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

Cisco SD-WAN
Release: 26.x and Later | Updated November 2, 2026

© 2026 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

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

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

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

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

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

Full Cisco Trademarks with Software License....ii

1 Ignition power management....5

Feature history of Ignition Power Management....6
Ignition Power Management in SD-WAN Manager....6
Supported devices for ignition power management....6
Use Cases for Ignition Power Management....7
Configure ignition power management using a configuration group....7
Enable Ignition Power Management Using a CLI Template....8
Monitor Ignition Power Management....9
Verify the Ignition Power Management Configuration....9

2 Digital IO....11

Feature history of Digital IO....12
Digital IO....12
Supported Devices....13
Use Cases for Digital IO....13
Enable Digital IO Using a CLI Template....13
Verify the Digital IO Status....16

3 GPS Dead Reckoning....17

Feature history of GPS Dead Reckoning....18
GPS Dead Reckoning in SD-WAN Manager....18
Supported devices for GPS Dead Reckoning....18
GPS Dead Reckoning prerequisites....18
Use cases for GPS Dead Reckoning....19
Enable GPS Dead Reckoning using a CLI template....19
Disable GPS Dead Reckoning using a CLI template....19
View the GPS Module Details....19
Verify the status of GPS Dead Reckoning....20

4 Configure WIM on Cisco Catalyst IR1800 Rugged Series Routers....23

Feature history of configuring WIM on Cisco Catalyst IR1800 rugged series routers....24
WIM configuration on Cisco Catalyst IR1800 rugged routers....24
Devices supporting WIM in Cisco Catalyst IR1800 rugged routers....25
Prerequisites for configuring WIM on Cisco Catalyst IR1800 rugged routers....25
Restrictions for configuring WIM on Cisco IR1800 rugged routers....25

Use cases for configuring WIM on Cisco Catalyst IR1800 rugged routers....25
Configure WIM on Cisco Catalyst IR1800 Rugged Routers in CAPWAP Mode....26
Configure WIM on Cisco Catalyst IR1800 Rugged Routers in WGB Mode....27
Verify WIM configuration on Cisco Catalyst IR1800 rugged routers....28
Monitor WIM on Cisco Catalyst IR1800 rugged routers using Cisco SD-WAN Manager....28

5 Global Navigation Satellite System Support on PIMs....31
Feature history of Global Navigation Satellite System support on PIMs....32
Global navigation satellite systems on pluggable interface modules....32
Benefits of GNSS....32
Supported devices for GNSS on PIMs....33
Configure GNSS on PIMs using a CLI template....33
Verify GNSS on PIMs....34

6 Raw socket....37
Feature history of Raw socket....38
Raw socket in SD-WAN Manager....38
TCP transport....38
UDP transport....39
Serial data processing....40
VRF-aware raw sockets....40
Restrictions for raw sockets....40
Supported devices for raw sockets....41
Configure a raw socket without VRF using a configuration group....41
Configure a raw socket with VRF using a configuration group....42
Monitor a raw socket....43
Monitor a raw socket using the CLI....43

7 Wireless monitoring....47
Feature history of wireless monitoring....48
Wireless monitoring in SD-WAN Manager....48
Restrictions for wireless monitoring in SD-WAN Manager....48
Monitor the wireless status in Cisco SD-WAN Manager....48

1 Ignition power management

Topics:

- Feature history of Ignition Power Management
- Ignition Power Management in SD-WAN Manager
- Supported devices for ignition power management
- Use Cases for Ignition Power Management
- Configure ignition power management using a configuration group
- Enable Ignition Power Management Using a CLI Template
- Monitor Ignition Power Management
- Verify the Ignition Power Management Configuration

Describes how Ignition Power Management enables control and monitoring of power supply to network devices. Helps users maintain optimal device performance and protection during power fluctuations or ignition events in industrial environments.

I

Feature history of Ignition Power Management

Describes ignition power management features for automotive routers. Helps users prevent battery drain and maintain router operation during vehicle stops, improving system reliability and reducing reload times.

