Configure the Cellular Gateways

Change the Password

Before you begin

To change the platform password, access the command-line-interface through SSH. Enter the configuration mode and then use the following commands to update the password:

Step 1 **aaa authentication users user admin change-password old-password**

Example:

```
CellularGateway(config)# aaa authentication users user admin change-password old-password
Value for 'old-password' (<string>): *********
Value for 'new-password' (<string>): ********
Value for 'confirm-password' (<string>): ********
```

Step 2 **commit**

Example:

```
CellularGateway(config)#
System message at 2020-06-01 22:07:57...
Commit performed by system via system using system
```

Note Any customized passwords must meet the following criteria:

- Contain at least one upper case letter
- Contain at least lower case letter
- Contain at least one special character (|,\, and / are not supported characters)
- Contain a number
- Contain a minimum of 8 characters
- Contain no more than 32 characters

Adjust IP MTU

In this scenario, the service provider is only providing a MTU of 1430 bytes. To configure an adjacent device with a MTU value of 1430 bytes or smaller, perform these steps on Cisco routing platforms:

Before you begin

If you are working with a service provider that does not support a standard 1500-byte MTU across their network, you will likely need to adjust the MTU configuration on the adjacent client device to match the MTU to the service provider or set optionally set it to a lower value. If you do not do this, the cellular gateway will be forced to fragment IP packets and that could result in sub-optimal performance compared to having outlying routing infrastructure reduce the size of packets before they arrive at the cellular gateway.

Note The configuration in this section is applicable for a Cisco device. If the client device is a non-Cisco router, then refer to the documentation for the device and adjust the MTU on the adjacent device.

Step 1 **configure terminal**

Example:

```
Device# configure terminal
```

Step 2 **interface** *interface-name*

Example:

```
Device(config)# interface GigabitEthernet 0/0
```

Step 3 **network mtu** *mtu-number*

Example:

```
Device(config-if)# mtu 1430
```

If you want to only affect IP traffic but allow other non-IP protocols to have a larger or different MTU use the following commands for the routing platforms:

Note These configuration steps are for Cisco devices only. The steps may vary for a vendor implementation.

Step 1 **configure terminal**

Example:

```
Device# configure terminal
```

Step 2 **interface** *interface-name*

Example:

```
Device(config)# interface GigabitEthernet 0/0
```

Step 3 **ip mtu** *mtu-number*

Example:

```
Device(config-if)# ip mtu 2203
```

Configure NTP Servers

To configure NTP servers, perform these steps:

Step 1 **configure terminal**

Example:

```
CellularGateway# configure terminal
```

Step 2 **ntp server** *ntp-server-name*

Example:

```
CellularGateway(config)# ntp server 10.20.100.111
```

Step 3 **ntp server** *server-pool*

Example:

```
CellularGateway(config)# ntp server 2.us.pool.ntp.org
```

Note Only 4 servers can be configured

Step 4 **commit**

Example:

```
CellularGateway(config)# commit
```

Step 5 **end**

Example:

```
CellularGateway(config)# end
```

Example

```
CellularGateway# show gw-system:ntp status
Clock is not synchronized, stratum 16, reference is INIT
frequency is 0.000 Hz, precision is -22
reference time is (no time),
clock offset is 0.000000 msec, root delay is 0.000 msec
root dispersion is 0.735
```

Instead of using NTP, the system clock can be set as in the following example:

request clock set date *date-time*

Example:

```
CellularGateway# gw-action:request clock set date 2020-10-26 time 12:30:00
```

The following is sample example of the system clock:

Example

```
CellularGateway# show gw-oper:clock
Current Time = Tue Oct 26 12:30:03 UTC 2020
```

Instead of using NTP, you can set the time zone as in the following example:

Step 1 **time-zone** *time-zone*

Example:

```
CellularGateway# timezone America/Chicago
```

Step 2 **commit**

Example:

```
CellularGateway# commit
```

Commit complete.

The following is sample example of the time-zone:

Example

```
CellularGateway# show gw-oper:clock
Current Time = Sat Jun 13 00:27:38 UTC 2020
```

Information on a Custom Cellular APN Profile

Customized profiles Access Point Name (APN) in mobile networks can be created and used on the Cellular Gateways. Maximum number of profiles that can be created are 16. Cisco SKU's shipping with specific firmware where default well known profiles are already populated and can be deployed readily.

But, if for some reason you need to configure Public or Private APN on the device below is the example how to do so. Very often, a misconfigured APN value will manifest as cellular connection that appears to be up but just cannot get an IP address.

Note The following options are also available for pdn-type:

- IPv4
- IPv4v6
- IPv6

Configure a Custom Cellular APN Profile

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `CellularGateway# configure terminal`	Enters global configuration mode.
Step 2	**controller cellular***number* **Example:** `CellularGateway# controller cellular 1`	Select controller cellular.
Step 3	**sim slot** *slot-number* **Example:** `Cellular Gateway(config-cellular-1)# sim slot x`	Select SIM slot under which you want to configure an Access Point Name (APN).
Step 4	**profile** *profile-number* **apn** *apn-name* **pdn-type** *pdn-type* **authentication** [**username** *username* **password** *password*] **Example:**	Creates a modem data profile. • The profile-number argument specifies the profile number created for the modem.

