Configuring Cisco Resilient Mesh and the WPAN Module

Resilient Mesh and WPAN Module Overview

This guide explains how to install the IEEE 802.15.4e/g Cisco Wireless Personal Area Network (WPAN) module and how to configure the Cisco Resilient Mesh. This guide addresses configuration for a Cisco IR8100 Series Router installed with Cisco IOS-XE software.

Note IoT FND provides the user interface for all Cisco Resilient Mesh configuration and management. Cisco Resilient Mesh has no CLI and no graphical user interface for configuration or management.

All configuration and management occur only by using IoT FND through the IR8140H Series WPAN module by using Cisco IOS-XE software commands.

Note For a description of Cisco Resilient Mesh operation, see Information About Cisco Resilient Mesh and WPAN.

On the IR8140H, the WPAN module serial PID is displayed in IOS-XE as IRMH-WPAN-NA, as shown in the following example:

```
Router#sh inv

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "Cisco Catalyst IR8140H Heavy Duty Series Router with PoE"
PID: IR8140H-P-K9      , VID: V00  , SN: FDO2441J91D

NAME: "Power Supply Module 0", DESCR: "60W AC Power Supply module"
PID: IRMH-PWR60W-AC    , VID: V01  , SN: LIT22503LDK

NAME: "module 0", DESCR: "Cisco Catalyst IR8140H-P-K9 Fixed and pluggable Interface Module
 controller"
PID: IR8140H-P-K9      , VID:      , SN:

NAME: "NIM subslot 0/1", DESCR: "IRMH-WPAN-NA Module"
PID: IRMH-WPAN-NA      , VID: V00  , SN: FDO24350D18
```

Configuring the WPAN Interface

At the IR8140H, configure the WPAN Module interface as follows:

Procedure

Step 1 Enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter the command **interface wpan** *slot*/*port* to specify the port and slot of the WPAN module:

WPAN slot is always 1 and port is 0/1.

Example:

```
Router(config)# int WPAN 0/1/0
```

Enabling dot1x, mesh-security and DHCPv6

You must enable the dot1x (802.1X), mesh-security, and DHCPv6 features to configure the WPAN interface. To enable these features, enter the following commands:

Procedure

Step 1 Enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enable 802.1X authentication globally on the router:

Example:

```
Router(config)# dot1x system-auth-control
```

Step 3 Enter interface configuration mode and specify the WPAN interface:

Example:

```
Router(config)# interface WPAN 0/1/0
```

Step 4 Enable the WPAN interface to respond to messages meant for an IEEE 802.1x authenticator:

Example:

```
Router(config-if)# dot1x pae authenticator
Router(config-if)#authentication host-mode multi-auth
Router(config-if)#authentication port-control auto
```

Step 5 Enable IPv6 and specify a destination address to which client messages are forwarded and to enable Dynamic Host Configuration Protocol (DHCP) for IPv6 relay service on the interface:

Example:

```
Router(config-if)#ipv6 enable
Router(config-if)#ipv6 dhcp relay destination  <IPv6 address >
```

Configuring IEEE154 Settings

Follow these steps to configure WPAN radio-related settings:

Procedure

Step 1 Enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enter interface configuration mode and specify the WPAN interface:

Example:

```
Router(config)# interface WPAN 0/1/0
```

Step 3 Configure the name of your IEEE 802.15.4 Personal Area Network Identifier (PAN ID):

Example:

```
Router(config-if)#ieee154 panid ?
  <0-65534>  Enter a value between 0 and 65534

Router(config-if)#ieee154 panid 121
```

Step 4 Configure the name of the Service Set Identifier (SSID).

The SSID identifies the owner of the Resilient Mesh Endpoint (RME). The SSID is set on a RME in manufacturing, and that same SSID must also be configured on the IR8100 WPAN interface.

Example:

```
Router(config-if)# ieee154 ssid ?
  WORD  ssid string (Max size 32)
Router(config-if)# ieee154 ssid myWPANssid
```

Step 5 Configure the notch.

A notch is a list of disabled channels from the 902-to-928 MHz range. If there is no notch at all, then all channels are enabled. if there is a notch [x, y], then channels between x and y are disabled.

Note A channel list is a list of enabled channels.

Notch configuration must comply with your regional regulations (for example, a notch configuration is not required for the U.S.). Notch configuration must match between the WPAN interface of the IR8100 and the RME.

Example:

```
Router(config-if)#ieee154 notch ?
  <0-128>  channel id
Router(config-if)#ieee154 notch 10-15
```

Note To verify the notch configuration, you can use the **show hardware channel-list** command, for example:

```
Router(config-if)# end
Router# show wpan 0/1/0 hardware channel-list
channel list: 0 1 2 3 4 5 6 7 8 9 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
```

Step 6 Specify the IEEE154 PHY mode (a value from 1-255) of the IRMH-WPAN module.

The IRMH-WPAN module operates within a RF900 wireless network to provide digital automation (DA) control over RMEs. The PHY mode setting selects the adaptive modulation, which enhances the backward compatibility with the classic Cisco Resilient Mesh network and improves the transmitting ability in the classic Cisco Resilient Mesh network. Adaptive modulation is supported in both Wi-SUN and Cisco mesh modes.

Supported PHY modes are:

- 1: Classic; Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=ON; Channel Spacing=200 kHz
- 17: Classic; Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=OFF; Channel Spacing=200 kHz
- 2: Classic; Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=ON; Channel Spacing=400 kHz
- 18: Classic; Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=OFF; Channel Spacing=400 kHz
- 64: Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=OFF; Channel Spacing=200 kHz

- 96: Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=ON; Channel Spacing=200 kHz
- 66: Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=OFF; Channel Spacing=400 kHz
- 98: Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=ON; Channel Spacing=400 kHz
- 128: Rate=100 kb/s; Modulation=OFDM; Option=1; MCS=0; Channel Spacing=1200 kHz
- 129: Rate=200 kb/s; Modulation=OFDM; Option=1; MCS=1; Channel Spacing=1200 kHz
- 130: Rate=400 kb/s; Modulation=OFDM; Option=1; MCS=2; Channel Spacing=1200 kHz
- 131: Rate=800 kb/s; Modulation=OFDM; Option=1; MCS=3; Channel Spacing=1200 kHz
- 132: Rate=1200 kb/s; Modulation=OFDM; Option=1; MCS=4; Channel Spacing=1200 kHz
- 133: Rate=1600 kb/s; Modulation=OFDM; Option=1; MCS=5; Channel Spacing=1200 kHz
- 134: Rate=2400 kb/s; Modulation=OFDM; Option=1; MCS=6; Channel Spacing=1200 kHz
- 144: Rate=50 kb/s; Modulation=OFDM; Option=2; MCS=0; Channel Spacing=800 kHz
- 146: Rate=200 kb/s; Modulation=OFDM; Option=2; MCS=2; Channel Spacing=800 kHz
- 147: Rate=400 kb/s; Modulation=OFDM; Option=2; MCS=3; Channel Spacing=800 kHz
- 149: Rate=800 kb/s; Modulation=OFDM; Option=2; MCS=5; Channel Spacing=800 kHz
- 150: Rate=1200 kb/s; Modulation=OFDM; Option=2; MCS=6; Channel Spacing=800 kHz
- 161: Rate=50 kb/s; Modulation=OFDM; Option=3; MCS=1; Channel Spacing=400 kHz
- 162: Rate=100 kb/s; Modulation=OFDM; Option=3; MCS=2; Channel Spacing=400 kHz
- 163: Rate=200 kb/s; Modulation=OFDM; Option=3; MCS=3; Channel Spacing=400 kHz
- 164: Rate=300 kb/s; Modulation=OFDM; Option=3; MCS=4; Channel Spacing=400 kHz
- 165: Rate=400 kb/s; Modulation=OFDM; Option=3; MCS=5; Channel Spacing=400 kHz
- 166: Rate=600 kb/s; Modulation=OFDM; Option=3; MCS=6; Channel Spacing=400 kHz
- 192: Rate=6.25 kb/s; Modulation=OQPSK; Chip Rate=100 kchip/s; Rate Mode=0; Channel Spacing=200 kHz

Note Adaptive modulation only supports configuring the same Orthogonal Frequency-division Multiplexing (OFDM) option PHY mode or the same OFDM option plus FSK PHY mode.

Cisco Resilient Mesh Release 6.3 only supports PHY mode 64, 66, 161, 162, 163, 165, and 166 for IRMH-WPAN.

The following example shows configuring adaptive modulation in Wi-SUN mode, which sets the channel to 254 and notch to none:

Example:

```
Router(config-if)#ieee154 phy-mode 166 165 164 163

Router(config-if)#
```

Note To verify PHY mode configuration, enter **show wpan 4/1 hardware config** in privileged EXEC mode.

Configuring Group Multicast

Follow these steps to configure group multicast on the router. Group multicast allows the router to forward multicast traffic to a specific group of devices. The devices in one group can cross multiple PANs.

Note This feature is not supported in Cisco Resilient Mesh Release 6.3.

Procedure

Step 1 Enter global configuration mode:

Example:

```
Router# configure terminal
```

Step 2 Enable IPv6 multicast-routing:

Example:

```
Router(config)# ipv6 multicast-routing
```

Step 3 Enable MPL:

Example:

```
Router(config)#fan-mpl domain 0
```

Step 4 Check the mcast address reported by node:

- show wpan 0/1/0 rpl mcast-info domains
- show wpan 0/1/0 rpl mcast-info groups

Step 5 Enter interface configuration mode and add the multicast agent interface (uplink interface):

Example:

```
Router(config)#interface WPAN 0/1/0
Router(config-if)#mcast-agent interface gi0/0/0
```

Step 6 Enable LFN:

Example:

```
Router(config)#interface WPAN 0/1/0
Router(config-if)#lfn
```

Step 7 Add the multicast agent port:

Example:

```
Router(config-if)#mcast-agent port
```

Step 8 Add the multicast agent group:

Example:

```
Router(config-if)#mcast-agent group-join ?
  X:X:X:X::X multicast group address
```

Step 9 Check the multicast agent port, interface, and groups:

Example:

```
show wpan 0/1/0 mcast-agent ?
 group-join multicast group address
 interface mcast-interface
 ports Mcast optional ports
```

Configuring RPL

Resilient Mesh Endpoints (RMEs) perform routing at the network layer using the Routing Protocol for Low-Power and Lossy Networks (RPL). For information about RPL, refer to "RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks".

To determine the available RPL functions, query the **rpl** command:

```
Router(config)#int WPAN 0/1/0
Router(config-if)#rpl ?
  dag-lifetime       RPL DAG lifetime
  dag-lifetime-unit  RPL DAG lifetime unit in seconds
  dio-dbl            RPL DIO dbl value
  dio-min            RPL DIO min value
  option             RPL option configuration for wisun mode
  pon                RPL PON configuration
  route-poisoning    Route poisoning
  storing-mode       Storing mode
  version-incr-time  Version increment time in minutes
```

Parameter	Range	Description
dag-lifetime	Value between 1 and 255	Destination-Oriented Directed Acyclic Graph (DODAG) lifetime duration. Each node uses the lifetime duration parameter to drive its own operation (such as Destination Advertisement Object (DAO) transmission interval). Also, the router uses this lifetime value as the timeout duration for each RPL routing entry.
dag-lifetime-unit	Value between 60 and 3600	DAG lifetime unit in seconds.

