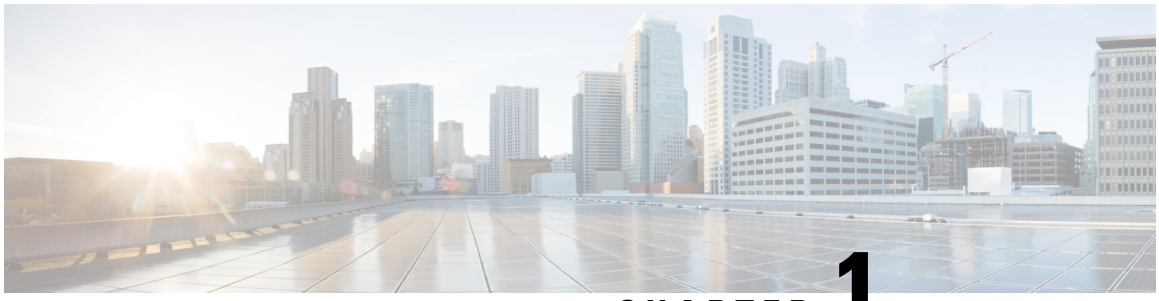
Cisco Catalyst SD-WAN Rugged Series Router Configuration Guide, Releases 26.x and Later

First Published: 2026-04-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Read Me First

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

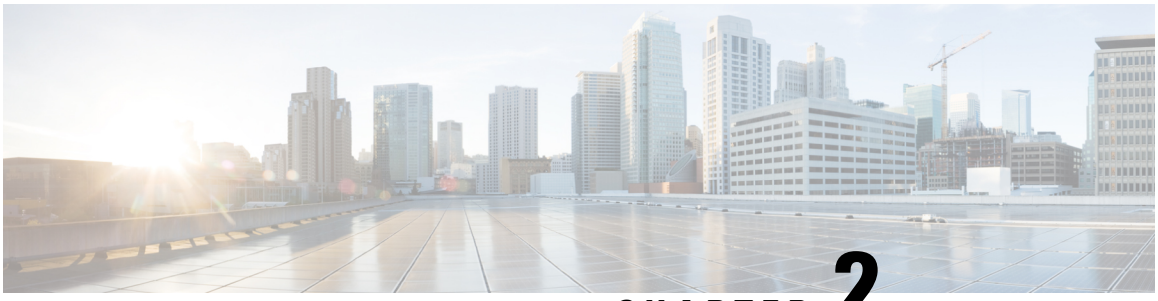
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

What's New in Cisco IOS XE (SD-WAN) and Cisco Catalyst SD-WAN Releases

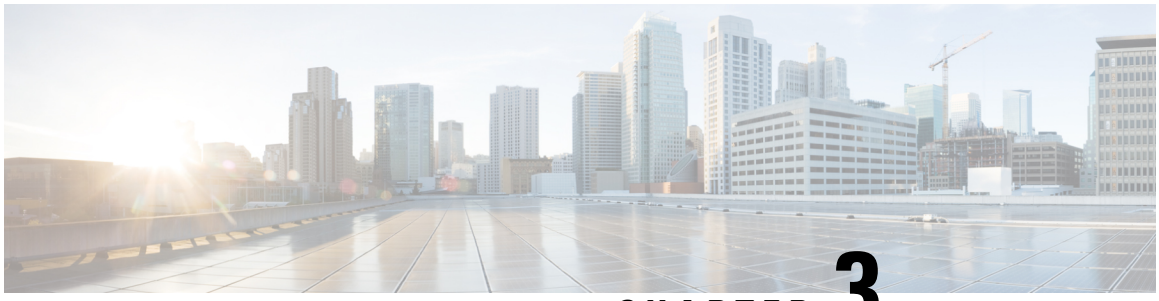
Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following links includes release-wise new and modified features that are documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x

What's New in Cisco IOS XE Catalyst SD-WAN Release 16.x

What's New in Cisco SD-WAN (vEdge) Release 20.x

What's New in Cisco SD-WAN (vEdge) Release 19.x



CHAPTER 3

Ignition Power Management

Ignition Power Management

Table 1: Feature History

Feature Name	Release Information	Description
Ignition Power Management	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	Ignition power management prevents a router from draining the charge of a vehicle battery in automotive applications.
Ignition power management: configuration group support and real-time monitoring	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Configure and monitor ignition power and sensing capabilities of IR1800 routers using Cisco SD-WAN Manager. It prevents the router from draining a vehicle's battery and keeps the router running when the vehicle is stopped, eliminating reload times each time the vehicle restarts.

Information About Ignition Power Management

When a router is installed in a vehicle and is powered by the electrical system of the vehicle, ignition power management prevents the router from draining the charge of the vehicle battery. When the vehicle engine is running, and charging the battery, the router remains operational. When the vehicle ignition is turned off, the router shuts down. You can configure a time interval to delay shutting down the router immediately.

For information about ignition power management, including feature limitations, see Ignition Power Management Overview in the *Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide*.

Supported devices for ignition power management

Cisco IR1800 router

Use Cases for Ignition Power Management

For a fleet of vehicles with Cisco IR1835 routers installed to provide network connectivity to each vehicle, you can configure the routers to sense the ignition status of the vehicle. The routers can start when the vehicle engine is running, and shut down shortly after the vehicle ignition is turned off. This ensures that the routers are operational and providing connectivity when the vehicles are in use, and not using power when the fleet vehicles are not in use.

Configure ignition power management using a configuration group

Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create and configure an ignition power management feature in a System profile.

Table 2: Ignition Power Management

Field	Description
Name	Name for the ignition power management configuration.
Description	Description for the ignition power management configuration.
Enable	Enable or disable ignition power management.

Field	Description
Ignition Sense Enable	When ignition sense is enabled, it monitors the power supply voltage to detect whether ignition is on or off based on the configured thresholds. When ignition sense is disabled (on IR1835), it uses the ignition signal pin to detect whether ignition is on or off. **Note** Disabling ignition sense is supported only on IR 1835 routers.
Battery Type	Type of battery used.
Shutdown Timer	Timer (seconds) to delay shutdown after ignition is turned off.
Under voltage Threshold	Minimum voltage (in millivolts) for the device to operate before triggering an undervoltage event.
Sense voltage Threshold	Voltage threshold (in millivolts) for the device to sense ignition status. **Note** If the newly configured value is higher than the current input voltage, the router will shut down.

What to do next

Also see Deploy a configuration group.

Enable Ignition Power Management Using a CLI Template

1. Enable ignition power management, which enables the router to detect whether a vehicle ignition is on or off.

   ```
   ignition enable
   ignition sense
   ```

Note To disable ignition power management, configure **no ignition enable** and **no ignition sense**.