	Command or Action	Purpose
	`Cellular Gateway(config-slot-x)# profile id x apn apn.com pdn-type IPv4v6 authentication pap username admin password admin`	• The apn argument specifies an Access Point Name (APN). An APN is provided by your service provider. Only a single APN can be specified for a single profile. • (Optional) The PDN type parameter specifies the type of packet data session established with mobile network using this profile. Acceptable parameters are ipv4, ipv6, and ipv4v6 (IPv4 and IPv6). • (Optional) The authentication parameter specifies the authentication type used. Acceptable parameters are none (no authentication), chap, pap, and pap_chap (PAP or CHAP authentication). • (Optional) The username and password arguments are given by a service provider. These are mandatory when an authentication type other than none is used.
Step 5	**attach profile** *profile-id* **Example:** `Cellular Gateway(config-slot-x)# attach profile x`	The attach profile is the profile used by the modem to attach to the cellular network.
Step 6	**cellular 1/1** *profile-id* **Example:** `Cellular Gateway(config-slot-x)# cellular1/1 x`	The data profile is the profile used to send and receive data over the cellular network.
Step 7	**commit** **Example:** `Cellular Gateway(config-slot-x)# commit`	Commit the configurations.

Managing SIM Configurations

The SIM card primary slot is selected when the Cisco Catalyst Cellular Gateway boots up. The default slot is SIM 0. To force switchover to SIM 1, execute the following:

Step 1 **configure terminal**

Example:

```
CellularGateway# configure terminal
```

Step 2 **controller cellular 1**

Example:

```
CellularGateway(config)# controller cellular 1
```

Step 3 **sim primary-slot** *slot-number*

Example:

```
CellularGateway(config-cellular-1)# sim primary-slot 1
```

Step 4 **commit**

Example:

```
CellularGateway(config-cellular-1)# commit
```

Step 5 **end**

Example:

```
CellularGateway(config-cellular-1)# end
```

To check for installed SIM cards:

Example

```
CellularGateway# show cellular 1 sim
Cellular Dual SIM details:
SIM 0 = Present
SIM 1 = Present
Active SIM = 1
```

Note It is not recommended to select SIM slot 0 to be the primary SIM since SIM slot 0 is selected as primary by default.

Manage SIM Failover Behavior

It is possible to limit the number of times that the system attempts to fail over between the two SIMs trying to acquire a connection. It is also possible to control how long the system will try to connect on a given SIM before switching over to the alternate SIM. The following is the configuration to manage that behavior:

Step 1 **configure terminal**

Example:

```
CellularGateway# configure terminal
```

Step 2 **controller cellular 1**

Example:

```
CellularGateway(config)# controller cellular 1
```

Step 3 **sim max-retry** *max-retry-number*

Example:

```
CellularGateway(config-cellular-1)# sim max-retry 5
```

Step 4 **sim failover** *failover-timer*

Example:

```
CellularGateway(config-cellular-1)# sim failovertimer 7
```

Step 5 **commit**

Example:

```
CellularGateway(config-cellular-1)# commit
```

Step 6 **end**

Example:

```
CellularGateway(config-cellular-1)# end
```

Example:

With the configuration above, the system would try to connect for 7 minutes using the primary SIM (SIM 0 be default). If no connection could be acquired after 7 minutes, the system would switch to SIM 1, load the appropriate firmware, and try to connect for 7 more minutes. This failover pattern would repeat 4 more times. If there is still no connection at that point, the system will continue to try and connect on the SIM active at that time.

To set dual SIM failover timer in minutes

```
CellularGateway# show running-config
…….
controller cellular 1
 sim failovertimer 7
```

There are certain error codes (33 and 209) that the service provider can send which will cause the cellular client to retry connecting but with increasing delays so as to decrease the burden on the providers infrastructure which could be congested. This command will show you if that mechanism is in use and what the current backoff profile is:

Example

```
CellularGateway# show cellular 1 connection
Profile ID = 1
---------------------------
APN = broadband
Connectivity = Attach
Profile ID = 1
---------------------------
APN = broadband
Connectivity = Data
Session Status = Disconnected
Call end mode = 3GPP
Session disconnect reason type = 3GPP specification defined(6)
Session disconnect reason = Option unsubscribed(33)
Cellular Interface = 1/1
Backoff timer is running
Backoff error count = 1
Backoff timer index = 1
Backoff timer array (in minutes) = 0 1 1 1 1 5 10 15 30 60
Enforcing cellular interface back-off
Period of Backoff = 1 minute(s)
```

What to do next

In this example, the backoff timer has been activated and is running. Currently the system is waiting one minute between connect attempts. If error messages continue to be received from the service provider,

eventually the longer backoff timers will be used and there will be 5, 10, 15, 30, and 60 minutes between connect attempts.

Manually Manage Firmware

By default, the AutoSIM feature is enabled. AutoSIM analyzes any active SIM card and determines which service provider network is associated with that SIM. Based on that analysis, AutoSIM will automatically load the appropriate firmware.

Note In the United States there is unique firmware associated with AT&T, Verizon, and T-Mobile. In other global markets a Generic firmware is used.

Use the following configuration to manually override the AutoSIM function:

Step 1 **conf t**

Example:

```
Device# conf t
```

Step 2 **controller cellular 1**

Example:

```
CellularGateway(config)# controller cellular 1
```

Step 3 **auto sim disable**

Example:

```
CellularGateway(config-cellular-1)# auto sim disable
```

Step 4 **commit**

Example:

```
CellularGateway(config-cellular-1)# commit
```

Step 5 **end**

Example:

```
CellularGateway(config-cellular-1)# end
```

What to do next

It is possible to check the identity of the attached cellular network (in highlights), in case there are doubts that the proper firmware is loaded.

```
CellularGateway# show cellular 1 network
Current System Time = Sat Jun 13 1:25:47 2020
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Home
Network Selection Mode = Automatic
```

```
Network = AT&T
Mobile Country Code (MCC) = 310
Mobile Network Code (MNC) = 410
Packet Switch domain(PS) state = Attached
EMM State = Registered
EMM Sub state = Normal-Service
RRC Connection State = RRC Connected
Tracking Area Code (TAC) = 9993
Cell ID = 195572745
Network MTU = 1430
```

```
CellularGateway# cellular 1 firmware-activate 1
```