Parameter	Range	Description
dio-dbl	Value between 0 and 9	DODAG Information Object (DIO) double parameter. DIO double is a doubling factor parameter used by the RPL protocol. **Caution** This command must only be used by an expert RPL protocol administrator.
dio-min	Value between 14 and 23	Minimum DIO value. **Caution** This command must only be used by an expert RPL protocol administrator.
pon	PON RPL instance.	Power Outage Notification (PON).
version-incr-time	Value between 10 and 255	Minimum time between RPL version increments.

Enabling the RPL PON Instance

The RPL Power Outage Notification (PON) instance is used in the power outage report. (See Configuring the Power Outage Server, on page 9.)

If you enable this option, the node uses the new PON instance in the outage report. If this option is disabled, the node uses the original RPL instance to report the outage event.

Note This option is supported only in WiSUN mode.

```
Router(config)#int WPAN 0/1/0
Router(config-if)#rpl pon ?
  dio-dbl   RPL PON DIO dbl value
  dio-min   RPL PON DIO min value
  instance  Enable RPL PON instance
Router(config-if)#rpl pon instance
```

Configuring Redistribution of RPL in Other Routing Protocols

On IR8100 Series routers, routes learned from RPL can be redirected to other routing protocols directly. The route type is RL instead of connected in the ipv6 routing table. The following commands show redistribution of RPL to the OSPF protocol:

```
Router(config)#ipv6 router ospf 100
Router(config-rtr)#redistribute rpl metric 3
```

Configuring the Power Outage Server

In the event of a power outage, Mesh Endpoints (MEs) perform the necessary functions to conserve energy and notify neighboring nodes of the outage. Routers relay the power outage notification to a power notification server, which then issues push notifications to customers to relate information on the outage. In most cases, the outage server is your IoT FND server.

To configure the power outage server, use the **outage server** command to specify an IPv6 address or IPv6 resolvable FQDN of a server. For example:

```
Router(config-if)# outage server 2001:c1::8a43:e1ff:fec3:2aa
```

or

```
Router(config-if)# outage server fnd.cisco.com
```

Configuring Cisco Resilient Mesh Security

RMEs use the IEEE 802.1X protocol, known as Extensible Authentication Protocol over LAN (EAPOL), for authentication.

Note Cisco Resilient Mesh does not support TLS 1.1. If the RADIUS server does not support TLS1.2, you need to disable TLS 1.1 on the RADIUS server for compatibility.

Configuring Mesh Key

Procedure

Step 1 Set the mesh key using the command **mesh-security set mesh-key interface wpan <slot>/<port> key <hex-string>**, where <hex-string> is an even number of hex digits, up to 32.

Example:

```
Router# mesh-security set mesh-key interface wpan 0/1/0 key 1234567891234567
```

Step 2 To configure mesh lfn key, use the **mesh-security set mesh-lfn-key**command.

Example:

```
Router# mesh-security set mesh-lfn-key interface wpan 0/1/0 key 12312311
```

Step 3 To configure the mesh key lifetime, use the **mesh-security mesh-key lifetime** command in interface configuration mode.

The **mesh-key lifetime** value should be less than 120 days (10368000 seconds).

Caution Use this command only if you are an expert mesh-security administrator.

Example:

```
Router(config)#int wpan 0/1/0
Router (config-if)# mesh-security mesh-key lifetime 60
```

Note Mesh-Security configuration and keys do not appear in **show running-config** or **show startup-config** command output.

Step 4 To configure lfn mesh-key lifetime, use the following commands:

Example:

```
mesh-security mesh-lfn-key revocation-lifetime-reduction 30
mesh-security mesh-lfn-key rollover-ratio 180
mesh-security mesh-lfn-key lifetime 7776000 ptk-lifetime 31104000 pmk-lifetime 46656000
```

Example Cisco Resilient Mesh Security Configuration

The following example shows what is required for mesh-security.

Note The MTU setting on the AAA server must be set to 800 bytes or lower, because IEEE802.1x implementation in RMEs limits the MTU to 800 bytes. RADIUS servers can use auth-port 1812 and acct-port 1813 instead of 1645 and 1646, respectively.

```
!
aaa new-model
!
!
aaa group server radius nps-group
 server name nps-radius
!
aaa authentication enable default none
aaa authentication dot1x default group nps-group
<...snip...>
dot1x system-auth-control
!
<...snip...>
!
!
interface Wpan0/1/0
 no ip address
 ip broadcast-address 0.0.0.0
 no ip route-cache
 ieee154 beacon-async min-interval 120 max-interval 900 suppression-coefficient 1
 ieee154 panid 7224
 ieee154 ssid migration_far2
 ieee154 txpower -30
 authentication host-mode multi-auth
 authentication port-control auto
 ipv6 address 2092:1:1:1::/64
 ipv6 enable
 ipv6 dhcp relay destination  2010:A0B0:1001:22::2
 dot1x pae authenticator
mesh-security mesh-key lifetime 259200
end
!
!
radius server nps-radius
```

```
 address ipv4 <IP address> auth-port 1645 acct-port 1646
 key <RADIUS key>
!
```

Verifying Cisco Resilient Mesh Security Configuration

Use the following commands to verify Cisco Resilient Mesh Security configuration:

- **show dot1x all details**

  Displays the configuration and clients of the Cisco Resilient Mesh 802.1X security configuration.

Note The output for this command shows only new or re-authentications. It does not show nodes that are in the process of warm-starting (and have cached the security credentials).

```
Router#show dot1x all details
Sysauthcontrol                  Enabled
Dot1x Protocol Version               3

Dot1x Info for WPAN0/1/0
-----------------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List Empty
```

- show mesh-security keys lfn

```
Router#show mesh-security keys lfn
Mesh Interface: WPAN0/1/0

LFN Pairwise Master Key Lifetime : 540 Days 0 Hours 0 Minutes 0 Seconds
LFN Pairwise Temporal Key Lifetime: 360 Days 0 Hours 0 Minutes 0 Seconds
LFN Mesh Key Lifetime : 90 Days 0 Hours 0 Minutes 0 Seconds

Rollover ratio: 180
Revocation reduction: 30

LFN Key ID : 0 *
Key expiry : Wed Jun 7 11:35:37 2023
Time remaining : 81 Days 21 Hours 23 Minutes 21 Seconds

LFN Key ID : 1
Key expiry : Tue Sep 5 11:35:37 2023
Time remaining : 171 Days 21 Hours 23 Minutes 21 Seconds
```

- **show mesh-security keys**

  Displays the mesh-security set-key configuration.

```
Router#show mesh-security keys
Mesh Interface: WPAN0/1/0

Pairwise Master Key Lifetime  : 120 Days 0 Hours 0 Minutes 0 Seconds
```

```
Pairwise Temporal Key Lifetime: 60 Days 0 Hours 0 Minutes 0 Seconds
Mesh Key Lifetime    : 30 Days 0 Hours 0 Minutes 0 Seconds

Key ID         : 3 *
Key expiry     : Sun Dec  6 20:28:12 2020
Time remaining : 0 Days 1 Hours 5 Minutes 11 Seconds
```

- **show mesh-security session all**

  Displays Cisco Resilient Mesh security session details.

Note The output for this command shows only new or re-authentications. It does not show nodes that are in the process of warm-starting (and have cached the security credentials).

```
Router# show mesh-security session all
MAC Address              State                    Mesh Keys
00:07:81:08:00:3C:25:03  Encryption Enabled       11..
00:17:3B:0B:00:21:00:2F  Encryption Enabled       .1..
00:07:81:08:00:3C:22:02  Encryption Enabled       11..
00:07:81:08:00:3C:25:02  Encryption Enabled       11..
00:07:81:08:00:3C:22:0A  Encryption Enabled       11..
00:07:81:08:00:3C:22:06  Encryption Enabled       11..
00:07:81:08:00:3C:24:05  Encryption Enabled       ....
00:07:81:08:00:3C:24:08  Encryption Enabled       ....
00:07:81:08:00:3C:23:01  Encryption Enabled       11..
```

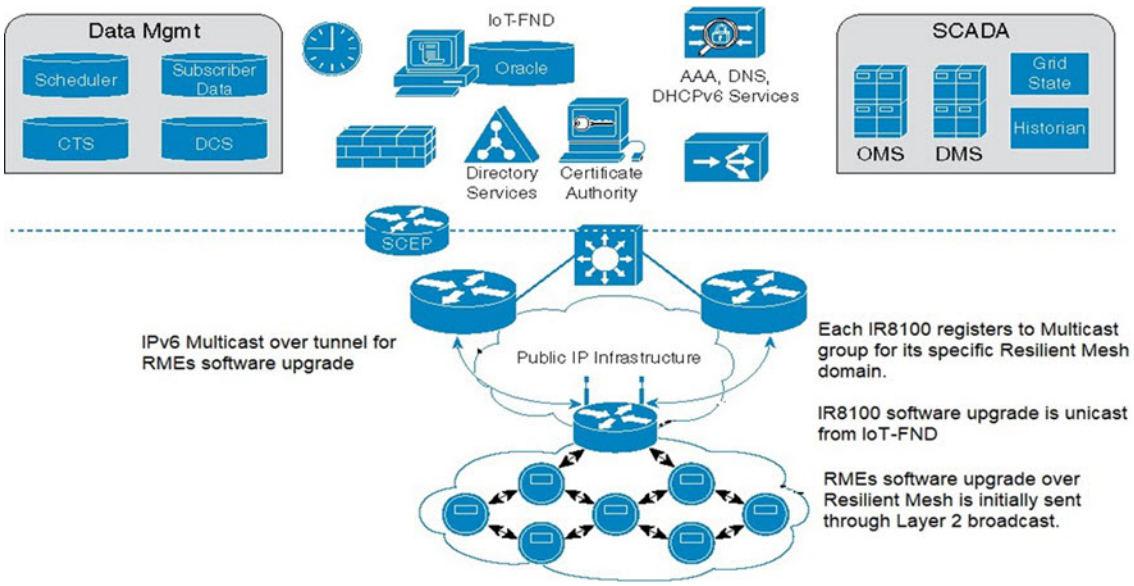
- **show mesh-security interface wpan <slot >/<port >**

Configuring the IPv6 Multicast Agent

You must configure an IPv6 multicast agent to enable multicasting traffic between IoT FND, or the Advanced-Metering Infrastructure (AMI) application server in a Network Operations Center (NOC), and the Cisco Resilient Mesh network.

IPv6-multicasting requires proper configuration on the head-end router (Cisco ASR 1000) as well as on IoT FND and the AMI head-end server.

