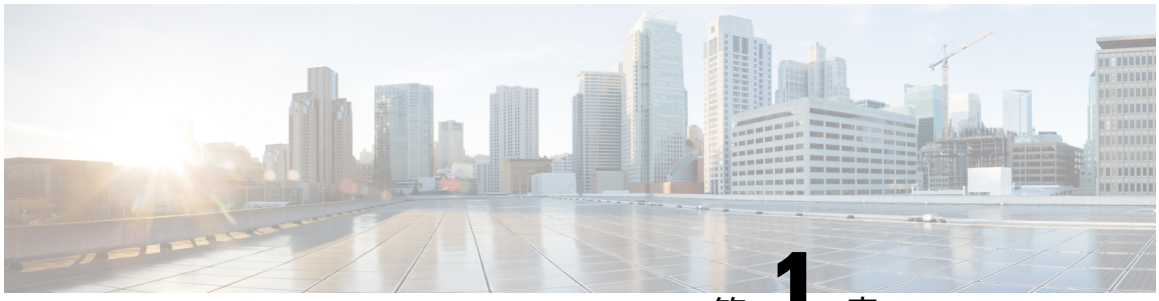
Cisco セルラーゲートウェイ ソフトウェア構成ガイド

初版：2023 年 7 月 5 日

最終更新：2023 年 7 月 5 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

Catalyst セルラーゲートウェイの概要

Cisco Catalyst セルラーゲートウェイは、従来の展開と SD-WAN 展開の両方で、最新のセルラーテクノロジーと展開の柔軟性、投資保護、および管理の容易さを兼ね備えています。

Catalyst セルラーゲートウェイ

Cisco Catalyst セルラーゲートウェイは、従来の展開と SD-WAN 展開の両方で、最新のセルラーテクノロジーと展開の柔軟性、投資保護、および管理の容易さを兼ね備えています。Cisco Catalyst セルラーゲートウェイでは、インターネットおよび MPLS のトランスポートモードに並ぶ主要な接続となっている高速な 4G と 5G をサポートしています。

Cisco Catalyst セルラーゲートウェイは、シスコのほぼすべてのホストプラットフォームに超高速セルラー接続を提供します。イーサネット経由でホストデバイスに接続され、Power over Ethernet（PoE）を利用できる Cisco Catalyst セルラーゲートウェイは、セルラー信号の受信が良好な場所であればどこにでも展開できます。クラウドホスト型とオンプレミス型の新しいアプリケーションをサポートし、より多くのデバイスを確実かつ柔軟に接続できるため、それらのデバイスを使用して QoS が保証されたワイヤレス WAN への移行が容易になります。

表 *1 : Cisco Catalyst* セルラーゲートウェイの *SKU*

Cisco 5G LTE	モード	動作領域	周波数帯域
CG418-E	LTE	グローバル	• **LTE バンド** 1 ～ 5、7、8、12 ～ 14、17、18 ～ 20、25、26、28 ～ 30、32、38 ～ 43、46、48、66、および 71 • **FDD LTE** 600 MHz（バンド 71）、700 MHz（バンド 12、13、14、17、28、29）、800 MHz（バンド 20）、850 MHz（バンド 5、18、19、26）、900 MHz（バンド 8）、1500 MHz（バンド 32）、1700 MHz（バンド 4 および 66）、1800 MHz（バンド 3）、1900 MHz（バンド 2 および 25）、2100 MHz（バンド 1）、2300 MHz（バンド 30）、2600 MHz（バンド 7） • **TDD LTE** 1900 MHz（バンド 39）、2300 MHz（バンド 40）、2500 MHz（バンド 41）、2600 MHz（バンド 38）、3500 MHz（バンド 42 および 48）、3700 MHz（バンド 43）、5200 MHz（バンド 46）
CG522-E	LTE、Sub-6、HSPA+/WCDMA	グローバル	• **LTE バンド** 1 ～ 8、12 ～ 14、17 ～ 20、25、26、28 ～ 30、32、34、38 ～ 43、46、48、66、および 71 • **Sub-6G** n1、n2、n3、n5、n28、n41、n66、n71、n77、n78、n79 • **HSPA+/WCDMA** バンド 1 ～ 6、8、9、および 19

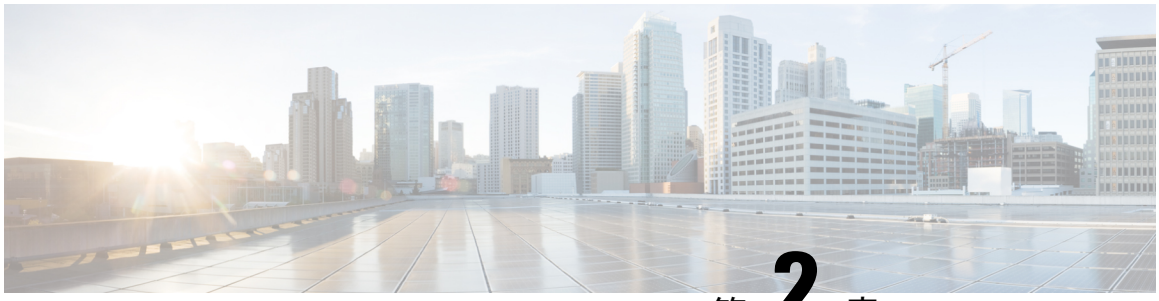
Catalyst セルラーゲートウェイの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2 : Catalyst* セルラーゲートウェイの機能情報

機能名	リリース	機能情報
CG418-E	Cisco IOS XE Amsterdam 17.3.2	このSKUが導入されました。
CG522-E	Cisco IOS XE Bengaluru 17.4.x	このSKUが導入されました。



第 2 章

プラットフォームの構成

プラットフォームアクセス - SSH

セルラーゲートウェイのプラットフォームには、初期設定用のルータからの**セキュアシェルセッション**でアクセスできます。初期接続用のパラメータは次のとおりです。

- IP アドレス：192.168.1.1
- ユーザ名：admin
- パスワード：デバイスのシリアル番号

これはユニットの底面に記載されています。また、ブートアップシーケンスを監視していれば、ブートアップシーケンスの一部として表示される次のメッセージで確認できます。

Device is using default day0 password: xxxxxxxxxxx

セルラーゲートウェイのプラットフォームは、デバイスを DHCP クライアントとして CG418-E の 2.5Gb/秒イーサネットポートおよび CG522-E の 10Gb/秒イーサネットポートに接続するだけで使用できます。必要に応じて、ポートは 1 Gb/秒の速度に戻ります。パブリック APN に接続していると仮定すると、AutoSIM 機能で適切なファームウェアとデフォルトの APN 値がロードされます。

（注） AutoSIM 機能は、すべてのキャリアでサポートされているわけではありません。

カスタムの APN 値が必要な場合は、このドキュメントで説明している手順に従って、その値をセルラーゲートウェイの CLI インターフェイスから指定します。

セルラーゲートウェイは、セルラー サービス プロバイダーから IPv4/IPv6 アドレスを取得します。その後、IP アドレスは DHCP を介して接続されたクライアントデバイスに送信されます。

プラットフォームアクセス - コンソールポート

セルラー ゲートウェイ プラットフォームには、初期構成用のコンソールセッションからアクセスできます。初期接続用のパラメータは次のとおりです。

- ボーレート：115200 ビット/秒、8 データビット、パリティなし、1 ストップビット（8N1）。フロー制御は必要ありません。
- ユーザ名：admin
- パスワード：デバイスのシリアル番号

