IPv6 connectivity over IPv6-based CG-Mesh to DA devices such as capacitor bank controllers, reclosers, or other SCADA devices.
- IR529 WPAN Range Extenders (Basic and Advanced) extend the range of an RF wireless mesh network, providing longer reach between WPAN endpoints and other WPAN networks. WPAN range extenders support the full CG-Mesh network platform, including IEEE 802.15.4g/e, IEEE 802.1X, IPv6, and RPL.

IR500 series operate with the CGR 1000 and Cisco Connected Grid Network Management (CG-NMS) as part of the Field Area Network (FAN) solution.

This release also adds support for the Cisco 819 Integrated Services Router (ISR). The 819 ISR supports 3G, 4G, and 3G with dual radio 802.11n Wi-Fi form factors combined with full features of Cisco IOS Software. The Cisco 819 ISR combines the latest cellular standards (4G LTE), 3G standards (High-Speed Packet Access Plus [HSPA+] release 7 and Evolution Data Optimized [EVDO] Rev A) with Cisco enterprise-class wireless LAN solutions into a single platform.

For more information about the IR500 series and the other FAN components, refer to the documents listed in Related Documentation, page 15.

You can download the software from this site (registered Cisco.com users with a login password):

http://software.cisco.com/download/navigator.html

Organization

This document includes the following sections:

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

New Features in Cisco IOS Release 15.5(2)T

Table 1 lists the new features added in Cisco IOS Release 15.5(2)T.

Table 1 New Feature Summary for Cisco IOS Release 15.5(2)T

Feature	Description	Related Documentation
Support for Cisco 500 Series WPAN Industrial Routers (IR500)	The IR500 series connects to DA devices using serial ports (RS232/RS485) and/or an Ethernet port using IPv4. The IR500 series provides remote connectivity to serial DA devices over CG-Mesh by transporting serial data over TCP/IP. The IR500 series also provides remote connectivity to IPv4 DA devices over the IPv6-based CG-Mesh by using Mapping of Address and Port using Translation (MAP-T). The IR500 series performs NAT44 translation to translate private IPv4 addresses used by DA devices connected to the Ethernet port to public IPv4 addresses used with MAP-T.	■ Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide
Support for CG-DM 4.1	The 4.1 release of Device Manager adds support for the IR500 series WPAN, in addition to support for the CGR 1000 running Cisco IOS. Device Manager connects to the IR500 directly over the laptop COM port, either with or without a work order. Device Manager displays IR500 hardware status and allows you to configure and view settings for MAP-T, TCP raw socket, WPAN, RPL, and other protocols used by the IR500 in the CG-Mesh network.	■ Connected Grid Device Manager 4.0 and 4.1 (Cisco IOS) Release Notes ■ Cisco Connected Grid Device Manager Installation and User Guide (Cisco IOS), Release 4.0 and 4.1
Support for CG-NMS 2.1.1	The 2.1.1 release of CG-NMS adds support for the IR500. CG-NMS manages the IR500 as a mesh endpoint device. You can also create work orders in CG-NMS that authorize a remote Device Manager to configure and manage the IR500.	■ *Release Notes for Cisco Connected Grid Network Management System, Release 2.1.1* ■ *Cisco Connected Grid Network Management System User Guide, Release 2.1.1*
Virtual WPAN (VWPAN) Interface	VWPAN provides the architecture for providing 802.1X and Mesh-security services to partner-developed module and mesh endpoints.	Refer to Documentation Updates, page 12.
Dynamic Multipoint VPN (DMVPN)	DMVPN is a Cisco IOS Software solution for building scalable IPsec Virtual Private Networks (VPNs) such as hub-spoke deployments.	http://www.cisco.com/c/en/us/support/security/dynamic-multipoint-vpn-dmvpn/tsd-products-support-series-home.html

Table 1 New Feature Summary for Cisco IOS Release 15.5(2)T (continued)