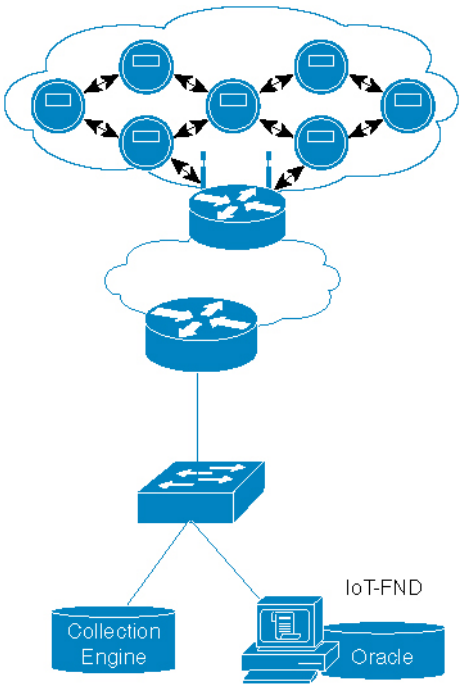
The following figure shows an IPv6 FAN with a multicast configuration.



The IPv6 multicast configuration has the following characteristics:

- IPv6 Multicast is used between the IoT FND or CE and the Cisco Resilient Mesh endpoints when performing:
  - Software upgrade of the endpoints
  - Demand reset messages
  - Demand response messages (there could be more than one group for this per meter)
  - Targeted pings (group of meters on a given feeder, for example)
  - Group of meters with the same read time/cycle
- Each PAN is a multicast group with the unicast-prefix-based multicast address (RFC 3306)
- The head-end router routes (PIMv6 SSM) all multicast traffic to the unicast-prefix-based multicast address to the IR8100 (MLDv2)
- IR8100 multicast agent receives the multicast

The following figure shows an overview of the Multicast operation in an IPv6 FAN:



There are two ways to forward multicast traffic to an IR8100 running Cisco IOS-XE from the head-end:

- Configure the IR8100 as a multicast client where the tunnel is configured with **ipv6 mld join-group**.

  For this method, configure the IR8100 tunnel interface with MLD as follows:

```
Router (config)# interface Tunnel100
Router (config-if)# ipv6 mld join-group ff38:40:2001:0db8:beef:cafe:0:1
```

- Enable IPv6 multicast routing on the and configure it as a PIM6 router. This is the preferred method and is shown in the next section.

Note Note: In above example, the IP address is constructed from the the IPv6 subnet of WPAN.

Configuring IR8100 as PIM6 Router

The preferred method of forwarding multicast traffic to the IR8100 is to enable ipv6 multicast routing on the IR8100 and configure it as a PIM6 router. Because the unicast-prefix-based multicast address is still needed for WPAN, you must configure it under loopback0 on the IR8100, and configure the IR8100 to become a PIM-neighbor with the ASR head-end.

To configure this method, perform the following steps on the IR8100:

Procedure

Step 1 Enable IPv6 multicast-routing:

Example:

```
Router(config)# ipv6 multicast-routing
```

Step 2 Configure MLD under the loopback0:

Example:

```
Router(config-if)# interface loopback 0
Router(config-if)# ipv6 mld join-group ff38:40:2001:0db8:beef:cafe:0:1
```

Step 3 Configure the IPv6 PIM Rendezvous Point (RP):

Example:

```
Router(config)# ipv6 pim rp-address 2333::1
```

Example

ASR/CSR configuration example:

```
ipv6 pim rp-address 2001:DB9::1 bidir
ipv6 pim spt-threshold infinity
 !
interface Loopback0
 ipv6 address 2001:DB9::1/128
 ipv6 pim hello-interval 500
ipv6 pim
 !
interface GigabitEthernet0/0/0
ipv6 pim
```

Configuring DTLS Relay for EST

The Cisco Resilient Mesh uses Enrollment over Secure Transport (EST) over CoAP/DTLS/UDP for certificate enrollment. During the initial bootstrapping process, nodes that have already joined the network (enrolled and authenticated) act as Datagram Transport Layer Security (DTLS) relays for nodes being bootstrapped.

Use the **dtls-relay** command in interface configuration mode to configure DTLS relay:

```
Router(config)#interface wpan 0/1/0
Router (config-if)#dtls-relay ?
X:X:X:X::X   IPv6 address (aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh, aaaa::bbb)
Router(config-if)#dtls-relay 2060:FACD::6 ?
lifetime     specify session lifetime
max-sessions specify maximum number of sessions
port         destination port
Router(config-if)#dtls-relay 2060:FACD::6 port 61629 max-sessions 10 lifetime 300
```

Use the **show wpan 0/1/0 config** command to verify the DTLS relay configuration.

Configuring Wi-SUN Mode

Wireless Smart Utility Network (Wi-SUN) mode is supported from Cisco Resilient Mesh Release 6.1.

Note

- Cisco Resilient Mesh Release 6.3 only supports Wi-SUN mode.
- Changing wisun-mode requires a module reload.
- In Wi-SUN mode, storing mode is not supported.
- In Wi-SUN mode, the mesh key should be reconfigured after changing PANID.

When the IR8100 is in Wi-SUN mode, if there are nodes in the WPAN route table and route poisoning is not enabled, changing the PANID will enable temporary RPL poisoning. It will be disabled automatically. The new PANID will take affect after 3 DIO messages are sent. Validate the connectivity to the IR8100 router.

To enable Wi-SUN mode, follow these steps:

Procedure

Step 1 Enter configuration mode:

Example:

```
Router#configure terminal
```

Step 2 Specify the WPAN interface and enter interface configuration mode:

Example:

```
Router(config)#interface wpan 0/1/0
```

Step 3 Enable wi-sun mode:

Example:

```
Router(config-if)#wisun-mode
```

Step 4 Set the beacon version increase interval to 0:

Example:

```
Router(config-if)#ieee154 beacon-ver-incr-time 0
```

Step 5 Set the phy mode to wisun supported phy mode:

Example:

```
Router(config-if)#ieee154 phy-mode 66
```

Step 6 (Optional) Change ucast dwell, bcast dwell, and bcast interval.

If not configured, all the parameters use the default values.

Example:

```
Router(config-if)#ieee154 wisun-dwell ucast-dwell-int <125> bcast-dwell-int <125> bcast-int
 <500>
```

Modulation and Data Rate (MDR)

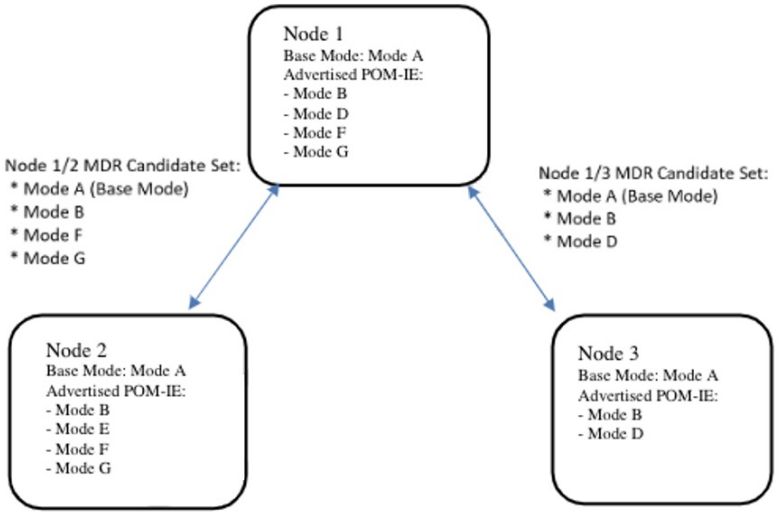
FAN networks typically consist of devices with different physical layer capabilities. The wireless links between different devices in the network may vary greatly due to distance, transmission power, noise, or other interference. Because of these differences, devices should be able to adapt the data rate or RF modulation based on the environment conditions and the neighboring devices communicated with. Multiple PHY mode configuration in Border Router (BR) and End points will help to achieve the above use case. MDR feature is an already supported feature (spec 1.1v2) with PCAP IE as a header for advertising the configured PHY mode. In FAN 1.1v5, this PCAP IE been advertised as POM IE (Phy Operating Mode Information Element). Refer to FAN 1.1v5 spec 6.3.4.7.1 PHY Operating Mode Discovery.

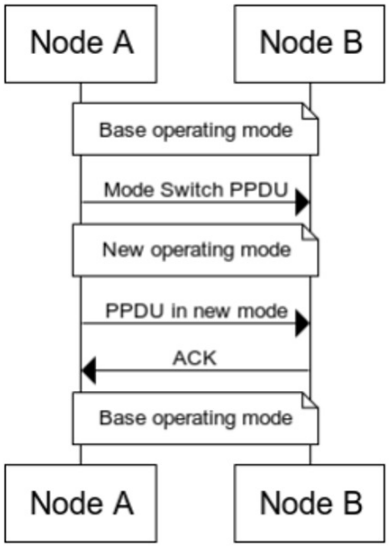
Supported platforms and software releases:

- Border Router: IR8140H, Cisco IOS XE Dulin 17.11.1
- Endpoint: IR510, IR530, WPAN (OFDM and FSK modules), Cisco Resilient Mesh Release 6.6

Selection of PHY Operating Mode and Switching

Based on the set of PHY operating modes advertised by both of a mesh node and a neighbour (indicated by their respective POM-IEs), the intersection of those PHY sets (including the base mode) are candidates for operating mode switching between the two nodes.





Prerequisites

All nodes in a PAN must be administratively configured to use the same base PHY operating mode. Neighbor nodes are able to mutually discover each other's PHY operating modes and make application layer decisions to temporarily "switch" to one of the non-base PHY operating modes.

The following combinations alone supported:

- FSK + FSK
- FSK + OFDM option1
- FSK + OFDM option2
- FSK + OFDM option3
- FSK + OFDM option4
- OFDM option1
- OFDM option2
- OFDM option3
- OFDM option4

Combination of different OFDM options are not supported for configuration.

Limitations

- Up to 4 phy mode configurations are supported on the Border Router.
- Up to 15 PHY operating modes in a POM IE can be processed, as specified in the Wi-SUN Spec.
- CR-Mesh 6.6 MDR feature cannot work with CR-Mesh 6.5 Release.
- CR-Mesh 6.6 supports Wi-SUN mode only.

MDR Configuration

When configuring multiple PHY modes, the first mode MUST be the base mode. On the mesh endpoint, it should be the same base mode.

On IR8140H, use the **ieee154 phy-mode** command to configure PHY mode:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#ieee154 phy-mode ?
Supported Phy-Modes:
64:Rate=50 kb/s; Modulation=2FSK; Modulation Index=1.0; FEC=OFF; Channel Spacing=200 kHz
66:Rate=150 kb/s; Modulation=2FSK; Modulation Index=0.5; FEC=OFF; Channel Spacing=400 kHz
134:Rate=2400 kb/s; Modulation=OFDM; Option=1; MCS=6; Channel Spacing=1200 kHz
144:Rate=50 kb/s; Modulation=OFDM; Option=2; MCS=0; Channel Spacing=800 kHz
147:Rate=400 kb/s; Modulation=OFDM; Option=2; MCS=3; Channel Spacing=800 kHz
149:Rate=800 kb/s; Modulation=OFDM; Option=2; MCS=5; Channel Spacing=800 kHz
150:Rate=1200 kb/s; Modulation=OFDM; Option=2; MCS=6; Channel Spacing=800 kHz
161:Rate=50 kb/s; Modulation=OFDM; Option=3; MCS=1; Channel Spacing=400 kHz
163:Rate=200 kb/s; Modulation=OFDM; Option=3; MCS=3; Channel Spacing=400 kHz
165:Rate=400 kb/s; Modulation=OFDM; Option=3; MCS=5; Channel Spacing=400 kHz
166:Rate=600 kb/s; Modulation=OFDM; Option=3; MCS=6; Channel Spacing=400 kHz
182:Rate=300 kb/s; Modulation=OFDM; Option=4; MCS=6; Channel Spacing=200 kHz

  <1-255>  Enter a value from the list given by: <config-if>ieee154 phy-mode ?

