Cisco Catalyst IR1101 高耐久性シリーズ ルータ ソフトウェア設定ガイド

初版：2018 年 5 月 18 日

最終更新：2023 年 1 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/

Full Cisco Trademarks with Software License

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

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

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

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

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

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

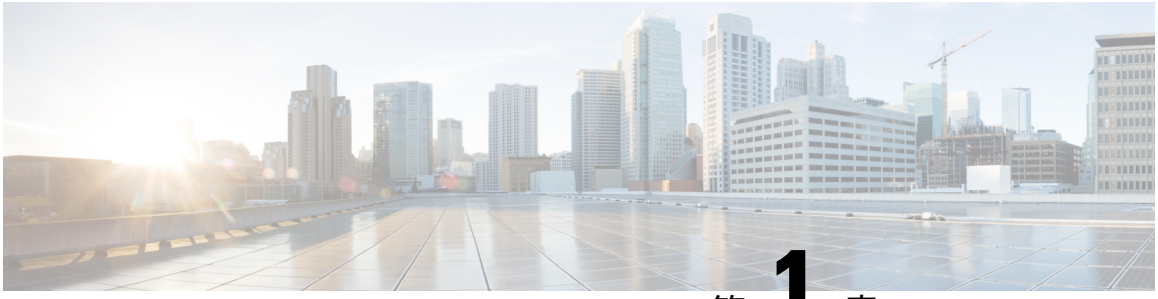
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

Full Cisco Trademarks with Software License



第 1 章

はじめに

Cisco Catalyst IR1101 高耐久性シリーズルータは、ベースモジュールを備えた次世代のモジュール型産業用ルータで、プラガブルモジュールを追加できます。プラガブルモジュールは、IR1101 プラットフォームに様々なインターフェイスを追加できる柔軟性を実現します。

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

IR1101 には、デュアル LTE プラガブル、mSATA SSD FRU、SFP、追加のイーサネットおよび非同期ポート、デジタル GPIO 接続などの重要な機能を追加する拡張モジュールも 2 つ用意されています。

IR1101 は、Cisco IOS XE オペレーティング システムを実行する初の IoT プラットフォームです。IOS-XE は Linux ベースの OS で、多数の機能が強化され、従来の IOS バージョンと比較して多くの機能を備えています。

ガイドのこの項には、次の内容も含まれています。

IR1101 ベースルータ

次の図は、IR1101 の前面パネルを示し、その一部の機能を強調表示しています。

図 *1 : IR1101* の前面パネル

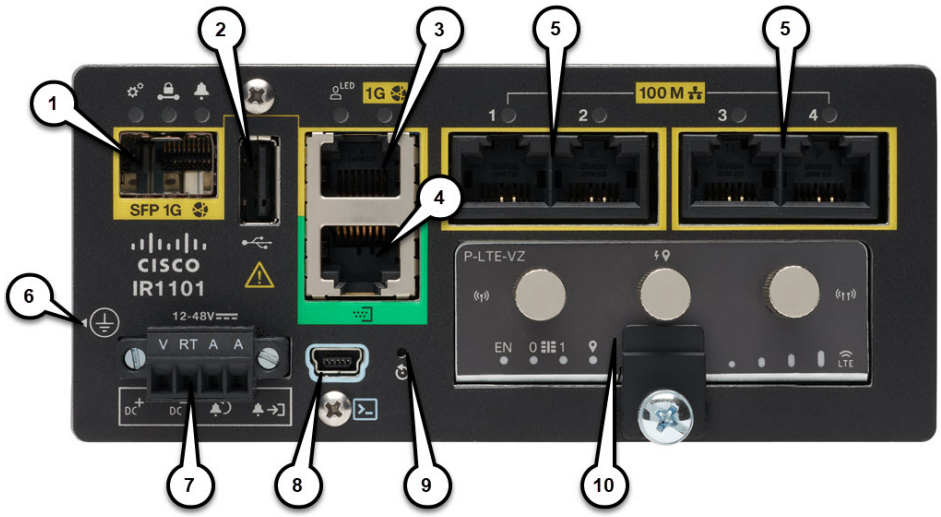


表 *1 :* 前面パネルの説明

項目	説明
1	SFP GigE WAN ポート（次の #3 のコンボ ポート）
2	タイプ A USB 2.0 ホスト ポート
3	RJ45 GigE WAN ポート（上記 #1 のコンボ ポート）
4	非同期シリアル ポート（DTE のみ）
5	RJ45 ファスト イーサネット LAN ポート
6	接地点 （デバイスの側面）
7	DC 電源およびアラーム入力
8	タイプ B ミニ USB コンソール ポート
9	リセット ボタン
10	プラガブル モジュール スロット（例：4G/LTE モジュール）

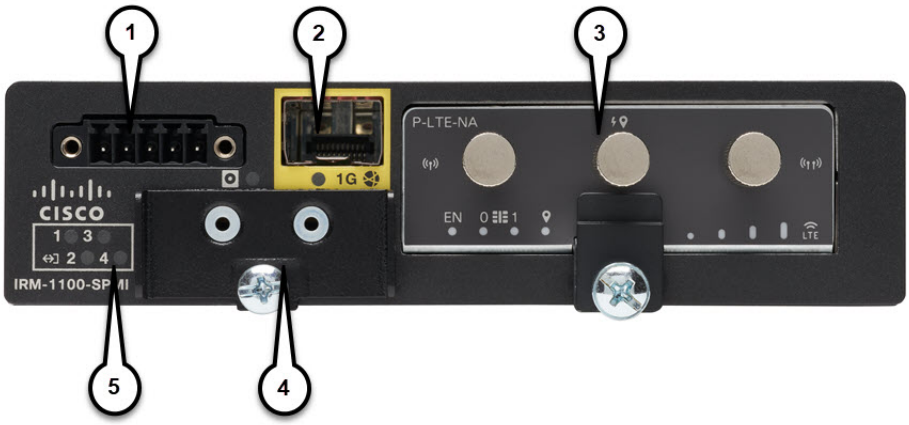
IRM-1100 拡張モジュール

拡張モジュールには、次の 2 つのタイプがあります。

- IRM-1100-SPMI
- IRM-1100-SP

次の図は、IRM-1100-SPMI の前面パネルを示し、その機能の一部を強調表示しています。

図 *2 : IR-1100-SPMI* 拡張モジュールの詳細



項目	説明
1	4 GPIO + 1 リターン（デジタル I/O） （注）　機能は Cisco IOS-XE リリース 16.12.1 以降で使用できます。
2	SFP コネクタ
3	プラガブルモジュール
4	mSATA SSD スロット
5	デジタル I/O LED

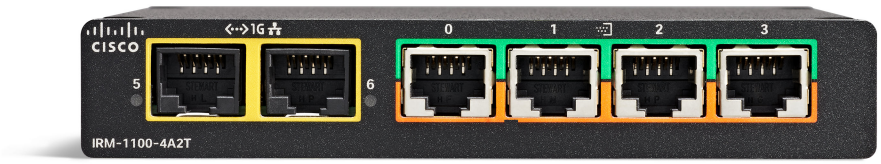
IR-1100-SP 拡張モジュールは、デジタル I/O および mSATA コンポーネントを持たない点以外は、IR-1100-SPMI モジュールと同じです。

詳細については、IRM-1101 拡張モジュール （305 ページ）を参照してください。

IR1101 の詳細については、製品データシートを参照してください。

IRM-1100-4A2T 拡張モジュール

IRM-1100-4A2T は、IR1101 に取り付けることのできる拡張モジュールです。IR1101 への追加の 4 つの非同期シリアルポートと 2 つのイーサネット インターフェイスを提供します。次の図は、IRM-1100-4A2T を示しています。



IRM-1100-4A2T イーサネット インターフェイスは、レイヤ 2 RJ45 10/100/1000 Mbps ポートです。

IRM-1100-4A2T シリアルポートは、RJ45 コンボポート（RS232/RS485/RS422）です。

IR1101 には、拡張モジュールを取り付けられる側面が 2 つあります。上部は拡張側、下部はコンピューティング側と呼ばれます。追加モジュールが上部に接続されている場合は、拡張モジュール（EM）側として参照されます。追加モジュールが下部に接続されている場合は、コンピューティング モジュール（CM）側として参照されます。機能は、拡張モジュールがどちら側に取り付けられているか、および使用されている拡張モジュールの数と種類によって異なります。

IRM-1100-4A2T は、次のツールから管理できます。

- Cisco DNA Center
- WebUI

詳細については、IRM-1100-4A2T 拡張モジュール （319 ページ）を参照してください。

- ルータ コンソールを使用して CLI にアクセスする方法 （4 ページ）
- リモート コンソールから CLI にアクセスする方法 （7 ページ）
- CLI セッション管理 （9 ページ）

ルータ コンソールを使用して CLI にアクセスする方法

Cisco IR1101 ルータには、USB のみに対応しているコンソール ポートがあります。コンソール ケーブル（Cisco P/N CAB-CONSOLE-USB、 長さ 6 フィート）は含まれていないため、注文する必要があります。

コンソール ポートは、シャーシの前面パネルにある USB 2.0 ミニ USB タイプ B コネクタです。デフォルトのボー レートは 9600 です。

ルータと通信する適切なドライバがないという警告がラップトップやPCに表示された場合は、ドライバをコンピュータ メーカーから入手するか、または次の URL を参照してください。
https://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

工場出荷時のデバイスでは、システム設定ダイアログが表示されるため、基本的な設定の質問に回答してください。Cisco PnP 接続サービスを使用するためにルータを注文した場合、中央集中型プロビジョニングでは、ルータは最初のダイアログをスキップします。次に、例を示します。

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: <your-host-name>

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: <your-password>

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: <your-password>

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: <your-password>
Setup account for accessing HTTP server? [yes]: <return>
    Username  [admin]: <your-username>
    Password  [cisco]: <your-password>
    Password is UNENCRYPTED.
  Configure SNMP Network Management? [no]: <return>

Current interface summary

Any interface listed with OK? value "NO" does not have a valid configuration

Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      NO  unset  up                    up
FastEthernet0/0/1      unassigned      YES unset  down                  down
FastEthernet0/0/2      unassigned      YES unset  down                  down
FastEthernet0/0/3      unassigned      YES unset  down                  down
FastEthernet0/0/4      unassigned      YES unset  up                    up
Async0/2/0             unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  up                    up
```

（注） この次のセクションの名前と IP アドレスは例として示されています。

```
Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface Vlan1:
  Configure IP on this interface? [no]: yes
    IP address for this interface: 192.168.1.1
    Subnet mask for this interface [255.255.255.0] : <return>
    Class C network is 192.168.1.0, 24 subnet bits; mask is /24

Would you like to configure DHCP? [yes/no]: yes
 Enter DHCP pool name: wDHCPool
 Enter DHCP network: 192.168.1.0
 Enter DHCP netmask: 255.255.255.0
 Enter Default router: 192.168.1.1

The following configuration command script was created:

hostname <your-hostname>
enable secret 9 $9$Z6fl74fvoEdMgU$XZYs8l4phbqpXsb48l9bzCng3u4Bc2kh1STsoLoHNes
enable password <your-enable-password>
line vty 0 4
password <your-password>
username <your-username> privilege 15 password <your-password>
no snmp-server
!
!
interface GigabitEthernet0/0/0
shutdown
no ip address
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
!
interface Vlan1
no shutdown
ip address 192.168.1.1 255.255.255.0
no mop enabled
ip dhcp pool wDHCPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
end


[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
Building configuration...

[OK]
```

```
Use the enabled mode 'configure' command to modify this configuration.


Press RETURN to get started! <return>


*Jul 27 21:35:24.369: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-3211716068
 has been generated or imported by crypto-engine
*Jul 27 21:35:24.372: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jul 27 21:35:24.448: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified.  Issue "write
 memory" to save new IOS PKI configuration
*Jul 27 21:35:24.532: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named
TP-self-signed-3211716068.server has been generated or imported by crypto-engine
hostname>
```

これでデバイスに構築可能な基本設定ができました。

コンソール インターフェイスの使用方法

ステップ 1 次のコマンドを入力します。

```
Router > enable
```

ステップ 2 （イネーブル パスワードが設定されていない場合は、ステップ 3 に進みます）パスワード プロンプトで、システム パスワードを入力します。

```
Password: enablepass
```

パスワードが許可されると、特権 EXEC モード プロンプトが表示されます。

```
Router#
```

これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。

ステップ 3 コンソール セッションを終了するには、**quit** コマンドを入力します。

```
Router# quit
```

リモート コンソールから CLI にアクセスする方法

IR1101 のリモート コンソールには、Telnet またはよりセキュアな SSH を使用してアクセスできます。telnet アクセスの詳細については、この章の以降の項を参照してください。SSH アクセスの詳細については、SSH の章を参照してください。

ここでは、リモート コンソールから CLI にアクセスする手順について説明します。

Telnet を使用してルータ コンソールに接続するための準備

詳細については、https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.htmlの Cisco IOS-XE デバイス強化ガイドを参照してください。

診断バナーおよび待機バナーの設定は任意ですが、設定することを推奨します。バナーは、特に Telnet または SSH 試行ステータスをユーザに示すインジケータとして役立ちます。

TCP/IP ネットワークから Telnet を使用してルータにリモート アクセスするには、**line vty** グローバル コンフィギュレーション コマンドを使用して、仮想端末回線をサポートするようにルータを設定します。ユーザに対してログインとパスワードの指定を要求するように、仮想端末回線を設定します。

line vty グローバル コンフィギュレーション コマンドの詳細については、『Cisco IOS Terminal Services Command Reference』ドキュメントを参照してください。

回線上でログインが無効化されないようにするには、**login** コマンドの設定時に **password** コマンドを使ってパスワードを指定します。

認証、認可、アカウンティング（AAA）を使用する場合は、**login authentication** コマンドを設定します。login authentication コマンドを使用してリストを設定するときに、回線上で AAA 認証に関するログインが無効化されないようにするには、**aaa authentication login** グローバル コンフィギュレーション コマンドを使用して、リストを設定する必要もあります。

AAA サービスの詳細については、『Cisco IOS XE Security Configuration Guide: Secure Connectivity』および『Cisco IOS Security Command Reference』を参照してください。**login line-configuration** コマンドの詳細については、『Cisco IOS Terminal Services Command Reference』を参照してください。

また、ルータに Telnet 接続する前に、ルータの有効なホスト名、またはルータに設定された IP アドレスを取得しておく必要もあります。Telnet を使用してルータに接続するための要件の詳細、Telnet サービスのカスタマイズ方法、および Telnet キー シーケンスの使用方法については、『Cisco IOS Configuration Fundamentals Configuration Guide』を参照してください。

Telnet を使用してコンソール インターフェイスにアクセスする方法

ステップ 1 端末または PC から次のいずれかのコマンドを入力します。

- **connect host** *[port] [keyword]*
- **telnet host** *[port] [keyword]*

ここで、*host* にはルータのホスト名または IP アドレスを指定し、*port* には 10 進数のポート番号（デフォルトは 23）を指定します。また、*keyword* にはサポートされるキーワードを指定します。これらのコマンドの詳細については、『Cisco IOS Terminal Services Command Reference』を参照してください。

（注） アクセスサーバを使用する場合は、ホスト名または IP アドレスに加えて、有効なポート番号（たとえば **telnet 172.20.52.40 2004**）を指定します。

次に、**telnet** コマンドを使用して、**router** という名前のルータに接続する例を示します。

```
unix_host% telnet router
Trying 172.20.52.40...
Connected to 172.20.52.40.
Escape character is '^]'.
unix_host% connect
```

ステップ 2 ログイン パスワードを入力します。

```
User Access Verification
Password: mypassword
```

（注） パスワードが設定されていない場合は、Return を押します。

ステップ 3 ユーザ EXEC モードから、**enable** コマンドを入力します。

```
Router> enable
```

ステップ 4 パスワード プロンプトで、システム パスワードを入力します。

```
Password: enablepass
```

ステップ 5 **イネーブル** パスワードが許可されると、特権 EXEC モード プロンプトが次のように表示されます。

```
Router#
```

ステップ 6 これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。

ステップ 7 Telnet セッションを終了するには、**exit** または **logout** コマンドを使用します。

```
Router# logout
```

CLI セッション管理

非アクティブ タイムアウトを設定して、強制的に適用することができます。セッション ロックにより、2 人のユーザが別々に行った変更を相互に上書きできないように保護できます。使用可能なすべてのキャパシティが内部プロセスによって使用されるのを防ぐために、CLI セッション アクセス用に予備の容量が予約されています。たとえば、これによりユーザはルータにリモート アクセスすることができます。

CLI セッション管理について

非アクティブ タイムアウトを設定して、強制的に適用することができます。セッション ロックにより、2 人のユーザがそれぞれ行った変更を相互に上書きできないように保護できます。使用可能なすべてのキャパシティが内部プロセスによって使用されるのを防ぐために、CLI セッション アクセス用に予備の容量が予約されています。たとえば、これによりユーザはルータにリモート アクセスできます。

CLI セッション タイムアウトの変更

ステップ 1 **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 **line console 0**

ステップ 3 **session-timeout** *minutes*

minutes の値により、タイムアウトになるまでの CLI の待機時間が設定されます。CLI セッション タイムアウトを設定すると、CLI セッションのセキュリティが強化されます。*minutes* に値 0 を指定すると、セッション タイムアウトが無効になります。

ステップ 4 **show line console 0**

セッション タイムアウトとして設定された値を確認します（"Idle Session" の値として表示されます）。

CLI セッションのロック

始める前に

CLI セッションの一時パスワードを設定するには、EXEC モードで **lock** コマンドを使用します。**lock** コマンドを使用するには、その前に **lockable** コマンドを使用して回線を設定する必要があります。次の例では、回線が **lockable** として設定され、その後 **lock** コマンドを使用して一時パスワードが割り当てられます。

ステップ 1 **Router# 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 **lock** コマンドを使用できるようにする回線を入力します。

```
Router(config)# line console 0
```

ステップ 3 **Router(config)# lockable**

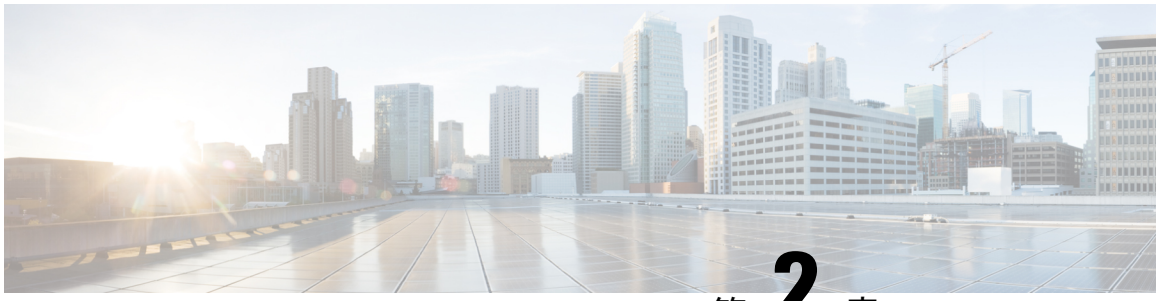
回線をロック可能にします。

ステップ 4 **Router(config)# exit**

ステップ 5 **Router# lock**

パスワードの入力が求められます。パスワードを 2 回入力する必要があります。

```
Password: <password>
Again: <password>
Locked
```



第 2 章

Cisco IOS XE ソフトウェアの使用

Cisco SDWAN テクノロジーを利用する場合は、Cisco IOS-XE SDWAN イメージ（cEdge）には異なるコマンドモードがあることに注意してください（Config-transaction、commit など）。

IR1101 SDWAN の機能は、cEdge IOS-XE 16.12.1 の機能に沿っています。URL フィルタリングや IPS/IDS など、一部の機能は IR1101 では使用できない場合があります。また、IR1101 の一部の機能は SDWAN イメージからは使用できない場合があります。

次の SDWAN のマニュアルを確認してください。 https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html%0A

この章は、次の項で構成されています。

コマンド モードについて

Cisco IOS XE で使用できるコマンド モードは、従来の Cisco IOS で使用できるコマンド モードと同じです。Cisco IOS XE ソフトウェアにアクセスするには、CLI を使用します。CLI には複数のモードがあることから、利用できるコマンドはその時点で利用しているモードにより異なります。CLI プロンプトでクエスチョン マーク（**?**）を入力すると、それぞれのコマンド モードで利用できるコマンドの一覧を取得できます。

CLI にログインしたときのモードはユーザ EXEC モードです。ユーザ EXEC モードでは、使用できるコマンドが制限されています。すべてのコマンドを使用できるようにするには、通常はパスワードを使用して、特権 EXEC モードを開始する必要があります。特権 EXEC モードからは、すべての EXEC コマンド（ユーザ モードまたは特権モード）を実行できます。また、グ

ローバル コンフィギュレーション モードを開始することもできます。ほとんどの EXEC コマンドは 1 回限りのコマンドです。たとえば、**show** コマンドであれば重要なステータス情報が表示され、**clear** コマンドであれば、カウンタやインターフェイスがクリアされます。EXEC コマンドはソフトウェアの再起動時に保存されません。

コンフィギュレーションモードでは、実行コンフィギュレーションを変更できます。その後、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しておくと、変更されたコマンドはソフトウェアの再起動後も保存されます。特定のコンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードでは、インターフェイス コンフィギュレーション モード、およびプロトコル専用モードなどその他のモードを開始できます。

ROM モニタ モードは、Cisco IOS XE ソフトウェアが適切にロードしない場合に使用される別個のモードです。ソフトウェアの起動時、または起動時にコンフィギュレーション ファイルが破損している場合に、有効なソフトウェア イメージが見つからなければ、ソフトウェアは ROM モニタ モードを開始することがあります。

次の表に、Cisco IOS XE ソフトウェアのさまざまな一般的なコマンド モードへのアクセス方法、またはアクセスを終了する方法について説明します。また、各モードで表示されるプロンプトの例も示します。

表 *2:* コマンド モードのアクセス方法および終了方法

コマンド モード	アクセス方法	プロンプト	終了方法
ユーザー EXEC	ログインします。	`Router>`	**logout** コマンドを使用します。
特権 EXEC	ユーザ EXEC モードから、**enable** コマンドを使用します。	`Router#`	ユーザ EXEC モードに戻るには、**disable** コマンドを使用します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure terminal** コマンドを使用します。	`Router(config)#`	グローバル コンフィギュレーション モードから特権 EXEC モードに戻るには、**exit** or **end** コマンドを使用します。
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを使用してインターフェイスを指定します。	`Router(config-if)#`	グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。 特権 EXEC モードに戻るには、**end** コマンドを使用します。

コマンド モード	アクセス方法	プロンプト	終了方法
診断	ルータは、次のような場合に、診断モードを開始するか、または診断モードにアクセスします。 • 場合によっては、Cisco IOS プロセスで障害が発生したときに、診断モードが開始することがあります。ただし、ほとんどの場合、ルータはリロードされます。 • ユーザが **transport-map** コマンドを使用して設定したポリシーにより、診断モードが開始する場合があります。 • ブレーク信号（**Ctrl-C**、**Ctrl-Shift-6**、または **send break** コマンド）を入力すると、ブレーク信号を受信したルータが診断モードに移行するように設定されている場合があります。	`Router(diag)#`	Cisco IOS プロセスの障害によって診断モードが開始された場合は、Cisco IOS の問題を解決したあとで、ルータを再起動して診断モードを解除する必要があります。 ルータが transport-map 設定によって診断モードを開始した場合、ルータにアクセスするには、別のポートを使用するか、または Cisco IOS CLI に接続するよう設定された方法を使用します。

コマンド モード	アクセス方法	プロンプト	終了方法
ROM モニタ	特権 EXEC モードで、**reload** EXEC コマンドを使用します。システムの起動時、最初の 60 秒以内に **Break** キーを押します。	`rommon#>`	ROM モニタ モードを終了するには、有効なイメージを手動でブートするか、または自動ブートを設定してリセットを実行し、有効なイメージがロードされるようにします。

キーボードのショートカット

コマンドには、大文字と小文字の区別はありません。また、コマンドおよびパラメータは、現在使用可能な他のコマンドまたはパラメータと区別可能な文字数まで省略できます。

次の表に、コマンドの入力および編集に使用するキーボード ショートカットを示します。

表 *3:* キーボードのショートカット

キー名	目的
Ctrl-B または←キー [1]	カーソルを 1 文字分だけ後ろに戻します。
Ctrl-F または→キー [1]	カーソルを 1 文字分だけ前に進めます。
Ctrl+A	カーソルをコマンドラインの先頭に移動させます。
Ctrl+E	カーソルをコマンドラインの末尾に移動させます。
Esc B	カーソルを 1 ワード分だけ後ろに戻します。
Esc F	カーソルを 1 ワード分だけ前に進めます。

コマンドの no 形式および default 形式の使用

ほぼすべてのコンフィギュレーション コマンドに **no** 形式があります。一般には、**no** 形式を使用して機能を無効にします。無効化されている機能を再び有効にしたり、デフォルトで無効な機能を有効にするには、**no** キーワードを指定しないでコマンドを使用します。たとえば、IP ルーティングはデフォルトで有効です。IP ルーティングを無効にするには、**no ip routing** コマンドを使用します。IP ルーティングを再び有効にするには、**ip routing** コマンドを使用します。Cisco IOS ソフトウェアのコマンド リファレンスには、コンフィギュレーション コマンドの完全な構文、および **no** 形式のコマンドの機能が記載されています。

多くの CLI コマンドには **default** 形式もあります。*<command>* **default** command-name を発行すると、コマンドをデフォルト設定に戻すことができます。Cisco IOS ソフトウェア コマンド リファレンスでは、プレーン形式や **no** 形式のコマンドとは異なる機能が **default** 形式のコマンドで実行される場合の、**default** 形式の機能が説明されています。システムで使用できるデフォルト コマンドを表示するには、該当するコマンド モードで **default?** と入力します。

履歴バッファによるコマンドの呼び出し

履歴バッファには、直前に入力した 20 のコマンドが保存されます。特別な省略コマンドを使用して、再入力せずに保存されているコマンドにアクセスできます。

次の表に、ヒストリ置換コマンドの一覧を示します。

表 *4:* ヒストリ置換コマンド

コマンド	目的
Ctrl+P または↑キー [1]	履歴バッファ内のコマンドを呼び出します。最後に実行したコマンドが最初に呼び出されます。キーを押すたびに、より古いコマンドが順次表示されます。
Ctrl+N または↓キー [1]	**Ctrl+P** または↑キーでコマンドを呼び出した後で、履歴バッファ内のより新しいコマンドに戻ります。
Router# show history	EXEC モードで、最後に入力したいくつかのコマンドの一覧を表示します。

[1] 矢印キーを使用できるのは、VT100 などの ANSI 互換端末に限られます。

コンフィギュレーション ファイルの管理

スタートアップ コンフィギュレーション ファイルは nvram: ファイル システムに保存され、実行コンフィギュレーション ファイルは system: ファイル システムに保存されます。このコンフィギュレーション ファイルの保存設定は、他のいくつかのシスコ ルータ プラットフォームでも使用されています。

IOS XE では、コンフィギュレーション ファイルの暗号化が可能です。暗号化については、次の URL から入手可能な IOS XE デバイス強化ガイドで詳しく説明されています。
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

シスコ ルータの日常的なメンテナンスの一環として、スタートアップ コンフィギュレーション ファイルを NVRAM から他のいずれかのルータ ファイル システムにコピーし（さらに追加でネットワーク サーバにもコピーして）、バックアップをとっておく必要があります。スタートアップコンフィギュレーションファイルをバックアップしておくと、何らかの理由でNVRAM

上のスタートアップ コンフィギュレーション ファイルが使用できなくなったときに、スタートアップ コンフィギュレーション ファイルを簡単に回復できます。

スタートアップ コンフィギュレーション ファイルのバックアップには、**copy** コマンドを使用できます。

コンフィギュレーション ファイルの管理の詳細については、『Cisco IOS XE Configuration Fundamentals Configuration Guide』の「Managing Configuration Files」の項を参照してください。

コンフィギュレーションの変更の保存

設定の変更をスタートアップ コンフィギュレーションに保存して、ソフトウェアのリロードや停電が発生した場合に変更内容が失われないようにするには、**copy running-config startup-config** コマンドを使用します。次に例を示します。

```
Router# copy running-config startup-config
Building configuration...
```

設定の保存に数分かかることがあります。設定が保存されると、次の出力が表示されます。

```
[OK]
Router#
```

この作業により、設定が NVRAM に保存されます。

show コマンドおよび more コマンドの出力のフィルタリング

show および **more** コマンドの出力を検索してフィルタリングできます。この機能は、大量の出力を並べ替える必要がある場合や、不要な出力を除外する場合に役立ちます。

この機能を使うには、**show** または **more** コマンドに「パイプ」記号（|）を続け、**begin**、**include**、**exclude** のキーワードのいずれかを入力します。さらに検索またはフィルタリングの内容を正規表現で指定します（大文字と小文字は区別されます）。

show | {**append** | **begin** | **exclude** | **include** | **redirect** | **section** | **tee**} *regular-expression*

この出力は、コンフィギュレーション ファイル内の情報の特定の行に一致します。

例

この例では、**show interface** コマンドの修飾子（**include protocol**）を使用して、式 **protocol** が表示される出力行のみを示します。

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is administratively down, line protocol is down (disabled)
0 unknown protocol drops
FastEthernet0/0/1 is down, line protocol is down (notconnect)
0 unknown protocol drops
FastEthernet0/0/2 is down, line protocol is down (notconnect)
0 unknown protocol drops
```

```
FastEthernet0/0/3 is down, line protocol is down (notconnect)
0 unknown protocol drops
FastEthernet0/0/4 is down, line protocol is down (notconnect)
0 unknown protocol drops
GigabitEthernet0/0/5 is up, line protocol is up (connected)
0 unknown protocol drops
Cellular0/1/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/1/1 is administratively down, line protocol is down
0 unknown protocol drops
Cellular0/3/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/3/1 is administratively down, line protocol is down
0 unknown protocol drops
Async0/2/0 is up, line protocol is down
0 unknown protocol drops
Vlan1 is up, line protocol is up , Autostate Enabled
0 unknown protocol drops
Vlan172 is up, line protocol is down , Autostate Enabled
0 unknown protocol drops
Vlan175 is down, line protocol is down , Autostate Enabled
0 unknown protocol drops
IR1101#
```

プラットフォームおよびシスコ ソフトウェアイメージのサポート情報の検索

Cisco IOS XE ソフトウェアは、特定のプラットフォームをサポートするソフトウェアイメージで構成されるフィーチャ セットとしてパッケージ化されています。

Cisco IOS-XE コンフィギュレーション ガイドはすべて以下で確認できます。
https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-16/tsd-products-support-series-home.html

特定のプラットフォームでどのフィーチャセットのグループを使用できるかは、リリースに含まれるシスコ ソフトウェア イメージによって異なります。特定のリリースで使用できる一連のソフトウェアイメージを特定したり、ある機能が特定の Cisco IOS XE ソフトウェアイメージで使用できるかどうかを確認するには、Cisco Feature Navigator を使用するか、または https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-16/products-release-notes-list.html を参照します。

Cisco Feature Navigator の使用

プラットフォームのサポートおよび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 は、特定のソフトウェアリリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できるツールです。Navigator ツールを使用するには、Cisco.com のアカウントは必要ありません。

ヘルプの表示

CLI プロンプトで疑問符（**?**）を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。またコンテキスト ヘルプ機能を使用すると、コマンドに関連するキーワードと引数のリストを取得できます。

コマンドモード、コマンド、キーワード、または引数に固有のヘルプを表示するには、次のコマンドのいずれかを使用します。

コマンド	目的
help	コマンドモードのヘルプ システムの概要を示します。
abbreviated-command-entry?	特定の文字ストリングで始まるコマンドのリストが表示されます （注） コマンドと疑問符の間にスペースは不要です。
abbreviated-command-entry<Tab>	特定のコマンド名を補完します。
?	特定のコマンド モードで使用できる全コマンドの一覧を表示します。
command ?	コマンドラインで次に入力する必要のあるキーワードまたは引数が表示されます （注） コマンドと疑問符の間にスペースを挿入してください。

コマンド オプションの検索：例

ここでは、コマンド構文の表示方法について説明します。コマンド構文には、任意または必須のキーワードおよび引数が含まれています。コマンドのキーワードおよび引数を表示するには、コンフィギュレーション プロンプトで疑問符（?）を入力するか、またはコマンドの一部を入力した後に 1 スペース空けて、疑問符（**?**）を入力します。Cisco IOS XE ソフトウェアにより、使用可能なキーワードおよび引数のリストと簡単な説明が表示されます。たとえば、グローバル コンフィギュレーション モードで **arap** コマンドのすべてのキーワードまたは引数を表示するには、**arap ?** と入力します。

コマンド ヘルプ出力の中の <cr> 記号は改行を表します。古いキーボードでは、CR キーは **Return** キーです。最近のキーボードでは、CR キーは **Enter** キーです。コマンド ヘルプの最後の <cr> 記号は、**Enter** キーを押してコマンドを完成させるオプションがあること、および <cr> 記号に先行するリスト内の引数およびキーワードはオプションであることを示します。<cr> 記号だけの場合は、使用可能な引数またはキーワードが他に存在せず、**Enter** キーを押してコマンドを完成させる必要があることを示します。

次の表に、コマンド入力支援のために疑問符（**?**）を使用する例を示します。

表 *5:* コマンド オプションの検索

コマンド	コメント
Router> **enable** Password: <password> Router#	**enable** コマンドとパスワードを入力して、特権 EXEC コマンドにアクセスします。プロンプトが「>」から「#」に変わったら（例：Router> から Router#）、特権 EXEC モードに切り替わっています。
Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	**configure terminal** 特権 EXEC コマンドを入力して、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。グローバル コンフィギュレーション モードが開始されると、プロンプトが Router(config)# に変わります。
Router(config)# interface GigabitEthernet ? <0-0> GigabitEthernet interface number Router(config)# interface GigabitEthernet 0/? <0-5> Port Adapter number Router (config)# interface GigabitEthernet 0/0/? <0-63> GigabitEthernet interface number Router (config)# interface GigabitEthernet 0/0/0? . <0-71> Router(config-if)#	インターフェイス コンフィギュレーション モードを開始するには、**interface GigabitEthernet** グローバル コンフィギュレーション コマンドを使用して、設定するインターフェイスを指定します。 次にコマンド ラインに入力する必要があるコマンドを表示するには、**?** と入力します。 <cr> 記号が表示されている場合は、**Enter** キーを押してコマンドを完了できます。 インターフェイス コンフィギュレーション モードが開始されると、プロンプトが Router(config-if)# に変わります。

コマンド	コメント

Router(config-if)# **?**
Interface configuration commands:
  .
  .
  .
  ip Interface Internet Protocol
  config commands
  keepalive Enable keepalive
  lan-name LAN Name command
  llc2 LLC2 Interface Subcommands
  load-interval Specify interval for load calculation
  for an interface
  locaddr-priority Assign a priority group
 	
  logging Configure logging for interface
  loopback Configure internal loopback on an
  interface
  mac-address Manually set interface MAC address
  mls mls router sub/interface commands
  mpoa MPOA interface configuration commands
  mtu Set the interface Maximum Transmission Unit (MTU)
  netbios Use a defined NETBIOS access list
  or enable name-caching
  no Negate a command or set its defaults
  nrzi-encoding Enable use of NRZI encoding
  ntp Configure NTP
  .
  .
  .
Router(config-if)#
	インターフェイスに使用できるすべてのインターフェイス コンフィギュレーション コマンドのリストを表示するには、**?**を入力します。次の例では、使用可能なインターフェイス コンフィギュレーション コマンドの一部だけを示しています。

コマンド	コメント
Router(config-if)# **ip ?** Interface IP configuration subcommands: access-group Specify access control for packets accounting Enable IP accounting on this interface address Set the IP address of an interface authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit broadcast-address Set the broadcast address of an interface cgmp Enable/disable CGMP directed-broadcast Enable forwarding of directed broadcasts dvmrp DVMRP interface commands hello-interval Configures IP-EIGRP hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures IP-EIGRP hold time . . . Router(config-if)# **ip**	インターフェイスの設定のためのコマンドを入力します。この例では、**ip** コマンドを使用します。 次にコマンド ラインに入力する必要があるコマンドを表示するには、**?**と入力します。次の例では、使用可能なインターフェイス IP コンフィギュレーション コマンドの一部だけを示しています。
Router(config-if)# **ip address ?** A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# **ip address**	インターフェイスの設定のためのコマンドを入力します。この例では、**ip address** コマンドを使用しています。 次にコマンド ラインに入力する必要があるコマンドを表示するには、**?**と入力します。この例では、IP アドレスまたは **negotiated** キーワードを入力する必要があります。 改行（<cr>）は表示されません。このため、コマンドを完成させるには、追加のキーワードまたは引数を入力する必要があります。

コマンド	コメント
Router(config-if)# ip address 172.16.0.1 ? A.B.C.D IP subnet mask Router(config-if)# **ip address 172.16.0.1**	使用するキーワードまたは引数を入力します。この例では、IP アドレスとして 172.16.0.1 を使用しています。 次にコマンド ラインに入力する必要があるコマンドを表示するには、**?** と入力します。この例では、IP サブネット マスクを入力する必要があります。 <cr> は表示されません。このため、コマンドを完成させるには、追加のキーワードまたは引数を入力する必要があります。
Router(config-if)# **ip address 172.16.0.1 255.255.255.0 ?** secondary Make this IP address a secondary address <cr> Router(config-if)# **ip address 172.16.0.1 255.255.255.0**	IP サブネット マスクを入力します。この例では、IP サブネット マスク 255.255.255.0 を使用しています。 次にコマンド ラインに入力する必要があるコマンドを表示するには、**?** と入力します。この例では、**secondary** キーワードを入力するか、Enter キーを押します。 <cr> が表示されます。Enter キーを押してコマンドを完了するか、または別のキーワードを入力します。
Router(config-if)# **ip address 172.16.0.1 255.255.255.0** Router(config-if)#	Enter キーを押してコマンドを完了します。

Software Advisor の使用

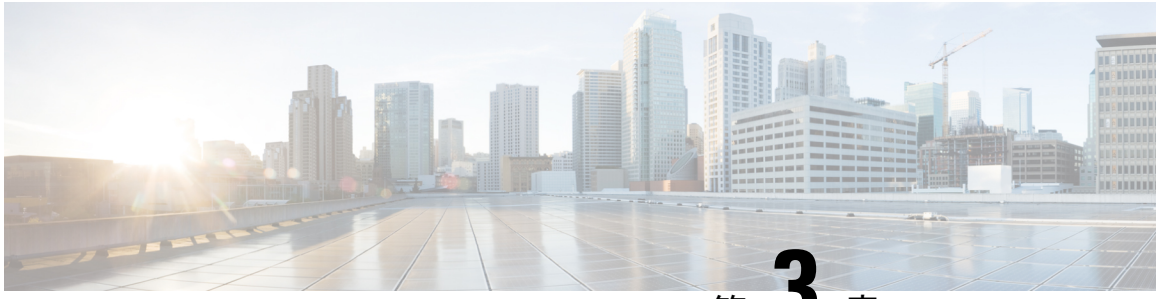
シスコは Software Advisor ツールを維持しています。「Tools and Resources」を参照してください。Software Advisor ツールを使用すると、ある機能が Cisco IOS XE リリースでサポートされているかどうか確認したり、その機能のソフトウェア マニュアルを検索したり、ルータに装着されているハードウェアでの Cisco IOS XE ソフトウェアの最小ソフトウェア要件を確認することができます。このツールにアクセスするには、Cisco.com の登録ユーザである必要があります。

ソフトウェア リリース ノートの使用

次の詳細については、リリース ノートを参照してください。

- メモリに関する推奨事項
- 重大度 1 および 2 の未解決および解決済みの注意事項

リリース ノートには、最新のリリースに固有の情報が記載されています。これらの情報には、以前のリリースに記載済みの機能に関する情報が含まれていないことがあります。機能に関するこれまでのすべての情報については、Cisco Feature Navigator（http://www.cisco.com/go/cfn/）を参照してください。



第 3 章

ルータの基本的な CLI 設定

この章は、次の項で構成されています。

IR1101 インターフェイスの命名

サポートされているハードウェア インターフェイスとその命名規則は、次の表に記載されています。

ハードウェア インターフェイス	命名ルール
ギガビット イーサネット コンボ ポート	gigabitethernet 0/0/0
ファスト イーサーネット ポート	fastethernet0/0/1-0/0/4
セルラー インターフェイス	cellular 0/1/0 and cellular 0/1/1
非同期シリアル インターフェイス	async 0/2/0
USB	usbflash0:
mSATA	msata

ハードウェア インターフェイス	命名ルール
IR1101 ベースユニットアラーム入力	alarm contact 0

さまざまな拡張モジュールのインターフェイス名は、次の章にあります。

- IRM-1100-4A2T 拡張モジュール （319 ページ）
- IRM-1101 拡張モジュール （305 ページ）

基本設定

基本設定は、初期設定ダイアログ中に作成したエントリの結果です。つまり、ルータには、WebUI を介して、または PnP プロセスを動作させるために、IP アドレスが到達可能なインターフェイスが少なくとも 1 つ設定されていることを意味します。初期設定を表示するには、次の例に示すように、**show running-config** コマンドを使用します。

```
Router# show running-config
Building configuration...

Current configuration : 8079 bytes
!
! Last configuration change at 17:33:19 GMT Tue Jun 25 2019
!
version 16.12
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service internal
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname IR1101
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone GMT 0 0
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact
email address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
!
ip name-server 171.70.168.183 198.224.173.135 8.8.8.8
no ip domain lookup
ip domain name cisco.com
!
login on-success log
ipv6 unicast-routing
```

```
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
chat-script hspa-R7 "" "AT!SCACT=1,1" TIMEOUT 60 "OK"
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
crypto pki trustpoint TP-self-signed-756885843
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-756885843
 revocation-check none
 rsakeypair TP-self-signed-756885843
!
!
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
   quit
crypto pki certificate chain TP-self-signed-756885843
 certificate self-signed 01
  3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 37353638 38353834 33301E17 0D313930 35333130 30303530
  385A170D 33303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3735 36383835
  38343330 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
  82010100 D2F61742 3B651909 95856431 9BC2CCB7 D4B04861 DD6E0924 4C3E6A51
  8BF2ABD9 5C3A597D 2EE0112C ECA615AA D0297F9E 071B6B5D 9B831332 021E61F4
  2352EEC9 EE70742E 46EFBAFC A03744D8 A22E4DA3 AAF919CC 0A7929A7 3BDB3B17
  C04DA5B9 028DD3EC 992493A6 EA864ED6 354CB3F4 094D3EBF 5307CAA3 192B5759
  E458712D 841A43CD 709D4D9E 72A9DE3E F935A688 59B6F278 65B59EE0 6B72469E
  7B97582A 64E511A6 D81735FF 117CE399 4C2A2973 F5FD407D BCEB62A6 FD7C6B08
  882E0749 ACE5BD44 32634790 3607ADEA 9F319343 4CA76B0D B1DE6A1C AD144548
  E38119E2 8B34F7AC 090C0450 03166B42 8C7C9EA7 5132687F E1F7BF6E B065CD4E
  889F02BB 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
  0603551D 23041830 16801405 77954127 36509205 7025CF4E 84B5D4A2 A3D53730
  1D060355 1D0E0416 04140577 95412736 50920570 25CF4E84 B5D4A2A3 D537300D
  06092A86 4886F70D 01010505 00038201 01004147 49C6A0A9 56F5BD4D 4892AEE0
```

```
  22955E06 AF192FA6 868D5556 959ACF05 398F3907 DFE3148B 0E2CFC12 20BEEA05
  DC23E8D7 A47DB4AE D6CB6665 BCAE7F39 24D010F0 DB8F0E70 5E7C3F73 25AB1783
  1346D540 47BB7E89 2BB1BE4D 16990318 A4612CC5 C7CC9376 7DF1A1F4 C09C0051
  4D950D99 3CC0C65B 0A98859A 3B81E324 BAB34EDF 64CA8C38 184DC796 47DDD9DD
  F71F8D5E D3B7A962 3D0FDE44 012AC034 D0E7F75A DB1BF12A CF23E2F5 6A4FDA14
  A588DCDA 8272CE33 36ABC57A BFF52980 5FFC7C34 4D4307BB AC0C0F18 AA783B9D
  27C61E89 0EC1C6AA 6AB3F73B EF8450FD 782DFC63 038F6A27 456CA32B D3FEDB97
  C8064523 EBB93FF5 8B98B546 44F853E9 0E04
   quit
!
license udi pid IR1101-K9 sn FCW222700KS
diagnostic bootup level minimal
!
spanning-tree extend system-id
memory free low-watermark processor 50357
file prompt quiet
!
!
username cisco privilege 15 password 0 cisco
username lab password 0 lab123
!
redundancy
!
!
controller Cellular 0/1/0
 no lte firmware auto-sim
 lte modem link-recovery disable
!
controller Cellular 0/3/0
!
vlan internal allocation policy ascending
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
!
interface FastEthernet0/0/1
 switchport access vlan 192
 switchport mode access
!
interface FastEthernet0/0/2
 switchport access vlan 172
 switchport mode access
!
interface FastEthernet0/0/3
 switchport access vlan 172
!
interface FastEthernet0/0/4
 switchport mode access
!
interface GigabitEthernet0/0/5
!
interface Cellular0/1/0
 ip address negotiated
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
!
interface Cellular0/1/1
```

```
 no ip address
 shutdown
!
interface Cellular0/3/0
 ip address negotiated
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 2
 ipv6 enable
 pulse-time 1
 ip virtual-reassembly
!
interface Cellular0/3/1
 no ip address
 shutdown
!
interface Vlan1
 ip address 192.168.10.15 255.255.255.0
!
interface Vlan172
 ip address 172.27.167.121 255.255.255.128
!
interface Vlan175
 ip address 175.1.1.1 255.255.255.0
!
interface Async0/2/0
 no ip address
 encapsulation scada
!
ip default-gateway 172.27.167.1
ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 172.27.167.1
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 253
ip route 8.8.4.0 255.255.255.0 Cellular0/3/0
ip route 171.70.0.0 255.255.0.0 172.27.167.1
ip route 192.1.1.0 255.255.255.0 Cellular0/1/0
ip route 192.168.193.0 255.255.255.0 192.168.10.1
!
!
ip access-list standard 1
 10 permit any
dialer watch-list 1 ip 5.6.7.8 255.255.255.255
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer watch-list 2 ip 5.6.7.8 255.255.255.255
dialer watch-list 2 delay route-check initial 60
dialer watch-list 2 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
ipv6 route ::/0 Cellular0/1/0
!
!
snmp-server community public RO
snmp-server community private RW
snmp-server host 171.70.127.43 version 2c public
snmp-server host 172.27.167.220 version 2c public
snmp-server manager
!
control-plane
```

```
!
line con 0
 exec-timeout 0 0
 stopbits 1
 speed 115200
line 0/0/0
line 0/2/0
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
 transport input none
!
!
end

IR1101#
```

グローバル パラメータの設定

ルータのグローバル パラメータを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`Router> enable`
	`Router# configure terminal`
	`Router(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（コンソール ポート使用時）。
		次のコマンドを使用して、ルータとリモート ターミナルを接続します。
		`telnet router-name or address`
		`Login: login-id`
		`Password: *********`
		`Router> enable`

ステップ 2	**hostname** *name* 例： `Router(config)# hostname Router`	ルータ名を指定します。
ステップ 3	**enable password** *password* 例： `Router(config)# enable password cr1ny5ho`	ルータへの不正なアクセスを防止するには、パスワードを指定します。 （注） この形式のコマンドでは、パスワードは暗号化されません。パスワードを暗号化するには、前述のデバイス強化ガイドに記載されているように、イネーブル シークレット パスワードを使用します。

ギガビット イーサネット インターフェイスの設定

IR1101 上のギガビットイーサネット インターフェイス (GI0/0/0) のデフォルト設定は、レイヤ 3 (L3) です。そのインターフェイスを、レイヤ 2（L2）インターフェイスとして設定することが可能です。IR1101 のギガビット イーサネット インターフェイスはコンボ ポートであり、これは RJ45+SFP コネクタであることを意味します。

IRM-1100-SPMI 拡張モジュールには SFP ポートも搭載されています。IRM-1100-SPMI のギガビット イーサネット インターフェイス（GI0/0/5）は、レイヤ 2（L2）のみです。つまり、このポートを任意の VLAN（switchport acc vlan #）に割り当てて SVI インターフェイスを使用できます。このポート直下に IP アドレスを割り当てることはできません。

正しいコネクタを選択する必要があります。次の場所にある『Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide』[英語] を参照してください。

オンボードのギガビット イーサネット インターフェイスを手動で定義するには、グローバル コンフィギュレーション モードから開始して、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**interface GigabitEthernet** *slot/bay/port* 例： `Router(config)# interface GigabitEthernet 0/0/0`	ルータ上でインターフェイスの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	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 192.168.12.2 255.255.255.0`	指定したインターフェイスの IP アドレスとサブネットマスクを設定します。IPv4 アドレスを設定する場合は、このステップを使用します。
ステップ 3	**ipv6 address** *ipv6-address/prefix* 例： `Router(config-if)# ipv6 address 2001.db8::ffff:1/128`	指定したインターフェイスの IPv6 アドレスとプレフィクスを設定します。IPv6 アドレスを設定する場合は、ステップ 2 の代わりにこのステップを使用します。IPv6 ユニキャスト ルーティングも設定する必要があります。詳細については、https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html にある『**IPv6 Addressing and Basic Connectivity Configuration Guide**』を参照してください。
ステップ 4	**ipv6 unicast-routing** 例：	IPv6 ユニキャスト データパケットの転送を有効にします。

	コマンドまたはアクション	目的
	`Router (config)# ipv6 unicast-routing`	
ステップ 5	**no shutdown** 例： `Router(config-if)# no shutdown`	インターフェイスを無効にします。状態が管理ダウンから管理アップに変化します。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイスのコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。

GigabitEthernet0/0/0 でのサブインターフェイスのサポート

Cisco IOS-XE リリース 16.11.1 以降では、g0/0/0 インターフェイスのサブインターフェイスと dot1q 設定がサポートされています。次に例を示します。

```
Router(config)#interface g0/0/0 ?
  <1-4294967295>  GigabitEthernet interface number
Router(config-subif)#encapsulation ?
  dot1Q            IEEE 802.1Q Virtual LAN
```

ループバック インターフェイスの設定

始める前に

ループバック インターフェイスは、スタティック IP アドレスのプレースホルダーとして機能し、デフォルトのルーティング情報を提供します。

ループバック インターフェイスを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**interface** *type number* 例： `Router(config)# interface Loopback 0`	ループバック インターフェイスの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	（オプション 1）**ip address** *ip-address mask* 例：	ループバック インターフェイスの IP アドレスとサブネットマスクを設定します。IPv6 アドレスを設定

	コマンドまたはアクション	目的
	`Router(config-if)# ip address 10.108.1.1 255.255.255.0`	する場合は、次に説明する **ipv6 address** *ipv6-address/prefix* コマンドを使用します。
ステップ 3	（オプション 2） **ipv6 address** *ipv6-address/prefix* 例： `Router(config-if)# ipv6 address 2001:db8::ffff:1/128`	ループバック インターフェイスの IPv6 アドレスとプレフィクスを設定します。
ステップ 4	**exit** 例： `Router(config-if)# exit`	ループバック インターフェイスのコンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

例

ループバック インターフェイス設定の確認

show interface loopback コマンドを入力します。次の例のような出力が表示されます。

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 192.0.2.0/16
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