Feature	Description	Related Documentation
Industrial Operations Kit (IOK)	IOK is a Cisco software solution that simplifies Cisco Field Area Network (FAN) deployment by automating the configuration of multiple network and security management system components as individual virtual machines within the Cisco Unified Computing System (UCS) server. The kit includes a single headend router, bundled with Cisco PRIME Access Registrar software for authentication, authorization and accounting, and the Connected Grid Network Management System with Cisco Embedded Services Routers for zero-touch deployment.	■ *Industrial Operations Kit Getting Started Guide* ■ *Industrial Operations Kit Management Software User Guide* ■ *Release Notes for Industrial Operations Kit*
Support for Cisco 819 Integrated Services Router	The Cisco 819 Integrated Services Router Family, designed in compact hardened and non-hardened form factors, is the smallest Cisco IOS Software router with support for integrated fourth-generation (4G LTE) wireless WAN (mobile broadband backhaul) capabilities. The Cisco 819 ISR gateway provides a rapidly deployable, highly available, reliable, and secure solution designed specifically for machine-to-machine (M2M) applications. The following hardened Cisco 819 ISR PIDs are supported beginning in Cisco IOS Release 15.5(1)T1: C819HG-4G-V-K9, C819HG-4G-A-K9, C819HG-U-K9, C819HGW-S-A-K9, and C819H-K9. This release expands support to include the following non-hardened Cisco 819 ISR PIDs: C819G-B-K9, C819G-U-K9, C819G-4G-V-K9, and C819G+7-K9.	http://www.cisco.com/c/en/us/products/routers/819-integrated-services-router-isr/index.html
Raw Socket over L2 VPN	This feature adds a new encapsulation type, **trans** for asynchronous mode serial interfaces to transport Raw Socket data over MPLS VPN.	Refer to Documentation Updates, page 12.
NTP timing based on GPS Clock	IOX platforms have an onboard GPS chip that provides time source as well as location. This feature supports use of GPS time as a time source for NTP, which eliminates the need to use an NTP server over the WAN.	Refer to Documentation Updates, page 12.
DNP3 Protocol Translation for 819H	The hardened Cisco 819 ISR serving as a SCADA gateway provides protocol translation of DNP3 serial to/from DNP3 IP protocols.	http://www.cisco.com/c/en/us/products/routers/819-integrated-services-router-isr/index.html
T101-T104 Protocol Translation support on 819H	The hardened Cisco 819 ISR serving as a SCADA gateway provides protocol translation of IEC 60870 T101 to/from IEC 60870 T104 protocols.	http://www.cisco.com/c/en/us/products/routers/819-integrated-services-router-isr/index.html

System Requirements

Table 2 lists the software versions associated with this release for Cisco products deployed in a FAN solution.

Table 2 Minimum Software Requirements

Component	Minimum Software Version
Cisco Connected Grid Device Manager (CG-DM) for CGR 1000 Series Routers (Cisco IOS)	CG-DM 4.1
Cisco Connected Grid Network Management System (CG-NMS)	CG-NMS 2.1.1
Cisco 500 Series WPAN Industrial Routers	Firmware version 5.5.80 or greater

Installation Notes

This section includes the following topics:

- Determining the Software Version, page 5
- Upgrading to a New Software Release, page 5
- Erasing the Configuration File, page 6

Determining the Software Version

To identify the software version operating on the Cisco IOS router, enter the following command:

show version

Upgrading to a New Software Release

The software image is a bundle image and includes the following components: Cisco IOS image, Guest OS, Hypervisor, and a Virtual Device Server. When you initiate installation of the software, all of the components automatically install on virtual machines with the router.

To install a new version of software, you copy the bundle image over to flash and issue the bundle install command to upgrade the software.

```
router# bundle install flash:cgr1000-universalk9-bundle.SSA.154-0.99.05.CG
```

You will then see output similar to the following:

```
Installing bundle image: /cgr1000-universalk9-bundle.SSA.154-0.99.05.CG...

updating Hypervisor image...
Sending file modes: C0444 22931642 cgr1000-hv.srp.SPA.0.30


updating IOS image...
Sending file modes: C0644 73830734 cgr1000-universalk9-mz.SSA.V154_0_99_05_CG
Done!
```

After the software installation bundle finishes and displays Done! on the screen, enter the following commands to save the configuration and complete the installation process on the router:

```
router# copy running-config startup-config
router# reload
```

Erasing the Configuration File

When you enter the **write erase** {**/all nvram:** } **/no-squeeze-reserve-space** *file-system:* **|** *file-system:* **| startup-config** command, it erases a specified item or initiates an action to save memory on the Cisco 1000 Series router. See specifics in Table 3.