It is also possible to check current firmware status with the following command:

```
CellularGateway# show cellular 1 firmware
Firmware Activation Mode = AUTO
                                PRI
INDEX  CARRIER  FW VERSION      VERSION  STATUS
-------------------------------------------------
1      Generic  32.00.112-B016  1022     INACTIVE
2      Verizon  32.00.122-B016  2019     INACTIVE
3      ATT      32.00.142-B016  4019     ACTIVE
4      TMUS     32.00.152-B016  5002     INACTIVE
```

In the example above, AutoSIM is active as the indicated mode is AUTO (in highlights). If AutoSIM was disabled, MANUAL would be shown. In this particular example AutoSIM has selected AT&T firmware.

After performing the configuration above, an exec mode command is used to activate a specific firmware. It takes upto 120 seconds for the new firmware to load. Here is an example of that action to manually specify the firmware:

Upload and Upgrade Modem Firmware

Before you begin

Use the following procedure to upload and then upgrade modem firmware.

- Create a subdirectory to hold the modem firmware
- Copy the firmware file to that directory
- Issue the following command to complete the upgrade process

Step 1 **gw-action:request file**

Example:

```
CellularGateway# gw-action:request file create_dir firm_new
```

Step 2 **gw-action:request file copy source**

Example:

```
CellularGateway# gw-action:request file copy source tftp://192.168.1.2/fw.bin destination
/storage/firm_new/fw.bin
```

Step 3 **cellular 1 upgrade firmware firm_new**

Example:

```
CellularGateway# cellular 1 upgrade firmware firm_new
```

Enable DM Logging

This section describes steps to enable and collect Diagnostic Monitor (DM) logs for 5G and 4G Wide Area Network (WAN) Cisco Catalyst Cellular Gateways. You can also refer to the different commands to verify DM logging information.

Use the following configuration to enable DM logging when requested:

Note Do not attempt this configuration without specific engineering guidance. Cisco engineering resources provides the exact command line options.

Step 1 **conf t**

Example:

```
Device# conf t
```

Step 2 **controller cellular 1**

Example:

```
CellularGateway(config)# controller cellular 1
```

Step 3 **dm log enable**

Example:

```
CellularGateway(config-cellular-1)# dm log enable
```

Step 4 **commit**

Example:

```
CellularGateway(config-cellular-1)# commit
```

Step 5 **end**

Example:

```
CellularGateway(config-cellular-1)# end
```

What to do next

The following commands are used to collect the DM logs:

```
CellularGateway# show cellular 1 modem-logging
modem-logging dm-logs-status collecting
modem-logging dm-log-file-name /storage/log/dmlog-slot0-20200613.bin
```

```
CellularGateway# gw-action:request file list /storage/log/dmlog-slot0-20200613.bin
Location: /storage/log/dmlog-slot0-20200613.bin
-rw-r--r--   1 root  root   1000 May 27 23:12 /storage/log/dmlog-slot0-20200613.bin
```

```
CellularGateway# gw-action:request file copy source /storage/log/dmlog-slot0-20200613.bin
destination tftp://192.168.1.2/dmlog-slot0-20200613.bin
```

Configuring Cisco Catalyst Cellular Gateways Using the Web-Based Interface

Information about the Cisco Catalyst Cellular Gateway Web-Based User Interface

The Cisco Catalyst Cellular Gateways are connected to the device using a physical port. The Web-Based User Interface feature acts as an assistive tool to perform configurations and also helps in monitoring the device's status and performance.

Restrictions for the Cisco Catalyst Cellular Gateway Web-Based User Interface

There are no known restrictions on configuring the web-based user interface for Cisco Catalyst Cellular Gateway Web-Based User Interface.

Logging In and Logging Out of the Cisco Catalyst Cellular Gateway Web-Based User Interface

To log in to the Cisco Catalyst Cellular Gateway Web-Based User Interface, open the link (http://192.168.1.1:8008, https://192.168.1.1:8008) in a web browser. For first time users, the default username is **admin** and the default password is the **serialnumber** provided on the device. Enter the credentials (**username**, **password**) in the login prompt. A default **Dashboard** opens displaying a summary of the device status.

To log out of the Cisco Catalyst Cellular Gateway Web-Based User Interface, click **Logout** on the **Dashboard**.

Viewing the Status of Cisco Catalyst Cellular Gateways

From the main menu, choose **Dashboard**.

The Dashboard summarizes the device status and displays the following information:

Field	Description
CPU Utilization	Provides a graphical representation of the CPU usage (consists of the **Idle** time (blue), **User** usage (amber), **System** usage(green)) with a timestamp. Hover the mouse pointer over the graph to view the usage (captured in percentage).

Field	Description
Memory Utilization	Provides the memory usage (in percentage) indicating **Used** (blue), **Free** (Orange), **Total** (Green) utilization.
System Information	Displays the device's current system time, serial number, device model ID, device uptime, device hostname, build version, and other device specific information.
System Temperature	Displays a meter graph indicating the system's temperature in degrees.
Disk Utilization	Provides the total usage graph capturing free (blue) and used (green) disk space.

Monitoring the Device Activity

From the main menu, choose **Monitoring**.

The **Monitoring** page displays the following:

Field	Description
Polling Time	Displays the statistics which are refreshed according to the time interval you set.
Signal Strength Chart	Displays a graph indicating the signal strength of the SIM card that is inserted into the device. Hover the mouse pointer over the graph to view the detailed SIM information.
Hardware	Shows the modem's hardware and firmware information which is inserted into the gateway.
Network	System time and cellular network information is displayed.
Radio	Displays cellular radio information formed with the connection to the modem.
Cellular Details	All the cellular information like IP address, subnet mask, IPv4 and IPv6 DNS addresses, modem status, and so on are included.

