CHAPTER 5

Operation and Configuration

This chapter describes the operation of the Cisco Industrial Routers (IR500) Series WPAN Gateway and WPAN Range Extender and how to configure the devices:

- Information about WPAN Gateway and WPAN Range Extender Operation, page 5-1
- WPAN Gateway and WPAN Range Extender Data Flow, page 5-3
- Information about Raw Socket Transport and MAP-T, page 5-5
- Information about WPAN Gateway and WPAN Range Extender Configuration, page 5-13
- Configuring the WPAN Gateway and WPAN Range Extender, page 5-14
- CG-NMS WPAN Device Management Related Operations, page 5-23

Information about WPAN Gateway and WPAN Range Extender Operation

- WPAN Gateway and WPAN Range Extender and the Cisco Field Area Network, page 5-1
- Role of the WPAN Gateway and WPAN Range Extender in the Cisco FAN, page 5-2

WPAN Gateway and WPAN Range Extender and the Cisco Field Area Network

The WPAN gateway and WPAN range extender operate in the Cisco Connected Grid (CG) Field Area Network (FAN).

The FAN solution provides an IPv6-based networking solution for connecting and managing a multitude of devices in a smartgrid architecture. The Cisco CG FAN consists of three components:

- Connected Grid Endpoint (CGE) devices
- Connected Grid Router (CGR) devices
- Cisco Connected Grid Network Management System (CG-NMS)

CGEs are the CG FAN end points. The CGEs may be electric meters or Distribution Automation (DA) devices. The CG FAN utilizes low-cost mesh networking technology to connect CGEs. The link technologies may utilize Radio Frequency (e.g. IEEE 802.15.4g) and, or Power Line Communication (e.g. IEEE P1901.2) media.
CGRs provide wide-area connectivity for CGEs. In addition to providing wide-area connectivity, because CGRs typically have more resources than CGEs, CGRs support critical functions for secure network access control, routing, and management of CGEs. In a typical deployment, a single CGR may provide wide-area connectivity for hundreds or thousands of CGEs.

CG-NMS provides the necessary back-end infrastructure for supporting the CGEs and CGRs in the Cisco CG FAN. CG-NMS is responsible for managing secure network access, configurations, and firmware updates for all CGR and CGEs in a CG FAN deployment. Each device registers with the CG-NMS and periodically reports information that assists a network operator in assessing the health of the network and diagnosing any issues that may occur.

The Cisco Industrial Routers (IR) 500 Series WPAN Gateway and WPAN Range Extender provide unlicensed 902-to-928 MHz ISM-band wireless personal area network (WPAN) communications to diverse Internet of things (IoT) applications. Among the IoT applications supported are smart grid, distribution automation (DA), and supervisory control and data acquisition (SCADA).

The devices supply radio frequency (RF) mesh connectivity to IPv4/Ethernet and serial IoT devices, including recloser control, cap bank control, voltage regulator controls, and other endpoint controllers. The devices provide an open standards RF mesh solution based on the following standards:

- IEEE 802.15.4 g/e
- RFC6775—Neighbor Discovery Optimization for Low Power and Lossy Networks (6LoWPAN)
- RFC6550—RPL: IP6 Routing Protocol for Low-Power and Lossy Networks
- IETF MAP-T—Mapping of Address and Port using Translation (MAP-T)
- RFC7252—The Constrained Application Protocol (CoAP)

Role of the WPAN Gateway and WPAN Range Extender in the Cisco FAN

- Role of the WPAN Gateway, page 5-2
- Role of the WPAN Range Extender, page 5-3

Role of the WPAN Gateway

The WPAN Gateway provides IPv4/IPv6 connectivity to attached devices, such as DA devices. The gateway connects to DA Devices using serial ports (RS232/RS485) or an Ethernet port using IPv4. The gateway provides remote connectivity to:

- Serial DA devices over CG-Mesh by transporting serial data over Raw Socket TCP/IP
- Ethernet/IPv4 DA devices over the IPv6-based CG-Mesh

Mapping of Address and Port using Translation (MAP-T), specified in draft-ietf-software-map-t, is used to transport both Raw Socket TCP/IP and Ethernet/IPv4 traffic over the IPv6 6LoWPAN infrastructure.