Table 3 write erase command

Command	Purpose
write erase {/all nvram: } /no-squeeze-reserve-space *file-system:* **|** *file-system:* **| startup-config**	**/all**–Erases all files in the specified file system. **nvram**–Erases all files in the NVRAM. *file-system:*–File system name, followed by a colon. For example, flash: or nvram:. This argument may not be used if the device memory contains logging persistent files. **/no-squeeze-reserve-space**–Disables the squeeze operation to conserve memory and makes the erase command compatible with older file systems. **startup-config**–Erases the contents of the configuration memory.

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with the router. These are known limitations that will not be fixed, and there is not always a workaround for these issues. Some features might not work as documented, and some features might be affected by recent changes to the CGR 1000 router hardware or software.

Hardware Limitations

Port Limitations

Table 4 lists the limitations in this release for hardware features that are described in detail in the *Cisco Connected Grid Router Hardware Installation Guide* for the Cisco CGR 1120 or CGR 1240.

Table 4 Hardware Limitations

Feature	Label	Limitation Description
Alarm port	ALARM	Currently not supported. Supports an external alarm system for monitoring system errors and events.
IRIG-B timing port	IRIG_B	Currently not supported. Provides timing output to a connected device.
USB ports (2)	0 1	Currently not supported.

Software Limitations

- **CSCuh18075**

  Symptom On the CGR, " %Please shutdown the interface before removing it" displays when you configure the dialer as a default interface.

  Conditions Dialer is already in a shutdown state, and the console displays " %Please shutdown the interface before removing it" . Dialer is configured as a default interface.

  Workaround Remove Dialer Pool and then the **default interface dialer 1** command executes with no errors.

Minimal Support for SNMP write on ciscoWan3gMib for Security Reasons

The read-write operation only permits the following OIDS in CISCO-WAN-3G-MIB.

```
c3gRssiOnsetNotifThreshold
c3gRssiAbateNotifThreshold
c3gEcIoOnsetNotifThreshold
c3gEcIoAbateNotifThreshold
c3gModemTemperOnsetNotifThreshold
c3gModemTemperAbateNotifThreshold
c3gModemReset
c3gModemUpNotifEnabled
c3gModemDownNotifEnabled
c3gServiceChangedNotifEnabled
c3gNetworkChangedNotifEnabled
c3gConnectionStatusChangedNotifFlag
c3gRssiOnsetNotifEnabled
c3gRssiAbateNotifEnabled
c3gEcIoOnsetNotifEnabled
c3gEcIoAbateNotifEnabled
c3gModemTemperOnsetNotifEnabled
c3gModemTemperAbateNotifEnabled
```

Note: See related **ciscoWan3gMib** caveats in this section **CSCuh85612, CSCuh88771, CSCuh88904, CSCuh88968, CSCui00861, CSCui01208, CSCui01347, CSCui03505**

- **CSCuh85612**

  Symptom A write on c3gGsmRoamingPreference results in commit failed."

  SNMP write on most of ciscoWan3gMib is not supported for security reasons.

  Conditions When you issue snmp set on c3gGsmRoamingPreference, you get the error message “Commit failed.”

  Workaround There is no workaround. Limitation is by design for security reasons.

- **CSCuh88771**

  Symptom c3gMsisdn shows an empty string in an SNMP walk.

  Conditions SNMPget on c3gMsisdn.

  Workaround There is no workaround. This issue is carrier dependent. When this issue is seen in the field, check with your service provider to see whether MsIsdn is populated by the service provider. For example, AT&T does provide the MsIsdn value and T-Mobile does not.

- **CSCuh88904**

  Symptom When a SNMP set is issued to create a row in the PDP profile table, commitFailed was seen.

```
snmpset -v 3 -u sgbublr -l authPriv -a MD5 -A cisco1234 -x AES128 -X cisco1234 172.27.168.114
c3gGsmPdpProfileRowStatus.22.2 i 4
Error in packet.
Reason: commitFailed
Failed object: CISCO-WAN-3G-MIB::c3gGsmPdpProfileRowStatus.22.2
```

Conditions SNMP set operations are not allowed on c3gGsmPdpProfileTable for security reasons.