Configuring Cisco Catalyst Cellular Gateways Using the Web-Based User Interface

The **Configuration** page allows you to configure the modem and SIM slot settings. There is an option to manage and configure Access Point Name (APN) profiles this page.

1. From the main menu, choose **Configuration** > **Cellular** tab, click the **Click to configure** link.

   • In **Cellular Configuration** page, the **General** window is used to configure diagnostic monitor (DM) logs

Field	Description
Auto SIM	Enable this option by clicking the toggle button.
Enable Logging	Helps in collecting DM logs.
DM log status	Allows you to download the DM logs for troubleshooting.
Rotation	If you enable the toggle, the device collects DM log files, which have a maximum size of 20 MB each, until the maximum DM log size is reached. When the maximum log size is reached, the oldest DM file is removed to provide storage space for a new DM log file.
Max DM Log Size	You can enter a minimum size of 60 MB to a maximum of 600 MB to collect the DM logs. If the logs reach this size, the device stops collecting DM log data.
Autostop Event	Choose an event that stops collection of the DM logs. • MODEM_STATE_IP_ACQUIRED: The device modem has received an IP address from the service provider but has not reached the MODEM_STATE_DNS_ACQUIRED state. • MODEM_STATE_DNS_ACQUIRED: The device has connected to the internet and acquired an IP address. • MODEM_STATE_SESSION_CONNECT: The device is disconnecting and reconnecting to the network repeatedly. • MODEM_STATE_ATTACHED_AND_REGISTERED: There is an error connecting to the packet data network (PDN) IP address. • MODEM_STATE_NETWORK_READY: The device modem has failed to connect to the network. • MODEM_STATE_DISCONNECTED: The device has detected a problem with its modem.
Filter Path	Add the bootflash or flash locations to store the DM log filter file.

Field	Description
Autostop Timer	You can configure the timer ranging from 1-120 seconds to wait after the autostop event before stopping the collection of DM logs.

Click **Save** to activate the new changed DM log parameters.

- In the **SIM** window, configure the **SIM** and **Slot** settings. Choose **SIM**, from the drop-down, click **SIM Primary**.

Field	Description
Active SIM	From the drop-down, select 0 or 1 depending on which SIM slot needs to be activated.
Failover Timer	A timer ranging from 1 to 7 can be set for the device to try to connect in case of failures.
Max Retry	A specific number can be defined to allow the number of reattempts to connect again.

Click **Save** to activate the new changed parameters.

- From the **SIM** drop-down, click **Slot**.

Field	Description
SIM Slots	Select 0 or 1 depending on which SIM slot needs to be activated on the device.
Attach Profiles	A maximum of 16 profiles can be created. Select the profile to be attached from the drop-down.
Data Profiles	From the drop-down, select the current profile to be attached and utilized.

Click **Save** to activate the new changed parameters.

The **Profiles** page allows multiple user profiles to be created, edited, and deleted.

1. From the main menu, choose **Configuration** > **Profiles** tab, click **Add** to create a new profile.

Field	Description
Profile ID	You can configure the ID between the range of 1 to 16.
APN Name	Add the name in string format.

Field	Description
PDN Type	Select the IPv4 or IPv6 address from the drop-down. • **Authentication**: **a.** If authentication is configured as **none**, then there is no requirement to add the username or password. **b.** If authentication is configured as **CHAP**, **PAP**, **PAP** or **CHAP**, you need to add the username and password.
Username	Enter a new authentication username.
Password	Enter a new authentication password.

Click **Save** to activate the new changed parameters.

Changing the Login Password

1. From the main menu, choose **Administration** > **User**.
2. Click on the 3 ellipses > **Change Password**.
3. Click **Submit** to activate the new changed password.

Use the Command Line Interface to Display Device Information

The command line interface (CLI) is provided to view all the configurations of the device. This is needed for debugging and troubleshooting. The show commands can be performed to view these details.

1. From the main menu, choose **Administration** > **Command Line Interface**.

2. On the **Command Line Interface** page, in the **Exec** field, enter a **show** command and press **Enter**. A list of all the available commands are displayed on the interface.

Additional Options

1. Click **Download Admin Tech Logs** on the display page that can be used for troubleshooting purposes.
2. Click the **Settings** icon, in **Preferences** > click the radio button for **Light** mode or **Dark** mode to change the theme.
3. Click **Save** to activate the new changed parameters.

Configuring Network Address Translation (NAT)

The Network Address Translation (NAT) feature enables translation of private IP addresses into public IP addresses. The device consists of 2 operational modes: IP passthrough mode and the NAT mode. On a Cellular Gateway device, IP passthrough is the default mode which can be switched to NAT mode. Enabling NAT on the Cisco Catalyst Cellular Gateway device provides the connected devices access to DHCP server and the local gateway.

Prerequisites for Configuring Network Address Translation (NAT)

There are no prerequisites required to configure Network Address Translation (NAT).

Restrictions for Configuring Network Address Translation (NAT)

A maximum of 16 Port Address Translation (PAT) rules can be configured on the device.

Information for Configuring Network Address Translation (NAT)

The Cisco Catalyst Cellular Gateways device can only be used with one host device in the IP pass through mode. In this mode, the device shares its WAN IP address with the connected host. Whereas, in the Gateway mode, the device functions in NAT mode.