Ignition power management prevents a router from draining the charge of a vehicle battery in automotive applications and enables real-time monitoring and configuration of power and sensing capabilities.

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.

Ignition Power Management in SD-WAN Manager

Describes how ignition power management prevents a router from draining a vehicle battery by controlling power based on the vehicle's ignition state. Helps users avoid battery depletion and configure shutdown delays.

Ignition power management is a feature that controls router power to prevent draining the vehicle battery when the router is installed in a vehicle.

- Router remains operational when the vehicle engine is running and charging the battery.
- Router shuts down when the vehicle ignition is turned off.
- User can configure a time interval to delay shutdown after ignition is turned off.

Ignition Power Management Example

For example, when the vehicle engine is running, the router stays powered. When the ignition is turned off, the router shuts down after a user-configured delay.

Supported devices for ignition power management

Describes the devices that support ignition power management. Provides users with information to identify compatible hardware for this feature.

The Cisco IR1800 router supports ignition power management.

Use Cases for Ignition Power Management

Describes how ignition power management enables routers to operate only when vehicles are in use, helping users optimize network connectivity and conserve power in fleet deployments.

Routers installed in fleet vehicles can be configured to sense ignition status, starting when the engine is running and shutting down after ignition is turned off. This ensures connectivity during vehicle use and conserves power when vehicles are idle.

Configure ignition power management using a configuration group

Configures ignition power management by creating and applying a feature within a System profile using a configuration group. This task enables centralized control of ignition power settings for SD-WAN devices.

Before you begin

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

Procedure

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

Field	Description
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

Enables ignition power management on the router using CLI commands to control detection of vehicle ignition status, battery type, shutdown delay, and undervoltage threshold. This task configures essential power management parameters for automotive deployments.

Ignition power management allows the router to detect whether a vehicle ignition is on or off and to control shutdown behavior based on ignition and voltage parameters.

- Configure battery type and shutdown delay for automotive power management.
- Set undervoltage thresholds to protect the device from low voltage conditions.

Ignition power management is used in vehicle deployments to ensure the router powers on and off in sync with the vehicle ignition and to prevent shutdown during brief ignition cycles.

- Default battery type is 12 V; off-timer and undervoltage settings are optional but recommended for optimal operation.

Procedure

1. ignition enable ignition sense

   Enables ignition power management and allows the router to detect ignition status.

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

2. ignition battery-type {12v | 24v}

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

3. ignition off-timer <seconds>

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

4. ignition undervoltage threshold <volts> <millivolts>

   (Optional) Configures the undervoltage parameter to trigger system shutdown if voltage drops below a specific threshold. Volts range from 9 to 24; millivolts range from 0 to 999. The default is 9.000 V.

Ignition power management is enabled, and the router is configured to detect ignition status, battery type, shutdown delay, and undervoltage threshold as specified.

Sample configuration:

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

Monitor Ignition Power Management

Monitors ignition power management for supported IR1800 devices using the vManage interface. Provides step-by-step instructions to access and view real-time ignition power management data.

Procedure

---

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices** .
2. Select a supported IR1800 device.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list, select **Ignition Power Management** .

Verify the Ignition Power Management Configuration

Describes how to verify the ignition power management configuration using device commands. Provides examples for both 12 V and 24 V battery types to help users confirm correct settings and thresholds.

Use device commands to verify ignition power management configuration and confirm battery type settings and voltage thresholds.