2. Configure the battery type as 12 V or 24 V. The default is 12 V.

   ignition *battery-type* {**12v** | **24v**}

3. (Optional) Configure an off-timer delay, to delay router shutdown after the ignition status changes to off. The range is 120 to 32,400 seconds, and the default is 300 seconds. Note that the device shutdown process begins approximately 100 seconds before the configured off-timer value.

   ignition off-timer *seconds*

4. (Optional) Configure the undervoltage parameter to trigger system shutdown if the voltage drops below a specific threshold. Configure the volts and millivolts as two separate inputs. The range of volts is 9 to 24, and the range of millivolts is 0 and 999. The default is 9.000 V.

   ignition undervoltage threshold *volts millivolts*

Here is a complete sample configuration, which configures a battery type of 12 V, an ignition off-timer of 300 seconds, and an undervoltage of 9 V (shown as 9 V and 0 millivolts)

```
ignition enable
ignition sense
ignition battery-type 12v
ignition off-timer 300
ignition undervoltage threshold 9 0
```

Monitor Ignition Power Management

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Select a supported IR1800 device.

Step 3 Click **Real Time** in the left pane.

Step 4 From the **Device Options** drop-down list, select **Ignition Power Management**.

Verify the Ignition Power Management Configuration

show running-config

On the device, use the **show running-config** command, filtering for ignition, to show the ignition power management configuration.

The following example is for a 12 V battery. Note that configuring the battery type as 12 V configures the sense-voltage threshold automatically to 13,000 mV.

```
Device#show running-config | section ignition
ignition off-timer 300
ignition undervoltage threshold 9 000
ignition battery-type 12v
ignition sense-voltage threshold 13 000
ignition sense
ignition enable
```

The following example is for a 24 V battery. Note that configuring the battery type as 24 V configures the sense-voltage threshold automatically to 26,000 mV.

```
Device#show running-config | section ignition
ignition off-timer 300
ignition undervoltage threshold 9 000
ignition battery-type 24v
ignition sense-voltage threshold 26 000
ignition sense
ignition enable
```

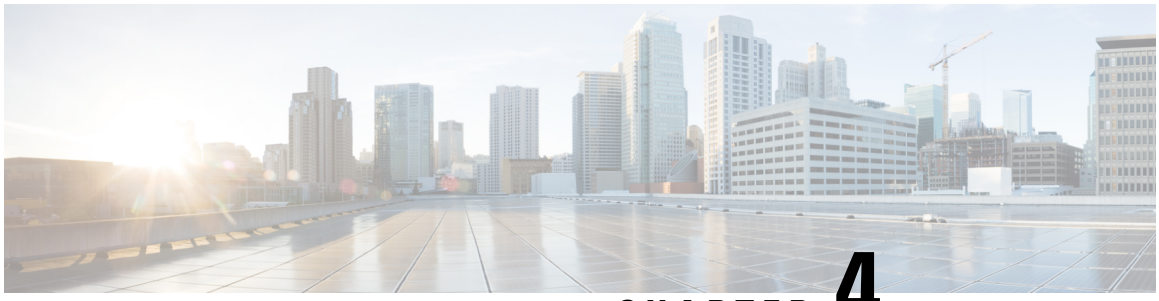
show ignition

On the device, use the **show ignition** command to show ignition power management configuration information.

- Configuring the battery type to 12 V configures the sense on value to 13.2 V and sense off to 12.8 V, and this appears in the **show ignition** output.
- Configuring the battery type to 24 V configures the sense on value to 26.2 V and sense off to 25.8 V, and this appears in the **show ignition** output.

The following example is for a 12 V battery:

```
Device#show ignition
Status:
Ignition management: Disabled
Input voltage: 17.672 V
Ignition status: Power on
Ignition Sense: Disabled
Shutdown timer: 0.0 s to off [will begin power down at ~100 sec]
Config-ed battery: 12v
Thresholds:
Undervoltage: 9.000 V
Overvoltage: 37.000 V
Sense on: 13.200 V
Sense off: 12.800 V
Undervoltage timer: 20.0 s
Overvoltage timer: 1.0 s
Ignition-Off timer: 300.0 s
```



CHAPTER 4

Digital IO

Digital IO

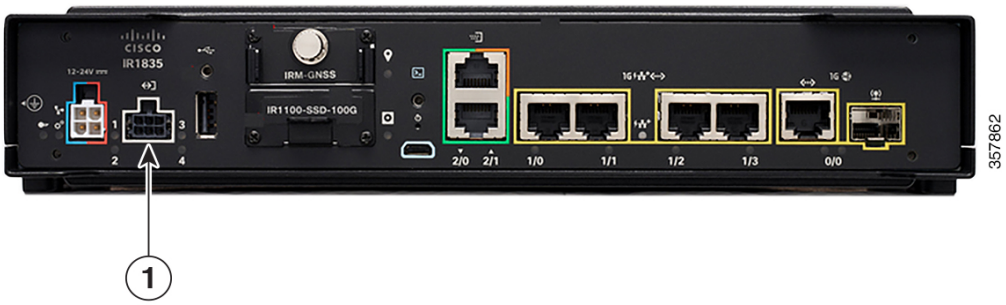
Table 3: Feature History

Feature Name	Release Information	Description
Digital IO	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	The Cisco IR1835 supports four general-purpose input/output (GPIO) ports. You can configure a GPIO port as an input or an output alarm.

Information About Digital IO

The Cisco IR1835 supports four general-purpose input/output (GPIO) ports, also called digital IO (or I/O) ports. You can configure contacts in the digital IO port to receive digital sensor input or provide digital output. For example, sensors might provide information about the environment in which the router is installed, and the digital output might trigger an external alarm or other notification device, or a type of actuator. Because the digital output for this feature is often used to trigger an external alarm, descriptions of this feature often use the alarm terminology. Each contact in the port can operate as a dry or wet contact. The contacts are protected up to +60 V.

Figure 1: Digital IO Port on a Cisco IR1835 Router



Digital IO is similar to the alarm in and alarm out features supported on Cisco Industrial Ethernet (IE) Series switches and Cisco Industrial Router (IR) Series routers. The differences are that the alarm in is a dedicated input and the alarm out is a dedicated output, whereas the digital IO ports can be used for input or output. alarm out includes a relay to provide normally open (NO) or normally closed (NC) terminals.

For more information, including digital IO limitations, see Digital IO in the *Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide*.

Supported Devices

Cisco IR1835 router

Use Cases for Digital IO

In one use case, a Cisco IR1835 router is installed in an outdoor utility cabinet exposed to weather conditions. Using the digital IO port, you can connect sensors to the router that indicate the heat and humidity in the cabinet, and indicate whether the cabinet is properly closed. Using these sensor inputs, you can configure an alarm state triggered by excessive heat or humidity, or when the cabinet is not properly closed.

The alarm state can trigger sending a message to a central location to enable you to take appropriate action if the utility cabinet conditions require attention.