Workaround Use the CLI to create a new profile for profile 3 as shown in the example below:

```
cgr1000# cellular 3/1 gsm profile create 3 PRO3
Profile 3 will be created with the following values:
PDP type = IPv4
APN = PRO3
Are you sure? [confirm]
Profile 3 written to modem
```

- **CSCuh88968**

  Symptom ciscoWan3Gmib does not support a **write** function for the c3gGsmChv1 object.

  Conditions When a user issues a **set c3gGsmChv1** command, the set fails. By design, the write function (disabled by default) does not work on most of the ciscoWan3gMib for security reasons.

  Workaround Enter the command **cellular** *slot/port* **gsm sim change-pin** *Old-PIN New-PIN* to set Card Holder Verification 1 (CHV1). Example below:

  ```
  CGR1K# cellular 5/1 gsm sim  change-pin  0000 1111
  ```

- **CSCui00861**

  Symptom A write on c3gCdmaSecurityTable results in commit failed.

  ```
  Error: Commit failed
  Error index: 1
  1: c3gCdmaPinSecurityStatus.23 (INTEGER) unknown(1)
  ***** SNMP SET-RESPONSE END *****
  ```

  Conditions User uses snmp create a row in the security table as the MIB has access to create a row. This results is failure as write is not supported in IOS for this MIB.

  Workaround There is no workaround for this issue. SNMP write on most of ciscoWan3gMib is not supported for security reasons.

  Either objects are pre-set or can be set through CLI. SNMP set is not supported.

- **CSCui01208**

  Symptom The OID c3gHdrDdtmPreference is not writable even though it is a read-write object. SNMP write on c3gHdrDdtmPreference is not supported for security reasons.

  Conditions The requested set on c3gHdrDdtmPreference always results in Commit Failed errors.

  Workaround Enter the [**no**] **cdma ddtm** command to set the c3gHdrDdtmPreference for a cellular preference as enabled or disabled. For example:

  To enable cdma ddtm for cellular 3/1:

  ```
  CGR1000#config terminal
  CGR1000(config)#controller cellular 3/1
  CGR1000(config-controller)# cdma ddtm
  ```

- **CSCui01347**

  Symptom MIB OID c3gCdmaRoamingPreference does not have corresponding CLI. The write operation of c3gCdmaRoamingPreference results in "Commit failed" errors. The write of c3gCdmaRoamingPreference is not supported due to security reasons.

  Conditions User wants to identify the Roaming Preference through CLI. its not shown. It is available only via mib get.

  The write of c3gCdmaRoamingPreference results in "Commit failed" errors.

  Workaround Use c3gCdmaRoamingPreference get to retrieve the Roaming Preference value.

- **CSCui03505**

  Symptom Issue snmpset on any of c3gMdn,c3gCurrentNid, c3gCurrentSid,c3gSipUsername or c3gSipPassword MIB objects. The following occurs:

  ```
  Error: Commit failed
  Error index: 1
  1: c3gSipUsername.23 (DisplayString) 0000005308@vzw3g.com
  [30.30.30.30.30.30.35.33.30.38.40.76.7A.77.33.67.2E.63.6F.6D (hex)]
  ```

  Conditions SNMP write on most of the ciscoWan3gMib is not supported for security reasons.

  Workaround There is no workaround.

- **CSCuj72458**

  Symptom Cannot SSH into the CGR with SSHv2 protocol.

  Conditions SSH process is operating in its default configuration. That is, it is neither configured with **ip ssh version** *X* nor is it configured with **ip ssh version 2**.

  In addition, the SSH process is not configured with **ip ssh rsa keypair-name** *XXXX* to specify a SSH host key.

  Subsequently, SSH process uses the SUDI RSA key as SSH host key.

  Workaround

  User should manually create a new SSH host key by following these steps:

  1) To generate a new key, enter command **crypto key generate rsa modulus 2048 label** *XXXX* in configuration (config) command mode.

  2) To specify the use of key *XXXX* as SSH host key, enter command **ip ssh rsa keypair-name** *XXXX* in config command mode.

  3) To specify the use of the SSHv2 protocol, enter command **ip ssh version 2** in config command mode.