これはユニットの底面に記載されています。また、ブートアップシーケンスを監視していれば、ブートアップシーケンスの一部として表示される次のメッセージで確認できます。

Device is using default day0 password: xxxxxxxxxxx

セルラー ゲートウェイ プラットフォームの使用を開始するために必要な操作は、デバイスを DHCP クライアントとして 2.5Gb/秒のイーサネットポートに接続することだけです。ポートの速度は必要に応じて 1Gb/秒になります。パブリック APN に接続していると仮定すると、AutoSIM 機能で適切なファームウェアとデフォルトの APN 値がロードされます。

カスタムの APN 値が必要な場合は、このドキュメントで説明している手順に従って、その値をセルラーゲートウェイの CLI インターフェイスから指定します。

DHCP クライアントは、セルラーゲートウェイから IP アドレスを受け取ります。この DHCP のアクションにより、セルラープロバイダーを指すデフォルトルートをクライアントにインストールするための情報が提供されます。さらに、DHCP サーバーから、管理接続用のセルラーゲートウェイを指す 192.168.1.1 へのルートをインストールするための情報が送信されます。

シングルステップによるプラットフォームイメージのダウンロードとアップグレード

ソフトウェアの変更方法として、マルチステージのプロセスに従う方法とシングルステップのプロセスを使用する方法があります。以下はシングルステージの方法です。

セルラーゲートウェイでは、ブートスペースにプライマリとセカンダリの 2 つのイメージを保持します。通常、過去の正常なイメージはバックアップとして示され、新しくインストールされたイメージはプライマリとして示されます。アップグレードプロセスで、古いセカンダリイメージは破棄され、古いプライマリイメージがセカンダリになり、新しくアップロードされたイメージがプライマリとして指定されます。システムでは、最初にプライマリイメージのブー

トが試行されます。それに失敗すると、正常であると認識されているセカンダリイメージのブートが試行されます。

ソフトウェアイメージを TFTP サーバーにコピーし、匿名の TFTP ユーザーがファイルにアクセスできるようにファイルの権限が設定されていることを確認します。TFTP サーバーが 192.168.1.0/24 のサブネットにあれば確実に接続できます。セルラーゲートウェイの現在の IP アドレスとルーティングの構成によっては、他のアドレス空間でも機能する場合があります。

TFTP サーバーからゲートウェイにイメージをダウンロードしてアップグレードします。

```
CellularGateway# gw-action:request software upgrade
tftp://192.168.1.2/cg-ipservices.2020-06-03_04.31_satikum3.SSA.bin
System is about to download and install the selected software, Continue? [no,yes] yes
Software successfully upgraded
```

システムをリブートして、バックアップイメージをプライマリにします。

```
CellularGateway# gw-action:request system reboot

System is about to reload, Continue? [yes,no]
```

システムパーティションを表示して、image2 がプライマリになっていることを確認します。

```
CellularGateway# show gw-system:system partition
System is about to reload, Continue? [yes,no]
show system partition
Primary Image
Partition    = image2
File name    = cg-ipservices.2020-06-03_04.31_satikum3.SSA.bin
Version      = 17.3.01.0.107173.1587052958..Amsterdam
Build Date   = Thu Apr 16 16:02:38 2020
Install Date = Sun Mar  5 08:04:14 2000
Boot Status  = Boot Successful.

Backup Image
Partition    = image1
File name    = cg-ipservices.2020-05-25_04.18_satikum3.SSA.bin
Version      = 17.3.01.0.1198.1590405489..Amsterdam
Build date   = Mon May 25 11:18:09 2020
Install Date = Wed Jun 17 23:52:27 2020
Boot Status  = Boot Successful.
```

マルチステップによるプラットフォームイメージのダウンロードとアップグレード

ソフトウェアの変更方法として、マルチステージのプロセスに従う方法とシングルステップのプロセスを使用する方法があります。以下はマルチステージの方法です。

セルラーゲートウェイでは、ブートスペースにプライマリとセカンダリの2つのイメージを保持します。通常、過去の正常なイメージはバックアップとして示され、新しくインストールされたイメージはプライマリとして示されます。アップグレードプロセスで、古いセカンダリイメージは破棄され、古いプライマリイメージがセカンダリになり、新しくアップロードされたイメージがプライマリとして指定されます。システムでは、最初にプライマリイメージのブートが試行されます。それに失敗すると、正常であると認識されているセカンダリイメージのブートが試行されます。

ソフトウェアイメージをルータにダウンロードし、新しいソフトウェアイメージの操作を使用するには、次の手順に従います。

ソフトウェアイメージを TFTP サーバーにコピーし、匿名の TFTP ユーザーがファイルにアクセスできるようにファイルの権限が設定されていることを確認します。TFTP サーバーが 192.168.1.0/24 のサブネットにあれば確実に接続できます。セルラーゲートウェイの現在の IP アドレスとルーティングの構成によっては、他のアドレス空間でも機能する場合があります。

セルラーゲートウェイにイメージをダウンロードします。

```
CellularGateway# gw-action:request software download tftp://192.168.1.x/image_file_name
```

イメージをインストールします。

```
CellularGateway# gw-action:request software install <image_file>
```

イメージをアクティブにします。

```
CellularGateway# gw-action:request software activate <image_file>
```

セルラーゲートウェイをリブートします。

```
CellularGateway# gw-action:request software system reboot
```

PID、稼働時間、メモリ、フラッシュサイズのチェック

```
CellularGateway# show gw-system:system status
SYSTEM INFO
Platform PID                    = CG418-E
Product Serial Number           = FHH2409P00X

System Up Time                  = up 5 days, 19 hours, 45 minutes
Current Time                    = Mon Mar 13 03:16:14 UTC 2000
Current CPU Usage               = 1%

RAM
Total Memory in KBytes          = 993540
Memory Used in KBytes           = 489524
Memory Free in KBytes           = 504016

STORAGE
Disk type                       = Bootflash
Disk Size in KBytes             = 999320
Disk Used in KBytes             = 3188
Disk Available in KBytes        = 927320
Disk Used Percentage            = 1%

TEMPERATURE
Ambient temperature             = 43 deg C
Power source                    = AC
```

ブートパーティションの手動切り替え

特定のブートパーティションからシステムを強制的にブートするには、次のEXECモードコマンドを使用します。

```
CellularGateway# gw-action:request software activate image1 | image2
Software Succesfully activated imageX
```

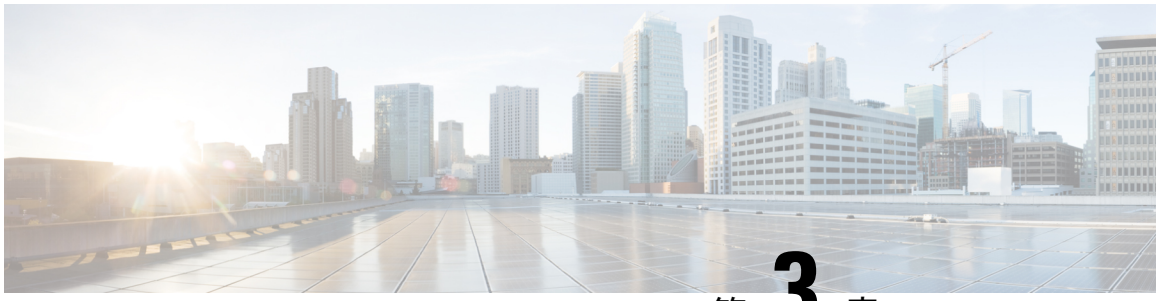
システムをリブートして、プライマリへのバックアップリクエストを開始します。

```
CellularGateway# gw-action:request system reboot
System is about to reload, Continue? [yes,no]
```