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
```

2 Digital IO

Topics:

- Feature history of Digital IO
- Digital IO
- Supported Devices
- Use Cases for Digital IO
- Enable Digital IO Using a CLI Template
- Verify the Digital IO Status

Describes the available reference information for users who need to understand this topic and its content.

Feature history of Digital IO

Describes GPIO support on Cisco IR1835, helping you understand port availability and configure each port as an input or output alarm.

The Cisco IR1835 supports four general-purpose input/output (GPIO) ports. You can configure a GPIO port as an input or an output alarm.

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.

Digital IO

Describes the digital IO ports on the Cisco IR1835 and how they support sensor input, external alarms, notifications, and actuators.

Digital IO consists of four general-purpose input/output (GPIO) ports on the Cisco IR1835 that can receive digital sensor input or provide digital output.

- Each contact can operate as a dry or wet contact.
- The contacts are protected up to +60 V.

Digital IO port capabilities

You can configure contacts in the digital IO port to receive digital sensor input or provide digital output. Sensors can provide information about the environment in which the router is installed, and digital output can trigger an external alarm, notification device, or actuator. Because digital output often triggers an external alarm, descriptions of this feature often use alarm terminology.

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. Alarm in is a dedicated input and alarm out is a dedicated output, whereas 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, refer to Digital IO in the *Cisco Catalyst IR1800 Rugged Series Router Software Configuration Guide* .

Figure 1: Digital IO Port on a Cisco IR1835 Router



Supported Devices

Lists the devices that support digital I/O, helping you identify compatible hardware.

Identify devices that support digital I/O.

Cisco IR1835 router

Use Cases for Digital IO

Describes how digital IO sensors can monitor conditions in an outdoor utility cabinet. This information helps you configure alarms and take action when cabinet conditions require attention.

Use digital IO sensors to monitor heat, humidity, and cabinet closure conditions and configure alarm states for conditions that require attention.

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

Configures digital IO contacts to trigger alarms or provide output current by using alarm contact CLI commands and contact-specific input or output parameters.

Procedure

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

   Example

   ```
   alarm contact
   contact-number
   enable
   ```

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

Example

```
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.

   Example

   ```
   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.

   Example

   ```
   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.

   Example

   ```
   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.

   Example

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

   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** .

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.

   Example

```
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

Describes how to view the status of a digital IO contact on the device. Use the command output to verify alarm details, status, and input settings.

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
```

3 GPS Dead Reckoning

Topics:

- Feature history of GPS Dead Reckoning
- GPS Dead Reckoning in SD-WAN Manager
- Supported devices for GPS Dead Reckoning
- GPS Dead Reckoning prerequisites
- Use cases for GPS Dead Reckoning
- Enable GPS Dead Reckoning using a CLI template
- Disable GPS Dead Reckoning using a CLI template
- View the GPS Module Details
- Verify the status of GPS Dead Reckoning

Describes GPS dead reckoning to help users understand the topic and identify relevant reference information.

Feature history of GPS Dead Reckoning

Describes GPS dead reckoning, which provides fallback location information when GPS satellite signals are unavailable and helps maintain position estimates using sensor input.

Dead reckoning provides a fallback mode for GPS location services when the GPS receiver cannot detect GPS satellite signals.

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.

GPS Dead Reckoning in SD-WAN Manager

Describes how GPS Dead Reckoning provides location information during satellite signal interruptions. It helps users estimate their current position from previously determined position, speed, elapsed time, and course.

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 using a previously determined position and advancing that position based on 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

Describes the Cisco routers that support GPS Dead Reckoning. Use this information to identify compatible devices.

GPS Dead Reckoning is supported on Cisco IR1833 and Cisco IR1835 routers.

- Cisco IR1833 router
- Cisco IR1835 router

GPS Dead Reckoning prerequisites

Provides prerequisites for GPS dead reckoning. A GPS field-replaceable unit (FRU) module must be installed to support operation.

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

Use cases for GPS Dead Reckoning

Describes how dead reckoning provides vehicle location information when GPS satellite signals are blocked. This information helps report location in areas such as tunnels where GPS reception is unavailable.

Provides location information when a vehicle enters an area that blocks reception of GPS satellite signals.

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

Describes the CLI commands that enable GPS dead reckoning, helping you configure the feature directly on the controller when needed.

Use the following commands to enable the dead reckoning feature.

```
controller gps-dr
```

```
dead-reckoning enable
```

Disable GPS Dead Reckoning using a CLI template

Describes how to disable the dead reckoning feature by using CLI commands, helping you remove the feature from the controller GPS configuration.

Use the following commands to disable the dead reckoning feature.