Enable Digital IO Using a CLI Template

1. Enable digital IO, such as to trigger an alarm, on a contact. For *contact-number*, the range is 1 to 4.

   alarm contact *contact-number* **enable**

2. Configure the alarm severity value. The default is minor. For *contact-number*, the range is 1 to 4.

   alarm contact *contact-number* **severity** {**none** | **minor** | **major** | **critical**}

3. Configure the alarm threshold, in the range of 1,600 to 2,700 mV. The default is 1,600 mV. For *contact-number*, the range is 1 to 4.

   alarm contact *contact-number* **threshold** *threshold*

4. Configure the alarm trigger mode. The default is closed, meaning that the digital input is triggered if the circuit connected to the contact is closed, providing current. This may be used to trigger an alarm. For *contact-number*, the range is 1 to 4.

   alarm contact *contact-number* **trigger** {**open** | **closed**}

5. For a particular contact, configure the router to provide power for an IO circuit (using the **wet** option) or not provide power (using the **dry** option). The default is **dry**. For *contact-number*, the range is 1 to 4.

   alarm contact *contact-number* **application** {**dry** | **wet**}

6. Configure a contact to be in output mode, and configure whether the router provides current on the contact. Use **1** for high (provide current) or **0** for low (do not provide current). The choice of high or low for a digital IO output depends on the digital IO circuitry that the router is communicating with, and is beyond the scope of this documentation. For *contact-number*, the range is 1 to 4.

   If you configure a contact to be in output mode, then for that contact, do not use any of the commands relevant only to input, such as **severity**, **threshold**, **trigger**, or **application**.

   alarm contact *contact-number* **output** {**0** | **1**}

7. Configure a description for the digital IO handled by a particular contact. The description string can be up to 80 alphanumeric characters long. The description is included in system messages that relate to the contact number. For *contact-number*, the range is 1 to 4.

   alarm contact *contact-number* **description** *descriptive-text*

Here is a complete configuration example that enables contact 1 in input mode and configures the input parameters:

```
alarm contact 1 enable
alarm contact 1 severity minor
alarm contact 1 threshold 1600
alarm contact 1 trigger closed
alarm contact 1 application dry
alarm contact 1 description "Sensor indicating enclosure open"
```

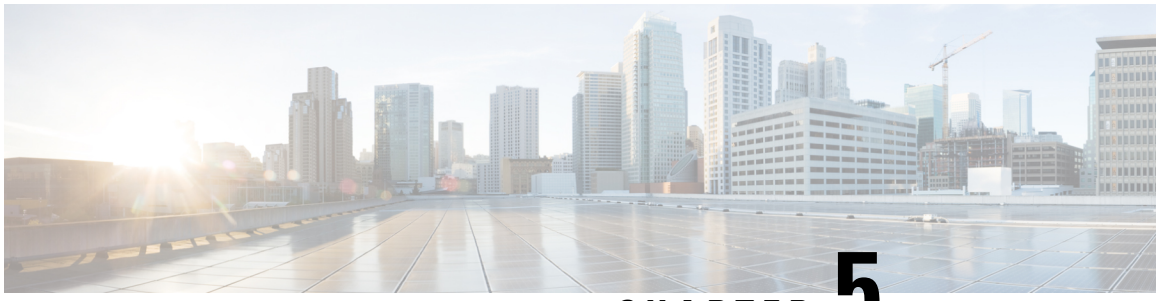
Here is a complete configuration example that enables contact 1 in output mode:

```
alarm contact 1 enable
alarm contact 1 output 1
alarm contact 1 description "Sensor indicating enclosure open"
```

Verify the Digital IO Status

On the device, use the **show alarm** command, filtering for digital IO and the contact (range 1 to 4) you want to view.

```
Router#show alarm | section Digital I/O 2
Digital I/O 2:
Description: External digital I/O port 2
Status: Not Asserted
Application: Dry
Severity: minor
Trigger: Closed
Voltage: 3300mV
Threshold: 1600mV
Mode: Input
```



CHAPTER 5

GPS Dead Reckoning

GPS Dead Reckoning

Table 4: Feature History

Feature Name	Release Information	Description
GPS Dead Reckoning	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	Dead reckoning provides a fallback mode for GPS location services when the GPS receiver cannot detect GPS satellite signals. Dead reckoning calculates the current position by using input from sensors such as accelerometers to measure movement from a previously known position. Dead reckoning is not as accurate as GPS, but provides a fallback method for providing location information.

Information About GPS Dead Reckoning

Dead Reckoning is a global positioning system (GPS) fallback feature that provides users with location information during satellite signal interruption by calculating the current position by using a previously determined position, and advancing that position based upon known or estimated speeds over elapsed time and course. For more information about GPS dead reckoning, including feature limitations, see Configuring GPS in the *Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide*.

Supported Devices for GPS Dead Reckoning

- Cisco IR1833 router
- Cisco IR1835 router

GPS Dead Reckoning Prerequisites

A GPS field-replaceable unit (FRU) module must be installed.

Use Cases for GPS Dead Reckoning

When a router is installed in a vehicle, such as a municipal services vehicle, the GPS receiver can provide accurate location information for reporting on the vehicle's location, as long as it can receive GPS satellite signals. If the vehicle enters an area that blocks reception of satellite signals, such as a tunnel, the dead reckoning feature continues to provide location information. The location determined by dead reckoning is not as reliable as the location information from functioning GPS.

Enable GPS Dead Reckoning Using a CLI Template

Use the following commands to enable the dead reckoning feature.

```
controller gps-dr
dead-reckoning enable
```

Disable GPS Dead Reckoning Using a CLI Template

Use the following commands to disable the dead reckoning feature.

```
controller gps-dr
no dead-reckoning enable
```

View the GPS Module Details

Use the **show inventory** command to view the GPS module details. Note the module information displayed for the Gps-Dr portion of the output.

```
Router#show inventory
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "Cisco Catalyst IR1835 Rugged Series Router"
PID: IR1835-K9         , VID: V00  , SN: FHH2416P00W
NAME: "Power Supply Module 0", DESCR: "Cisco IR1800 DC Power Supply"
PID: PWR-12V           , VID:      , SN:
```

```
NAME: "GE-POE Module", DESCR: "POE Module for On Board GE for Cisco IR183X"
PID: IR-183X-POE       , VID:      , SN:
NAME: "module 0", DESCR: "Cisco IR-1835-K9 Built-In NIM controller"
PID: IR-1835-K9        , VID:      , SN:
NAME: "NIM subslot 0/0", DESCR: "Front Panel 1 port Gigabitethernet Module"
PID: IR1835-1x1GE      , VID: V01  , SN:
NAME: "NIM subslot 0/1", DESCR: "IR1835-ES-4"
PID: IR1835-ES-4       , VID: V01  , SN:
NAME: "module F0", DESCR: "Cisco IR1835-K9 Forwarding Processor"
PID: IR1835-K9         , VID:      , SN:
NAME: "Gps-Dr", DESCR: "Dedicated GNSS/GPS/DR module"
PID: IRM-GNSS          , VID:V03 , SN:FOC243645DJ
```

Verify the Status of GPS Dead Reckoning

On a router, use the commands described in the sections that follow to verify the status of GPS dead reckoning. The status has three possibilities:

- GPS and dead reckoning are enabled and the GPS receiver has received satellite location information.
- GPS and dead reckoning are enabled and the GPS receiver has not received satellite location information, so it falls back on using the dead reckoning method.
- The GPS feature is not enabled.