システムパーティションを表示して、イメージ 1 | イメージ 2 がプライマリになっていることを確認します。

```
CellularGateway# show gw-system:system partition
System is about to reload, Continue? [yes,no]
show system partition
Primary Image Partition= image2
File name= cg1000-ipservices.2020-04-16_09.02_satikum3.SSA.bin
Version= 17.3.01.0.107173.1587052958..Amsterdam
Build Date= Thu Apr 16 16:02:38 2020
Install Date = Sun Mar 5 08:04:14 2000
Boot Status = Boot Successful.

Backup Image Partition= image1
File name= cg-ipservices.2020-05-25_04.18_satikum3.SSA.bin
Version= 17.3.01.0.1198.1590405489..Amsterdam
Build date= Mon May 25 11:18:09 2020
Install Date = Wed Jun 17 23:52:27 2020 Boot Status = Boot Successful
```



第 3 章

セルラーゲートウェイの構成

パスワードの変更

始める前に

プラットフォームのパスワードを変更するには、SSH 経由でコマンド ライン インターフェイスにアクセスします。コンフィギュレーション モードを開始し、次のコマンドを使用してパスワードを更新します。

ステップ 1　aaa authentication users user admin change-password old-password

例：

```
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>): ********
```

ステップ 2 commit

例：

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

（注） パスワードをカスタマイズするときは、次の基準を満たす必要があります。

- 大文字を 1 文字以上含める
- 小文字を 1 文字以上含める
- 特殊文字を 1 文字以上含める（|、\、/ はサポートされない）
- 数字を含める
- 8 文字以上にする
- 32 文字以下にする

IP MTU の調整

ここでは、サービスプロバイダーが 1430 バイトの MTU のみを提供しているとします。隣接デバイスの MTU の値を 1430 バイト以下に構成するには、シスコのルーティング プラットフォームで次の手順を実行します。

始める前に

使用しているサービスプロバイダーのネットワークで標準の 1500 バイト MTU がサポートされていない場合、隣接するクライアントデバイスで MTU 設定の調整が必要になることがあります。MTU をサービスプロバイダーに合わせるか、必要に応じてそれよりも低い値に設定します。これを行わないと、セルラーゲートウェイで IP パケットがフラグメント化され、セルラーゲートウェイに到達する前に外部のルーティングインフラストラクチャによってパケットのサイズが削減される場合と比較してパフォーマンスが最適にならない可能性があります。

（注） このセクションで示す構成は、シスコデバイスの場合のものです。クライアントデバイスがシスコ以外のルータの場合は、デバイスのドキュメントを参照して隣接デバイスの MTU を調整してください。

ステップ 1 **configure terminal**

例：

```
Device# configure terminal
```

ステップ 2 **interface** *interface-name*

例：

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

ステップ 3 **network mtu** *mtu-number*

例：

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

この MTU を IP トラフィックのみに適用し、他の非 IP プロトコルにはこれよりも大きい別の MTU を許可する場合は、ルーティング プラットフォームで次のコマンドを使用します。

（注） これらの設定手順は、シスコデバイスのみに対応したものです。手順は、ベンダーの実装によって異なる場合があります。

ステップ 1 **configure terminal**

例：

```
Device# configure terminal
```

ステップ 2 **interface** *interface-name*

例：

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

ステップ 3 **ip mtu** *mtu-number*

例：

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

NTP サーバの設定

NTP サーバーを構成するには、次の手順を実行します。

ステップ 1 **configure terminal**

例：

```
CellularGateway# configure terminal
```

ステップ 2 **ntp server** *ntp-server-name*

例：

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

ステップ 3 **ntp server** *server-pool*

例：

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

（注） サーバーは 4 台だけ構成できます。

ステップ 4 **commit**

例：

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

ステップ 5 **end**

例：

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

例

```
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
```

NTP を使用する代わりに、次の例のようにシステムクロックを設定できます。

---

request clock set date *date-time*

例：

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

次に、システムクロックの例を示します。

例

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

NTP を使用する代わりに、次の例のようにタイムゾーンを設定できます。

ステップ 1 **time-zone** *time-zone*

例：

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

ステップ 2 **commit**

例：

```
CellularGateway# commit
```

Commit complete.

次に、タイムゾーンの例を示します。

例

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

カスタムセルラー APN プロファイルに関する情報

モバイルネットワークのカスタマイズされたプロファイル アクセス ポイント名（APN）を作成し、セルラーゲートウェイで使用できます。作成できるプロファイルの最大数は 16 です。特定のファームウェアを含む Cisco SKU の発送の場合、デフォルトの周知のプロファイルはすでに入力されており、すぐに展開できます。

ただし、何らかの理由によりデバイスでパブリックまたはプライベート APN を設定する必要がある場合は、下記がその方法の例になります。セルラー接続が起動しているようなのに IP アドレスを取得できないことで、APN 値の設定間違いが判明することが非常に多いです。

（注） pdn-type には次のオプションも使用できます。

- IPv4
- IPv4v6
- IPv6

カスタムセルラー APN プロファイルの構成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `CellularGateway# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**controller cellular***number* 例： `CellularGateway# controller cellular 1`	コントローラセルラーを選択します。
ステップ 3	**sim slot** *slot-number* 例： `Cellular Gateway(config-cellular-1)# sim slot x`	アクセスポイント名（APN）を設定する SIM スロットを選択します。
ステップ 4	**profile** *profile-id* **apn** *apn-name* **pdn-type** *pdn-type* **authentication** [**username** *username* **password** *password*] 例： `Cellular Gateway(config-slot-x)# profile id x apn apn.com pdn-type IPv4v6 authentication pap username admin password admin`	モデムデータプロファイルを作成します。 • profile-number 引数には、モデム用に作成されたプロファイル番号を指定します。 • apn 引数は、アクセスポイント名（APN）を指定します。APN はサービス プロバイダーによって提供されます。1 つのプロファイルに指定できるのは 1 つの APN のみです。 •（オプション）PDN 型パラメータは、このプロファイルを使用してモバイル ネットワークで確立されたパケット データ セッションのタイプを指定します。許容可能なパラメータは、ipv4、ipv6、および ipv4v6（IPv4 および IPv6）です。 •（任意）authentication パラメータは、使用する認証タイプを指定します。許容可能なパラメータは、none（認証なし）、chap、pap、および pap_chap（PAP または CHAP 認証）です。 •（任意）username および password 引数は、サービス プロバイダーが指定します。[none] 以外の認証タイプが使用されている場合、これらは必須です。
ステップ 5	**attach profile** *profile-id* 例：	attach profile は、携帯電話ネットワークに接続するモデムで使用されるプロファイルです。