- **CSCul82192**

  Symptom When using Airspan base station with CGR1000 dot16 modules, the latency may increase if the dot16 uplink throughput is very low (around 200 Kbps or less).

  Conditions If the uplink throughput is very low (around 200 Kbps or less), the latency may increase (especially with the Best Effort service-class). This is because Airspan base stations expect a certain minimum rate of traffic before processing the traffic.

  Workaround Configure a QoS scheduling method like rTPS on the base station to minimize the increase in the uplink latency at very low traffic rates.

- **CSCum84292**

  Symptom You cannot download the software image bundle for this release when operating with SSHv1.

  Conditions By default, the GOS image that comes with the software bundle image only supports SSHv2. You must enable SSHv2 in Cisco IOS in order to download any TPMC package or application to the GOS.

  Workaround Enable SSH2 in Cisco IOS.

- **CSCun11696**

  Symptom The system reset-reason may show "Thermal Trip" after a power outage.

  Conditions When a CGR is power-cycled due a power loss event, the system reset-reason may show a false "Thermal Trip" reset instead of "Power-on". This is because the unstable voltage on the mainboard may trigger a false "Thermal Trip" reset-reason.

  Workaround After the CGR comes back up, issue **show environment temperature** to check the sensor temperature. If they show normal values, the Thermal Trip reset-reason can be ignored and no further action needs to be taken.

- **CSCun77609**

  Symptom The line protocol on the dot16 interface may not go down after restoring the interface to default configuration.

  Conditions Configure the necessary settings for the dot16 interface to come online. Restore the interface to default settings. The dot16 interface line protocol may stay up.

  Workaround Perform a shutdown on the interface.

Caveats

This section addresses the open caveats in this release and provides information on how to use the Bug Search Tool to find further details on those caveats. This section includes the following topics:

- Open Caveats, page 10
- Accessing Bug Search Tool, page 12

Open Caveats

- **CSCuh79081**

  Symptom The message, modem is not present, is seen when the modem is plugged in.

  Conditions Module is stressed with power UP/DOWN, dual SIM failovers, and modem power cycles and resets along with traffic.

  Workaround There is no workaround for this issue. Reboot the CGR.

- **CSCui66025**

  Symptom Modem crash memdump from the modem is not retrieved.

  Conditions Even when the modem crash tool is enabled, the memdump is not retrieved.

  Workaround There is no workaround for this issue.

- **CSCuj43190**

  Symptom The AT Command response from the modem is very slow when bidirectional traffic is sent across the cellular interface.

  Conditions Bidirectional traffic is sent across the cellular interface.

  Workaround Stop all traffic and reload the CGR to access the AT commands.

- **CSCuj51188**

  Symptom The following tracebacks are seen when GSM/CDMA modem crashes:

  %SYS-3-BAD_RESET: Questionable reset of process 314 on tty3/1

  -Process= " TTY Daemon" , ipl= 0, pid= 333

  -Traceback= 1845341z 1733927z 1734FA8z 22D2AA0z

  Conditions Occurs when CDMA/GSM modem crashes.

  Workaround Perform module reload by entering the command: hw-module reload *slot-number.*

- **CSCul57458**

  Symptom After booting, a cellular interface might not automatically be placed in an admin non-shut state when its 3G module is administratively powered up from a powered-down state.

  Conditions When the 3G module is powered down, its cellular interface will also be put in admin shut state. When the 3G module is powered up again, its 3G interface will be automatically put back in admin no-shut state.

  However, if the 3G module is powered-down and the CGR is rebooted, the 3G interface may not be put in admin no-shut state when the 3G module is powered up again. Users may see this error " cellular_error_log: DS instance init issue" . When such an error occurs, the cellular interface will not be automatically put in admin no-shut state when the 3G module is powered up.

  Workaround Try to manually bring up the cellular interface by using the **no shutdown** command

- **CSCul63882**

  Symptom Cellular 3G interface is shown in shutdown state even after the module is powered on.

  Conditions CGR (with a 3G module installed) was powered off and reloaded to ensure that the cellular interface was not in an admin down state. After the CGR boots up and the 3G module is powered on, the module remained in an admin down state.

  Workaround Shutdown and no shutdown commands need to be performed on the cellular interface after the CGR boots up.