```
controller gps-dr
```

```
no dead-reckoning enable
```

View the GPS Module Details

Describes how to view GPS module details by using the **show inventory** command. The output identifies module information for the Gps-Dr portion.

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

Describes how to use router show commands to verify GPS dead reckoning status. The command output helps you determine whether GPS coordinates, dead reckoning, or neither method is in use.

Use the commands described in the following sections to verify the status of GPS dead reckoning on a router.

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
```

4 Configure WIM on Cisco Catalyst IR1800 Rugged Series Routers

Topics:

- Feature history of configuring WIM on Cisco Catalyst IR1800 rugged series routers
- WIM configuration on Cisco Catalyst IR1800 rugged routers
- Devices supporting WIM in Cisco Catalyst IR1800 rugged routers
- Prerequisites for configuring WIM on Cisco Catalyst IR1800 rugged routers
- Restrictions for configuring WIM on Cisco IR1800 rugged routers
- Use cases for configuring WIM on Cisco Catalyst IR1800 rugged routers
- Configure WIM on Cisco Catalyst IR1800 Rugged Routers in CAPWAP Mode
- Configure WIM on Cisco Catalyst IR1800 Rugged Routers in WGB Mode
- Verify WIM configuration on Cisco Catalyst IR1800 rugged routers
- Monitor WIM on Cisco Catalyst IR1800 rugged routers using Cisco SD-WAN Manager

Describes how to configure WIM on Cisco Catalyst IR1800 Rugged Series Routers. It helps you set up WIM for these routers.

Feature history of configuring WIM on Cisco Catalyst IR1800 rugged series routers

Provides information about how to configure and manage the Wi-Fi Interface Module (WIM) on Cisco Catalyst IR1800 Rugged Series Routers using Cisco SD-WAN Manager.

This reference describes how to configure and manage the Wi-Fi Interface Module (WIM) on Cisco Catalyst IR1800 Rugged Series Routers using Cisco SD-WAN Manager.

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.

WIM configuration on Cisco Catalyst IR1800 rugged routers

Explains how to configure the Wi-Fi Interface Module (WIM) on Cisco Catalyst IR1800 Rugged Routers, including supported operation modes and radio setup for wireless access and WGB uplink.

A WIM configuration is a wireless module setup that

- provides a pluggable 802.11ax module with WiFi-6 (802.11ax), 2x2 MIMO, two spatial streams, and extended temperature range
- offers versatile RF coverage with external RP-SMA antenna connectors and Flexible Antenna Port feature support, and
- supports three operation modes: CAPWAP, Cisco Embedded Wireless Controllers (EWC), and Work Group Bridge (WGB).

Operation modes and radio setup

The WIM module supports three modes of operation:

- 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. In CAPWAP mode, an external wireless LAN controller manages the module. The WIM module features two radios. In 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 radios using Root AP mode. Only one radio can be configured for WGB uplink activity.

WIM configuration example

For more information on WIM, see Cisco Wi-Fi Interface Module Overview.

Devices supporting WIM in Cisco Catalyst IR1800 rugged routers

Provides a list of Cisco Catalyst IR1800 modules that Cisco SD-WAN Manager supports for WIM configuration.

This reference lists the Cisco Catalyst IR1800 modules that Cisco SD-WAN Manager supports 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

Describes the software prerequisite for configuring WIM on Cisco Catalyst IR1800 rugged routers. Using a supported release helps ensure successful deployment.

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

Outlines important restrictions when configuring the Wireless Interface Module (WIM) on Cisco IR1800 rugged routers. Consider these limitations to ensure proper operation and avoid unsupported actions during configuration.

Restrictions for WIM configuration

- 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

Describes configuring and monitoring the WIM and WAN connections on Cisco Catalyst IR1800 Rugged Routers. Supports WAN connections such as LTE, MPLS, broadband, and satellite using Cisco SD-WAN Manager .

Configure and monitor the WIM and WAN connections on Cisco Catalyst IR 1800 Rugged routers using Cisco SD-WAN Manager .