Dead Reckoning Is Enabled, GPS Receiver Has Received Satellite Location Information

When the GPS receiver has received satellite location information, the **show platform hardware gps status** command indicates that GPS coordinates have been acquired.

```
Router#show platform hardware gps status
GPS Feature =  enabled
GPS Status =  GPS coordinates acquired
```

The **show platform hardware gps mode** command indicates that dead reckoning (DR) is not in use.

```
Router#show platform hardware gps mode
GPS Feature =  enabled
DR in use for location fix: No
```

Use the **show platform hardware gps detail** command to show the location information received by satellite. Note that the output includes "GPS Mode Used = GPS standalone" to indicate that GPS has received satellite information.

```
Router#show platform hardware gps detail
GPS Feature =  enabled
GPS Status =  GPS coordinates acquired
Latitude =  37 Deg 25 Min 4.7460 Sec North
Longitude =  121 Deg 55 Min 11.1840 Sec West
Timestamp (GMT) =  Tue Nov 24 03:03:55 2020
Fix type index =  0, Height =  40 m
HDOP =  4.1, GPS Mode Used =  GPS standalone
Satellite Info
----------------
Satellite #30, elevation 72, azimuth 43, SNR 0
Satellite #28, elevation 68, azimuth 277, SNR 0
Satellite #7, elevation 49, azimuth 89, SNR 0
Satellite #13, elevation 37, azimuth 312, SNR 0
Satellite #17, elevation 26, azimuth 185, SNR 25
Satellite #8, elevation 21, azimuth 43, SNR 0
```

```
Satellite #9, elevation 15, azimuth 160, SNR 17
Satellite #5, elevation 11, azimuth 260, SNR 26
Satellite #21, elevation 10, azimuth 77, SNR 0
Satellite #19, elevation 7, azimuth 194, SNR 24
Satellite #1, elevation 7, azimuth 103, SNR 0
Satellite #15, elevation 6, azimuth 322, SNR 0
```

Dead Reckoning Is Enabled, GPS Receiver Has Not Received Satellite Location Information

The **show platform hardware gps mode** command indicates that dead reckoning (DR) is in use.

```
Router#show platform hardware gps mode
GPS Feature =  enabled
DR in use for location fix: Yes
```

Use the **show platform hardware gps detail** command to show the location information. Note that the output includes "GPS Mode Used = DR based GPS" to indicate that the dead reckoning method is being used for location information. The output also provides the most recent satellite location information available.

```
Router#show platform hardware gps detail
GPS Feature =  enabled
GPS Status =  GPS coordinates acquired
Latitude =  37 Deg 25 Min 4.7460 Sec North
Longitude =  121 Deg 55 Min 11.1840 Sec West
Timestamp (GMT) =  Tue Nov 24 03:03:55 2020
Fix type index =  0, Height =  40 m
HDOP =  4.1, GPS Mode Used =  DR based GPS

Satellite Info
----------------
Satellite #30, elevation 72, azimuth 43, SNR 0
Satellite #28, elevation 68, azimuth 277, SNR 0
Satellite #7, elevation 49, azimuth 89, SNR 0
Satellite #13, elevation 37, azimuth 312, SNR 0
Satellite #17, elevation 26, azimuth 185, SNR 12
Satellite #8, elevation 21, azimuth 43, SNR 0
Satellite #9, elevation 15, azimuth 160, SNR 14
Satellite #5, elevation 11, azimuth 260, SNR 10
Satellite #21, elevation 10, azimuth 77, SNR 0
Satellite #19, elevation 7, azimuth 194, SNR 8
Satellite #1, elevation 7, azimuth 103, SNR 0
Satellite #15, elevation 6, azimuth 322, SNR 0
```

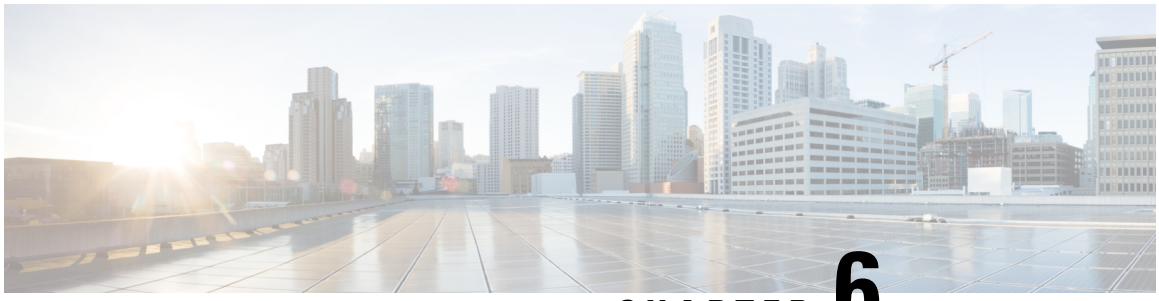
GPS Is Not Enabled

The following show commands indicate that the GPS feature is disabled.

```
Router#show platform hardware gps mode
GPS Feature =  disabled

Router#show platform hardware gps status
GPS Feature =  disabled
GPS Status =  GPS mode not enabled

Router#show platform hardware gps detail
GPS Feature =  disabled
GPS Status =  GPS mode not enabled
```



CHAPTER 6

Configure WIM on Cisco Catalyst IR1800 Rugged Series Routers

Configure WIM on Cisco Catalyst IR1800 Rugged Series Routers

Table 5: Feature History

Feature	Release Information	Description
Configure WIM on Cisco Catalyst IR 1800 Rugged Series Routers	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Manager Release 20.14.1	Configure and manage the Wi-Fi Interface Module (WIM) on Cisco Catalyst IR1800 Rugged Series Routers using Cisco SD-WAN Manager.

Information about Configuring WIM on Cisco Catalyst IR1800 Rugged Routers

The WIM features a pluggable 802.11ax module with WiFi-6 (802.11ax), 2x2 MIMO, two spatial streams, an extended temperature range, and versatile RF coverage with external RP-SMA antenna connectors, including Flexible Antenna Port feature support. For more information on WIM, see Cisco Wi-Fi Interface Module Overview.

The WIM module supports three modes of operation and they are:

- Control and Provisioning of Wireless Access Points (CAPWAP) mode
- Cisco Embedded Wireless Controllers (EWC) mode
- Work Group Bridge (WGB) mode

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, configure WIM on Cisco Catalyst IR1800 Rugged Routers using Cisco SD-WAN Manager in CAPWAP and WGB modes. When you configure the WIM in the CAPWAP mode, an external wireless LAN controller manages the module. The WIM module features two radios. In the WGB mode, set up each radio for either wireless access or WGB uplink. To enable Wireless Access, configure one or both radios to Root AP Mode. For WGB uplink, set up one radio to operate in WGB mode.

Note Configure either or both the radios using the Root AP mode. Only one of the radios can be configured for WGB uplink activity.

Supported Devices for Configuring WIM in Cisco Catalyst IR1800 Rugged Routers

The following Cisco Catalyst IR1800 modules are supported by Cisco SD-WAN Manager for configuring WIM:

- Catalyst IR1821-K9
- Catalyst IR1831-K9
- Catalyst IR1833-K9
- Catalyst IR1835-K9

Prerequisites for Configuring WIM on Cisco Catalyst IR1800 Rugged Routers

Ensure that the Cisco Catalyst IR1800 devices are running Cisco IOS XE Catalyst SD-WAN Release 17.14.1a or later releases.