Configuring Network Address Translation (NAT) on Cisco Catalyst Cellular Gateways

To configure a Cisco Catalyst Cellular Gateways device using NAT, perform the following steps:

SUMMARY STEPS

1. **gw-system:system passthrough false**
2. **commit**
3. **gw-system: ip dhcp pool network** *network-number* | *subnet-mask*
4. **gw-system:ip dhcp excluded-address** *low-address high-address*
5. **gw-system:ip dhcp pool lease-time** *days hours minutes*
6. **gw-system:ip nat inside source static tcp** *ip-address local-port***interface***interface-nameport-number*
7. **no gw-system:ip nat inside source static tcp** *ip-address local-port***interface***interface-nameport-number*
8. **show gw-system:ip dhcp binding**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**gw-system:system passthrough false** **Example:** `Device> gw-system:system passthrough false`	Enables the NAT mode. The default IP address is 10.0.23.0/24. To modify the default IP address pool, follow step 3.

	Command or Action	Purpose
Step 2	**commit** **Example:** `Device# commit`	If this step is performed, the device is enabled with the NAT mode. Proceed with step 3.
Step 3	**gw-system: ip dhcp pool network** *network-number* | *subnet-mask* **Example:** `Device(config)# gw-system: ip dhcp pool network 192.0.2.0/24`	(Optional) Specifies the subnet network number and mask of the DHCP address pool.
Step 4	**gw-system:ip dhcp excluded-address** *low-address high-address* **Example:** `Device(config-if)# gw-system:ip dhcp excluded-address 192.0.2.1 192.0.2.11`	(Optional) Exclude any specific IP addresses by configuring the low and high IP address. The default DHCP address pool is 10.0.23.0/24.
Step 5	**gw-system:ip dhcp pool lease-time** *days hours minutes* **Example:** `Device(config-if)# gw-system:ip dhcp pool lease-time 2 20 50`	(Optional) Configure the lease time. Default lease time is 24 hours.
Step 6	**gw-system:ip nat inside source static tcp** *ip-address local-port***interface***interface-nameport-number* **Example:** `Device(config-if)# gw-system:ip nat inside source static tcp 192.0.2.2 2022 interface GigabitEthernet 0/0 22`	(Optional) Configure PAT (port forwarding) rules using an IPv4 address.
Step 7	**no gw-system:ip nat inside source static tcp** *ip-address local-port***interface***interface-nameport-number* **Example:** `Device(config-if)# no gw-system:ip nat inside source static tcp 192.0.2.2 2022 interface GigabitEthernet 0/0 22`	(Optional) Disables NAT port forwarding by removing the PAT rule from active configurations.
Step 8	**show gw-system:ip dhcp binding** **Example:** `Device(config-if)# show gw-system:ip dhcp binding`	Verifies the list of client devices that are connected to the Cellular Gateway device.

Configuring WAN Secure Shell (SSH) on Cisco Catalyst Cellular Gateways

Prerequisites for Configuring WAN Secure Shell (SSH) on Cisco Catalyst Cellular Gateways

- To configure WAN SSH, the NAT mode must be enabled on a Cellular Gateways device.
- To configure WAN SSH, it is mandatory to use a cellular static public IP address issued by service providers.

Restrictions for Configuring WAN Secure Shell (SSH) on Cisco Catalyst Cellular Gateways

- A maximum of 16 Port Address Translation (PAT) rules can be configured on the device.
- The SSH default timeout is set to 30 minutes on the gateway after which the session disconnects automatically.

Configuring Cisco Catalyst Cellular Gateways using WAN SSH

To configure a Cisco Catalyst Cellular Gateways device using WAN SSH, perform the following steps:

SUMMARY STEPS

1. **config**
2. **gw-system:system passthrough false**
3. **gw-system: ip dhcp pool network** *ip-addresssubnet-mask*
4. **gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*
5. **show gw-system ip dhcp binding**
6. **no gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**config**	Enters global configuration mode.
Step 2	**gw-system:system passthrough false**	Enables the NAT mode.
Step 3	**gw-system: ip dhcp pool network** *ip-addresssubnet-mask*	(Optional) Configures the DHCP server and DHCP pool using an IPv4 address on the Cisco Catalyst Cellular Gateways.

	Command or Action	Purpose
Step 4	**gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*	Configures PAT (port forwarding) rules using an IPv4 address.
Step 5	**show gw-system ip dhcp binding**	Verifies the clients that are connected to the Cisco Catalyst Cellular Gateways.
Step 6	**no gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*	Disables access to SSH by removing the PAT rule from active configurations.

Information on Enabling WAN SSH using PAT Rules

SUMMARY STEPS

1. **gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*
2. **gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*

DETAILED STEPS

Step 1 **gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*

To enable SSH on the Cisco Catalyst Cellular Gateways, configure PAT rules using the following command:

```
Device(config)# gw-system:ip nat inside source static tcp 10.0.23.2 22 interface GigabitEthernet0/0
 22
```

Step 2 **gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*

If you need to establish an SSH session to the client device connected to the Cellular Gateway, configure PAT rules and use the IPv4 address assigned by the DHCP server and use the following command to connect to the adjacent client device:

```
Device(config)# gw-system:ip nat inside source static tcp 10.0.23.64 2022 interface GigabitEthernet0/0
 22
```

Verifying Port Address Translation (PAT) on the Cisco Catalyst Cellular Gateways

To verify PAT rules on the device, use the following command:

SUMMARY STEPS

1. **Device# show pat pat-list**

DETAILED STEPS

Device# show pat pat-list

```
SN   PORT      PROTO    DEST IP    DEST PORT   HITS
-------------------------------------------------
0    22        tcp   10.0.23.2        22      5219
1    2022      tcp   10.0.24.64       22       2
```

Note To establish an SSH session to the Cisco Catalyst Cellular Gateways or to the client device attached to the Cisco Catalyst Cellular Gateways, use the cellular public static IPv4 address. Note that dynamic cellular IP address will not work to enable an SSH session to the gateway device.

```
bash> ssh [username]@ipv4 address -p local_port
```

Example

```
bash> ssh admin@ipv4 address -p 22
```

To SSH into the device attached to the gateway, use the following command:

```
bash> ssh [device-username]@ipv4 address -p local_port
```

```
bash> ssh admin@ipv4 address -p 22
```

Configuring System Logging

Configuring System Logging

Event notification system log (syslog) messages can be logged to files on the local device, and/or sent to a remote host or hosts.