または、次の例に示すように、**ping** コマンドを使用してループバック インターフェイスを確認します。

```
Router# ping 192.0.2.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.0, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Cisco Discovery Protocol の有効化

ルータでは、Cisco Discovery Protocol（CDP）がデフォルトで有効に設定されています。セキュリティ上の理由から、必要に応じて無効にすることができます。

CDP の使用法の詳細については、『Cisco Discovery Protocol Configuration Guide, Cisco IOS XE Release 3S』を参照してください。

コマンドライン アクセスの設定

ルータへのアクセスを制御するパラメータを設定するには、次の手順を実行します。

（注） トランスポート入力は、このガイドの Telnet と SSH のセクションで先に説明されているとおりに設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**line** ［**aux**	**console**	**tty**	**vty**］ *line-number* 例： `Router(config)# line console 0`	回線コンフィギュレーションモードを開始します。続いて、回線のタイプを指定します。 ここに示す例では、アクセス用のコンソール端末を指定します。
ステップ 2	**password** *password* 例： `Router(config-line)# password 5dr4Hepw3`	コンソール端末回線に固有のパスワードを指定します。
ステップ 3	**login** 例： `Router(config-line)# login`	端末セッションログイン時のパスワードチェックを有効にします。

ステップ 4	**exec-timeout** *minutes* ［*seconds*］
	例：
	`Router(config-line)# exec-timeout 5 30`
	`Router(config-line)#`
		ユーザ入力が検出されるまで EXEC コマンド インタープリタが待機する間隔を設定します。デフォルトは 10 分です。任意指定で、間隔値に秒数を追加します。
		ここに示す例は、5 分 30 秒のタイムアウトを示しています。「**00**」のタイムアウトを入力すると、タイムアウトが発生しません。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-line)# exit`	回線コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを再開します。

ステップ 6	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	例：
	`Router(config)# line vty 0 4`
	`Router(config-line)#`
		リモート コンソール アクセス用の仮想端末を指定します。

ステップ 7	**password** *password* 例： `Router(config-line)# password aldf2ad1`	仮想端末回線に固有のパスワードを指定します。
ステップ 8	**login** 例： `Router(config-line)# login`	仮想端末セッション ログイン時のパスワード チェックを有効にします。
ステップ 9	**end** 例： `Router(config-line)# end`	回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

例

次の設定は、コマンドライン アクセス コマンドを示します。デフォルトは transport input none ですが、SSH が有効になっている場合は SSH に設定する必要がある点に注意してください。

default と示されているコマンドは、入力する必要はありません。これらのコマンドは、**show running-config** コマンドの使用時に、生成されたコンフィギュレーション ファイルに自動的に示されます。

```
!
line console 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

スタティック ルートの設定

スタティック ルートは、ネットワークを介した固定ルーティング パスを提供します。これらは、ルータ上で手動で設定されます。ネットワーク トポロジが変更された場合には、スタティック ルートを新しいルートに更新する必要があります。スタティック ルートは、ルーティング プロトコルによって再配信される場合を除き、プライベート ルートです。

スタティック ルートを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	（オプション 1） **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} 例： `Router(config)# ip route 192.10.2.3 255.255.0.0 10.10.10.2`	IP パケットのスタティック ルートを指定します。（IPv6 アドレスを設定する場合は、次に説明する **ipv6 address** コマンドを使用してください）。
ステップ 2	（オプション 2） **ipv6 route** *prefix/mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]} 例： `Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0`	IP パケットのスタティック ルートを指定します。IPv6 の詳細については、次を参照してください。https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html
ステップ 3	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

次の設定例は、宛先 IP アドレスが 192.168.1.0、サブネット マスクが 255.255.255.0 のすべての IP パケットを、IP アドレス 10.10.10.2 の他の装置に対して、ギガビット インターフェイス上からスタティック ルートで送信します。具体的には、パケットが設定済みの PVC に送信されます。

default と示されているコマンドは、入力する必要はありません。このコマンドは、**running-config** コマンドの使用時に、生成されたコンフィギュレーション ファイルに自動的に示されます。

```
!
ip classless (default)
ip route 2001:db8:2::/64 2001:db8:3::0
```

設定の確認

スタティック ルートが正しく設定されていることを確認するには、**show ip route** コマンド（または **show ipv6 route** コマンド）を入力し、文字 S で示されるスタティック ルートを見つけます。

IPv4 アドレスを使用する場合は、次のような確認用の出力が表示されます。

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, FastEthernet0
```

IPv6 アドレスを使用する場合は、次のような確認用の出力が表示されます。

```
Router# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE -
Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       ls - LISP site, ld - LISP dyn-EID, a - Application

C   2001:DB8:3::/64 [0/0]
       via GigabitEthernet0/0/2, directly connected
S   2001:DB8:2::/64 [1/0]
       via 2001:DB8:3::1
```

ダイナミック ルートの設定

ダイナミック ルーティングでは、ネットワーク トラフィックまたはトポロジに基づいて、ネットワーク プロトコルがパスを自動調整します。ダイナミック ルーティングの変更は、ネットワーク上の他のルータにも反映されます。

Cisco IOS-XE コンフィギュレーション ガイドはすべて以下で確認できます。
https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-16/products-installation-and-configuration-guides-list.html

Routing Information Protocol の設定

ルータの RIP を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**router rip** 例： `Router(config)# router rip`	ルータ コンフィギュレーション モードを開始します。続いて、ルータの RIP を有効にします。
ステップ 2	**version** {**1** | **2**} 例： `Router(config-router)# version 2`	RIP version 1 または 2 の使用を指定します。

ステップ 3	**network** *ip-address*
	例：
	`Router(config-router)# network 192.168.1.1`
	`Router(config-router)# network 10.10.7.1`
		直接接続しているネットワークの各アドレスを使用して、RIP を適用するネットワーク リストを指定します。

ステップ 4	**no auto-summary** 例： `Router(config-router)# no auto-summary`	ネットワーク レベル ルートへのサブネット ルートの自動サマライズを無効にします。これにより、サブプレフィックス ルーティング情報がクラスフル ネットワーク境界を越えて送信されます。
ステップ 5	**end** 例： `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例

設定の確認

RIP が正しく設定されていることを確認するには、**show ip route** コマンドを入力し、文字 R で示される RIP ルートを見つけます。次の例のような出力が表示されます。

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
R    3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0/0
```

Enhanced Interior Gateway Routing Protocol の設定

Enhanced Interior Gateway Routing Protocol（EIGRP）は、シスコによって開発された Interior Gateway Routing Protocol（IGRP）の拡張バージョンです。EIGRP のコンバージェンス プロパティおよび作業効率は、IGRP よりも大幅に改善され、IGRP は使用されなくなりました。

EIGRP のコンバージェンス テクノロジーは、Diffusing Update Algorithm（DUAL）と呼ばれるアルゴリズムに基づいています。このアルゴリズムは、ルート計算中のどの時点でもループが発生しないようにし、トポロジ変更に関与するすべてのデバイスを同期できるようにします。トポロジ変更の影響を受けないデバイスは、再計算に含まれません。

Enhanced Interior Gateway Routing Protocol（eigrp）の設定の詳細については、次のガイドを参照してください。 https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-16-10/ire-xe-16-10-book/ire-enhanced-igrp.html

モジュラ QoS（MQC）

この項では、モジュラ QoS CLI（MQC）の概要、つまり IoT 統合型サービスルータでの QoS のすべての機能の設定方法を示します。MQC は、シスコのルーティングおよびスイッチング プラットフォームで QoS を有効にするための標準化されたアプローチです。

『QoS Modular QoS Command-Line Interface Configuration Guide, Cisco IOS XE 17 guide』の手順に従います。

シリアル インターフェイスの設定

このセクションでは、シリアル インターフェイス管理の設定について説明します。

IR1101 は、SCADA、raw ソケット、またはリバース Telnet に使用される非同期シリアル インターフェイス プロトコルをサポートしています。単一のシリアル インターフェイスと専用の非同期 0/2/0 を装備しています。シリアル インターフェイスは DTE のみです。

（注） 非同期シリアル ケーブルの説明については、次の場所にある IR1101 HW 設置ガイドを参照してください。 https://www.cisco.com/c/en/us/td/docs/routers/access/1101/hardware/installation/guide/1101hwinst.html

非同期インターフェイスの指定

非同期シリアル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

コマンドまたはアクション	目的
Router (config) # interface async 0/2/0	インターフェイス コンフィギュレーション モードを開始します。

非同期シリアル カプセル化の指定

非同期シリアル インターフェイスは、次のシリアル カプセル化方式をサポートします。

- Raw-TCP
- Raw-UDP
- SCADA
- カプセル化リレー

コマンドまたはアクション	目的
Router(config-if)# encapsulation {raw-tcp | raw-udp | scada}	非同期シリアル カプセル化を設定します。

カプセル化の方式は、Cisco IOS ソフトウェアで設定するプロトコルまたはアプリケーションのタイプに応じて設定されます。

その他のカプセル化方式は、プロトコルまたはアプリケーションについて説明するそれぞれの文書および章で定義されています。

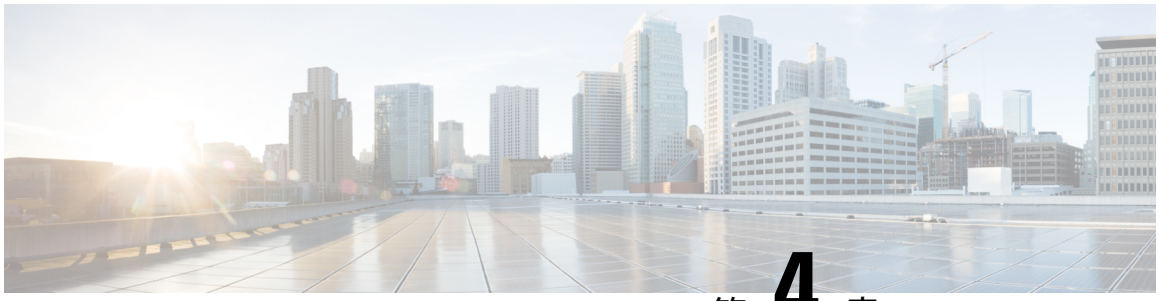
シリアル ポートの設定

シリアル ポートを設定するには、次の手順を実行します。

```
IR1101#sh run int async 0/2/0
Building configuration...
Current configuration : 62 bytes
!
interface Async0/2/0
no ip address
encapsulation raw-tcp
end
IR1101#show line
   Tty Line Typ     Tx/Rx    A Modem  Roty AccO AccI  Uses  Noise Overruns  Int
*     0    0 CTY              -    -      -    -    -     0      0    0/0      -
  0/2/0   50 TTY   9600/9600  -    -      -    -    -     0      0    0/0      -
     74   74 VTY              -    -      -    -    -     3      0    0/0      -
     75   75 VTY              -    -      -    -    -     0      0    0/0      -
     76   76 VTY              -    -      -    -    -     0      0    0/0      -
     77   77 VTY              -    -      -    -    -     0      0    0/0      -
     78   78 VTY              -    -      -    -    -     0      0    0/0      -
```

回線が非同期モードではない、または、ハードウェア サポートがない：

1-49、51-73、79-726



第 4 章

Web ユーザインターフェイス（WebUI）

この章は、次の項で構成されています。

Web ユーザーインターフェイスの概要

Web ユーザーインターフェイス（WebUI）は、ネットワーク管理者に、デバイスをプロビジョニング、モニタリング、最適化するための単一ソリューションを提供します。ハードウェアの取り付けが完了したら、トラフィックがネットワークを通過するのに必要な設定を行ってデバイスをセットアップする必要があります。新しいデバイスを使用する最初の日には、さまざまなタスクを実行することにより、デバイスがオンライン状態かつ到達可能で、簡単に設定されることを確認できます。これは、Day 0 インターフェイスと呼ばれます。

（注） Day 0 の設定は、スタートアップ コンフィギュレーションのない初期状態のデバイスとして定義されます。

初期 Day 0 設定の後、WebUI を使用して日常の設定を行うことができます。

IOS-XE リリース 17.3.1 より Day 0 の Web ユーザーインターフェイス（WebUI）が IR1101 でサポートされます。Day 0 WebUI は LAN ポートでのみサポートされます。これらのポートは、IR1101 の FastEthernet ポート 0/0/1 ー 0/0/4 です。PC を IR1101 のいずれかの LAN ポートに接続し、Day 0 でルータを起動します。PC は、静的 IP アドレス 192.168.1.2/255.255.255.0 で設定する必要があります。

Day 0 でルータが起動すると、PC は 192.168.1.x ネットワークに接続でき、任意のブラウザで IP アドレス 192.168.1.1 を使用して WebUI にアクセスできます。WebUI を介して設定が適用されると、ルータに「Day 0 config done. Stopping autoinstall」というメッセージが表示されます。

Day 0 セルラーモード

Cisco IOS XE リリース 17.9.1 は、セルラー プラガブル モジュールを介して初期設定できるようにする新機能を提供します。これは、セルラー プラガブル モジュールがすでにインストールされていることを前提としています。

このモードは、お客様が WAN バックホールとしてプライベート APN（またはプライベート LTE/5G）を取得すると仮定して、セルラー APN を設定するために役立ちます。そうすることで、APN 値がモデムに保存されます。ルーターが再起動すると、工場出荷時のデフォルトにリセットされ、プライベート APN が使用されている場合は、ルータがセルラー経由で PnP を実行できるようになります。

（注） パブリックまたはプライベート APN を含むセルラー WAN を設定するには、拡張モードが必要です。これは、SIM のサービスプロバイダから提供される必要があります。

（注） プラガブルインターフェイスはホットスワップ可能ではありません。SIM を変更する場合は、ルータの電源をオフにします。

セルラー プラガブル モジュールを使用して設定する手順は次のとおりです。

1. [WAN type] でセルラーインターフェイスを選択します。
2. APN 名を入力します。
3. バックアップ WAN を選択する必要はありません。
4. ルータを再起動します。

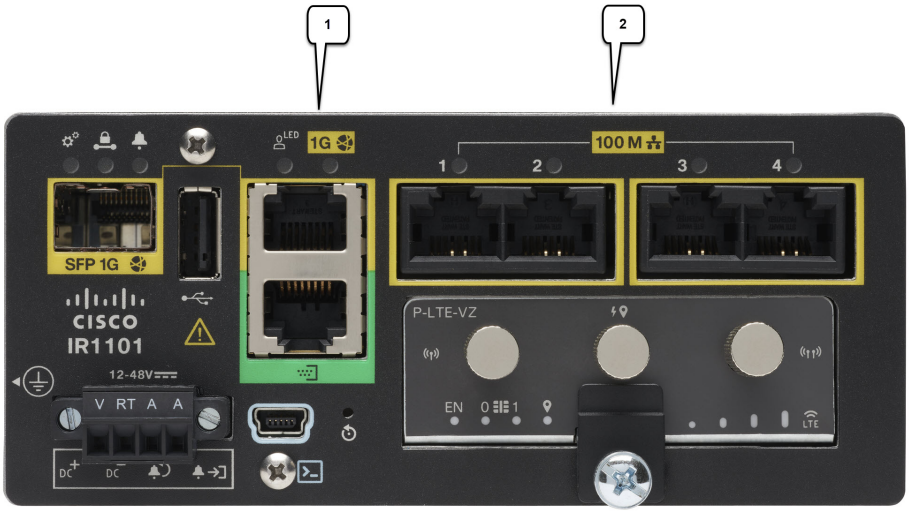
PnP は、IoT OD、vManage、または DNA-C に接続するためにプライベート APN で実行できるようになります。

設定に関する注意事項

WebUI を使用する場合の重要な注意事項は次のとおりです。

- このインターフェイスは PnP 専用であるため、WebUI は 1G ポートではサポートされません。100M ポート 1 ー 4 でのみサポートされます。下の図を参照してください。

- Plug and Play（PnP）は、Day 0 WebUI インターフェイスを使用してルータを設定する場合は使用できません。これは、Day 0 WebUI を使用して設定が適用されると PnP が中断されるためです。
- リリース 17.1.2 以降では、WebUI を使用して設定が適用されると、明示的な **write memory** は不要になります。



1	WAN ポート（GigabitEthernet 0/0/0 ー IOS-XE）
2	LAN ポート 1 ー 4（0/0/1 - 0/0/4 ー IOS-XE）

ルータへ接続するためのコンピュータの設定

次の項では、IR1101 と正しくインターフェイスするようにコンピュータを設定するためのガイダンスを示します。

クライアント Web ブラウザからアプリケーションにアクセスできます。次の Web クライアント要件を満たしていることを確認してください。

- ハードウェア：次のいずれかのテスト済み対応ブラウザとの互換性を備えた Mac（OS バージョン 10.9.5）または Windows（OS バージョン 10）ラップトップまたはデスクトップ
  - Google Chrome 59 以降

- Mozilla Firefox 54 以降
- Apple Safari 10 以降
- Microsoft Edge ブラウザ

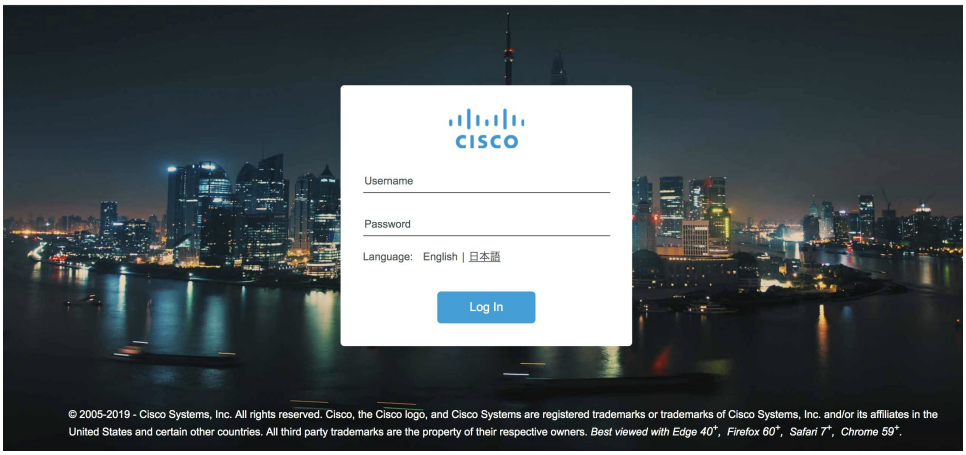
- 表示解像度：画面解像度を 1280 x 800 以上に設定することを推奨します。

ブラウザを使用した基本モード WebUI の設定

次に、PC またはラップトップのブラウザを使用して WebUI を設定する手順を示します。

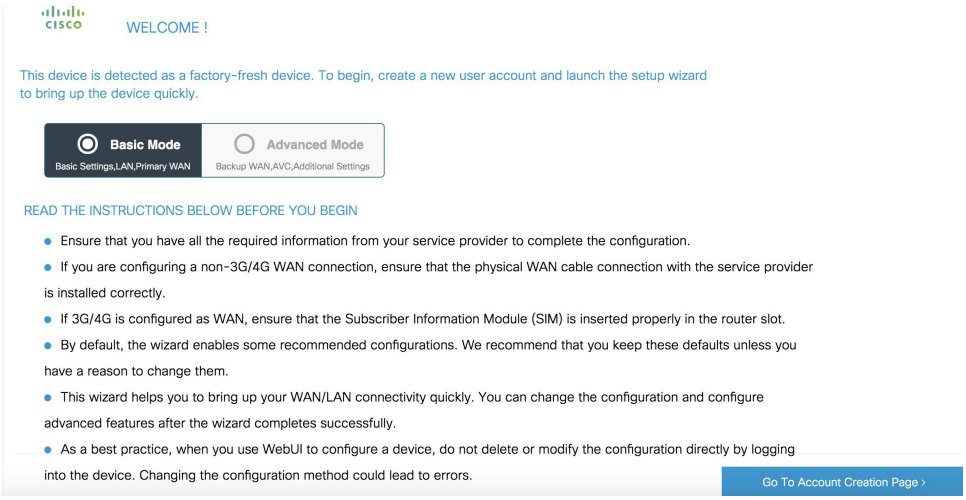
ステップ 1 ブラウザを開き、アドレスバーに 192.168.1.1 と入力します。ログイン画面が表示されます。ユーザ名 **webui** とパスワード **cisco** を入力します。次に、**Log In** をクリックします。

図 *3:* ログイン画面



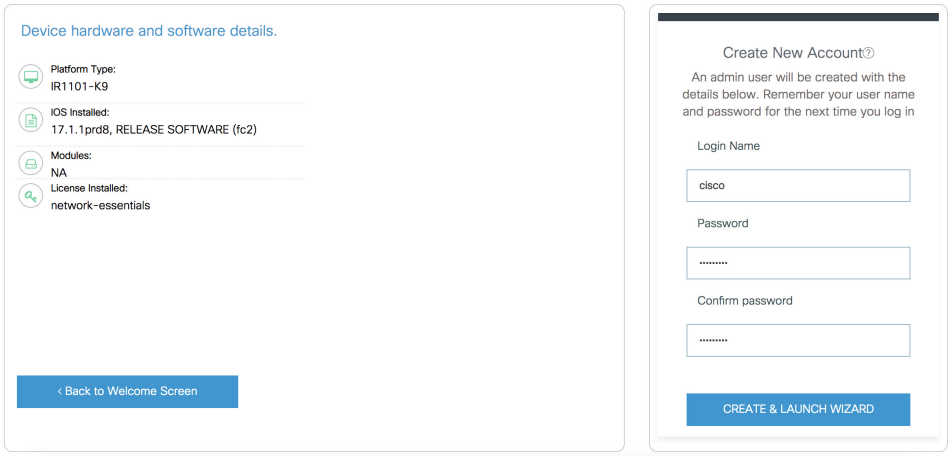
ステップ 2 [Welcome] 画面が表示されます。[Advanced Mode] または [Basic Mode] を選択します。[Basic Mode] では、基本設定、LAN、およびプライマリ WAN を設定できます。[Advanced Mode] では、追加のバックアップ WAN、AVC、および追加の設定を行うことができます。このセクションでは、[Basic Mode] を使用します。**Basic Mode** を選択します。

図 *4 : [Welcome]* 画面



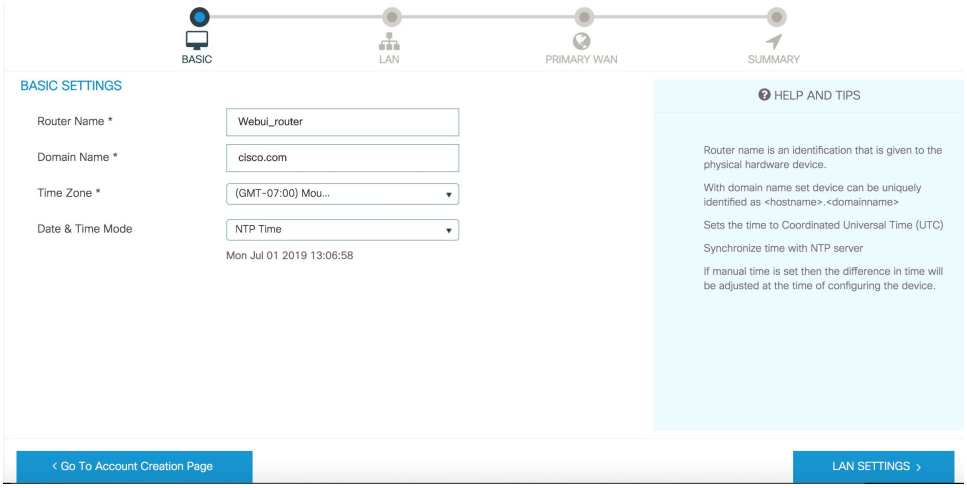
ステップ 3　**Go To Account Creation Page** をクリックします。[Create New Account] 画面が表示されます。WebUI にアクセスするための新しいログイン名とパスワードを作成します。

図 *5 : [Create New Account]* 画面



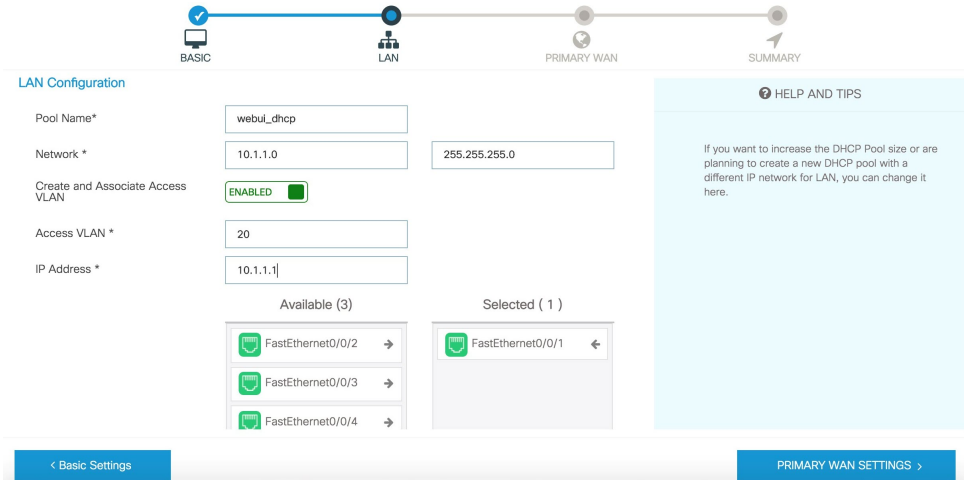
ステップ 4　**CREATE & LAUNCH WIZARD** をクリックします。[Basic Settings] 画面が表示されます。ルータ名（ホスト名）、ドメイン名、タイムゾーン、および日時モードを入力します。

図 *6 : [BASIC SETTINGS]* 画面



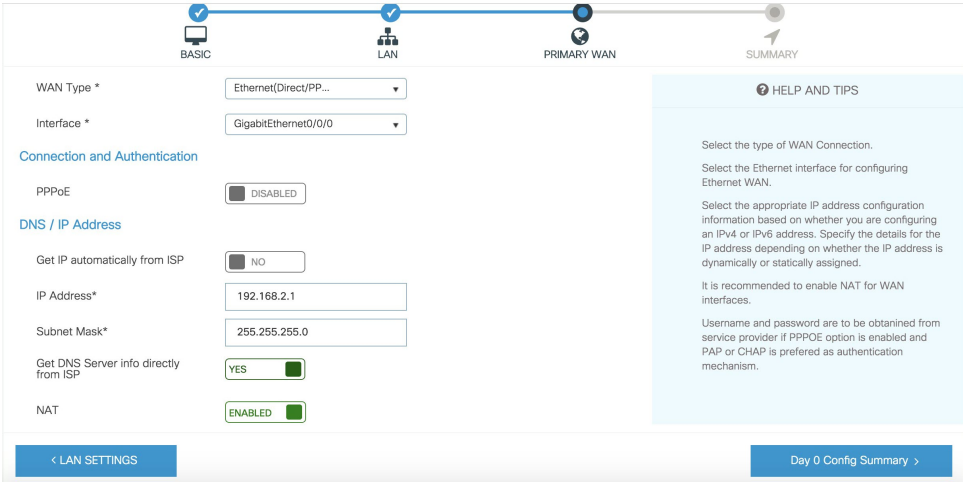
ステップ 5　**LAN SETTINGS** をクリックします。[LAN Configuration] 画面が表示されます。プール名 webui_dhcp と VLAN インターフェイスの IP アドレスを入力し、使用可能なインターフェイスのリストからラップトップに接続されているインターフェイスを選択します。

図 *7 : [LAN Configuration]* 画面



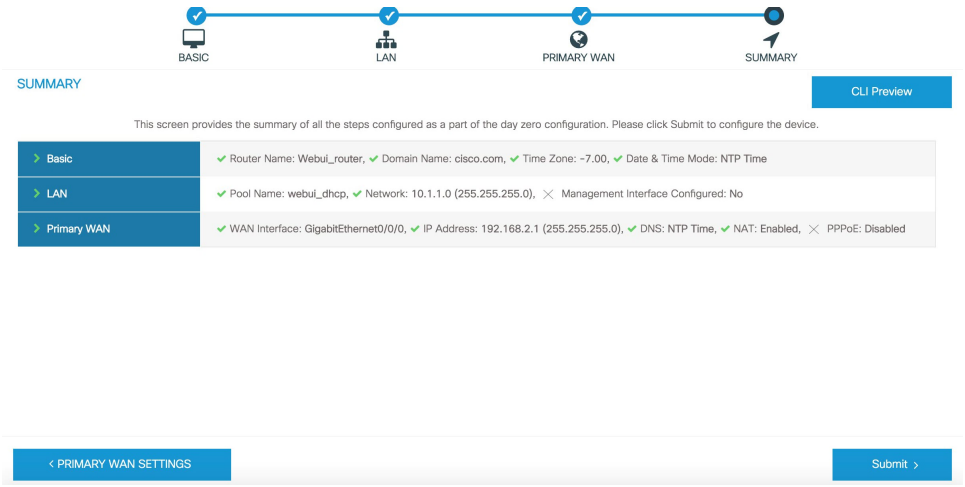
ステップ 6　**PRIMARY WAN SETTINGS** をクリックします。[PRIMARY WAN] 設定画面が表示されます。使用可能なオプションから WAN タイプとインターフェイスを選択して、WAN インターフェイスを設定します。次に、[DNS IP Address] に情報を入力し、NAT を有効にするか、または無効にするかを選択します。

図 *8 : [Primary WAN Interface]* 画面



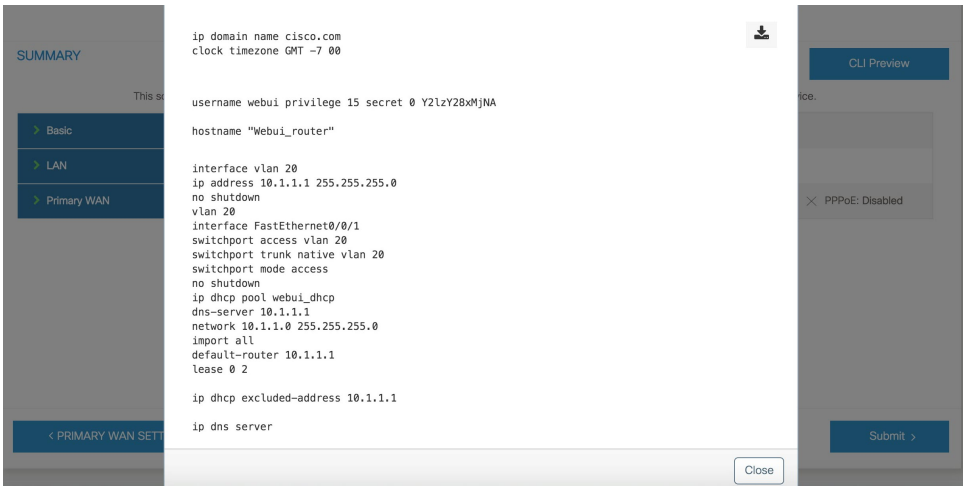
ステップ 7　**Day 0 Config Summary** をクリックします。[Review Summary] 画面が表示されます。エントリを確認してから設定を適用します。

図 *9 : [Summary]* 画面



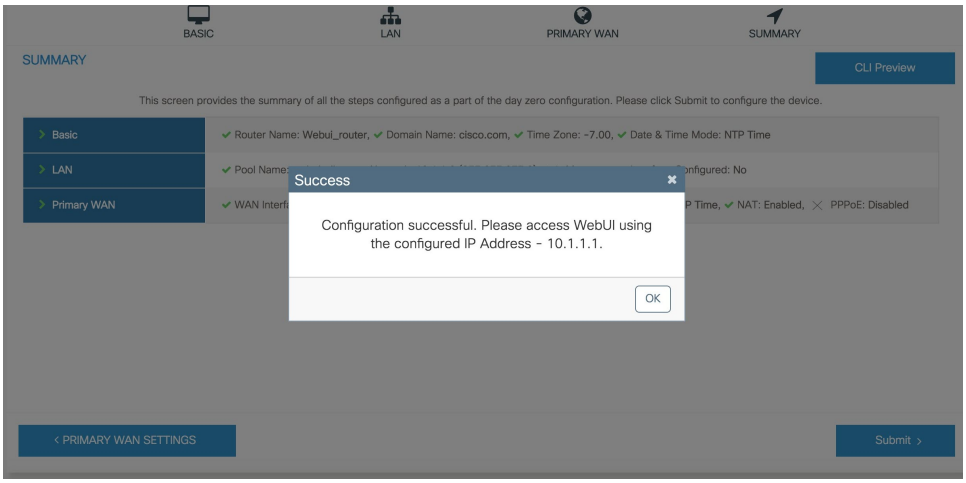
ステップ 8　（任意）[**CLI Preview**] をクリックして、ルータに適用されている設定を表示します。[CLI Preview] を閉じ、準備が整っている場合は **Submit** をクリックします。

図 *10 : [CLI Preview]* 画面



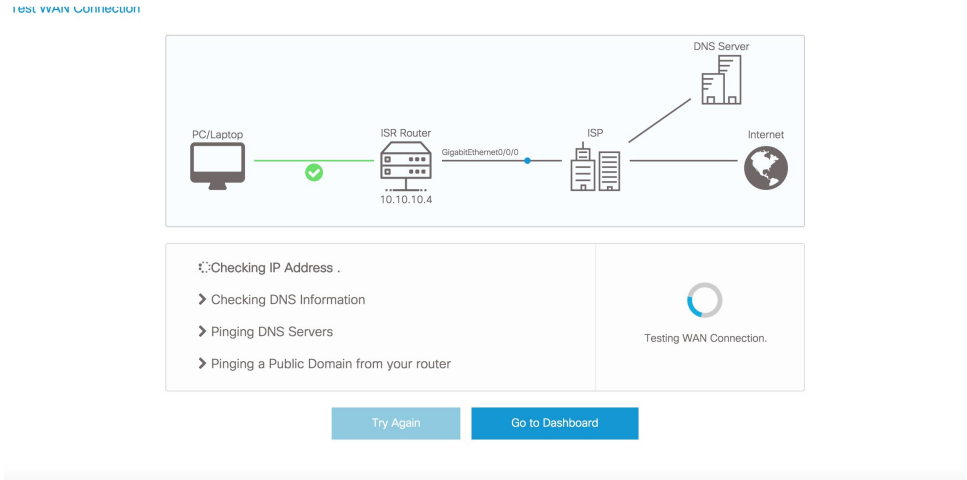
ステップ 9 [Submit] をクリックすると、設定が正常に適用されたことを通知するダイアログボックスが表示されます。新しい WebUI IP アドレスも表示されます。

図 *11 : [Submit]* ダイアログボックス



ステップ 10 Web接続がある場合、デバイスが接続を試みます。ブラウザセッションを閉じ、新しく設定されたWebUI IP アドレスに移動することをお勧めします。

図 *12 : [Test VLAN Connection]* 画面



ブラウザを使用した Advanced モード WebUI の設定

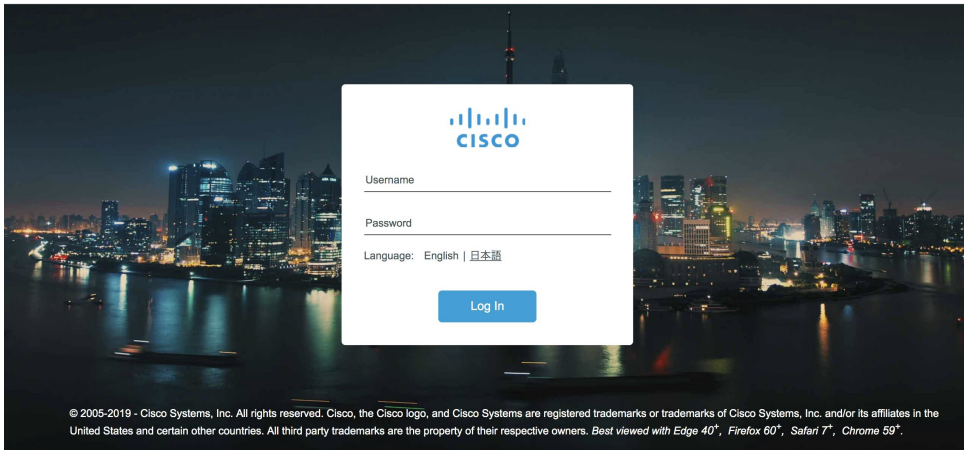
次に、PC のブラウザを使用して WebUI を設定する手順を示します。

ラップトップが DHCP 経由で IP アドレスを取得するように設定されていることを確認するか、デフォルトのサブネットに一致する IP アドレス *n.n.n.n* を割り当てます。

（注） パブリックまたはプライベート APN を含むセルラー WAN を設定するには、拡張モードが必要です。

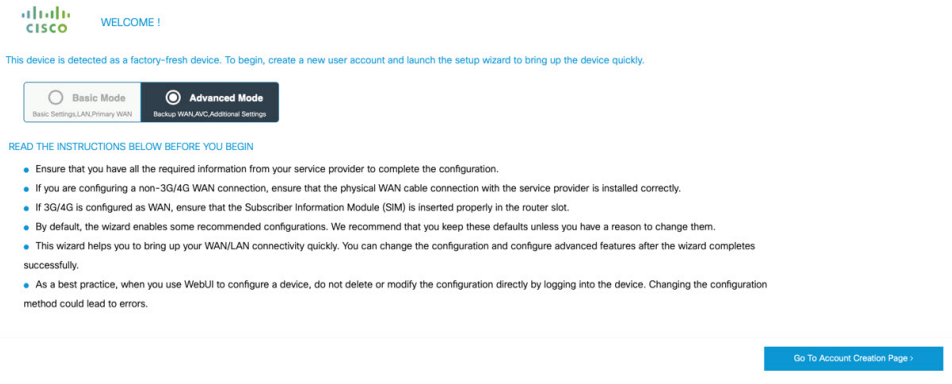
ステップ 1 ブラウザを開き、アドレスバーに 192.168.1.1 と入力します。ログイン画面が表示されます。ユーザ名 **webui** とパスワード **cisco** を入力します。次に、**Log In** をクリックします。

図 *13* : ログイン画面



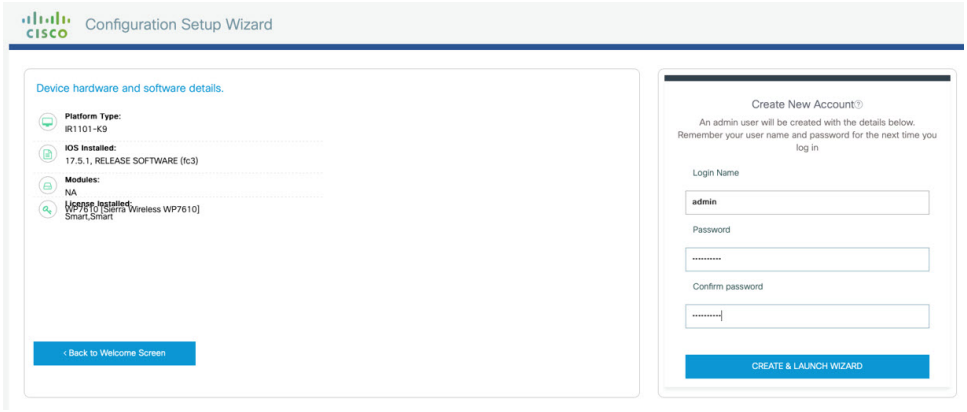
ステップ 2 [WELCOME] 画面が表示されます。[Advanced Mode] または [Basic Mode] を選択します。[Basic Mode] では、基本設定、LAN、およびプライマリ WAN を設定できます。[Advanced Mode] では、追加のバックアップ WAN、AVC、および追加の設定を行うことができます。このセクションでは、詳細モードを使用します。

図 *14* : *[WELCOME]* 画面



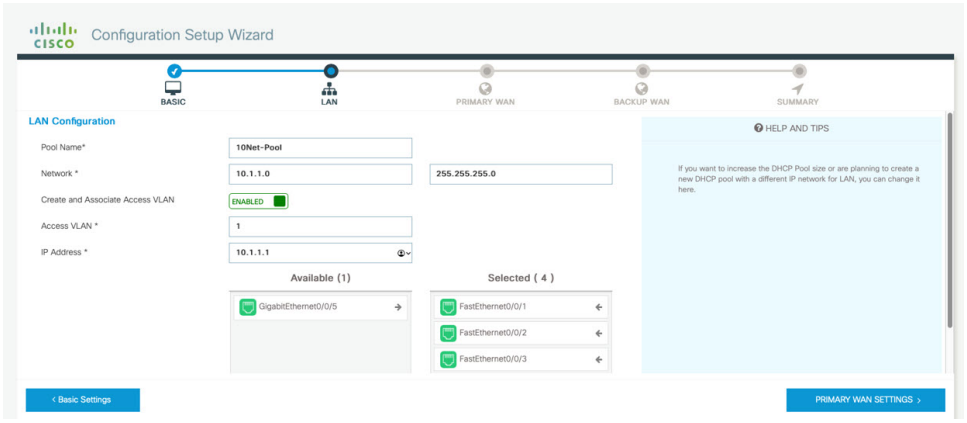
ステップ 3 **Advanced Mode**を選択し、**Go To Account Creation Page**をクリックします。[Create New Account] 画面が表示されます。WebUI にアクセスするための新しいログイン名とパスワードを作成します。

図 *15 : [Create New Account]* 画面



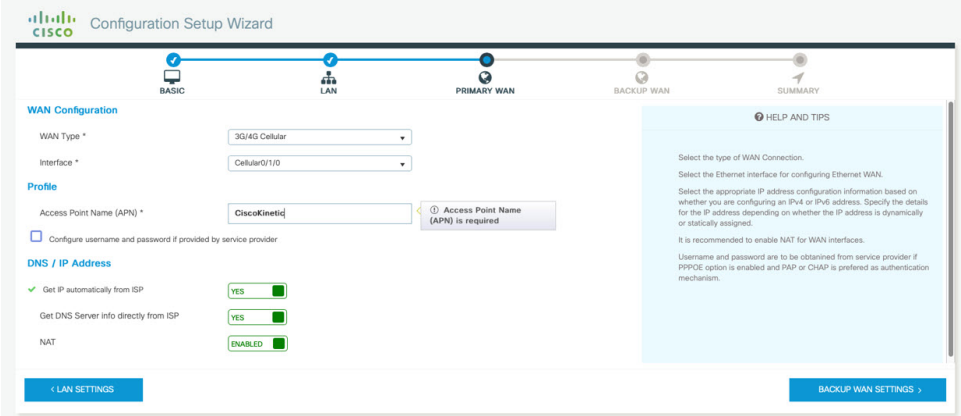
ステップ 4 **CREATE & LAUNCH WIZARD**をクリックすると、[LAN Configuration] 画面が表示されます。プール名、ネットワーク IP アドレス、サブネット、アクセス VLAN、およびデバイス IP アドレスを入力します。選択可能なインターフェイスのリストが表示されます。FastEthernetインターフェイスのみを使用できます。

図 *16 : [LAN Configuration]* 画面



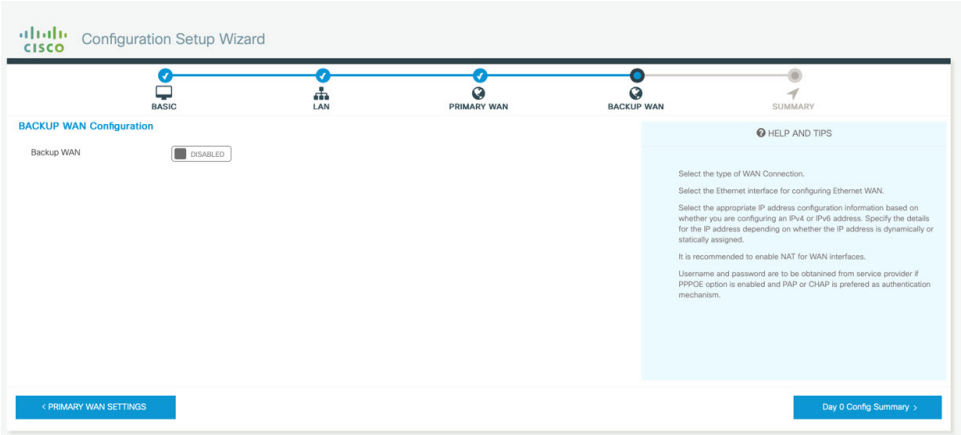
ステップ 5 **PRIMARY WAN SETTINGS** をクリックします。[WAN Configuration] 画面が表示されます。WAN タイプとインターフェイスをプルダウンメニューから選択します。LTE サービスプロバイダから APN（アクセスポイント名）を入力し、ネットワークの DNS および IP アドレスの設定を選択します。

図 *17 : [WAN Configuration]* 画面



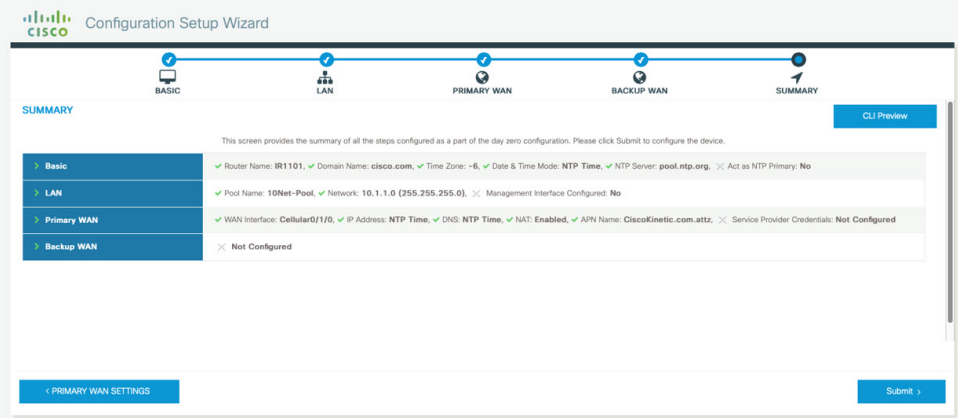
ステップ 6 **BACKUP WAN SETTINGS** をクリックします。[BACKUP WAN Configuration] 画面が表示されます。バックアップ WAN を有効または無効にするボタンを選択します。

図 *18 :* バックアップ *WAN* の設定



ステップ 7 **Day 0 Config Summary** をクリックします。[SUMMARY] 画面が表示されます。エントリを確認してから設定を適用します。

図 *19 : [Summary]* 画面

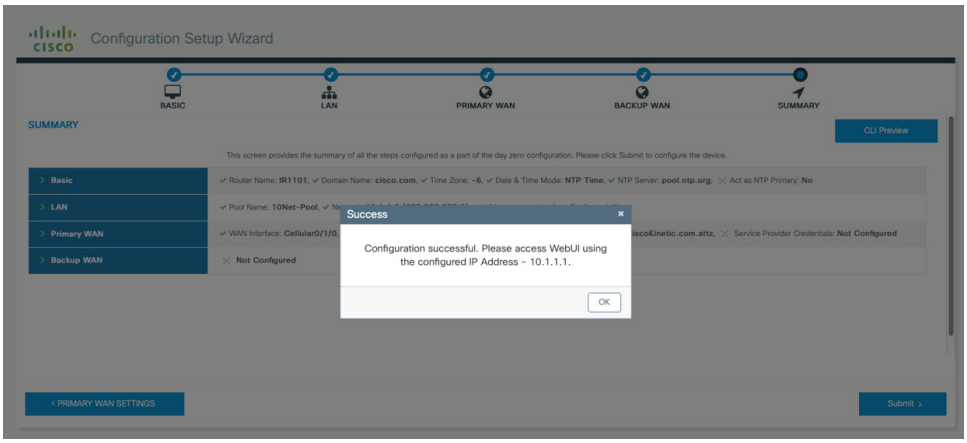


ステップ 8 （任意）[**CLI Preview**] をクリックして、ルータに適用されている設定を表示します。[CLI Preview] を閉じ、準備が整っている場合は [**Submit**] をクリックします。

（注） CLI プレビューの例は、このセクションの最後にあります。

ステップ 9 [Submit] をクリックすると、設定が正常に適用されたことを通知するダイアログボックスが表示されます。新しい WebUI IP アドレスも表示されます。

図 *20 : [Submit]* ダイアログボックス



例

次に、CLI プレビューの例を示します。

```
 ip domain name cisco.com
clock timezone GMT -6 00
ntp server pool.ntp.org

username admin privilege 15 secret 0 Mjc1N0dsb2NrIQ==

hostname "IR1101"
```

```
interface vlan 1
ip address 10.1.1.1 255.255.255.0
no shutdown
vlan 1
interface FastEthernet0/0/1
switchport access vlan 1
switchport trunk native vlan 1
switchport mode access
no shutdown
interface FastEthernet0/0/2
switchport access vlan 1
switchport trunk native vlan 1
switchport mode access
no shutdown
interface FastEthernet0/0/3
switchport access vlan 1
switchport trunk native vlan 1
switchport mode access
no shutdown
interface FastEthernet0/0/4
switchport access vlan 1
switchport trunk native vlan 1
switchport mode access
no shutdown
ip dhcp pool 10Net-Pool
dns-server 10.1.1.1
network 10.1.1.0 255.255.255.0
import all
default-router 10.1.1.1
lease 0 2

ip dhcp excluded-address 10.1.1.1

ip dns server
ip dns view default
default dns forwarder
default dns forwarding
default domain lookup
default domain name-server
interface Cellular0/1/0
description primary_wan
ip address negotiated
dialer in-band
dialer-group 1
pulse-time 1
shutdown
no shutdown
ip nat outside
exit
dialer-list 1 protocol ip permit

controller Cellular 0/1/0
lte sim data-profile 2 attach-profile 2 slot 0

ip route 0.0.0.0 0.0.0.0 Cellular0/1/0

ip nat inside source list 197 interface Cellular0/1/0 overload
access-list 197 permit ip any any
```

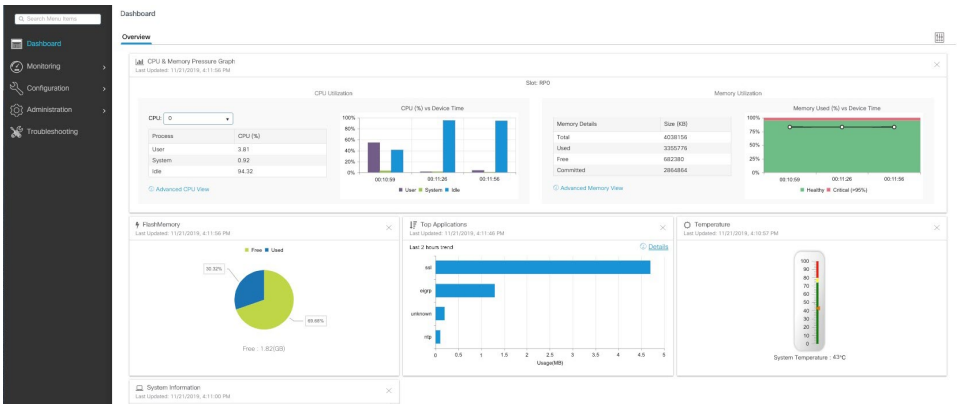
WebUI ダッシュボード

Day 0 のセットアップが完了すると、WebUI を日常の管理に使用できるようになります。WebUI が開き、使いやすいダッシュボードが表示されます。

（注） WebUI 機能のサポートは、デバイスのライセンスとプラットフォームタイプによって異なります。

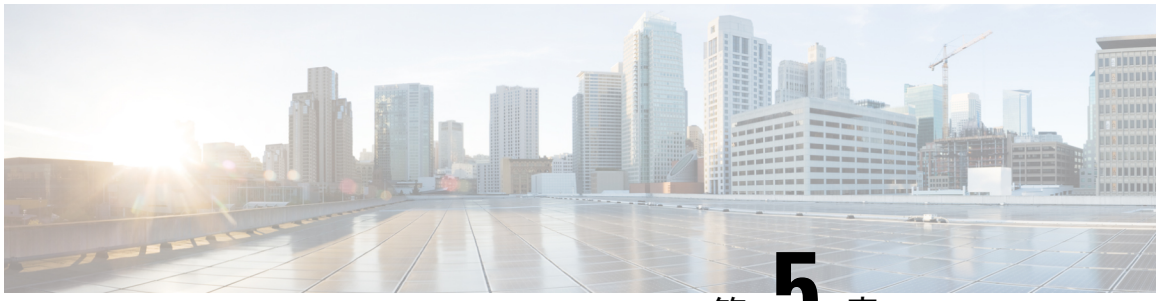
次の図は、ダッシュボードを示しています。

図 *21* : ダッシュボード



次の表に、ダッシュボードの概要を示します。

ダッシュボード	CPU とメモリの使用率とシステム情報のスナップショットを提供するダッシュレットを表示します。
モニターリング	日単位でネットワークをモニターし、ネットワーク デバイス インベントリと設定管理に関連するその他の臨時の処理を実行します。
設定	デバイスを設定します。
管理	システム設定とユーザー管理設定を指定します。
トラブルシューティング	Ping と Traceroute を使用して接続の問題とパケット損失をトラブルシューティングし、Web サーバーのログと syslog を使用してデバイスの状態とパフォーマンスをモニターします。



第 5 章

セキュア シェルの設定

この章は、次の項で構成されています。

セキュア シェルの概要

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

セキュア シェルを設定するための前提条件

セキュア シェル（SSH）用にデバイスを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。
- セキュア シェル（SSH）サーバは、IPsec（データ暗号規格（DES）または 3DES）の暗号化ソフトウェア イメージを必要とします。SSH クライアントは、IPsec（DES または 3DES）の暗号化ソフトウェア イメージが必要です。
- グローバル コンフィギュレーション モードで hostname および ip domain-name コマンドを使用して、デバイスのホスト名とホスト ドメインを設定します。**hostname** と **ip domain-name** コマンドをグローバル コンフィギュレーション モードで使用します。