Restrictions for Configuring WIM on Cisco IR1800 Rugged Routers

- You can't change the login credentials of the WIM using Cisco SD-WAN Manager. For more information see, Default WIM Passwords.

- The Cisco SD-WAN Manager doesn't support changing from the CAPWAP to the WGB mode and the vice-versa. To change modes, see Converting Between Modes.
- You can map a SSID profile to only one radio at a time.

Use Cases for Configuring WIM on Cisco Catalyst IR1800 Rugged Routers

Configure the WIM for different types of WAN connections, such as LTE, MPLS, broadband, or satellite using Cisco SD-WAN Manager and monitor the WIM using real time commands. Configure, manage and deploy both the WIM and WAN connections on Cisco Catalyst IR 1800 Rugged routers using Cisco SD-WAN Manager.

Configure WIM on Cisco Catalyst IR1800 Rugged Routers in CAPWAP Mode

In Cisco SD-WAN Manager, configure WIM on Cisco Catalyst IR1800 Rugged Routers in CAPWAP Mode using the CLI templates. For more information about using CLI templates, see CLI Add-on Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

1. Create a VLAN interface dedicated only to the layer 2 interface:

   ```
   interface Vlan id
   ```

2. Assign the layer 2 interface to the VLAN that you created:

   ```
   interface Wlan-GigabitEthernet0/1/4 switchport access vlan id
   switchport trunk native vlan vlan id
   switchport mode trunk
   ```

3. Create a DHCP pool for the VLAN:

Note Skip this step if you are using an external DHCP server.

```
ip dhcp pool vlan id
network ip subnet ip mask
default-router router ip address
```

The following example shows how to create a VLAN interface:

```
interface Vlan 50,100-200
```

The following example shows how to assign a layer 2 interface to the created VLAN

```
interface Wlan-GigabitEthernet0/1/4 switchport access vlan id
switchport access vlan 50,100-200
switchport trunk native vlan vlan 50,100-200
switchport mode trunk
```

The following example shows how to create a DHCP pool for the VLAN:

```
ip dhcp pool vlan 50,100-200
network 255.255.255.0 255.0.0
default-router 192.0.2.1
```

Configure WIM on Cisco Catalyst IR1800 Rugged Routers in WGB Mode

In Cisco SD-WAN Manager, configure WIM on Cisco Catalyst IR1800 Rugged Routers in WGB Mode using the CLI templates. For more information about using CLI templates, see CLI Add-on Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

1. Enter the wireless-bridge submode:

   wireless-bridge
2. Create a WLAN profile for open authentication:

   ssid-profile *ssid profile name* **ssid** *ssid name* **authentication** *open*
3. Create a WLAN profile for WPA2-PSK authentication:

   ssid-profile *ssid profile name* **ssid** *ssid name* **authentication** *auth-type* **key-management** *wpa2* **secret-key** *secret key word the unencrypted secret key*
4. Assign the WLAN profile to the Wi-Fi radio using the WGB mode:

   dot11Radio *0 or 1* **mode** *wgb* **ssid-profile** *ssid profile name*
5. Assign the WLAN profile to the Wi-Fi radio using the uWGB mode:

   dot11Radio *0 or 1* **mode** *uwgb client_mac* **ssid-profile** *ssid profile name*
6. Assign the WLAN profile to the root-AP mode to serve wireless clients:

   dot11Radio *0 or 1* **mode** *root-ap*
7. Add a VLAN interface:

   dot11Radio *0 or 1* **mode** *root-ap* **wlan** *wlan profile name*
8. Enable the radio:

   dot11Radio *0 or 1 enable*
9. Assign the operating channel for radio in root-AP mode:

   dot11Radio *0 or 1* **channel** *channel-number width*

The following example shows how to configure a clear text password:

```
wireless-bridge
ssid-profile wlan2 ssid secured_ssid authentication psk key-management wpa2 secret-key 0
12345678
dot11Radio 0 mode wgb ssid-profile test-ssid
```

```
dot11Radio 0 mode root-ap
dot11Radio 1 mode root-ap wlan test-wlan
dot11Radio 0 enable
dot11Radio 1 enable
dot11Radio 0 channel 5 10
```

Verify Configuring WIM on Cisco Catalyst IR1800 Rugged Routers

Verify the Status of WIM

The following is a sample output from the **show wireless-bridge status** command:

```
Device# show wireless-bridge status
Module Operating Mode : CAPWAP Mode
Module Status         : Module State Ready
Software Version      : 17.11.0.155
Module Session Status : Login Success
```

Verify the Status of WIM in WGB Mode

The following is a sample output from the **show wireless-bridge wlans** command:

```
Device# show wireless-bridge wlans
wlan  band  oper  vlan  #client  wlan-mode  SSID
 ----  ----  ----  ----  -------  ---------  -----------------
    0    5g    up     0        0     uplink  WGB_uplink
```

Verify the Status of the Connected Clients

The following is a sample output from the **show wireless-bridge clients** command:

```
Device# show wireless-bridge clients
Client-MAC-Addr    band  status        wlan  DeviceType  SSID
-----------------  ----  ------------  ----  ----------  -------------
 40:ED:00:1C:7E:EC  2.4g  Associated      2   wireless    000_aab
40:ED:00:1C:85:3B  2.4g  Associated      2   wireless    000_aab
```

Monitor WIM on Cisco Catalyst IR1800 Rugged Routers Using Cisco SD-WAN Manager

Monitor WLAN Output

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** > **Real Time**.
2. In the **Device Options** field, type **`Wireless SSID`** and choose **Wireless SSID** from the drop-down list.

   See the details of the WLAN along with the VLAN ID associated with them.

Note The real-time command **`Wireless SSID`** doesn't show the SSID type.

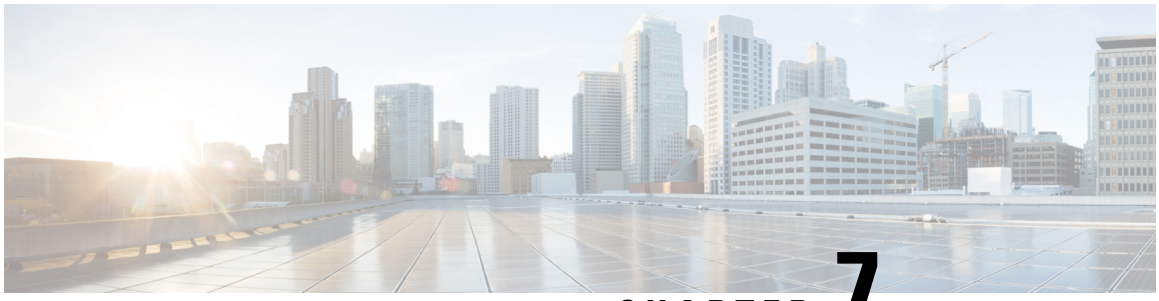
Monitor Client Details

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** > **Real Time**.
2. In the **Device Options** field, type **`Wireless Clients`** and choose **Wireless Clients** from the drop-down list.

   See the details of the clients with their MAC addresses.