	コマンドまたはアクション	目的
	`Cellular Gateway(config-slot-x)# attach profile x`	
ステップ 6	**cellular 1/1** *profile-id* 例： `Cellular Gateway(config-slot-x)# cellular1/1 x`	data profile は、携帯電話ネットワークでデータの送受信に使用するプロファイルです。
ステップ 7	**commit** 例： `Cellular Gateway(config-slot-x)# commit`	設定をコミットします。

SIM 構成の管理

SIM カードのプライマリスロットは、Cisco Catalyst セルラーゲートウェイの起動時に選択されます。デフォルトのスロットは SIM 0 です。SIM 1 に強制的にスイッチオーバーするには、以下を実行します。

ステップ 1 **configure terminal**

例：

```
CellularGateway# configure terminal
```

ステップ 2 **controller cellular 1**

例：

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

ステップ 3 **sim primary-slot** *slot-number*

例：

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

ステップ 4 **commit**

例：

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

ステップ 5 **end**

例：

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

取り付けられている SIM カードをチェックするには、次のように入力します。

例

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

（注） SIM スロット 0 はデフォルトでプライマリとして選択されるため、SIM スロット 0 をプライマリ SIM として選択することはお勧めしません。

SIM フェールオーバー動作の管理

接続を取得しようとする 2 つの SIM 間でシステムがフェールオーバーを試みる回数を制限することができます。また、別の SIM に切り替える前にシステムが特定の SIM で接続を試みる時間を制御することもできます。以下は、その動作を管理するための構成です。

ステップ 1 **configure terminal**

例：

```
CellularGateway# configure terminal
```

ステップ 2 **controller cellular 1**

例：

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

ステップ 3 **sim max-retry** *max-retry-number*

例：

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

ステップ 4 **sim failover** *failover-timer*

例：

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

ステップ 5 **commit**

例：

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

ステップ 6 **end**

例：

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

例：

上記の構成では、システムはプライマリ SIM（デフォルトは SIM 0）を使用して 7 分間接続を試みます。7 分経過しても接続を取得できなかった場合、システムは SIM 1 に切り替えて適切なファームウェアをロードし、さらに 7 分間接続を試みます。このフェールオーバーパターンがあと 4 回繰り返されます。その時点でまだ接続を取得できない場合、システムはその時点のアクティブな SIM で接続を試行し続けます。

デュアル SIM フェールオーバータイマー（分単位）を設定するには、次のように入力します。

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

サービスプロバイダーから特定のエラーコード（33 および 209）が送信されることがあり、その場合、セルラークライアントで接続が再試行されますが、プロバイダーのインフラストラクチャで輻輳が発生しないように負担を軽減するため、遅延が増えます。次のコマンドを使用すると、そのメカニズムが使用されているかどうかと現在のバックオフプロファイルの内容を確認できます。

例

```
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)
```

次のタスク

この例では、バックオフタイマーがアクティブ化されて実行されています。現在、システムは次の接続を試行するまで 1 分間待機しています。サービスプロバイダーからのエラーメッセージの受信が続くと、より長いバックオフタイマーが使用されるようになり、接続を試行する間隔が 5 分、10 分、15 分、30 分、60 分と延びていきます。

ファームウェアの手動管理

デフォルトでは、AutoSIM 機能が有効になっています。AutoSIM は、アクティブな SIM カードを分析し、その SIM に関連付けられているサービス プロバイダー ネットワークを特定します。その分析に基づいて、AutoSIM は適切なファームウェアを自動的にロードします。

（注） 米国には、AT&T、Verizon、および T-Mobile に関連付けられた独自のファームウェアがあります。他のグローバル市場では、汎用ファームウェアが使用されています。

AutoSIM 機能を手動でオーバーライドするには、次の構成を使用します。

ステップ 1 **conf t**

例：

```
Device# conf t
```

ステップ 2 **controller cellular 1**

例：

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

ステップ 3 **auto sim disable**

例：

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

ステップ 4 **commit**

例：

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

ステップ 5 **end**

例：

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

次のタスク

適切なファームウェアがロードされているかどうか疑わしい場合、接続されているセルラーネットワークの ID（ハイライトされた箇所）を確認できます。

```
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
```

次のコマンドを使用して、現在のファームウェアのステータスを確認することもできます。

```
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
```

上記の例では、モードが AUTO（ハイライトされた箇所）と示されており、AutoSIM がアクティブになっています。AutoSIM が無効になっている場合は、MANUAL と表示されます。この例では、AutoSIM で AT&T のファームウェアが選択されています。

上記の構成を実行した後、execモードのコマンドを使用して特定のファームウェアをアクティブにします。新しいファームウェアのロードには最大120秒かかります。ファームウェアを手動で指定するアクションの例を次に示します。

モデムファームウェアのアップロードとアップグレード

始める前に

次の手順を使用して、モデムのファームウェアをアップグレードしてからアップグレードします。

- モデムのファームウェアを格納するサブディレクトリを作成します。
- そのディレクトリにファームウェアファイルをコピーします。
- 次のコマンドを発行してアップグレードプロセスを完了します。

ステップ 1 **gw-action:request file**

例：

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

ステップ 2 **gw-action:request file copy source**

例：

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

ステップ 3 cellular 1 upgrade firmware firm_new

例：

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

DM ロギングの有効化

このセクションでは、5G および 4G のワイドエリアネットワーク（WAN）Cisco Catalyst セルラーゲートウェイの診断モニター（DM）ログを有効にして収集する手順について説明します。DM ロギング情報を確認するためのさまざまなコマンドを参照することもできます。

DM ロギングを求められたときは、次の構成を使用して有効にします。

（注） この構成は、エンジニアリングから具体的なガイダンスがあったとき以外は実行しないでください。シスコのエンジニアリングリソースから正確なコマンドラインオプションが提供されます。

ステップ 1 conf t

例：

```
Device# conf t
```

ステップ 2 controller cellular 1

例：

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

ステップ 3 dm log enable

例：

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

ステップ 4 commit

例：

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

ステップ 5 end

例：

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

次のタスク

次のコマンドを使用して、DM ログを収集します。

```
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
```

Web ベースのインターフェイスを使用した Cisco Catalyst セルラーゲートウェイの設定

Cisco Catalyst セルラーゲートウェイの Web ベースのユーザーインターフェイスに関する情報

Cisco Catalyst セルラーゲートウェイは、物理ポートを使用してデバイスに接続されています。Web ベースのユーザーインターフェイス機能は、設定を実行するための支援ツールとして機能し、デバイスのステータスとパフォーマンスのモニタリングにも役立ちます。

Cisco Catalyst セルラーゲートウェイの Web ベースのユーザーインターフェイスに関する制約事項

Cisco Catalyst セルラーゲートウェイの Web ベースのユーザーインターフェイスについて、Web ベースのユーザーインターフェイスの設定に関する既知の制約事項はありません。

Cisco Catalyst セルラーゲートウェイの Web ベースのユーザーインターフェイスのログインとログアウト

Cisco Catalyst セルラーゲートウェイの Web ベースのユーザーインターフェイスにログインするには、Web ブラウザでリンク（http://192.168.1.1:8008、https://192.168.1.1:8008）を開きます。初めてのユーザーの場合、デフォルトのユーザー名は **admin** で、デフォルトのパスワードはデバイスで提示される**シリアル番号**です。ログインプロンプトにログイン情報（**ユーザー名**、**パスワード**）を入力します。デフォルトの**ダッシュボード**が開き、デバイスのステータスの概要が表示されます。