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

Configures WIM on Cisco Catalyst IR1800 Rugged Routers in CAPWAP Mode using CLI templates in Cisco SD-WAN Manager . CLI templates execute commands in global config mode.

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.

Procedure

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

   Example

   ```
   interface Vlanid
   ```

   The following example shows how to create a VLAN interface:

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

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

   Example

   ```
   interfaceWlan-GigabitEthernet0/1/4 switchport accessvlan id
    switchport trunk native vlanvlan idswitchport modetrunk
   ```

   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
   ```

3. Create a DHCP pool for the VLAN:

   Example

   ```
   ip dhcppoolvlan id
    networkip subnetip mask
   default-routerrouter ip address
   ```

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

```
ip dhcp pool vlan 50,100-200
          network 255.255.255.0 255.0.0.0
          default-router 192.0.2.1
```

Note

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

Configure WIM on Cisco Catalyst IR1800 Rugged Routers in WGB Mode

Configures WIM on Cisco Catalyst IR1800 Rugged Routers in WGB Mode through CLI templates in Cisco SD-WAN Manager. CLI templates execute commands in global config mode by default.

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.

Procedure

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 WIM configuration on Cisco Catalyst IR1800 rugged routers

Provides sample command outputs to verify the configuration and operational status of the Wireless Interface Module (WIM) on Cisco Catalyst IR1800 Rugged Routers.

This reference lists sample command outputs to help you verify the configuration and operational status of the Wireless Interface Module (WIM) on Cisco Catalyst IR1800 Rugged Routers.

Verify the status of WIM

This 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

This 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

This 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

Monitors WLAN output and client details on Cisco Catalyst IR1800 rugged routers through Cisco SD-WAN Manager . The real-time commands display WLAN VLAN IDs and client MAC addresses.

Procedure

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.

   Note

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

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

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

   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.

   See the details of the clients with their MAC addresses.

5 Global Navigation Satellite System Support on PIMs

Topics:

- Feature history of Global Navigation Satellite System support on PIMs
- Global navigation satellite systems on pluggable interface modules
- Benefits of GNSS
- Supported devices for GNSS on PIMs
- Configure GNSS on PIMs using a CLI template
- Verify GNSS on PIMs

Describes Global Navigation Satellite System support on PIMs, helping you identify the supported capability for PIM deployments in your network configuration.

Feature history of Global Navigation Satellite System support on PIMs

Describes support for configuring and managing the Global Navigation Satellite System (GNSS) PIM module on routers using Cisco SD-WAN Manager. This information helps you identify the supported release information.

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

Feature History
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.

Global navigation satellite systems on pluggable interface modules

Explains how pluggable interface modules provide satellite navigation services, including geolocation and time synchronization, to Cisco IOS XE Catalyst SD-WAN devices and their connected devices.

A global navigation satellite system on pluggable interface modules is a satellite navigation feature that

- offers geolocation services and precise time synchronization to Cisco IOS XE Catalyst SD-WAN devices and their connected devices
- supports satellite networks such as GPS, GLONASS, Galileo, and BeiDou, and
- enables configuration through Cisco SD-WAN Manager for Cisco IOS XE Catalyst SD-WAN devices equipped with PIM modules that support GNSS.

Satellite navigation services on pluggable interface modules

Pluggable interface modules provide satellite navigation services from multiple satellite networks.

These modules deliver geolocation and time synchronization capabilities.

- GPS
- GLONASS
- Galileo
- BeiDou

Configuration is possible using Cisco SD-WAN Manager for supported Cisco IOS XE Catalyst SD-WAN devices.

Benefits of GNSS

Explains the advantages of GNSS, including time synchronization and precise geolocation, and describes how GNSS enables devices to maintain accurate time and location information without relying on external time servers.

A GNSS benefit is a feature of global navigation satellite systems that

- enables devices to synchronize time directly from GNSS signals
- provides precise geolocation data, and
- ensures accurate timekeeping even without connectivity to external time servers.

GNSS advantages for Cisco IOS XE Catalyst SD-WAN devices

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.

GNSS precise geolocation

GNSS provides precise geolocation data.

Supported devices for GNSS on PIMs

Describes the Cisco Catalyst IR1101 and IR1800 Rugged Series Routers as supported devices for GNSS functionality on Pluggable Interface Modules (PIMs), enabling precise location and timing services in industrial networking environments.

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

Configure GNSS on PIMs using a CLI template

Configure GNSS on PIMs using a CLI template. Configure the slot number of the cellular interface and specify a GNSS constellation on a supported device using a CLI template.

This task enables you to configure GNSS on PIMs by specifying the slot number of the cellular interface and selecting a GNSS constellation using a CLI template.

- Use this procedure to set up GNSS functionality for accurate location services on supported devices.

Use this task when you need to configure GNSS on a PIM using a CLI template on a supported device.

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

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

Before you begin

Ensure you have access to a Cisco IOS XE Catalyst SD-WAN device and the necessary permissions to apply CLI templates.

- Identify the slot number of the cellular interface to be configured.

Follow these steps to configure GNSS on PIMs using a CLI template:

Procedure

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

Example