FDO2553J6BF(config-if)#ieee154 phy-mode
FDO2553J6BF(config-if)#ieee154 phy-mode 64 144 147 150
```

PHY mode configured on Endpoint(IR510) – tlv 35 output

```
▼ phyModeList
  ▼ PhyModeInfo
      phyMode          0x40 (64)
      txPower          30 dBm
  ▼ PhyModeInfo
      phyMode          0x90 (144)
      txPower          28 dBm
  ▼ PhyModeInfo
      phyMode          0x93 (147)
      txPower          26 dBm
    bandID             4
    networkScale       small (1)
```

Verifying the Configuration

The following command shows the operating on base PHY mode.

```
FDO2553J6BF#show wpan 0/1/0 link-neighbors table
------------------------ WPAN LINK NEIGHBOR TABLE [1] ----------------------------------------
EUI64                RSSIF   RSSIR   LQIF    LQIR    FIRST_HEARD   LAST_HEARD    MODF        MODR
00173B0500540024     -76     -97     255     95      18:38:04      00:04:57      64          64
6C8BD310003DA362     -43     -67     255     65      18:37:34      00:05:07      64          64
6C8BD310003DA3C4     -44     -67     255     65      18:37:31      00:04:33      64          64
Number of Entries in WPAN LINK NEIGHBOR TABLE: 3
```

The following example shows that the node operating PHY mode is switched from 64 to 147, which is the common highest operating mode between BR and IR510.

```
FDO2553J6BF#show wpan 0/1/0 link-neighbors table
------------------------ WPAN LINK NEIGHBOR TABLE [1] ------------------------------------------
EUI64                  RSSIF   RSSIR   LQIF    LQIR    FIRST_HEARD   LAST_HEARD    MODF       MODR
00173B0500540024       -76     -97     255     95      18:38:04      00:04:57      64         64
6C8BD310003DA362       -45     -69     255     65      18:37:34      00:06:07      147         147
6C8BD310003DA3C4       -44     -67     255     65      18:37:31      00:05:35      64         64
Number of Entries in WPAN LINK NEIGHBOR TABLE: 3
```

Limited Function Node (LFN)

Limited Function Nodes (LFNs) are battery powered end devices. Battery lifetime is expected in the range of 15 to 20 years. LFNs are RPL leaf nodes in the Mesh network, therefore LFNs are relieved of RPL routing functionality. LFN cannot be the parent of other nodes in the Mesh network. Wi-SUN FAN 1.1v5 details the implementation of LFN node in a FAN Mesh network. LFN node has its own unicast interval, broadcast schedule, mesh keys in a FAN.

CR-Mesh 6.6 release enhances LFN support in IR8140 (CABO) WPAN Border router and IR510. IOS XE 17.11 release implements the authentication of LFN node in a FAN.

Supported Platforms:

- IR8140H, Cisco IOS XE Dulin 17.11.1
- WPAN-OFDM module, Cisco Resilient Mesh Release 6.6

LFN Configuration

Cisco IOS XE Dulin 17.11.1 support both FAN 1.0 and FAN 1.1 specifications. In order to have LFN in the Border Router, enable LFN for onboarding LFN mesh nodes in your PAN by using the following commands:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#lfn
```

LFN follows different PAN version in the FAN network and it has its own unicast interval and broadcast schedule. From Border Router, you can configure the broadcast interval for LFN by using the following commands:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#ieee154 lfn-bcast interval 300000 sync-period 1
```

Configure LFN mesh key in Border Router:

```
FDO2553J6BF#mesh-security set mesh-lfn-key interface wpaN 0/1/0 key 12312312
```

Configure LFN mesh key lifetime in Border Router under global CLI:

```
FDO2553J6BF#mesh-security mesh-lfn-key lifetime 7776000 ptk-lifetime 31104000 pmk-lifetime
 46656000
```

Configure LFN mesh rollover-ratio and revocation-lifetime-reduction:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#mesh-security mesh-lfn-key revocation-lifetime-reduction 30
FDO2553J6BF(config-if)#mesh-security mesh-lfn-key rollover-ratio 180
```

Configure Mesh-key-exchange timeout:

By default, retry timer of LFN node is 10s during key exchange. Use the following commands to increase the key exchange timeout retry.

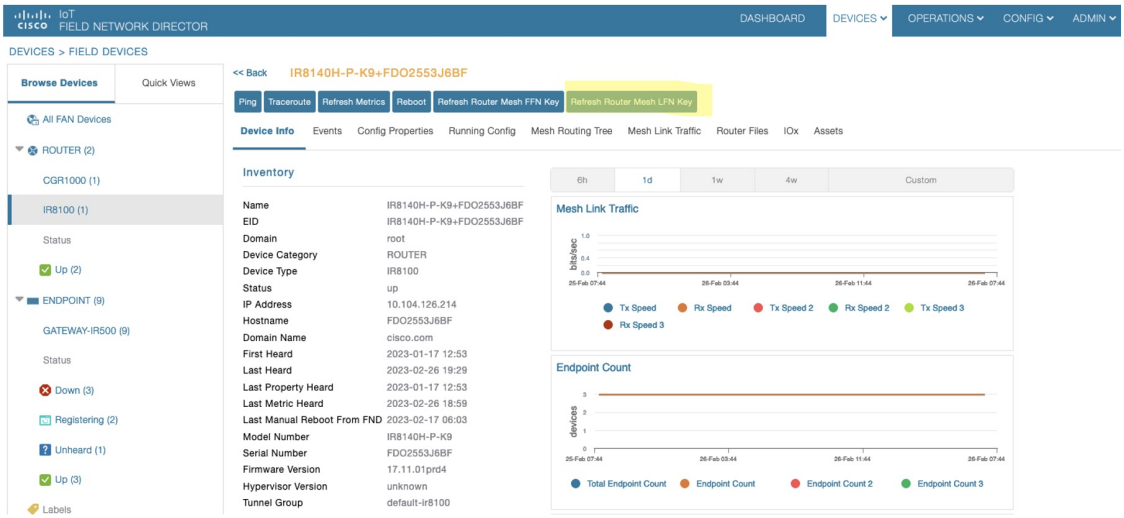
```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#mesh-security key-exchange-message-timeout 30
```

Configure Routing Lifetime for LFN:

LFN nodes are battery powered node. By default, the recommended Registration-lifetime is 24hrs. In Border Router, LFN needs to be maintained in routing table for 24hrs by using the following commands:

```
FDO2553J6BF(config)#interface wpan 0/1/0
FDO2553J6BF(config-if)#rpl dag-lifetime 60
FDO2553J6BF(config-if)#rpl dag-lifetime-unit 1440
```

Configuring Mesh Refresh Key for LFN from FND



Verifying the Configuration

To check the LFN version in Border Router:

```
FDO2553J6BF#show wpan 0/1/0 config | i LFN
LFN version: 8929 (2232)
FDO2553J6BF#
```

To check LFN broadcast interval:

```
FDO2553J6BF#show wpan 0/1/0 hardware config | i lfn
lfn_bcast:      interval 300000 sync-period 1
FDO2553J6BF#
```

Border router supports up to 3 keys for LFN. To check LFN Mesh-security Key:

```
FDO2553J6BF#show mesh-security keys lfn
```

```
FDO2553J6BF#show mesh-security keys lfn
Mesh Interface: WPAN0/1/0

LFN Pairwise Master Key Lifetime  : 540 Days 0 Hours 0 Minutes 0 Seconds
LFN Pairwise Temporal Key Lifetime: 360 Days 0 Hours 0 Minutes 0 Seconds
LFN Mesh Key Lifetime     : 90 Days 0 Hours 0 Minutes 0 Seconds

Rollover ratio: 180
Revocation reduction: 30

LFN Key ID     : 0 *
Key expiry     : Wed May 24 13:29:48 2023
Time remaining : 86 Days 12 Hours 36 Minutes 29 Seconds

LFN Key ID     : 1
Key expiry     : Tue Aug 22 13:29:48 2023
Time remaining : 176 Days 12 Hours 36 Minutes 29 Seconds

LFN Key ID     : 2
Key expiry     : Mon Nov 20 13:29:48 2023
Time remaining : 266 Days 12 Hours 36 Minutes 29 Seconds
```

Limitations

LFNs are battery powered nodes and work in their own unicast schedule. It is recommended to use long timeout values (180s) when trying to onboard LFN from Border Router.

IR8140H does not support direct parenting of LFN.

Direct Parenting of LFN Support in Wi-SUN Mesh Deployment

From Cisco IOS-XE Release 17.14.1, the IR8140 routers support direct parenting of Limited Function Nodes (LFNs) in Wi-SUN Mesh deployments. LFNs are the battery-powered low-energy endpoints typically used for utility metering of electricity, gas, and water. Several such LFN endpoints connect to a border router forming a sensor network to implement an Advanced Metering Infrastructure (AMI) deployment. LFN endpoints can connect to IR8140 as a child but cannot parent other devices in a Mesh network.

Previous releases supported IR8140 indirectly parenting LFNs through a partner Full Function Node (FFN) device. For more information, see Limited Function Node.

Use the following command to determine if the router has enabled LFN support:

```
IR8140#show wpan 0/2/0 hardware configuration
lfn support: Enabled
```

Use the following command to verify the node connected to the router is an LFN or FFN:

```
IR8140#show wpan 0/2/0 link-neighbors ns
------------------------ WPAN LINK NEIGHBOR TABLE WITH NS [2] -------------------------
EUI64            IPV6 address                              Lifetime   Last NS   Node Type
00173B05004D0030 2001:1111:1111:1111:55DC:BEF3:4D9C:FD87   240        15:29:08   LFN
Number of Entries in WPAN LINK NEIGHBOR TABLE: 1
Current time : 15:30:29
```

Verifying WPAN Configuration

Use WPAN show and debug commands to view WPAN configuration or troubleshoot operation.

To see all WPAN show commands, enter the following command:

```
Router# show wpan 0/1/0 ?
  config             Configuration information
  data-rate          Data rate during last 1 minute
  eap-table          Recent EAP node table
  hardware           Hardware information
  ieee154            IEEE 802.15.4 related information
  ieeep19012         IEEE P1901.2 related information
  link-neighbors     Layer 3 link neighbor information
  module-type        Module type (RF or PLC)
  oui-table          OUI mapping table for 8-to-6 MAC address translation
                     (EUI64 <-->IEEE MAC)
  outage-server      WPAN outage server
  outage-table       WPAN outage table
  packet-count       Packet counts
  restoration-table  WPAN restoration table
  rpl                RPL related information
  service-state      WPAN service state
  slave-mode         Slave mode
```

The following table describes some WPAN show commands and debug command.