Cisco Catalyst セルラーゲートウェイの Web ベースのユーザーインターフェイスからログアウトするには、**ダッシュボード**で **[Logout]** をクリックします。

Cisco Catalyst セルラーゲートウェイのステータスの表示

メインメニューから **[Dashboard]** を選択します。

ダッシュボードには、デバイスのステータスの概要と次の情報が表示されます。

フィールド	説明
CPU 使用率	CPU使用状況（**アイドル**時間（青）、**ユーザー**の使用状況（黄）、**システム**の使用状況（緑）で構成）を、タイムスタンプ付きでグラフィカルに表示します。グラフ上にマウスポインタを合わせると、使用状況（パーセンテージでキャプチャ）が表示されます。
メモリ使用率	**使用中**（青）、**空き**（オレンジ）、**合計**（緑）の使用率を示す、メモリの使用状況（パーセンテージ）を表示します。
システム情報	デバイスの現在のシステム時刻、シリアル番号、デバイスモデル ID、デバイスの稼働時間、デバイスのホスト名、ビルドバージョン、およびその他のデバイス固有の情報を表示します。
システム温度	システムの温度を度単位で示すメーターグラフを表示します。
ディスク使用率	空き（青）と使用中（緑）のディスク容量をキャプチャした合計使用状況グラフを表示します。

デバイスアクティビティのモニタリング

メインメニューから **[Monitoring]** を選択します。

[Monitoring] ページには次の情報が表示されます。

フィールド	説明
Polling Time	設定した時間間隔で更新された統計を表示します。
信号強度チャート	デバイスに挿入されている SIM カードの信号強度を示すグラフを表示します。グラフ上にマウスポインタを置くと、詳細な SIM 情報が表示されます。

フィールド	説明
ハードウェア	ゲートウェイに挿入されているモデムのハードウェアおよびファームウェア情報を表示します。
Network	システム時刻と携帯電話ネットワーク情報が表示されます。
無線機	モデムへの接続で形成されたセルラー無線情報を表示します。
セルラーの詳細	IP アドレス、サブネットマスク、IPv4 および IPv6 DNS アドレス、モデムステータスなどのすべてのセルラー情報が含まれています。

Web ベースのユーザーインターフェイスを使用した Cisco Catalyst セルラーゲートウェイの設定

[Configuration] ページでは、モデムと SIM スロットの設定ができます。このページには、アクセスポイント名（APN）のプロファイルを管理および設定するオプションがあります。

1. メインメニューから **[Configuration]** > **[Cellular]** タブを選択し、**[Click to configure]** リンクをクリックします。

   • **[Cellular Configuration]** ページで、**[General]** ウィンドウを使用して診断モニター（DM）ログを設定します。

フィールド	説明
Auto-SIM	トグルボタンをクリックして、このオプションを有効にします。
Enable Logging	DM ログの収集に役立ちます。
DM ログのステータス	トラブルシューティングのために DM ログをダウンロードできます。
[Rotation]	このトグルを有効にすると、デバイスは最大 DM ログサイズに達するまで、それぞれ最大サイズが 20 MB の DM ログファイルを収集します。最大ログサイズに達すると、最も古い DM ファイルが削除され、新しい DM ログファイル用のストレージスペースが提供されます。

フィールド	説明
最大 DM ログサイズ	DM ログを収集するために、60 MB から 600 MB までのサイズを入力できます。ログがこのサイズに達すると、デバイスはDMログデータの収集を停止します。
自動停止イベント	DM ログの収集を停止するイベントを選択します。 • MODEM_STATE_IP_ACQUIRED：デバイスモデムはサービスプロバイダーから IP アドレスを受け取りましたが、MODEM_STATE_DNS_ACQUIRED 状態に達していません。 • MODEM_STATE_DNS_ACQUIRED：デバイスはインターネットに接続し、IP アドレスを取得しました。 • MODEM_STATE_SESSION_CONNECT：デバイスはネットワークの切断と再接続を繰り返しています。 • MODEM_STATE_ATTACHED_AND_REGISTERED：パケットデータネットワーク（PDN）IP アドレスへの接続中にエラーが発生しました。 • MODEM_STATE_NETWORK_READY：デバイスモデムはネットワークに接続できませんでした。 • MODEM_STATE_DISCONNECTED：デバイスがモデムの問題を検出しました。
フィルタパス	DM ログフィルタファイルを保存するためにブートフラッシュまたはフラッシュの場所を追加します。
自動停止タイマー	自動停止イベントの後、DM ログの収集を停止するまで待機するように、1～120 秒の範囲のタイマーを設定できます。

[Save] をクリックして、新たに変更した DM ログパラメータをアクティブにします。

- **[SIM]** ウィンドウで、**SIM** と**スロット**の設定を行います。**[SIM]** を選択し、ドロップダウンから **[SIM Primary]** をクリックします。

フィールド	説明
アクティブ SIM	ドロップダウンから、アクティブにする必要のある SIM スロットに応じて 0 または 1 を選択します。
フェールオーバータイマー	失敗した場合にデバイスが接続を試みるように、1 から 7 までのタイマーを設定できます。
Max Retry	許容される再接続の試行回数を定義できます。

[Save] をクリックして、新たに変更したパラメータをアクティブにします。

- **[SIM]** ドロップダウンから、**[Slot]** をクリックします。

フィールド	説明
SIM スロット	デバイスでどの SIM スロットを有効にする必要があるかに応じて、0 または 1 を選択します。
プロファイルの付加	最大 16 個のプロファイルを作成できます。ドロップダウンから付加するプロファイルを選択します。
データプロファイル	ドロップダウンから、付加して利用する現在のプロファイルを選択します。

[Save] をクリックして、新たに変更したパラメータをアクティブにします。

[Profiles] ページでは、複数のユーザープロファイルを作成、編集、および削除できます。

1. メインメニューから **[Configuration]** > **[Profiles]** タブを選択し、**[Add]** をクリックして新しいプロファイルを作成します。

フィールド	説明
プロファイル ID	ID は 1～16 の範囲で設定できます。
APN 名	名前を文字列形式で追加します。

フィールド	説明
PDN タイプ	ドロップダウンから IPv4 または IPv6 アドレスを選択します。 • **認証**： 1. 認証が [**none**] に設定されている場合、ユーザー名またはパスワードを追加する必要はありません。 2. 認証が [**CHAP**]、[**PAP**]、[**PAP** or **CHAP**] と設定されている場合は、ユーザー名とパスワードを追加する必要があります。
ユーザー名	新しい認証ユーザー名を入力します。
Password	新しい認証パスワードを入力します。

[Save] をクリックして、新たに変更したパラメータをアクティブにします。

ログイン パスワードの変更

1. メインメニューから **[Administration]** > **[Users]** を選択します。
2. 3 つの省略記号 > **[Change Password]** をクリックします。
3. **[Submit]** をクリックして、新たに変更したパスワードをアクティブにします。

コマンド ライン インターフェイスを使用したデバイス情報の表示

コマンドラインインターフェイス（CLI）は、デバイスのすべての設定を表示するためのものです。これはデバッグやトラブルシューティングに必要となります。詳細を表示するために、show コマンドを実行できます。