WPAN Gateway and Serial-based DA Devices

The WPAN gateway connects serial-based DA devices and exports them over the IPv6-based Field Area Network by the following means:

- RS232/RS485 Port (Serial Interface 0 (DCE))—The gateway RS232/RS485 serial port is used to connect RS232/RS485-based DA devices and transport serial data traffic over Raw Socket TCP. The gateway configuration and management of the serial port is done via CSMP and the CG-NMS.
WSN Gateway and Ethernet-based DA Devices

The WSN gateway connects IPv4-based DA devices to the IPv6-based FAN by the following means:

- Ethernet Port—the gateway Ethernet port is used to provide IPv4 connectivity to DA devices. The gateway exports configuration and management of the Ethernet port via CSMP and the CG-NMS.
- DHCP—the gateway implements a DHCP Server to support dynamic configuration of IPv4-based DA devices. The gateway exports DHCP configuration and management via CSMP.
- Mapping of Address and Port using Translation (MAP-T)—The gateway provides shared or uniquely addressed IPv4 host connectivity to and across an IPv6 domain using MAP-T. The gateway implements the MAP Customer Edge (CE) functionality, as described in draft-ietf-software-map-t. Each MAP domain must also include a device that implements the MAP-T Border Relay (BR) functionality (for example, the ASR 1000). The gateway configuration and management of MAP-T is done via CSMP and the CG-NMS.
- NAT44—The gateway uses NAT44 to translate private IPv4 addresses used by DA devices connected to the Ethernet port to public IPv4 addresses used with MAP-T.
  - Dynamic NAT44 performs translation for outgoing communications (Device to Server).
  - Static NAT44 performs translation for incoming communications (Server to Device).
  - 4 NAT44 sessions are supported.
  - Static NAT44 requires proper setup through CG-NMS.

Role of the WSN Range Extender

The WSN range extender is an IEEE 802.15.4g-2012 IPv6 router device that allows additional flexibility in locating IEEE 802.15.4g devices, resulting in extra connectivity among CG-Mesh devices. For example, while CG-Mesh electric meters must be placed where electric metering occurs, the range extender may be placed anywhere AC power is available. The range extenders support the full CG-Mesh network platform, including IEEE 802.15.4g, IEEE 802.1X, IPv6, and RPL.

WSN Gateway and WSN Range Extender Data Flow

- Data Flow Prerequisites, page 5-3
- Data Flow Paradigms, page 5-4

Data Flow Prerequisites

The mandatory components for a Cisco IR 500 Series WSN gateway and WSN range extender deployment are:

- Cisco ASR 1000 Series Router or Cisco CSR 1000V Series Router configured as a MAP-T border relay
WPAN Gateway and WPAN Range Extender Data Flow

- Cisco CGR 1000 Series Router configured as a WPAN router (a WPAN module is installed)
- Cisco IR 500 Series WPAN gateway and WPAN range extender configured and installed

Data Flow Paradigms

There are two potential data flow paradigms with the WPAN gateway and WPAN range extender devices:

- Serial DA device remote connectivity over CG-Mesh by transporting serial data in TCP/IP—this is achieved by routing traffic between a WPAN gateway serial port attached DA device and an application server through a Raw Socket connection. The Raw Socket TCP connection is established over IPv4, then translated to IPv6 through Mapping of Address and Port using Translation (MAP-T).
- IPv4 DA device remote connectivity over the IPv6-based CG-Mesh by using MAP-T—this is achieved by routing traffic between a WPAN gateway Ethernet port connected IPv4 DA device and an application server

Both traffic flows involve MAP-T enabling non-IPv6 traffic to be transparently forwarded over 6LoWPAN, or the mesh network that is IPv6 only.

Figure 5-1 shows the deployment of the WPAN gateway and WPAN range extender devices and the role of Raw Socket and MAP-T.
Information about Raw Socket Transport and MAP-T

- Raw Socket TCP, page 5-6
- MAP-T, page 5-8
Raw Socket TCP

Raw Socket is a method for transporting serial data through an IP network. It transports streams of characters from one serial interface to another over an IP network for utility applications. The feature can be used to transport Supervisory Control and Data Acquisition (SCADA) data from endpoint controllers. For the WPAN gateway and WPAN range extender deployment, Raw Socket Transport uses TCP as the transport protocol.

Raw Socket Transport supports the following for each asynchronous serial interface:

- TCP as the transport protocol, with built-in auto TCP connection retry mechanism.
- Interface configuration as either a server or a client. The WPAN gateway can only be set up as a server or as a client but not both simultaneously.
- One server per interface, but multiple clients.

Note

For the one server per interface with multiple clients arrangement, the number of clients may be limited to one or two. Contact Cisco for more information.

For more information about the Raw Socket deployment read the following sections:

- TCP Transport, page 5-6
- Raw Socket Configurations, page 5-6
- Raw Socket and Serial Protocol Operation, page 5-8

TCP Transport

The TCP transport CG FAN scenario is that one router acts as a Raw Socket server, listening for TCP connection requests from the other CG FAN routers, which are configured as Raw Socket clients. In Figure 5-1, for example, the CGR 2010 acts as the Raw socket server, and it listens for TCP connection requests from the WPAN gateways, which are configured as Raw Socket clients.