Prerequisites for Configuring System Logging

The remote logging server must be reachable from the Cisco Catalyst Cellular Gateways.

Restrictions for Configuring System Logging

A maximum of 4 servers can be configured for system logging.

Information for Configuring System Logging

- Logging into a local device's hard disk of syslog messages with a priority level of "information" is enabled by default.
- The log files are in the local disk under /var/log directory.

Logging System Log Default Parameters on a Local Device

To modify the syslog default parameters on a local device, perform the following commands:

SUMMARY STEPS

1. **gw-system:system loggingdisk**|**server**
2. **enable**
3. **file rotate***number***size***megabytes*
4. **severity** *severity*
5. **source-interface-ip address***ip address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**gw-system:system loggingdisk**|**server**	Enables logging into a local device's hard disk or server of syslog messages with a priority level of information.
Step 2	**enable**	Enables logging to the local disk.
Step 3	**file rotate***number***size***megabytes*	**Rotate**: Once the threshold of 10 files is met, the oldest file is removed to create a new file for newer syslog messages. **Size**: The default size of the log files is 10MB. It can be configured anywhere from 1MB to 20MB.
Step 4	**severity** *severity*	Changes the severity from "default" which is informational level to a different level.
Step 5	**source-interface-ip address***ip address*	Configures the source interface IP which is seen on the remote syslog servers.

A total of 10 syslog files are created. The **rotate** command allows configuring this size to anything from 1 to 10.

The default severity value is "informational", so by default, all syslog messages are recorded. The severity level can be one of the following (in order of decreasing severity):

- **Emergency**: System is unusable (corresponds to syslog severity 0).
- **Alert**: Action must be taken immediately (corresponds to syslog severity 1).
- **Critical**: A serious condition (corresponds to syslog severity 2).
- **Error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3).
- **Warn**: A minor error condition (corresponds to syslog severity 4).
- **Normal**: A normal, but significant condition (corresponds to syslog severity 5).
- **Information**: Routine condition (the default) (corresponds to syslog severity 6).

Disabling System Logging Parameters on a Local Device

To disable the logging of syslog messages to remote servers, perform the following command:

SUMMARY STEPS

1. **no gw-system:system logging disk enable**

DETAILED STEPS

no gw-system:system logging disk enable

Example:

```
Device(config)# no gw-system:system logging disk enable
```

Logging System Log Messages on a Remote Device

To log event notification syslog messages to a remote host, configure information about the server using the following commands:

SUMMARY STEPS

1. **gw-system:system loggingserver**{*dns-name*|*hostname*|*ip-address*}
2. **severity** *severity*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**gw-system:system loggingserver**{*dns-name*|*hostname*|*ip-address*}	Configures the server location by DNS name, hostname, or IP address.
Step 2	**severity** *severity*	Configures the priority of the syslog messages to send to the server.

Example

Example

To log event notification syslog messages to a remote host, use the following command:

```
Device(config)# gw-system:system logging server {dns-name | hostname | ip-address}

Device(config)# gw-system:system logging server 192.0.2.14 severity warn source-interface
Cellular1/0
```

Disabling System Logging Parameters on a Remote Device

To disable the logging of syslog messages to remote servers, perform the following command:

SUMMARY STEPS

1. **no gw-system:system logging server**

DETAILED STEPS

no gw-system:system logging server

Example:

```
Device(config)# no gw-system:system logging server
```

System Log Files

The default or configured syslog messages priority values are recorded in a number of files in the directory **/var/log**:

- **auth.log**: Login, logout, and superuser access events, and usage of authorization systems.
- **kern.log**: Kernel messages.
- **messages**: Consolidated log file that contains syslog messages from all sources.
- **vdebug**: All debug messages for modules whose debugging is turned on and all syslog messages above the configured priority value are saved to the file /var/log/tmplog/ vdebug. Debug logging supports various levels of logging based on the module. Different modules implement the logging levels differently.

  For example, the system manager (sysmgr) has two logging levels (on and off), while the chassis manager (chmgr) has four different logging levels (off, low, normal, and high). Debug messages cannot be sent to a remote host. To enable debugging, use the **debug** operational command.
- **vsyslog**: All syslog messages from Cellular Gateway processes (daemons) above the configured priority value are stored in the file /var/log/vsyslog. The default priority value is "informational", so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages are saved.
- **daemon**.**log**: All the boot up, lifecycle information of the daemons being spawned and restarted.

The Cellular Gateways software does not use the following standard LINUX files, which are present in /var/log, for logging: cron.log, debug, lpr.log, mail.log, and syslog.

Examples

Syslog message generated by the Cellular Gateway software have the following format.

Local logs stored on the local disk:

```
Oct 20 08:00:34 CellularGateway CWAND[8176]: CWAN:dev_ready_handler:QMI channels
initialization failed...retry_count[0] vendor:Sierra
```

Remote logs on the remote server:

Following is an example of a syslog message. In the file, this message would be on a single line.

```
2022-10-20T08:00:34+00:00 CellularGateway CWAND[8176] CWAN:dev_ready_handler:QMI channels
initialization failed...retry_count[0] vendor:Sierra
```

Configuring TACACS (Terminal Access Controller Access Control System)

Introduction to TACACS (Terminal Access Controller Access Control System)

TACACS is a security application that provides centralized validation of users attempting to gain access to a router or network access server. You must have access to and must configure a TACACS server before the configured TACACS features on your network access server are available.