1. メイン メニューから、**[Administration]** > **[Command Line Interface]** を選択します。

2.**[Command Line Interface]** ページの **[Exec]** フィールドに **show** コマンドを入力して **Enter** キーを押します。使用可能なすべてのコマンドのリストがインターフェイスに表示されます。

その他のオプション

1. トラブルシューティングの目的で使用できるディスプレイページで、**[Download Admin Tech Logs]** をクリックします。

2. **[Settings]** アイコンをクリックし、**[Preferences]** で、**[Light]** モードまたは **[Dark]** モードのラジオボタンをクリックしてテーマを変更します。
3. **[Save]** をクリックして、新たに変更したパラメータをアクティブにします。

ネットワーク アドレス変換（NAT）の設定

ネットワークアドレス変換（NAT）機能により、プライベート IP アドレスをパブリック IP アドレスに変換できます。このデバイスは、IP パススルーモードと NAT モードの 2 つの動作モードで構成されています。セルラーゲートウェイのデバイスでは、IP パススルーがデフォルトモードであり、NAT モードに切り替えることができます。Cisco Catalyst セルラーゲートウェイのデバイスで NAT を有効にすると、接続されたデバイスが DHCP サーバーとローカルゲートウェイにアクセスできるようになります。

ネットワークアドレス変換（NAT）の設定の前提条件

ネットワークアドレス変換（NAT）の設定に必要な前提条件はありません。

ネットワークアドレス変換（NAT）の設定に関する制約事項

最大 16 のポートアドレス変換（PAT）ルールをデバイスに設定できます。

ネットワークアドレス変換（NAT）の設定に関する情報

Cisco Catalyst セルラーゲートウェイのデバイスは、IP パススルーモードの 1 つのホストデバイスでのみ使用できます。このモードでは、デバイスは接続されたホストと WAN IP アドレスを共有します。一方、ゲートウェイモードでは、デバイスは NAT モードで機能します。

Cisco Catalyst セルラーゲートウェイでのネットワークアドレス変換（NAT）の設定

NAT を使用して Cisco Catalyst セルラーゲートウェイのデバイスを設定するには、次の手順を実行します。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**gw-system:system passthrough false** 例： `Device> gw-system:system passthrough false`	NAT モードを有効にします。デフォルトの IP アドレスは 10.0.23.0/24 です。デフォルトの IP アドレスプールを変更するには、手順 3 に従います。
ステップ 2	**commit** 例： `Device# commit`	この手順を実行すると、デバイスは NAT モードで有効になります。ステップ 3 に進みます。
ステップ 3	**gw-system: ip dhcp pool network** *network-number* | *subnet-mask* 例： `Device(config)# gw-system: ip dhcp pool network 192.0.2.0/24`	（オプション）DHCP アドレスプールのサブネットネットワーク番号とマスクを指定します。
ステップ 4	**gw-system:ip dhcp excluded-address** *low-address high-address* 例： `Device(config-if)# gw-system:ip dhcp excluded-address 192.0.2.1 192.0.2.11`	（オプション）低 IP アドレスと高 IP アドレスを設定して、特定の IP アドレスを除外します。デフォルトの DHCP アドレスプールは 10.0.23.0/24 です。
ステップ 5	**gw-system:ip dhcp pool lease-time** *days hours minutes* 例： `Device(config-if)# gw-system:ip dhcp pool lease-time 2 20 50`	（オプション）リース時間を設定します。デフォルトのリース時間は 24 時間です。
ステップ 6	**gw-system:ip nat inside source static tcp** *ip-address local-port***interface***interface-nameport-number* 例： `Device(config-if)# gw-system:ip nat inside source static tcp 192.0.2.2 2022 interface GigabitEthernet 0/0 22`	（オプション）IPv4 アドレスを使用して PAT（ポートフォワーディング）ルールを設定します。
ステップ 7	**no gw-system:ip nat inside source static tcp** *ip-address local-port***interface***interface-nameport-number* 例： `Device(config-if)# no gw-system:ip nat inside source static tcp 192.0.2.2 2022 interface GigabitEthernet 0/0 22`	（オプション）アクティブな設定から PAT ルールを削除して、NAT ポートフォワーディングを無効にします。

	コマンドまたはアクション	目的
ステップ 8	**show gw-system:ip dhcp binding** 例： `Device(config-if)# show gw-system:ip dhcp binding`	セルラーゲートウェイのデバイスに接続されているクライアントデバイスのリストを確認します。

Cisco Catalyst セルラーゲートウェイでの WAN セキュアシェル（SSH）の設定

Cisco Catalyst セルラーゲートウェイでの WAN セキュアシェル（SSH）の設定の前提条件

- WAN SSH を設定するには、セルラーゲートウェイのデバイスで NAT モードを有効にする必要があります。
- WAN SSH を設定するには、サービスプロバイダーが発行したセルラー スタティック パブリック IP アドレスの使用が必須です。

Cisco Catalyst セルラーゲートウェイでの WAN セキュアシェル（SSH）の設定に関する制約事項

- 最大 16 のポートアドレス変換（PAT）ルールをデバイスに設定できます。
- SSH のデフォルトのタイムアウトはゲートウェイで 30 分に設定されており、それを過ぎるとセッションは自動的に切断されます。

WAN SSH を使用した Cisco Catalyst セルラーゲートウェイの設定

WAN SSH を使用して Cisco Catalyst セルラーゲートウェイのデバイスを設定するには、次の手順を実行します。

手順の概要

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*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**config**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**gw-system:system passthrough false**	NAT モードを有効にします。
ステップ 3	**gw-system: ip dhcp pool network** *ip-addresssubnet-mask*	（オプション）Cisco Catalyst セルラーゲートウェイの IPv4 アドレスを使用して、DHCP サーバーと DHCP プールを設定します。
ステップ 4	**gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*	IPv4 アドレスを使用して PAT（ポートフォワーディング）ルールを設定します。
ステップ 5	**show gw-system ip dhcp binding**	Cisco Catalyst セルラーゲートウェイに接続されているクライアントを確認します。
ステップ 6	**no gw-system: ip nat inside source static tcp** *ip-addresslocal-port***interface***interfacenat-port*	アクティブな設定から PAT ルールを削除して、SSH へのアクセスを無効にします。

PAT ルールを使用した WAN SSH の有効化に関する情報

手順の概要

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*

手順の詳細

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

Cisco Catalyst セルラーゲートウェイで SSH を有効にするには、次のコマンドを使用して PAT ルールを設定します。

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

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

セルラーゲートウェイに接続されているクライアントデバイスへの SSH セッションを確立する必要がある場合は、PAT ルールを設定し、DHCP サーバーによって割り当てられた IPv4 アドレスを使用し、次のコマンドを使用して隣接するクライアントデバイスに接続します。