```
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

The GNSS constellation is configured on the specified cellular interface.

After completing this task, the device will have GNSS enabled on the specified PIM, allowing it to use the selected constellation for location services.

What to do next

Verify GNSS on PIMs

Provides information about using the show cellular GPS detail command to retrieve GNSS constellation details, including feature status, mode, configuration, port selection, GPS status, location coordinates, timestamp, and satellite information for GPS, GLONASS, Galileo, and BeiDou.

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

This 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 *
```

6 Raw socket

Topics:

- Feature history of Raw socket
- Raw socket in SD-WAN Manager
- Restrictions for raw sockets
- Supported devices for raw sockets
- Configure a raw socket without VRF using a configuration group
- Configure a raw socket with VRF using a configuration group
- Monitor a raw socket
- Monitor a raw socket using the CLI

Introduces the core functions and use cases of raw sockets. Provides an overview of their application in network operations.

Raw sockets provide core functions and use cases for network operations.

Feature history of Raw socket

Describes the raw socket feature and its ability to transport serial data across IP networks using TCP or UDP options. Provides context for configuring this feature on Cisco rugged routers.

Explains that you can transport serial data across IP networks by configuring TCP or UDP options through configuration groups on supported Cisco rugged routers.

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 in SD-WAN Manager

Describes how raw socket transports serial data over IP networks, enabling SCADA data transfer from RTUs. Provides an alternative to BSTUN and supports both TCP and UDP protocols for flexible application needs.

Raw socket is a transport mechanism that enables serial data to be sent over an IP network, supporting SCADA data transfer from RTUs and serving as an alternative to BSTUN.

- Supports both TCP and UDP as transport protocols, but only one can be configured at a time per interface.
- TCP transport is suitable for control applications requiring acknowledged and sequenced delivery, while UDP is preferred for latency-sensitive applications.
- Provides VRF-awareness, allowing traffic to be sent through a VRF interface to a server host.

Raw socket transport features and configuration

Raw Socket Transport provides several features for asynchronous serial interfaces, including protocol selection, session management, and interface roles.

- Includes a built-in auto TCP connection retry mechanism.
- Supports up to 32 TCP sessions.
- Allows configuration of the interface as a server, a client, or both.
- Permits one server interface and multiple clients.

TCP transport

Describes how TCP raw socket transport enables serial data transfer between devices over an IP network using a client-server model. This approach supports multiple clients and a single server, providing flexible connectivity for utility management systems.

TCP raw socket transport is a method for transferring serial data between devices over an IP network using a client-server model.

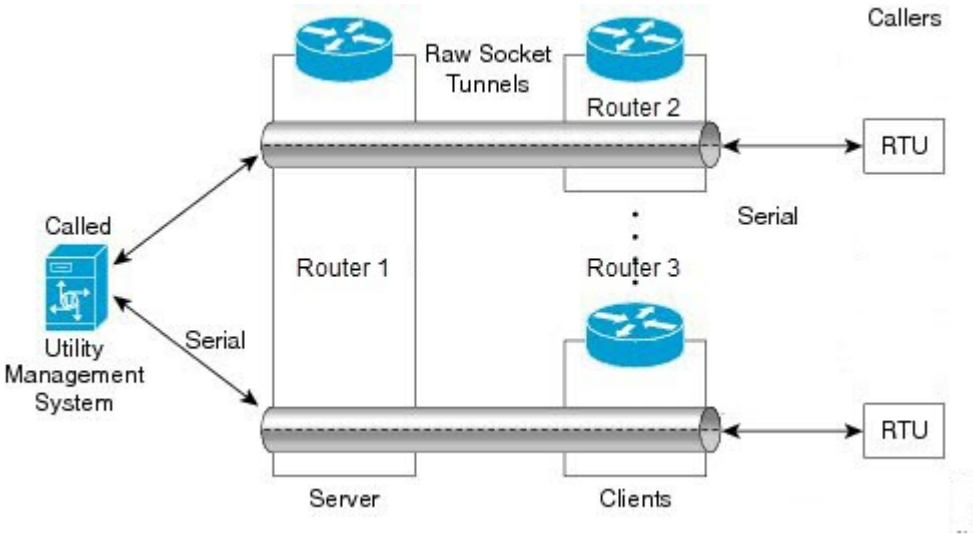
- Supports one server and multiple clients on a single asynchronous serial line.
- Allows the client device to initiate up to 32 TCP sessions to raw socket servers.
- Enables packetization of serial data for efficient transmission across the network.

TCP raw socket transport operation and configuration

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. 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.

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.

Figure 2: TCP raw socket transport connections



UDP transport

Describes how UDP transport uses a peer-to-peer model to transfer serial data between devices over an IP network. Provides context for configuring multiple UDP connections on asynchronous serial lines for utility management systems.

UDP transport is a method that uses a peer-to-peer model to transfer serial data between devices over an IP network.

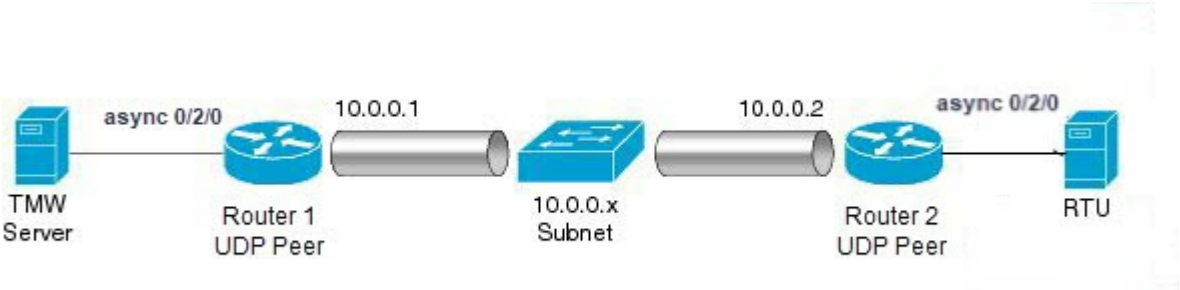
- Supports multiple UDP connections on an asynchronous serial line.
- Transfers serial data between RTUs and utility management systems using routers as raw socket UDP peers.
- Packetizes serial data based on user-specified criteria for transmission across the network.

UDP transport reference information