セキュア シェルの設定に関する制約事項

セキュア シェル用に IR1101 を設定するための制約事項は、次のとおりです。

- ルータは RSA 認証をサポートしています。

- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、データ暗号規格（DES）（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。

（注） 3DES 暗号化はより強力であるため、シスコでは強く推奨しています。

詳細については、https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.htmlの Cisco IOS-XE デバイス強化ガイドを参照してください。

- このソフトウェア リリースは、IP Security（IPSec）をサポートしています。
- IR1101 は、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- ログイン バナーはセキュア シェル バージョン 1 ではサポートされません。シスコが優れたセキュリティのため推奨しているセキュア シェル バージョン 2 でサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-l キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。

SSH とルータ アクセス

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。IPv6 の SSH 機能は IPv4 における機能と同じです。IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュア シェル（SSH）統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いて Telnet のアウトバウ

ンド接続と同様の機能を提供します。SSHクライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSHサーバおよびSSH統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSHクライアントは、市販の一般的なSSHサーバと連動します。SSH クライアントは、Data Encryption Standard（DES）、3DES、およびパスワード認証の暗号をサポートします。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対するTelnetセッションの認証と同様に実行されます。SSHは、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

SSH 設定時の注意事項

デバイスを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます（逆の場合も同様です）。
- **crypto key generate rsa**グローバル コンフィギュレーション コマンドを入力した後、CLI エラー メッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。
- RSA キーのペアを生成する場合に、メッセージ「*No hostname specified*」が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用して IP ホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

関連タスク

SSH を実行するための IR1101 の設定 （60 ページ）
#unique_62

セキュア シェルの設定方法

SSH を実行するための IR1101 の設定

SSH を実行するようにデバイスをセットアップするには、次の手順を実行してください。

始める前に

ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。この手順は必須です。詳細については、次の関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `IR1101# 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	**hostname** *hostname* 例： `IR1101(config)# hostname your_hostname`	device のホスト名および IP ドメイン名を設定します。 （注） この手順を実行するのは、device を SSH サーバとして設定する場合だけです。
ステップ 3	**ip domain-name** *domain_name* 例： `IR1101(config)# ip domain-name your_domain_name`	device のホストドメインを設定します。
ステップ 4	**crypto key generate rsa** 例： `IR1101(config)# crypto key generate rsa`	device 上でローカルおよびリモート認証用に SSH サーバをイネーブルにし、RSA キーペアを生成します。device の RSA キー ペアを生成すると、SSH が自動的にイネーブルになります。 最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。 （注） この手順を実行するのは、device を SSH サーバとして設定する場合だけです。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `IR1101(config)# end`	特権 EXEC モードに戻ります。

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。

（注） デバイスを SSH サーバとして設定する場合にのみ、この手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `IR1101# 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	**ip ssh version** [2] 例： `IR1101(config)# ip ssh version 2`	（任意）SSH バージョン 2 を実行するように device を設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。

ステップ 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}
	例：
	`IR1101(config)# ip ssh timeout 90`
	`ip ssh authentication-retries 2`
		SSH 制御パラメータを設定します。
		• タイムアウト値は秒単位で指定します（デフォルト値は 120 秒）。指定できる範囲は 0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されると、デバイスは CLI ベース セッションのデフォルトのタイムアウト値を使用します。
		デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用でき

	コマンドまたはアクション	目的
		ます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。

ステップ 4	次のいずれかまたは両方を使用します。
	• **line vty** *line_number* [*ending line number*]
	• **transport input ssh**
	例：
	`IR1101(config)# line vty 1 10`
	または
	`IR1101(config-line)# transport input ssh`
		（任意）仮想端末回線設定を設定します。
		• ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。*line_number* 引数と *ending_line_number* 引数の有効な範囲は 0 ～ 15 です。
		• device で SSH 以外の Telnet 接続を防ぎ、デバイスを SSH 接続のみに限定するように指定します。

ステップ 5	**end** 例： `IR1101(config-line)# end`	回線コンフィギュレーションモードを終了します。続いて、特権 EXEC モードに戻ります。

SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 *6: SSH* サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

ルータのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。ルータは、認証と許可を処理します。この設定ではアカウンティング機能は使用できません。

ローカル モードで AAA を実装するようにルータを設定して、サーバがなくても動作するように AAA を設定するには、次の手順を実行します。

（注） AAA 方式を使用して HTTP アクセスに対しルータのセキュリティを確保するには、ip http authentication aaa グローバル コンフィギュレーション コマンドでを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しルータのセキュリティは確保しません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `IR1101# 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	aaa new-model 例： `IR1101(config)# aaa new-model`	AAA の有効化
ステップ 3	aaa authentication login default local 例： `IR1101(config)# aaa authentication login default local`	ローカル ユーザ名データベースを使用するログイン認証を設定します。default キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 4	aaa authorization exec local 例： `IR1101(config-line)# aaa authorization exec local`	ユーザの AAA 許可を設定し、ローカル データベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 5	aaa authorization network local 例：	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。

	コマンドまたはアクション	目的
	`IR1101(config-line)# aaa authorization network local`	
ステップ 6	**username** *name* **privilege** *level* **password** *encryption-type password* 例： `IR1101(config-line)# username your_user_name privilege 1 password 7 secret567`	ローカルデータベースを入力し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 1. *name* には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 2. （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 3. encryption-type には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 4. password には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。
ステップ 7	**end** 例： `IR1101(config-line)# end`	回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

セキュア コピーに関する情報

セキュア コピー（SCP）機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCP は、セキュア シェル（SSH）、アプリケーション、および Berkeley r ツールのセキュアな代替手段を提供するプロトコルに依存します。

セキュア コピーの前提条件

セキュア シェル（SSH）用にデバイスを設定するための前提条件は、次のとおりです。

- SCP を有効にする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。

- SCP は SSH に依存して安全な伝送を行っているため、ルータには RSA キー ペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、およびアカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。

セキュア コピーの設定に関する制約事項

- SCP を有効にする前に、ルータ上で SSH、認証、および認可を正しく設定する必要があります。
- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

セキュアコピーの設定

シスコの IR1101 にセキュア コピー（SCP）サーバ側機能の設定をするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**aaa new-model** 例： `Device(config)# aaa new-model`	ログイン時の AAA 認証を設定します。

	コマンドまたはアクション	目的
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Device(config)# aaa authentication login default group tacacs+`	AAA アクセス コントロール システムをイネーブルにします。
ステップ 5	**username** *name* [**privilege** *level*] **password** *encryption-type encrypted-password* 例： `Device(config)# username superuser privilege 2 password 0 superpassword`	ユーザ名をベースとした認証システムを構築します。 （注） TACACS+ や RADIUS などのネットワークベースの認証メカニズムが設定されている場合は、この手順を省略できます。
ステップ 6	**ip scp server enable** 例： `Device(config)# ip scp server enable`	SCP サーバ側機能を有効にします。
ステップ 7	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	（任意）SCP サーバ側機能を表示します。
ステップ 9	**debug ip scp** 例： `Device# debug ip scp`	（任意）SCP 認証問題を解決します。

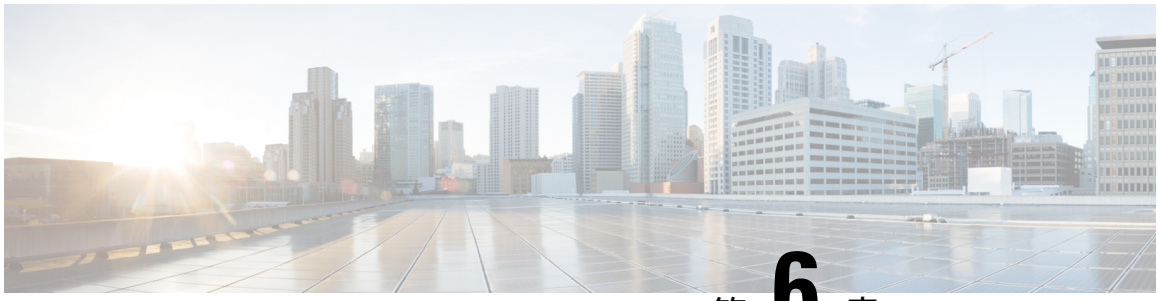
例

IR1101# **copy scp <*somefile*> your_username@remotehost:/<*some/remote/directory*>**

その他の参考資料

ここでは、SSH 機能に関する関連資料について説明します。

関連項目	マニュアル タイトル
セッション アウェアなネットワーキングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービステンプレートの設定。	『Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE』： https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.pdf
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	『 Secure Shell Configuration Guide, Cisco IOS XE Gibraltar 16.11.x』： https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-11/configuration_guide/sec/b_1611_sec_9500_cg/configuring_secure_shell__ssh_.html



第 6 章

GPS クロックに基づく NTP タイミング

この章は、次の項で構成されています。

GPS 時間を使用した NTP の設定

コマンド **ntp refclock gps** を使用して、GPS 時間を NTP の基準クロックとして設定できます。

（注） この機能は、IOS XE リリース 17.6.1 で使用できます。詳細については、『Cellular Pluggable Interface Module Configuration Guide』の「NTP Clock Sync with GPS」を参照してください。

GPS 時間はストラタム 0 ソースとして機能し、Cisco IOS NTP サーバーはストラタム 1 デバイスとして機能します。次に Cisco IOS NTP サーバーから NTP クライアント（ストラタム 2 および 3）にクロック情報が提供されます。

ステップ 1 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。

例：

```
Router# configure terminal
```

ステップ 2 NTP 基準クロックを GPS に設定します。

例：

```
Router(config)#ntp refclock gps
```

ステップ 3 次の例では、設定を確認するために **show** コマンドを使用しています。

例：

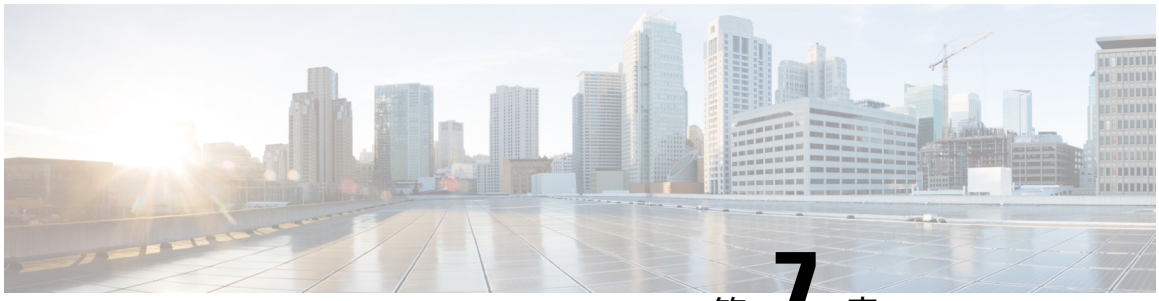
```
Router#
Sep 24 19:58:43.046 GMT: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Router#show ntp status
Clock is synchronized, stratum 1, reference is .GPS.
```

```
nominal freq is 250.0000 Hz, actual freq is 249.9970 Hz, precision is 2**10
ntp uptime is 94000 (1/100 of seconds), resolution is 4016
reference time is E31778F3.0B851ED8 (19:58:43.045 GMT Thu Sep 24 2020)
clock offset is 11.0000 msec, root delay is 0.00 msec
root dispersion is 3950.55 msec, peer dispersion is 3938.47 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000011995 s/s
system poll interval is 64, last update was 7 sec ago.
Router#
Router#
Router#show ntp associations

address ref clock st when poll reach delay offset disp
*~127.127.5.1 .GPS. 0 38 64 7 0.000 11.000 1938.8
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Router#
Router#show clock
20:00:43.660 GMT Thu Sep 24 2020
Router#
```

ステップ 4 **debug ntp refclock** コマンドを使用して、設定をトラブルシュートします。

例：

```
Router#debug ntp ?
adjust NTP clock adjustments
all NTP all debugging on
core NTP core messages
events NTP events
packet NTP packet debugging
refclock NTP refclock messages

Router#debug ntp re
Router#debug ntp refclock
*Sep 24 19:58:43.045 GMT: GPS: Poll Requested
*Sep 24 19:58:43.045 GMT: GPS (19:58:43.056 GMT Thu Sep 24 2020)
*Sep 24 19:58:43.045 GMT: Valid time rcvd from GPS: 2020/09/24 19:58:43.056 (frac = 0x0E560440)
*Sep 24 19:58:43.045 GMT: RTS poll timestamp (local clock) was 0xE31778F3.0B851ED8
*Sep 24 19:58:43.045 GMT: GPS timestamp is 0xE31778F3.0E560440
*Sep 24 19:58:43.045 GMT: NTP Core(NOTICE): ntpd PPM
*Sep 24 19:58:43.046 GMT: NTP Core(NOTICE): trans state : 5
*Sep 24 19:58:43.046 GMT: NTP Core(NOTICE): Clock is synchronized.
```



第 7 章

Cisco IOS-XE 17.1.1 の新機能

次に、IOS-XE リリース 17.1.1 の IR1101 で使用可能な新機能を示します。

X25 over TCP（XOT）のサポート

X.25 は、パケットスイッチングのワイドエリアネットワーク（WAN）に関する ITU 標準です。これは、シリアルインターフェイスを介した通信業界で使用されていますが、IP ネットワークに置き換えられています。X25 接続は、Telnet/SSH と同様の PAD 接続を使用して確立できます。IR1101 ルータには、X25 の機能がサポートされていない非同期シリアルインターフェイスが 1 つのみ搭載されています。ただし、TCP over X25（XOT）機能を使用して X25 エッジデバイスと通信することは可能です。XOT を使用すると、X25 エッジデバイスへの PAD 接続を直接確立できます。また、X25 パケットのさまざまなパラメータを変更することで、デフォルトまたはカスタマイズされたプロファイルをアクセスグループに割り当てることができます。

IOS-XE の XOT の詳細については、次を参照してください。

『Wide-Area Networking Configuration Guide: X.25 and LAPB, Cisco IOS XE』

YANG データモデル（Call-home）のサポート

call-home 機能でサポートされている YANG モデルは、Cisco-IOS-XE の以前のリリースと同様であり、IR1101 の IOS-XE の 17.1 リリースでもサポートされています。次の参考資料は、以前の YANG モデルで使用できます。

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1651

IOS-XE の call-home の詳細については、次を参照してください。

『Software Activation Configuration Guide, Cisco IOS XE Release 3S』

SCADA に対する YANG データモデルのサポート

Cisco IOS XE 17.1.1 には、SCADA システム向けの Cisco IOS XE YANG モデルのサポートが導入されています。他の領域においては、以前のリリースで YANG モデルが提供されていました。

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1711

GNMI テレメトリダイヤルインに対するモデル駆動型サポートのサポート

YANG モデルと同様に、IOS-XE では Google が定義したオープンソースモデルがサポートされており、Google Network Management Interface（GNMI）と呼ばれます。GNMI の設定は、セキュアモードでも、非セキュアモードでも確認できます。

- セキュアモード

セキュアモードは OpenSSL 証明書を使用してクライアントとサーバ間にセキュアな接続を確立します。オープンソースの gnmi_cli ツールを使用して GNMI テレメトリの更新を送信します。

- 非セキュアモード

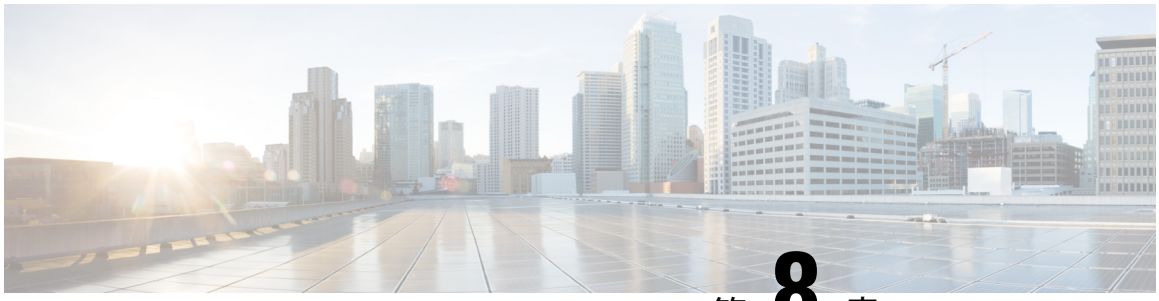
非セキュアモードは、オープンソースの pygnmi ツールを使用して、クライアントとサーバ間で GNMI テレメトリの更新を送信します。

GNMI テレメトリの詳細については、次の参考資料を参照してください。

Cisco IOS XE プログラマビリティ コンフィギュレーション ガイド

USB アクセスを有効または無効にするためのオプション

Day 0 Web ユーザインターフェイス



第 8 章

Cisco IOS-XE 17.2.1 の新機能

ネイティブ Docker のサポート

ネイティブ Docker のサポートが 17.2.1 リリースに追加されました。この機能により、ユーザは Docker アプリケーションを IR1101 に展開できます。アプリケーションのライフサイクルプロセスは、「アプリケーションのインストールとアンインストール」の項の手順と同様です。Dockerアプリケーションの場合、アプリケーション設定の一部としてエントリポイント設定が必要です。エントリポイントの設定については、次の例を参照してください。

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#app-hosting appid app3
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.0.7 netmask 255.255.255.0
Router(config-app-hosting-gateway0)#app-default-gateway 192.168.0.1 guest-interface 0
Router(config-app-hosting)#app-resource docker
Router(config-app-hosting-docker)#run-opts 1 "--entrypoint '/bin/sleep 10000'"
Router(config-app-hosting-docker)#end
Router#
```

Docker アプリケーションの出力を次の例に示します。

```
Router#show app-hosting detail
App id : app1
Owner : iox
State : RUNNING
Application
Type : docker
Name : aarch64/busybox
Version : latest
Description :
Path : bootflash:busybox.tar
Activated profile name : custom
```

```
Resource reservation
Memory : 431 MB
Disk : 10 MB
CPU : 577 units
VCPU : 1
Attached devices
Type Name Alias
---------------------------------------------
serial/shell iox_console_shell serial0
serial/aux iox_console_aux serial1
serial/syslog iox_syslog serial2
serial/trace iox_trace serial3
Network interfaces
---------------------------------------
eth0:
MAC address : 52:54:dd:e9:ab:7a
IPv4 address : 192.168.0.7
Network name : VPG0
Docker
------
Run-time information
Command :
Entry-point : /bin/sleep 10000
Run options in use : --entrypoint '/bin/sleep 10000'
Application health information
Status : 0
Last probe error :
Last probe output :
Router#
```

raw ソケットトランスポートに対する YANG データモデルのサポート

リリース 17.2.1 では、追加の YANG データモデルに対するサポートが追加されています。これらの追加モデルには、raw ソケットトランスポートが含まれています。

YANG データモデルは次の URL で確認できます。

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/1721

メインの Cisco-IOS-XE ネイティブモデルに属する raw ソケットには 2 つの機能モジュールがあります。その内容は次のとおりです。

- Cisco-IOS-XE-rawsocket.yang

このモジュールには raw ソケットトランスポートのコンフィギュレーションコマンドの YANG 定義のコレクションが含まれています。

次に、このモジュールに対応する CLI コマンドを示します。

```
# encapsulation raw-tcp
# encapsulation raw-udp
# raw-socket packet-length
<length>
# raw-socket packet-timer
<timer>
# raw-socket special-char
```

```
<value>
# raw-socket tcp server
<port> <ip>
# raw-socket tcp idle-timeout
<value>
# raw-socket tcp client <
dest-ip> <dest-port>
# raw-socket tcp idle-timeout
<timeout>
# raw-socket tcp tcp-session
<value>
# raw-socket tcp dscp
 <value>
# raw-socket udp connection
<dest-ip> <dest-port> <local_port>
```

- Cisco-IOS-XE-rawsocket-oper.yang

このモジュールには、raw ソケットトランスポートの運用データの YANG 定義のコレクションが含まれています。

次に、このモジュールに対応する CLI コマンドを示します。

```
# show raw udp statistics
# show raw tcp statistics
# show raw tcp session
# show raw udp session
# show raw tcp session local
# show raw udp session local
```

次に、依存モジュールのリストを示します。

- Cisco-IOS-XE-native
- Cisco-IOS-XE-features
- ietf-inet-types
- Cisco-IOS-XE-interfaces
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @（すべてのリビジョン）
- cisco-semver

IOx コンテナアプリケーションのデジタル IO

リリース 17.2.1 では、IOx コンテナアプリケーションがデジタル IO にアクセスできるようになりました。alarm contact コマンドに新しい CLI が追加されました。

```
Router(config)# alarm contact ?
  <0-4>          Alarm contact number (0: Alarm port, 1-4: Digital I/O)
  attach-to-iox  Enable Digital IO Ports access from IOX
Router (config)# alarm contact attach-to-iox
```

attach-to-iox コマンドを有効にすると、IOx へのすべてのデジタル IO ポートを完全に制御できます。ポートは、4 文字のデバイス /dev/dio-[1-4] として IOX アプリケーションに公開されま

す。読み取りまたは書き込みの機能を使用して、デジタル IO ポートの値を取得または設定できます。

モードを更新する場合は、モード値を文字型デバイスファイルに書き込むことができます。これは、状態の読み取り/書き込み、モードの変更、およびポートの真のアナログ電圧の読み取りを行う IOCTL コールによって実行されます。この方法に従って、アナログセンサーを IR1101 に接続できます。すべてのポートが最初に入力モードに設定され、電圧は 3.3v にプルアップされます。

次に、IOCTL コールの例を示します。

デジタル IO ポートの読み取り：

```
cat /dev/dio-1
```

デジタル IO ポートへの書き込み：

```
echo 0 > /dev/dio-1
echo 1 > /dev/dio-1
```

モードの変更：

```
echo out > /dev/dio-1
echo in > /dev/dio-1
```

サポートされている IOCTL のリスト：

```
DIO_GET_STATE = 0x1001
DIO_SET_STATE = 0x1002
DIO_GET_MODE = 0x1003
DIO_SET_MODE_OUTPUT = 0x1004
DIO_SET_MODE_INPUT = 0x1005
DIO_GET_THRESHOLD 0x1006
DIO_SET_THRESHOLD = 0x1007
DIO_GET_VOLTAGE = 0x1009
```

IOCTL を使用した状態の読み取り：

```
import fcntl, array
file = open("/dev/dio-1","rw")
state = array.array('L',[0])
fcntl.ioctl(file, DIO_GET_STATE, state)
print(state[0])
```

IOCTL を使用したモードの変更：

```
import fcntl
file = open("/dev/dio-1","rw")
fcntl.ioctl(file, DIO_SET_MODE_OUTPUT, 0)
```

L2 スティッキセキュア MAC アドレス

これは IR1101 には新機能ですが、IOS-XE にはしばらく前から搭載されていました。

スティッキー ラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキー セキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。インターフェイスはスティッキ ラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミック セキュア MAC アドレスをスティッキー セキュア MAC アドレスに変換します。すべてのスティッキー セキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキー セキュア MAC アドレスは、コンフィギュレーション ファイル（スイッチが再起動されるたびに使用されるスタートアップ コンフィギュレーション）に、自動的には反映されません。スティッキー セキュア MAC アドレスをコンフィギュレーション ファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキ セキュア アドレスを保存しない場合、アドレスは失われます。

セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレス テーブルに追加されている状態で、アドレス テーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。

違反が発生した場合の対処に基づいて、次の 3 種類の違反モードのいずれかにインターフェイスを設定できます。

- protect（保護）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。

Note：スティッキラーニングが無効になっている場合は、スティッキセキュア MAC アドレスがダイナミック セキュア アドレスに変換され、実行コンフィギュレーションから削除されます。

- restrict（制限）：セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないかぎり、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- shutdown（シャットダウン）：ポート セキュリティ違反により、インターフェイスが error-disabled になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。セキュア ポートが error-disabled ステートの場合は、errdisable recovery cause psecure-violation グローバル コンフィギュレーション コマンドを入力してこのステートを解除するか、shutdown および no shut down インターフェイス コンフィギュレーション コマンドを入力して手動で再び有効にできます。これは、デフォルトのモードです。

- shutdown vlan（VLAN シャットダウン）：VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が errdisable になります。

コマンドライン インターフェイス

スイッチインターフェイスに port-security cli を追加します。

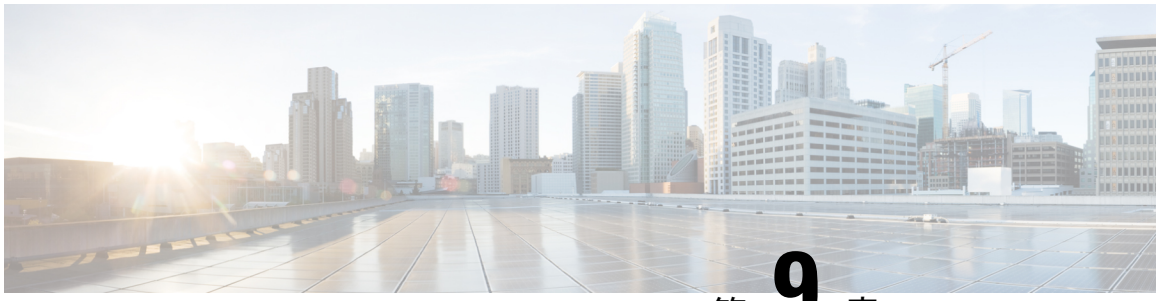
```
Router(config-if)#switchport port-security ?
  aging        Port-security aging commands
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>         <cr>
Router(config-if)#switchport port-security mac-address sticky
```

署名付きアプリケーションのサポート

シスコの署名付きアプリケーションが IR1101 でサポートされるようになりました。署名付きアプリケーションをインストールするには、デバイスで署名付き検証を有効にする必要があります。署名付き検証を有効にするには、次の手順を実行します。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#app-hosting signed-verification
Router(config)#
Router(config)#exit
```

署名付き検証を有効にした後、「IOx アプリケーションホスティング」の「アプリケーションのインストールとアンインストール」の項の手順に従ってアプリケーションをインストールします。



第 9 章

Cisco IOS-XE 17.3.1 の新機能

IOS-XE リリース 17.3.1 の IR1101 で使用可能な新機能は次のとおりです。

IO ポートに対する YANG のサポート

この機能により、コマンド ライン インターフェイスと YANG モデル間の互換性が向上します。Cisco IOS-XE YANG データモデルは次のとおりです。

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

各リリースにはディレクトリがあり、17.3.1 リリースは 1731 の下にあります。デジタル IO の 2 つのモジュールは、Cisco-IOS-XE-digital-io-oper と Cisco-IOS-XE-digitalio です。

次に、関連する使用可能な IOS-XE CLI コマンドを示します。

コマンドの表示

- show run
- show alarm
- show led

コンフィギュレーション コマンド

- alarm contact attach-to-iox
- no alarm contact attach-to-iox
- alarm contact 1 enable enable
- no alarm contact <1-4> enable
- alarm contact <1-4> application <wet | dry>
- no alarm contact <1-4> application
- alarm contact <1-4> description <alarm description>

- no alarm contact <1-4> description
- alarm contact <1-4> severity <critical | major | minor | none>
- no alarm contact <1-4> severity
- alarm contact <1-4> threshold <1600-2700>
- no alarm contact <1-4> threshold
- alarm contact <1-4> trigger <closed | open>
- no alarm contact <1-4> trigger
- alarm contact <1-4> output <1 | 0>
- alarm contact <1-4> output relay temperature <critical | major | minor>
- alarm contact <1-4> output relay input-alarm <0-4>
- no alarm contact <1-4> output

Security-Enhanced Linux（SELinux）のサポート

Security-Enhanced Linux は Linux カーネルと一部のユーティリティに対する一連のパッチであり、強力で柔軟性の高い強制アクセス制御（MAC）アーキテクチャをカーネルの主要なサブシステムに導入します。SELinux には機密性と整合性の要件に基づいて情報を分離するための拡張メカニズムが備わっています。これにより、アプリケーションのセキュリティメカニズムの改ざんやバイパスの脅威に対処し、悪意のあるアプリケーションや欠陥のあるアプリケーションによって引き起こされる可能性のある障害を封じ込めることができます。

SELinux はユーザプログラムやシステムサーバを、ジョブを実行するために必要になる最小限の権限に制限する強制アクセス制御ポリシーを適用します。これにより、侵害された場合（バッファのオーバーフローや設定ミスなどによって）害を生じさせるこれらのプログラムやデーモンの能力が削減または排除されます。この制限メカニズムは、従来の Linux アクセス制御メカニズムとは独立して動作します。

SELinux 機能を有効化または操作するために必要な追加の要件や設定手順はありません。ソリューションは、サポートされているプラットフォームの基本 IOS-XE ソフトウェアの一部として、デフォルトで有効または動作可能になります。

次に、SELinux 関連の監査ログを表示するために定義された拡張 show コマンドを示します。

show platform software audit all

show platform software audit summary

show platform software audit switch *<<1-8> | active | standby> <FRU identifier from a drop-down list>*

コマンドの例

次に、**show software platform software audit summary** コマンドの出力例を示します。

```
Device# show platform software audit summary
=====================================
AUDIT LOG ON switch 1
-------------------------------------
```

```
AVC Denial count: 58
===================================
```

次に、**show software platform software audit all** コマンドの出力例を示します。

```
Device# show platform software audit all
===================================
AUDIT LOG ON switch 1
-----------------------------------
========== START ============
type=AVC msg=audit(1539222292.584:100): avc:  denied  { read } for  pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc:  denied  { getattr } for  pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc:  denied  { getattr } for  pid=14028 comm="ls"
 path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
 name="crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc:  denied  { execute } for  pid=8300 comm="sh"
 name="id" dev="loop0" ino=6982
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
========== END ============
```

（簡潔にするために出力は省略）

次に、**show software platform software audit switch** コマンドの出力例を示します。

```
Device# show platform software audit switch active R0
========== START ============
type=AVC msg=audit(1539222292.584:100): avc:  denied  { read } for  pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc:  denied  { getattr } for  pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc:  denied  { getattr } for  pid=14028 comm="ls"
 path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
 name="crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc:  denied  { execute_no_trans } for  pid=8600
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc:  denied  { execute_no_trans } for  pid=9307
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc:  denied  { name_connect } for  pid=26421
```

```
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc:  denied  { execute_no_trans } for  pid=10057
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc:  denied  { execute_no_trans } for  pid=10858
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc:  denied  { execute_no_trans } for  pid=11579
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc:  denied  { execute_no_trans } for  pid=12451
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
========== END ============
====================================
```

Syslog メッセージリファレンス

機能重大度ニーモニック

- %SELINUX-3-MISMATCH

重大度の意味

- エラーレベルログ

メッセージの説明

- リソースのアクセスポリシーが定義されていないプロセスによって、リソースアクセスが行われました。操作にフラグが付けられましたが、拒否されませんでした。
- 操作は正常に続行され、中断されませんでした。操作が拒否されたプロセスによるリソースアクセスについてのポリシーが欠落していることに関してシステムログが生成されました。

推奨処置

- 次の関連情報を添付ファイルとして CISCO TAC にご連絡ください。
  - コンソールまたはシステムログに出力されるとおりのメッセージ。
  - 「show tech-support」の出力（テキストファイル）
  - 次のコマンドを使用したボックスからの BTrace ファイルのアーカイブ（「"request platform software trace archive target <URL>"」）。例：Device#**request platform software trace archive target flash:selinux_btrace_logs**

P-LTEAP18-GL モデム PID に対するサポートの追加

P-LTEAP18-GL PID は Telit モデム LM960 モデムを使用します。すべての IR1101 モデムの詳細については、次を参照してください。

https://www.cisco.com/c/en/us/td/docs/routers/access/1101/b_IR1101HIG/b_IR1101HIG_chapter_01.html#con_1161147

初期ブートアップセキュリティの改善点

この項の内容は、次のとおりです。

デフォルトパスワード変更の適用

以前のソフトウェアバージョンでは、ユーザが新しいイネーブルパスワードの設定をバイパスできました。工場出荷時の状態へのリセット後、または工場出荷時の状態からデバイスを最初に起動すると、コンソールに次のプロンプトが表示されます。

Would you like to enter the initial configuration dialog? [yes/no]:

以前のソフトウェアバージョンでは **no** の応答が許可されており、イネーブルパスワードが空白のままのデバイスは**Router>**プロンプトになりました。この時点でルータを設定し、イネーブルパスワードが空白のまま稼働状態にすることができます。

以前のドキュメントでは、**enable password** コマンドの代わりに **enable secret** コマンドを使用することを推奨しています。これは、暗号化アルゴリズムが改善されるためでした。

17.3.1 以降では、初期のダイアログが強制的に新しいイネーブルパスワードを設定し、かつ **enable secret** コマンドを代わりに使用して適用するよう変更されました。次に、例を示します。

```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: router-1

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: ********
  Confirm enable secret: ********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: **********

The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: *********
  Configure SNMP Network Management? [yes]: no
```

```
Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0

Configuring interface Ethernet0/0:
  Configure IP on this interface? [yes]: no

The following configuration command script was created:
hostname router-1
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
.
.
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
```

次に、初期設定ダイアログに **no** と応答した場合の動作の例を示します。

```
Would you like to enter the initial configuration dialog? [yes/no]: no
The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: ********
  Confirm enable secret: ********
Would you like to terminate autoinstall? [yes]: yes

.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
```

最初のログイン時にイネーブルシークレットが要求され、管理者がパスワードを入力すると、管理者が入力したパスワードは常にマスクされます。管理者が脆弱なパスワードを入力すると、強力なパスワード（つまり、大文字と小文字、特殊文字、数字などの標準的な組み合わせ）を入力するように求められます。プロンプトは、管理者が強力なパスワードを入力するまで表示されます。管理者は、強力なシークレットパスワードを2回入力して、管理者が設定したシークレットを確認する必要があります。

Telnet と HTTP

Telnet と HTTP のブート設定が変更されました。工場出荷時の状態へのリセット後または工場出荷時の状態からデバイスを初めて起動した場合は、次の処理が行われます。

- Telnet を無効にする。
- HTTPS サーバを無効にする。HTTP クライアントが動作する。
- SSH の有効化

• HTTPS サーバを有効にする。

Note：これは IR1101 にのみ適用され、他の IoT ルータの設定は変わりません。

初期ブートアップセキュリティの改善点

この項の内容は、次のとおりです。

デフォルトパスワード変更の適用

以前のソフトウェアバージョンでは、ユーザが新しいイネーブルパスワードの設定をバイパスできました。工場出荷時の状態へのリセット後、または工場出荷時の状態からデバイスを最初に起動すると、コンソールに次のプロンプトが表示されます。

Would you like to enter the initial configuration dialog? [yes/no]:

以前のソフトウェアバージョンでは **no** の応答が許可されており、イネーブルパスワードが空白のままのデバイスは**Router>**プロンプトになりました。この時点でルータを設定し、イネーブルパスワードが空白のまま稼働状態にすることができます。

以前のドキュメントでは、**enable password** コマンドの代わりに **enable secret** コマンドを使用することを推奨しています。これは、暗号化アルゴリズムが改善されるためでした。

17.3.1 以降では、初期のダイアログが強制的に新しいイネーブルパスワードを設定し、かつ **enable secret** コマンドを代わりに使用して適用するよう変更されました。次に、例を示します。

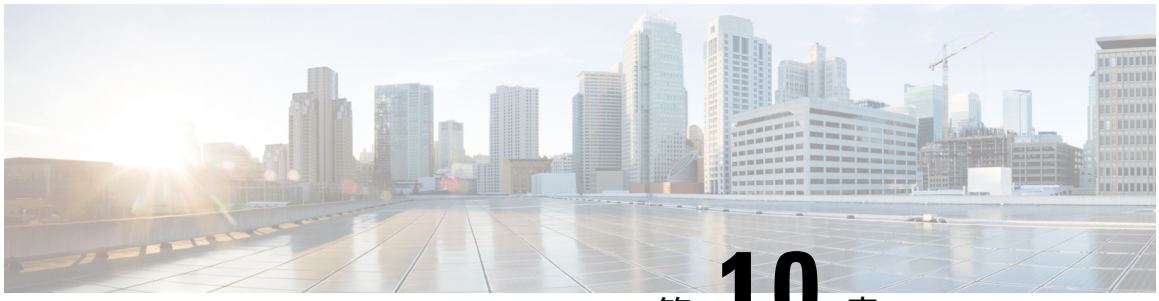
```
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [Router]: router-1

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: ********
  Confirm enable secret: *********

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: **********

The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: *********
  Configure SNMP Network Management? [yes]: no

Enter interface name used to connect to the
management network from the above interface summary: Ethernet0/0

Configuring interface Ethernet0/0:
  Configure IP on this interface? [yes]: no
```

```
The following configuration command script was created:
hostname router-1
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
.
.
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: 2
.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
```

次に、初期設定ダイアログに **no** と応答した場合の動作の例を示します。

```
Would you like to enter the initial configuration dialog? [yes/no]: no
The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: ********
  Confirm enable secret: ********
Would you like to terminate autoinstall? [yes]: yes

.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
```

最初のログイン時にイネーブルシークレットが要求され、管理者がパスワードを入力すると、管理者が入力したパスワードは常にマスクされます。管理者が脆弱なパスワードを入力すると、強力なパスワード（つまり、大文字と小文字、特殊文字、数字などの標準的な組み合わせ）を入力するように求められます。プロンプトは、管理者が強力なパスワードを入力するまで表示されます。管理者は、強力なシークレットパスワードを2回入力して、管理者が設定したシークレットを確認する必要があります。



第 10 章

Cisco IOS-XE 17.4.1 の新機能

次に、IOS-XE リリース 17.4.1 の IR1101 で使用可能な新機能を示します。

Cisco IOS-XE 17.4.1 の機能

次の機能が IoT ルーティングに導入されました。

Cisco Cyber Vision サポート機能については、この章で後述します。

アウトオブバンド管理については、次を参照してください。 https://www.cisco.com/c/en/us/td/docs/routers/access/1101/software/configuration/guide/b_IR1101config/m-out-of-band-management.html

Small Form-Factor Pluggable（SFP）ネットワーク インターフェイス モジュールを使用した DSL 機能は次のとおりです。 https://www.cisco.com/c/en/us/td/docs/routers/access/1101/software/configuration/guide/b_IR1101config/m_configuring_dsl.html

Cyber Vision のサポート

Cisco Cyber Vision Center（CVC）は、制御ネットワークとデータネットワークをリアルタイムでモニタすることにより、産業用制御システム（ICS）全体の産業用 IoT ネットワークの可視性を高めます。リリース 17.4 以降の IoT IOS-XE プラットフォームでは、IOX Cyber Vision センサーを展開することで CVC の統合がサポートされます。このセンサーを IoT ルータに展開すると、プラットフォームは IOX アプリケーションからのトラフィックを Cyber Vision Center に転送してリアルタイムでモニタし、キャプチャした PCAP ファイルを IOX アプリケーションから Vision Center に転送できます。

IOS-XE プラットフォームでの Cyber Vision Center（CVC）の展開

ステップ 1 次の場所から、シスコがサポートしている Cyber Vision IOX アプリケーションをダウンロードします。

https://software.cisco.com/download/home/286325414/type/286325316/release/3.1.1?catid=268438162

Cisco Cyber Vision Sensor IOx Application 3.1.1 for IE3400 and IR1101 を選択します。

ステップ 2 仮想マシンまたは任意のハイパーバイザに CVC バージョン 3.1.1 をインストールします。次の場所は、さまざまなバージョンの CVC のダウンロードリンクです。

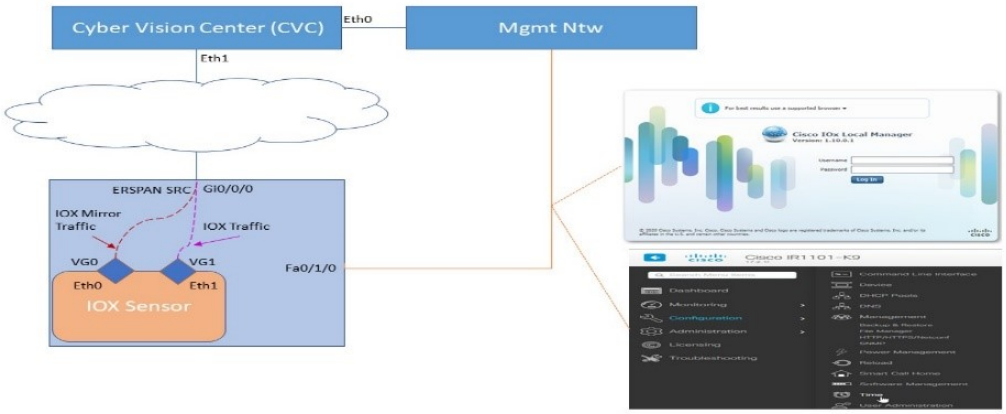
https://software.cisco.com/download/home/286325414/type

Cisco Cyber Vision リリース 3.1.1 のリリースノート：

https://www.cisco.com/c/dam/en/us/td/docs/security/cyber_vision/Cisco-Cyber-Vision_Release-Note-3-1-1.pdf

ステップ 3 CVC センサーには 2 つの VirtualPort Group インターフェイスが必要です。一つは IOx トラフィック用であり、もう一つは物理インターフェース、SVI、トンネルインターフェース等の ERSPAN ソースでミラーされたトラフィック用です。次の図を参照してください。

図 *22 : L3* インターフェイスを介した *CVC*



ステップ 4 CVC センサーの展開は、LMGUI または CLI からインストールできます。

仮想ポートグループとともに L3 設定を介した ERSPAN の設定例

物理ポートと仮想ポートの設定：

```
interface virtualportgroup 0
ip address 169.254.1.1 255.255.255.252
interface virtualportgroup 1
ip nat inside
ip address 169.254.0.1 255.255.255.252
interface gi0/0/0
ip address 101.0.0.151 255.255.255.0
ip nat outside
no shut
```

ERSPAN 設定：

```
monitor session 1 type erspan-source
source interface Gi0/0/0
no shutdown
destination
erspan-id 1
mtu 1464
ip address 169.254.1.2
origin ip address 169.254.1.1
```

アクセスリストを使用した NAT 設定：

```
ip nat inside source list NAT_ACL interface Gi0/0/0 overload
ip access-list standard NAT_ACL
 10 permit 169.254.0.0 0.0.0.3
```

CLI からのインストール

CLIを使用してアプリケーションをインストールするには、CVCセンサーをブートフラッシュ、USB、または mSATA にコピーします。次に、アプリケーションホスティング CLI を使用してアプリケーションをインストールし、Dockerオプションを指定してからアプリケーションをアクティブ化します。次に例を示します。

```
Router(config-if)#iox
Router# app-hosting install app-id <app-id> package {bootflash:/|usbflash0:|msata:}
app-hosting appid  <app-id>
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 169.254.1.2 netmask 255.255.255.252
 app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 169.254.0.2 netmask 255.255.255.252
 app-default-gateway 169.254.0.1 guest-interface 1
 app-resource docker
  run-opts 1 "--rm --tmpfs /tmp:rw,size=128m"
Router# app-hosting {activate|start|stop|deactivate|uninstall} app-id <app-id>
```

LMGUI からのインストール

LMGUI に到達するには、次を設定します。

```
iox
ip http server
ip http secure-server
ip http authentication local
Username cisco privilege 15 password cisco
Login URL: http://<Mgmt_IP>/iox/login
```

その他の詳細については、次を参照してください。 LM GUI を使用した CVC センサーのインストール （94 ページ）

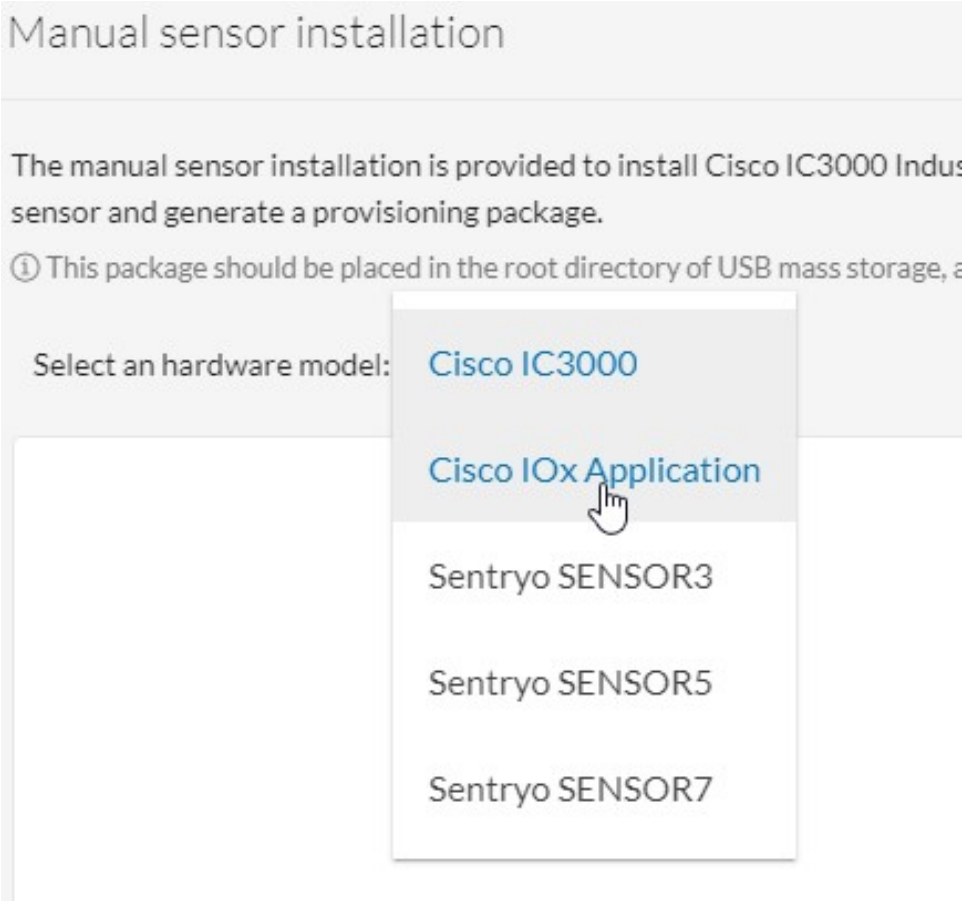
ルータ詳細の登録

ステップ 1 ログインして次の場所に移動し、CVC に IOS-XE ルータの詳細を登録します。

Admin > Sensors > Install Sensor Manually

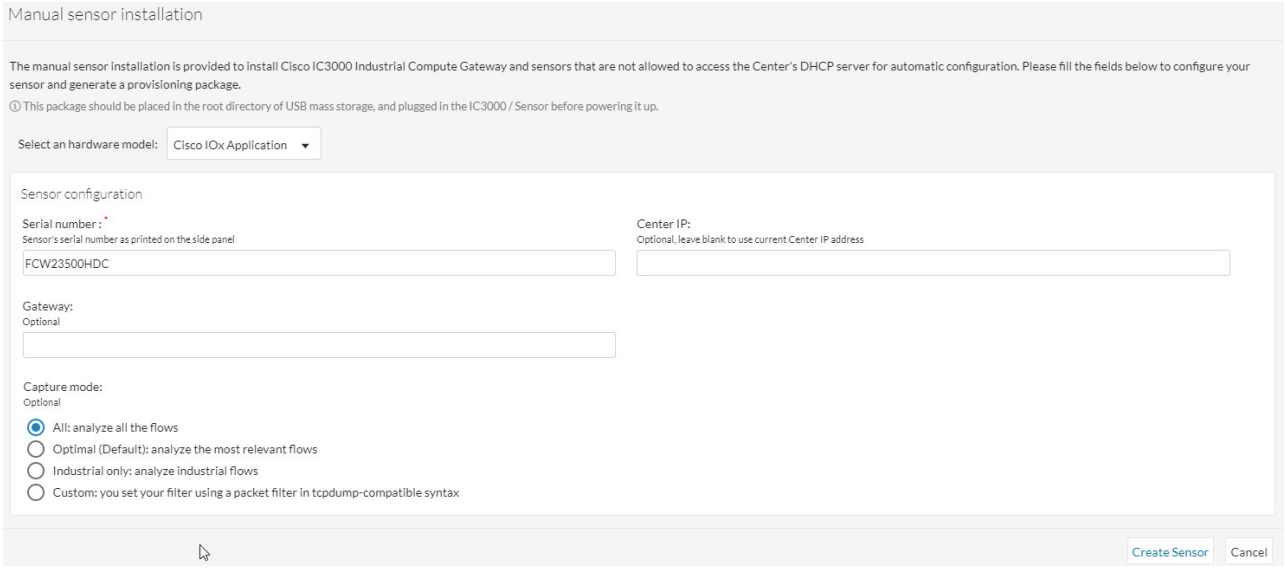
次に、[Cisco IOx Application] をクリックします。次を参照してください。

図 *23 :* センサーのインストール



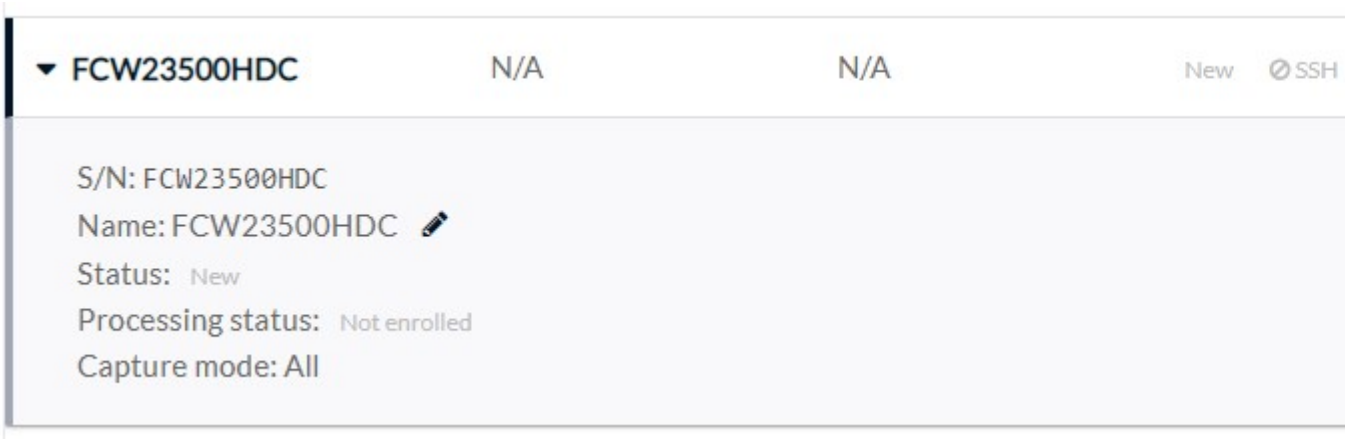
ステップ 2 ルータのシリアル番号を入力します。**show inventory** の出力と完全に一致する必要があります。次に [**Create Sensor**] をクリックします。次を参照してください。