Command	Description
show wpan config	Displays the WPAN basic configuration.
show wpan hardware	Displays WPAN hardware information. Enter **show wpan 0/1/0 hardware ?** to see a list of options. **Note** The output of the command **show wpan <slot >/1 hardware key** shows mesh-security keys (GTKs) that reside on the WPAN hardware. The **show wpan <slot>/1 hardware key** output should agree with the output of **show mesh-security-keys**. The **show wpan <slot>/1 hardware link-neighbor** command shows the list of recently heard IEEE 802.15.4 link neighbors. These link neighbors are RMEs within a 1-hop transmit range from the IR8100 and from which the IR8100 has recently heard IEEE 802.15.4 frames. The list shows only the most recently heard subset from all possible 1-hop neighbors.
show wpan packet-count	Displays incoming and outgoing packet counts for WPAN traffic.

Command	Description
show wpan link-neighbors	Shows the information about the WPAN link neighbors. These link neighbors are RMEs within a 1-hop transmit range from the IR8100 that sent at least one IPv6 or IEEE 802.1X packet to the CGR during the last hour. **Note** The minimum RSSI to join a mesh network is -95 dBm; a lower RSSIF/RRSIR value will not allow the node to establish connectivity.
show wpan outage-table	Shows recent power-outage notification (PON) events in the PAN during the past hour.
show wpan restoration-table	Shows recent power restoration notification (PRN) events in the PAN during the past hour.
show wpan rpl	Displays WPAN RPL information. Enter **show wpan 0/1/0 rpl ?** to see a list of options.
debug wpan all	Displays all WPAN debugging messages, including errors, fan-mpl, info, packets, and rpl.

Example IR8100 Basic WPAN Configuration

The following example is for a IR8100 with a basic WPAN configuration.