UDP transport enables the transfer of serial data between remote terminal units and utility management systems using routers configured as raw socket UDP peers.

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. 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.

Figure 3: UDP transport reference



Serial data processing

Describes how the IR1800 packetizes streams of serial data using the Asynchronous Communication Protocol. Helps users understand the criteria for data packetization and how to configure serial data transmission.

Serial data processing refers to the method by which the IR1800 packetizes streams of serial data received by a raw socket peer using the Asynchronous Communication Protocol.

- **Packet length** – A specified packet length prompts the IR1800 to transmit serial data to the peer once the buffer reaches this amount.
- **Packet-timer value** – The IR1800 uses a timer to determine how long to wait for the next character before packetizing and sending accumulated data.
- **Special character** – A designated character, such as CR/LF, triggers the IR1800 to packetize and forward the buffered data.

VRF-aware raw sockets

Describes how VRF-aware raw socket transport enables isolation of raw socket traffic for efficient management and control of serial data. Users can associate serial interfaces with a VRF to improve traffic handling.

The VRF-aware raw socket transport feature allows isolation of raw socket traffic using a VRF, enabling efficient management and control of serial data.

Restrictions for raw sockets

Provides guidelines for configuring firewalls to permit Raw Socket UDP traffic. Ensures network connectivity by addressing common firewall restrictions that may block UDP traffic.

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

Lists Cisco Catalyst IR1800, IR1101, and IR8340 Rugged Series Routers that support raw socket functionality. Helps users identify compatible hardware for raw socket deployment.

This topic identifies which Cisco Catalyst Rugged Series Routers support raw socket features.

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

Configure a raw socket without VRF using a configuration group

Configures a raw socket feature without VRF by using a configuration group in vManage. This process involves accessing the appropriate menus, creating or editing profiles, and saving the configuration.

To configure a raw socket feature without VRF, use the configuration group workflow in vManage. This ensures the raw socket is set up correctly within the transport and management profile.

Procedure

1. From the Cisco SD-WAN Manager menu, click **Configuration** > **Configuration Groups** .
2. Under the **Transport and Management Profile** , create or edit an existing transport profile.
3. Click **Add New Feature** and select **Transport VPN** to create a Transport VPN feature.
4. In the **Transport VPN** section, click the **+** icon and select **Raw Socket** .
5. Click **Add New** from the drop-down menu in the **Raw Socket** section.
6. Configure the raw socket parameters.
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

Configures a raw socket feature with VRF by using a configuration group in vManage. This process involves creating or editing a service profile, adding the Service VPN and Raw Socket features, and saving the configuration.

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

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups** .
2. Under the **Service Profile** , create or edit an existing service profile.
3. Click **Add New Feature** and select **ServiceVPN** to create a Service VPN feature.
4. In the **Service VPN** section, click the **+** icon and select **Raw Socket** .
5. Click **Add New** from the drop-down list in the **Raw Socket** section.
6. Configure the raw socket parameters.
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.
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.

Monitor a raw socket

Monitors the status and activity of a raw socket using the vManage interface. This process provides visibility into device operations for supported rugged series routers.

Procedure

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

Describes how to monitor raw socket sessions and statistics using CLI commands. Provides sample outputs to help users interpret session and statistics information for device troubleshooting and management.

Use CLI commands to monitor raw socket sessions and statistics on a device. Review sample outputs to understand session states and traffic statistics for UDP and TCP sockets.

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
```