図 *24* : ルータのシリアル番号



ステップ 3 [Get Provisioning File] をクリックして、CVC からプロビジョニングファイルを生成します。次を参照してください。

図 *25* : プロビジョニングファイルの生成



ステップ 4 ローカルディレクトリにプロビジョニングファイルをダウンロードします。ファイルは次のようなファイル名の zip ファイルとして提供されます。

例：

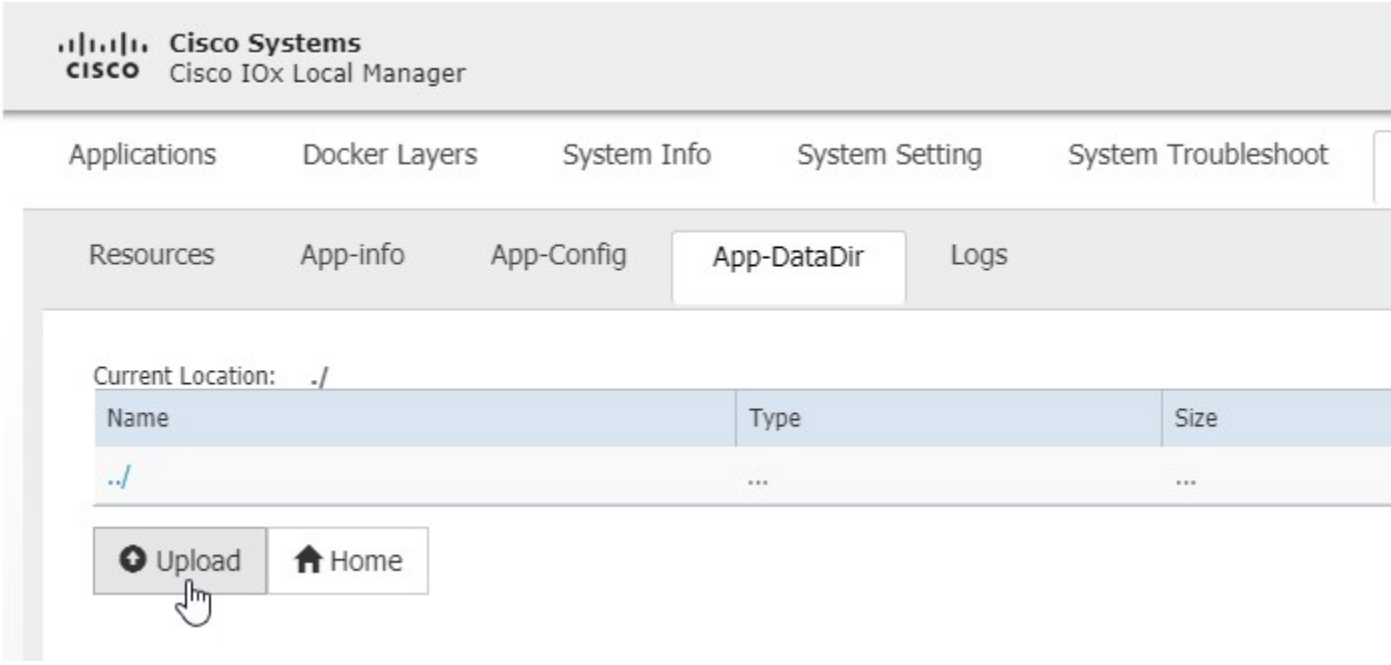
sbs-sensor-config-*<S/N of Router>.zip*

ステップ 5 LM GUI を使用して、プロビジョニングファイルをルータにインポートします。LM GUI アプリケーションから次の場所に移動します。

Applications > CVC App (Application Name) > Manage > App-DataDir

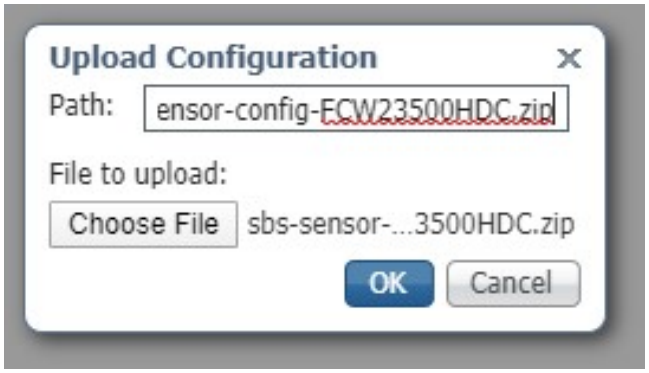
次を参照してください。

図 *26* : プロビジョニングファイルのアップロード



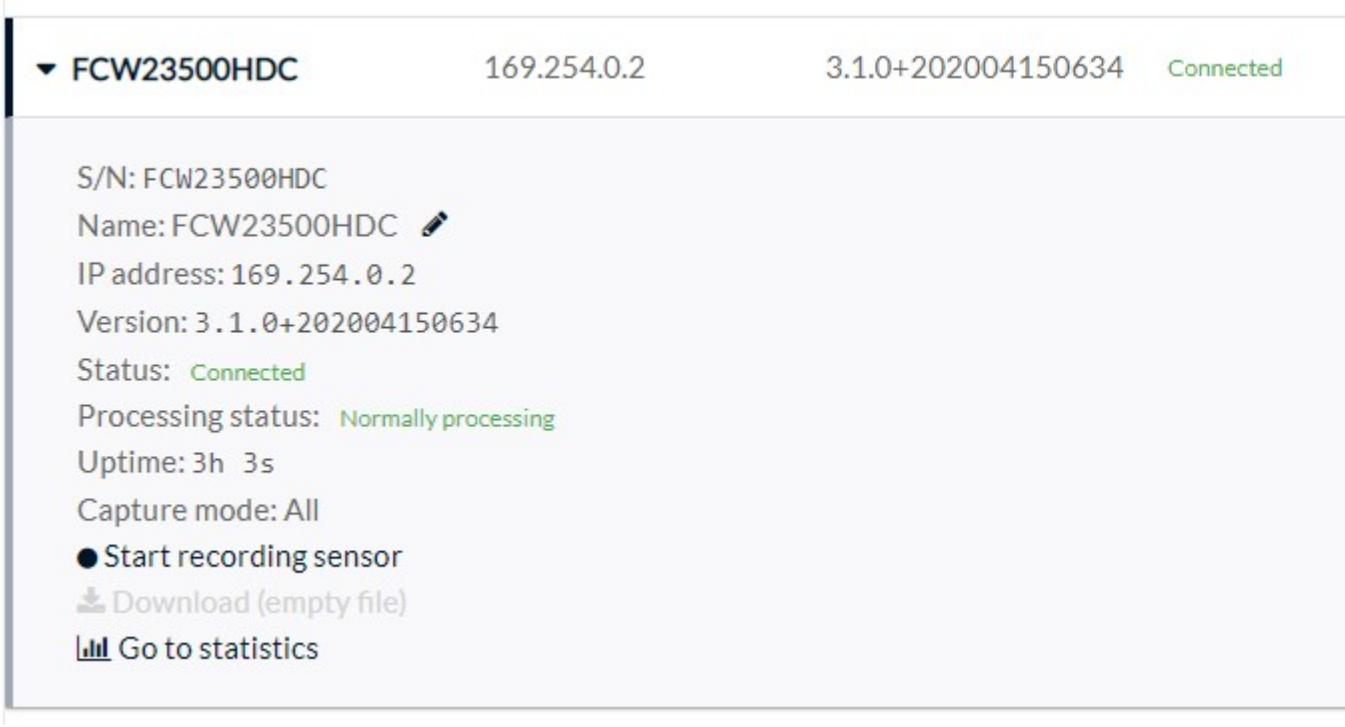
ステップ 6 [**Upload**] をクリックします。[Upload Configuration] ウィンドウが表示されます。ダウンロードしたプロビジョニング済みのファイルを同じ名前で CVC からアップロードします。次を参照してください。

図 *27* : アップロード設定



ステップ 7 CVC の認証を確認します。インストールされているセンサーのステータスが **Connected** または **Waiting for Data** に変更されたかどうかを検証します。次を参照してください。

図 *28 : Sensor Status*



ライブトラフィックのキャプチャ

ステップ 1 CVC とルータ間で日時を同期します。ライブトラフィックをキャプチャするには、ルータと CVC の間に正確なクロック同期が必要です。

ステップ 2 IOX トラフィックをシミュレートするか、またはキャプチャされた PCAP ファイルを再生します。ルータにインストールされている CVC センサーは Docker アプリです。アプリのコンソールにログインするには、次のコマンドを実行します。

例：

```
app-hosting connect app-id <app-name> session
```

ステップ 3 LM-GUI から PCAP ファイルをアプリケーションにアップロードします。次のとおりに移動します。

Applications > CVC App (Application Name) > Manage >App-Dir

次のコマンドは、PCAP ファイルの再生方法を示しています。

例：

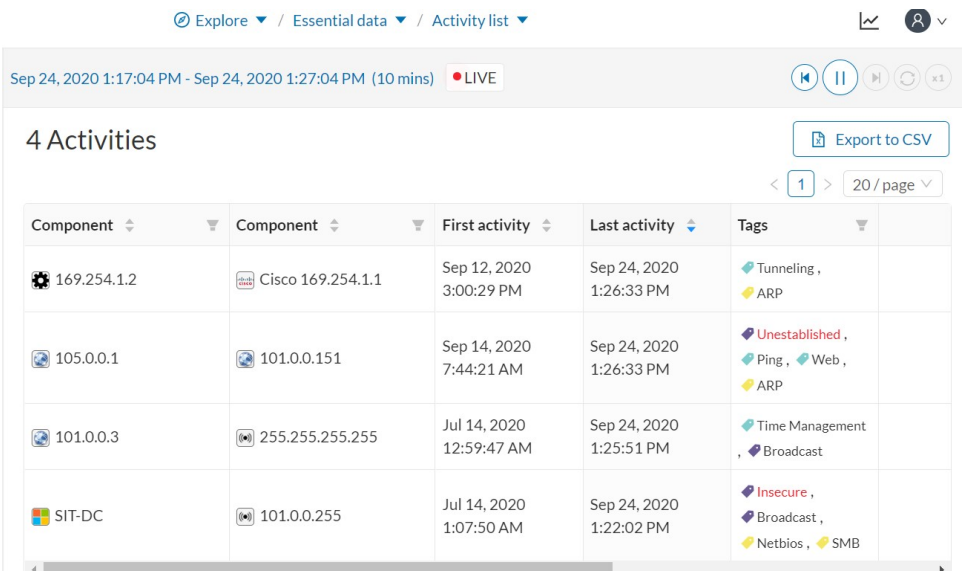
```
Router# show app-hosting list
App id    State
---------------------------------------------
CVC Sensor    RUNNING
```

```
Router# app-hosting connect appid CVCSensor session
sh-5.0#
*Jul 14 08:45:05.603: %SELINUX-3-MISMATCH: R0/0: audispd: type=AVC msg=audit(15! in/busybox.nosuid"
 dev="overlay" ino=72930 scontext=system_u:system_r: polaris_bexecute_*
sh-5.0# flowctl read-capture-file /iox_data/appdata/tl04
OK
sh-5.0#
```

ステップ 4 CVC のトラフィックをモニタします。次の場所に移動します。 **Explore > Essential Data > Activity List**

次を参照してください。

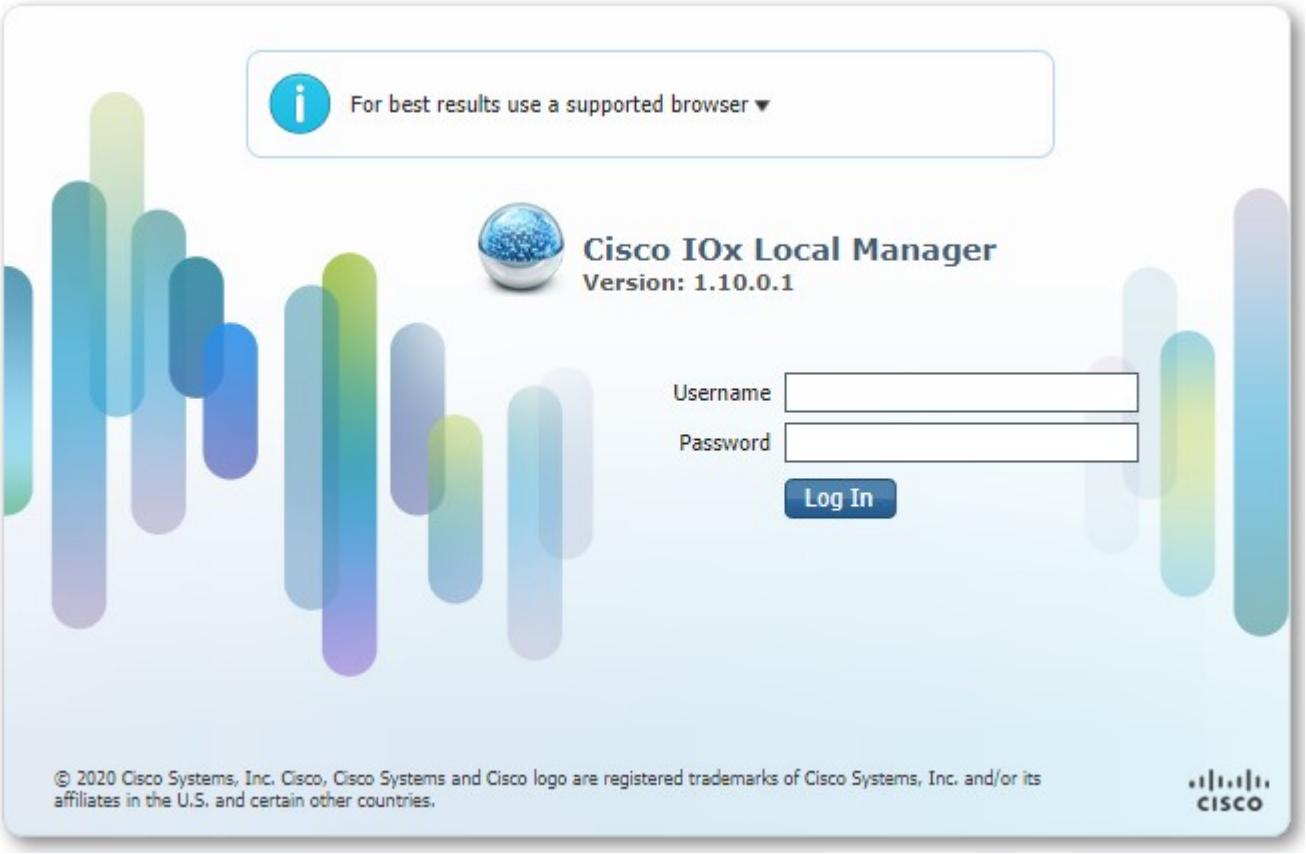
図 *29 : Activity List*



LM GUI を使用した CVC センサーのインストール

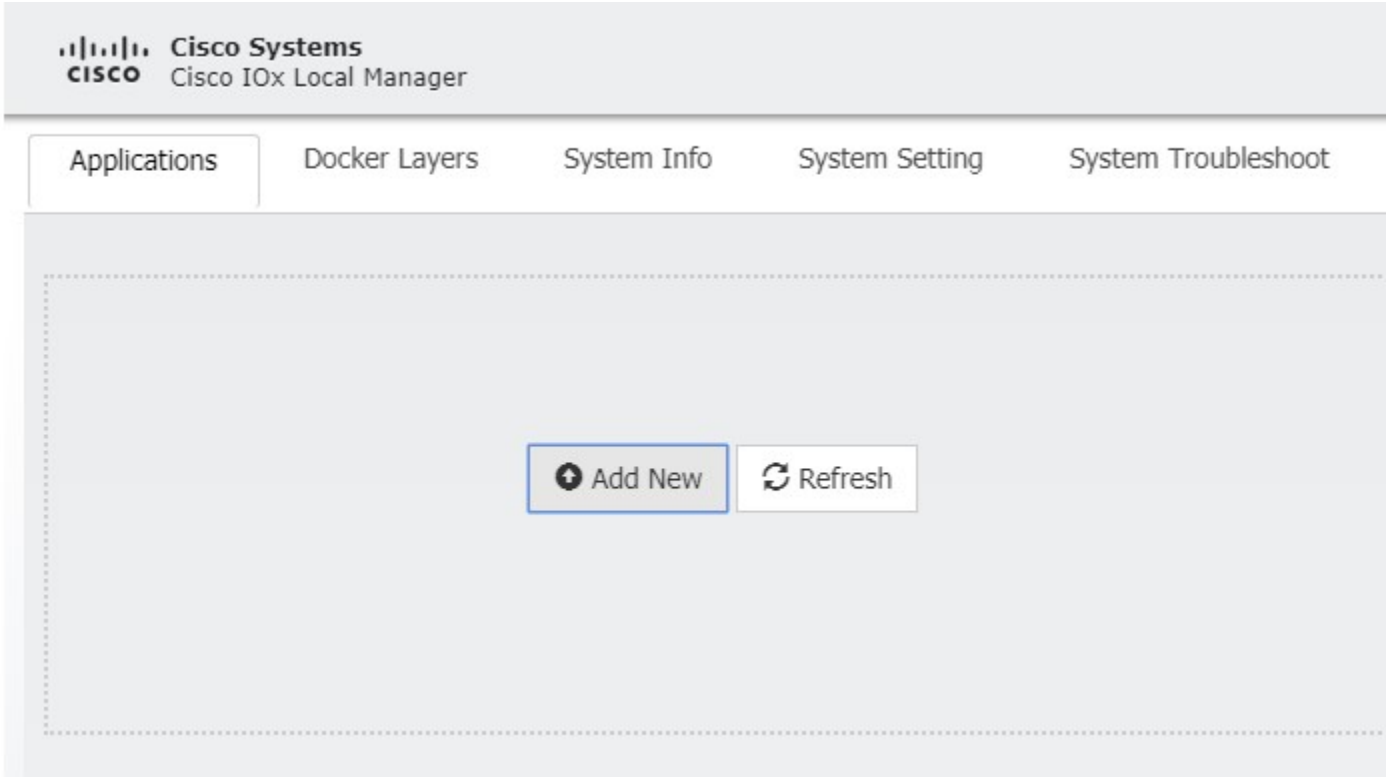
ステップ 1 ユーザアカウントとパスワードを使用してログインします。

図 *30* : ローカルマネージャのログイン



ステップ 2 センサー仮想アプリケーションをインストールします。ログインすると、次のメニューが表示されます。

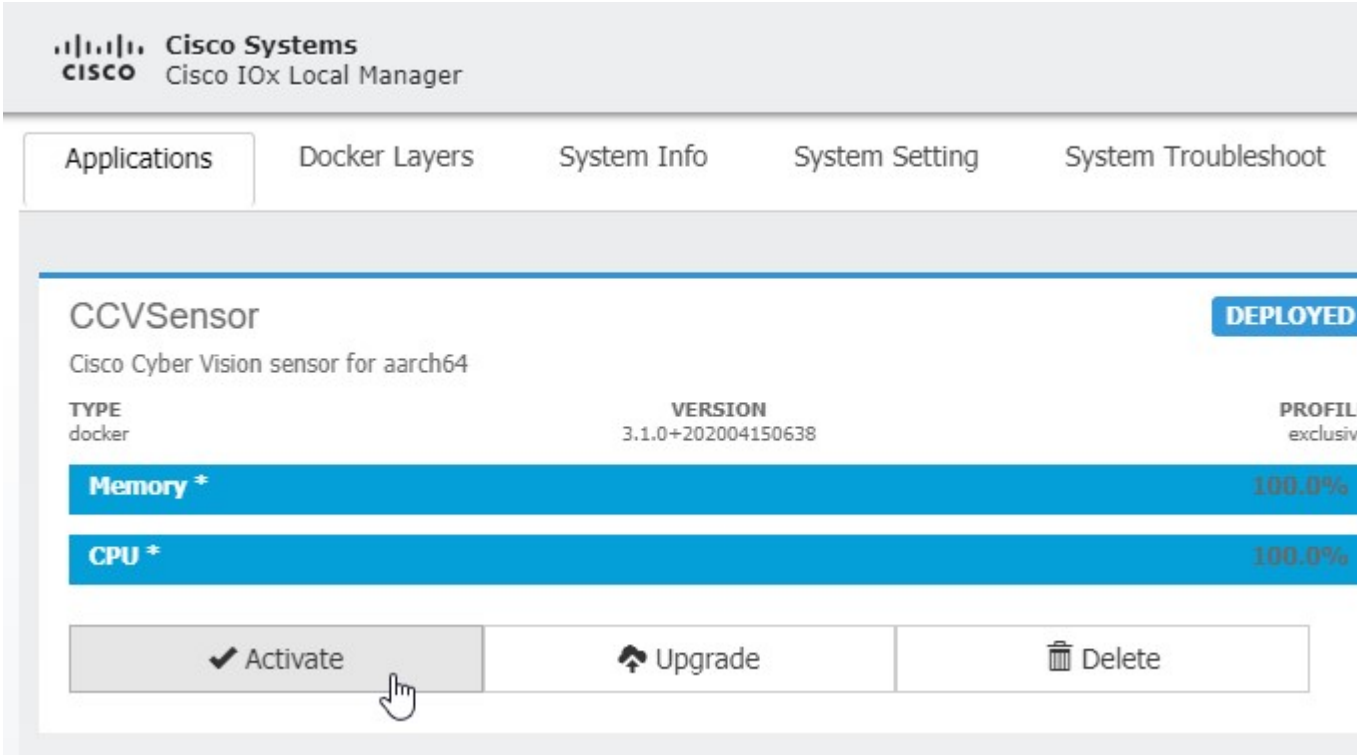
図 *31 : LM GUI* アプリケーションのインストール



ステップ 3 [**Add New**] をクリックします。アプリケーションファイル（CiscoCyberVision-IOx-aarch64-xxx.tar など）に移動します。アプリケーションの名前（**CCVSensor** など）を追加します。

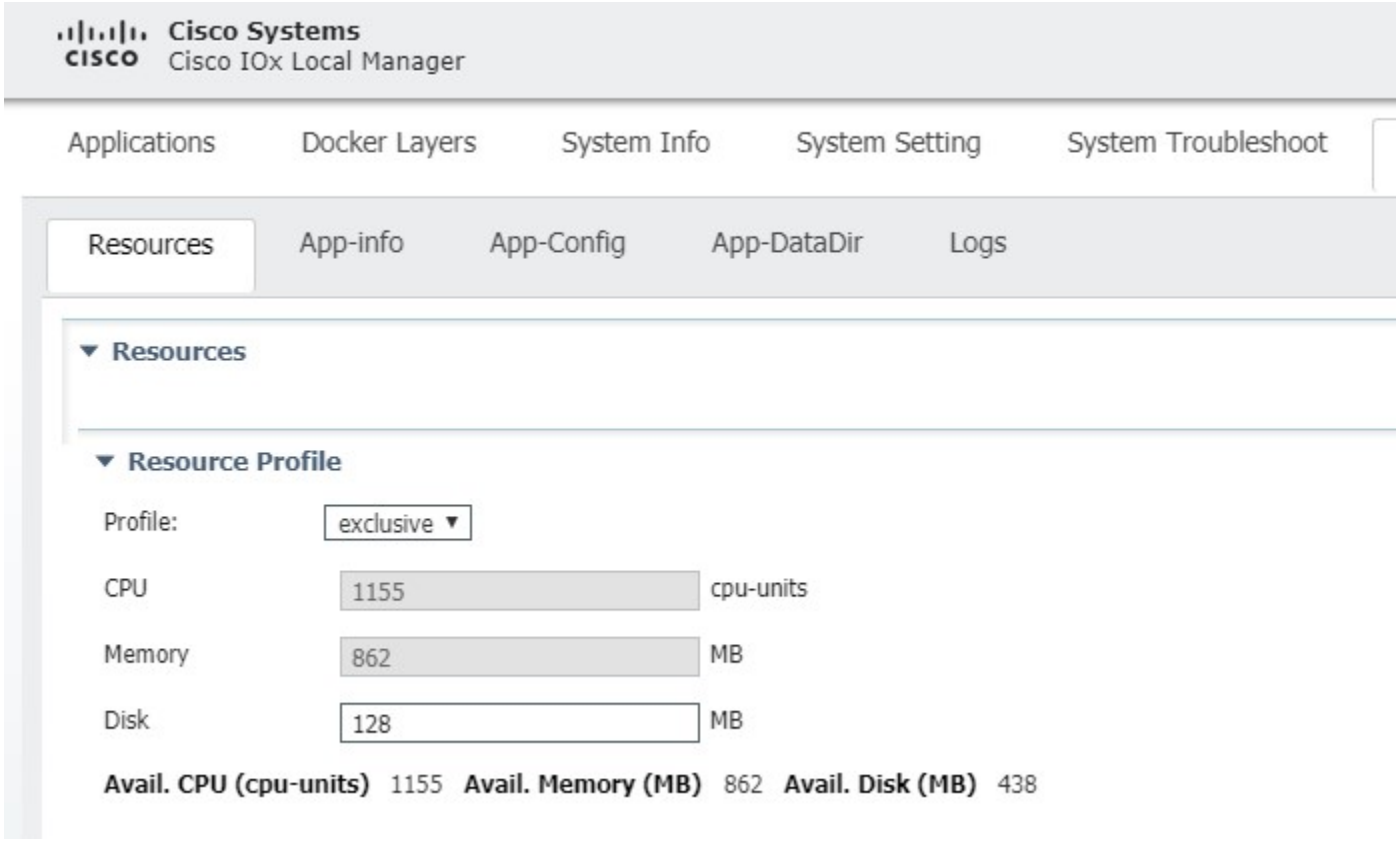
センサー仮想アプリケーションを設定します。次を参照してください。

図 *32 : CCVSensor* のアクティブ化



ステップ 4 **Activate** をクリックして、センサーアプリケーションの設定を起動します。[**CCVSensor**] タブをクリックし、[**Resources**] をクリックします。次を参照してください。

図 *33* : センサー *LM IOXAppDisk* のセットアップ



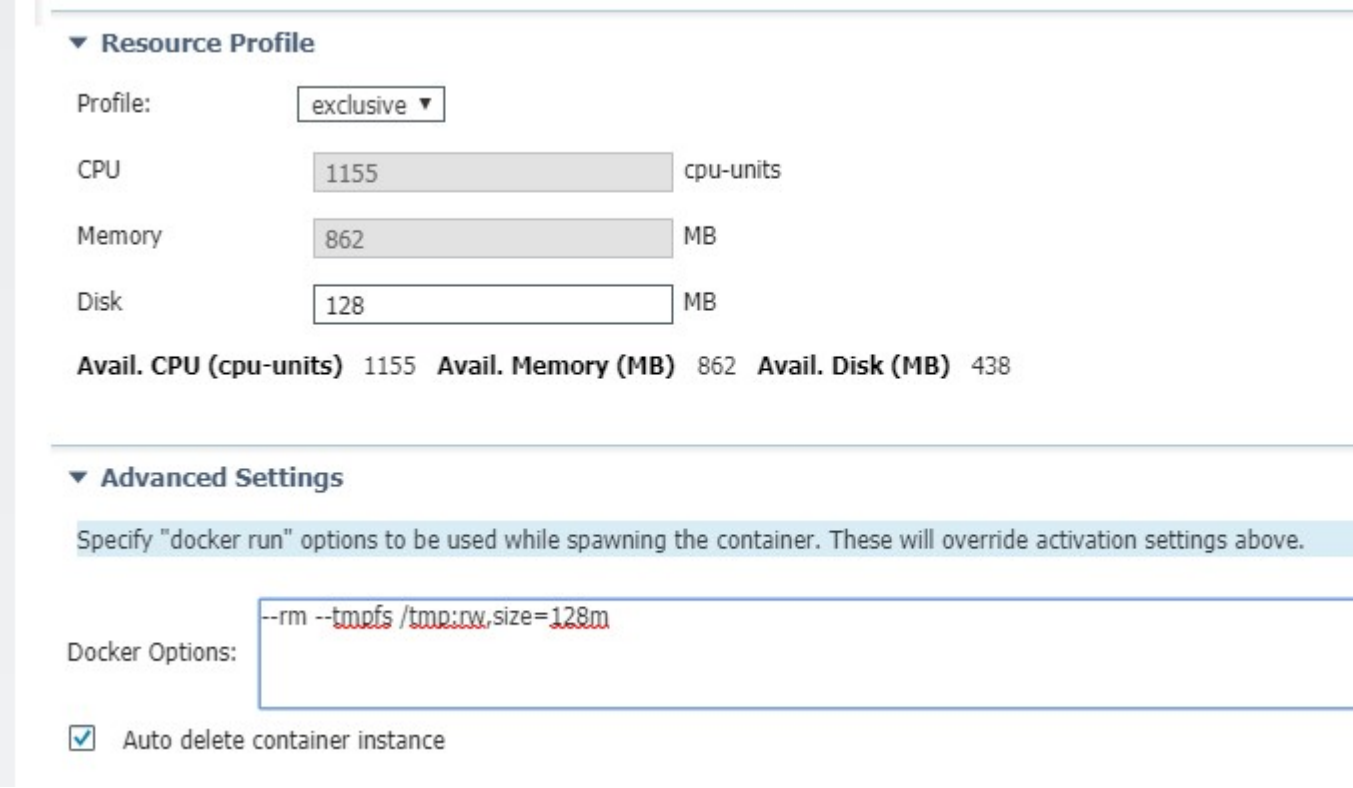
ディスクサイズを 128 MB に変更します。

（注） それ以上の領域を使用しないでください。

ステップ 5 **Advanced Settings** にアクセスします。詳細オプションで、[Docker Options] の横にあるテキスト領域に次を追加して、tmpfs を設定します。

--tmpfs /tmp:rw,size=128m

図 *34 : Advanced Settings*



ステップ 6 **Network Configuration** セクション内のホスト上のインターフェイスにコンテナ内のインターフェイスをバインドします。

次のタスク

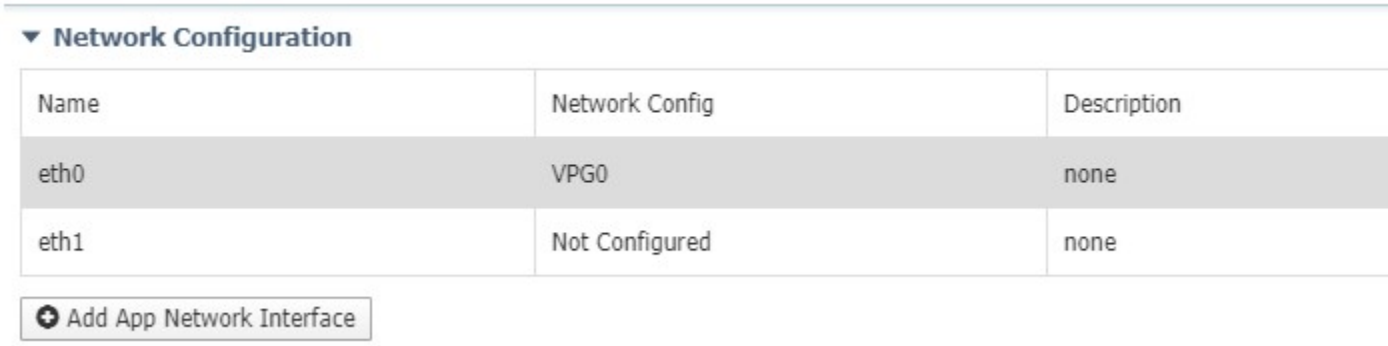
次のセクション（Binding eth0 と Binding eth1）に移動します。

eth0 のバインディング

eth0 を設定するには、次の手順を実行します。

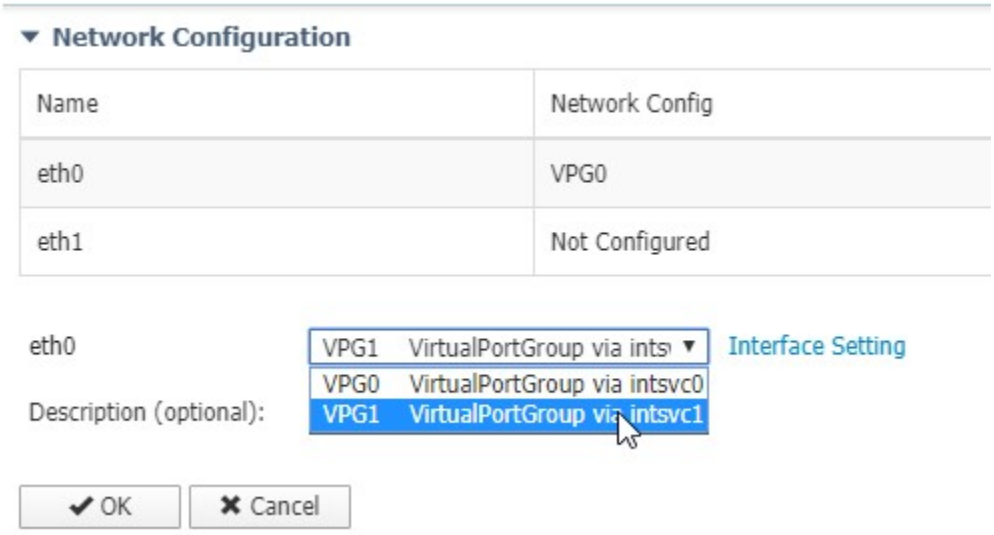
ステップ 1 interface eth0 を選択し、[**edit**] をクリックします。

図 *35 : eth0*



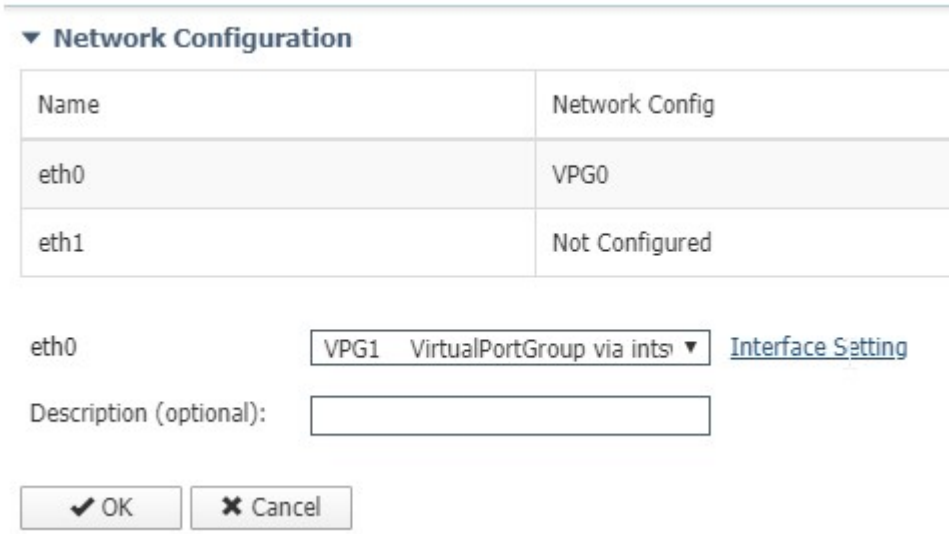
ステップ 2 インターフェイス **VPG1** を選択します。

図 *36 : VPG1*



ステップ 3 [**Interface Setting**] をクリックします。

図 *37* : インターフェイスの設定

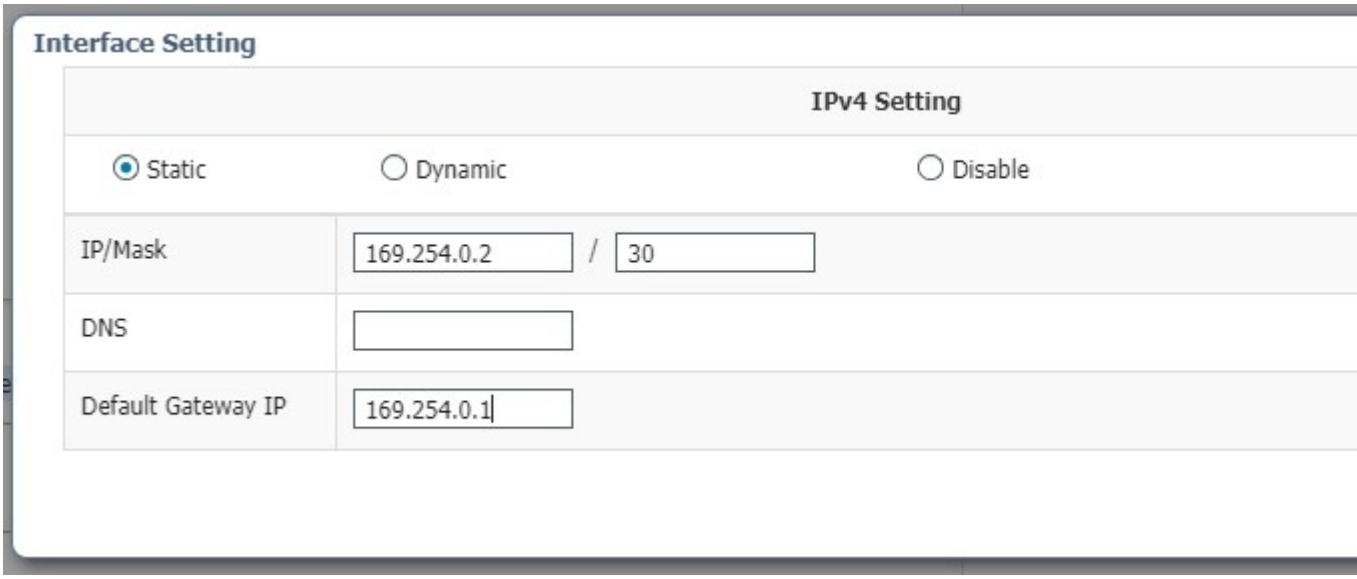


ステップ 4 次の設定を適用します。

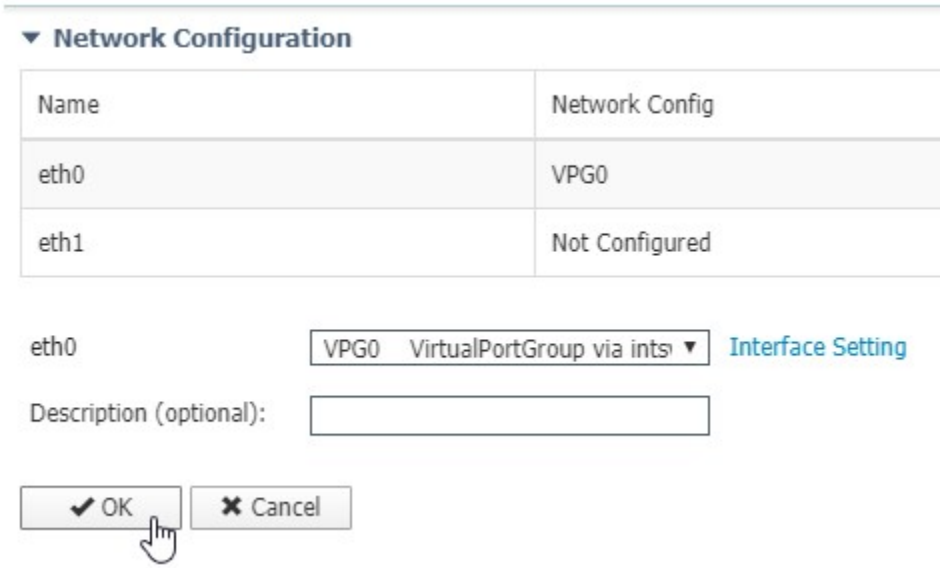
- • **Static** オプションを選択します。
  • IP/Mask で次を追加 **169.254.0.2 / 30**
  • デフォルトゲートウェイの IP は **169.254.0.1**

次に [**OK**] をクリックします。

図 *38* : *IPv4* 設定

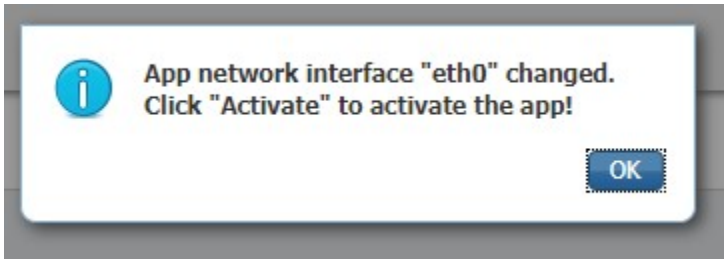


ステップ 5 もう一度 [**OK**] をクリックします。



ステップ 6 [**Activate**（SIP MWI notification mechanism）] ウィンドウが表示されます。[**OK**] をクリックします。

図 *39* : ウィンドウのアクティブ化

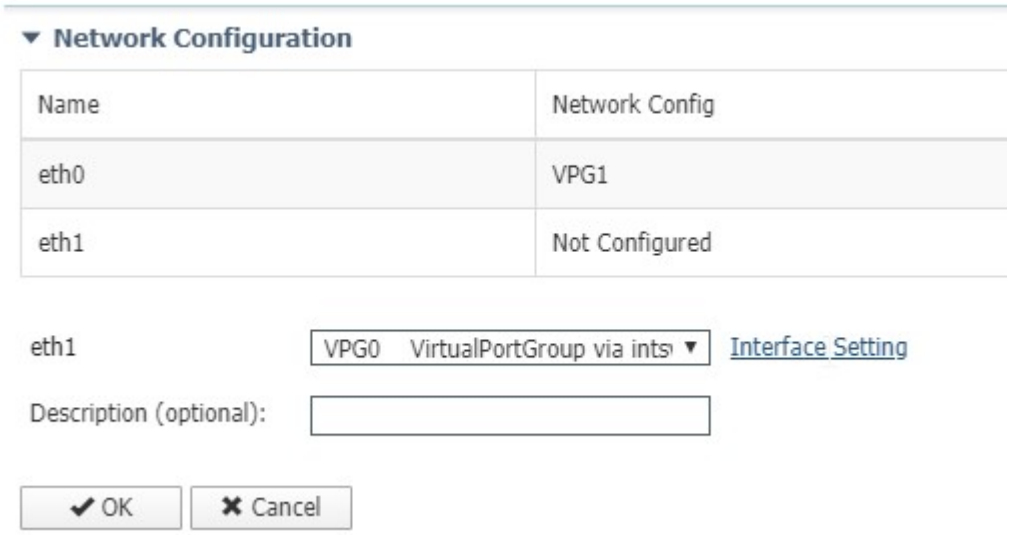


eth1 のバインディング

eth1 インターフェイスを設定するには、次の手順を実行します。

ステップ 1 VPG0 を選択します。

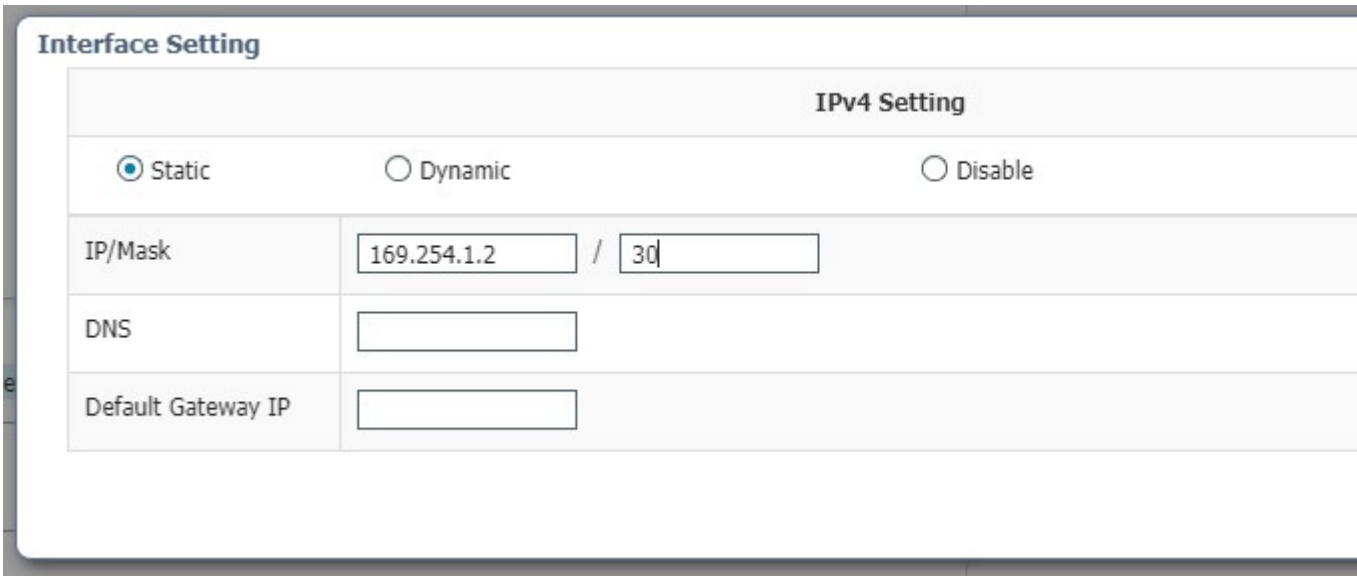
図 *40 : VPG0*



ステップ 2 **Interface Setting** をクリックして、次の設定を適用します。

- • **Static** オプションを選択します。
  • IP/Mask で次を追加 **169.254.1.2 / 30**

図 *41 : IPv4* 設定

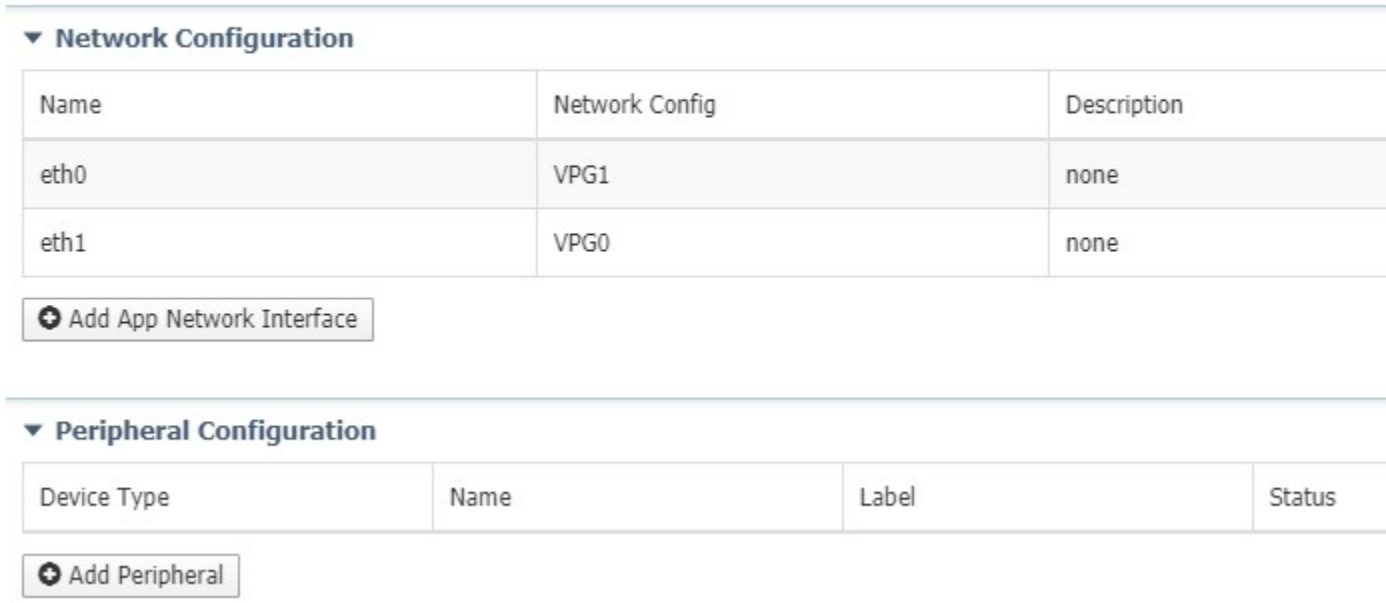


アプリケーションのアクティブ化

これで、センサーアプリケーションがアクティブになります。

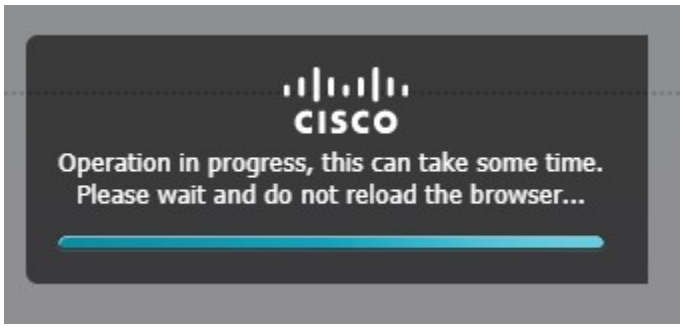
ステップ 1 [**Activate App**] をクリックします。次を参照してください。

図 *42*：アプリケーションのアクティブ化



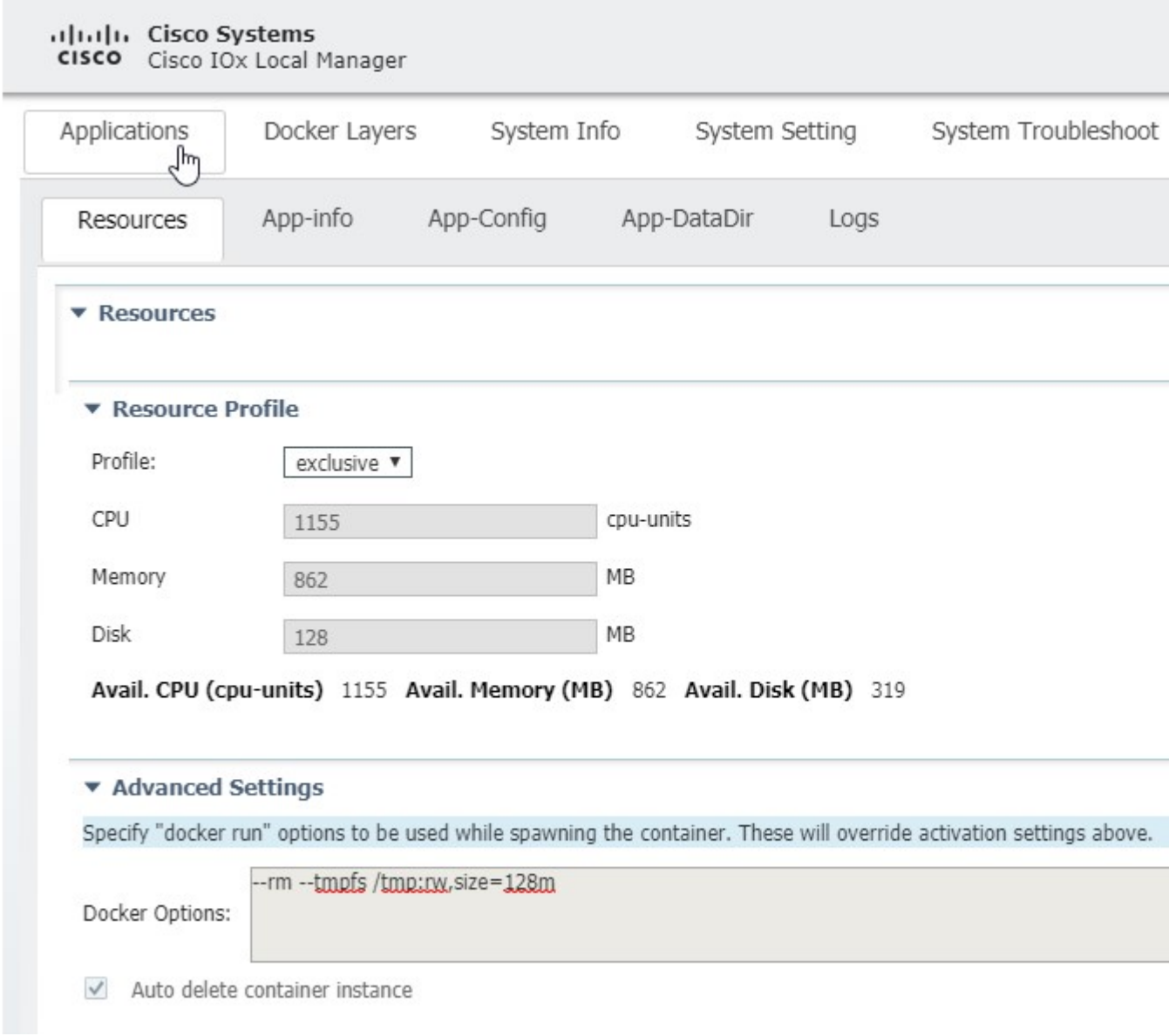
ステップ 2 進捗状況ウィンドウが表示されます。これが完了するまでに数秒かかる場合があります。