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

Cisco Catalyst セルラーゲートウェイでのポートアドレス変換（PAT）の確認

デバイスの PAT ルールを確認するには、次のコマンドを使用します。

手順の概要

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

手順の詳細

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
```

（注） Cisco Catalyst セルラーゲートウェイ、または Cisco Catalyst セルラーゲートウェイに接続されたクライアントデバイスへの SSH セッションを確立するには、セルラー パブリック スタティック IPv4 アドレスを使用します。ダイナミックセルラー IP アドレスは、ゲートウェイデバイスへの SSH セッションの有効化には機能しないことに注意してください。

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

例

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

ゲートウェイに接続されたデバイスに SSH で接続するには、次のコマンドを使用します。

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

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

システム ログ機能の設定

システム ログ機能の設定

イベント通知システムログ（syslog）メッセージは、ローカルデバイス上のファイルに記録したり、リモートホストに送信したりできます。

システム ロギングの設定に関する前提条件

リモートロギングサーバーは、Cisco Catalyst セルラーゲートウェイから到達可能である必要があります。

システムロギングの設定に関する制約事項

システムロギングには最大 4 つのサーバーを設定できます。

システムロギングの設定に関する情報

- デフォルトでは、syslog メッセージを「情報」の優先度とともにローカルデバイスのハードディスクにロギングできるようになっています。
- ログファイルは、ローカルディスクの /var/log ディレクトリにあります。

ローカルデバイスでのシステム ログ デフォルト パラメータのロギング

ローカル デバイスで syslog のデフォルトパラメータを変更するには、次のコマンドを実行します。

手順の概要

1. **gw-system:system loggingdisk**|**server**
2. **enable**
3. **file rotate***number***size***megabytes*
4. **severity** シビラティ（重大度）
5. **source-interface-ip address***ip address*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**gw-system:system loggingdisk**|**server**	syslog メッセージを情報の優先度とともにローカルデバイスのハードディスクまたはサーバーにロギングできるようにします。
ステップ 2	**enable**	ローカルディスクへのロギングを有効にします。
ステップ 3	**file rotate***number***size***megabytes*	**ローテーション**：しきい値の 10 ファイルに達すると、最も古いファイルが削除され、新しい syslog メッセージ用に新しいファイルが作成されます。 **サイズ**：ログファイルのデフォルトサイズは 10MB です。1MB から 20MB の範囲で設定できます。

	コマンドまたはアクション	目的
ステップ 4	**severity** シビラティ（重大度）	シビラティ（重大度）を informational レベルである「デフォルト」から別のレベルに変更します。
ステップ 5	**source-interface-ip address***ip address*	リモート syslog サーバーに表示されるソースインターフェイス IP を設定します。

合計 10 個の syslog ファイルが作成されます。**rotate** コマンドを使用すると、このサイズを 1 ～ 10 の任意の値に設定できます。

デフォルトのシビラティ（重大度）値は「informational」であるため、デフォルトでは、すべてのsyslogメッセージが記録されます。シビラティ（重大度）には次のいずれかを指定できます（シビラティ（重大度）の高い順）。

- **Emergency**：システム使用不可（syslog シビラティ（重大度）0 に相当）
- **Alert**：ただちに対処が必要（syslog シビラティ（重大度）1 に相当）
- **Critical**：深刻な状態（syslog シビラティ（重大度）2 に相当）
- **Error**：システムのユーザビリティを完全に損なうことはないエラー状態（syslog シビラティ（重大度）3 に相当）
- **Warn**：軽微なエラー状態（syslog シビラティ（重大度）4 に相当）
- **Normal**：正常だが重大な状態（syslog シビラティ（重大度）5 に相当）
- **Information**：ルーチンの状態（デフォルト）（syslog シビラティ（重大度） 6 に相当）

ローカルデバイスのシステムロギングパラメータの無効化

リモートサーバーへのsyslogメッセージのロギングを無効にするには、次のコマンドを実行します。

手順の概要

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

手順の詳細

no gw-system:system logging disk enable

例：

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

リモートデバイスでのシステムログメッセージのロギング

イベント通知 syslog メッセージをリモートホストに記録するには、次のコマンドを使用してサーバーに関する情報を設定します。

手順の概要

1. **gw-system:system loggingserver**{*dns-name*|*hostname*|*ip-address*}
2. **severity** シビラティ（重大度）

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**gw-system:system loggingserver**{*dns-name*|*hostname*|*ip-address*}	DNS 名、ホスト名、または IP アドレスでサーバーの場所を設定します。
ステップ 2	**severity** シビラティ（重大度）	サーバーに送信する syslog メッセージの優先順位を設定します。

例

例

イベント通知 syslog メッセージをリモートホストに記録するには、次のコマンドを使用します。