A Raw Socket client receives streams of serial data from the endpoint controllers and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The Raw Socket client initiates a TCP connection with the Raw Socket server and sends the packetized data across the IP network to the Raw Socket server, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.

Raw Socket Configurations

Raw Socket transport uses a client-server model on the WPAN gateway. The WPAN gateway can be either a server or a client but not both. At most one server and multiple clients can be configured on a single asynchronous serial line.

Figure 5-2, Figure 5-3, and Figure 5-4 show three different Raw Socket configurations and scenarios involving the WPAN gateway. In these examples, serial data is transferred between endpoint controllers and a utility management system across an IP network that includes several CGR 1000 and CGR 2010 routers.
In Figure 5-2, a Raw Socket CGR1000 router client receives streams of serial data from the WPAN gateway attached endpoint controllers and accumulates the data before placing it into packets. A MAP-T Border Relay (BR) provides IPv4/IPv6 address translation for the Raw Socket TCP connection. The CGR 2010 router acts as a Raw Socket server, listening for TCP connection requests from the WPAN gateways, which are configured as Raw Socket clients. The WPAN gateway Raw Socket client initiates a TCP connection with the CGR2010 Raw Socket server, and sends the packetized data across the IP network to the CGR2010 Raw Socket server, which retrieves the serial data from the packets and sends it to the serial interface, and on to the SCADA server.

In Figure 5-3, a Raw Socket CGR1000 router client receives streams of serial data from the WPAN gateway attached endpoint controllers and accumulates the data before placing it into packets. A MAP-T BR provides IPv4/IPv6 address translation for the Raw Socket TCP connection. The CGR1000 Raw Socket client initiates a TCP connection with the SCADA server, and sends the packetized data across the IP network to the SCADA server. The SCADA server communicates through COM ports mapped to IP and TCP/UDP ports, by IP/Serial Redirector software.
In Figure 5-4, a Raw Socket CGR1000 router client receives streams of serial data from the WPAN gateway attached endpoint controllers and accumulates the data before placing it into packets. A MAP-T BR provides IPv4/IPv6 address translation for the Raw Socket TCP connection. The CGR1000 Raw Socket client initiates a TCP connection with the SCADA server, and sends the packetized data across the IP network to the SCADA server. The SCADA server communicates directly over Raw Socket IP and TCP/UDP ports.

**Raw Socket and Serial Protocol Operation**

When running a serial protocol over a Raw Socket, there are two different layers that establish their own connectivity:

- **Raw Socket layer**—Assuming the SCADA server handles the Raw Socket session (the other alternative is the Raw Socket is handled by a router), the Raw Socket session is established between the SCADA server and the WPAN gateway. One side is the listener (Raw Socket TCP server), the other is the client (Raw Socket TCP client).
- **Serial protocol layer**—The serial protocol session, i.e. DNP3, IEC 60870-5-101, MODBUS, etc., runs on the serial protocol layer, and this also has server/master and client sides. This serial protocol session runs from the SCADA server to the attached endpoint controller.

**MAP-T**

6LoWPAN is an IPv6-only adaptation layer for the physical (PHY) and media access control (MAC) layer technologies implementing it. No IPv4 adaptation layer is defined for these PHY and MAC layers, so the Mapping of Address and Port using Translation (MAP-T) architecture is used as an IPv4-IPv6 translation mechanism. The “mapping of address and port” mechanism defines how IPv4 nodes can communicate over an IPv6-only infrastructure.

MAP-T was developed as a transition mechanism due to IPv4 address exhaustion. MAP-T is based on a double stateless NAT64 translation. It specifies a stateless algorithmic address and transport layer port mapping scheme, and allows embedding of IPv4 address and port numbers in an IPv6 address when forwarding the IPv4 traffic across an IPv6-only network.
When MAP-T is used in the WPAN gateway, the IPv4 address of the attached device can be a private address with local significance only since the traffic goes through NAT44. By using MAP-T, the WPAN gateway is using an open standard to integrate non-IP from serial interface through Raw Socket TCP, and IPv4 communications over 6LOWPAN/RPL networks.

In a Field Area Network (FAN) scenario, where hundreds of WPAN gateways are deployed across multiple Field Area Routers (FARs), such as CGR 1000, a MAP-T domain begins at the WPAN gateway level and ends with the head-end aggregation routers, such as ASR1000 as shown in Figure 5-5.