図 *43*：アクティブ化の進捗



ステップ 3 [**Applications**] をクリックしてアプリのステータスを表示します。次を参照してください。

図 *44* : アプリケーションのリソース

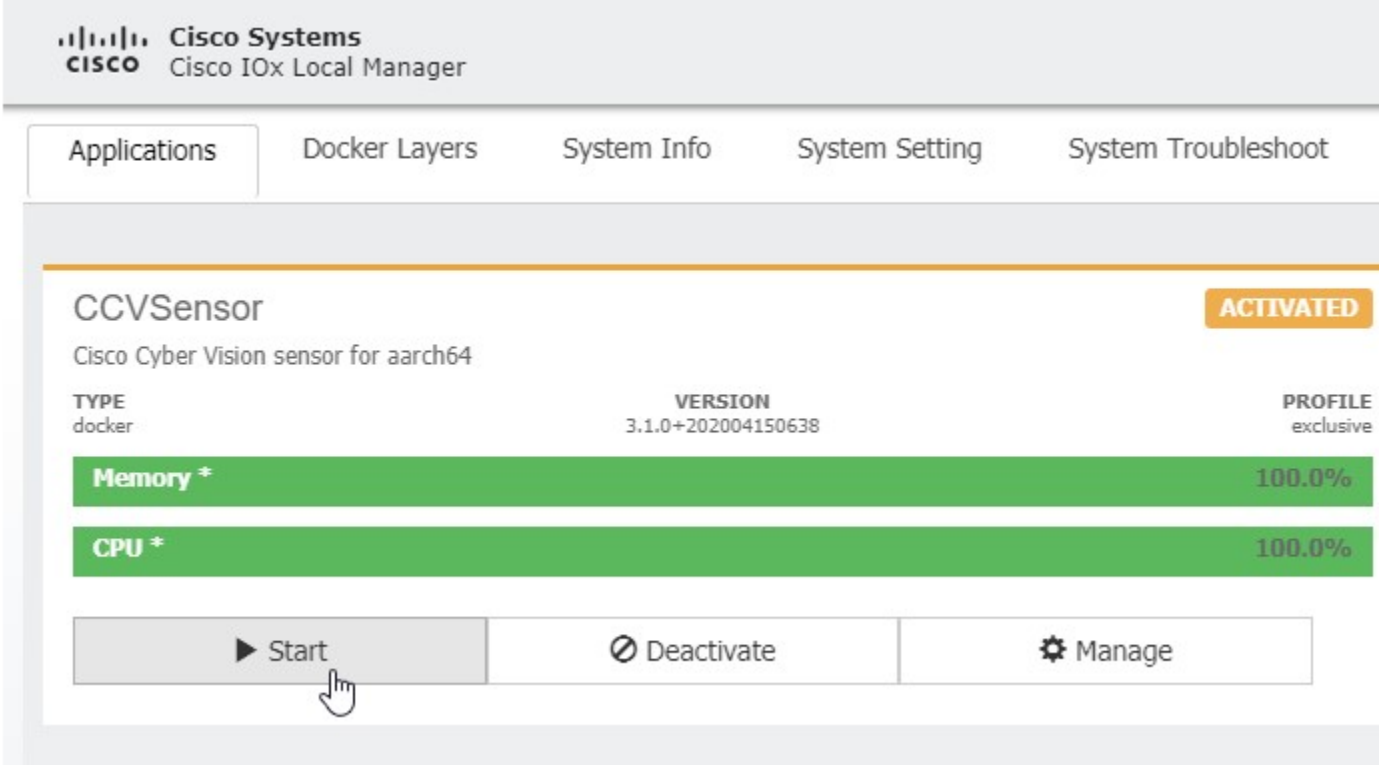


ステップ 4 アプリケーションがアクティブ化されており、起動する必要があります。

アプリケーションの起動

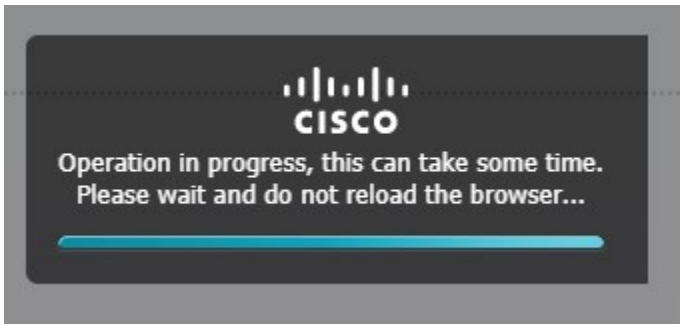
ステップ 1 [**Start**] をクリックします。次を参照してください。

図 *45* : アプリケーションの起動



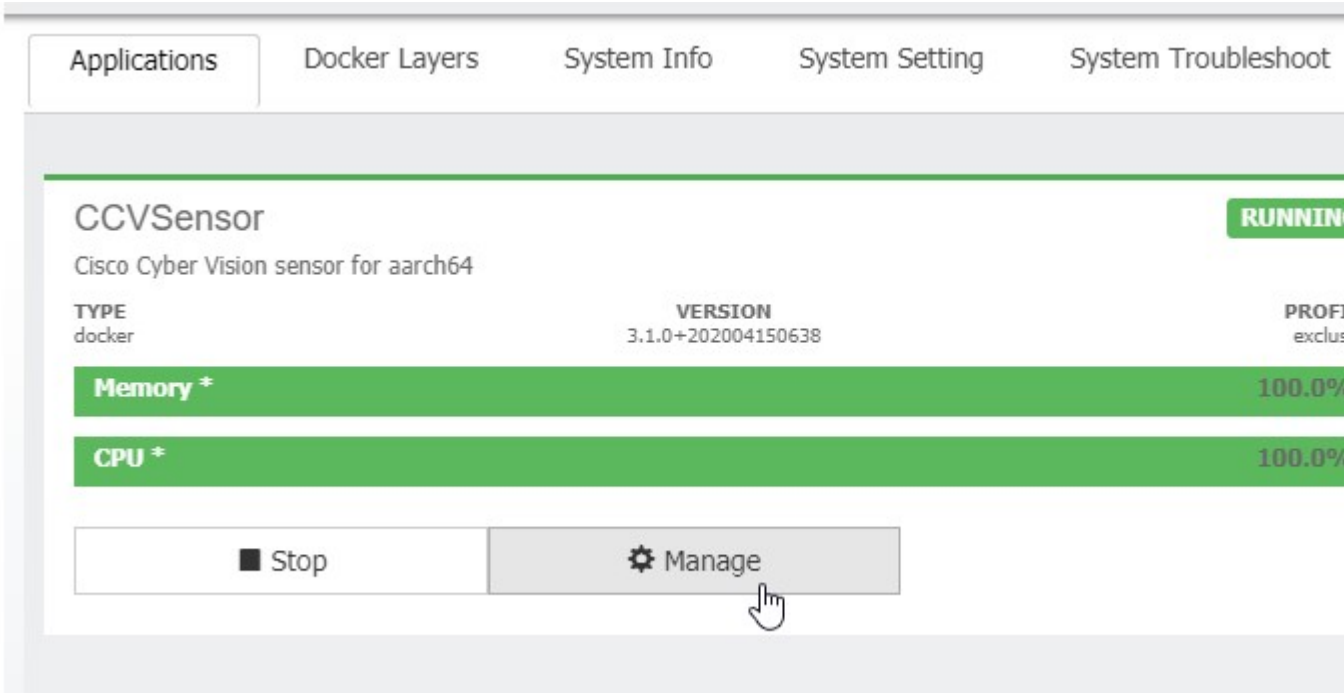
ステップ 2 進捗状況ウィンドウが表示されます。これが完了するまでに数秒かかる場合があります。

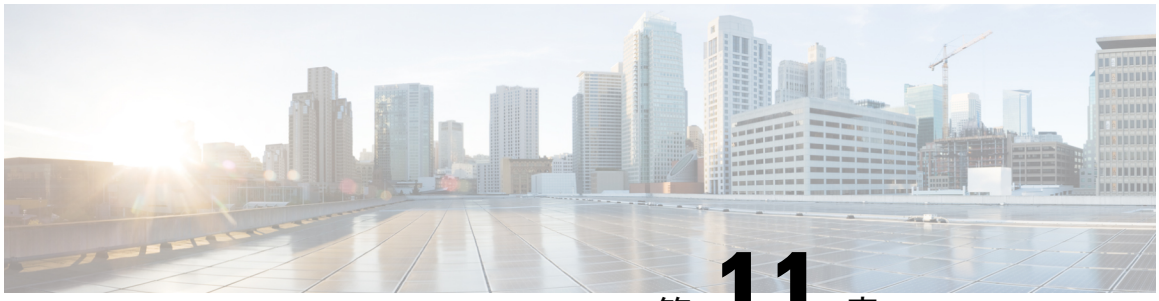
図 *46* : *[Progress]* ウィンドウ



ステップ 3 しばらくすると、アプリのステータスが実行中に変わります。

図 *47* : アプリケーション実行中





第 11 章

Cisco IOS-XE 17.5.1 の新機能

次に、IOS-XE リリース 17.5.1 の IR1101 で使用可能な新機能を示します。

DSL SFP Annex J のサポート

IOS-XE リリース 17.5.1 では、コントローラインターフェイスで Annex-J 設定のサポートが追加されています。

（注） ADSL2+ J はサポートされていますが、ADSL2 J は 17.5.1 ではまだサポートされていません。

Annex-J を有効にするには、次の手順を実行します。

```
router#config term
router(conf)#controller vdsl 0/0/0
router(conf-if)#capability annex-j
router#(conf-if)#exit
router#
```

Annex-J を削除するには、次の手順を実行します。

```
To remove Annex-J:
router#config term
router(conf)#controller vdsl 0/0/0
router(conf-if)#no capability annex-j
router#(conf-if)#exit
router#
```

17.5.1 では、新しいコマンド **rx-padding** が追加されています。このコマンドは、MTU が 64 バイト未満のパケットに使用されます。

重要 サービスプロバイダからのダウンストリームで64mtu未満のフレームが想定される場合、VLAN設定は vlan 96 である必要があります。

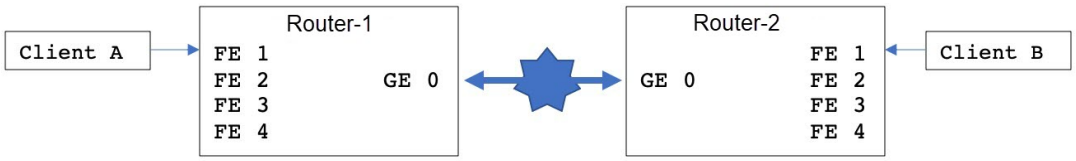
コマンドの例は次のとおりです。

```
router#config term
router#controller vdsl 0/0/0
router(conf-if)#rx-padding
router(conf-if)#end
```

write memを実行して設定を保存します。

VXLAN

VXLAN は、24 ビットのセグメント ID（VXLAN ID の形式）を持つ、MAC in IP/UDP（MAC-in-UDP）カプセル化技術です。大きな VXLAN ID の場合、クラウド ネットワークにおいて、LANセグメントを1600万個まで拡張できます。また、IP/UDP のカプセル化により、各LANセグメントを既存のレイヤ3ネットワーク全体に拡張して、レイヤ3 Equal-Cost Multi-Path（ECMP; 等コストマルチパス）を使用できます。



次の表に、2 つのデバイスの設定を示します。

Router-1	Router-2
bridge-domain 1 member vni 6001 member Vlan100 service-instance 1 ! interface Loopback1 ip address 200.200.200.200 255.255.255.255 ! interface GigabitEthernet0/0/0 ip address 192.168.1.2 255.255.255.0 media-type rj45 ! interface FastEthernet0/0/1 switchport access vlan 100 ! interface Vlan100 no ip address service instance 1 ethernet encapsulation dot1q 100 //untag ! interface nve1 no ip address source-interface Loopback1 member vni 6001 ingress-replication 100.100.100.100 ! ip forward-protocol nd ip pim rp-address 200.200.200.200 ip http server ip http secure-server ip route 0.0.0.0 0.0.0.0 192.168.1.3 !	bridge-domain 1 member vni 6001 member Vlan100 service-instance 1 ! interface Loopback1 ip address 100.100.100.100 255.255.255.255 ! interface GigabitEthernet0/0/0 ip address 192.168.1.3 255.255.255.0 media-type rj45 ! interface FastEthernet0/0/1 switchport access vlan 100 ! interface Vlan100 no ip address service instance 1 ethernet encapsulation dot1q 100 //untag ! interface nve1 no ip address source-interface Loopback1 member vni 6001 ingress-replication 200.200.200.200 ! ip forward-protocol nd ip pim rp-address 100.100.100.100 no ip http server ip http secure-server ip route 0.0.0.0 0.0.0.0 192.168.1.2 !

EM74XX モデムの Dying-Gasp SMS 通知

前提条件：

- ハードウェア周辺機器：P-LTEA-EA、P-LTEA-LA
- 初回リリース：IOS-XE 17.5.1
- ライセンス：Cisco Network-Advantage

EM7430 または EM7455 モデムを使用する Pluggable Interface Module（PIM）には、モジュールへの電力が失われた場合に備えて、モデムに電力を供給するための追加のコンデンサがあります。これにより、モデムの正常な電源オフが可能になります。電力の損失が検出されると、モデムは設定時に dying gasp SMS を送信することが想定されます。

次に、電話番号と SMS メッセージを使用して dying gasp を設定する例を示します。

```
#controller Cellular 0/1/0
#lte dyinggasp sms send 9119110911 "Losing Power"
Warning: Enabling Dying Gasp SMS configuration completed successfully.
Please reset Modem for the changes to take effect
```

設定手順

ステップ	コマンド	目的
1	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。
2	controller Cellular <slot>	セルラーモジュールコントローラ スロットのインターフェイス コマンド モードを開始します。
3	lte dyinggasp detach enable	送信切断要求で dying-gasp 機能を有効にします。
4	lte dyinggasp sms send <phone number> <SMS message>	プラットフォームまたはモジュールの電源がオフになったときに、モデムから送信する SMS テキストメッセージおよびテキストメッセージの内容を受信する電話番号を設定します。
5	exit	コンフィギュレーションを終了します。
6	write mem	ルータ設定の変更を保存します。

設定例

次の例は、スロット 0/1/0 のセルラーモジュールで dying-gasp 機能を有効にし、SMS を受信する電話番号と、電源障害時にモデムから送信される特定の SMS テキストメッセージを指定する方法を示しています。

```
router# configure terminal

router(config)# controller cellular 0/1/0
router (config-controller)# lte dyinggasp detach enable
router (config-controller)# lte dyinggasp sms send 4081112222
 IR1101-#999_EM7455_powered_off!
```

デジタル I/O 用の SNMP MIB

デジタル I/O は、他の IR デバイスでサポートされているアラーム入力およびアラーム出力に似ています。他のデバイスでは、ALARM IN は専用の入力で、ALARM OUT は専用の出力です。デジタル I/O では、入力または出力になります。IRM-1100 拡張モジュールを搭載した IR1101 では、4 つのデジタル I/O を使用できます。

MIB サポートは、デジタル I/O のみの show alarm 出力を反映します。

CISCO-DIGITAL-IO-MIB.my には 4 つのデジタル I/O ノードがあります。各デジタル I/O ノードには、各デジタル I/O ノードの説明、有効化、重大度、アプリケーション、出力、しきい値、トリガーリーフノードなどの対応する属性があります。

IOx アプリケーションへの GPS アクセス

以前は、モデムで GPS が有効になっていると、NMEA ストリームが IOx に転送されませんでした。このリリースでは、NMEA ストリームを ngiolite モジュールから IOx に転送できます。これを有効にするには 2 つの手順があります。

- Linux と IOx の間にトンネルを作成する。
- すべての NMEA メッセージをトンネル経由で IOx に転送する。

システムコードはトンネルの存在を確認し、存在しない場合はデータを IOx に送信できません。

この機能をサポートするために、IR1101 と IR1800 の 2 つのセルラーモデム用に 2 つの新しいトンネルが作成されます。デフォルトでは 2 つのトンネルが作成され、どちらのモデムでも GPS/NMEA が有効になっていれば、次のように NMEA ストリームが対応するトンネルを介して送信されます。

Modem0：

[Linux] /dev/ttyTun5 および /dev/ttyTun6 [IOx]。/dev/ttyTun5 へのソフトリンクは /dev/ttyTunNMEA0 という名前で作成され、/dev/ttyTun6 へのソフトリンクは /dev/ttyNMEA0 という名前で作成されます。これらは、IOx からアクセスできます。

Modem1：

[Linux] /dev/ttyTun7 and /dev/ttyTun8 [IOx]。/dev/ttyTun7 へのソフトリンクは /dev/ttyTunNMEA1 という名前で作成され、/dev/ttyTun8 へのソフトリンクは /dev/ttyNMEA1 という名前で作成されます。これらは、IOx からアクセスできます。

次のコマンドは、GPS の状態を表示します。

```
IR1101#show app-hosting list
App id State
---------------------------------------------------------
gps RUNNING
```

mSATA の Yang モデル

YANG は、NETCONF や RESTCONF などのネットワーク管理プロトコルを介して送信されるデータを表す一般的なデータモデリング言語です。Cisco-IOS-XE-device-hardware-oper YANG モデルは、mSATA 情報を表示するように変更されました。 mSATA には、関連データを表示するための 2 つの CLI があります。

これら 2 つの CLI は次のとおりです。

show platform hardware msata status

- CLI は、SSD が存在するかどうかに関する情報を提供します。
- SSD が存在する場合は、「SSD is present」というメッセージが表示されます。

- SSD が存在しない場合は、「SSD is not present」というメッセージが表示されます。

show platform hardware msata lifetime

- SSD が存在する場合、SSD のライフタイムを % で表す出力（「SSD lifetime remaining (%): 99」）が表示されます。
- SSD が存在しない場合は、「SSD is not present」というメッセージが表示されます。

デバイスインベントリ内の mSATA の一般的な YANG 応答は次のとおりです。

```
 <device-inventory>
          <hw-type>hw-type-ssd</hw-type>
          <hw-dev-index>5</hw-dev-index>
          <version>V00</version>
          <part-number>IR-SSD-MSATA-100G</part-number>
          <serial-number>FOC21520XFV</serial-number>
          <hw-description>mSATA Module</hw-description>
          <dev-name>Expansion module 2 - mSATA Module</dev-name>
          <field-replaceable>true</field-replaceable>
          <hw-class>hw-class-virtual</hw-class>
          <lifetime>99</lifetime>
</device-inventory>
```

Cisco IOS-XE YANG データモデルは次のとおりです。

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

各リリースにはディレクトリがあり、17.5.1 リリースは 1751 の下にあります。

IOx コンテナアプリケーションとしてのゲストシェル

ゲスト シェルは、仮想化された Linux ベースの環境であり、Cisco デバイスの自動制御と管理のための Python アプリケーションを含む、カスタム Linux アプリケーションを実行するように設計されています。ゲストシェルを使用すると、ユーザーはサードパーティ製 Linux アプリケーションのインストール、更新、操作、および IOS CLI へのアクセスを行うこともできます。

ゲスト シェル環境は、ネットワーキングではなく、ツール、Linux ユーティリティ、および管理性を意図したものです。

ゲストシェルは、ホスト（ルータ）システムとカーネルを共有します。ユーザーは、ゲストシェルの Linux シェルにアクセスし、コンテナの rootfs にあるスクリプトおよびソフトウェアパッケージを更新することができます。ただし、ゲスト シェル内のユーザーは、ホストのファイル システムおよびプロセスを変更することはできません。

ゲストシェルコンテナは、IOx を使用して管理されます。IOx は、Cisco IOS XE デバイスのためのシスコのアプリケーション ホスティング インフラストラクチャです。IOx は、シスコ、パートナー、およびサードパーティの開発者によって開発されたアプリケーションおよびサービスをネットワーク エッジ デバイスでシームレスにホスティングすることを、各種の多様なハードウェア プラットフォームにおいて可能にします。

ゲストシェルは通常、システムイメージとともにバンドルされており、Cisco IOS コマンド **guestshell enable** を使用してインストールできます。ただし、この方法では、イメージのサイ

ズが約 75 MB 増加します。これは、帯域幅が限られているか、LTE を介してイメージをダウンロードする一部のユーザーにとっては問題です。

これらのユーザーを考慮して、ゲストシェルは単一の tar ファイルとして使用できるようになり、他の IOX アプリケーションと同様にダウンロードしてシステムにインストールできます。その結果、ユニバーサル リリース イメージのサイズは増加しません。

（注） 第 0 日のゲストシェル プロビジョニングは、このアプローチでは機能しません。

ゲストシェルは、デフォルトで、管理インターフェイスを介してアプリケーションによる管理ネットワークへのアクセスを許可します。IR1101 のように専用管理ポートを持たないプラットフォームの場合、VirtualPortGroup を IOS 設定内のゲストシェルに関連付けることができます。

ゲストシェルの設定例は、次の URL のページにあります。
https://www.cisco.com/c/ja_jp/td/docs/ios-xml/ios/prog/configuration/1612/b_1612_programmability_cg/guest_shell.html#id_45931

ゲストシェルをデバイスにインストールするには、tar ファイルをルータにコピーし、次のコマンドを実行します。

```
app-hosting install appid guestshell package <path to tar file>
```

ステータスを確認するには、次のコマンドを使用します。

```
show app-hosting list
```

ゲストシェルが正常に展開されると、**guestshell enable**、**guestshell run bash**、**guestshell run python3** などの標準のゲストシェルコマンドが機能します。

次のリソースでは、guesthell を使用した Python スクリプトの実行について説明しています。

https://www.cisco.com/c/ja_jp/td/docs/ios-xml/ios/prog/configuration/1612/b_1612_programmability_cg/cli_python_module.html

（注） 17.5.1 では python3 のみがサポートされています。

重要：インストールする前に

デバイスにゲストシェルをインストールする前に、次のコマンドを実行して、デバイスに IOx コンテナキーがプログラムされていることを確認してください。

```
Router#show software authenticity keys | i Name
Product Name : SFP-VADSL2-I
Product Name : SFP-VADSL2-I
Product Name : IR1101
Product Name : IR1101
Product Name : Cisco Services Containers
Product Name : Cisco Services Containers
```

出力には、製品名が「Cisco Services Containers」の行が 1 つ以上含まれている必要があります。コンテナキーがデバイスにプログラムされていない場合は、ゲストシェルをインストールできません。

次のようなエラーが表示されます。

```
*Aug 26 15:47:21.484: %IOSXE-3-PLATFORM: R0/0: IOx: App signature verification failed
with non-zero exit code
*Aug 26 15:47:21.588: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install failed: App
 package signature (package.sign)
verification failed for package manifest file package.mf. Re-sign the application and
then deploy again.
```

コンテナキーをデバイスにインストールするためのソフトウェアベースのメカニズムはありません。キーは製造施設でプログラムする必要があります。2020 年 1 月 1 日以降に出荷された IR1100 デバイスでは、コンテナキーがプログラムされています。

ゲストシェルの tar ファイルは、特定のリリースの IOS-XE イメージとともに発行されます。詳細については、https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloadsを参照してください。

show power CLI をサポートする SNMP MIB

show power CLI の SNMP MIB サポートは、新しい mib ファイル（CISCO-ENTITY-SENSOR-MIB.my）で使用できます。

次に、**show power** CLI の例を示します。

```
#show power
Main PSU :
    Total Power Consumed: 8.77 Watts
    Configured Mode : N/A
    Current runtime state same : N/A
    PowerSupplySource : External PS
```

次に、CISCO-ENTITY-SENSOR-MIB.my MIB の例を示します。

```
SensorDataType (INTEGER) watts(6)
SensorDataScale (INTEGER) milli(8)
SensorValue(INTEGER) 8770
```

次のコマンドを使用して設定します。

```
Router#config term
Router#(config) snmp-server community public RW
Router#(config) end
```

送信元インターフェイスとしてセルラーインターフェイスをサポートする ERSPAN

カプセル化リモート スイッチド ポート アナライザ （ERSPAN）を使用すると、セルラーインターフェイスからのトラフィックを監視できます。ERSPAN は、監視対象のトラフィックをネットワークアナライザに送信します。

以下に設定サンプルを示します。

```
Router(config)#monitor session 1 type erspan-source
Router(config-mon-erspan-src)#no shut
Router(config-mon-erspan-src)#source interface Cellular0/1/0
Router(config-mon-erspan-src)#destination
Router(config-mon-erspan-src-dst)#erspan-id 1
Router(config-mon-erspan-src-dst)#mtu 146
Router(config-mon-erspan-src-dst)#ip address 169.254.1.2
Router(config-mon-erspan-src-dst)#origin ip address 169.254.1.1
Router#show monitor session erspan-source
Session 1
---------
Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
Both : Ce0/1/0
Destination IP Address : 169.254.1.2
MTU : 1464
Destination ERSPAN ID : 1
Origin IP Address : 169.254.1.1
```

ERSPAN の設定の詳細については、次のガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-3s/lanswitch-xe-3s-book/lnsw-conf-erspan.pdf

DSL の Yang モデル

YANG は、NETCONF や RESTCONF などのネットワーク管理プロトコルを介して送信されるデータを表す一般的なデータモデリング言語です。

Cisco-IOS-XE-controller-vdsl-oper は、コントローラの vdsl 設定を編集するために導入されました。これにより、DSL の yang のサポートが提供されます。

dsl コントローラの設定の編集で一般的な yang 応答の例を次に示します。

```
<native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
          <controller>
            <VDSL xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-controller">
              <name>0/0/0</name>
              <adsl-pvc xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-adsl">
                <vpi-vci>255/65535</vpi-vci>
                <bridge-dot1q>21</bridge-dot1q>
                <encapsulation>vcmux</encapsulation>
              </adsl-pvc>
            </VDSL>
          </controller>
        </native>
      </nc:config></nc:edit-config></nc:rpc>
```

（注） コントローラ設定は、Cisco-IOS-XE-native yang モデルの **get** および **get-config** 操作を使用して取得できます。

Cisco IOS-XE YANG データモデルは次のとおりです。

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe

各リリースにはディレクトリがあり、17.5.1 リリースは 1751 の下にあります。

DNP3 拡張

以前は古い RTU がピアツーピアモードで使用されていた場合もあります。これらの RTU は、メッセージヘッダーのビット DIR=1 を設定することで、DNP 3 シリアル下位およびプライマリのロールを動的にスワップしました。Cisco ルータで使用される ASE の SCADA スタックは、常に DNP3 シリアルプライマリとして設定さています。この場合、DIR=1 の DNP3 シリアルから受信したすべてのパケットが無視され、RTU からの多くのメッセージが廃棄されました。これらのシナリオを処理するために、新しい SCADA 設定 CLI が追加されました。

scada-gw protocol ignore directionを使用して無効にすることができます。

この CLI を有効にすると、DIR=1 の場合でも、ルータは RTU からの着信パケットを受け入れることができます。新しい CLI は、Cisco-IOS-XE-scada-gw.yang 設定モデルにも追加されます。

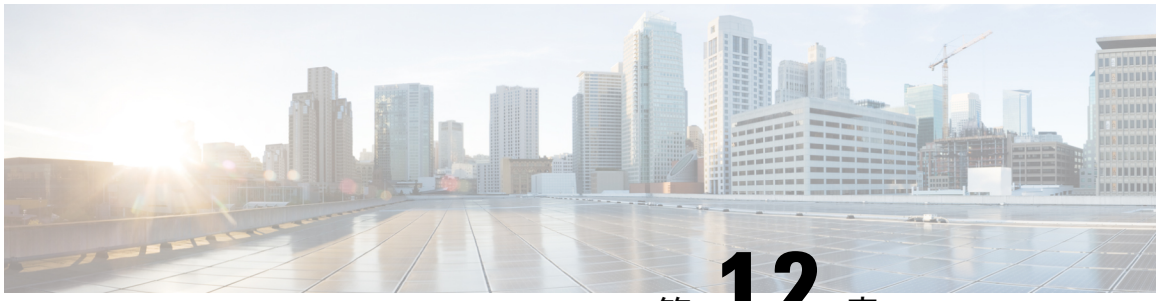
次に、使用例を示します。

```
Router# config term
Router(config)# scada-gw protocol ignore direction
```

設定

T101/T104 での scada-gw プロトコル方向無視の設定例

```
scada-gw protocol t101
channel rt-chan
link-addr-size two
bind-to-interface Async0/2/0
session rt-sess
attach-to-channel rt-chan
common-addr-size one
cot-size two
info-obj-addr-size three
link-addr 31
sector rt-sec
attach-to-session rt-sess
asdu-addr 100
scada-gw protocol t104
channel mt-chan
t3-timeout 20
tcp-connection 0 local-port 8001 remote-ip 192.168.1.0/24
session mt-sess
attach-to-channel mt-chan
sector mt-sec
attach-to-session mt-sess
asdu-addr 101
map-to-sector rt-sec
scada-gw protocol ignore direction
scada-gw enable
```



第 12 章

Cisco IOS-XE 17.6.1 の新機能

リリース17.6.1 の IR1101 で使用可能な新機能は次のとおりです。

ポートごとの DHCP アドレス割り当て

新しい CLI は追加されていません。インターフェイス A0/0/1 のデバイスは 192.0.2.90 になります。

最小設定は次の例のようになります。

```
conf t
  ip dhcp excluded-address 192.0.2.1 192.0.2.80
  ip dhcp excluded-address 192.0.2.100 192.0.2.255
  ip dhcp use subscriber-id client-id
end

conf t
  ip dhcp pool 16
    network 192.0.2.0 255.255.255.0
      address 192.0.2.90 client-id Fa0/0/1 ascii
end
```

show output CLI は次のように表示されます。

```
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address Client-ID/ Lease expiration Type State Interface
Hardware address/
User name
192.0.2.90 0046.6130.2f30.2f31 Infinite Manual Active Unknown
```

（注） client-id は、インターフェイスの短縮名である必要があります。FastEthernet インターフェイスには「Fa」を使用します。GigabitEthernet インターフェイスには「Gi」を使用します。

カスタム制御 LED

IR-1101 には点滅しない 3 色のカスタム LED があり、次のエグゼクティブ権限 CLI で制御できます。

```
router# set platform hardware custom-led <0-7>
```

0 ー 7 の番号は次のとおりです。

- 0：消灯
- 1：青
- 2：緑
- 3：赤
- 4：青/緑
- 5：青/赤
- 6：緑/赤
- 7：青/緑/赤

DSL SFP ファームウェアの署名と署名の検証のサポート

オプションの IOS ファイルパスが既存のアップグレードコマンドの最後に追加されました。ファイルは SFP-VADSL2-I キーで署名する必要があります。ファイルは bootflash:/flash:、usbflash0、または msata: のものが使用できます。リモートファイルシステムからは使用できません。

コマンドライン インターフェイス

モジュールをアップグレードするためのコマンドラインインターフェイスは次のとおりです。

router# **upgrade hw-module subslot 0/0 sfp 0** *<IOS filepath>*

コマンドのオプションは次のとおりです。

```
Router#upgrade hw-module subslot 0/0 sfp 0 ?
  bootflash:  Firmware filename on local driver
  crashinfo:  Firmware filename on local driver
  flash:      Firmware filename on local driver
  usbflash0:  Firmware filename on local driver
```

次に、コマンドの使用例を示します。

```
Router#upgrade hw-module subslot 0/0 sfp 0 bootflash:sfp8455_rel.bin
Digital signature successfully verified in file bootflash:sfp8455_rel.bin
Upgrade SFP firmware on interface GigabitEthernet0/0/0 from 1_62_8463 to 1_62_8455
Connection will be disrupted, Continue(Y/N)?y
Start ebm upgrade!!
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................................

firmware update success!!
```

DSL SFP Annex M のサポート

サポートは、17.5.1 の Annex-J の場合と同じです。

4 つの ADSL MIB オブジェクトをサポート

IR1101 の回線速度と達成可能なレートを取得するために、MIB のサポートが追加されました。

新しい MIB を次に示します。

1.3.6.1.2.1.10.94.1.1.4.1.2 ADSL-LINE MIB:adslAtucChanCurrTxRate

1.3.6.1.2.1.10.94.1.1.5.1.2 ADSL-LINE MIB:adslAturChanCurrTxRate

1.3.6.1.2.1.10.94.1.1.2.1.8 ADSL-LINE MIB:adslAtucCurrAttainableRate

1.3.6.1.2.1.10.94.1.1.3.1.8 ADSL-LINE MIB:adslAturCurrAttainableRate

コマンドライン インターフェイス

DSL SFP が ADSL DSLAM に接続されているルータでは、次の既存の SNMP CLI を使用して、上記の OID のサポートを確認できます。

```
!configure SNMP Server
!---------------------
snmp-server community public RO
snmp-server manager
!
!verify MIB OIDs
!---------------
snmp get-next v2c 33.33.33.102 public oid 1.3.6.1.2.1.10.94.1.1.4.1.2
!
```

次のコマンドを使用して、別の SNMP クライアント（Linux デバイスなど）から MIB 値を収集することもできます。

```
$ snmpwalk -v 2c -c public 33.33.33.102 1.3.6.1.2.1.10.94.1.1.4.1.2
```

デジタル IO 拡張機能

一部のデジタル I/O ポートを IOSd で管理し、他のデジタル IO ポートを IOx コンテナアプリで管理できるようにサポートが追加されました。更新された CLI が追加され、デジタル IO 拡張機能の YANG モデルが更新されました。

CLI の 17.5.1 バージョンは次のとおりです。

```
Router(config)# alarm contact attach-to-iox
```

（注） リリース 17.5.1 では、**alarm contact attach-to-iox**によりすべてのデジタル IO ポート（1 ー 4）に対し IOX で制御できました。

CLI の 17.6.1 バージョンは次のとおりです。

```
Router(config)#alarm contact 1 ?
application Set the alarm application
attach-port-to-iox Enable selected Digital IO Ports access from IOX
description Set alarm description
enable Enable the alarm/digital IO port
output Set mode as output
severity Set the severity level reported
threshold Set the digital IO threshold
trigger Set the alarm trigger

Router(config)#alarm contact 1 attach-port-to-iox

Router#show alarm
Alarm contact 0:
Not enabled.
Digital I/O 1:
Attached to IOX.
Digital I/O 2:
Not enabled.
Digital I/O 3:
Not enabled.
Digital I/O 4:
Not enabled.
```

更新された CLI では、1 ー 4 はコンテナアプリケーションの IOx に割り当てるデジタル I/O ポートの数です。

（注） リリース 17.6.1 では、各デジタル IO ポートを IOX に個別に割り当てることができます。

第 13 章

Cisco IOX XE 17.7.1 の新機能

この章は、次の項で構成されています。

コンピューティング側の IRM-1100 拡張モジュール

IR1101 には、拡張モジュール用の 2 つの接続ポイントがあります。ルータの上部を拡張側と呼びます。ルータの下部をコンピューティング側と呼びます。

IOS XE リリース 17.7.1 よりも前は、拡張側でのみサポートされていました。

17.7.1 リリース以降では、追加のモジュールをコンピューティング側に接続できます。

機能および制限事項

次は、リリース 17.7.1 の IRM-1100 に適用されます。

- コンピューティング側に何かが接続されている場合、スイッチポートは機能しません。
- IRM-1100-SPMI の mSATA ピンと GPIO ピンは、17.7.1 のコンピューティング側（下部）に接続されている場合はサポートされません。
- IR1101 は、最大 2 つの LTE インターフェイスのみをサポートできます。両側に IRM-1100 を接続することはできません。この設定で接続すると、拡張側のみがアクティブになります。
- LTE インターフェイスがコンピューティング側に接続されている場合、セルラー 0/4/0 とセルラー 0/4/1 が列挙されます。
- CAT18 LTE モジュールはコンピューティング側ではサポートされていません。
- IRM-1100-SP または IRM-1100-SPMI がコンピューティング側に接続されている場合、LTE インターフェイスのみが機能します。

ADSL MIB オブジェクトのサポート

IR1101 では、次の ADSL MIB OID がサポートされる予定です。

```
1.3.6.1.2.1.10.94.1.1.6.1.15 ADSL-LINE-MIB adslAtucPerfCurr15MinInits
1.3.6.1.2.1.10.94.1.1.6.1.22 ADSL-LINE-MIB adslAtucPerfCurr1DayInits
```

VDSL MIB オブジェクトのサポート

IR1101 では、次の VDSL MIB OID がサポートされる予定です。

```
1.3.6.1.2.1.10.251.1.4.1.2.1.3    VDSL2-LINE-MIB   xdsl2PMLInitCurr15MTimeElapsed
1.3.6.1.2.1.10.251.1.4.1.2.1.4    VDSL2-LINE-MIB   xdsl2PMLInitCurr15MFullInits
1.3.6.1.2.1.10.251.1.4.1.2.1.5    VDSL2-LINE-MIB   xdsl2PMLInitCurr15MFailedFullInits
1.3.6.1.2.1.10.251.1.4.1.2.1.6    VDSL2-LINE-MIB   xdsl2PMLInitCurr15MShortInits
1.3.6.1.2.1.10.251.1.4.1.2.1.7    VDSL2-LINE-MIB   xdsl2PMLInitCurr15MFailedShortInits
1.3.6.1.2.1.10.251.1.4.1.2.1.10   VDSL2-LINE-MIB   xdsl2PMLInitCurr1DayTimeElapsed
1.3.6.1.2.1.10.251.1.4.1.2.1.11   VDSL2-LINE-MIB   xdsl2PMLInitCurr1DayFullInits
1.3.6.1.2.1.10.251.1.4.1.2.1.12   VDSL2-LINE-MIB   xdsl2PMLInitCurr1DayFailedFullInits
1.3.6.1.2.1.10.251.1.4.1.2.1.13   VDSL2-LINE-MIB   xdsl2PMLInitCurr1DayShortInits
1.3.6.1.2.1.10.251.1.4.1.2.1.14   VDSL2-LINE-MIB   xdsl2PMLInitCurr1DayFailedShortInits
1.3.6.1.2.1.10.251.1.4.1.1.1.2    VDSL2-LINE-MIB   xdsl2PMLCurr15MValidIntervals
1.3.6.1.2.1.10.251.1.4.1.1.1.3    VDSL2-LINE-MIB   xdsl2PMLCurr15MInvalidIntervals
1.3.6.1.2.1.10.251.1.4.1.1.1.4    VDSL2-LINE-MIB   xdsl2PMLCurr15MTimeElapsed
1.3.6.1.2.1.10.251.1.4.1.1.1.5    VDSL2-LINE-MIB   xdsl2PMLCurr15MFecs
1.3.6.1.2.1.10.251.1.4.1.1.1.6    VDSL2-LINE-MIB   xdsl2PMLCurr15MEs
1.3.6.1.2.1.10.251.1.4.1.1.1.7    VDSL2-LINE-MIB   xdsl2PMLCurr15MSes
1.3.6.1.2.1.10.251.1.4.1.1.1.8    VDSL2-LINE-MIB   xdsl2PMLCurr15MLoss
1.3.6.1.2.1.10.251.1.4.1.1.1.9    VDSL2-LINE-MIB   xdsl2PMLCurr15MUas
1.3.6.1.2.1.10.251.1.4.1.1.1.10   VDSL2-LINE-MIB   xdsl2PMLCurr1DayValidIntervals
1.3.6.1.2.1.10.251.1.4.1.1.1.11   VDSL2-LINE-MIB   xdsl2PMLCurr1DayInvalidIntervals
1.3.6.1.2.1.10.251.1.4.1.1.1.12   VDSL2-LINE-MIB   xdsl2PMLCurr1DayTimeElapsed
1.3.6.1.2.1.10.251.1.4.1.1.1.13   VDSL2-LINE-MIB   xdsl2PMLCurr1DayFecs
1.3.6.1.2.1.10.251.1.4.1.1.1.14   VDSL2-LINE-MIB   xdsl2PMLCurr1DayEs
1.3.6.1.2.1.10.251.1.4.1.1.1.15   VDSL2-LINE-MIB   xdsl2PMLCurr1DaySes
1.3.6.1.2.1.10.251.1.4.1.1.1.16   VDSL2-LINE-MIB   xdsl2PMLCurr1DayLoss
1.3.6.1.2.1.10.251.1.4.1.1.1.17   VDSL2-LINE-MIB   xdsl2PMLCurr1DayUas
1.3.6.1.2.1.10.251.1.4.1.3.1.3    VDSL2-LINE-MIB   xdsl2PMLHist15MMonitoredTime
1.3.6.1.2.1.10.251.1.4.1.3.1.4    VDSL2-LINE-MIB   xdsl2PMLHist15MFecs
1.3.6.1.2.1.10.251.1.4.1.3.1.5    VDSL2-LINE-MIB   xdsl2PMLHist15MEs
1.3.6.1.2.1.10.251.1.4.1.3.1.6    VDSL2-LINE-MIB   xdsl2PMLHist15MSes
1.3.6.1.2.1.10.251.1.4.1.3.1.7    VDSL2-LINE-MIB   xdsl2PMLHist15MLoss
1.3.6.1.2.1.10.251.1.4.1.3.1.8    VDSL2-LINE-MIB   xdsl2PMLHist15MUas
1.3.6.1.2.1.10.251.1.4.1.3.1.9    VDSL2-LINE-MIB   xdsl2PMLHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.1.4.1.3    VDSL2-LINE-MIB   xdsl2PMLHist1DMonitoredTime
1.3.6.1.2.1.10.251.1.4.1.4.1.4    VDSL2-LINE-MIB   xdsl2PMLHist1DFecs
1.3.6.1.2.1.10.251.1.4.1.4.1.5    VDSL2-LINE-MIB   xdsl2PMLHist1DEs
1.3.6.1.2.1.10.251.1.4.1.4.1.6    VDSL2-LINE-MIB   xdsl2PMLHist1DSes
1.3.6.1.2.1.10.251.1.4.1.4.1.7    VDSL2-LINE-MIB   xdsl2PMLHist1DLoss
1.3.6.1.2.1.10.251.1.4.1.4.1.8    VDSL2-LINE-MIB   xdsl2PMLHist1DUas
1.3.6.1.2.1.10.251.1.4.1.4.1.9    VDSL2-LINE-MIB   xdsl2PMLHist1DValidInterval
1.3.6.1.2.1.10.251.1.4.2.1.1.2    VDSL2-LINE-MIB   xdsl2PMChCurr15MValidIntervals
1.3.6.1.2.1.10.251.1.4.2.1.1.3    VDSL2-LINE-MIB   xdsl2PMChCurr15MInvalidIntervals
1.3.6.1.2.1.10.251.1.4.2.1.1.4    VDSL2-LINE-MIB   xdsl2PMChCurr15MTimeElapsed
1.3.6.1.2.1.10.251.1.4.2.1.1.5    VDSL2-LINE-MIB   xdsl2PMChCurr15MCodingViolations
1.3.6.1.2.1.10.251.1.4.2.1.1.6    VDSL2-LINE-MIB   xdsl2PMChCurr15MCorrectedBlocks
```

```
1.3.6.1.2.1.10.251.1.4.2.1.1.7    VDSL2-LINE-MIB   xdsl2PMChCurr1DayValidIntervals
1.3.6.1.2.1.10.251.1.4.2.1.1.8    VDSL2-LINE-MIB   xdsl2PMChCurr1DayInvalidIntervals
1.3.6.1.2.1.10.251.1.4.2.1.1.9    VDSL2-LINE-MIB   xdsl2PMChCurr1DayTimeElapsed
1.3.6.1.2.1.10.251.1.4.2.1.1.10   VDSL2-LINE-MIB   xdsl2PMChCurr1DayCodingViolations
1.3.6.1.2.1.10.251.1.4.2.1.1.11   VDSL2-LINE-MIB   xdsl2PMChCurr1DayCorrectedBlocks
1.3.6.1.2.1.10.251.1.4.2.2.1.3    VDSL2-LINE-MIB   xdsl2PMChHist15MMonitoredTime
1.3.6.1.2.1.10.251.1.4.2.2.1.4    VDSL2-LINE-MIB   xdsl2PMChHist15MCodingViolations
1.3.6.1.2.1.10.251.1.4.2.2.1.5    VDSL2-LINE-MIB   xdsl2PMChHist15MCorrectedBlocks
1.3.6.1.2.1.10.251.1.4.2.2.1.6    VDSL2-LINE-MIB   xdsl2PMChHist15MValidInterval
1.3.6.1.2.1.10.251.1.4.2.3.1.3    VDSL2-LINE-MIB   xdsl2PMChHist1DMonitoredTime
1.3.6.1.2.1.10.251.1.4.2.3.1.4    VDSL2-LINE-MIB   xdsl2PMChHist1DCodingViolations
1.3.6.1.2.1.10.251.1.4.2.3.1.5    VDSL2-LINE-MIB   xdsl2PMChHist1DCorrectedBlocks
1.3.6.1.2.1.10.251.1.4.2.3.1.6    VDSL2-LINE-MIB   xdsl2PMChHist1DValidInterval
```

1G SFP のサポート

リリース 17.7.1 では、次の SFP のサポートが追加されます。

GLC-T-RGD

CWDM-SFP-1470=

CWDM-SFP-1610=

CWDM-SFP-1530=

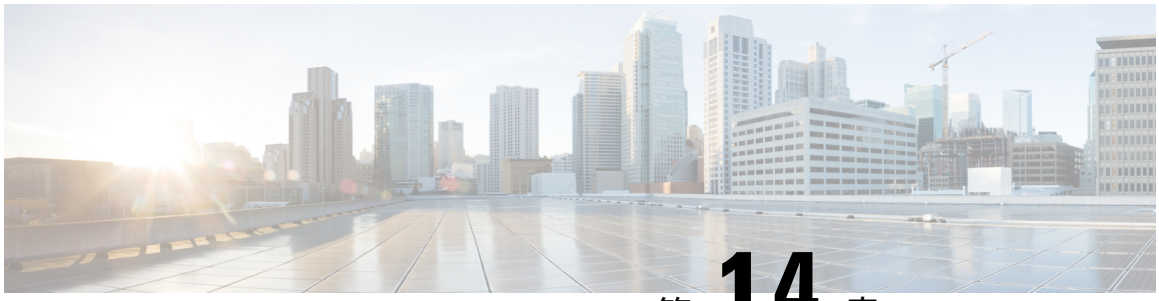
DWDM-SFP-3033=

DWDM-SFP-3112=

GLC-BX-D-I=

GLC-BX-U-I=

GLC-TE



第 14 章

Cisco IOS XE 17.8.1 の新機能

この章は、次の項で構成されています。

DSL Annex B のサポート

17.8.1 リリースでは、ADSL2+ Annex B がサポートされます。

Annex B はデフォルトでは設定されていません。Annex B を有効にするには、次のコマンドを使用します。

```
controller VDSL 0/0/0
  capability annex-b
```

mSATA のサポートおよび CM 側の IRM-1100-SPMI の IO サポート

以前のソフトウェアリリースでは、IRM-1100-SPMI の mSATA およびデジタル I/O は、IR1101 の拡張モジュール側でのみサポートされていました。17.8.1 では、コンピューティングモジュール（CM）側でサポートを利用できますが、次の制限があります。

両側に IRM-1100-SPMI を取り付けた場合：

- この組み合わせはサポートされていません。
- EM 側からの mSATA とデジタル I/O のみが機能します。

- CM 側からのデジタル I/O は機能しません。

CM 側に IRM-1100-SPMI を取り付けた場合：

- mSATA とデジタル I/O は動作します。
- デジタル I/O のインスタンスには 1 ～ 4 の番号が付けられます。

セルラーの有用性機能強化

セルラー機能と GPS 機能が次のように強化されました。

手動による介入なしでデバッグデータを自動的に生成およびトラップするために、トリガーポイントとデバッグコードを controller cellular CLI によって有効にすることができます。次の CLI オプションを使用できます。

```
(config-controller)#lte modem serviceability ?
  gps               GPS debugging
  interface-resets  Interface resets/Bearer deletion
  modem-crash       Modem-crash debugging
  modem-resets      IOS initiated unknown modem-resets
```

デバッグデータには次のものが含まれます。

- コンテキストベースのデバッグログ（トレースバック、GPS ロケーション）。
- 適切にフォーマットされたデバッグメッセージ。
- より広い範囲のベンダー固有のデバッグデータ。

デバッグログは次の flash: の場所にあります。

```
router#dir flash:servelogs
Directory of bootflash:/servelogs/

259340  -rw-              122   Sep 7 2021 17:40:44 +00:00  gpslog-slot5-20210907-174044
259339  -rw-             1734   Sep 7 2021 12:14:07 +00:00  celllog-slot5-20210905-164628
```

GPS およびセルラーのログファイルは、作成時のタイムスタンプを使用したファイル名で個別に作成されます。これらのファイルは次のように作成されます。

- 既存のファイルが 10Mb に達した場合、新しいファイルが作成されます。
- 機能（GPS またはセルラー）を完全に無効にしてから再度有効にすると、新しいファイルが作成されます。

GNMI ブローカ（GNMIB）の更新

GNMI ブローカ（GNMIB）が拡張され、gRPC ネットワーク操作インターフェイス（gNOI）reset.proto サービスをサポートするようになりました。このサービスは、gRPC を介してデバイスを工場出荷時の初期状態に復元する機能を提供します。

サービスが実行されると、「factory-reset all」コマンドと同様に動作し、その後リロードがトリガーされます。さらに、このサービスは現在起動されているイメージを維持します。reset.proto サービスに準拠するために、以下の追加の手順が実行されます。

- rommon BOOT 変数を現在起動されているイメージに設定し、工場出荷時の状態へのリセット後にリロードするまでそれを維持します
- 自動ブートを有効にして、工場出荷時の状態へのリセット後に現在起動されているイメージでデバイスを起動します。

gRPC ネットワーク操作インターフェイスの更新

gNOI（gRPC ネットワーク操作インターフェイス）は、OS のインストール、アクティベーション、検証といったネットワークデバイス上の操作コマンドや手順を実行するための gRPC ベースのマイクロサービスセットを定義します。

gNOI を通じて os.proto は、OS のアクティベーション、インストール、詳細な概要、OS の内部コマンドなどのオペレーティングシステム関連のタスクを実行し、さらに OS 操作の概要を出力することができます。

また、gNOI os.proto を使用して、gnmib の詳細な状態を表示したり、gnmib の動作統計を確認したり、修飾子を出力することもできます。

raw ソケット機能強化

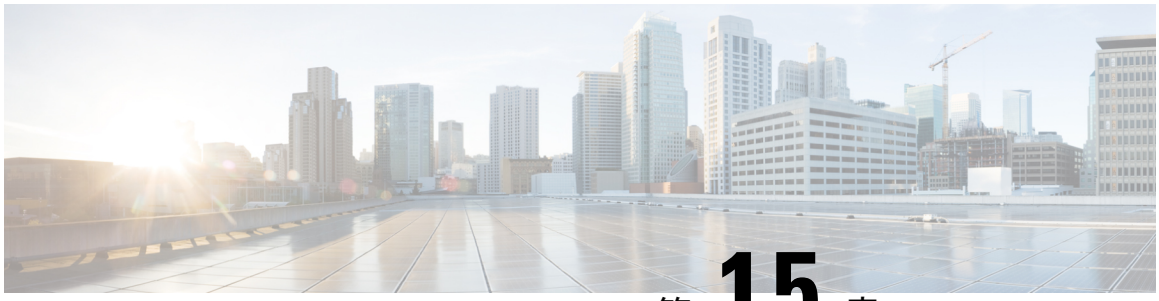
この機能強化により、ユーザーは書き込みソケットで使用できる最大再試行回数を入力できます。再試行回数の範囲は 1 ～ 1000 回です。デフォルトの再試行回数は 10 回です。この機能に対応するために、**raw-socket tcp max-retries <1-1000>** という新しい CLI が作成されました。<1-1000> は最大再試行回数です。

TNB の SCADA 機能強化

この機能強化により、次のような TNB の WG RTU との互換性が提供されます。

- TNB RTU では、シリアルの正しい初期化を確実にするために、リセットリンクメッセージをリンクステータスメッセージとともに送信する必要があります。この機能は、新しいコンフィギュレーション CLI **scada-gw protocol force reset-link** を使用して選択的にオンにすることができます。
- クロックパススルーが有効になっていて、ルータが DNP3-IP マスターからタイムスタンプを受け取っていない場合は、ルータのハードウェアの時刻がダウンストリームの RTU に送信されます。DNP3-IP マスターから新しいタイムスタンプを受信すると、ルータは DNP3-IP マスターから送信された新しいタイムスタンプを RTU に送信し始めます。
- メモリ内のバッファ可能な DNP3 イベントの数が 600 から 10000 に増加します。

- **scada-gw プロトコルインターロック** コマンドは、DNP3 でサポートされます。以前は、T101 と T104 のみがサポートされていました。この新しい機能強化により、DNP3-IP マスターがダウンしているか到達不能な場合、ルータはシリアルリンクを切断します。同様に、RTU へのシリアルリンクがダウンすると、DNP3-IP マスターへの TCP 接続が解除されます。
- カスタムの「リクエスト」は優先度に基づいて自動的に順序付けられるため、ユーザーは好きな順序でリクエストを指定できます。



第 15 章

Cisco IOS XE 17.9.1 の新機能

この章は、次の項で構成されています。

セルラーの起動時間の改善

IOS-XE リリース 17.9.1 では、セルラーリンクのアップタイムに多くの改善が加えられています。以前のリリースでは、ルータの起動後、セルラーインターフェイスが起動してトラフィックを渡すまでに約 2 分 30 秒かかりました。このリリースでは、セルラーリンクのアップタイムが約 20% 改善されています。

IOS XE ダウングレードの警告

この機能は、**boot system flash** コマンドに続けて、実行中のイメージのいずれかよりバージョン番号が小さいイメージのファイル名を発行すると、警告を表示します。ユーザーに表示される警告メッセージを無視することで、ダウングレード操作は引き続き可能です。実行中のイメージと同じまたはそれ以上のバージョンでのイメージの起動は、警告なしで許可されます。この機能は、ルータのブートフラッシュにすでにロードされているイメージのみ、つまり、**boot system flash** <*file_name*> CLI のみを対象としています（ftp、mop、rpc、tftp、rom などのその他のソース/デバイスを除く）。