Note

- The real-time command **`Wireless Clients`** doesn't show the client types.
- View both the wired and wireless client details using the **`Wireless Clients`** realtime command.



CHAPTER 7

Global Navigation Satellite System Support on PIMs

Global Navigation Satellite System Support on PIMs

Table 6: Feature History

Feature	Release Information	Description
Global Navigation Satellite System Support on PIMs	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	This feature allows you to configure and manage the Global Navigation Satellite System (GNSS) PIM module on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager.

Information About GNSS on PIMs

Specific Cisco IOS XE Catalyst SD-WAN devices support pluggable interface modules (PIMs) that offer satellite navigation services from satellite networks such as GPS, GLONASS, Galileo, and BeiDou. These satellite networks, collectively knows as Global Navigation Satellite System (GNSS), deliver geolocation services and precise time synchronization to Cisco IOS XE Catalyst SD-WAN devices and their connected devices.

Using Cisco SD-WAN Manager, you can configure a Cisco IOS XE Catalyst SD-WAN device equipped with a PIM module that supports GNSS.

Benefits of GNSS

- Time Synchronization

  Cisco IOS XE Catalyst SD-WAN devices equipped with GNSS receivers can directly synchronize to the time provided by GNSS, ensuring accurate timekeeping even without connectivity to time servers, and enabling all connected devices to maintain synchronized time.

- Precise Geolocation

  GNSS provides precise geolocation data.

Supported Devices for GNSS on PIMs

- Cisco Catalyst IR1101 Rugged Series Routers
- Cisco Catalyst IR1800 Rugged Series Routers

Configure GNSS on PIMs Using a CLI Template

For information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, the CLI Profile and CLI **show sdwan bfd sessions** templates execute commands in global configuration mode.

On a Cisco IOS XE Catalyst SD-WAN device, configure the slot number of the cellular interface and specify a GNSS constellation:

```
controller cellular slot_number
 lte gps constellation {beidou | galileo | glonass | gps | gnss}
```

Here's a complete configuration example for setting up a GNSS constellation with **gps** selected as the GNSS constellation.

```
controller cellular 0/1/0
 lte gps constellation gps
```

Verify GNSS on PIMs

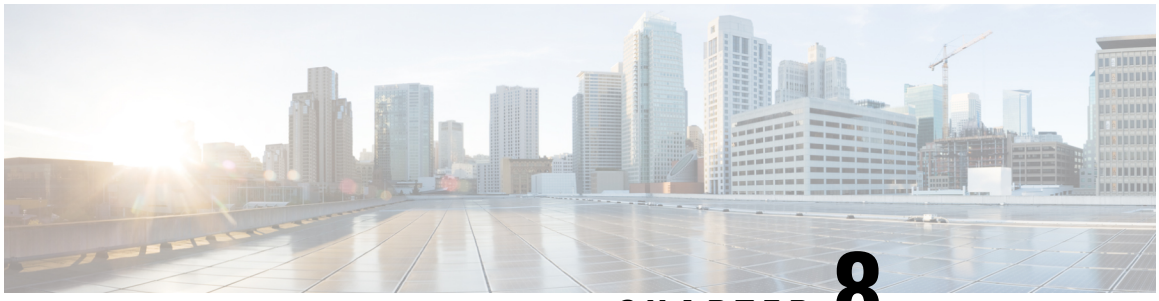
Use the **show cellular** command with **gps detail** to retrieve detailed information about GNSS constellations. The output shows the GNSS details such as feature status, mode, constellation configuration, GPS port selection, current GPS status, location coordinates, timestamp, and details of individual satellites such as GPS, GLONASS, Galileo, and BeiDou.

The following is a sample output from the **show cellular** command using the **gps detail** keyword:

```
Device# show cellular 0/3/0 gps detail
GPS Feature = enabled
GPS Mode Configured = standalone
Current Constellation Configured = gnss
GPS Port Selected = Dedicated GPS port
GPS Status = GPS coordinates acquired
Last Location Fix Error = Offline [0x0]
Latitude = 37 Deg 25 Min 6.0448 Sec North
Longitude = 121 Deg 55 Min 9.6295 Sec West
Timestamp (GMT) = Fri Jul 12 16:11:30 2024

Fix type = 2D, Height = 20m
HDOP = 0.7, GPS Mode Used = standalone

Satellite Info
----------------
GPS:
Satellite #5, elevation 60, azimuth 108, SNR 31 *
Satellite #11, elevation 24, azimuth 50, SNR 34 *
Satellite #12, elevation 40, azimuth 163, SNR 33 *
Satellite #15, elevation 1, azimuth 151, SNR 19 *
Satellite #18, elevation 30, azimuth 248, SNR 33 *
Satellite #20, elevation 46, azimuth 59, SNR 36 *
Satellite #25, elevation 64, azimuth 206, SNR 35 *
Satellite #26, elevation 6, azimuth 320, SNR 27 *
Satellite #28, elevation 13, azimuth 274, SNR 33 *
Satellite #29, elevation 59, azimuth 327, SNR 37 *
Satellite #31, elevation 8, azimuth 305, SNR 27 *
Satellite #46, elevation 0, azimuth 0, SNR 34 **
Glonass:
Satellite #74, elevation 35, azimuth 312, SNR 34 *
Satellite #82, elevation 21, azimuth 52, SNR 35 *
Satellite #73, elevation 52, azimuth 248, SNR 41 *
Satellite #80, elevation 20, azimuth 187, SNR 34 *
Satellite #84, elevation 30, azimuth 278, SNR 22
Satellite #83, elevation 51, azimuth 9, SNR 27 *
Satellite #67, elevation 24, azimuth 61, SNR 36 *
Satellite #66, elevation 2, azimuth 16, SNR 0
Satellite #68, elevation 21, azimuth 115, SNR 0
Galileo:
Satellite #13, elevation 33, azimuth 247, SNR 38 *
Satellite #15, elevation 75, azimuth 330, SNR 39 *
Satellite #27, elevation 68, azimuth 271, SNR 37 *
Satellite #3, elevation 2, azimuth 118, SNR 0
Satellite #5, elevation 4, azimuth 71, SNR 0 *
Satellite #21, elevation 21, azimuth 316, SNR 0
Satellite #30, elevation 42, azimuth 164, SNR 0
Beidou:
Satellite #6, elevation 3, azimuth 322, SNR 30
Satellite #12, elevation 15, azimuth 274, SNR 30 *
Satellite #19, elevation 33, azimuth 108, SNR 0
Satellite #20, elevation 21, azimuth 54, SNR 0 *
Satellite #22, elevation 14, azimuth 161, SNR 0
Satellite #24, elevation 28, azimuth 295, SNR 0
Satellite #26, elevation 37, azimuth 232, SNR 0 *
Satellite #29, elevation 25, azimuth 73, SNR 0 *
```



CHAPTER 8

Raw socket

Raw socket

Table 7: Feature history

Feature name	Release information	Description
Raw socket	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	You can transport serial data across your IP networks by configuring TCP or UDP options through configuration groups on supported Cisco rugged routers.

Raw socket

Raw socket transports serial data through an IP network. This feature enables the transportation of Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). It serves as an alternative to the Block Serial Tunnel (BSTUN) protocol.