This section contains:

- MAP-T Mapping Rules and Map Domain Parameters, page 5-10
- MAP-T IPv6 Address Formats—MAP-T Draft-00 and MAP-T Draft-01+, page 5-11
- MAP-T Addressing Rules Example, page 5-12
There are defined IPv6 and IPv4 MAP-T prefixes inside the MAP-T domain enabling the NAT64 translation process to identify addresses to be translated, as well as get proper reachability and routing through the MAP-T domain.

NAT44 is a component of the MAP solution, but the NAT44 in MAP differs from traditional NAT44 deployments in that instead of assigning a public IPv4 address range to each field device for translation (in the case of NAT), or a single public IPv4 address for translation (in the case of Port Address Translation (PAT)) to each field device, it extends the granularity beyond a single public IPv4 address, by being able to assign a port range to each of the field devices sharing the same IPv4 public address. This unique address and port range combination is then translated into the IPv6 address space when transitioning into the IPv6 domain using the MAP field device. The MAP algorithm still retains the ability to assign the full IPv4 address or an IPv4 prefix to the MAP field device, but the WPAN gateway only leverages the full IPv4 address to be allocated on a per WPAN gateway basis.

**MAP-T Mapping Rules and Map Domain Parameters**

Inside the MAP-T domain are defined IPv6 and IPv4 MAP-T prefixes enabling the NAT64 translation process to identify addresses to be translated as well as get proper reachability and routing through the MAP-T domain. Those are known as:

- **MAP-T Default Mapping Rule (DMR):** an IPv6 prefix used to address all destinations outside the MAP-T domain.
  - DMR IPv6 prefix and prefix length embeds any IPv4 addresses outside the MAP-T domain. For example, within a MAP-T domain using a DMR IPv6 prefix = 2610:D0:1200:CAFE::/64, all IPv4 translated packet sources and destinations outside the MAP-T domain have an IPv6 address based on this prefix, i.e. sending packets to IPv4 100.1.1.2 translated to IPv6 2610:d0:1200:cafe:64:101:200:0. The SCADA server IPv4 address is an example of a destination outside of the MAP-T domain.

- **MAP-T Basic Mapping Rule (BMR):** the IPv6 and IPv4 prefixes used to address MAP-T nodes inside the MAP-T domain
  - BMR IPv4 prefix and prefix length are the IPv4 subnet selected to address all IPv4 nodes in a MAP-T domain. For example, a MAP-T domain set-up with 153.10.10.0/24 as IPv4 subnet has all IPv4 nodes configured with IPv4 address from this subnet, BMR IPv4 prefix = 153.10.10.0 and prefix length = 24
- BMR IPv6 prefix and prefix length are used to embed the IPv4 address of nodes inside the MAP-T domain. For example, a MAP-T domain is configured with a MAP-T IPv6 BMR = 2031:6f8:147e:10::/56. Packets sent or received from IPv4 nodes inside the MAP-T domain have a translated IPv6 address based on this prefix, i.e. 2031:6f8:147e:10fe:99:a0:a:fe00:0 for a MAP-T IPv4 node set-up with IPv4 153.10.10.254.

- BMR Share ratio: MAP-T being designed for various deployment scenarios, it could be feasible to allocate to a MAP-T node either an IPv4 prefix (smaller than the MAP-T BMR IPv4 prefix), or a single IPv4 address (/32) or share a single IPv4 address (/32) between several nodes. In the later case, it requires indicating how many bits for port numbers are assigned, which is called “BMR share ratio”. In case of IR 500 deployment, it is recommended to use a single IPv4 address (/32) per IR 500 with a share ratio = 1 to keep the addressing simple.

- BMR Embedded Address (EA) bits indicate – in the case of share ration = 1 – the length of the IPv4 suffix embedded in the MAP-T IPv6 End-user IPv6 prefix. For example, in case of an IPv4 /24 prefix allocated to a MAP-T domain, the BMR EA value derived from it is 8.

### MAP-T IPv6 Address Formats—MAP-T Draft-00 and MAP-T Draft-01+

The MAP-T Internet Engineering Task Force (IETF) draft, *Mapping of Address and Port using Translation (MAP-T)*, changed the MAP-T interface identifier (IID) format of an IPv6 MAP-T address between draft-00, and draft-01 or later drafts. For example, *Table 5-1* highlights the difference between a draft-00 address and a draft-05 address.