システムがバージョンを比較する方法の例を次に示します。

次のように 2 つのバージョン番号を比較する場合：

- 17.7.1
- 17.7.1c

文字の付いたバージョン（17.7.1c）が、最新のバージョンとみなされます。

次のように 2 つのバージョン番号を比較する場合：

- 17.7.3a
- 17.7.3f

比較は、アルファベット順を考慮して行われます。上記の場合、17.7.3fが最新のバージョンとみなされます。

温度 OID の SNMP ポーリング

SNMP MIB が温度センサーから値を返せるようにするためのサポートが追加されました。出力は、**show environment** CLI のようになります。

IR1101 の **show environment** の出力：

```
IR1101#show env

Number of Critical alarms:  0
Number of Major alarms:     0
Number of Minor alarms:     0

 Slot        Sensor          Current State   Reading
Threshold(Minor,Major,Critical,Shutdown)
 ----------  --------------  --------------- ------------
---------------------------------------
 R0          Temp: TS1       Normal          42    Celsius      (75 ,80 ,90 ,na )(Celsius)

 R0          Temp: TS2       Normal          37    Celsius      (75 ,80 ,90 ,na )(Celsius)
```

snmpwalk からの出力は次のようになります。

```
[root@sg-centos-hv ~]# snmpwalk -v 2c -c public 33.33.33.204 1.3.6.1.4.1.9.9.13.1.3.1
SNMPv2-SMI::enterprises.9.9.13.1.3.1.2.1 = STRING: "Sensor 1"
SNMPv2-SMI::enterprises.9.9.13.1.3.1.3.1 = Gauge32: 48
SNMPv2-SMI::enterprises.9.9.13.1.3.1.4.1 = INTEGER: 93
SNMPv2-SMI::enterprises.9.9.13.1.3.1.5.1 = INTEGER: 0
SNMPv2-SMI::enterprises.9.9.13.1.3.1.6.1 = INTEGER: 1
SNMPv2-SMI::enterprises.9.9.13.1.3.1.7.1 = INTEGER: 0
```

ciscoEnvMonTemperatureStatusEntry oid は 1.3.6.1.4.1.9.9.13.1.3.1 です。

- ciscoEnvMonTemperatureStatusIndex (.1)
- ciscoEnvMonTemperatureStatusDescr (.2)
- ciscoEnvMonTemperatureStatusValue (.3)
- ciscoEnvMonTemperatureThreshold (.4)
- ciscoEnvMonTemperatureLastShutdown (.5)
- ciscoEnvMonTemperatureStatus (.6)

GPS モードのデフォルト有効化

17.9.1 より前の IOS XE バージョンでは、GPS はデフォルトで有効になっていましたが、GPS モードはデフォルトで無効になっていました。このため、ルーターが起動した後、GPS を使用するためにユーザーが追加でモデムの電源を再投入する必要がありました。

IOS XE 17.9.1 以降、GPS モードはデフォルトで有効になり、スタンドアロンモードに設定されます。これにより、セルラーリンクのアップタイムを短縮できます。

（注） これは、セルラーベースの GPS にのみ適用されます。これは、IR1800（DR モジュール）、IR8140（ネイティブ GPS）および IR8340（タイミングモジュール）の GPS/GNSS モジュールには適用されません。

セルラー GPS ステータスを確認するには、次のコマンドを使用します：IR1101-4001#sh cellular 0/3/0 gps

```
Router# show cellular <slot> gps
auto-reset Enable reset modem automatically after configuring GPS enable or mode
```

インストールモードのサポート

次の表に、バンドルモードとインストールモードの違いを示します。

IoT ルータで実行されている Cisco IOS XE は、通常、バンドル起動モードを使用しています。バンドル起動モードは統合起動とも呼ばれ、単一の圧縮イメージを使用します。一般的な命名規則は、<product>-universalk9.<release>.SPA.bin です。

このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。.bin イメージ経由で起動するということは、ルータは、起動する前にまずイメージを解凍する必要があることを意味します。これにより、ルータを起動するためにより長い時間がかかっていました。

ルータを新しいバージョンの IOS XE にアップグレードするには、「boot system」が新しいソフトウェアイメージをポイントするようにします。この方法はよく知られており、製品設定ガイドに詳細が記載されています。

IOS XE リリース 17.9.1 以降、インストールモードと呼ばれる新しい起動モードが IoT ルータに追加されました。インストールモードでは、packages.conf ファイルによって読み取られるブートフラッシュにロードされたパッケージが使用されます。この方法では、ソフトウェアのインストールプロセスをより正確に制御できます。

（注） SMU のインストールは、バンドル起動モードとインストールモードの両方でサポートされていました。Cisco IOS XE リリース 17.9.x 以降、ルータがバンドルモードで起動された場合、SMU のインストールは停止されます。ルータがインストールモードで起動された場合、SMU のインストールは以前のリリースと同様に機能します。

表 7: バンドルモードとインストールモード

バンドルモード	インストールモード
このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。	このモードでは、ブートプロセスにローカル（ブートフラッシュ）の packages.conf ファイルを使用します。
このモードでは、1 つの .bin ファイルを使用します。	このモードでは、.bin ファイルは拡張された .pkg ファイルに置き換えられます。
CLI： `Router(config)#boot system bootflash:<filename>`	CLI： `#install add file bootflash: [activate commit]`
このモードでアップグレードするには、boot system が新しいソフトウェアイメージをポイントするようにします。	このモードでアップグレードするには、**install** コマンドを使用します。
イメージの自動アップグレード：新しい Field Replaceable Unit（FRU）がモジュラ型シャーシに挿入された場合、アクティブな FRU と同じバージョンで新しい FRU を実行するには、手動による作業が必要です。	イメージの自動アップグレード：新しい FRU がモジュラ型シャーシに挿入された場合、結合する FRU は、アクティブな FRU と同期してイメージバージョンに自動アップグレードされます。
ロールバック：複数のソフトウェアメンテナンスの更新（SMU）を使用して以前のイメージにロールバックするには、複数回のリロードが必要になる場合があります。	ロールバック：1 回のリロードで、複数のパッチを含む、Cisco IOS XE ソフトウェアの以前のバージョンへのロールバックを有効にします。

詳細については、「Cisco IOS XE Installation Methods」を参照してください。

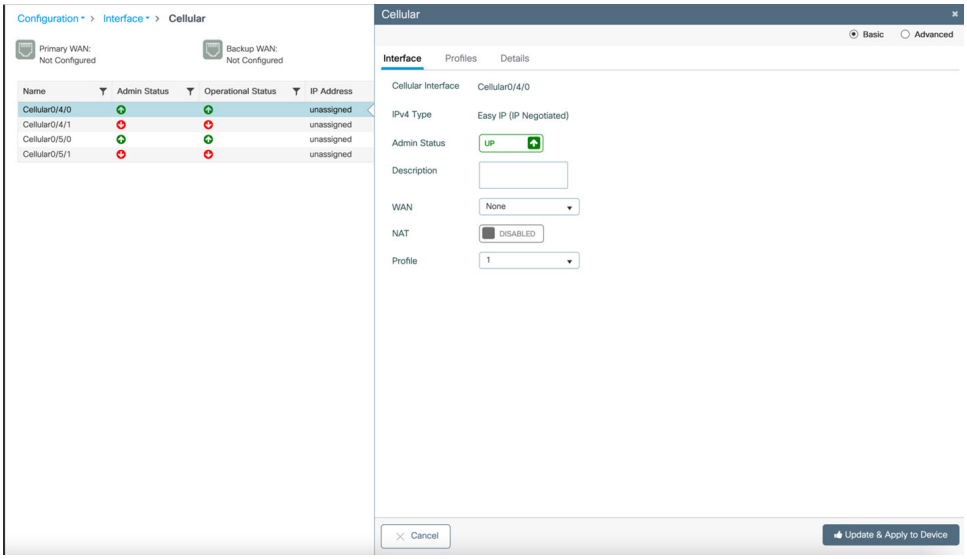
Cisco WebUI アクセスポイント名（APN）

IOS XE 17.9.1 では、Cisco WebUI インターフェイスから APN を追加、編集、または削除する機能が追加されました。以下に、この機能を実行する方法の概要を示します。

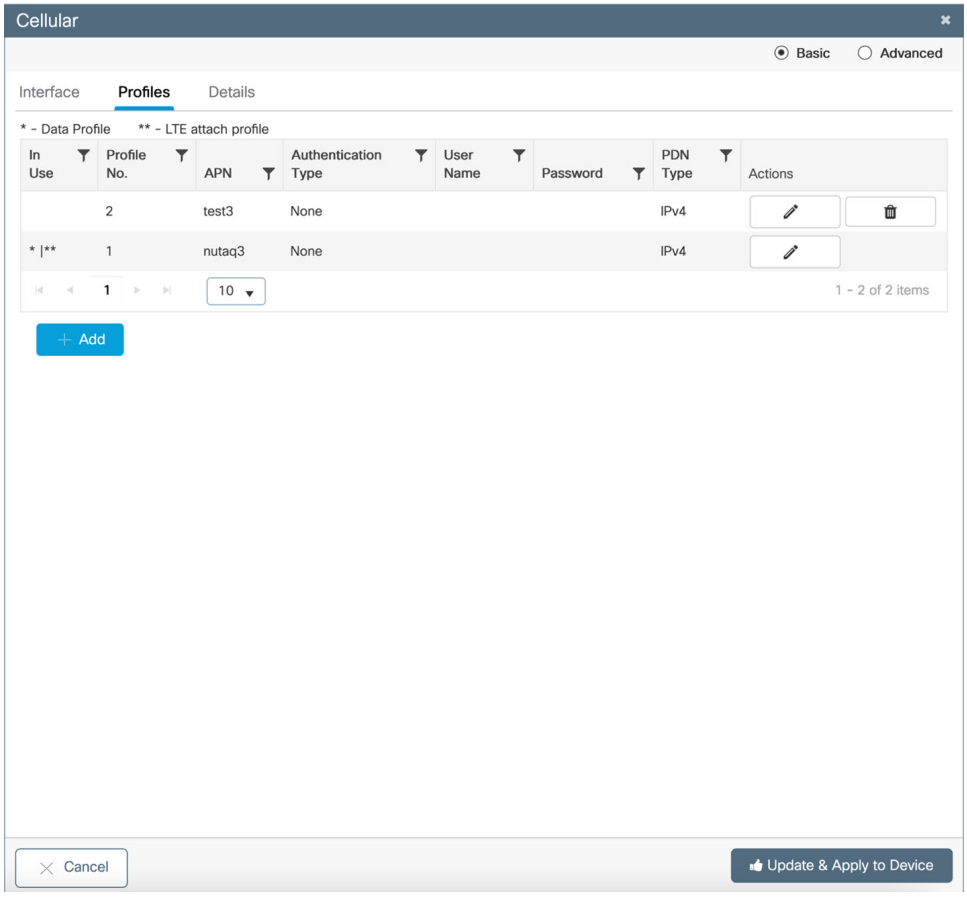
（注） このセクションでは、新機能についてのみ説明します。WebUI の完全な概要ではありません。

APN の追加

WebUI から、[Configuration] > [Interface] > [Cellular] に移動します。プラットフォームに基づいてセルラーインターフェイスをダブルクリックします。



[Cellular] ウィンドウで、[Profiles] タブをクリックします。

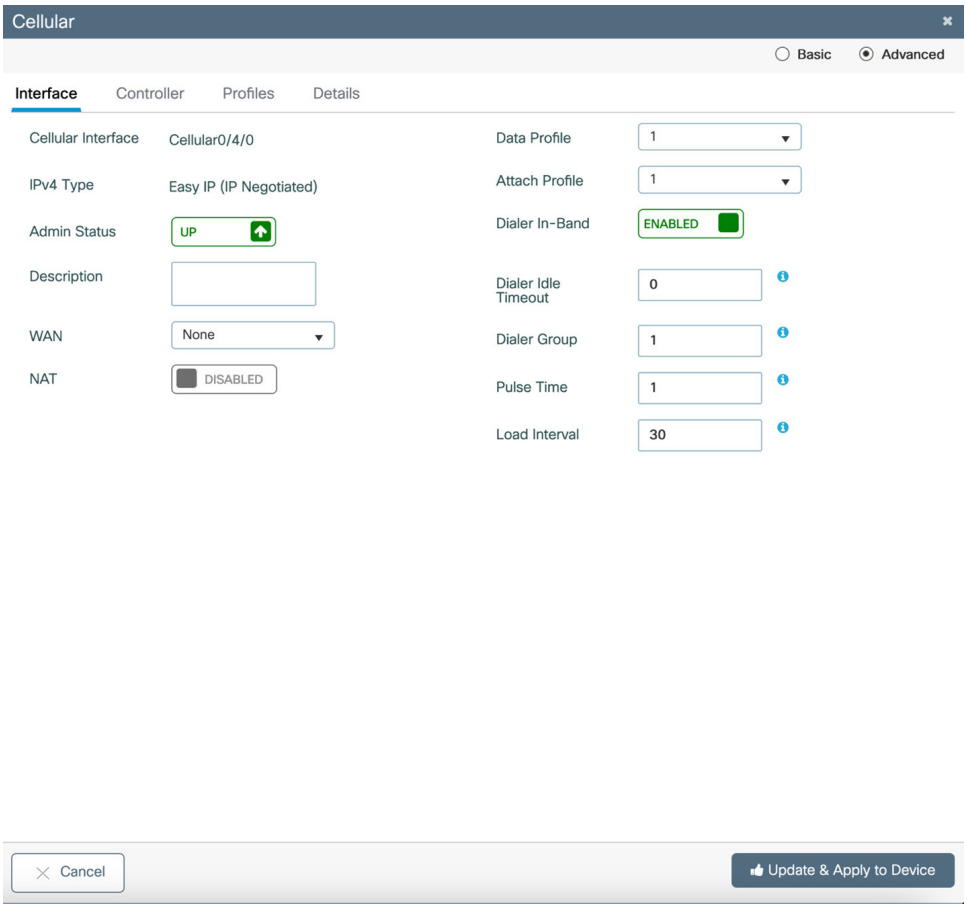


[Profiles] タブから、APN を追加、削除、または編集できます。プロファイルが変更されたら、ウィンドウの下部にある [Update & Apply to Device] をクリックします。

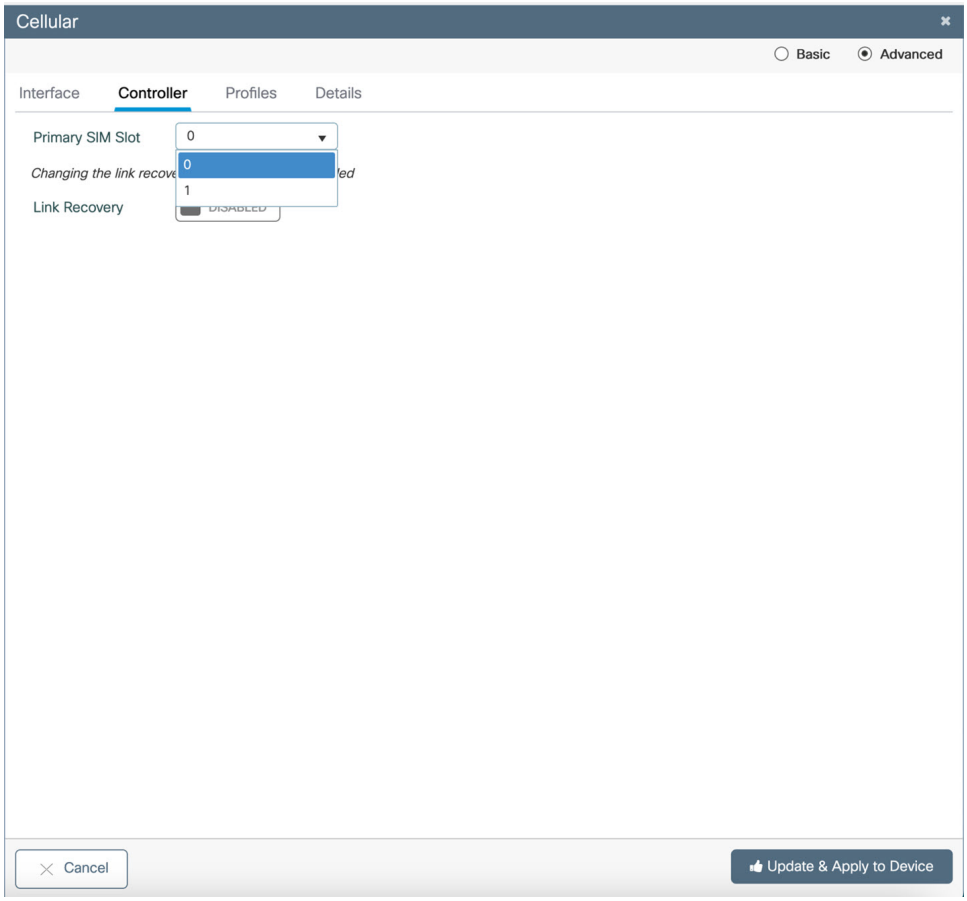
SIM スロットの変更

デフォルトでは、APN は SIM スロット 0 に接続されています。WebUI を使用して、APN を SIM スロット 1 に変更できます。

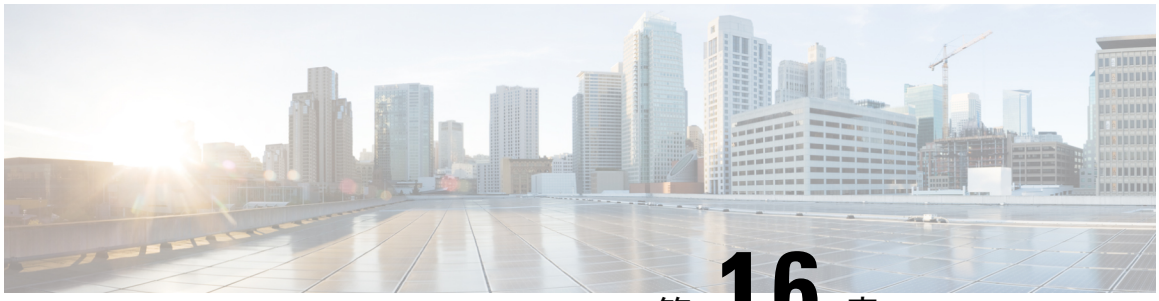
WebUI から、[Configuration] > [Interface] > [Cellular] に移動します。ウィンドウ上部にある [Advanced] オプションボタンをクリックします。



ウィンドウ上部にある [Controller] タブをクリックします。



[Primary SIM Slot] プルダウンをクリックして、スロット 1 を選択します。ウィンドウの下部にある [Update & Apply to Device] をクリックします。



第 16 章

Cisco IOS XE 17.10.1a の新機能

この章は、次の項で構成されています。

ソフトウェアによる MACsec

概要

既存のすべての Cisco IOS XE ベースのルータ/スイッチは、特殊なトランシーバを使用して MACsec 暗号化/暗号解読を実行します。このソフトウェア MACsec は、QFP の CDAL インフラストラクチャを使用して暗号化操作を実行します。ハードウェアの選択と比較すると、設定/ステータス/データパスの実行方法が異なるため、機能にいくつかの制限が生じます。

リリース 17.10.1a は、L2 インターフェイスでのみ MACsec をサポートします。MACsec ポートをアクセスモードにする必要があります。暗号化は出力 SVI インターフェイスで行われるため、ポートに使用される VLAN は一意である必要があります。つまり、他のインターフェイスはその VLAN を使用できません。この制限は、QFP に MAC テーブル情報がないために生じています。

（注） MACsec はソフトウェアを介して実行されるため、パフォーマンスは L2 インターフェイスのラインレートではありません。

出力パケットの場合、SVI は、特定のインターフェイスに関する情報はなく、パケットが VLAN に送信される必要があることのみを認識しています。どのポートを使用するかを決定するのはスイッチチップです。MACsec タグのないパケットはすべて、通常どおり受信できます。発信 L2 パケットも、暗号化や変更なしで出力されます。

NE ライセンスと NA ライセンスの両方が GCM-AES-128 をサポートしています。この機能は、実行中の NPE イメージでは使用できません。

MACsec プロトコルは、IEEE802.1AE で定義されています。

機能の制約事項

- MACsec は、このリリースのコントローラモードではサポートされていません。
- MACsec インターフェイスには一意の VLAN ID が必要です。
- この初期リリースでは、gcm-aes-128 のみがサポートされています。
- 入力側では、明示的および非明示的な SCI の両方がサポートされています。IR1101 はエンドシステムではないため、明示的な SCI パケットのみを送信します。
- IR1101 は機密性オフセットをサポートしていません。
- この最初のリリースでは、「完全性のみ」がサポートされていません。
- gcm-aes-128 の場合、プレーンパケットと比較して、暗号化されたパケットには最大 32 バイトが追加されます。そのため、MTU セットアップは、正しく動作するために 32 を追加する必要があります。
- MACsec キーは MKA モジュールによって管理されます。そのデバイスでは、MKA が MACsec キーをネゴシエートするために静的キーが必要です。
- MIB のサポートはありません。

関連資料

詳細については、次を参照してください。

- MACsec and the MACsec Key Agreement (MKA) Protocol
- MACSEC and MKA Configuration Guide, Cisco IOS XE 17

MKA 設定の例

次の例を参照してください。

```
conf t
   aaa new-model
   mka policy p1
       key-server priority 1
       macsec-cipher-suite gcm-aes-128
       sak-rekey interval 3600
end
conf t
   key chain cak1 macsec
      key 414243
         cryptographic-algorithm aes-128-cmac
         key-string 0 12345678901234567890123456789012
         lifetime local 00:00:00 29 November 2021 infinite
end
conf t
   int fa 0/0/2
      switchport mode access
      switchport access vlan 77
      mtu 1532
```

```
      mka policy p1
      mka pre-shared-key key-chain cak1
      macsec network-link
      macsec replay-protection window-size 128
end
```

コマンドの表示

cpp_cp 内部情報を表示します。

```
show platform hardware cpp active feature soft-macsec server tx [dp] [item]
show platform hardware cpp active feature soft-macsec server rx [dp] [item]
show platform hardware cpp active feature soft-macsec server control [dp] [item]
```

その他の show コマンド：

```
show macsec summary
show macsec status int fa 0/0/2
show macsec statistics int fa 0/0/2A
```

統計のクリア

```
Clear macsec statis int fa 0/0/2
```

テストコマンド

デバッグ用に 10 MKA パケットを出力します。

```
test platform software smacsec mka-ingress
```

高セキュリティ（HSEC）ライセンス

HSEC（High Security）ライセンスは、ネットワークライセンス（NE/NA）に加えて設定できる機能ライセンスです。HSEC ライセンスは、強力なレベルの暗号化に対応した輸出規制を提供します。HSEC は、現在輸出入が禁止されている国を除くすべての国のお客様に利用可能です。これらの国は、米国商務省のリストに記載されています。HSEC ライセンスがない場合、SEC のパフォーマンスは各方向への IPsec スループットが合計 250 Mbps に制限されます。HSEC ライセンスによってこの制限を排除できます。

コマンドライン インターフェイス

IR1101 で HSEC を有効にする設定モード CLI は次のとおりです。

```
IR1101(config)# license feature hsec9
```

HSEC ライセンスにより、新しい帯域幅が利用可能になります。新しい帯域幅は **uncapped** と呼ばれ、設定モードから次の CLI で使用できます。

```
IR1101(config)# platform hardware throughput level ?
250M throughput in bps
uncapped throughput in bps
IR1101# platform hardware throughput level uncapped
```

上記のコマンドを実行した後、mem を書き込んでルータをリロードします。設定は、ルータが再起動すると有効になります。

ライセンスタイプ

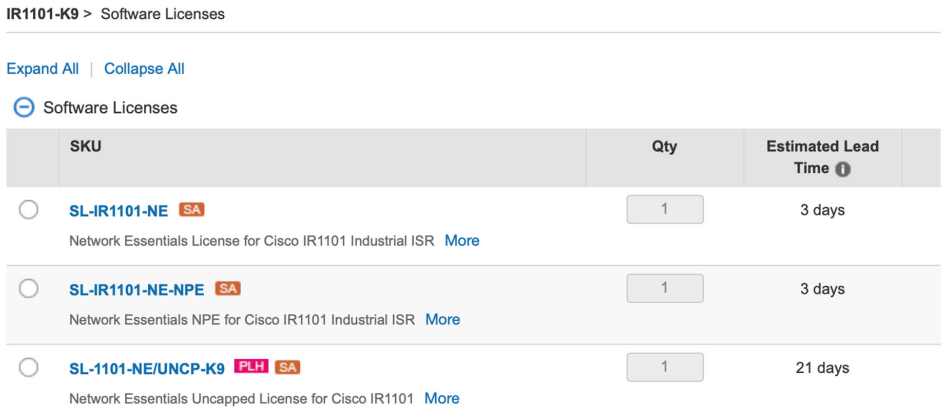
この新機能により、IR1101 は次の帯域幅/ライセンスタイプをサポートします。

- Network-essentials 250 Mbps
- Network-advantage 250 Mbps
- Network-essentials uncapped
- Network-advantage uncapped
- HSEC

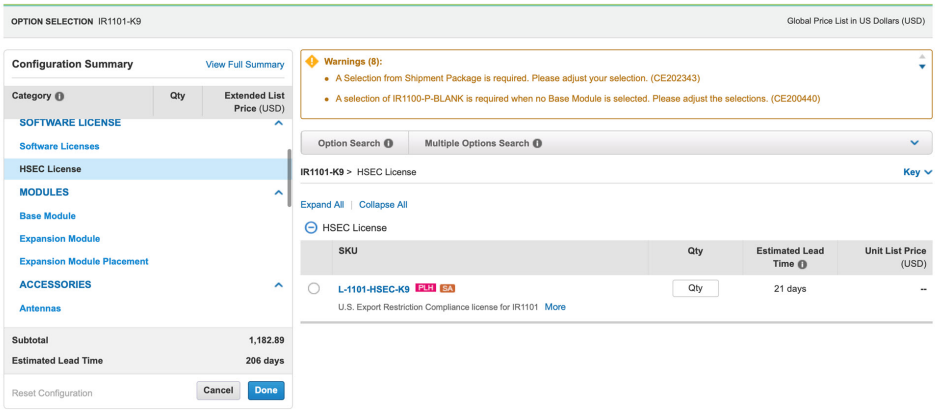
注文

以下は IR1101-K9 の例です。このライセンスは、IR1101-A-K9 でも利用できます。

次の例では、SL-1101-NE/UNCP-K9（Network Essentials Uncapped ライセンス）を選択します。



L-1101-HSEC-K9 ライセンスは、次に示すように、uncapped（上限なし）ライセンスを選択すると自動的に含まれます。



Cisco Software Central

このガイドでは、シスコスマートライセンスを注文、アクティブ化、および管理する方法について説明します。

https://software.cisco.com/software/csws/ws/platform/home?locale=en_US&locale=en_US&locale=en_US#

セキュアデータワイプ機能の有効化

セキュアデータワイプは、すべての IOS XE ベースのプラットフォーム上のストレージデバイスが NIST SP 800-88r1 準拠の安全に消去するコマンドを使用して適切に消去されるようにするためのシスコ全体のイニシアチブです。可能な限り常に、IoT プラットフォームは、対応する ENG の設計とこれまでのプラットフォームで利用可能な実装を活用します。

この機能は、次の IoT プラットフォームでサポートされます。

- IR1101
- IR1800
- IR8140
- ESR6300

セキュアデータワイプの有効化が実行されると、以下が消去されます。

- IR1101、IR1800、IR8140：NVRAM、rommon 変数、ブートフラッシュ、および msata
- ESR6300：NVARM、rommon 変数、ブートフラッシュ

コマンドの実行後、ルータは工場出荷時のデフォルト設定（ボーレート 9600）で rommon プロンプトになります。TFTP ダウンロード（プラットフォームでサポートされている場合）または usbflash を介して IOS イメージで起動するまで、ブートフラッシュはフォーマットされません。

セキュアデータワイプの実行

この機能を有効にするには、次を実行します。

```
Router#factory-reset all secure
The factory reset operation is irreversible for securely reset all. Are you sure?
[confirm]Y
```

重要 この操作には数時間かかる場合があります。電源を入れ直さないでください。

コマンドの実行後にログを確認し、IOS XE を起動するには、次の手順を実行します。

```
Router#show platform software factory-reset secure log
Factory reset log:
#CISCO DATA SANITIZATION REPORT:# IR1800
Purge ACT2 chip at 12-08-2022, 15:17:28
ACT2 chip Purge done at 12-08-2022, 15:17:29
mtd and backup flash wipe start at 12-08-2022, 15:17:29
mtd and backup flash wipe done at 12-08-2022, 15:17:29.
```

raw ソケットキープアライブ設定 CLI

非同期インターフェイスの raw ソケットキープアライブは、従来の IOS プラットフォームに存在していた機能の 1 つです。17.10.1a の一部として、この機能は IOS-XE ベースのプラットフォームに拡張されます。次の構文を持つ新しい CLI が raw ソケットの下に追加されます。

```
Router(config-line)#raw-socket tcp keepalive interval
```

CLI の変更

17.10.1a 以降の IOS-XE プラットフォームでは、CLI の修正があり、追加の CLI が raw ソケットの一部として追加されました。

修正は、**raw-socket idle timeout** コマンドに対するものです。以前の設定では分のみを使用していましたが、分と秒に基づいてタイムアウトを設定するオプションが追加されました。

```
Router(config-line)# raw-socket tcp idle-timeout [0-1440] [<0-59> | cr]
```

追加の CLI は、raw ソケット TCP クライアントをクリアするためのものです。コマンドの構文は **clear raw-socket line** *[1-145|tty|x/y/z]* です。例：

```
Router# clear raw-socket line 0/2/0
```

（注） clear raw-socket line を開始すると、**show raw-socket tcp sessions** コマンドから raw ソケットクライアントの raw ソケットセッションがクリアされます。接続は、TCP ハンドシェイク後に再確立されます。これは、TCP 接続インターフェイスで shut/no shut を実行することで達成できます。

第 17 章

コンフィギュレーション ファイルの管理

この章は、次の項で構成されています。

コンフィギュレーション ファイルの概要

コンフィギュレーションファイルには、現在のシスコ製ルーティングデバイス（ルータ、アクセスサーバー、スイッチなど）の機能をカスタマイズするために使用される、Cisco IOS XE ソフトウェアコマンドが含まれています。コマンドは、システムを起動したとき（startup-config ファイルから）、またはコンフィギュレーションモードでCLIにコマンドを入力したときに、Cisco IOS XE ソフトウェアによって解析（変換および実行）されます。

コンフィギュレーション ファイルのタイプ

スタートアップ コンフィギュレーションファイル（startup-config）は、ソフトウェアを設定するためにシステムの起動時に使用されます。実行コンフィギュレーション ファイル（running-config）には、ソフトウェアの現在の設定が含まれています。2つのコンフィギュレーションファイルは別々の設定にできます。たとえば、コンフィギュレーションを永続的ではなく短期間だけ変更する場合があります。このような場合、configure terminal EXEC コマンドを使用して実行コンフィギュレーションを変更しますが、copy running-config startup-config EXEC コマンドを使用して設定を保存することはありません。

実行コンフィギュレーションを変更するには、configure terminal コマンドを使用します。Cisco IOS XE コンフィギュレーション モードの使用時には、通常コマンドはすぐに実行され、入力直後またはコンフィギュレーションモードを終了した時点で実行コンフィギュレーションファイルに保存されます。

スタートアップ コンフィギュレーション ファイルを変更するには、copy running-config startup-config EXEC コマンドを使用してスタートアップ コンフィギュレーションに実行コンフィギュレーション ファイルを保存するか、ファイルサーバーからスタートアップ コンフィギュレーションへコンフィギュレーション ファイルをコピーします。

コンフィギュレーション ファイルの場所

コンフィギュレーション ファイルは、次の場所に保存することができます。

- 実行コンフィギュレーションは RAM に格納されます。
- スタートアップ コンフィギュレーションはCONFIG_FILE環境変数で指定された場所に格納されます。

  CONFIG_FILE 変数は、デフォルトではNVRAMになりますが、次のファイル システムのファイルも指定できます。

  - nvram:（NVRAM）
  - bootflash:（内部フラッシュメモリ）
  - usbflash0:（外部 USB メディア）

ソフトウェア バージョンの確認

Cisco IOS XE ソフトウェアのパッケージファイルは、システムボードのフラッシュデバイスのフラッシュ（flash:）または前述の外部デバイスのいずれかにあります。

show version 特権 EXEC コマンドを使用すると、デバイスで稼働しているソフトウェアバージョンを参照できます。

（注） **show version** の出力にはデバイスで稼働しているソフトウェアイメージが常に表示されますが、最後に表示されるモデル名は工場出荷時の設定であり、ソフトウェアライセンスをアップグレードしても変更されません。

また、**dir** *filesystem*: 特権 EXEC コマンドを使用して、フラッシュメモリに保存している可能性のある他のソフトウェアイメージのディレクトリ名を表示できます。

copyおよびbootコマンドを使用した統合パッケージの管理と設定

統合パッケージをアップグレードするには、ルータの bootflash: ディレクトリに統合パッケージをコピーします。こうして統合パッケージのコピーを作成した後、統合パッケージファイルを使ってブートするようルータを設定します。

次の例は、bootflash: ファイルシステムに統合パッケージファイルをコピーする方法を示しています。さらに、boot system コマンドを使用して起動するようにコンフィギュレーション レジスタを設定し、このコマンドにより、bootflash: ファイルシステムに保存されている統合パッ

ケージを使用して起動するようルータに指示します。その後、新しい設定は copy running-config startup-config コマンドにより保存され、システムがリロードされてプロセスが終了します。

bootflash ディレクトリの内容を表示します。

```
Router# dir bootflash:
Directory of bootflash:/
13      drwx           278528  May 19 2022 05:20:04 +00:00  tracelogs
11      drwx             4096  May 17 2022 14:24:54 +00:00  .installer
84      drwx            20480  May 17 2022 14:22:00 +00:00  license_evlog
83      -rw-               30  May 17 2022 14:21:41 +00:00  throughput_monitor_params
12      drwx             4096  May 17 2022 14:21:39 +00:00  .prst_sync
22      -rw-              335  May 17 2022 14:20:50 +00:00  boothelper.log
14      -rwx            41040  May 17 2022 14:20:39 +00:00  mode_event_log
259     -rw-        682679541  May 17 2022 12:54:32 +00:00
ir1800-universalk9.17.07.01.SPA.bin
```

新しいイメージを bootflash: ディレクトリにコピーします。

（注） セキュアコピー（scp）を使用するには、最初に SSH の設定をセットアップする必要があります。「Configuring Secure Shell」を参照してください。

```
Router# copy scp: bootflash:
Address or name of remote host []? 192.168.1.2
Source username [xxxxx]?Enter
Source filename []? /auto/users/IR1800-universalk9.17.08.01.SPA.bin
Destination filename [IR1800-universalk9.17.08.01.SPA.bin]?

This is a Cisco managed device to be used only for authorized purposes.
Your use is monitored for security, asset protection, and policy compliance.

Password: <your-password>
Sending file modes: C0644 208904396 IR1800-universalk9.17.08.01.SPA.bin
...........
[OK - 208904396 bytes]
208904396 bytes copied in 330.453 secs (632176 bytes/sec)
```

bootflash: ディレクトリの内容を表示します。

```
Router# dir bootflash:
Directory of bootflash:/
13      drwx           278528  May 19 2022 05:20:04 +00:00  tracelogs
11      drwx             4096  May 17 2022 14:24:54 +00:00  .installer
84      drwx            20480  May 17 2022 14:22:00 +00:00  license_evlog
83      -rw-               30  May 17 2022 14:21:41 +00:00  throughput_monitor_params
12      drwx             4096  May 17 2022 14:21:39 +00:00  .prst_sync
22      -rw-              335  May 17 2022 14:20:50 +00:00  boothelper.log
14      -rwx            41040  May 17 2022 14:20:39 +00:00  mode_event_log
259     -rw-        682679541  May 17 2022 12:54:32 +00:00
ir1800-universalk9.17.07.01.SPA.bin
12      -rw-        208904396  May 17 2022 16:17:34 -07:00
ir1800-universalk9.17.08.01.SPA.bin
```

統合パッケージファイルを使用してブートするようにルータを設定します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system bootflash:ir1800-universalk9.17.08.01.SPA.bin
Router(config)# exit
```

設定の変更を確認します。

```
Router# show run | include boot
boot-start-marker
boot system bootflash:IR1800-universalk9.17.08.01.SPA.bin
boot-end-marker
```

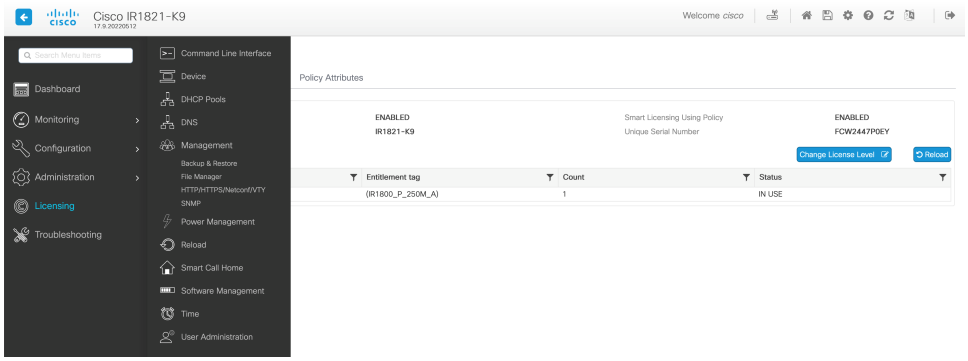
実行コンフィギュレーションをコピーして保存します。その後、ルータをリロードすると、保存した設定で再起動します。

```
Router# copy running-config startup-config
Destination filename [startup-config]? <enter>
Building configuration...
[OK]

Router# reload
Proceed with reload? [confirm] <enter>
Dec 04 17:42:54.445 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit
with reload

Initializing Hardware ...
```

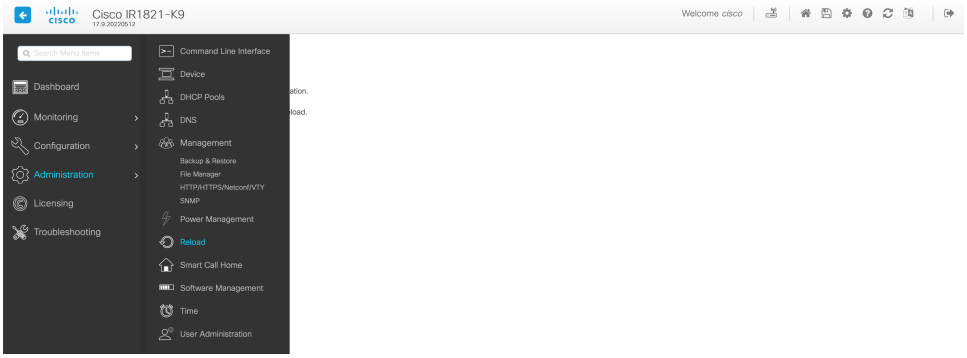
WebUI によるルータイメージのアップグレード

ルータは、Web ユーザーインターフェイス（WebUI）を使用してアップグレードすることもできます。WebUI の使用方法の詳細については、「Web ユーザーインターフェイス（WebUI）」の章を参照してください。

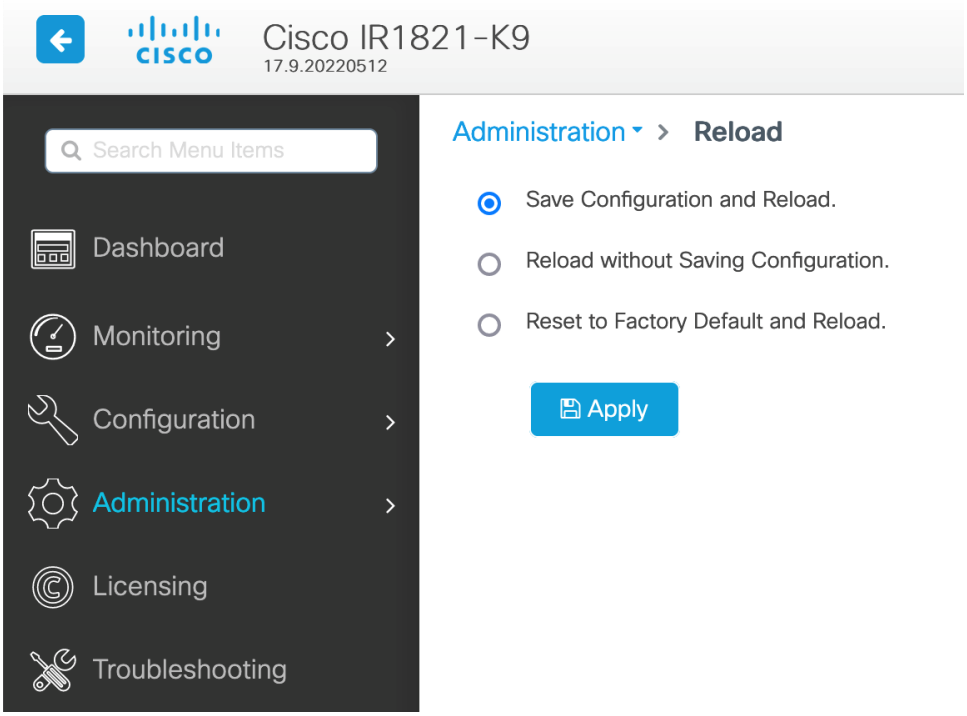
WebUI を起動したら、[Administration] タブに移動します。



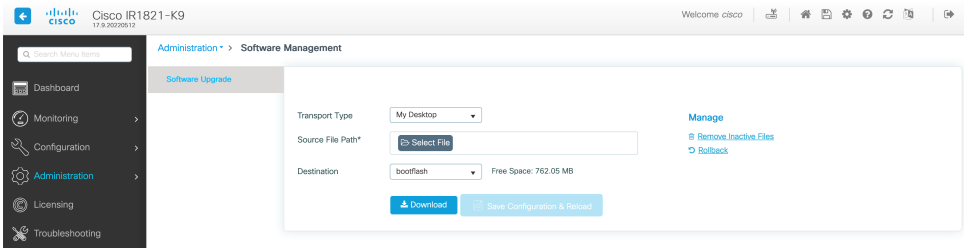
[Administration] > [Reload] を選択して、ルータをリロードします。



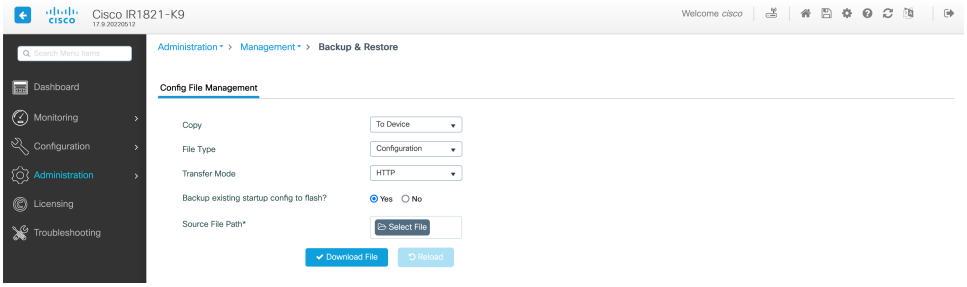
選択肢からオプションを選択し、[Apply] をクリックします。



[Administration] タブの [Software Management] を選択します。PC 上の新しい IOS XE イメージファイルの場所を参照します。



[Administration] > [Management] > [Backup & Restore] を選択します。ラップトップからルータにイメージファイルをコピーします。この例では、HTTP を転送に使用します。



WebUI の上部にあるフロッピードライブアイコンをクリックして、設定を保存します。

第 18 章

新しい Cisco IOS XE のインストール方法

この章は、次の項で構成されています。

バンドルモードとインストールモード

IoT ルータで実行されている Cisco IOS XE は、通常、バンドル起動モードを使用しています。バンドル起動モードは統合起動とも呼ばれ、単一の圧縮イメージを使用します。一般的な命名規則は、<product>-universalk9.<release>.SPA.bin です。

このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。.bin イメージ経由で起動するということは、ルータは、起動する前にまずイメージを解凍する必要があることを意味します。これにより、ルータを起動するためにより長い時間がかかっていました。

ルータを新しいバージョンの IOS XE にアップグレードするには、「boot system」が新しいソフトウェアイメージをポイントするようにします。この方法はよく知られており、製品設定ガイドに詳細が記載されています。

IOS XE リリース 17.9.1 以降、インストールモードと呼ばれる新しい起動モードが IoT ルータに追加されました。インストールモードでは、packages.conf ファイルによって読み取られるブートフラッシュにロードされたパッケージが使用されます。この方法では、ソフトウェアのインストールプロセスをより正確に制御できます。

インストールモードでは、ファイル用にブートフラッシュにより多くのスペースが必要です。パッケージは .bin イメージよりわずかに大きく、製品ごとにサイズが異なります。

インストールコマンドを使用したソフトウェアのインストール

Cisco IOS XE 17.9.1 以降、Cisco IoT ルータはデフォルトでインストールモードで出荷されます。ユーザーは、一連の **install** コマンドを使用して、プラットフォームを起動し、Cisco IOS XE ソフトウェアバージョンにアップグレードまたはダウングレードできます。

インストールコマンドを使用したソフトウェアのインストールに関する制約事項

- インストールモードでは、システムの再起動が必要です。
- SMU のインストールは、バンドル起動モードとインストールモードの両方でサポートされていました。Cisco IOS XE リリース 17.9.x 以降、ルータがバンドルモードで起動された場合、SMU のインストールは停止されます。ルータがインストールモードで起動された場合、SMU のインストールは以前のリリースと同様に機能します。

インストールコマンドを使用したソフトウェアのインストールに関する情報

Cisco IOS XE 17.9.1 リリースから、IoT ルータはバンドルモードではなくインストールモードで出荷されます。したがって、工場からの新しいルータはすべてインストールモードで起動します。

IOS XE の以前のリリースを使用している既存のインストールには、必要に応じて、バンドルモードでデバイスを引き続き使用するオプションがあります。または、デバイスをインストールモードに変換できます。

インストールモードは、自律モードとコントローラモードの両方に適用できます。

新しいリリースは、vManage を使用してインストールモードでインストールできます。IOT OD や FND などの他の管理ツールは、将来のリリースで利用可能になる予定です。

次の表に、バンドルモードとインストールモードの違いを示します。

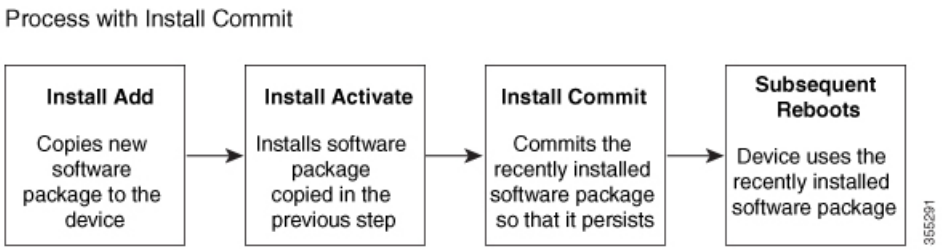
表 *8*：バンドルモードとインストールモード

バンドルモード	インストールモード
このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。	このモードでは、ブートプロセスにローカル（ブートフラッシュ）の packages.conf ファイルを使用します。
このモードでは、1 つの .bin ファイルを使用します。	このモードでは、.bin ファイルは拡張された .pkg ファイルに置き換えられます。
CLI： `Router(config)#boot system bootflash:<filename>`	CLI： `#install add file bootflash: [activate commit]`
このモードでアップグレードするには、boot system が新しいソフトウェアイメージをポイントするようにします。	このモードでアップグレードするには、**install** コマンドを使用します。
イメージの自動アップグレード：新しい Field Replaceable Unit（FRU）がモジュラ型シャーシに挿入された場合、アクティブな FRU と同じバージョンで新しい FRU を実行するには、手動による作業が必要です。	イメージの自動アップグレード：新しい FRU がモジュラ型シャーシに挿入された場合、結合する FRU は、アクティブな FRU と同期してイメージバージョンに自動アップグレードされます。
ロールバック：複数のソフトウェアメンテナンスの更新（SMU）を使用して以前のイメージにロールバックするには、複数回のリロードが必要になる場合があります。	ロールバック：1 回のリロードで、複数のパッチを含む、Cisco IOS XE ソフトウェアの以前のバージョンへのロールバックを有効にします。

インストールモードのプロセスフロー

インストールモードのプロセスフローは、プラットフォームでソフトウェアのインストールとアップグレードを実行するための次の 3 つのコマンドで構成されています：**install add**、**install activate**、および **install commit**。

次のフローチャートは、**install** コマンドを使用したインストールプロセスを説明しています。



install add コマンドは、ソフトウェアパッケージをローカルまたはリモートの場所からプラットフォームにコピーします。このコマンドは、パッケージファイルの個々のコンポーネントをサブパッケージと packages.conf ファイルに展開します。またファイルを検証して、イメージファイルがこれからインストールする先のプラットフォーム用のものであることを確認します。

次のコマンドの出力に示されているように、ソフトウェアパッケージはいくつかの場所に置いておけます。

```
IR1831#install add file ?
bootflash: Package name
crashinfo: Package name
flash: Package name
ftp: Package name
http: Package name
https: Package name
pram: Package name
rcp: Package name
scp: Package name
sftp: Package name
tftp: Package name
webui: Package name
```

install activate コマンドは、必要な検証を実行し、**install add** コマンドを使用して前段で追加されたパッケージをプロビジョニングします。また、システムのリロードをトリガーします。

install commit コマンドは、**install activate** コマンドを使用して前段でアクティブ化されたパッケージを確認し、リロード後も更新が持続されるようにします。

（注） 更新をインストールすると、以前にインストールしたソフトウェアイメージが置換されます。どんな時でも、1 つのデバイスにインストールできるのは 1 つのイメージのみです。

次の一連のインストールコマンドが使用できます。

表 *9:* インストールコマンド一覧

コマンド	構文	目的
install add	**install add file** *location:filename.bin*	イメージ、パッケージ、およびSMUの内容をソフトウェアリポジトリにコピーします。ファイルの場所はローカルでもリモートでもかまいません。このコマンドは次のことを行います。 • ファイルのチェックサム、プラットフォームの互換性チェックなどを検証します。 • パッケージの個々のコンポーネントをサブパッケージと packages.conf に展開します。 • イメージをローカルインベントリにコピーし、次の手順で使用できるようにします。
install activate	**install activate**	**install add** コマンドを使用して追加されたパッケージをアクティブ化します。 • **show install summary** コマンドを使用して、非アクティブなイメージを確認します。このイメージがアクティブ化されます。 • このコマンドを実行すると、システムがリロードされます。アクティベーションを続行するかどうかを確認します。確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。

コマンド	構文	目的
(install activate) auto abort-timer	**install activate auto-abort timer** *<30-1200>*	**auto-abort timer** は自動的に開始され、デフォルト値は 120 分です。指定された時間内に **install commit** コマンドが実行されない場合、アクティベーションプロセスは中止され、システムは最後にコミットされた状態に戻ります。 • **install activate** コマンドを実行しながらタイマーの値を変更できます。 • **install commit** コマンドはタイマーを停止し、インストールプロセスを続行します。 • **install activate auto-abort timer stop** コマンドは、パッケージをコミットせずにタイマーを停止します。 • 確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。 • このコマンドは、3 ステップインストールのバリアントでのみ有効です。
install commit	**install commit**	**install activate** コマンドを使用してアクティブ化されたパッケージをコミットし、リロード後も持続するようにします。 • **show install summary** コマンドを使用して、コミットされていないイメージを確認します。このイメージがコミットされます。

コマンド	構文	目的
install abort	**install abort**	インストールを中止し、システムを最後にコミットされた状態に戻します。 • このコマンドは、パッケージがアクティブ化された状態（コミットされていない状態）の場合にのみ適用されます。 • **install commit** コマンドを使用してイメージをすでにコミットしている場合は、**install rollback to** コマンドを使用して望みのバージョンに戻ります。
install remove	**install remove {file** <*filename*> **| inactive}**	プラットフォームリポジトリから非アクティブなパッケージを削除します。このコマンドを使用して、スペースを解放します。 • **file**：指定されたファイルを削除します。 • **inactive**：非アクティブなファイルをすべて削除します。

コマンド	構文	目的
install rollback to	**install rollback to {base | label | committed | id}**	保存されているインストールポイントか、最後にコミットされたインストールポイントに、ソフトウェアセットをロールバックします。このコマンドには次のような特長があります。 • リロードが必要です。 • パッケージがコミットされた状態の場合にのみ適用されます。 • 確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。 （注） 以前のイメージへのインストールのロールバックを実行する場合は、以前のイメージはインストールモードでインストールされている必要があります。バンドルモードでは SMU ロールバックのみが可能です。
install deactivate	**install deactivate file** <*filename*>	プラットフォームリポジトリからパッケージを削除します。このコマンドは、SMU でのみサポートされています。 • 確認プロンプトを自動的に無視するには、このコマンドと **prompt-level none** キーワードを使用します。

次の show コマンドも使用できます。

表 *10 : show* コマンドの一覧

コマンド	構文	目的
show install log	**show install log**	プラットフォームがブートされた後に実行されたすべてのインストール操作の履歴と詳細を提供します。
show install package	**show install package** <*filename*>	指定された .pkg/.bin ファイルに関する詳細を提供します。
show install summary	**show install summary**	イメージバージョンとそれに対応するインストール状態の概要を提供します。
show install active	**show install active**	アクティブなパッケージに関する情報を提供します。
show install inactive	**show install inactive**	非アクティブなパッケージに関する情報を提供します。
show install committed	**show install committed**	コミットされたパッケージに関する情報を提供します。
show install uncommitted	**show install uncommitted**	コミットされていないパッケージに関する情報を提供します。
show install rollback	**show install rollback {point-id | label}**	保存されているインストールポイントに関連付けられたパッケージを表示します。
show version	**show version [rp-slot] [installed [user-interface] | provisioned | running]**	ハードウェアとプラットフォームの情報とともに、現在のパッケージに関する情報を表示します。

プラットフォームをインストールモードで起動

単一のコマンド（1 ステップインストール）または複数の個別のコマンド（3 ステップインストール）を使用してソフトウェアパッケージをインストールして、アクティブ化し、コミットできます。

プラットフォームがバンドルモードで動作している場合、1 ステップインストールの手順を使用して、最初にバンドルモードからインストールモードに変換する必要があります。その後のプラットフォームでのインストールとアップグレードは、1 ステップまたは 3 ステップのバリアントのいずれかで実行できます。

show romvar および **show bootvar** コマンドを使用して、デバイスがどのように起動するように設定されているかを確認できます。