```
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
```

リモートデバイスのシステムロギングパラメータの無効化

リモートサーバーへのsyslogメッセージのロギングを無効にするには、次のコマンドを実行します。

手順の概要

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

手順の詳細

no gw-system:system logging server

例：

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

システムのログファイル

デフォルトまたは設定された syslog メッセージの優先度の値は、**/var/log** ディレクトリ内のいくつかのファイルに記録されます。

- **auth.log**：ログイン、ログアウト、スーパーユーザーのアクセスイベント、および承認システムの使用状況。
- **kern.log**：カーネルメッセージ。
- **messages**：すべてのソースからの syslog メッセージが記録された統合ログファイル。
- **vdebug**：デバッグ機能が有効になっているモジュールのすべてのデバッグメッセージと、設定された優先度の値を超えるすべての syslog メッセージが、/var/log/tmplog/ vdebug ファイルに保存されます。デバッグロギングは、モジュールに基づいてさまざまなレベルのロギングをサポートします。実装されているロギングレベルは、モジュールごとに異なります。

  たとえば、システムマネージャ（sysmgr）には 2 つのロギングレベル（オンとオフ）があり、シャーシマネージャ（chmgr）には 4 つの異なるロギングレベル（オフ、低、標準、高）があります。デバッグメッセージをリモートホストに送信することはできません。デバッグを有効にするには、**debug** 操作コマンドを使用します。
- **vsyslog**：セルラーゲートウェイのプロセス（デーモン）からの syslog メッセージで、設定された優先度の値を超えるものはすべて、/var/log/vsyslog ファイルに保存されます。デフォルトのプライオリティ値は「informational」であるため、デフォルトでは「notice」、「warning」、「error」、「critical」、「alert」、および「emergency」のすべての syslog メッセージが保存されます。
- **daemon**.**log**：すべての起動、生成および再起動されるデーモンのライフサイクル情報。

セルラーゲートウェイのソフトウェアは、/var/log にある標準の Linux ファイル（cron.log、debug、lpr.log、mail.log、syslog）をロギングに使用しません。

例

セルラーゲートウェイのソフトウェアによって生成される syslog メッセージの形式は次のとおりです。

ローカルディスクに保存されるローカルログ：

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

リモートサーバー上のリモートログ：

次に、syslog メッセージの例を示します。ファイルでは、このメッセージは 1 行になります。

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

TACACS（Terminal Access Controller Access Control System）の設定

TACACS（Terminal Access Controller Access Control System）の概要

TACACS は、ユーザーによるルータまたはネットワーク アクセス サーバーへのアクセス試行の集中的な確認を可能にするセキュリティアプリケーションです。ネットワーク アクセス サーバーに設定した TACACS 機能を使用可能にするには、TACACS サーバーにアクセスして TACACS サーバーを設定しておく必要があります。

TACACS は、個別のモジュール式認証機能を備えています。TACACS では、単一のアクセス コントロール サーバー（TACACS）で各サービスの認証を行うことができます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理する方法を提供することです。アクセス サーバーおよびルーティングのシスコ ファミリおよび（ルータとアクセス サーバー両方の）Cisco IOS および Cisco IOS XE ユーザー インターフェイスは、ネットワーク アクセス サーバーにすることができます。

ネットワーク アクセス ポイントによって、従来の「低機能な」端末、端末エミュレータ、ワークステーション、パーソナル コンピュータ（PC）、およびルータと、適切なアダプタ（たとえば、モデムまたは ISDN アダプタ）を併用して、Point-to-Point Protocol（PPP）、Serial Line Internet Protocol（SLIP）、Compressed SLIP（CSLIP）、または AppleTalk Remote Access（ARA）プロトコルを使用する通信が可能になります。つまり、ネットワーク アクセス サーバーは、単一のユーザー、ネットワークまたはサブネットワーク、および相互接続したネットワークに対して、接続を提供できます。ネットワーク アクセス サーバを介して接続されているエンティティは、ネットワーク アクセス クライアントと呼ばれます。たとえば、音声グレードの回路で PPP を実行する PC は、ネットワーク アクセス クライアントです。TACACS は、AAA セキュリティサービスによって管理され、次のようなサービスを提供できます。

• 認証：ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージングのサポートによって、認証の完全制御を行います。

認証機能には、ユーザーに任意のダイアログを実行する機能があります（たとえば、ログインとパスワードの指定後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号などの複数の質問をユーザーに試行する機能）。さらに、TACACS 認証サービスは、ユーザー画面へのメッセージ送信をサポートします。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

TACACS プロトコルは、ネットワーク アクセス サーバーと TACACS の間に認証機能を提供します。また、ネットワーク アクセス サーバーと TACACS 間のすべてのプロトコル交換が暗号化されるため、機密性を確保できます。

ネットワーク アクセス サーバーで TACACS 機能を使用するには、TACACS ソフトウェアを実行するシステムが必要です。

独自の TACACS ソフトウェアの開発に関心があるお客様のために、シスコでは、TACACS プロトコル仕様をドラフトの RFC として使用できるようにしています。

TACACS の設定に関する前提条件

TACACS サーバーは、Cisco Catalyst セルラーゲートウェイから到達可能である必要があります。

TACACS の設定に関する制約事項

TACACS の設定に必要な制約事項はありません。

AAA 認証フォールバックおよび認証順序の設定

AAA 認証フォールバックおよび認証順序の設定例を以下に示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**gw-system:system aaa**	
ステップ 2	**auth-fallbackauth-ordertacacslocal**	**auth-fallbackauth-ordertacacslocal** は、ローカル認証と TACACS 認証の両方を設定します。TACACS サーバーが使用できない場合は、ローカル認証をフォールバックとして使用できます。

Cisco Catalyst セルラーゲートウェイの TACACS の設定

次の例は、TACACS のサンプル設定です。

手順

	コマンドまたはアクション	目的
ステップ 1	**gw-system:system tacacs server***ip-address*	1 つ以上の TACACS サーバーの IP アドレスを指定します。
ステップ 2	**auth-port***port-number***secret-key**	• TACACS サーバーへの接続時に使用する TCP ポート番号を指定します。デフォルト ポート番号は 49 です。 • セルラーゲートウェイと TACACS デーモン間のすべてのトラフィックを暗号化および暗号解除

	コマンドまたはアクション	目的
		するための暗号化キーを指定します。暗号化を成功させるために、TACACS サーバーで同じキーを設定します。 secret-key コマンドを使用して、ネットワークアクセス サーバーと TACACS サーバーの間のすべてのやり取りの暗号化に使用する暗号化キーを指定します。TACACS サーバーでこのキーを設定します。
ステップ 3	**source-interface** *interface*	すべての発信 TACACS パケットに対して、プライマリインターフェイスを指定します。
ステップ 4	**priority** *value*	各 TACACS サーバーの優先度を指定します。ゼロはデフォルトの優先度値であり、最も優先順位の高い TACACS サーバーになります。セルラーゲートウェイが最も優先順位の高いサーバーとの接続を確立できない場合、スイッチは次に優先順位の高いサーバーとの接続を確立しようとします。範囲は 0 ～ 7 です。
ステップ 5	**gw-system:system tacacs timeout** *value*	ゲートウェイがタイムアウトしてエラーを宣言するまで、TACACS からの応答を待つ時間（秒）を指定します。デフォルトの数値は 5 で、1～1000 の間で設定できます。

IP 送信元アドレスの違反

セルラーゲートウェイには、送信元アドレスが DHCP サーバーから DHCP クライアントに提供されたアドレスでない受信トラフィックをすべて破棄する機能があります。この機能により、ブロードキャストの送信元、マルチキャストの送信元、または潜在的な攻撃者からサービス拒否の試みとしてセルラーゲートウェイにトラフィックが送信されるシナリオでセルラーの帯域幅を削減できます。

（注） この機能を非アクティブ化する方法も示してありますが、非アクティブ化することはお勧めしません。

ステップ 1 **configure terminal**

例：

```
CellularGateway# configure terminal
```

ステップ 2　controller cellular 1

例：

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

ステップ 3　ip-source-violation-action ipv4-permit

例：

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

ステップ 4　ip-source-violation-action ipv6-permit

例：

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

ステップ 5　commit

例：

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

ステップ 6　end

例：

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

次のタスク

この機能が有効になっているときに破棄されたパケットは、次のコマンドで確認できます。

```
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
```

ステップ 1　configure terminal

例：

```
CellularGateway# configure terminal
```

ステップ 2　controller cellular 1

例：

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

ステップ 3　no ip-source-violation-action ipv4-permit

例：

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

ステップ 4 **no ip-source-violation-action ipv6-permit**

例：

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

ステップ 5 **commit**

例：

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

ステップ 6 **end**

例：

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

次のタスク

IPv4v6 IP 送信元違反の許可アクションが削除されているかどうかを表示するには、次のコマンドを使用します。

```
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
```

Catalyst セルラーゲートウェイの検証

セルラーゲートウェイのハードウェアの情報を確認するには、**show cellular 1 hardware** コマンドを使用します。

ステップ 1 **show cellular 1 hardware**

例：

```
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) = zzzzzzzzzzzzzzzzzzzz
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
```

ステップ 2 controller cellular 1

例：

```
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
```

次のタスク

（注） セルラー無線のバージョンとセルラーの SIM 識別子がハイライトされています。

CLI を使用してセルラー無線の状態に関する具体的な情報を取得できます。

Catalyst セルラーゲートウェイの構成例

定義済みプロファイルのチェック

ロードされるファームウェアには、構成モードで定義されたプロファイルが関連付けられています。AutoSIM 機能によって異なるファームウェアがロードされるため、定義されたプロファイルが変わることがあります。以前にカスタム APN プロファイルが作成されたファームウェアがロードされると、以前に定義されたプロファイルが復元され、そのファームウェアに関連付けられていたプロファイルが置き換えられます。

次の CLI を使用して、ロードされたファームウェアに対して現在定義されているすべてのプロファイルを確認できます。最初の例は、AT&T SIM が SIM スロット 0 でアクティブだったときの出力を示しています。

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

Verizon SIM に強制的にフェールオーバーした後、次のプロファイルが自動的に提供されます。

```
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     -         -
```

セルラーゲートウェイのインターフェイス

セルラーゲートウェイのインターフェイスに関する詳細情報を取得するには、次のコマンドを使用します。

```
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
```

（注） ハイライトされているアドレスは、サービスプロバイダーから取得されて、接続されたクライアントに DHCP を介して提供されたものです。