7 Wireless monitoring

Topics:

- Feature history of wireless monitoring
- Wireless monitoring in SD-WAN Manager
- Restrictions for wireless monitoring in SD-WAN Manager
- Monitor the wireless status in Cisco SD-WAN Manager

Describes wireless monitoring for reviewing wireless activity and status.

Feature history of wireless monitoring

Describes release-specific wireless monitoring developments and helps you identify supported releases and Wi-Fi module visibility capabilities for Cisco Catalyst IR1800 Rugged Series Routers.

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 26.1.1.1	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

Describes wireless monitoring data for Wi-Fi modules on Cisco Catalyst IR1800 Rugged Series routers, helping users identify current module operating modes.

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

Provides restrictions for monitoring wireless status on IR1800 routers. Incorrect operating mode displays can lead users to misinterpret hardware states in Cisco 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 the wireless status in Cisco SD-WAN Manager

Monitors the real-time operating mode and firmware status of the Wi-Fi module installed in an IR1800 router. The status is available through 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.

Before you begin

- 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 in Cisco SD-WAN Manager :

Procedure

1. From the **Cisco SD-WAN Manager** menu, choose **Monitor** > **Devices** .
2. Choose a IR1800 device by clicking its name in the **Hostname** .
3. Click **Real Time** in the left pane.
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.