- **CSCul63973**

  Symptom The dot16 interface may be set to admin shut in startup-config under some race conditions.

  Conditions Under some race condition (e.g. a copy run start operation is happening during a module power-cycle due to recovery or wan-mon), the dot16 interface configuration may be set to administrative shutdown. If the CGR is reloaded, this interface may stay in admin shut state

  Workaround Issue **no shutdown** in the interface configuration mode if the interface stays in the admin shut state after a reload.

- **CSCul67773**

  Symptom c3gModemTemperAbateNotif trap generates only after the c3gModemTemperOnsetNotif trap has already been generated once.

  Conditions c3gModemTemperAbateNotif is working like recovery trap rather than a discrete trap.

  Workaround There is no workaround.

- **CSCuo01279**

  Symptom Malloclite memory leak occurs every 15-20 minutes.

  Conditions This issue is reproducible, but not consistently. An example is shown below:

  ```
  Chunk Elements:

  AllocPC  Address  Size  Parent   Name
   396D354 11EBC210   100 12F462CC (MallocLite)
   396D354 13EFD8C4    48 13036424 (MallocLite)
   396D354 13EFE484    48 13036424 (MallocLite)
   396D354 13EFE504    48 13036424 (MallocLite)
  ```

  Workaround There is no workaround. Router reboot does not help.

Accessing Bug Search Tool

You can use the Bug Search Tool to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To access the Bug Search Tool, enter the following URL:

https://tools.cisco.com/bugsearch/search

To access the Bug Search Tool to search on a specific caveat, enter the following URL:

https://tools.cisco.com/bugsearch/search/<BUGID>

Documentation Updates

This section includes the following late updates to documentation for the CGR 1000:

- Virtual WPAN (VWPAN) Interface, page 13
- Raw Socket over L2 VPN, page 14
- NTP timing based on GPS Clock, page 15

Virtual WPAN (VWPAN) Interface

The CGR 1000 provides security services to wireless and power-line communication (PLC) mesh endpoints. This is done by enabling these services on corresponding WPAN and PLC IOS interfaces. For a partner-developed WPAN module that connects to Guest-OS (GOS), the same set of services are not directly available.

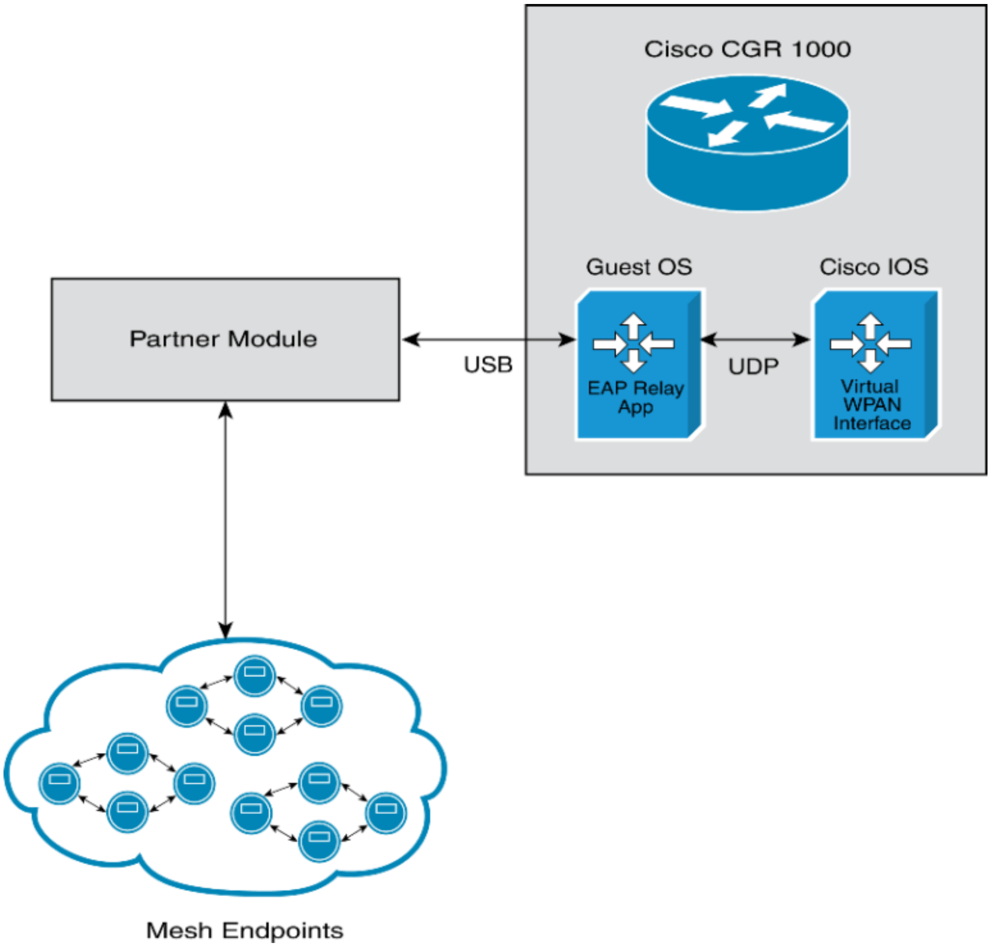
A new Virtual WPAN interface is included in this Cisco IOS release to provide 802.1X and Mesh-security services. This interface serves as the anchor to the Port Access Entity (PAE) for the partner module and the end-points. It also provides configuration and monitoring CLI commands.