<table>
<thead>
<tr>
<th>Address Format</th>
<th>MAP-T IPv6 prefix</th>
<th>2031:6F8:147E:1000:/56</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP-T IPv4 address:</td>
<td></td>
<td>153.10.10.254</td>
</tr>
<tr>
<td>MAP-T draft-00 IPv6 address format:</td>
<td></td>
<td>2031:6f8:147e:10fe:99:a0:fe00:0</td>
</tr>
<tr>
<td>MAP-T draft-05 IPv6 address format:</td>
<td></td>
<td>2031:6f8:147e:10fe:0:990a:0afe:0</td>
</tr>
</tbody>
</table>

In order to identify these formats, the following nomenclature is used:
- MAP-T Draft-00—this represents MAP-T using the draft-00 IETF IID format
- MAP-T Draft-00+—this represents MAP-T using the draft-01 or later IETF IID format

Cisco’s initial software release on the gateway (Cisco IR509 5.5.72 release) was in draft-00 format, as the MAP-T border relay (also known as the Cisco ASR1000 or CSR1000) Cisco IOS XE only ran draft-00.

Beginning with Cisco IOS XE 3.13S release, Cisco ASR1000 or CSR1000 only runs the new format. It requires a new gateway software release (Cisco IR509 5.5.80 release), a new TLV 110 parameter, and CG-NMS 2.1.1, since draft-00 and draft-01 or later are incompatible.

---

**Note**

Beginning with Cisco IR509 5.5.80 release in CG-NMS 2.1.1, the TLV 110 parameter, contains a new field: MAP-T version, with 0=MAP-T draft-00, 1= MAP-T draft-01+. It must be set in accordance with the ASR1000 Cisco IOS XE 3.13S release.

All devices in a MAP-T domain must run the same IPv6 MAP-T IID format.
MAP-T Addressing Rules Example

Figure 5-6 is an example of a MAP-T domain, and the domain parameters are provided in Table 5-2. The Table 5-3 details the translated addresses.

The Default Mapping Rule (DMR) is 2610:D0:1200:CAFE::

Table 5-2 MAP-T Domain Parameters

<table>
<thead>
<tr>
<th>MAP-T Domain Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Mapping Rule (BMR) IPv6 Prefix</td>
<td>2031:6F8:147E:1000::</td>
</tr>
<tr>
<td>DMR IPv6 prefix length</td>
<td>/64</td>
</tr>
<tr>
<td>BMR IPv6 prefix length</td>
<td>/56 -&gt; as allowed by RFC 6052 (prefix length = 32, 48, 56, 64 or 96)</td>
</tr>
<tr>
<td>BMR Rule IPv4 Prefix</td>
<td>153.10.10.0</td>
</tr>
<tr>
<td>Rule IPv4 Prefix Length</td>
<td>/24</td>
</tr>
<tr>
<td>BMR Share Ratio</td>
<td>1</td>
</tr>
<tr>
<td>EA bits length</td>
<td>8</td>
</tr>
</tbody>
</table>

Note
If EA bits + Rule IPv4 prefix lengths are equal to 32, then a full IPv4 address is to be assigned. The address is created by concatenating the Rule IPv4 prefix and the EA-bits.

Note
End-user IPv6 prefix = Rule IPv6 Prefix + IPv4 Suffix (EA bits field)

Table 5-3 MAP-T Draft 01+ Translated Addresses

<table>
<thead>
<tr>
<th>Case No.</th>
<th>MAP IPv4 address</th>
<th>End-user IPv6 prefix</th>
<th>MAP IPv6 address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>153.10.10.32</td>
<td>2031:6f8:147e:1020::</td>
<td>2031:6f8:147e:1020:0:990a:0a20:0</td>
</tr>
<tr>
<td>2</td>
<td>153.10.10.254</td>
<td>2031:6f8:147e:10fe::</td>
<td>2031:6f8:147e:10fe:0:990a:0afe:0</td>
</tr>
</tbody>
</table>
Role of CG-NMS

The IR500 series WPAN gateway and WPAN range extender are managed and configured by the Connected Grid Network Management System (CG-NMS) application.

CG-NMS Device Classification

CG-NMS uses groups to manage devices. Each device must be classified into a group.

For CG-NMS based management and configuration, the WPAN gateway and WPAN range extender are classified according to the device category, device type, and group information in Table 5-4.

<table>
<thead>
<tr>
<th>Classification Entity</th>
<th>Classification Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeviceCategory</td>
<td>Endpoint</td>
</tr>
<tr>
<td>deviceType</td>
<td>ir500</td>
</tr>
<tr>
<td>default config group</td>
<td>default-ir500</td>
</tr>
<tr>
<td>default firmware group</td>
<td>default-ir500</td>
</tr>
<tr>
<td>tunnel provisioning group</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

CSMP Client

CSMP Client is a GUI field tool used to manage and monitor the WPAN gateway and WPAN range extender hardware and networking information.