Note The **dwell** attribute indicates the maximum transmission time on a channel to comply with government regulations, most of which limit transmissions on a channel to *X* ms within *Y* ms (minimum and maximum duration). The **dwell** command allows you to set both *X* and *Y* . In the U.S., they are typically 400 ms to 20000 ms.

```
IR8140H #sh run
Building configuration...

Current configuration : 24773 bytes
!
! Last configuration change at 21:43:01 PST Sun Dec 6 2020 by iox
! NVRAM config last updated at 21:16:59 PST Fri Dec 4 2020 by iox
!
version 17.5
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
!
hostname IR8140H
!
boot-start-marker
```

```
boot system flash bootflash:ir8100-universalk9.BLD_POLARIS_DEV_LATEST_20201118_061101.SSA.bin
boot-end-marker
!
!
!
aaa new-model
!
!
aaa group server radius aaa-radius-group
 server name aaa-radius-server
!
aaa authentication login default local
aaa authentication dot1x default group aaa-radius-group
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
!
!
!
!
aaa session-id common
aaa password restriction
clock timezone PST -8 0
clock summer-time PDT recurring
!
!
!
!
!
!
!
!
!
!
login on-success log
ipv6 unicast-routing
ipv6 dhcp database flash:/DHCP-DB write-delay 60
ipv6 dhcp pool MeterNetwork
 prefix-delegation pool MeterNetwork lifetime 1814400 1360800
 address prefix AAAA:BBBB:CCCC:3::/112 lifetime 1814400 1360800
 vendor-specific 26484
  suboption 1 address 3000::4
  suboption 2 address 3000::5
!
ipv6 multicast-routing
!
!
!
!
!
!
!
subscriber templating
!
!
!
!
!
!
!
parameter-map type webauth global
 watch-list dynamic-expiry-timeout 0
!
```

```
multilink bundle-name authenticated
!
!
!
!
!
!
!
access-session mac-move deny
!
!
crypto pki trustpoint LDevID
 enrollment retry count 10
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number none
 fqdn none
 ip-address none
 password
 fingerprint 7107DAB5FBDAC555893B7C047D202B5676F6C9AB
 subject-name serialNumber=PID:IR8140H-P-K9 SN:FDO2420J79N,CN=IR8140H_FDO2420J79N
 revocation-check none
 rsakeypair LDevID 2048
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-138894244
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-138894244
 revocation-check none
 rsakeypair TP-self-signed-138894244
!
crypto pki trustpoint fnd
 enrollment url bootflash://PnP-cert_22_57_57_UTC_Thu_Dec_3_2020
 revocation-check none
!
crypto pki profile enrollment LDevID
 enrollment url  http://ca.iok.cisco.com/certsrv/mscep/mscep.dll
!
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = sit-dc-sit-dc-ca
!
crypto pki certificate chain LDevID
 certificate 5B00005E81DF0B79B1968437E1000000005E81
  308205B3 3082049B A0030201 0202135B 00005E81 DF0B79B1 968437E1 00000000
  5E81300D 06092A86 4886F70D 01010B05 00305F31 13301106 0A099226 8993F22C
  64011916 03636F6D 31153013 060A0992 268993F2 2C640119 16056369 73636F31
  16301406 0A099226 8993F22C 64011916 06736974 2D646331 19301706 03550403
  13107369 742D6463 2D534954 2D44432D 43413020 170D3230 31323033 32323531
  30385A18 0F323036 30313132 33323235 3130385A 30483128 30260603 55040513
  1F504944 3A495238 31343048 2D502D4B 3920534E 3A46444F 32343230 4A37394E
  311C301A 06035504 030C1349 52383134 30485F46 444F3234 32304A37 394E3082
  0122300D 06092A86 4886F70D 01010105 00038201 0F003082 010A0282 010100B0
  1C3E3320 97FF0E0F 583A7D41 8E7EA4E0 94CC6797 7CC99CEC 1742BBEE BD810E10
  EEE9B8BD F7AE212D AE17D1BD 40269478 1DB95762 7A157557 F1CFE31D 68A6FABE
  26E80E3E F98004DD 8AEA6DC6 95510EC1 96178014 8EB23D2A E35EF02A 820DDCE9
  4316EEE4 86830E86 09D64A02 1DDD26B4 7664378E 90EC8435 FAD9DC8A 269DF984
  91AB0047 029051A2 11BEBB8C 947700DD 48C32030 6CF19F6E 6218AD1F D06F611A
  57DA077C 45E97DEF 2441EC3F 6CD72D08 B2B34653 1901A30B 869792A7 6356A900
```

```
  E8C76625 AFE8318F 7728C40B 05D12D3D 4B56B553 A5CA6241 4B042ED4 259088C1
  7C9E7CAD 7708C4B7 89CD5973 20E5B17C A81F01DA 89553289 FCD88605 2E805102
  03010001 A382027B 30820277 300B0603 551D0F04 04030204 F0301D06 03551D0E
  04160414 A0895FE6 72E3C526 DC18D1AE 64A2E846 91B942A0 301F0603 551D2304
  18301680 1422A59D B25D909E DA074C00 39B59575 B3F8898F 533081D5 0603551D
  1F0481CD 3081CA30 81C7A081 C4A081C1 8681BE6C 6461703A 2F2F2F43 4E3D7369
  742D6463 2D534954 2D44432D 43412C43 4E3D7369 742D6463 2C434E3D 4344502C
  434E3D50 75626C69 63253230 4B657925 32305365 72766963 65732C43 4E3D5365
  72766963 65732C43 4E3D436F 6E666967 75726174 696F6E2C 44433D73 69742D64
  632C4443 3D636973 636F2C44 433D636F 6D3F6365 72746966 69636174 65526576
  6F636174 696F6E4C 6973743F 62617365 3F6F626A 65637443 6C617373 3D63524C
  44697374 72696275 74696F6E 506F696E 743081CA 06082B06 01050507 01010481
  BD3081BA 3081B706 082B0601 05050730 028681AA 6C646170 3A2F2F2F 434E3D73
  69742D64 632D5349 542D4443 2D43412C 434E3D41 49412C43 4E3D5075 626C6963
  2532304B 65792532 30536572 76696365 732C434E 3D536572 76696365 732C434E
  3D436F6E 66696775 72617469 6F6E2C44 433D7369 742D6463 2C44433D 63697363
  6F2C4443 3D636F6D 3F634143 65727469 66696361 74653F62 6173653F 6F626A65
  6374436C 6173733D 63657274 69666963 6174696F 6E417574 686F7269 7479303B
  06092B06 01040182 37150704 2E302C06 242B0601 04018237 15088593 BB6B8585
  8C6C8289 810E86C7 AC03E7EF 037D84B1 A57EB4FB 34020164 02010730 1D060355
  1D250416 30140608 2B060105 05070301 06082B06 01050507 03023027 06092B06
  01040182 37150A04 1A301830 0A06082B 06010505 07030130 0A06082B 06010505
  07030230 0D06092A 864886F7 0D01010B 05000382 010100AA F097FF39 BF324E9B
  9D469801 1EBA004A 0308BB2A 737576A7 F32F9323 F963233D 9431E83A 66E77B74
  B4F5D25B 6D746729 E38EF0FA D50A77C4 C37E9FD6 B45DED13 8600F7EE 91AD2D90
  B1361A82 E5C59706 B36FC8BE A6AD4949 EB58817F 8AEE3E63 91E0D7BF 1248AE8D
  3EEB0D41 47458C36 4B172593 81561D71 E4204D86 8E2E264C FBB74463 1CA8315A
  C5F98B8E 6FE4C2D5 84A0F922 3A3E5FE8 74405FEB 3E53AF71 A45D81B6 92FC66C1
  7A907EBC F28A497B 64FA458D 90A16A32 5370169B AC92EE7C 26B1BF0A 254F05CC
  2977143A DAE495D4 A53EC612 224745D2 2E74D281 AF8911C2 FC865C4A F5ACA85D
  6C3D6292 AB40CAB9 C4E5E536 2A1D0FC1 D20D8DE0 DF0CE0
        quit
 certificate ca 118989AFB1C4AD944B97A1CD898BD73B
  3082039B 30820283 A0030201 02021011 8989AFB1 C4AD944B 97A1CD89 8BD73B30
  0D06092A 864886F7 0D01010B 0500305F 31133011 060A0992 268993F2 2C640119
  1603636F 6D311530 13060A09 92268993 F22C6401 19160563 6973636F 31163014
  060A0992 268993F2 2C640119 16067369 742D6463 31193017 06035504 03131073
  69742D64 632D5349 542D4443 2D434130 20170D31 38303932 35313134 3735335A
  180F3230 36383039 32353131 35373533 5A305F31 13301106 0A099226 8993F22C
  64011916 03636F6D 31153013 060A0992 268993F2 2C640119 16056369 73636F31
  16301406 0A099226 8993F22C 64011916 06736974 2D646331 19301706 03550403
  13107369 742D6463 2D534954 2D44432D 43413082 0122300D 06092A86 4886F70D
  01010105 00038201 0F003082 010A0282 010100AF 6FB5E529 DEF701CD E5ACB737
  D2790873 875E9DBB 53ADAFC2 94C3D991 EC658A69 B1AB69BA C32307BE BF9D225D
  4FEADF33 F396AB70 A4E49526 AE637FE4 6BA0BB32 C98528D0 94658C48 DBE550A1
  ECA35F7A 4279F16C 5F3C2B11 185F95BB 9D68B2C9 82ECB523 BC3E5833 436BD1D1
  AE9616BD 1E0FC85D 67EF135B 6BC68840 3103DA89 923156FC EADD0914 3DD1F75E
  B166E550 A9F0FBEA 80DDE1F4 1B4D7789 3872EEA0 5B375344 03CDDFBA 72DC6F53
  6C3D25A3 BF8E215F 8D55C8D1 D0C279ED 9E061673 3FC6F225 6C405AA3 E6B96310
  4C2798A9 EC561A29 FF875907 B3527352 61A09CF2 D7916631 1F5215E5 6077E8C4
  A5042B6E 3039B222 BCFA1133 53FA51AD 2E972D02 03010001 A351304F 300B0603
  551D0F04 04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
  0E041604 1422A59D B25D909E DA074C00 39B59575 B3F8898F 53301006 092B0601
  04018237 15010403 02010030 0D06092A 864886F7 0D01010B 05000382 01010039
  6F03857F 8B5F0A38 E6DFA0E9 8598FE40 9231C4DF 5D747EA8 B968606B DD1593A8
  2348303C 7948DD69 1FDEA891 2A249CCC 9B9C9071 D51B1AC6 EF1567EF 64E8C11A
  85BDA86C AC45954E 7A86861C 1D7C622B 2211652C C8CC6359 09000B78 0E6ABF6E
  06D4247B 572E91B2 1216BC9A 5D715B8D E3220C4B 4B6B1B1A 3AA4B2CB 67F7F6B5
  2B3D9820 0E5A50A3 123E41F5 3C0D46E0 63E7212B 4730D9DA 4E0E8227 AEEAE386
  3C1A1B3A C680B486 5F71B0B5 80C82F6C 58126809 39193ABF D145BA7D 4D695762
  5DB055D4 077E779D AEA96655 576B3085 0CD9E01F 6805EF8B 494EE44B 16ACEED8
  F6529B1F AA324C9F 464FA153 9DAF12C1 74872179 1DA83009 26D36774 77C52F
        quit
crypto pki certificate chain SLA-TrustPoint
```

```
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
       quit
crypto pki certificate chain TP-self-signed-138894244
 certificate self-signed 01
  3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31333838 39343234 34301E17 0D323031 32303332 32353735
  305A170D 33303132 30333232 35373530 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3133 38383934
  32343430 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
  82010100 B6A01EE3 667B8D0E EF1BC93C 6F5925CA 9C4223CC 37FC5F61 53264E2D
  E5D89F9B A4B32F70 732C76F0 ECBABD98 B53EEBD3 6411EB5E F66F6C23 F6E20FE7
  2E2BA210 0E82D6D2 DC99670A 00A511D4 8006BD04 0ED4928C 0187028C 9513FA42
  61C41C4A D37D249E 7F331130 769CC58A C06AA7EB 48CCF781 C11549FF A2289F13
  CEBE4076 D58280A2 015689DA 4AC29732 5BB395B8 A3E94411 1EC943AC DA949659
  592FFEE6 1F40FE6C A9736E1A 1A4D7D4C 54B2DD87 AF20AAED 5D139637 F9816736
  2AC0E22A 86981E8C F56EBD49 0EA893E1 E3A14D59 4503EC8A B578A4F3 E8C6ADDA
  35B6324C 751F714A 874483DB 1974F177 753FC641 8CBB04FC 1C5BE284 1A637231
  B9E90233 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
  0603551D 23041830 1680146D 23D38934 824F75AC 853375D6 557CE3E4 5A252830
  1D060355 1D0E0416 04146D23 D3893482 4F75AC85 3375D655 7CE3E45A 2528300D
  06092A86 4886F70D 01010505 00038201 0100A685 7A44E9DD E4185176 742D91A8
  3FBC514C EA66F095 3D6202DB E730B178 99DB7C4E 9CA8F398 E9F9306A BCAFC0B1
  27458D65 72A202CE 55B42843 E71743EA 347EEBDD 10BDC71E 5840BEAC 627B25C1
  F7FDE729 7E1011F4 1A160803 CF1CED13 4AFB4402 CEAB7F5C A9E4C783 711062A3
  3F551D7F 58A847C9 C0C4D8BE 576DEFA1 A2383F74 BDF0ABEE 17FB784B 32DDFE16
  AEE23933 979A4C9E 2545114F 651206DD C668FA4C 2D54CCD7 87D22AE8 52D240F7
  8E5548B7 F411BE02 0DA89663 779794B0 90C4B69C 935E584B C9E945E7 40C17C69
  AC5E71AA 274C6363 7438F423 0C139869 68A399D6 97662323 E9543C9A A185B589
  F8977558 EEADBC59 F8C60924 E68E2BF7 3E69
       quit
crypto pki certificate chain fnd
 certificate ca 118989AFB1C4AD944B97A1CD898BD73B
  3082039B 30820283 A0030201 02021011 8989AFB1 C4AD944B 97A1CD89 8BD73B30
  0D06092A 864886F7 0D01010B 0500305F 31133011 060A0992 268993F2 2C640119
  1603636F 6D311530 13060A09 92268993 F22C6401 19160563 6973636F 31163014
  060A0992 268993F2 2C640119 16067369 742D6463 31193017 06035504 03131073
  69742D64 632D5349 542D4443 2D434130 20170D31 38303932 35313134 3735335A
```

```
  180F3230 36383039 32353131 35373533 5A305F31 13301106 0A099226 8993F22C
  64011916 03636F6D 31153013 060A0992 268993F2 2C640119 16056369 73636F31
  16301406 0A099226 8993F22C 64011916 06736974 2D646331 19301706 03550403
  13107369 742D6463 2D534954 2D44432D 43413082 0122300D 06092A86 4886F70D
  01010105 00038201 0F003082 010A0282 010100AF 6FB5E529 DEF701CD E5ACB737
  D2790873 875E9DBB 53ADAFC2 94C3D991 EC658A69 B1AB69BA C32307BE BF9D225D
  4FEADF33 F396AB70 A4E49526 AE637FE4 6BA0BB32 C98528D0 94658C48 DBE550A1
  ECA35F7A 4279F16C 5F3C2B11 185F95BB 9D68B2C9 82ECB523 BC3E5833 436BD1D1
  AE9616BD 1E0FC85D 67EF135B 6BC68840 3103DA89 923156FC EADD0914 3DD1F75E
  B166E550 A9F0FBEA 80DDE1F4 1B4D7789 3872EEA0 5B375344 03CDDFBA 72DC6F53
  6C3D25A3 BF8E215F 8D55C8D1 D0C279ED 9E061673 3FC6F225 6C405AA3 E6B96310
  4C2798A9 EC561A29 FF875907 B3527352 61A09CF2 D7916631 1F5215E5 6077E8C4
  A5042B6E 3039B222 BCFA1133 53FA51AD 2E972D02 03010001 A351304F 300B0603
  551D0F04 04030201 86300F06 03551D13 0101FF04 05300301 01FF301D 0603551D
  0E041604 1422A59D B25D909E DA074C00 39B59575 B3F8898F 53301006 092B0601
  04018237 15010403 02010030 0D06092A 864886F7 0D01010B 05000382 01010039
  6F03857F 8B5F0A38 E6DFA0E9 8598FE40 9231C4DF 5D747EA8 B968606B DD1593A8
  2348303C 7948DD69 1FDEA891 2A249CCC 9B9C9071 D51B1AC6 EF1567EF 64E8C11A
  85BDA86C AC45954E 7A86861C 1D7C622B 2211652C C8CC6359 09000B78 0E6ABF6E
  06D4247B 572E91B2 1216BC9A 5D715B8D E3220C4B 4B6B1B1A 3AA4B2CB 67F7F6B5
  2B3D9820 0E5A50A3 123E41F5 3C0D46E0 63E7212B 4730D9DA 4E0E8227 AEEAE386
  3C1A1B3A C680B486 5F71B0B5 80C82F6C 58126809 39193ABF D145BA7D 4D695762
  5DB055D4 077E779D AEA96655 576B3085 0CD9E01F 6805EF8B 494EE44B 16ACEED8
  F6529B1F AA324C9F 464FA153 9DAF12C1 74872179 1DA83009 26D36774 77C52F
        quit
!
!
!
!
!
!
!
!
!
no license feature hseck9
license udi pid IR8140H-P-K9 sn FDO2420J79N
license boot level network-advantage
archive
 path bootflash:/archive/fnd_
 maximum 8
memory free low-watermark processor 47508
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
service-template webauth-global-inactive
 inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
 linksec policy must-secure
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
 linksec policy should-secure
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
dot1x system-auth-control
!
username iox privilege 15 secret 8
$8$MCZ4.RbP0h3mhk$oD4slpuk7rxM8A1Q4sVfct5i.90A91bSQ.Z0BOXJghk
username admin privilege 15 secret 8
$8$EPbjkRKro7I9G.$XEDUTW4a7kSfE4Eg57AdaC9UqHxks/.mFHAZ44nFsPw
username cg-nms-administrator privilege 15 secret 8
$8$EvudyM9Ko4qx5E$1jwTxrgxTgzkH2pkGPHa9vvP/jBMHffknWiBn2dBYWk
!
redundancy
```

```
 mode none

!
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_IPv4_LAN
 route set access-list ipv6 FlexVPN_Client_IPv6_LAN
!
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 dpd 120 3 periodic
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
!
crypto ikev2 dpd 60 10 periodic
crypto ikev2 client flexvpn FlexVPN_Client
  peer 1 1001::3
  client connect Tunnel10
!
!
controller Cellular 0/2/0
!
!
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match result-type aaa-timeout
 match authorization-status authorized
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match result-type aaa-timeout
 match authorization-status unauthorized
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
!
```

```
!
policy-map type control subscriber POLICY_WP0/1/0
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  10 class always do-until-failure
   10 terminate dot1x
   20 authentication-restart 60
 event agent-found match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
!
!
!
!
!
!
!
!
crypto ipsec transform-set FlexVPN_IPsec_Transform_Set esp-aes esp-sha256-hmac
 mode tunnel
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set transform-set FlexVPN_IPsec_Transform_Set
 set pfs group14
 set ikev2-profile FlexVPN_IKEv2_Profile
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.10.34 255.255.255.255
 ipv6 address 2000::182B/128
!
interface Tunnel10
 description IPsec tunnel to CISCO-IOK-HER
 no ip address
 ipv6 unnumbered Loopback0
 ipv6 mtu 1362
 ipv6 tcp adjust-mss 1302
 ipv6 ospf 10 area 10
 tunnel source GigabitEthernet0/0/1
 tunnel mode gre ipv6
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
interface VirtualPortGroup0
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/0/0
 ip address dhcp
```

```
 negotiation auto
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd autoconfig default-route
 ipv6 nd ra suppress all
 ipv6 dhcp client request vendor
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface Cellular0/2/0
 ip address negotiated
 ipv6 enable
!
interface Cellular0/2/1
 no ip address
 shutdown
!
interface WPAN0/1/0
 wisun-mode
 ieee154 phy-mode 66
 ieee154 beacon-async min-interval 15 max-interval 60 suppression-coefficient 1
 ieee154 panid 12571
 ieee154 ssid sit-cabo
 ieee154 beacon-ver-incr-time 0
 rpl dag-lifetime 60
 rpl dio-min 14
 rpl version-incr-time 10
 ipv6 address AAAA:BBBB:CCCC:3::1/64
 ipv6 dhcp server MeterNetwork rapid-commit
 authentication host-mode multi-auth
 authentication port-control auto
 dot1x pae authenticator
!
router ospfv3 10
 !
 address-family ipv6 unicast
 exit-address-family
!
iox
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication aaa login-authentication default
ip http secure-server
ip http secure-client-auth
ip http secure-trustpoint LDevID
ip http max-connections 10
ip http timeout-policy idle 600 life 86400 requests 3
ip http client connection timeout 5
ip http client connection retry 5
ip http client connection forceclose
ip http client source-interface Loopback0
ip http client secure-trustpoint LDevID
ip forward-protocol nd
ip tftp source-interface GigabitEthernet0/0/1
ip ssh rsa keypair-name LDevID
ip ssh version 2
!
!
ip access-list standard FlexVPN_Client_IPv4_LAN
 10 permit 10.10.10.34
```

```
!
!
ip radius source-interface Loopback0
!
snmp-server group cgnms v3 priv
snmp-server community readonly RO
snmp-server community readwrite RW
snmp-server trap-source Loopback0
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps wpan
snmp-server enable traps cisco-sys heartbeat
snmp-server enable traps fru-ctrl
snmp-server enable traps aaa_server
snmp-server enable traps c3g
snmp-server host 3000::4 version 3 priv cg-nms-administrator
!
!
!
!
radius server aaa-radius-server
 address ipv6 3000::6 auth-port 1812 acct-port 1813
 key Cisco12345!
!
!
ipv6 access-list FlexVPN_Client_IPv6_LAN
 sequence 20 permit ipv6 host 2000::182B any
 sequence 30 permit ipv6 AAAA:BBBB:CCCC:2::/64 3000::/112
!
control-plane
!
!
mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 length 0
 transport preferred none
 stopbits 1
 speed 115200
line vty 0 4
 session-timeout 10
 exec-timeout 0 0
 length 0
 transport preferred none
 transport input all
line vty 5 15
 session-timeout 10
 exec-timeout 0 0
 privilege level 15
 length 0
 transport preferred none
 transport input all
!
call-home
```

```
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
ntp server ntp.iok.cisco.com
ntp server her.iok.cisco.com
!
wsma agent exec
 profile exec
!
wsma agent config
 profile config
!
!
!
!
wsma profile listener exec
 transport https path /wsma/exec
!
wsma profile listener config
 transport https path /wsma/config
!
cgna gzip
!
cgna heart-beat interval 1
cgna heart-beat active
!
cgna profile cg-nms-tunnel
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 interval 2
 url https://tps.iok.cisco.com:9120/cgna/ios/tunnel
 gzip
!
cgna profile cg-nms-register
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 interval 10
 url https://fnd.iok.cisco.com:9121/cgna/ios/registration
 gzip
!
cgna profile cg-nms-periodic
 add-command show version | format flash:/managed/odm/cg-nms.odm
 add-command show hosts | format flash:/managed/odm/cg-nms.odm
 add-command show interfaces | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
 add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
 add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
 add-command show inventory | format flash:/managed/odm/cg-nms.odm
 add-command show iox-service | format flash:/managed/odm/cg-nms.odm
 add-command show wpan 0/1/0 hardware version | format flash:/managed/odm/cg-nms.odm
 add-command show wpan 0/1/0 rpl brief | format flash:/managed/odm/cg-nms.odm
```

```
 add-command show wpan 0/1/0 conf | format flash:/managed/odm/cg-nms.odm
 add-command show wpan 0/1/0 packet-count | format flash:/managed/odm/cg-nms.odm
 add-command show cellular 0/2/0 all | format flash:/managed/odm/cg-nms.odm
 interval 1
 url https://fnd.iok.cisco.com:9121/cgna/ios/metrics
 gzip
 active
!
!
cgna exec-profile CGNA-default-exec-profile
 add-command cgna exec profile cg-nms-register
 interval 1
 exec-count 1
!
!
event manager environment ZTD_SCEP_CGNA_Profile cg-nms-tunnel
event manager environment ZTD_SCEP_LDevID_trustpoint_name LDevID
event manager environment ZTD_SCEP_Period 180
event manager directory user policy "tmpsys:/eem_policy"
event manager policy no_config_replace.tcl type system authorization bypass
event manager policy tm_ztd_scep.tcl type system authorization bypass
!
app-hosting appid sparrow_iperf_app_1
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.0.2 netmask 255.255.255.0
 app-default-gateway 192.168.0.1 guest-interface 0
gnxi
gnxi server
netconf-yang
end
```