```
Router#show romvar
ROMMON variables:
PS1 = rommon ! >
CM = IR1100
DEVICE_MANAGED_MODE = autonomous
LICENSE_SUITE =
RET_2_RTS =
THRPUT = 250
BOOT = flash:packages.conf,12;
LICENSE_BOOT_LEVEL = network-advantage,all:IR1101;
BSI = 0
RET_2_RCALTS =
RANDOM_NUM = 212626522
Router#

Router#show bootvar
BOOT variable = flash:packages.conf,12;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102

Standby not ready to show bootvar

Router#
```

1 ステップインストールまたはバンドルモードからインストールモードへの変換

（注）

- すべての CLI アクション（追加、アクティブ化など）が実行されます。
- 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
- このワークフローの 2 番目のステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。
- プロンプトレベルが [None] に設定されていて、保存されていない設定がある場合、インストールは失敗します。コマンドを再発行する前に、設定を保存する必要があります。

以下で説明する 1 ステップインストールの手順を使用して、バンドルブートモードで実行されているプラットフォームをインストールモードに変換します。コマンドの実行後、プラットフォームはインストールブートモードでリブートします。

後で、1 ステップインストールの手順を使用してプラットフォームをアップグレードすることもできます。

この手順では、特権 EXEC モードで **install add file activate commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**install add file location:** *filename* [**activate commit**] 例： `Device#install add file bootflash:<router_image>.SSA.bin activate commit`	ソフトウェア インストール パッケージをローカルまたはリモートの場所（FTP、HTTP、HTTPs、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよびpackages.confファイルに展開します。プラットフォームおよびイメージバージョンの検証および互換性チェックを実行し、パッケージをアクティブ化し、そのパッケージをコミットして複数回リロードしても維持されるようにします。 このコマンドを実行すると、プラットフォームがリロードされます。
ステップ 3	**exit** 例： `Device#exit`	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

3 ステップインストール

（注）
- すべての CLI アクション（追加、アクティブ化など）が実行されます。
- 保存されていない設定が検出されると、設定保存プロンプトが表示されます。
- このワークフローの install activate ステップの後に、リロードプロンプトが表示されます。確認プロンプトを自動的に無視するには、**prompt-level none** キーワードを使用します。

3 ステップインストール手順は、プラットフォームがインストールモードになった後でのみ使用できます。このオプションにより、インストール時により多くの柔軟性と制御がもたらされます。

この手順では、個別の **install add**, **install activate**、および **install commit** コマンドを使用して、ソフトウェアパッケージをインストールし、プラットフォームを新しいバージョンにアップグレードします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**install add file location:** *filename* 例： `Device#install add file bootflash:<router_image>.SSA.bin`	ソフトウェア インストール パッケージをリモートの場所（FTP、HTTP、HTTPs、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよび packages.conf ファイルに展開します。
ステップ 3	**show install summary** 例： `Device#show install summary`	（オプション）イメージバージョンとそれに対応するインストール状態の概要を提供します。
ステップ 4	**install activate auto-abort-timer** <*time*> 例： `Device# install activate auto-abort-timer 120`	以前に追加されたパッケージをアクティブ化し、プラットフォームをリロードします。 • ソフトウェアの完全インストールを実行する場合は、パッケージ ファイル名を指定しないでください。 • 3 ステップインストールのバリアントでは、**install activate** コマンドで **auto-abort-timer** が自動的に開始されます。タイマーのデフォルトは 120 分です。タイマーの期限が切れる前に **install commit** コマンドが実行されない場合、インストールプロセスは自動的に中止されます。プラットフォームがリロードされ、最後にコミットされたバージョンで起動します。
ステップ 5	**install abort** 例： `Device#install abort`	（オプション）ソフトウェアインストールのアクティブ化を中止し、プラットフォームを最後にコミットされたバージョンに戻します。 • このコマンドは、イメージがアクティブ化されている状態でのみ使用できます。イメージがコミットされた状態の場合は使用できません。
ステップ 6	**install commit** 例： `Device#install commit`	新しいパッケージのインストールをコミットし、リロード後も変更が持続されるようにします。

	コマンドまたはアクション	目的
ステップ 7	**install rollback to committed** 例： `Device#install rollback to committed`	（オプション）最後にコミットした状態にプラットフォームをロールバックします。
ステップ 8	**install remove** {**file** *filesystem: filename* | **inactive**} 例： `Device#install remove inactive`	（オプション）ソフトウェア インストール ファイルを削除します。 • **file**：特定のファイルを削除します • **inactive**：未使用および非アクティブ状態のインストールファイルを削除します。
ステップ 9	**show install summary** 例： `Device#show install summary`	（オプション）現在のシステムの状態に関する情報を表示します。このコマンドの出力は、このコマンドよりも先に実行された **install** コマンドに応じて変化します。
ステップ 10	**exit** 例： `Device#exit`	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

インストール モードでのアップグレード

1 ステップインストールまたは 3 ステップインストールを使用して、インストールモードでプラットフォームをアップグレードします。

インストールモードでのダウングレード

ダウングレード先のイメージがインストールモードでインストールされている場合、**install rollback** コマンドを使用して適切なイメージをポイントすることにより、プラットフォームを以前のバージョンにダウングレードします。

この **install rollback** コマンドはプラットフォームをリロードし、以前のイメージで起動します。

（注） **install remove inactive** コマンドを使用して前のファイルを削除していない場合にのみ、**install rollback** コマンドは成功します。

または、**install** コマンドを使用して古いイメージをインストールすることでダウングレードすることもできます。

ソフトウェアインストールの中止

ソフトウェアパッケージのアクティブ化は次の方法で中止できます。

- 新しいイメージをアクティブ化した後にプラットフォームをリロードすると、3 ステップインストールのバリアントでは auto-abort-timer がトリガーされます。**install commit** コマンドを発行する前にタイマーが期限切れになった場合、インストールプロセスが中止されます。プラットフォームはリロードし、最後にコミットしたバージョンのソフトウェアイメージで起動します。

  または、**install commit** コマンドを使用せずに、**install auto-abort-timer stop** コマンドを使用してこのタイマーを停止します。このプロセスでは、新しいイメージはコミットされていないままです。

- **install abort** コマンドを使用すると、プラットフォームが新しいソフトウェアのインストール前に実行していたバージョンに戻ります。このコマンドは、**install commit** コマンドを発行する前に使用します。

設定例

このセクションでは、インストールコマンドの使用例を示します。

1 ステップインストール

以下は、1 ステップインストールまたはバンドルモードからインストールモードへの変換の例です。

```
Router# install add file
flash:ir1101-universalk9.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.bin activate commit
install_add_activate_commit: START Mon May 30 20:45:11 UTC 2022
install_add: Adding IMG
--- Starting initial file syncing ---
Copying flash:ir1101-universalk9.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.bin from
R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
 [1] Finished Add package(s) on  R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.09.01.0.157857

install_activate: Activating IMG
Following packages shall be activated:
/flash/ir1101-mono-universalk9_iot.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.pkg
/flash/ir1101-rpboot.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
```

```
--- Starting Activate ---
Performing Activate on all members
Building configuration...
[OK] [1] Activate package(s) on  R0
 [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
 [1] Commit package(s) on  R0
 [1] Finished Commit on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_add_activate_commit Mon May 30 20:48:01 UTC 2022
%PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action requested
watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system


System Bootstrap, Version 3.3(REL), RELEASE SOFTWARE
Copyright (c) 1994-2021  by cisco Systems, Inc.

IR1101-K9 platform with 4169728 Kbytes of main memory

MCU Version - Bootloader: 4, App: 6
MCU is in application mode.


........


Loading: bootflash:packages.conf
#

################################################################################################
################################################################################################
################################

%BOOT-5-OPMODE_LOG: R0/0: binos: System booted in AUTONOMOUS mode
Press RETURN to get started!

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01.0.157857

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

3 ステップインストール

以下は、3 ステップインストールの例です。

Install Add

```
Router# install add file flash:ir1101-universalk9.17.09.01prd1.SPA.bin
install_add: START Tue May 31 01:35:40 UTC 2022
install_add: Adding IMG
--- Starting initial file syncing ---
Copying flash:ir1101-universalk9.17.09.01prd1.SPA.bin from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
 [1] Finished Add package(s) on  R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.09.01.0.1

SUCCESS: install_add /flash1/ir1101-universalk9.17.09.01prd1.SPA.bin Tue May 31 01:37:10
 UTC 2022
Router#

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   I    17.09.01.0.1

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Install Activate

```
Router#install activate
install_activate: START Tue May 31 01:37:14 UTC 2022
install_activate: Activating IMG
Following packages shall be activated:
/flash/ir1101-mono-universalk9_iot.17.09.01prd1.SPA.pkg
/flash/ir1101-rpboot.17.09.01prd1.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y


--- Starting Activate ---
Performing Activate on all members
 [1] Activate package(s) on  R0
 [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

SUCCESS: install_activate Tue May 31 01:41:03 UTC 2022
Router#
```

```
May 31 01:41:08.684: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
 reload action requested

watchdog: watchdog0: watchdog did not stop!
reboot: Restarting system

System Bootstrap, Version 3.3(REL), RELEASE SOFTWARE
Copyright (c) 1994-2021  by cisco Systems, Inc.

IR1101-K9 platform with 4169728 Kbytes of main memory

MCU Version - Bootloader: 4, App: 6
MCU is in application mode.

........


Loading: bootflash:packages.conf
#

################################################################################
################################################################################
#######################

Press RETURN to get started!

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   U    17.09.01.0.1

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Install Commit

```
Router#install commit
install_commit: START Tue May 31 01:47:56 UTC 2022
--- Starting Commit ---
Performing Commit on all members
 [1] Commit packages(s) on  R0
 [1] Finished Commit packages(s) on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation


SUCCESS: install_commit Tue May 31 01:48:04 UTC 2022

Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01.0.1

--------------------------------------------------------------------------------
```

```
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

インストール済みパッケージの表示

```
Router# show install package flash:ir1101-universalk9.17.09.01prd1.SPA.bin
  Package: ir1101-universalk9.17.09.01prd1.SPA.bin
    Size: 674114352
    Timestamp:
  Canonical path: /flash1/ir1101-universalk9.17.09.01prd1.SPA.bin

    Raw disk-file SHA1sum:
      e54ba5a59824156af7515eaf4367ebe51b920316
  Header size:     1148 bytes
  Package type:    30000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: rp_super
    BuildTime: 2022-04-27_00.47
    ReleaseDate: 2022-04-27_07.05
    BootArchitecture: arm64
    RouteProcessor: IR1101
    Platform: IR1101
    User: mcpre
    PackageName: universalk9
    Build: 17.09.01prd1
    CardTypes:

  Package is bootable from media and tftp.
  Package contents:

  Package: ir1101-mono-universalk9_iot.17.09.01prd1.SPA.pkg
    Size: 673776700
    Timestamp:

    Raw disk-file SHA1sum:

    Header size:     1084 bytes
    Package type:    30000
    Package flags:   0
    Header version:  3

    Internal package information:
      Name: mono
      BuildTime: 2022-04-27_00.47
      ReleaseDate: 2022-04-27_07.05
      BootArchitecture: arm64
      RouteProcessor: IR1101
      Platform: IR1101
      User: mcpre
      PackageName: mono-universalk9_iot
      Build: 17.09.01prd1
      CardTypes:

    Package is bootable from media and tftp.
    Package contents:
```

show install active コマンドを使用して、アクティブなパッケージを判別できます。

```
Router#show install active
[ R0 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
IMG C 17.09.01.0.1193

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

コミット済みパッケージと非コミットパッケージの表示

これらの2つのshowコマンドは、コミットされているパッケージとコミットされていないパッケージに関する情報を提供します。

```
Router# show install committed
[ R0 ] Committed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    17.09.01.0.1

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------

Router#show install uncommitted
[ R0 ] Uncommitted Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
No Uncommitted Packages
```

非アクティブパッケージの削除

このコマンドは、未使用のインストールファイル（.conf/.pkg/.bin）をインストールメディアから削除します。

（注） このコマンドは、未使用のインストールファイルの起動ディレクトリをクリーンアップするために使用されます。ブート可能イメージは削除しません。

```
Router#install remove inactive
install_remove: START Tue May 31 01:49:10 UTC 2022
install_remove: Removing IMG
Cleaning up unnecessary package files
No path specified, will use booted path /bootflash/packages.conf

Cleaning /flash
  Scanning boot directory for packages ... done.
```

```
  Preparing packages list to delete ...
    [R0]: /flash/packages.conf File is in use, will not delete.
    [R0]: /flash/ir1101-mono-universalk9_iot.17.09.01prd1.SPA.pkg File is in use, will
not delete.
   [R0]: /flash/ir1101-universalk9.17.09.01prd1.SPA.conf File is in use, will not delete.

    [R0]: /flash/ir1101-rpboot.17.09.01prd1.SPA.pkg File is in use, will not delete.

The following files will be deleted:
    [R0]: /flash/ir1101-universalk9.17.09.01prd1.SPA.bin
   [R0]: /flash/ir1101-mono-universalk9_iot.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.pkg

    [R0]: /flash/ir1101-universalk9.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.conf
    [R0]: /flash/ir1101-rpboot.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.pkg

Do you want to remove the above files? [y/n]y


Deleting file /flash/ir1101-universalk9.17.09.01prd1.SPA.bin ... done.
Deleting file
/flash/ir1101-mono-universalk9_iot.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.pkg ...
done.
Deleting file /flash/ir1101-universalk9.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.conf
 ... done.
Deleting file /flash/ir1101-rpboot.BLD_POLARIS_DEV_LATEST_20220421_143208.SSA.pkg ...
done.
Deleting /bootflash/.images/17.09.01.0.1.1651045630 ... done.
SUCCESS: Files deleted.

--- Starting Post_Remove_Cleanup ---
Performing REMOVE_POSTCHECK on all members
Finished Post_Remove_Cleanup
SUCCESS: install_remove Tue May 31 01:49:14 UTC 2022

Router#show install inactive
[ R0 ] Inactive Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
No Inactive Packages
```

インストールコマンドを使用したソフトウェアインストールのトラブルシューティング

問題 ソフトウェアインストールのトラブルシューティング

解決法 インストールの概要、ログ、およびソフトウェアバージョンを表示するには、次の show コマンドを使用します。

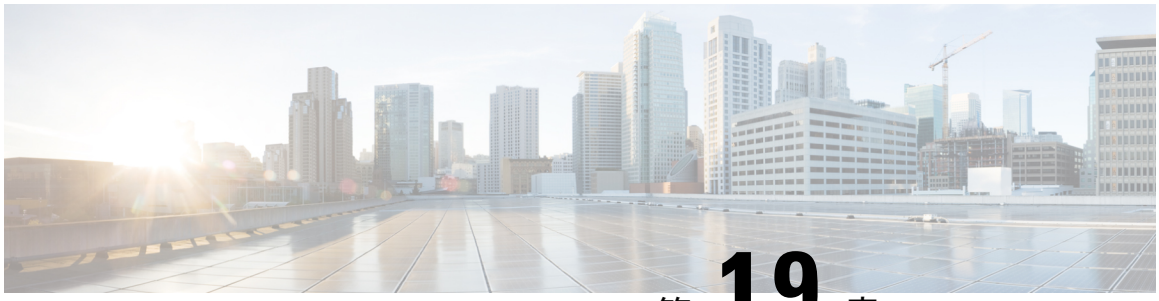
- **show install summary**
- **show install log**
- **show version**

- **show version running**

問題 インストールに関するその他の問題

解決法 インストールに関する問題を解決するには、次のコマンドを使用します。

- **dir** <*install directory*>
- **more location:***packages.conf*
- **show tech-support install**：このコマンドはインストール情報に固有の情報を表示する **show** コマンドを自動的に実行します。
- **request platform software trace archive target bootflash** <*location*>：このコマンドは、最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、この情報を指定された場所に保存します。



第 19 章

ソフトウェアのインストール

この章は、次の項で構成されています。

ソフトウェアのインストール

ルータにソフトウェアをインストールする際には、統合パッケージ（ブート可能イメージ）をインストールします。これはサブパッケージ（モジュール型ソフトウェアユニット）のバンドルで構成されており、各サブパッケージはそれぞれ異なる機能セットを制御します。

ソフトウェアをインストールする主要な方法として、次の 2 つの方法があります。

- 統合パッケージを使用して実行されるルータの管理および設定：この方法では、サブパッケージを個別にアップグレードでき、次に説明する方法と比較して、通常はブート時間が短くなります。モジュールのソフトウェアを個別にアップグレードする場合は、この方法を使用します。
- 個別のパッケージを使用して実行されるルータの管理および設定：これは、Cisco ルータ全般でサポートされている標準的なCiscoルータイメージインストールおよび管理に類似した、シンプルな方法です。

サービスの中断が可能な、予定されている保守期間内にソフトウェアのアップグレードを実行することをお勧めします。ソフトウェアアップグレードを有効にするには、ルータをリブートする必要があります。

ライセンス

この項の内容は、次のとおりです。

シスコ ソフトウェアのライセンス

シスコ ソフトウェア ライセンスは、シスコ ソフトウェア ライセンスを入手して検証することで Cisco IOS ソフトウェアのセットをアクティブ化するためのプロセスとコンポーネントで構成されています。

ライセンス付き機能を有効にし、ルータのブートフラッシュにライセンスファイルを格納することができます。ライセンスは、統合パッケージ、テクノロジーパッケージ、または個別の機能を対象とします。

IR1101 はスマート ライセンスを使用します。これについては、次の章で詳しく説明します。

IR1101 は使用権ライセンスをサポートせず、Specific License Reservation（SLR）のみをサポートしています。

統合パッケージ

ルータのソフトウェア イメージを取得するには、 次にアクセスしてください。
https://software.cisco.com/download/home/286319772/type/282046477/release/Gibraltar-16.11.1

（注） IR1101 にすべての IOS XE 機能セットが適用されない場合があります。一部の機能はまだ実装されていないか、このプラットフォームに適していない可能性があります。

あるライセンスに対応するすべてのサブシステムを起動させるために、イメージベースのライセンスが使用されます。このライセンスは、ブート時にのみ適用されます。

IR1101 ルータには、次のイメージベース ライセンスのいずれかを事前にインストールできます。

- Network-Essentials
- Network-Advantage

（注） Network-Essentials および Network-Advantage の内容の詳細については、次の製品データシートを参照してください。

https://www.cisco.com/c/en/us/products/collateral/routers/1101-industrial-integrated-services-router/datasheet-c78-741709.html

Network-Essentials

Network-Essentials テクノロジー パッケージには、ベースライン機能が含まれています。また、セキュリティ機能もサポートしています。

Network-Essentials_npe パッケージ（npe=ペイロード暗号化なし）には、ペイロード暗号化機能を除く Network-Essentials テクノロジー パッケージのすべての機能が含まれています。これは、輸出規制要件への準拠に伴うものです。Network-Essentials_npe は、Network-Essentials_npe イメージでのみ使用できます。したがって Network-Essentials パッケージと Network-Essentials_npe パッケージの機能の相違点は、ペイロード暗号化機能（IPsec や Secure VPN など）のセットです。

Network-Advantage

Network-Advantage テクノロジー パッケージには、すべての暗号化機能が含まれています。

Network-Advantage_npe パッケージ（npe = ペイロード暗号化なし）には、ペイロード暗号化機能を除く **Network-Advantage** テクノロジー パッケージのすべての機能が含まれています。これは、輸出規制要件への準拠に伴うものです。**Network-Advantage_npe** パッケージは、**Network-Advantage_npe** イメージでのみ使用できます。したがって **Network-Advantage** パッケージと **Network-Advantage_npe** パッケージの機能の相違点は、ペイロード暗号化対応機能（IPsec や Secure VPN など）のセットです。

関連資料

ソフトウェア ライセンスの詳細については、「スマートライセンス」の章を参照してください。

Cisco IOS XE 用ソフトウェアのインストール方法

ソフトウェアをインストールするには、以下に示す統合パッケージまたは個別パッケージのソフトウェアのいずれかの使用方法に従います。「概要」セクションも参照してください。

- 「統合パッケージで実行するルータの管理および設定」セクション
- 「個別のパッケージを使用して実行されるルータの管理および設定」セクション
- 「*boot* コマンドを使用して *TFTP* 経由で統合パッケージを起動するようにルータを設定する例」セクション

Cisco IOS XE リリースのインストール

デバイスは Cisco IOS XE イメージを使って初めて起動するとき、インストールされている ROMMON のバージョンをチェックし、システムが古いバージョンを実行している場合はアップグレードします。アップグレードプロセス中はデバイスの電源を再投入しないでください。新しいバージョンの ROMMON がインストールされると、システムは自動的にデバイスを再起動します。インストール後、システムは Cisco IOS XE イメージを通常どおりに起動します。

（注） デバイスを初めて起動したときにアップグレードが必要な場合、起動プロセス全体に数分かかることがあります。このプロセスでは、ROMMON をアップグレードするため、通常の起動よりも長くなります。

次の例は、統合パッケージの起動プロセスを示しています。

```
Router# configure terminal
 Router(config)#boot sys bootflash:ir1101-universalk9.16.10.01.SPA.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router#
*Nov  7 00:07:06.784: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router#show run | inc license
license udi pid IR1101-K9 sn FCW2150TH0F
license boot level network-advantage
Router#
Router#reload ?
  /noverify  Don't verify file signature before reload.
  /verify    Verify file signature before reload.
  at         Reload at a specific time/date
  cancel     Cancel pending reload
  in         Reload after a time interval
  pause      Pause during reload
  reason     Reload reason
  <cr>       <cr>

Router#reload /verify

System configuration has been modified. Save? [yes/no]: yes
Building configuration...

[OK]
*Nov  7 00:08:48.101: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
Verifying file integrity of bootflash:/ir1101-universalk9.16.10.01.SPA.bin.....
.................................

Embedded Hash   SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Computed Hash   SHA1 : B0315BDC4F545D624BB128CE0FFAA468E6EF7587
Starting image verification
Hash Computation:    100%Done!
Computed Hash   SHA2: 03febcc07fbeadeed664f2f5ef87f6c3
                      5b343e6f7aecdd70e50e5203909aec8f
                      3d276529d2a6af6859d4c77237f812d5
                      0da93678edc942c8874edca2d5224101

Embedded Hash   SHA2: 03febcc07fbeadeed664f2f5ef87f6c3
                      5b343e6f7aecdd70e50e5203909aec8f
                      3d276529d2a6af6859d4c77237f812d5
                      0da93678edc942c8874edca2d5224101

Digital signature successfully verified in file
bootflash:/ir1101-universalk9.16.10.01.SPA.bin
Signature Verified

Proceed with reload? [confirm]

*Jul  9 06:43:37.910: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
 Command. Jul  9 14:43:59.134: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting:
 process exit with reload chassis code

watchdog watchdog0: watchdog did not stop!
reboot: Restarting system



Press RETURN to get started!
```

ROMMON イメージ

ROMMONイメージは、ルータのROMモニタ（ROMMON）ソフトウェアで使用されるソフトウェア パッケージです。このソフトウェア パッケージは、ルータの起動に通常使用される統合パッケージとは別のものです。

独立したROMMONイメージ（ソフトウェア パッケージ）がリリースされることがあります。新しいROMMONソフトウェアを使ってルータをアップグレードできます。詳細な手順については、ROMMON イメージに付属のマニュアルを参照してください。

（注） ROMMONイメージの新しいバージョンは、常にルータの統合パッケージと同時にリリースされるとは限りません。

ファイル システム

次の表に、シスコ IR1101 シリーズ ルータで表示可能なファイル システムのリストを示します。

表 *11* : ルータのファイル システム

ファイルシステム	説明
bootflash:	ブートフラッシュ メモリのファイル システム。
flash:	上記のブートフラッシュ メモリのファイル システムのエイリアス。
cns:	Cisco Networking Service のファイル ディレクトリ。
nvram:	ルータの NVRAM。NVRAM 間で startup-config をコピーできます。
obfl:	オンボード障害ロギング（OBFL）ファイル用のファイル システム。
system:	実行コンフィギュレーションを含む、システム メモリ用のファイル システム。
tar:	アーカイブ ファイル システム。
tmpsys:	一時システム ファイルのファイル システム。
usbflash0:	Universal Serial Bus（USB）フラッシュ ドライブのファイル システム。 （注） USB フラッシュ ドライブのファイル システムは、USB ドライブUSBポートに装着されている場合にのみ表示されます。

上の表に記載されていないファイルシステムがある場合は、**?**ヘルプオプションを使用します。

USB アクセスを有効または無効にするためのオプション

USB フラッシュドライブは、イメージ、コンフィギュレーション ファイル、その他のファイルを保存するたの安価で簡単に使えるストレージを提供します。

Note：IR1101 は、USB フラッシュドライブの ext2 および vfat ファイルシステムをサポートしています。

IR1101 は、USB フラッシュドライブのホットプラグ/アンプラグをサポートしています。USB フラッシュドライブにアクセスするには、デバイスをルータの USB インターフェイスに挿入します。USB が認識されると、コンソールにアラートメッセージが表示されます。

```
Aug  1 11:08:53.198 PDT: %IOSD_INFRA-6-IFS_DEVICE_OIR: Device usbflash0 added
```

このメッセージが表示されたら、USB フラッシュドライブにアクセスできます。ユーザは、**dir usbflash0:** コマンドを使用して USB コンテンツにアクセスできます。

```
Device#dir usbflash0:
Directory of usbflash0:/
    5  drwx              512  Aug 23 2019 10:42:18 -07:00  System Volume Information
    6  -rwx               35  Aug 27 2019 17:40:38 -07:00  test.txt
206472192 bytes total (206470144 bytes free)
Device#
```

copy コマンドを使用して、USB フラッシュドライブとの間で内容をコピーできます。コピーが完了すると、コピーされたバイト数を示すログメッセージが表示されます。

```
Device#copy flash:test.txt usbflash0:
Destination filename [test.txt]? <Enter>
Copy in progress...C
35 bytes copied in 0.020 secs (1750 bytes/sec)
Device#
```

USB フラッシュドライブのホットプラグ/アンプラグはサポートされていますが、この機能にはセキュリティの脆弱性が伴います。ユーザが機密情報を USB フラッシュドライブにコピーできないようにするために、USB の有効化/無効化機能が追加されました。

デフォルトでは、USB フラッシュドライブは有効になっています。ユーザが USB を無効にする場合は、disable コマンドを使用します。

```
Device# config terminal
Device(config)#platform usb disable

Device(config)#end
```

USB フラッシュドライブを無効にするとファイルシステムはデバイスに表示されず、USB を挿入しても syslog メッセージは表示されません。ユーザは USB の内容にアクセスできません。

次に例を示します。

```
Device#dir usbflash0:
dir usbflash0:
    ^
```

```
% Invalid input detected at '^' marker.
Device#
```

disable コマンドで「**no**」を発行すると、USB が有効になります。

```
Device#config terminal

Device(config)#no platform usb disable
Device(config)#end
```

USB のステータスは、次のコマンドで表示できます。

```
Device#show platform usb status
USB enabled
Device#
```

USB ポートは潜在的なセキュリティリスクと見なされる可能性があります。USB ポートを無効にするには、次の手順を実行します。

```
Configure terminal
platform usb disable
exit

show platform usb
```

自動生成されるファイル ディレクトリおよびファイル

ここでは、作成可能な自動生成ファイルとディレクトリについて、およびこれらのディレクトリ内のファイルを管理する方法について説明します。

表 *12:* 自動生成されるファイル

ファイルまたはディレクトリ	説明
crashinfo ファイル	crashinfo ファイルが bootflash: ファイルシステムに保存されることがあります。 これらのファイルにはクラッシュに関する説明情報が含まれており、調整やトラブルシューティングに役立ちます。ただし、これらのファイルはルータ動作には使用されないため、消去してもルータの機能には影響がありません。
core ディレクトリ	.core ファイルのストレージ領域 このディレクトリは消去されると、ブートアップ時に自動的に再生成されます。このディレクトリ内の .core ファイルは、ルータ機能に影響を及ぼさずに消去することはできますが、ディレクトリ自体は消去しないでください。

ファイルまたはディレクトリ	説明
managed ディレクトリ	システム チェックが実行されると、ブートアップ時にこのディレクトリが作成されます。このディレクトリが表示されることは完全に正常な状態であり、ルータに問題が発生したわけではありません。
tracelogs ディレクトリ	trace ファイルのストレージ領域 trace ファイルはトラブルシューティングに役立ちます。たとえば Cisco IOS プロセスに障害が発生した場合、ユーザやトラブルシューティング担当者は診断モードを使って trace ファイルにアクセスし、Cisco IOS 障害に関連する情報を収集できます。 ただし、trace ファイルはルータ動作には使用されないため、消去してもルータのパフォーマンスには影響がありません。

自動生成されるディレクトリに関する重要事項

自動生成されるディレクトリに関する重要な情報は次のとおりです。

- Cisco カスタマー サポートからの指示がない限り、bootflash: ディレクトリに自動生成されたファイルの削除、名前変更、移動、またはその他の変更を行わないでください。

（注） bootflash: に自動生成されたファイルを変更すると、システム パフォーマンスに予期せぬ結果をもたらす場合があります。

- core および tracelogs ディレクトリ内の Crashinfo ファイルとファイルは削除できます。

フラッシュ ストレージ

サブパッケージは、フラッシュなどのローカル メディア ストレージにインストールされます。フラッシュ ストレージの場合は **dir bootflash:** コマンドを使用するとファイル名がリストされます。

（注） ルータが正常に動作するためにはフラッシュ ストレージが必要です。

LED インジケータ

ルータの LED の詳細については、『Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide』の「Product Overview」の項の「LED Indicators」を参照してください。

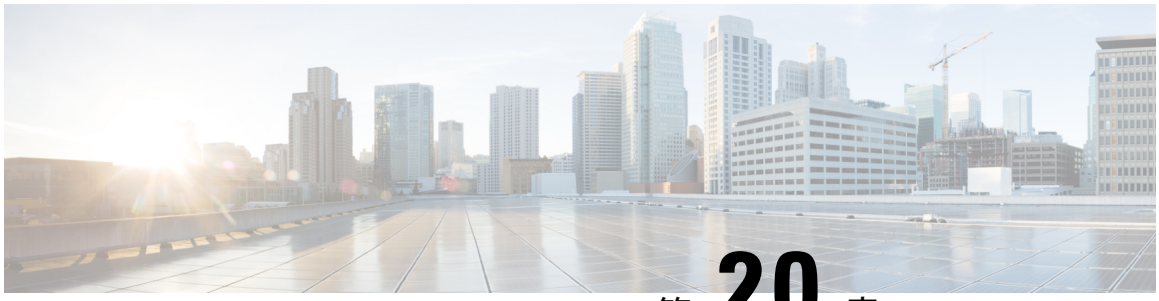
システムの LED ステータス、アラームおよびインターフェイス ポートを監視するため、IOS モードでは show LED コマンド ラインがサポートされています。

```
Router# show LED
SYSTEM LED : Green

Custom LED : Off

VPN LED : Off

ALARM LED : Off

GigabitEthernet0/0/0 LED : Off
FastEthernet0/0/1 LED : Off
FastEthernet0/0/2 LED : Off
FastEthernet0/0/3 LED : Off
FastEthernet0/0/4 LED : Off
GigabitEthernet0/0/5 LED : On

EM Module digital I/O 1 LED : Off
EM Module digital I/O 2 LED : Off
EM Module digital I/O 3 LED : Off
EM Module digital I/O 4 LED : Off

*System LTE Pluggable*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On

*EM Module LTE Pluggable*
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Off
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : On
Router#
```

関連資料

ソフトウェア ライセンスの詳細については、「スマートライセンス」の章を参照してください。

機能ライセンスの取得とインストールの詳細については、「Configuring the Cisco IOS Software Activation Feature」を参照してください。



第 20 章

Cisco Network Plug and Play エージェント

この章は、次の項で構成されています。

Cisco Network Plug and Play エージェントの前提条件

- Cisco Network Plug and Play（PnP）の展開方法は、お客様が必要とする検出プロセスのタイプによって異なります。
- PnP を起動する前に、DHCP サーバ検出プロセスか、またはドメインネームサーバ（DNS）検出プロセスのいずれかの検出メカニズムを展開します。
- PnP を展開する前に DHCP サーバまたは DNS サーバを設定します。
- PnP サーバが PnP エージェントと通信できることを確認します。
- Cisco Network PnP エージェント が PnP サーバと接続していることを確認します。Cisco Network PnP エージェントはサーバに ping できる必要があります。
- PnP エージェントは、どの要求についてもユーザ クレデンシャルを送信するよう PnP サーバに求めます。Cisco では、HTTP Secure（HTTPS）プロトコルの使用を推奨しています。

（注）

- このガイドでは、Cisco Network Plug and Play と PnP という用語は区別なく使用されており、すべて同じ意味です。
- このガイドでは、PnP エージェント、エージェント、および展開エージェントという用語は区別なく使用されており、すべて同じ意味です。
- このガイドでは、PnP サーバ、サーバ、および展開サーバという用語は区別なく使用されており、すべて同じ意味です。

Cisco Network Plug and Play エージェントの制約事項

- Cisco Network Plug and Play（PnP）エージェントは、サーバとの HTTP と HTTPS トランスポートベースの通信を促進します。
- 暗号化対応イメージがサポートされていないプラットフォームでは、HTTPS を使用することはできません（また、暗号化対応のイメージが使用されている場合も、セキュアソケットレイヤ（SSL）プロトコルや Transport Layer Security（TLS）プロトコルを使用しません）。
- 非 VLAN 1 設定 - デフォルトでは、Cisco Network Plug and Play は、VLAN 1 を使用してデバイスをサポートします。1 以外の VLAN を使用するには、隣接するアップストリームデバイスでサポート対象のリリースが実行されていなければなりません。また、そのアップストリームデバイスに **pnp startup-vlan x** グローバル CLI コマンドを設定して、以降の Plug and Play デバイスにこの CLI をプッシュする必要があります。隣接するアップストリームデバイスでこのコマンドを実行した場合、そのアップストリーム デバイスでは VLAN メンバーシップの変更は行われません。ただし、以降の Plug and Play デバイス上のすべてのアクティブ インターフェイスは、指定された VLAN に変更されます。このガイドラインはルータとスイッチの両方に該当します。

（注）

PNP プロセス中にファームウェア アップグレードを実行するときは、ルータ上の古いイメージを削除して、間違ったイメージがロードされないようにすることをお勧めします。

詳細については、CSCwd68868 を参照してください。

Cisco Network Plug and Play エージェントに関する情報

Cisco Network Plug and Play 展開ソリューション

Cisco Network PnP エージェントは、Cisco Network Plug and Play ソリューションに含まれています。シスコ主導の Network Plug and Play（PnP）展開ソリューションではリダイレクトの概念がサポートされており、PnP エージェント、PnP サーバ、およびその他のコンポーネントが含まれています。シスコのデバイスの簡素化された展開プロセスは、運用タスク関連の次の展開を自動化します。

- デバイスの初期ネットワーク接続を確立する
- デバイス設定を配信する
- ソフトウェアおよびファームウェアのイメージを配信する
- ライセンスを配信する
- 導入スクリプト ファイルを配信する
- ローカル クレデンシャルをプロビジョニングする
- 導入関連のイベントについて他の管理システムに通知する

簡素化された展開により、コストと複雑さが軽減され、展開の速度とセキュリティが向上します。

Cisco Network Plug and Play（PnP）エージェントは、Cisco IOS または IOS-XE デバイスで実行されているソフトウェアアプリケーションです。PnP エージェントと PnP 展開サーバは、労力のかからない展開サービスを提供します。デバイスに最初に電源を投入すると、PnP エージェントプロセスがデバイスコンソールにスタートアップ コンフィギュレーションやユーザ入力なしで起動し、PnP サーバのアドレスを検出しようとします。PnP エージェントは DHCP、ドメインネームシステム（DNS）他の方式を使用して、PnP サーバの目的の IP アドレスを取得します。PnP エージェントが IP アドレスを正常に取得すると、サーバとの長期間の双方向レイヤ 3 接続を開始し、サーバからのメッセージを待ちます。PnP サーバアプリケーションは、デバイスで実行される情報とサービスを要求するメッセージをエージェントに送信します。

PnP エージェントは、既存のソリューションを統合エージェントに統合し、現在のソリューションを強化する機能を追加します。PnP エージェントの主な目的は次のとおりです。

- すべての展開シナリオに一貫した Day 1 展開ソリューションを提供する。
- 既存のソリューションを改善するための新機能を追加する。
- Day 2 の管理フレームワークを、主に設定およびイメージのアップグレードとの関連で提供する。

Cisco Network Plug and Play の機能

次に、Cisco Network Plug and Play エージェントが提供する一部の機能を示します。

- Day 0 ブートストラップ：設定、イメージ、ライセンス、およびその他のファイル
- Day 2 管理：Simple Network Management Protocol（SNMP）と syslog メッセージの設定およびイメージのアップグレードと継続的なモニタリング
- オープン通信プロトコル — 顧客およびパートナーがアプリケーションを作成することが可能
- サーバとエージェント間の HTTP を介した XML ベースのペイロード。
- セキュリティ：管理アプリとエージェント間の認証と暗号化された通信チャネル
- ファイアウォールとネットワークアドレス変換（NAT）の背後にあるデバイスの展開と管理
- 1 対 1 および 1 対多の通信サポート
- ポリシー ベースの導入サポート（デバイスの製品 ID またはロケーション）
- 一意 ID（一意のデバイス ID（UDI）または MAC）に基づく導入
- Cisco のさまざまなプラットフォームを通じての統一ソリューション（IOS Classic を含む）
- さまざまな導入シナリオとユース ケースのサポート
- 可能ならゼロタッチ、必要ならロータッチ

Cisco Network Plug and Play エージェントのサービスと機能

Cisco Network Plug and Play エージェントのサービスと機能は次のとおりです。

1. Backoff
2. CLI の実行
3. 設定のアップグレード
4. デバイス情報
5. ファイル転送
6. イメージのインストール
7. ライセンスのインストール
8. PnP タギング
9. スクリプトの実行
10. トポロジ情報

（注） PnP サーバは、PnP エージェントによるイメージのインストールと設定のアップグレードサービス要求で使用されるオプションのチェックサムタグを提供します。チェックサムが要求に含まれている場合、イメージのインストールプロセスはそのチェックサムを実行中の現在のイメージのチェックサムと比較します。

チェックサムが同じである場合、インストールまたはアップグレードされるイメージは、デバイスで実行されている現在のイメージと同じです。このシナリオでは、イメージのインストールプロセスは他の操作を実行しません。

チェックサムが同じでない場合、新しいイメージがローカルファイルシステムにコピーされ、チェックサムが再度計算されて、要求で指定されたチェックサムと比較されます。同じ場合は、新しいイメージのインストールまたはデバイスの新しいイメージへのアップグレードが続行されます。チェックサムが異なる場合、プロセスはエラーで終了します。

Backoff

PnP プロトコル（HTTP トランスポートを使用）をサポートする Cisco IOS デバイスでは、PnP エージェントが PnP サーバに継続的に作業要求を送信する必要があります。PnP サーバに、PnP エージェントが実行するスケジュール済みまたは未処理の PnP サービスがない場合は、連続的な no operation 作業要求によってネットワーク帯域幅とデバイスリソースの両方が使い果たされます。この PnP バックオフサービスにより、PnP サーバは PnP エージェントに指定された時間だけ休止し、後でコールバックするように通知できます。

CLI の実行

Cisco IOS は、EXEC モードとグローバル コンフィギュレーション モードの 2 つのコマンド実行モードをサポートしています。EXEC コマンドのほとんどは、**show** コマンド（現在のコンフィギュレーション ステータスを表示）、**clear** コマンド（カウンタまたはインターフェイスを消去）などのように、一回限りのコマンドです。EXEC コマンドは、デバイスをリブートするときには保存されません。コンフィギュレーションモードでは、ユーザが実行コンフィギュレーションを変更できます。設定を保存すると、これらのコマンドはデバイスの再起動後も保存されます。

（注） **show** コマンドの要求と応答の詳細、およびすべての PnP 設定コマンドについては、『*Cisco Network Plug and Play Agent Command Reference*』を参照してください。

設定のアップグレード

シスコのデバイスで実行する可能性がある設定のアップグレードは 2 種類あります。1 つはスタートアップ コンフィギュレーションへの新しいコンフィギュレーション ファイルのコピー、もう 1 つは実行コンフィギュレーションへの新しいコンフィギュレーション ファイルのコピーです。

スタートアップ設定への新しい設定ファイルのコピー：新しいコ設定ファイルは **copy** コマンドを使用してファイルサーバからデバイスにコピーされ、ファイルの有効性を確認するためにファイルチェックが実行されます。ファイルが有効な場合、そのファイルがスタートアップ設定にコピーされます。使用可能なディスク領域が十分にある場合は、以前の設定ファイルのバックアップが実行されます。デバイスを再度リロードすると、新しい設定が表示されます。

実行コンフィギュレーションへの新しいコンフィギュレーションファイルのコピー：新しいコンフィギュレーション ファイルは、**copy** コマンドまたは **configure replace** コマンドを使用してファイルサーバからデバイスにコピーされます。ロールバックが効率的に実行されると、コンフィギュレーションファイルの置換とロールバックによってシステムが不安定な状態のままになることがあります。したがって、ファイルをコピーして設定をアップグレードすることをお勧めします。

デバイス情報

PnP エージェントは、要求に応じてデバイスインベントリとその他の重要な情報を PnP サーバに抽出する機能を提供します。次の 5 種類のデバイスプロファイル要求がサポートされています。

1. all：固有のデバイス識別子（UDI）、イメージ、ハードウェア、およびファイルシステムのインベントリデータを含む完全なインベントリ情報を返します。
2. filesystem：ファイルシステムの名前とタイプ、ローカルサイズ（バイト単位）、空きサイズ（バイト単位）、読み取りフラグ、書き込みフラグなど、ファイルシステムのインベントリ情報を返します。
3. hardware：ホスト名、ベンダー文字列、プラットフォーム名、プロセッサタイプ、ハードウェアリビジョン、メインメモリサイズ、I/O メモリサイズ、ボード ID、ボードリワーク ID、プロセッサリビジョン、ミッドプレーンリビジョンおよび場所など、ハードウェアインベントリ情報を返します。
4. image：バージョン文字列、イメージ名、ブート変数、rommon への復帰理由、ブートローダ変数、コンフィギュレーション レジスタ、次回ブート時のコンフィギュレーション レジスタ、およびコンフィギュレーション変数など、イメージインベントリ情報を返します。バージョン文字列、イメージ名、ブート変数、rommon への復帰理由、ブートローダ変数、コンフィギュレーション レジスタ、次回ブート時のコンフィギュレーション レジスタ、およびコンフィギュレーション変数など、
5. UDI：デバイス UDI を返します。

ファイル転送

PnP ファイルサーバは、ネットワーク内の展開デバイスによってコピーできるファイルをホストします。ファイルサーバは、ファイルをホストする専用サーバ、または PnP サーバをホストするデバイスの一部にすることができます。PnP エージェントは、標準のファイル転送プロトコルを使用して、リモートファイルサーバからデバイスにファイルをコピーします。デバイスが暗号化イメージを実行している場合は、SFTP、SCP、HTTPS などのセキュアなファイル転

送プロトコルがサポートされます。非暗号化イメージを実行するデバイスの場合、PnP エージェントは FTP、TFTP、HTTP などのセキュアでないコピープロトコルをサポートします。

イメージのインストール

イメージインストールサービスを使用すると、PnP 対応デバイスが PnP サーバから要求を受信した時点でイメージのアップグレードを実行できます。

スタンドアロン デバイス

スタンドアロンデバイス上の PnP エージェントが PnP サーバから要求を受信すると、エージェントは XML ペイロードを解析し、その要求をイメージアップグレード要求として識別します。次に、エージェントは ImageInstall プロセスを作成します。このプロセスは、スタンドアロンイメージ インストール要求として識別されます。PnP エージェントは、ImageInstall サービスによって定義されたデータ構造を入力し、それを ImageInstall サービスに渡します。

その後、イメージ インストール サービスは次の操作を実行して、新しいイメージをデバイスに正常にロードします。

1. ファイルサーバからローカルディスクにイメージをコピーします（ファイルサーバ情報は、要求で PnP サーバによって提供されます）。
2. **boot system** コマンドを実行して、次回のリロード時に新しいイメージをロードするようにデバイスを設定します。
3. デバイスをリロードし、PnP サーバにメッセージを送信します。

PnP タギング

Cisco IOS は、すべてのシスコのデバイスをより適切にグループ化および追跡するために、デバイスにタグを割り当てる機能を提供します。PnP エージェントは、デバイスでタグ情報を設定し、Cisco Discovery Protocol（CDP）を使用してネットワーク内でタグ情報を伝達するための XML サービスを提供します。このサービスの目的は、PnP エージェントがタグ情報を認識し、要求に応じてこの情報を PnP サーバに渡すことです。

トポロジ情報

デフォルトでは、ネットワーク上のすべてのシスコのデバイスが Cisco Discovery Protocol（CDP）を実行します。ネットワーク内のデバイスは、CDP を介して直接のネイバーを検出し、プロトコルを介して学習または取得した属性をデータベースに入力します。このネイバー情報はデータベースに保存され、デバイスが PNP サーバに対してオンデマンドで使用できます。一般的なネイバー情報には、ネイバーデバイス ID、ソフトウェアバージョン、ハードウェア プラットフォーム、インターフェイス IP、および CDP メッセージが送受信されるポートが含まれます。

ソフトウェア メンテナンス アップグレード

ソフトウェア メンテナンス アップグレード（SMU）は特定の障害の修正やリリース済みのイメージに対するセキュリティの解決策を含むパッケージです。SMU は、直近の問題に対処するために作成され、新しい機能は含まれていません。SMU はルータ動作に大きく影響を及ぼ

すことはありません。SMU のバージョンは、アップグレードするパッケージのメジャー、マイナー、およびメンテナンス バージョンに同期されます。

ソフトウェア メンテナンス アップ グレード パッケージをインストールし、アクティブ化するには、次の手順を実行します。

ステップ 1 **install add** <*filename*> コマンドを使用してパッケージ ソフトウェア ファイルを解凍し、それを起動デバイス（通常は disk0）にコピーします。ファイルがリモートソースにある場合は、tftp/ftp オプションを使用してファイルをデバイスにコピーします。

ファイルがデバイスにコピーされると、パッケージ内の情報を使用して、対象カードとの互換性と、他のアクティブなソフトウェアとの互換性が確認されます。パッケージの互換性とアプリケーション プログラム インターフェイス（API）の互換性が確認された場合に限り、実際のアクティブ化が実行されます。

ステップ 2 パッケージをアクティブ化するには、**install activate** <*filename*> コマンドを使用します。アクティブ化操作により互換性チェックが実行され、ソフトウェア メンテナンス アップグレード パッケージがインストールされます。リロード ソフトウェア メンテナンス アップグレードの場合は、自動的にリロードが開始されます。

ステップ 3 **install commit** コマンドを使用して変更をコミットします。

ステップ 4 パッケージを非アクティブ化するには、**install deactivate** <*filename*> コマンドを使用します。

ステップ 5 以前のパッケージセットの方が現在アクティブなパッケージセットよりも適切であることがわかった場合は、**install rollback to committed** コマンドを使用して、以前アクティブだったパッケージ セットを再びアクティブにできます。

ステップ 6 インストールされているバージョンを削除するには、**install remove** <*filename*> コマンドを使用します。

次に、ソフトウェア メンテナンス アップグレード パッケージをデバイスにインストールし、削除する例を示します。

```
install add <filename>
install activate <filename>
install commit
install rollback to committed
install remove <filename>
```

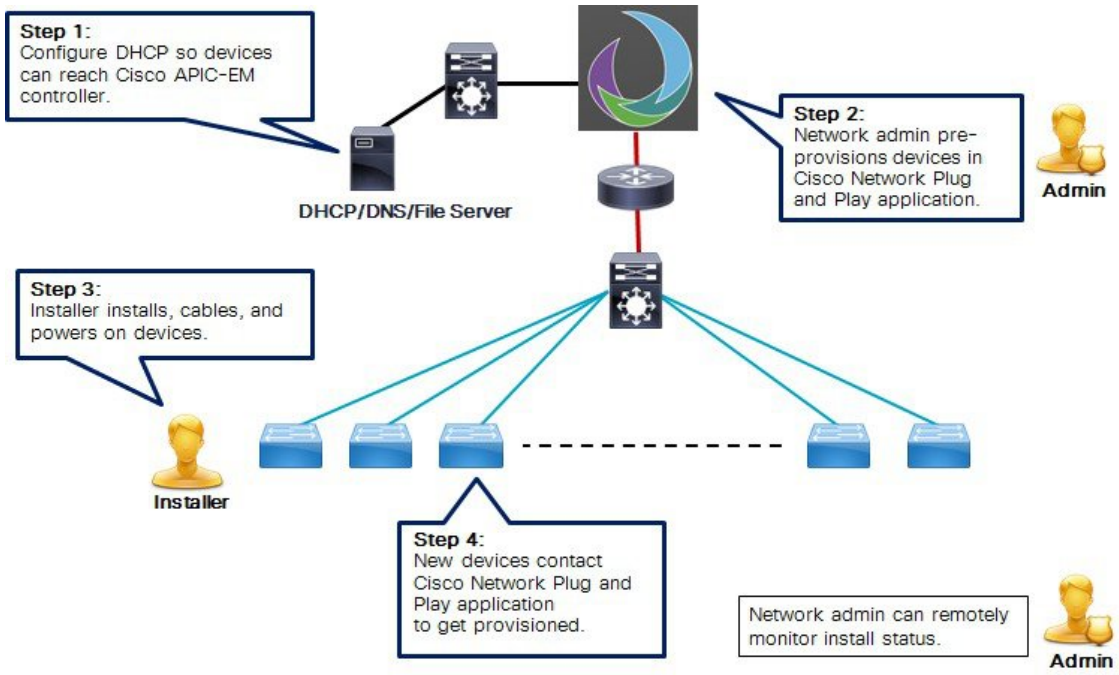
Cisco Network Plug and Play エージェント

Cisco Network Plug and Play エージェントは、シスコのネットワーク デバイスのうち、簡素化された展開アーキテクチャをサポートするものすべてに含まれている組み込みソフトウェア コンポーネントです。PnP エージェントが認識し、対話する対象は PnP サーバのみです。PnP エージェントはまず、通信可能な PnP サーバの検出を試みます。サーバが検出されて接続が確立されると、エージェントはサーバと通信し、設定、イメージ、ライセンス、ファイル更新などの展開関連のアクティビティを実行します。また、アウトオブバウンドの設定変更やインターフェイス上の新しいデバイス接続などの対象のすべての展開関連イベントをサーバに通知します。