The “GET” function in the field tool is used to obtain status and performance information about the devices in real time. The “POST” function is used to set device parameters in real time. CSMP Client can be used as a diagnostic tool to check a single device or the whole mesh network.

The field tool has two connection modes to connect a WPAN gateway or WPAN range extender:

- Point-to-Point Protocol (PPP) over Serial console port
- IPv6 through WPAN network
Role of CG-DM

CG-DM is a GUI field tool used to troubleshoot, configure and to update firmware images on WPAN Gateway devices.

Configuring the WPAN Gateway and WPAN Range Extender

- Accessing the Configuration through the Console Port, page 5-14
- Uploading a Device to CG-NMS, page 5-18
- Registering with CG-NMS, page 5-19
- Configuring an IR 500 Series Device with CG-NMS, page 5-19

Accessing the Configuration through the Console Port

You can access the WPAN gateway or WPAN range extender configuration by connecting to the console port on either device.

Warning
Do not connect or disconnect cables to the ports while power is applied to the switch or any device on the network because an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed from the switch and cannot be accidentally be turned on, or verify that the area is nonhazardous before proceeding. Statement 1070

Warning
If you connect or disconnect the console cable with power applied to the switch or any device on the network, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding. Statement 1080

- Connecting to the WPAN Gateway Console Port, page 5-14
- Connecting to the WPAN Range Extender Console Port, page 5-15

Connecting to the WPAN Gateway Console Port

Note
The required cables are:
- RJ-45-to-DB-9 adapter cable (not supplied). You can order this cable from Cisco (part number CAB-CONSOLE-RJ45=).
- USB-to-DB-9 adapter cable (not supplied).

To connect to the WPAN gateway console port:

Step 1
Connect the USB-to-DB-9 adapter cable to a USB port on the PC. Connect the RJ-45-to-DB-9 adapter cable to the WPAN gateway console port.

Step 2
Connect the DB-9 end of the USB-to-DB-9 adapter cable to the DB-9 end of the RJ-45-to-DB-9 adapter cable.
Connecting to the WPAN Range Extender Console Port

**Note**

The required cables are:
- RJ-45-to-DB-9 adapter cable (not supplied). You can order this cable from Cisco (part number CAB-CONSOLE-RJ45=).
- USB-to-DB-9 adapter cable (not supplied).

To connect to the WPAN range extender console port:

**Step 1**

Use a 0.5 in. (13 mm) socket wrench to remove the console port cover. See Figure 5-8.
Figure 5-8 Removing the Console Port Cover

Step 2 Connect the USB-to-DB-9 adapter cable to a USB port on the PC. Connect the RJ-45-to-DB-9 adapter cable to the WPAN range extender console port. See Figure 5-9.

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Console port cover</td>
</tr>
<tr>
<td>1</td>
<td>0.5 in. (13 mm) Socket wrench</td>
</tr>
</tbody>
</table>
Step 3 Connect the DB-9 end of the USB-to-DB-9 adapter cable to the DB-9 end of the RJ-45-to-DB-9 adapter cable.

Step 4 When you are finished configuring the WPAN range extender, disconnect the cable from the console port, and place the console port cover back on the console port to cover it. Use a 0.5 in. (13 mm) socket wrench to torque the console port cover to 6–7 ft-lbs (8.13–9.49 N-m). See Figure 5-10.
Uploading a Device to CG-NMS

WPAN gateway and WPAN range extender devices can be uploaded to CG-NMS using a Device Properties CSV file. For more information see the “Common Device Operations” section of the Cisco Connected Grid Network Management System User Guide.

A sample file content for a WPAN gateway device is:

eid, deviceType, endUserIPv6Prefix, endUserIPv6PrefixLen, lat, lng
00173b12003d003b, ir500, 2001:dead:beaf:2::,64,12,12

A sample file for a WPAN range extender is:

eid, deviceType, lat, lng
00173b12003d003b, ir500, 12, 12

Note: The WPAN range extender does not require an endUserIPv6Prefix.

Note: eid: Is the EUI64 version of the MAC of WPAN interface of the device
endUserIPv6Prefix and endUserIPv6PrefixLen are described in the configuration section below. Every uploaded WPAN gateway and WPAN range extender device is put in the "default-ir500" config and firmware groups if a group name is not specified in the csv.

Registering with CG-NMS

WPAN gateway and WPAN range extender devices use CSMP for communicating with CG-NMS. The registration process involves handshaking between the devices and the CG-NMS.