Example IR8100 Configuration for CG-Mesh

The following example shows the configuration for an IR8100 in a Cisco Resilient Mesh network.

```
IR8100#sh run
Building configuration...

Current configuration : 9107 bytes
!
! Last configuration change at 16:53:48 CST Tue Feb 16 2021 by cisc0
!
version 17.5
service timestamps debug datetime msec localtime show-timezone year
service timestamps log datetime msec
service call-home
service unsupported-transceiver
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
platform shell
!
hostname IR8100
!
boot-start-marker
boot system
flash:ir8100-universalk9.BLD_V175_THROTTLE_LATEST_20210207_015223_V17_5_0_161.SSA.bin
boot-end-marker
!
!
logging buffered 1000000
no logging console
enable password cisc0
```

```
!
aaa new-model
!
!
aaa group server radius CGCDN
server name wisun_radius
!
aaa authentication login default local
aaa authentication dot1x default group CGCDN
aaa authorization exec default local
!
aaa common-criteria policy iiot_policy
min-length 10
max-length 127
numeric-count 1
upper-case 1
lower-case 1
char-changes 4
!
!
aaa session-id common
clock timezone CST 8 0
!
!
login on-success log
no ipv6 address-validate
ipv6 unicast-routing
ipv6 dhcp pool dhcp-node
address prefix 2001:CABB::/64 lifetime 60000 36000
vendor-specific 26484
suboption 1 address 2060:FACD::50
suboption 2 address 2060:FACD::50
!
ipv6 multicast-routing
!
!
subscriber templating
!
!
multilink bundle-name authenticated
!
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint TP-self-signed-3764981121
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3764981121
revocation-check none
rsakeypair TP-self-signed-3764981121
!
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
```

```
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
crypto pki certificate chain TP-self-signed-3764981121
certificate self-signed 01
30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 33373634 39383131 3231301E 170D3230 31313130 30373239
31385A17 0D333031 31313030 37323931 385A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 37363439
38313132 31308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201
0A028201 0100E821 301D5675 0B3BA0B8 81273D9F B82581E9 9BACAE41 D501A5E9
A8E98EFB 2C25B7C9 A0E0CF17 C39FEBBA E673C855 BDA9379C BDDC68DC 377C2589
21CD8189 6AC98A97 9B5FA5D5 17E51A1F 3DB8BC88 1A844B1E EE69DA60 8D84620A
8A023D87 D93F3ADF 75D99D81 E06BCEF6 AC7C3A2E D70C79F1 C7E8E893 F08BE954
E0184F0D 0E0112BD 497C87E8 5E4788C4 ACF56F92 9134B85B 7D08F6BA 703CF11B
BC8E1377 DC0450E0 A9939952 90F1D84F F235BB5B D54517E9 B636D334 5569278A
3A629DC7 03CC08FF F067EE3F 0EADFAC0 A03C650C A2253E4C 13DD8910 E9726929
9ACD8403 CD16D710 6D5F1FA5 F7F0E310 9060340C 3309446B 99DC10E2 25908D03
D3FBA3E3 54D70203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF
301F0603 551D2304 18301680 14C73ACD 622756FB EB532701 66D605BC 49F9FFF2
BE301D06 03551D0E 04160414 C73ACD62 2756FBEB 53270166 D605BC49 F9FFF2BE
300D0609 2A864886 F70D0101 05050003 82010100 DC4AC08A D11E0E05 239FEBCB
694CC50F E0712807 A52F5714 C1501C4A A8283929 23F00BD1 B6F5310E 917C7501
B585E8AE 4CC88BE4 ED5555BF F46F2917 621577D6 6E14E796 B9A24FC7 3191F259
D61C6718 05E2FCB6 443E5D34 CBB90C02 3066F77C 3E3361E0 F975FB8E C026F652
DF2F3B2F FBBF0ABF 6600FD3D 9DB94163 330239C0 3F948CB1 30CEA1EE 3730FDA1
83A37AD9 940D8240 3B5A6D11 2601E91B 401CAB81 7FCC7C6E F3C48F19 B225FBCE
02523D36 8EAA3D42 3C232231 138F8EB0 BD3FF413 5FB879BE 5511A0D2 5953DB50
06E5CC26 082013B8 39D83819 EAA03533 B242A46C 679BE60F 0D9ED9BD 20D03F09
71159FAC 4DFD2DA8 71C5A1DD 94397BA5 6D2CEB0B
quit
!
!
no license feature hseck9
license udi pid IR8140H-P-K9 sn FDO2438J7BK
memory free low-watermark processor 47507
!
diagnostic bootup level minimal
!
spanning-tree extend system-id
dot1x system-auth-control
!
username cisc0 password 0 cisc0
!
redundancy
mode none
!
!
```

```
interface Loopback1
no ip address
ipv6 address 4008::8/128
!
interface GigabitEthernet0/0/0
ip address 10.79.56.221 255.255.255.0
negotiation auto
ipv6 address 2060:FACD::221/64
ipv6 enable
!
interface GigabitEthernet0/0/1
ip address 192.168.254.101 255.255.255.0
load-interval 30
negotiation auto
ipv6 address 2111:ABCD::111/64
ipv6 enable
ipv6 nd ra suppress
ipv6 ospf 1 area 0
!
interface WPAN0/1/0
no ip address
wisun-mode
ieee154 beacon-async min-interval 15 max-interval 60 suppression-coefficient 1
ieee154 dwell window 12400 max-dwell 400
ieee154 notch 10-20
ieee154 panid 15294
ieee154 ssid regression
ieee154 beacon-ver-incr-time 0
rpl dag-lifetime 60
rpl dio-dbl 1
rpl dio-min 14
rpl version-incr-time 10
ipv6 address 2001:CABB::1/64
ipv6 enable
ipv6 mld join-group FF38:40:2001:CABB::1
ipv6 dhcp server dhcp-node rapid-commit
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
!
no ip http server
ip http auth-retry 3 time-window 1
ip http authentication local
ip http secure-server
ip forward-protocol nd
ip tftp blocksize 8192
ip route 10.0.0.0 255.0.0.0 10.79.56.254
ip route 10.79.0.0 255.255.0.0 10.79.56.254
!
!
ipv6 route 2001:DB8:6:D6FF::/64 2111:ABCD::200
ipv6 route 2001:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 route 2015:ABCD::/64 2111:ABCD::200
ipv6 route 3001:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 route 3002:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 route 3002:ABCD::/64 2111:ABCD::200
ipv6 route 9001:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 route 9002:DB8:7:D7FF::/64 2111:ABCD::200
ipv6 router ospf 1
redistribute rpl
!

tftp-server bootflash:cg-mesh-bridge-6.4weekly-6404-ir510-8546385.bin
!
```

```
!
radius server wisun_radius
address ipv4 10.79.42.79 auth-port 1812 acct-port 1813
key Wi-SUN_radius
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
transport preferred none
stopbits 1
speed 115200
line vty 0 4
exec-timeout 0 0
password cisc0
transport input telnet
line vty 5 15
exec-timeout 0 0
password cisc0
transport input telnet
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
ntp server 171.68.38.66
ntp server 10.64.58.51
!
end
```