The VWPAN interface has three main subsystems:

- Partner Module - The module connects to GOS directly 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 likewise 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.

Figure 1 on page 14 shows the high-level architecture.

Figure 1 VWPAN Architecture



Interface Configuration and Monitoring

VWPAN 1X and Mesh-security interface configuration and monitoring is identical to the physical WPAN interface. All the 802.1X and Mesh-security CLI commands are available and behave the same way.

For example, the following creates and configures a VWPAN interface and sets up the 802.1X authenticator in multi-auth mode:

```
conf t
interface Virtual-WPAN 0
 authentication host-mode multi-auth
 authentication port-control auto
 dot1x pae authenticator
```

Raw Socket over L2 VPN

To configure raw socket over MPLS VPN, enable **encapsulation trans** on the asynchronous interface, then use the **xconnect** command to configure the MPLS virtual connection.

When data comes in from the asynchronous mode serial port (or UART), the CGR 1000 packetizes the data using the configured criteria for raw socket and passes the packet to a pre-configured MPLS connection to another point. Then the packet is delivered to a local UART. This process is bidirectional.

The following example shows a serial interface on the CGR 1000 configured for Raw Socket MPLS VPN:

```
cgr1000# show run inter async1/1
Building configuration...

Current configuration : 132 bytes
!
interface Async1/1
 physical-layer async
 no ip address
 encapsulation trans
 xconnect 9.9.10.1 112000 encapsulation mpls
end
```

For more information about raw socket configuration on the CGR 1000, see *Raw Socket Transport Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)*.

NTP timing based on GPS Clock

A new global configuration command configures the GPS time as the reference clock for NTP:

[no] ntp refclock gps

The GPS time acts as a stratum 0 source, and the Cisco IOS NTP server acts as a stratum 1 device, which in turn provides clock information to its NTP clients (stratum 2 and 3).

Related Documentation

Table 5 Related Documentation

Device or Feature	Related Documents
Cisco 1000 Series Connected Grid Routers	Configuration and Installation Guides: http://www.cisco.com/go/cgr1000-docs
Cisco 500 Series WPAN Industrial Routers (IR500)	Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide
Cisco 819 Integrated Services Router	Product information: http://www.cisco.com/c/en/us/products/routers/819-integrated-services-router-isr/index.html
CG-NMS	*Cisco Connected Grid Network Management System User Guide, Release 2.1.1*

Table 5 Related Documentation (continued)

Device or Feature	Related Documents
Device Manager	Cisco Connected Grid Device Manager Installation and User Guide (Cisco IOS), Release 4.0 and 4.1
WPAN and CG-Mesh	Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide (Cisco IOS)
Industrial Operations Kit	*Industrial Operations Kit Getting Started Guide* *Industrial Operations Kit Management Software User Guide* *Release Notes for Industrial Operations Kit*

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/c/en/us/td/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 delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

No combinations are authorized or intended under this document.