During registration, CG-NMS pushes a configuration file from a user defined CG-NMS configuration file to each device.

You use a configuration template to define the configuration file for each group dedicated to the WPAN gateway and WPAN range extender devices. The configuration file and its contents are pushed to the devices when they register with CG-NMS.

Configuring an IR 500 Series Device with CG-NMS

During registration, CG-NMS pushes the user defined configuration from the "template" to each device. You can also initiate an on demand configuration push to all devices in the group using a "Push Configuration" option in CG-NMS.

For more information see the “Editing the ENDPOINT Configuration Template” and the “Pushing Configurations to Endpoints” sections of the Cisco Connected Grid Network Management System User Guide.

The configuration tasks include:

- Configuring Serial Interface Settings, page 5-19
- Configuring MAP-T Settings, page 5-20
- Configuring Raw Socket Settings, page 5-20
- Configuring Mesh Link Settings, page 5-21
- Configuring NAT44, page 5-21

Configuring Serial Interface Settings

The WPAN gateway serial interface settings include:

- Media Type (RS232 or RS485)
- Parity
- Baud Rate
- Stop Bit
- Data bits
- Flow control

For more information see the “Editing the ENDPOINT Configuration Template” section of the Cisco Connected Grid Network Management System User Guide.
Configuring MAP-T Settings

The MAP-T draft-01+ settings for the WPAN gateway are:
- DefaultMapping IPv6 Prefix
- IPv4 Prefix
- IPv6 Prefix Length
- IPv4 Prefix Length
- EA Bits Length

For more information see the “Editing the ENDPOINT Configuration Template” section of the *Cisco Connected Grid Network Management System User Guide*.

MAP-T Settings for a WPAN Gateway in FAN

**Note**
On the Cisco IOS ASR1000, MAP-T rules are set-up by indicating the following MAP-T domain rules:
- IPv6 BMR
- IPv4 BMR
- IPv6 DMR

On the WPAN gateway, the MAP-T IPv6 is an End-user IPv6 prefix that integrates the MAP-T BMR IPv6 rules + IPv4 suffix value, the length being based on the BMR EA length value.

For example, a CG-NMS CSV file for a WPAN gateway contains:

```
eid,devicetype,lat,lng,meshPanid,status,endUserIPv6Prefix,endUserIPv6PrefixLen
00173B1500340036,ir500,37.4187911,-121.9196689,10,unheard,2019:1111:2222:1000::,48
```

The file content can be read as:
- IPv6 BMR = 2019:1111:2222::
- IPv6 BMR prefix length = 48
- IPv6 End-User prefix = IPv6 BMR = 2019:1111:2222:1000:: giving the WPAN gateway an IPv4 address = MAP-T IPv4 prefix = CG-NMS set-up + IPv4 suffix = 10 (or .16 decimal)

Configuring Raw Socket Settings

The Raw Socket settings for the WPAN gateway are:
- TCP idle timeout (min)—Sets the time to maintain an idle connection.
- Local port—Sets the port number of the device.
- Peer port—Sets the port number of the client/server connected to the device.
- Peer IP address—Sets the IP address to the host connected to the device.
- Connect timeout—Sets the TCP client connect timeout for WPAN gateway devices. When the connect timeout is 0, the WPAN gateway role is changed to the to the TCP server.

For more information, see the “Editing the ENDPOINT Configuration Template” and the “Raw Sockets Metrics and Sessions” sections of the *Cisco Connected Grid Network Management System User Guide*. 
Configuring Mesh Link Settings

For configuring mesh link settings such as ‘Mesh SSID’ and ‘Transmit Power’ see the “Managing Devices” chapter of the Cisco Connected Grid Network Management System User Guide.

Transmit Power Values

For more information about the transmit power values, see the “Regulatory Domain or Geographic Region Transmission Specifications” section on page A-5.

Configuring NAT44

Note

This section only applies to the WPAN gateway.

NAT44 settings for the WPAN gateway can be configured. In order to configure NAT44 properties you can edit the device template or use the import a CSV file method.

For more information see the “Editing the ENDPOINT Configuration Template” or “Adding a File to CG-NMS” sections of the Cisco Connected Grid Network Management System User Guide.

The following fields can be specified:

- nat44InternalAddress0
- nat44InternalPort0
- nat44ExternalPort0

where 0-3 are four valid map index.

You must make sure that the config group that the device belongs to has Ethernet enabled. You can select the Enable Ethernet checkbox and save the config template for the config group before the config push.

Because all three fields for a map index are required values, all three fields must be specified for the NAT44 configuration to be applied.