Raw Socket Transport uses either TCP or UDP as the transport protocol. You can configure an interface to use one protocol at a time, but not both simultaneously. TCP transport suits control applications that require acknowledged and sequenced data delivery. For latency-sensitive applications, such as line SEL relays, UDP transport delivers serial data faster than TCP.

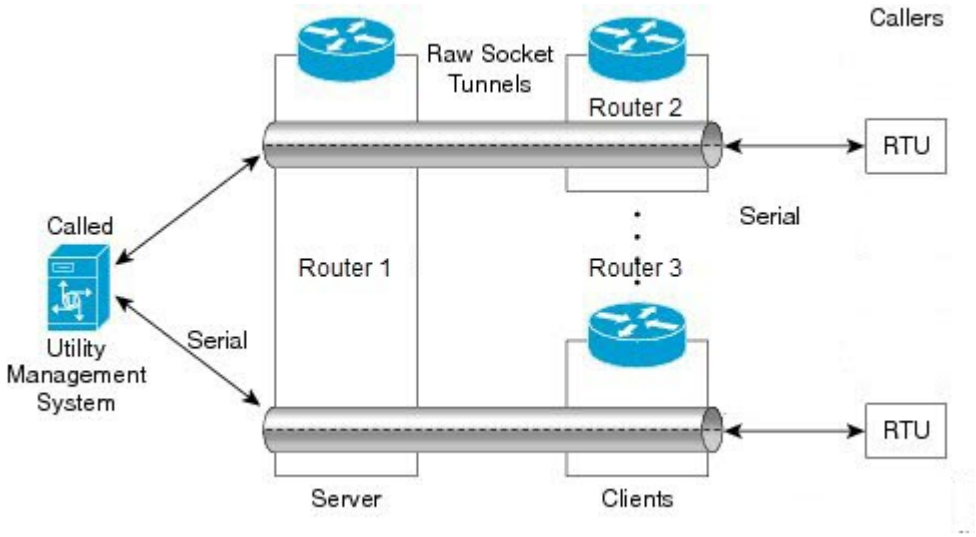
Raw Socket Transport provides the following support for the asynchronous serial interface:

- It uses TCP as the transport protocol and includes a built-in auto TCP connection retry mechanism.
- It supports up to 32 TCP sessions.
- You can configure the interface as a server, a client, or both.
- It allows one server interface and multiple clients.
- It provides VRF-awareness, enabling the router to send Raw socket transport traffic to a server host connected through a Virtual Routing and Forwarding (VRF) interface.

TCP transport

TCP raw socket transport uses a client-server model. At most one server and multiple clients can be configured on a single asynchronous serial line. In client mode, the IR1800 can initiate up to 32 TCP sessions to raw socket servers, which can be other IR1800 routers or third-party devices. The following figure shows a sample raw socket TCP configuration. In this example, serial data is transferred between RTUs and a utility management system across an IP network that includes several IR1800 routers. One IR1800 router (Router 1) acts as a raw socket server, listening for TCP connection requests from the other IR1800 routers (Router 2 and Router 3), which are configured as raw socket clients. A raw socket client receives streams of serial data from the RTUs 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.

Note When you configure the router's serial link interface as a server, the client router's serial link interface acts as its peer, and vice versa.



UDP transport

UDP transport uses a peer-to-peer model. Multiple UDP connections can be configured on an asynchronous serial line.

The following figure shows a sample raw socket UDP configuration. In this example, serial data is transferred between RTUs and a utility management system across an IP network that includes two routers (Router 1 which is an IR1800 and Router 2 which is an IR807) that are configured as raw socket UDP peers.

In this example, the raw socket UDP peer receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The raw socket UDP peer sends the packetized data across the IP network to the raw socket peer at the other end, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.

Serial data processing

When the default serial protocol, Asynchronous Communication Protocol, is used, the IR1800 packetizes streams of serial data received by a raw socket peer based on the following criteria:

- **Packet length** – You can specify a packet length that prompts the IR1800 to transmit the serial data to the peer. Once the IR1800 collects this amount of data in its buffer, it packetizes the accumulated data and forwards it to the raw socket peer.
- **Packet-timer value** – The IR1800 uses the packet timer to determine how long to wait for the next character in a stream. If the IR1800 does not receive a character before the timer expires, it packetizes the data accumulated in its buffer and sends it to the raw socket peer.
- **Special character** – You can specify a character that triggers the IR1800 to packetize the data in its buffer and forward it to the raw socket peer. When the IR1800 detects the special character (such as a CR/LF), it packetizes the accumulated data and sends it to the raw socket peer.

VRF-aware raw sockets

The VRF-aware raw socket transport feature enables you to isolate raw socket traffic using a VRF for efficient management and control of serial data. After configuring a VRF, you can associate the serial interface configured for raw socket transport with the VRF.

Restrictions for raw sockets

Firewalls in the network typically block UDP traffic. If the network includes such firewalls, configure pinholes to allow the Raw Socket UDP traffic.

Supported devices for raw sockets

- Cisco Catalyst IR1800 Rugged Series Routers
- Cisco Catalyst IR1101 Rugged Series Routers
- Cisco Catalyst IR8340 Rugged Series Routers

Configure raw socket without VRF using a configuration group

Follow these steps to configure a raw socket feature without VRF.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, click **Configuration** > **Configuration Groups**.

Step 2 Under the **Transport and Management Profile**, create or edit an existing transport profile.

Step 3 Click **Add New Feature** and select **Transport VPN** to create a Transport VPN feature.

Step 4 In the **Transport VPN** section, click the **+** icon and select **Raw Socket**.

Step 5 Click **Add New** from the drop-down menu in the **Raw Socket** section.

Step 6 Configure the raw socket parameters.

Step 7 Click **Save**.

Table 8: Raw socket

Field	Description
Loopback configuration	You can enable or disable the loopback configuration. Note that loopback is supported only on Cisco Catalyst IR8340 rugged series routers.
Interface name	Enter a name for the interface.
Packet length	Specify the length of the packet.
Packet time	Define the time duration to send packets.
Special character	Defines a specific character that triggers the router to send all buffered data to the raw socket peer.

Field	Description
Encapsulation	Choose TCP or UDP as the protocol to encapsulate and transport serial data. If you select TCP, configure the following options: • Set the local port. • Specify the local IP. • Choose the TCP mode. • Configure any advanced TCP options as needed. If you select UDP, configure the relevant UDP connection fields.

Configure a raw socket with VRF using a configuration group

Follow these steps to configure a raw socket feature with VRF.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Under the **Service Profile**, create or edit an existing service profile.

Step 3 Click **Add New Feature** and select **ServiceVPN** to create a Service VPN feature.

Step 4 In the **Service VPN** section, click the + icon and select **Raw Socket**.

Step 5 Click **Add New** from the drop-down list in the **Raw Socket** section.

Step 6 Configure the raw socket parameters.

Step 7 Click **Save**.