TACACS provides for separate and modular authentication facilities. TACACS allows for a single access control server (the TACACS) to provide each service--authentication. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The goal of TACACS is to provide a methodology for managing multiple network access points from a single management service. The Cisco family of access servers and routers and the Cisco IOS and Cisco IOS XE user interface (for both routers and access servers) can be network access servers.

Network access points enable traditional “dumb” terminals, terminal emulators, workstations, personal computers (PCs), and routers in conjunction with suitable adapters (for example, modems or ISDN adapters) to communicate using protocols such as Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), Compressed SLIP (CSLIP), or AppleTalk Remote Access (ARA) protocol. In other words, a network access server provides connections to a single user, to a network or subnetwork, and to interconnected networks. The entities connected to the network through a network access server are called network access clients; for example, a PC running PPP over a voice-grade circuit is a network access client. TACACS, administered through the AAA security services, can provide the following services:

• Authentication--Provides complete control of authentication through login and password dialog, challenge and response, messaging support.

The authentication facility provides the ability to conduct an arbitrary dialog with the user (for example, after a login and password are provided, to challenge a user with a number of questions, like home address, mother’s maiden name, service type, and social security number). In addition, the TACACS authentication service supports sending messages to user screens. For example, a message could notify users that their passwords must be changed because of the company’s password aging policy.

The TACACS protocol provides authentication between the network access server and the TACACS, and it ensures confidentiality because all protocol exchanges between a network access server and a TACACS are encrypted.

You need a system running TACACS software to use the TACACS functionality on your network access server.

Cisco makes the TACACS protocol specification available as a draft RFC for those customers interested in developing their own TACACS software.

Prerequisites for Configuring TACACS

The TACACS server must be reachable from the Cisco Catalyst Cellular Gateways.

Restrictions for Configuring TACACS

There are no restrictions required to configure TACACS.

Configuring AAA Authentication Fall Back and Authentication Order

The following example shows a sample configuration for AAA authentication fall back and authentication order:

Procedure

	Command or Action	Purpose
Step 1	**gw-system:system aaa**	
Step 2	**auth-fallbackauth-ordertacacslocal**	The **auth-fallbackauth-ordertacacslocal** configures both local and TACACS authentication. Local authentication can be used as a fallback if TACACS servers are unavailable.

Configuring TACACS on Cisco Catalyst Cellular Gateways

The following example shows a sample configuration for TACACS:

Procedure

	Command or Action	Purpose
Step 1	**gw-system:system tacacs server***ip-address*	Specifies the IP address of one or more TACACS servers.
Step 2	**auth-port***port-number***secret-key**	• Specifies the TCP port number to be used when making connections to the TACACS server. The default port number is 49. • Specifies an encryption key for encrypting and decrypting all traffic between the Cellular Gateways and the TACACS daemon. Configure the same key on the TACACS server for encryption to be successful. Use the secret-key command to specify an encryption key that is used to encrypt all exchanges between the network access server and the TACACS server. Configure this key on the TACACS server.
Step 3	**source-interface** *interface*	Specifies the primary interface for all outgoing TACACS packets.
Step 4	**priority** *value*	Specifies a priority level of each TACACS server. Zero is a default priority value and is the highest priority TACACS server. If the Cellular Gateways is unable to establish a connection with the highest priority server, then the switch

	Command or Action	Purpose
		tries to establish connections with the next highest priority server. The range is from 0 to 7.
Step 5	**gw-system:system tacacs timeout** *value*	Specifies the period of time (in seconds) the gateway waits for a response from the TACACS before it times out and declares an error. The default number is 5, the number can be set from 1-1000.

IP Source Address Violation

The Cellular Gateway offers the ability to drop any traffic it receives that does not have the source address of the address which it offered from its DHCP server to the DHCP client. This feature saves cellular bandwidth in the scenario where a broadcast source, multicast source, or potentially a bad actor sends traffic to the cellular gateway as an attempt at denial of service.

Note This feature can be deactivated as shown, however, it is not recommended to deactivate this feature.

Step 1 **configure terminal**

Example:

```
CellularGateway# configure terminal
```

Step 2 **controller cellular 1**

Example:

```
CellularGateway(config)# controller cellular 1
```

Step 3 **ip-source-violation-action ipv4-permit**

Example:

```
CellularGateway(config-cellular-1)# ip-source-violation-action ipv4-permit
```

Step 4 **ip-source-violation-action ipv6-permit**

Example:

```
CellularGateway(config-cellular-1)# ip-source-violation-action ipv6-permit
```

Step 5 **commit**

Example:

```
CellularGateway(config-cellular-1)# commit
```

Step 6 **end**

Example:

```
CellularGateway(config-cellular-1)# end
```

What to do next

Packets dropped by this feature when enabled can be checked with the following command:

```
CellularGateway# show cellular 1 drop-stats
Ip Source Violation details:
 Ipv4 Action = Permit
 Ipv4 Packets Drop = 0
 Ipv4 Bytes Drop   = 0
 Ipv6 Action = Drop
 Ipv6 Packets Drop = 0
 Ipv6 Bytes Drop   = 0
```

Step 1 **configure terminal**

Example:

```
CellularGateway# configure terminal
```

Step 2 **controller cellular 1**

Example:

```
CellularGateway(config)# controller cellular 1
```

Step 3 **no ip-source-violation-action ipv4-permit**

Example:

```
CellularGateway(config-cellular-1)# no ip-source-violation-action ipv4-permit
```