Default values of 127.0.0.1, 0, 0 respectively have to be explicitly specified from CSV for a device in case any of the other settings for a particular map index need not be configured.

If an invalid IPv4 address or other invalid values for a port is specified then NAT44 settings for that particular map index will be ignored during config push.

Related CGR 1000 and ASR 1000 Configurations

- Configuring Raw Socket Configuration on CGR 1000 Series and CGR 2010 Routers, page 5-22
- Configuring the WPAN Settings on CGR 1000 Series Routers, page 5-22
- Configuring an IPv6 DHCP Address Pool on CGR 1000 Series Routers, page 5-22
- Configuring MAP-T on ASR 1000 Series or CSR 1000V Series Routers, page 5-22
- Configuring IPv6 Routing on the CGR 1000 Series and ASR 1000 Routers, page 5-22
Configuring Raw Socket Configuration on CGR 1000 Series and CGR 2010 Routers

For information about configuring Raw Socket on the CGR 1000 series and ASR 1000 routers, see the following guides:

- Raw Socket Transport Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)
- “Raw Socket Transport” chapter of Cisco 1000 Series Connected Grid Routers SCADA Software Configuration Guide
- Configuring Raw Socket Protocol on the CGR 2010 Router

Configuring the WPAN Settings on CGR 1000 Series Routers

An SSID and PAN ID must be configured on the CGR1000 series router. For information about configuring and SSID and PAN ID, see the Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide on Cisco.com.

Configuring an IPv6 DHCP Address Pool on CGR 1000 Series Routers

The IPv6 addresses of the WPAN gateway and WPAN range extender are allocated from a central DHCPv6 server during the process of joining the mesh. The CGR1000 router only needs to be configured as a DHCPv6 Relay.

For information about configuring the CGR 1000 series router as a DHCP relay, see the “Configuring IPv6 DHCP Relay” section of the Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide.

Configuring MAP-T on ASR 1000 Series or CSR 1000V Series Routers

MAP-T must be configured on the ASR 1000 or CSR 1000V router.

For information about configuring MAP-T on the ASR 1000 series router, see the “Mapping of Address and Port Using Translation” chapter of the IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S (ASR 1000).


Configuring IPv6 Routing on the CGR 1000 Series and ASR 1000 Routers

IPv6 routing needs to be configured on the CGR 1000 series and ASR 1000 routers. For information about configuring IPv6 on the CGR 1000 series and ASR 1000 routers, see the following guides:

- “Configuring IPv6 Multicast Agent” chapter of Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide
- IP Routing: BGP Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)
CG-NMS WPAN Device Management Related Operations

- Performing Periodic Inventory, page 5-23
- Uploading Firmware, page 5-24
- Creating Rules and Events, page 5-24

Performing Periodic Inventory

Depending on the report periodic interval set in the configuration template, devices report regular inventory metrics to CG-NMS using CSMP. CG-NMS stores the reported properties and metrics.

For more information, see the “Configuring Rules” section of the Cisco Connected Grid Network Management System User Guide.

The properties and metrics of a sample WPAN device reported include:

- Inventory
  - Name
  - EID
  - Device Category
  - Manufacturer
  - Status
  - IP Address
  - Last Heard
  - Last Property Heard
  - Last Metric Heard
  - Model Number
  - Serial Number
  - Firmware Version
  - Config Group
  - Firmware Group
  - Location
  - Labels
  - Meter Certificate
- Mesh Device Health
  - Uptime
- Mesh Link Settings
  - SSID
  - PANID

- Transmit Power
- Security Mode

- Mesh Link Metrics
  - Mesh Link Transmit Speed
  - Mesh Link Receive Speed
  - Mesh Link Transmit Packet Drops
  - Mesh route RPL Hops
  - Mesh Route RPL Link Cost
  - Mesh Route RPL Path Cost
  - Mesh Route RSSI
  - Mesh Route Reverse RSSI

- Network Routes Metrics
- Routing Path Metrics
- Raw Socket Metrics
- MAP-T Information

**Uploading Firmware**

Uploading of firmware to WPAN gateway and WPAN range extender devices can be performed by the CG-NMS. You can:

- Upload ir500 firmware images to CG-NMS via the GUI.
- Execute a firmware upload to a specific group of devices.
- Perform “Set Backup” and “Schedule Reload” operations.

For more information, see the “Configuring Devices” and “Pushing Configurations to Endpoints” sections of the *Cisco Connected Grid Network Management System User Guide*.

**Creating Rules and Events**

You can create rules and events for WPAN gateway and WPAN range extender devices using CG-NMS.

For more information, see the “Configuring Rules” section of the *Cisco Connected Grid Network Management System User Guide*. 