Table 9: Raw socket

Field	Description
Loopback configuration	You can enable or disable the loopback configuration. Note that loopback is supported only on Cisco Catalyst IR8340 rugged series routers.
Interface name	Enter a name for the interface.
Packet length	Specify the length of the packet.
Packet time	Define the time duration to send packets.

Field	Description
Special character	Defines a specific character that triggers the router to send all buffered data to the raw socket peer.
Encapsulation	Choose TCP or UDP as the protocol to encapsulate and transport serial data. If you select TCP, configure the following options: • Set the local port. • Specify the local IP. • Choose the TCP mode. • Configure any advanced TCP options as needed. If you select UDP, configure the relevant UDP connection fields.

Monitor a raw socket

Follow these steps to monitor a raw socket.

1. From Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Select a supported rugged series router.
3. Click **Real Time** in the left pane.
4. From the **Device options** drop-down list, select relevant raw socket options.

Monitor a raw socket using the CLI

Use the following commands to monitor raw socket sessions and statistics on a device.

Raw socket sessions

The following is a sample output of the **show raw-socket udp sessions** command:

```
device# show raw-socket udp sessions
 UDP Sessions
Interface   tty/(Idx)  vrf_name  socket   mode     local_ip_addr  local_port    dest_ip_addr
  dest_port   up_time     idle_time/timeout
   0/3/0    74            0      client  15.1.1.1      15001        15.1.1.2       15002
               00:00:14       00:00:14/300sec
```

The following is a sample output of the **show raw-socket tcp sessions** command:

```
device# show raw-socket tcp sessions
TCP Sessions
Interface   tty/(Idx) vrf_name   socket    mode       local_ip_addr  local_port
```

```
dest_ip_addr  dest_port    up_time     idle_time/timeout
 As0/3/0   74           0         server   15.1.1.1    15001          listening
 0/3/0      74          1         server   15.1.1.1    15001           15.1.1.2    15002
                   00:00:41    00:00:41/300sec
```

The following is a sample output of the **show raw-socket udp sessions local** command:

```
device# show raw-socket udp sessions local
Locally configured UDP client State
Interface  tty  dest_ip    dest_port  local_ip    local_port  state
0/3/0      74   15.1.1.2    15002     15.1.1.1      15001      UP
```

The following is a sample output of the **show raw-socket tcp sessions local** command:

```
device1# show raw-socket tcp sessions local
Locally configured TCP client State
Interface  tty  dest_ip    dest_port  local_ip   local_port  state
0/2/0      26   15.1.1.1    15001     15.1.1.2     15002      UP
```

Note The **show raw-socket tcp session local** command is supported exclusively on a client device.

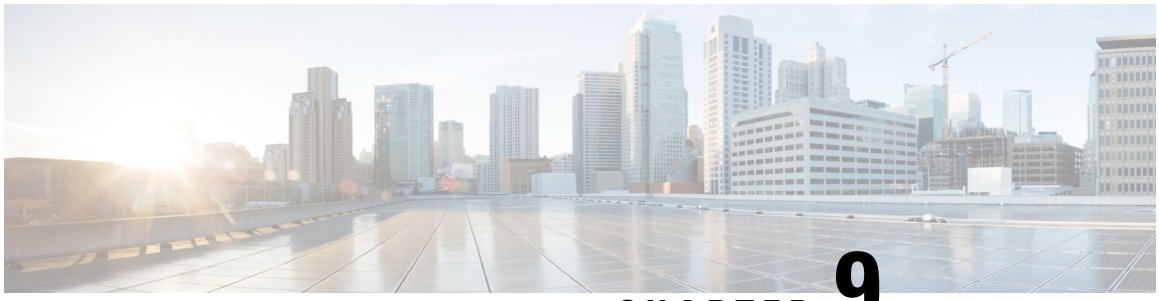
Raw socket statistics

The following is a sample output of the **show raw-socket udp statistics** command:

```
device# show raw-socket udp statistics
UDP-Serial Statistics
Interface  idx     vrf_name             sessions      udp_in_bytes         udp_out_bytes
 udp_to_tty_frames    tty_to_udp_frame
As0/3/0    74        1                   0                    0                    0
             0
```

The following is a sample output of the **show raw-socket tcp statistics** command:

```
device# show raw-socket tcp statistics
TCP-Serial Statistics
Interface  idx    vrf_name  sessions tcp_in_bytes   tcp_out_bytes   tcp_to_tty_frames
tty_to_tcp_frames
  As0/3/0   74    1             0                    0                    0
    0
```



CHAPTER 9

Wireless monitoring

Feature history for wireless monitoring

This table describes the developments of this feature, by release.

Table 10: Feature history

Feature Name	Release Information	Description
Wireless monitoring in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Cisco Catalyst SD-WAN Manager Release 26.1.1	Wireless monitoring in Cisco SD-WAN Manager provides real-time visibility into the status and operating mode of the Wi-Fi module installed in Cisco Catalyst IR1800 Rugged Series Routers. This feature enables you to monitor the health, operational mode, and firmware version of the Wi-Fi module.

Wireless monitoring in SD-WAN Manager

The wireless monitoring feature is a capability in Cisco SD-WAN Manager that

- provides real-time status of the Wi-Fi modules and firmware on Cisco Catalyst IR1800 Rugged Series routers, and
- displays the current operating mode of the Wi-Fi module.

Wireless monitoring in the Cisco SD-WAN Manager displays operational data directly from the IR1800 router, allowing users to view which operating mode (such as WGB mode or CAPWAP mode) the Wi-Fi module is using.

The wireless monitoring feature currently supports only SD-WAN controller mode, and autonomous mode.

Restrictions for wireless monitoring in SD-WAN Manager

Adhere to these restrictions when monitoring wireless status on IR1800 routers to avoid misinterpreting hardware states in Cisco SD-WAN Manager.

- If no Wi-Fi module is present in the IR1800 router, SD-WAN Manager may still display the operating mode as EWC, which does not reflect the actual hardware state.
- While the Wi-Fi module is reloading or booting, the wireless status may not update correctly and can show an incorrect operating mode.

Monitor wireless status in Cisco SD-WAN Manager

View the real-time status and operating mode of the Wi-Fi module installed in an IR1800 router using Cisco SD-WAN Manager.

Use this task to quickly check the operational mode (such as WGB mode or CAPWAP mode) and firmware status of Wi-Fi modules managed through the Cisco SD-WAN Manager interface.

- Ensure the IR1800 router is managed by Cisco SD-WAN Manager and is operating in controller mode.
- Confirm that a Wi-Fi module is installed in the IR1800 router.

Follow these steps to monitor the wireless status:

Procedure

Step 1 From the **Cisco SD-WAN Manager** menu, choose **Monitor** > **Devices**.

Step 2 Choose a IR1800 device by clicking its name in the **Hostname**.

Step 3 Click **Real Time** in the left pane.

Step 4 From the **Device Options** drop-down list in the right pane, choose **Wireless Status** to view the current operating mode and firmware information of the Wi-Fi module.

The wireless status page displays the real-time operating mode and firmware version of the Wi-Fi module for the selected IR1800 router.

What to do next

If the displayed status seems inaccurate (for example, EWC is shown when no module is present), verify the physical installation and operational state of the Wi-Fi module on the device.