Step 4 **no ip-source-violation-action ipv6-permit**

Example:

```
CellularGateway(config-cellular-1)# no ip-source-violation-action ipv6-permit
```

Step 5 **commit**

Example:

```
CellularGateway(config-cellular-1)# commit
```

Step 6 **end**

Example:

```
CellularGateway(config-cellular-1)# end
```

What to do next

To show if IPv4v6 IP source violation action permit is removed with the following command:

```
CellularGateway# show cellular 1 drop-stats
Ip Source Violation details:
 Ipv4 Action = Permit
 Ipv4 Packets Drop = 0
 Ipv4 Bytes Drop   = 0
 Ipv6 Action = Drop
 Ipv6 Packets Drop = 0
 Ipv6 Bytes Drop   = 0
```

Verify Catalyst Cellular Gateway

For information about the Cellular Gateways' hardware, use the **show cellular 1 hardware** command:

Step 1 **show cellular 1 hardware**

Example:

```
CellularGateway# show cellular 1 hardware
Modem Firmware Version = 32.00.142-B016
Host Firmware Version = 32.00.002-B016
Device Model ID = LM960A18
International Mobile Subscriber Identity (IMSI) = xxxxxxxxxxxxxx
International Mobile Equipment Identity (IMEI) = yyyyyyyyyyyyyy
Integrated Circuit Card ID (ICCID) = zzzzzzzzzzzzzzzzzzz
Mobile Subscriber Integrated Services Digital Network Number (MSISDN) =
Current Modem Temperature = 36 deg C
PRI Version = 4019
Carrier = ATT
OEM PRI Version = 32101005
Modem Status = MODEM_STATE_DNS_ACQUIRED
Host Device Manufacturer = Cisco Systems, Inc.
Host Device Model = EIO-LTEAP18-GL
Host Device Software Version = 17.3.01.0.1507.1591183906..Amsterdam
Host Device ID = 10JbWPwEQf
```

Step 2 **controller cellular 1**

Example:

```
CellularGateway# show cellular 1 radio
Radio Power Mode = online
Radio Access Technology(RAT) Selected = LTE
LTE Rx Channel Number(PCC) = 950
LTE Tx Channel Number(PCC) = 18950
LTE Band = 2
LTE Bandwidth = 20 MHz
Current RSSI = -53 dBm
Current RSRP = -83 dBm
Current RSRQ = -10 dB
Current SNR = 18.2 dB
Physical Cell Id = 138
```

What to do next

Note The cellular radio version and cellular SIM identifier are in highlights.

The CLIs can be used to get specific information about the state of the cellular radio.

Configuration Examples for Catalyst Cellular Gateway

Check Defined Profiles

Profiles defined in configuration mode are associated with the loaded firmware. As different firmware is loaded by the AutoSIM function, the defined profiles may change. When a firmware that has previously had custom APN profiles created is loaded, those previously defined profiles will be restored and replace those associated with the firmware that was replaced.

The following CLI can be used to check all of the currently defined profiles for the loaded firmware. The first example shows the output from when an AT&T SIM was active in SIM slot 0.

```
CellularGateway# show cellular 1 profile
PROFILE
ID       APN           PDP TYPE   STATE     AUTHENT  USERNAME  PASSWORD
-------------------------------------------------------------------------
1        broadband     IPv4v6     ACTIVE    None     -         -
4        attm2mglobal  IPv4v6     INACTIVE  None     -         -
```

After forcing a failover to a Verizon SIM, the following are the profiles provided automatically:

```
CellularGateway# show cellular 1 profile
PROFILE
ID       APN          PDP TYPE   STATE     AUTHENT  USERNAME  PASSWORD
-------------------------------------------------------------------------
1        ims          IPv4v6     INACTIVE  None     -         -
2        vzwadmin     IPv4v6     INACTIVE  None     -         -
3        vzwinternet  IPv4v6     ACTIVE    None     -         -
4        vzwapp       IPv4v6     INACTIVE  None     -         -
5                     IPv4v6     INACTIVE  None     -         -
6        vzwclass6    IPv4v6     INACTIVE  None     -         -
```

Interfaces on the Cellular Gateway

Use the following command to get detailed information about the interfaces on the Cellular Gateway:

```
CellularGateway# show interface detail cellular 1
Interface = Cellular 1/0
    Interface Type    = WAN
    Admin Status      = UP
    Operation Status  = UP
    IP address        = 10.19.1.2
    Total Rx Pkts     = 106
    Total Rx Bytes    = 8528
    Total Rx Errors   = 0
    Total Rx Drops    = 0
    5 min Input Rate  = 45 bits/sec, 0 packets/sec
    5 min Output Rate = 45 bits/sec, 0 packets/sec
    Total Tx Pkts     = 119
    Total Tx Bytes    = 8884
    Total Tx Errors   = 0
    Total Tx Drops    = 0
    MTU Size          = 1500
```

```
CellularGateway# show interface detail GigabitEthernet
Interface = GigabitEthernet 0/0
    Interface Type    = LAN
    Admin Status      = UP
    Operation Status  = UP
    IP address        = 192.168.1.1
    Total Rx Pkts     = 125
    Total Rx Bytes    = 18240
    Total Rx Errors   = 0
    Total Rx Drops    = 15
    5 min Input Rate  = 64 bits/sec, 0 packets/sec
    5 min Output Rate = 63 bits/sec, 0 packets/sec
    Total Tx Pkts     = 87
    Total Tx Bytes    = 16937
    Total Tx Errors   = 0
    Total Tx Drops    = 0
    MTU Size          = 2026
```

Note The address highlighted is the one acquired from the service provider and subsequently offered through DHCP to the attached client.