Example ASR Configuration for CG-Mesh

The following example shows the configuration for an ASR in a Cisco Resilient Mesh network.

```
SOL-ASR-7# show run brief
Building configuration...
Current configuration : 5512 bytes
!
! Last configuration change at 10:38:26 PST Fri May 16 2014 by admin
! NVRAM config last updated at 13:44:36 PST Thu May 15 2014 by admin
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime localtime
no platform punt-keepalive disable-kernel-core
!
hostname SOL-ASR-7
!
boot-start-marker
boot system flash:asr1000rp1-adventerprisek9.03.11.00.S.154-1.S-std.bin
boot-end-marker
!
aqm-register-fnf
!
vrf definition Mgmt-intf
 !
```

```
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
no logging console
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization network FlexVPN_Author local
!
!
!
!
!
aaa session-id common
clock timezone PST -8 0
!
!
!
!
!
!
!
no ip domain lookup
ip domain name ipv6lab.com
!
!
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
crypto pki trustpoint LDevID
 enrollment retry count 10
 enrollment retry period 2
 enrollment mode ra
 enrollment profile LDevID
 serial-number
 ip-address none
 password
 fingerprint F23314787BD98B99AF1FE0B2D338961D125EAE51
 revocation-check none
 rsakeypair LDevID
```

```
!
crypto pki profile enrollment LDevID
 enrollment url  http://192.168.100.120/certsrv/mscep/mscep.dll
!
!
!
crypto pki certificate map FlexVPN_Cert_Map 1
 issuer-name co cn = ipv6lab-sol-radius1-ca
!
crypto pki certificate chain LDevID
 certificate 4B88014800010000000FC
 certificate ca 2539E6B5CFF2FB894AC90A73EA69A645
spanning-tree extend system-id
!
username admin privilege 15 password 0 cisco
!
redundancy
 mode none
!
crypto ikev2 authorization policy FlexVPN_Author_Policy
 route set interface
 route set access-list FlexVPN_Client_Default_IPv4_Route
 route set access-list ipv6 FlexVPN_Client_Default_IPv6_Route
!
crypto ikev2 redirect gateway init
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-128
 integrity sha1
 group 5
!
crypto ikev2 policy FLexVPN_IKEv2_Policy
 proposal FlexVPN_IKEv2_Proposal
!
!
crypto ikev2 profile FlexVPN_IKEv2_Profile
 match certificate FlexVPN_Cert_Map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint LDevID
 aaa authorization group cert list FlexVPN_Author FlexVPN_Author_Policy
 virtual-template 1
!
!
crypto ikev2 cluster
 port 2000
 standby-group group1
 slave priority 90
 slave max-session 10
 no shutdown
!
!
cdp run
!
ip tftp source-interface GigabitEthernet0/0/3
ip ssh version 2
!
!
!
!
!
!
!
!
```

```
crypto ipsec transform-set AES_128_SHA1 esp-aes esp-sha-hmac
 mode transport
!
crypto ipsec profile FlexVPN_IPsec_Profile
 set transform-set AES_128_SHA1
 set ikev2-profile FlexVPN_IKEv2_Profile
 responder-only
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 20.0.0.3 255.255.0.0
 ipv6 address 2003:20::1/128
 ipv6 address 2333::1/64
 ipv6 enable
 ipv6 ospf 1 area 1
!
interface GigabitEthernet0/0/0
 ip address 173.36.248.224 255.255.255.192
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/0/1
 ip address 10.0.2.70 255.255.255.0
 ip pim sparse-mode
 negotiation auto
 ipv6 address 2001:A02::A00:246/64
 ipv6 enable
 ipv6 ospf 1 area 1
 ipv6 ospf mtu-ignore
 cdp enable
!
interface GigabitEthernet0/0/2
 ip address 11.0.0.70 255.255.255.0
 standby 1 ip 11.0.0.100
 standby 1 priority 110
 standby 1 name group1
 negotiation auto
 ipv6 enable
 cdp enable
!
interface GigabitEthernet0/0/3
 ip address 11.0.1.70 255.255.255.0
 negotiation auto
 cdp enable
!
interface GigabitEthernet0/1/0
 description WIMAX-BASESTATION
 ip address 192.10.0.88 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0/1/1
 no ip address
 ip pim sparse-mode
 negotiation auto
 ipv6 address 2010:DEAD:BEEF:CAFE::1/64
 ipv6 enable
 ipv6 ospf 1 area 1
 ipv6 ospf mtu-ignore
```

```
!
interface GigabitEthernet0/1/2
 no ip address
 ip pim sparse-mode
 negotiation auto
 ipv6 address 2011:DEAD:BEEF:CAFE::1/64
 ipv6 enable
 ipv6 ospf 1 area 1
 ipv6 ospf mtu-ignore
!
interface GigabitEthernet0/1/3
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 no ip address
 shutdown
 negotiation auto
!
interface Virtual-Template1 type tunnel
 description ip pim sparse-mode
 ip unnumbered Loopback0
 ipv6 address autoconfig
 ipv6 unnumbered Loopback0
 ipv6 enable
 ipv6 ospf 1 area 1
 ipv6 ospf mtu-ignore
 tunnel protection ipsec profile FlexVPN_IPsec_Profile
!
router ospf 1
 redistribute static subnets
 network 10.0.2.0 0.0.0.255 area 1
 network 11.0.0.0 0.0.0.255 area 1
 network 11.0.1.0 0.0.0.255 area 1
 network 173.36.0.0 0.0.255.255 area 1
 network 192.10.0.0 0.0.0.255 area 1
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 10.0.0.0 255.255.255.0 173.36.248.193
!
ip access-list standard FlexVPN_Client_Default_IPv4_Route
 permit any
!
ipv6 route 2005:DEAD:BEEF:CAFE::/64 2001:420:7BF:7E8::1
ipv6 route 2006:DEAD:BEEF:CAFE::/64 2001:420:7BF:7E8::B
ipv6 local pool IPV6_POOL 2001:10::/64 64
ipv6 pim rp-address 2333::1
ipv6 router ospf 1
 redistribute static
!
!
!
!
!
```

```
!
ipv6 access-list FlexVPN_Client_Default_IPv6_Route
 permit ipv6 any any
!
control-plane
!
 !
 !
 !
 !
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 privilege level 15
 transport input all
 transport output all
!
ntp server 192.168.100.250
netconf max-sessions 16
netconf ssh
!
end
SOL-ASR-7#
```

Checking and Upgrading the WPAN Firmware Version

This section describes how to check the WPAN hardware and firmware versions and perform firmware upgrades. For the IR8100, only IRMH WPAN is supported and the minimum version is 6.2.19.

Note WPAN firmware is not integrated in IR8100 firmware and must be upgraded separately.

To check the version of the WPAN hardware in slot 1, run the following command:

```
Router# sh wpan 0/1/0 hardware hwversion
hardware version: CGM-WPAN, 1.0, IRMH-WPAN/1.0/2.0
```

To check the installed firmware version of the WPAN, run the following command:

```
Router# sh wpan 0/1/0 hardware version
firmware version: 6.2RC(6.2.20), cg-mesh-bridge, origin/master-6.2, 6dd02f0, Jul 22 2020
```

The **show wpan <slot>/1 config** command also displays the WPAN firmware version:

```
Router# show wpan 0/1/0 config
module type:    RF-WPAN (IEEE 802.15.4e/g RF 900MHz)
.
.
.
firmware version:      6.2RC(6.2.20)
```

Upgrading WPAN Firmware

The appropriate WPAN firmware image must be copied and available on the IR8100 flash in the root directory.

To upgrade the WPAN firmware, follow these steps:

Procedure

Step 1 Install the firmware:

Example:

```
Router(config-if)# install-firmware image
Firmware upgrade starting. This may take several minutes. Please do not interrupt.
.....................
Installed the WPAN 6.0 firmware successfully (94 sec).
Please reload the WPAN module in slot 1!!
```

Step 2 Power down the WPAN module:

Example:

```
Router# config t
Router(config)# hw-module subslot 0/1 shutdown unpowered
```

Step 3 Wait for WPAN power-down messages, and then wait another 60-90 seconds. Then, power up the module:

Example:

```
Router(config)# no hw-module subslot 0/1 shutdown unpowered
```

Step 4 Wait for WPAN power-up messages, and then wait at least 500 seconds before proceeding with any task on a WPAN under reload. Then, check WPAN status and hardware version:

Example:

```
Router# show ip interface brief | inc Wpan
  Wpan0/10                   unassigned      YES unset  up                    up
Router# show wpan 0/1/0 hardware version
firmware version: 6.2RC(6.2.20), cg-mesh-bridge, origin/master-6.2, 6dd02f0, Jul 22 2020
```

Upgrading WPAN Firmware (CG-Mesh to WiSUN)

Follow these steps to upgrade the WPAN firmware from 6.2 to 6.3, which upgrades the WPAN module from cgmesh mode to wisun mode.

Procedure

Step 1 Install the firmware:

Example:

```
Router(config-if)# install-firmware image
Firmware upgrade starting. This may take several minutes. Please do not interrupt.
.....................
```

```
Installed the WPAN 6.3 firmware successfully (94 sec).
Please reload the WPAN module in slot 1!!
```

Step 2 Enter configuration mode:

Example:

```
Router#configure terminal
```

Step 3 Specify the WPAN interface and enter interface configuration mode:

Example:

```
Router(config)#interface wpan 0/1/0
```

Step 4 Enable wi-sun mode:

Example:

```
Router(config-if)#wisun-mode
```

Step 5 Set the beacon version increase interval to 0:

Example:

```
Router(config-if)#ieee154 beacon-ver-incr-time 0
```

Step 6 Set the phy mode to wisun supported phy mode:

Example:

```
Router(config-if)#ieee154 phy-mode 66
```

Step 7 Exit interface configuration mode and return to privileged EXEC mode:

Example:

```
Router(config-if)#end
```

Step 8 Power down the WPAN module:

Example:

```
Router# config t
Router(config)# hw-module subslot 0/1 shutdown unpowered
```

Step 9 Wait for WPAN power-down messages, and then wait another 60-90 seconds. Then, power up the module:

Example:

```
Router(config)# no hw-module subslot 0/1 shutdown unpowered
```

Step 10 Wait for WPAN power-up messages, and then wait at least 500 seconds before proceeding with any task on a WPAN under reload. Then, check WPAN status and hardware version:

Example:

```
Router# show ip interface brief | inc Wpan
  Wpan0/1/0                  unassigned      YES unset  up                    up
Router# show wpan 0/1/0 hardware version
firmware version: 6.2RC(6.2.20), cg-mesh-bridge, origin/master-6.2, 6dd02f0, Jul 22 2020
```