Cisco Network Plug and Play サーバ

Cisco Network Plug and Play サーバは、導入するデバイスの展開情報（イメージ、設定、ファイル、およびライセンス）の管理や配布のロジックを符号化する中央サーバです。このサーバは、特定の展開プロトコルを使用することで、簡素化された展開プロセスをサポートするデバイス上のエージェントと通信します。

図 *48 :* 簡素化された展開サーバ



PnP サーバは、スマートフォンと PC の導入アプリケーションなどのプロキシサーバ、Neighbor Assisted Provisioning Protocol（NAPP）として動作する他の PnP エージェント、および VPN ゲートウェイのようなその他のタイプのプロキシ導入サーバと通信します。

PnP サーバは、エージェントを別の展開サーバにリダイレクトできます。リダイレクトの一般的な例は PnP サーバによるリダイレクトで、ブートストラップ設定を NAPP サーバを介して送信した後に直接通信するデバイスをリダイレクトします。PnP サーバは企業がホストできます。このソリューションでは、シスコが提供するクラウドベースの展開サービスが可能です。この場合、デバイスはシスコのクラウドベースの展開サービスを検出して通信し、初期導入を実行します。その後、お客様の展開サーバにそのデバイスをリダイレクトできます。

デバイスとの通信に加え、サーバは認証、承認、アカウンティング（AAA）システム、プロビジョニングシステム、その他の管理アプリケーションなどのさまざまな外部システムと連動します。

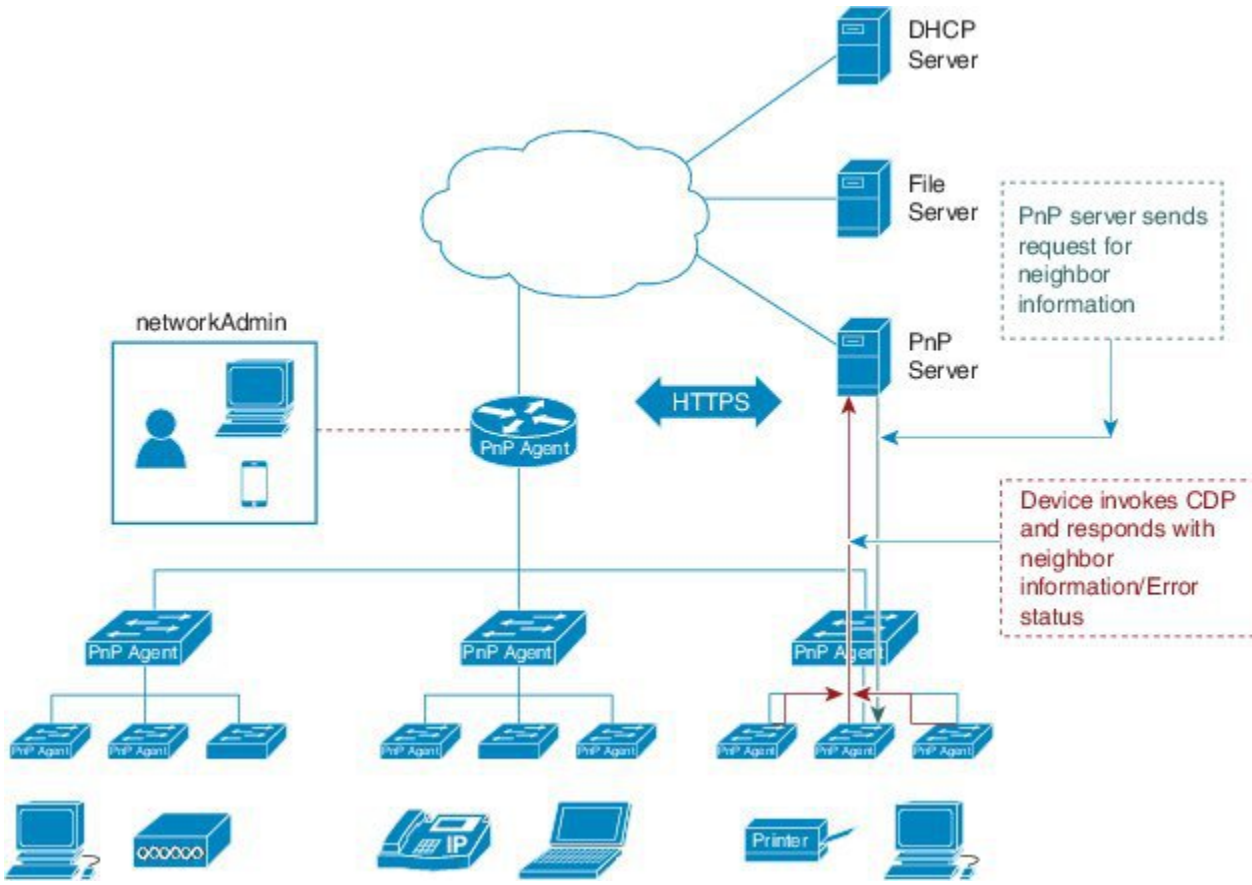
Cisco Network Plug and Play エージェントの展開

次に、シスコのデバイスでの Cisco Network Plug and Play エージェントの展開手順を示します。

1. PnP エージェントを備えているシスコのデバイスは PnP サーバに問い合わせタスクを要求します。つまり、PnPエージェントは作業の要求とともに、一意のデバイス識別子（UDI）を送信します。
2. デバイスのタスクがある場合は、PnP サーバは作業要求を送信します。たとえば、イメージのインストール、設定のアップグレードなどです。
3. PnP エージェントが作業要求を受信すると、タスクを実行し、タスクのステータス、成功かエラーかと要求された対応する情報に関する応答を PnP サーバに返します。

Cisco Network Plug and Play エージェントのネットワークトポロジ

図 *49 : Cisco Network Plug and Play* エージェントの展開のネットワークトポロジ



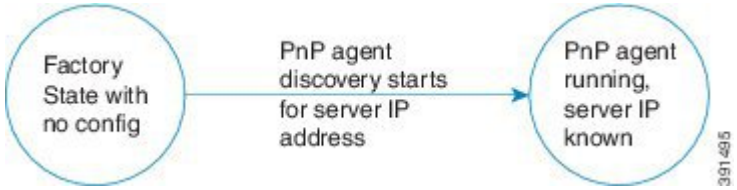
Cisco Network Plug and Play エージェントの初期化

Cisco Network Plug and Play エージェントソフトウェアは現在すべての Cisco IOS XE プラットフォームで使用でき、デフォルトで有効になっています。PnPエージェントは次の方法でデバイス上で開始できます。

スタートアップ コンフィギュレーションなし

新しいシスコのデバイスは、デバイスのNVRAMの中にスタートアップ コンフィギュレーションファイルのない状態でお客様に出荷されます。新しいデバイスがネットワークに接続され、電源が投入された時点でスタートアップ コンフィギュレーションとユーザ入力ファイルがデバイス上にない場合は、Cisco Network Plug and Play エージェントが自動的に起動され、PnP サーバの IP アドレスを検出します。

図 *50* : スタートアップ コンフィギュレーションなしの *PnP* トリガーの状態図



Open Plug-n-Play エージェントの CLI 設定

ネットワーク管理者は CLI 設定を使用すると Plug-n-Play（PnP）エージェントプロセスをいつでも開始できます。CLI を介して PnP プロファイルを設定することによって、ネットワーク管理者はデバイス上で PnP エージェントを開始したり停止したりできます。CLI を使用して PnP プロファイルを設定すると、デバイスはPnPエージェントプロセスを開始し、次にそのプロセスが PnP プロファイル内の IP アドレスを使用して PnP サーバとの接続を開始します。

図 *51* : *CLI* 設定 *PnP* プロファイルによる *PnP* トリガーの状態図

Cisco Network Plug and Play エージェントの展開ソリューション

この項では、デバイスの導入と管理のために PnP サーバに公開される Cisco Network Plug and Play エージェントの機能について説明します。PnP エージェントの展開ソリューションは、エージェント、デバイス、エージェント、およびサーバ間の通信、ならびにPnPエージェントサービスによって開始される検出プロセスで構成されています。PnP ソリューションについては、次の項で詳しく説明します。

Cisco Network Plug and Play エージェント検出プロセス

デバイスが起動すると、NVRAMのスタートアップ コンフィギュレーションのいずれかがない場合は PnP 検出エージェントによって PnP サーバの IP アドレスが取得されます。PnP サーバの IP アドレスを取得するため、PnPエージェントは次の検出機能のうちの 1 つを実行します。

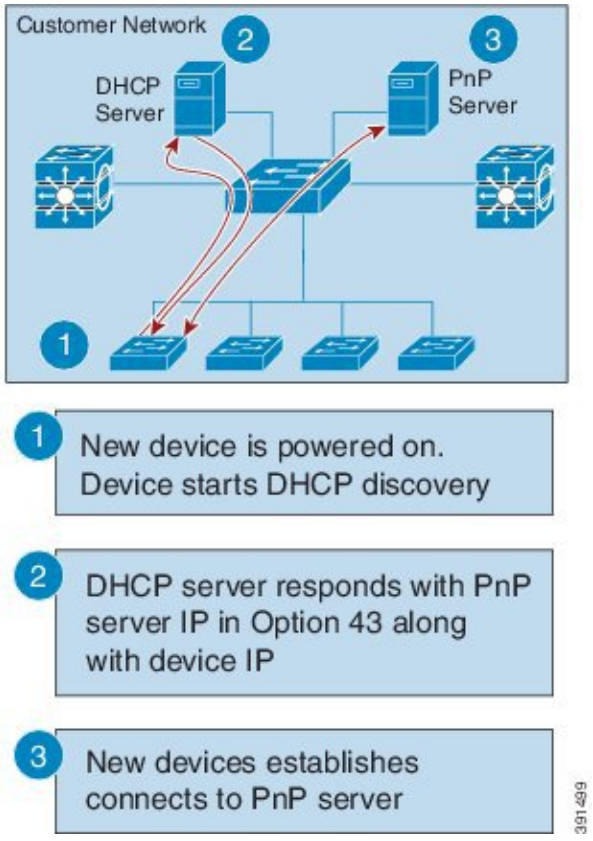
1. DHCP サーバによる PnP の検出
2. DHCP スヌーピングによる PnP の検出

3. DNS ルックアップによる PnP の検出
4. レイヤ 2 およびレイヤ 3 デバイスの PnP プロキシ
5. PnP 導入アプリケーション

DHCP サーバを介した Cisco Network Plug and Play 検出

NVRAM にスタートアップ コンフィギュレーションのないデバイスは、Cisco Network Plug and Play エージェントを起動し、DHCP サーバからデバイスに必要な IPv4 設定を取得する DHCP 検出プロセスを開始します。DHCP サーバは、文字列「cisco pnp」のあるデバイスからオプション 60 を受信した時点でベンダー固有のオプション 43 を使用して追加の情報を挿入し、PnP サーバの IPv4 アドレスまたはホスト名を要求側のデバイスに渡します。デバイスが DHCP 応答を受信すると、PnP エージェントは応答からオプション 43 を抽出して、PnP サーバの IP アドレスまたはホスト名を取得します。PnP エージェントは、PnP サーバと通信するためにこの IPv4 アドレスまたはホスト名を使用します。

図 *52 : PnP* サーバの *DHCP* 検出プロセス



前提条件：

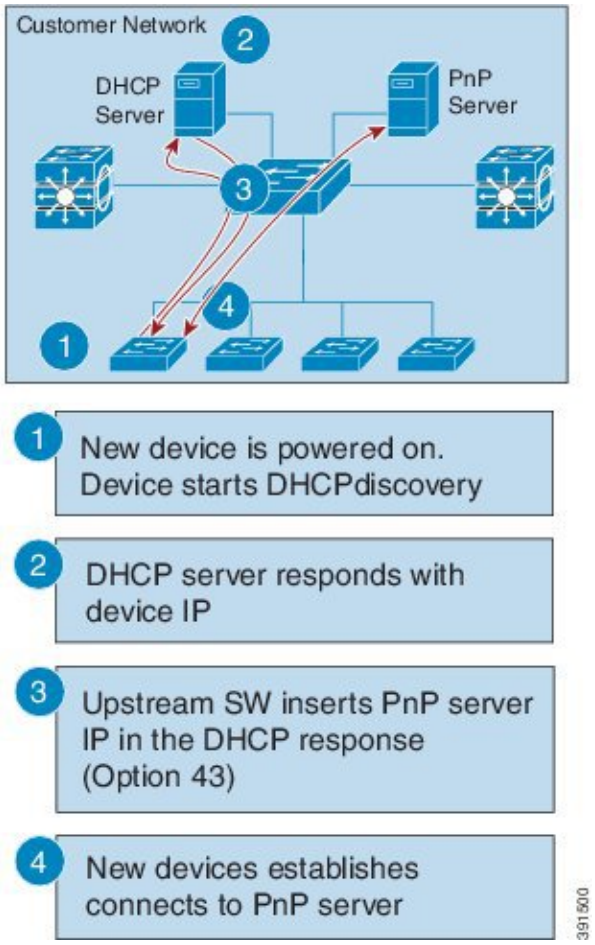
- 新しいデバイスが DHCP サーバに到達できる
- お客様がネットワークデバイスの DHCP サーバを設定する意思がある

DHCP スヌーピングによる Plug-n-Play 検出

ベンダー固有のオプションを挿入するようにサードパーティ製DHCPサーバを設定することができない場合、DHCP 応答にスヌーピングし、PnP サーバの IP アドレスを持つ PnP 固有のオプション 43 を挿入するように、既存の Cisco Open Plug-n-Play（PnP）対応デバイスを設定できます。

オプション 43 を挿入する前に、スヌーピング エージェントにより、DHCP メッセージがネットワーク内のシスコデバイスからのものかどうかが確認されます。DHCP検出プロセスの残りの部分は、前のセクションで説明したものと同じです。

図 *53 : PnP* サーバによる *DHCP* スヌーピング



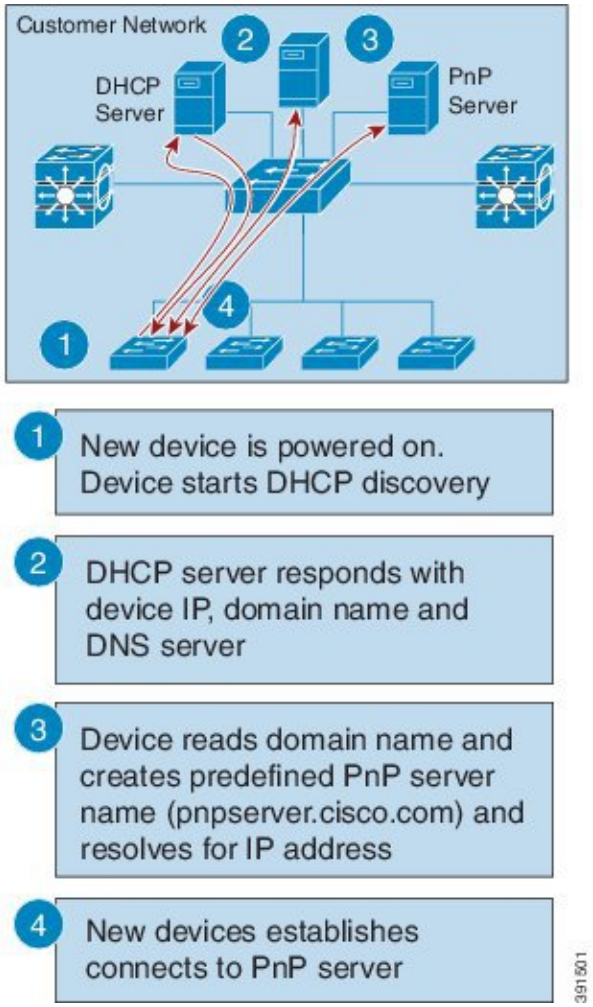
前提条件：

- 新しいデバイスが DHCP サーバに到達できる
- 新しいデバイスが DNS サーバに到達できる
- お客様がネットワークデバイスの DHCP サーバを設定することを希望していない
- DHCP をスヌーピングし、PnP サーバ IP を挿入するようにアップストリームスイッチ（SW）が設定されている

DNS ルックアップによる Cisco Network Plug and Play 検出

DHCP 検出で Cisco Network Plug and Play サーバの IP アドレスが取得できないと、エージェントはドメインネームシステム（DNS）ルックアップ方式にフォールバックします。次に、PnP エージェントはプリセットの展開サーバ名を使用します。エージェントは、DHCP応答から顧客のネットワークのドメイン名を取得し、完全修飾ドメイン名（FQDN）を形成します。次の FQDN は、DHCP応答のプリセットの展開サーバ名とドメイン名情報（*deployment.customer.com*）を使用して PnP エージェントによって構成されます。次に、エージェントは、ローカル ネーム サーバでの検索を実行し、前述の FQDN の IP アドレスの解決を試みます。

図 *54 : deployment.customer.com* の *DNS* ルックアップ



前提条件：

- 新しいデバイスが DHCP サーバに到達できる
- 「pnpserver」という名前でお客様がネットワークに PnP サーバを展開した

レイヤ 3 デバイスとレイヤ 2 デバイス用の Cisco Network Plug and Play プロキシサーバ

このデバイスは、特定のポートで PnP 着信メッセージをリッスンします。PnP デバイスとしての登録を試みるシスコ デバイスは、ネットワークに UDP ブロードキャスト メッセージを 30 分ごとに 10 回送信します。したがって、デバイスが応答を受信しない場合、ブロードキャストは 300 分後に停止します。

図 *55 :* レイヤ *3* デバイスとレイヤ *2* デバイスの *DNS* ルックアップ

プロキシ サーバ プロセスのホスト デバイスが着信ブロードキャストを受信すると、要求中のバージョン フィールドを検証し、バージョンの検証が成功すると、PnP サーバに要求を転送します。また、プロキシ サーバ プロセスは、PnP サーバに要求を転送する前に、着信データグラムにより要求元クライアントの Unique Device Identifier（UDI）をキャッシュに入れます。

プロキシ サーバは PnP サーバからコンフィグレット データグラムを受信すると、UDI キャッシュ内のエントリを使用して、着信データグラムの UDI の検証を実行します。検証が成功すると、プロキシ サーバ プロセスはそのデータグラムを、プロキシ クライアント プロセスがデータグラムを受信するために予約されている特定のポート番号にブロードキャストします。

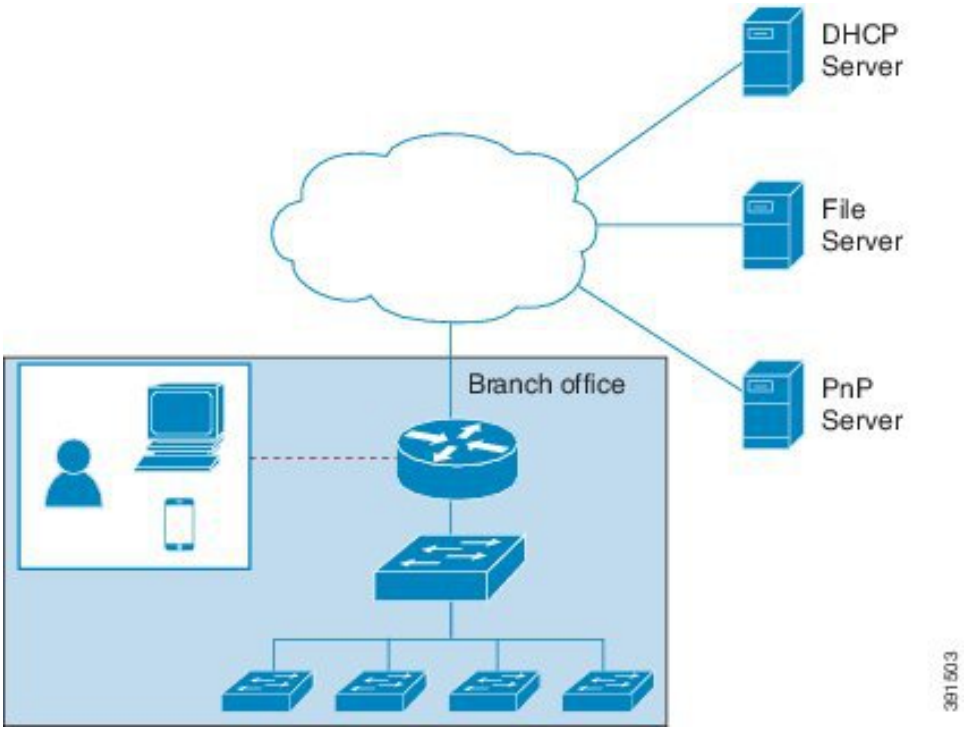
そのデータグラムを受信すると、プロキシクライアントプロセスを実行するデバイスは、ターゲット UDI を得るため着信データグラムを解析します。そのデータグラムのターゲット UDI がデバイスの UDI と一致すると、プロキシ クライアント プロセスは、フレーミング、エラー制御、およびコンフィグレットの設定に進みます。

データグラムのターゲット UDI がデバイスの UDI と一致しない場合、パケットはドロップされます。

Plug-n-Play エージェント展開アプリケーション

また、シスコのデバイスは、PC またはスマートフォンで実行されている展開アプリケーションを使用してネットワーク管理者が手動で設定することができます。PC またはスマートフォンは、USB またはイーサネットケーブルを使用してデバイスに接続できます。

図 *56*：手動で設定された *PnP* エージェント



Plug-n-Play エージェント展開プロトコル

展開はさまざまなトランスポートを介して実行できます。これらのトランスポートには、イーサネットと Transport Layer Security（TLS）を使用した IP が含まれます。レイヤ 2 トランスポートは通常、展開エージェントと、展開アプリケーションなどのプロキシ展開サーバ間、またはプロキシとして機能する展開エージェントとして使用されます。エージェントとサーバ間のトランスポートは、セキュリティのために TLS を使用した IP 接続を介して行われます。プロキシ展開サーバと展開サーバ間のトランスポートも、TLS を使用した IP を介して行われます。

Plug-n-Play エージェント アプリケーション プロトコル

Cisco Open Plug-n-Play（PnP）エージェント アプリケーション プロトコルは、ネットワークデバイスをリモートアプリケーションでモニタおよび制御可能なメカニズムを定義する XML ベースのプロトコルです。PnP エージェントは、シスコのデバイスで実行するソフトウェアモジュールです。PnP サーバは、ネットワークデバイスをリモートで管理するネットワークマネージャとして実行するアプリケーションです。PnP プロトコルの主な機能は次のとおりです。

1. HTTP プロトコルをサポート
2. HTTP の Transport Level Security（TLS）ベースの暗号化をサポート
3. TLS ハンドシェイクに HTTP セキュア（HTTPS）証明書を使用

イーサネットトランスポートによる Plug-n-Play

Cisco Open Plug-n-Play（PnP）エージェントは、次の 2 つのシナリオでイーサネットベースのトランスポートを使用します。

- **PC 上の展開アプリケーションと通信する展開エージェント**：この場合、PC はイーサネットケーブルを使用して展開されるデバイスに接続されます。展開アプリケーションは、イーサネットトランスポートをサポートする展開サーバとしてそれ自体をアドバタイズします。
- **展開エージェントがプロキシ展開サーバとして機能する、すでに展開されているデバイスと通信している場合**：この場合、展開する新しいデバイスには、すでに展開されているデバイスへのイーサネット接続が備わっています。展開されたデバイス上の展開エージェントは検出要求に応答し、新しいデバイスのプロキシ展開サーバとして機能します。

検出が完了すると、展開エージェントはイーサネットを介して展開サーバとのセキュアでない XML ストリームを開始します。このプロトコルは、このために Ethertype（0xXX TBD）を予約します。展開エージェントとサーバは、拡張可能認証プロトコル/トランスポート層セキュリティ（EAP-TLS）を使用して通信を保護し、EAP-TLS セッションの確立を完了します。次に、展開サーバは HTTP セキュア（HTTPS）証明書またはその他のサポートされているメカニズムを使用してデバイスを認証します。

IP を介した Plug-n-Play トランスポート

Cisco Network Plug-n-Play（PnP）エージェントでは、展開エージェントが展開サーバへの TCP 接続を開き、メッセージの XML ストリームを開始します。サーバはこの時点で Transport Layer Security（TLS）の使用を要求できます。エージェントは既存の XML ストリームを閉じ、サー

バへの TLS 接続を開始してから XML ストリームを再起動します。サーバは TLS 接続を介してエージェント認証を要求できます。

Plug-n-Play エージェントのセキュリティ

すべての Cisco Open Plug-n-Play（PnP）デバイスに対するセキュリティは、トランスポートレベルとアプリケーションレベルの両方で提供されます。以降の項では、セキュリティメカニズムについて詳しく説明します。

Plug-n-Play トランスポートレイヤ 3 セキュリティ

非暗号化または非暗号化対応イメージの場合、TLS セキュリティを選択することはできません。代わりとなるもう 1 つの最小セキュリティは、指定した信頼できる PnP サーバへの接続を PnP エージェントがポート 5222 で開始することです。

Plug-n-Play エージェントとサーバ間の認証と承認

Cisco Open Plug-n-Play（PnP）展開エージェントが PnP サーバを検出すると、エージェントは Transport Layer Security（TLS）ハンドシェイクを実行します。サーバに対してそのエージェント自体を認証するために、エージェントは HTTP セキュア（HTTPS）証明書を提示します。PnP サーバの管理者は、特定の展開に受け入れられるデバイス認証メカニズムを設定します。

展開サーバは、エージェントがサーバを認証できるように、展開エージェントに証明書を提示します。エージェントがサーバ証明書を確認できるかどうかに関係なく、エージェントは TLS 後の認証交換で展開サーバを使用します。この交換で、エージェントはサーバにサーバ認証トークンの提示を要求します。この要求に応じて、サーバはシスコから取得した認証トークンを提示します。エージェントは認証トークンの署名を確認します。認証トークンが Unique Device Identifier（UDI）に固有の場合、エージェントはその UDI が認証トークンのリストに存在していることも確認します。この手順の最後に、展開エージェントとサーバ間にセキュアな通信チャネルが確立されます。このセキュアな通信チャネルは、展開情報をエージェントに送信するためにサーバが活用します。

PnP 検出プロセスのセキュリティ方式

このセクションでは、PnP エージェント サーバ通信をさまざまなシナリオで保護するために使用する方法について説明します。セキュリティオプションは、ゼロタッチ PnP サーバ検出時に PnP エージェントによって使用されます。この項では、次のトピックについて取り上げます。

- 自己署名証明書ベースの認証 （202 ページ）
- モバイルデバイスベースのセキュアなインストール （202 ページ）
- CA 署名付き証明書ベースの認証 （203 ページ）
- IPv4 ネットワークを介した DHCP オプションベースの検出 （203 ページ）

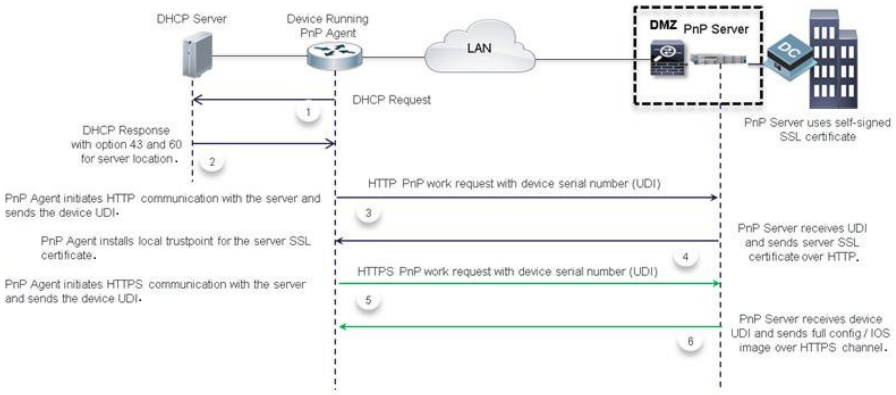
自己署名証明書ベースの認証

PnP サーバには、サーバ側の認証に自己署名 SSL 証明書を使用するオプションがあります。PnP サーバが自己署名証明書を使用する場合、PnP 検出を使用してエージェントからサーバへのセキュアな通信を自動的に開始することはできません。デバイスは通常の PnP 検出メカニズムを通過し、サーバが検出されると、エージェントは HTTP 経由で作業要求を送信します。サーバは PnP 証明書インストールサービスを使用してサーバの自己署名証明書をインストールして HTTPS を介してサーバに自動的に再接続するようにエージェントに指示する必要があります。

ソリューションのセキュリティを確保するには、サーバの非セキュアなポート 80 を使用して、1 回限りの証明書のインストールをデバイスに配信することを推奨します。他のすべてのサービスは、セキュアなポートを介して送信する必要があります。

次の図に、自己署名サーバ SSL 証明書を使用したエンドツーエンドのセキュアな PnP ワークフローを示します。

図 *57*：自己署名証明書を使用した *PnP* の展開

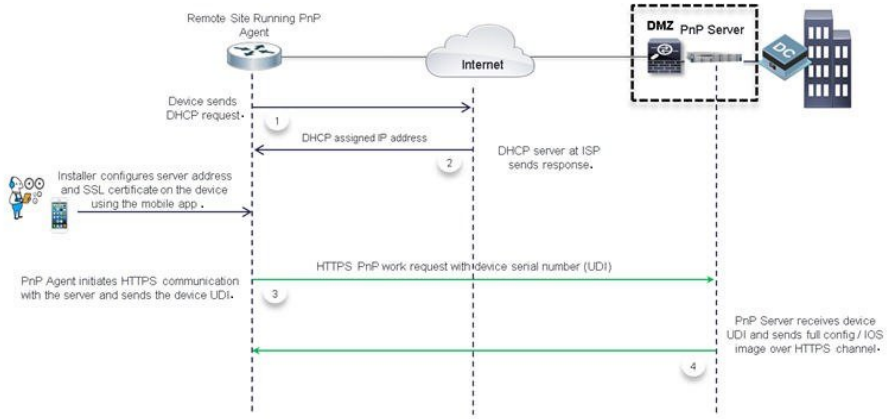


モバイルデバイスベースのセキュアなインストール

このソリューションの一部として、モバイルデバイス用のアプリケーションを使用してデバイスにブートストラップを設定できます。モバイルアプリケーションを使用して、他のブートストラップ設定とともに各デバイスにサーバ証明書を直接インストールし、PnP エージェントがサーバとのセキュアな通信を開始できるようにすることができます。この方法では、サーバは証明書インストール用のセキュアでないポートを開きません。

次の図に、モバイルデバイスでアプリケーションを使用するエンドツーエンドのセキュアな PnP ワークフローを示します。

図 *58* : モバイルアプリケーションによるセキュアな *PnP* 展開



CA 署名付き証明書ベースの認証

シスコでは、署名機関によって署名された証明書を .tar ファイル形式で配布し、シスコの認証局（CA）の署名を使用してバンドルに署名します。この証明書バンドルは、cisco.com でのパブリックダウンロード向けに Cisco infoSec によって提供されます。

このバンドルの証明書は、SSL ハンドシェイク時にサーバ側の検証用 Cisco IOS デバイスにインストールできます。サーバでは、バンドルで使用可能な CA のいずれかによって署名された証明書を使用するものとします。

PnP エージェントは、組み込み PKI 機能を使用して証明書バンドルを検証します。バンドルはシスコの CA によって署名されるため、エージェントはデバイスに証明書をインストールする前に、改ざんされたバンドルを特定できます。エージェントによってバンドルの整合性が確認されると、デバイスに証明書がインストールされます。証明書がデバイスにインストールされると、サーバから追加手順を実行しなくても PnP エージェントがサーバへの HTTPS 接続を開始します。次のメカニズムは PnP エージェントがゼロタッチのセキュアな通信を開始するのに役立ちます。

IPv4 ネットワークを介した DHCP オプションベースの検出

DHCP オプション 43 とオプション 60 は、PnP サーバを検出して接続するために PnP エージェントが使用するベンダー固有の識別子です。複数のベンダーをサポートするために、シスコのデバイスの PnP エージェントは DHCP 検出時にオプション 60 文字列として大文字と小文字を区別して「ciscopnp」を送信します。DHCP サーバは各ネットワークデバイスからの異なるオプション 60 文字列と一致する複数のクラスで設定できます。オプション 60 の文字列が一致すると、DHCP サーバは対応するオプション 43 の文字列をデバイスに送り返します。次に、PnP 展開のオプション 43 を定義するための形式を示します。

*option 43 ascii "5A;K5;B2;I10.30.30.10;J443;**Ttftp://10.30.30.10/ ios.p7b**;Z10.30.30.1*

PnP 文字列のフィールド「T」は、ネットワーク管理者がローカルまたはリモートのファイルサーバでホストできる証明書バンドルの場所を指定するためのオプションを提供します。

指定された場所で証明書バンドルが使用可能な場合、エージェントは次の処理を実行します。

1. ファイルサーバからデバイスにバンドルをダウンロードします。
2. ダウンロードしたバンドルの署名を調べて、正規のシスコの署名があることを確認します。
3. デバイスに証明書をインストールします。

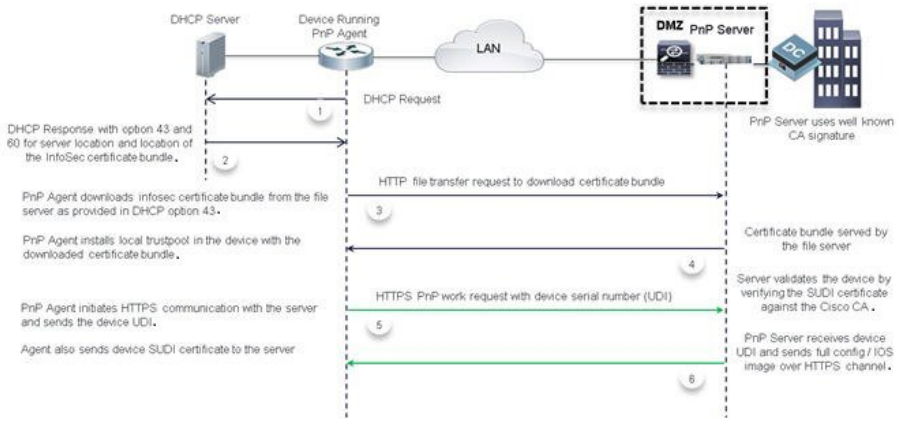
「T」オプションが指定されておらず、トランスポートメカニズムがオプション 43 文字列で HTTPS として指定されている場合、PnP エージェントは同じサーバ（*http://10.30.30.10:443/certificates/default/cert.p7b*）のデフォルトフォルダでシスコの署名付き証明書バンドルを検索します。

証明書がデフォルトの場所にある場合、エージェントは上記の手順を実行して証明書をインストールします。

証明書がインストールされ、サーバ検出が完了すると、エージェントは追加設定なしでサーバとの HTTPS 接続を開始します。HTTPS ハンドシェイク時に、デバイスはバンドルからインストールされた証明書を使用してサーバ証明書を検証します。

次に、CA バンドルベースの証明書を使用した、S エンドツーエンドのセキュアな PnP ワークフローの図を示します。

図 *59 :* トラストプールによるセキュアな *PnP* 展開



このフローは、バンドルで使用可能な既知の署名機関のいずれかによって署名された証明書をサーバが使用している場合にのみ機能します。サーバがバンドルに含まれていない証明書を使用する場合、HTTPS ハンドシェイクは失敗します。トランスポートオプションとして HTTPS を使用してオプション 43 の文字列を指定し、バンドルのダウンロードが失敗した場合、サーバが到達可能であっても、エージェントはセキュアでない通信プロトコルにフォールバックしません。トランスポートオプションが HTTP として有効な証明書バンドルの場所を指すパラメータ「T」を使用して指定されている場合、エージェントは転送オプションHTTP をオーバーライドし、セキュアな通信を確保するために HTTPS に変更します。通常、エージェントは使用可能なオプションから最もセキュアな通信を選択します。

証明書バンドルファイルを見つけるために DHCP オプション 43 で指定されたパスは絶対 URL または相対 URL のいずれかです。相対 URL を指定すると、エージェントはオプション 43 の文字列で指定されているサーバの IP アドレスまたはホスト名を使用して完全な URL を形成し、ファイル転送プロトコルとして HTTP を使用します。

また、証明書をインストールするために、エージェントはデバイスのシステムクロックが更新されていると想定しています。DHCP サーバを最初に設定するため、DHCP サーバで現在時刻を指定することはできません。このようなシナリオでは、IP アドレスまたは URL をオプション 43 の代替パラメータとしてプレフィックス「Z」を付けて指定できます。これにより、デバイスは NTP サーバをポイントできます。エージェントは、デバイスのクロックを NTP サーバと同期し、証明書をインストールします。

IPv6 ネットワークを介した DHCP オプションベースの検出

Cisco Network PnP は、IPv6 DHCP 検出プロセスに DHCP オプション 16 とオプション 17 を使用します。オプション 16 とオプション 17 はベンダー固有の識別子です。これらは、Cisco Network PnP エージェントが Cisco Network PnP サーバを検出して接続するために使用されます。DHCP サーバはベンダー固有のオプション 17 を使用して追加情報を挿入するように設定できます。DHCP サーバが文字列 *cisco pnp* を含むオプション 16 をデバイスから受信し、オプション 17 の文字列と一致する場合、サーバは要求元のデバイスに Cisco PnP サーバの IP アドレスまたはホスト名を渡します。デバイスが DHCPv6 応答を受信すると、Cisco Network PnP エージェントは応答からオプションを抽出し、Cisco PnP サーバの IPv6 アドレスを識別します。Cisco PnP エージェントはこの IPv6 アドレスを使用して Cisco PnP サーバと通信します。証明書を取得してインストールするには、「IPv4 ネットワークを介した DHCP オプションベースの検出」の項で説明したのと同じプロセスを使用します。

次に、ベンダー固有のオプションを使用してプール（DHCPv6-pool）を設定する例を示します。

```
ipv6 dhcp pool dhcpv6-pool
 address prefix 2003::/64 lifetime infinite infinite
 vendor-specific 9
  suboption 16 ascii "ciscopnp"
  suboption 17 ascii "5A1D;K4;B3;IFE80::2E0:81FF:FE2D:3799;J6088"
```

DNS ベースの検出

DNS ベースの検出では、DHCP サーバはカスタマーネットワークのドメイン名を受け取ります。ドメイン名は、*pnpserver.<domain_name>* などの PnP 固有の完全修飾ドメイン名（FQDN）の作成に使用されます。この方法では、カスタマーネットワークはこの URL を有効な PnP サーバの IP アドレスに解決します。証明書の場所を指定するメカニズムがないため、エージェントは HTTPS 接続を開始するサーバ証明書を見つけます。手動での介入は必要ありません。

システムの起動時に、デバイスはドメイン名とともに IP ネットワーク情報を DHCP サーバから取得します。お客様固有のドメイン名を使用して、Cisco PnP エージェントは URL *pnpserver.<domain_name>* を作成し、シスコの署名付き証明書バンドルをサーバのデフォルトフォルダ *<domain_name>/ca/trustpool/cabundle.p7b* で検索します。

指定された場所で証明書バンドルが使用可能な場合、エージェントは次の処理を実行します。

1. ファイルサーバからデバイスにバンドルをダウンロードします。

2. ダウンロードしたバンドルの署名を調べて、正規のシスコの署名があることを確認します。
3. デバイスに証明書をインストールします。

指定した場所で証明書バンドルが使用できない場合、PnPエージェントは事前定義されたURL *pnpcertserver.<domain_name>* を使用してサーバのデフォルトフォルダ *<domain_name>/ca/trustpool/cabundle.p7b* でシスコの署名付き証明書バンドルを検索します。

指定された場所に証明書がある場合、エージェントは証明書をインストールするために上記の手順を実行します。

証明書がインストールされ、サーバの検出が完了すると、設定を追加することなく、エージェントはURL *pnpserver.<domain_name* > でサーバとのHTTPS接続を開始します。HTTPSハンドシェイク時にデバイスはバンドルからインストールされた証明書を使用してサーバ証明書を検証します。

また、証明書をインストールするために、エージェントはデバイスのシステムクロックが更新されていると想定しています。DHCPサーバを最初に設定するため、DHCPサーバで現在時刻を指定することはできません。このようなシナリオでは、エージェントは事前に設定されたURL *pnpntpserver.<domain_name>* を使用します。このURLは証明書をインストールする前にNTPサーバにマッピングしてデバイス上のクロックと同期させる必要があります。

ただし、証明書がどちらのURLにも存在しない場合、Cisco PnPエージェントはフォールバックし、作成したFQDN pnpserver.<domain_name> を使用してサーバへのHTTP接続を確立します。このワークフローでは、エージェントはサーバが証明書インストールサービスを使用して自己署名証明書をインストールし、プロビジョニング手順を開始すると想定しています。

IPv6 ネットワークを介した DNS ベースの検出

IPv6 ネットワークを介した DNS ベースの検出を有効にするには、次の手順を実行します。

ステップ 1 IPv6 オプションを使用して DNS サーバを設定します。Cisco Network PnP DNS 検出を有効にするには、次の例のように DNS サーバを設定します。

```
ip host pnpntpserver.domain.com 2001::1
ip host pnptrustpool.domain.com 2001::2
ip host pnpserver.domain.com   2001::3
```

ステップ 2 DHCPv6 サーバは、DHCP ブートストラッププロセスによって検出されます。次に、DHCP サーバを設定する例を示します。

```
ipv6 unicast routing
ipv6 cef

ipv6 dhcp pool test
dns-server 2001::4
domain-name example.com
```

デバイスは、IPv6 ネットワークを介して DHCPv6 パケットをサーバに送信します。DHCPv6 パケットを受信すると、DNS サーバ情報とドメイン名がそれぞれオプション 23 とオプション 24 としてデバイスに返されます。

ステップ 3 NTP サーバを設定します。次に、NTP サーバを設定する例を示します。

```
ntp master 1
```

（注） 同様に、デバイスの NTP 設定では NTPv4 オプションを使用する必要があります。

ステップ 4 IPv6 ネットワークでトラストプールサーバをホストします。トラストプールは、DHCP オプション T と Z でのみサポートされています。オプション T が設定されている場合は、トラストプール CA バンドルの URL を指定します。オプション Z が設定されている場合は、NTP サーバの IP アドレスを指定します。

（注） Cisco Network PnP エージェントが IPv6 オプションを使用して HTTP 経由でトラストプールバンドルをダウンロードしようとすると、トラストプールサーバは IPv6 ネットワーク経由の HTTP をサポートする必要があります。また、トラストプールを設定する前にクロックを同期する必要があります。

ステップ 5 IPv6 ネットワークで Cisco Network PnP サーバをホストします。

IPv4 および IPv6 ネットワークを介した Cisco Cloud リダイレクト

Cisco Cloud リダイレクトサービスは、Cisco Network PnP ゼロタッチ検出をサポートしています。IPv4 および IPv6 ベースの Cisco Cloud 検出でサポートされています。

（注） 一部の Cisco PnP デバイスには、デバイスにルート証明書が組み込まれている場合があります。これらのデバイスは、最初から HTTPS を使用して CCO サーバと通信します。デバイスに組み込み証明書がない場合は、レガシー動作が開始されます。

デバイスがスタートアップ コンフィギュレーションまたは認証証明書なしで起動し、DHCP および DNS 検出が失敗した場合、デバイスは *devicehelper.cisco.com* の Cisco Cloud サーバに接続しようとします。

devicehelper.cisco.com に到達できる場合、Cisco Network PnP エージェントはトラストプールバンドルをダウンロードし、Cisco Cloud リダイレクトサービスとのセキュアな HTTP 接続を確立します。デバイスが Cisco Cloud 検出を初めて試行すると、Cisco Network PnP エージェントは、この場所（*devicepooler.cisco.com/ca/trustpool*）からトラストプールをダウンロードし、ローカルフラッシュメモリに保存します。この場所は、トラストプールのインストール用の公開キーインフラストラクチャと共有されます。Cisco Cloud 検出が失敗した場合、トラストプールバンドルはフラッシュメモリ内に保持され、Cisco Network PnP はローカルデバイスのフラッシュメモリ内の trustpool バンドルのコピーを確認します。コピーがローカルフラッシュメモリで使用できない場合は、この場所（*devicehelper.cisco.com/ca/trustpool download*）からトラストプールバンドルのダウンロードを再試行します。

Cisco Network PnP エージェントは、HTTPS hello メッセージを Cisco Cloud に送信します。Cisco Cloud サーバで実行されている Cisco Network PnP リダイレクトサービスは、HTTP 要求に応答します。次の例に示すように、Cisco Cloud サーバの PnP プロファイルがデバイスに作成されます。

```
pnp profile pnp_cco_profile
transport https host devicehelper.cisco.com port 443
```

Cisco Cloud プロファイルが作成された後、デバイスは一意のデバイス識別子情報を含む作業情報メッセージを Cisco Cloud サーバに送信します。Cisco Cloud リダイレクトサービスは、Cisco Network PnP サーバ情報とともにリダイレクト非バックオフ PnP 要求を送信します。IPv4 アドレス、IPv6 アドレス、またはホスト名を指定できます。リダイレクトが成功すると、次のリダイレクトプロファイルがデバイスに設定されます。

```
pnp profile pnp_redirection_profile
transport https ipv4 172.19.153.133 port 443
```

非バックオフ PnP 要求をデフォルトの待機時間内に受信しなかった場合、Cisco Network PnP 検出プロセスは次の検出メカニズムを続行します。

4G インターフェイスを介した Cisco Network PnP 検出

4G インターエイスを介した Cisco Network PnP は、4G NIM を搭載し、Cisco IOS XE を実行しているプラットフォームで使用できます。アクティブになっている SIM カードを搭載したデバイスが起動すると、4G インターフェイスがアクティブになり、Cisco Network PnP クラウド検出プロセスに使用されます。SIM カードがアクティブになっていないデバイスが起動すると、検出プロセスには4G以外のインターフェイスが優先されます。4Gインターフェイスを介した Cisco Network PnP クラウド検出は、4G 以外のインターフェイスを使用できない場合や、4G 以外のインターフェイスで Cisco Network PnP 検出が成功しない場合に試行されます。デバイスにアクティブな SIM カードを備えた複数の 4G インターフェイスがある場合、Cisco Network PnP は、いずれかが成功するまで、すべての 4G インターフェイスでクラウド検出を試行します。

（注） Cisco Network PnP 検出に 4G インターフェイスを使用するには、4G NIM にアクティブ化された SIM カードが必要です。

4G インターフェイスを介した Cisco Network PnP クラウド検出は、すべての 4G インターフェイスがデバイス起動時にデフォルトでアクティブになっている場合に機能します。スタートアップ コンフィギュレーションがない場合、デバイスはデフォルトで 4G インターフェイスを起動しようとし、クラウドを介して Cisco PnP を試行します。デバイスがリダイレクトされると、デバイスは Cisco Network PnP サーバに接続し、適切なイメージと設定をデバイスにダウンロードします。

（注） DNS サーバは 4G ネットワークの一部として使用でき、クラウドポータルはデバイスをプロビジョニングするために適切な Cisco Network PnP サーバに発信側デバイスをリダイレクトするようにプログラムする必要があります。現在、4G インターフェイスを介した Cisco Network PnP のサポートでは、IPv4 ネットワークのみが使用されます。

Cisco Network PnP サーバを介してプッシュされた設定に、4G インターフェイスを介した Cisco Network PnP サーバへのルートが含まれていることを確認します。これはデフォルトルートで

ある可能性があり、プロビジョニングが完了した後も 4G インターフェイス上で動作するように、Cisco Network PnP エージェントとサーバの通信を維持する必要があります。

管理インターフェイスを介した Cisco Network PnP 検出

Cisco Network PnP Agent は、デフォルトの VPN ルーティング/転送（VRF）を使用し、管理インターフェイスを介して検出と 4 方向ハンドシェイクをサポートします。VRF インターフェイスを介して DHCP トラフィックを送受信するには、IOS DHCP サーバを設定する必要があります。この機能は、管理インターフェイスのみがアクティブな場合に、新しいデバイスが Cisco Network PnP 機能にアクセスするのに役立ちます。

デバイスが起動すると、デフォルトの VRF 管理インターエイスに IP アドレスが DHCP を介して割り当てられます。このインターフェイスは Cisco Network PnP サーバへの接続を確立し、デバイス上の Cisco Network PnP エージェントがこの情報（VRF 名と送信元インターフェイス）を記録します。この情報は Cisco Network PnP サーバとの今後の PnP 通信に使用されます。この場合、デバイスで作成される Cisco PnP プロファイルには追加のキーワード **VRF** が付加されます。

EtherChannel を介した Cisco PnP

Cisco Network Plug and Play を使用してアクセススイッチを展開する場合、プロビジョニングされたスイッチ（トランクとして動作）に LACP EtherChannel が存在するため、デバイスを設定できません。アクセスデバイスが LACP を使用して L2 EtherChannel を介してプロビジョニングされたスイッチ経由で接続しようとすると、接続が切断されます。設定がアクセスデバイスに存在しないため、アクセスデバイスはスイッチで EtherChannel を起動できません。これにより、EtherChannel ポートが中断状態になり、L2 接続が切断されます。Cisco Network PnP エージェントは、EtherChannel の存在を検出し、デバイスの EtherChannel を自動設定して、Day-Zero 設定のレイヤ 2 接続を自動的に起動します。

PnP 検出プロセス完了後のセキュリティ方式

この項では、Cisco PnP エージェントによって提供される、検出プロセスの完了後のクライアント/サーバ通信を保護するために Cisco PnP サーバで使用できる方法について説明します。ここでは、次の内容について説明します。

• 証明書インストールサービス （209 ページ）

証明書インストールサービス

Cisco PnP エージェントは、Cisco PnP サーバに証明書インストールサービスを提供することで、デバイス上の SSL 証明書を管理するメカニズムを提供します。certificate-install サービスは、HTTPS 接続を開始する前に、サーバの自己署名証明書またはデバイスの標準 CA 証明書によって署名された証明書をインストールするためのシンプルな XML を提供します。certificate-install サービスには、クライアントの SSL 証明書をインストールし、次のデバイス認証プロセス時に同じ SSL 証明書を使用するようにデバイスに指示するオプションもあります。

SUDI ベースの PnP アプリケーションレベルの認証

SSL 通信はサーバとデバイス間で交換されるデータパケットを確実に暗号化しますが、デバイスを認証するためのソリューションは提供しません。

サーバが正規のシスコのデバイスと通信していることを確認するために、エージェントはデバイスに組み込まれている Secure Unique Device Identifier（SUDI）証明書サポートを使用します。SUDI は製造時にデバイスの安全なチップ（ACT2）に書き込まれた X.509 準拠のデバイス証明書です。SUDI 証明書には、デバイスのシリアル番号、秘密/公開キー、および Cisco CA の署名が含まれています。エージェントは、サーバがデバイスを正規のシスコのデバイスとして認証するのに使用できる次のメカニズムを提供します。

• SUDI ベースのクライアント証明書の検証 （210 ページ）
• SUDI ベースのシリアル番号 （210 ページ）

SUDI ベースのクライアント証明書の検証

エージェントがサーバとの HTTPS 接続を開始する前に、エージェントはデバイスに組み込みの SUDI 証明書があるかどうかを確認します。デバイスに証明書がある場合は、エージェントは検証のための SSL ハンドシェイク時に SUDI 証明書をクライアントに送信します。必要に応じて、HTTPS サーバは、SSL ハンドシェイク時に SUDI 証明書を使用してデバイスを検証することもできます。検証後、HTTPS サーバはデバイスがサーバに接続できるようにします。デバイスの SUDI 証明書を検証するには、サーバが Cisco CA を使用して検証を完了する必要があります。

SUDI ベースのシリアル番号

デバイスに SUDI 証明書がロードされている場合、PnP エージェントは SUDI 証明書からシリアル番号を読み取り、サーバとのすべての通信の作業要求の本文に同じ情報を追加タグとして提示します。これを実現するために、次のオプションのタグが作業情報メッセージに追加されます。これは、すべての作業要求でデバイスから送信されます。このフィールドはオプションであり、SUDI 証明書がないデバイスには表示されません。

シャーシインベントリから読み取られる既存の UDI メカニズムに変更はありません。プライマリ識別子としてシャーシ UDI を送信することで、エージェントは引き続き下位互換性を維持します。サーバは追加で提供された SUDI ベースのシリアル番号を使用してデバイスを認証するとプライマリ UDI を引き続き使用できます。SUDI 証明書のないデバイスの場合、エージェントはこの追加の SUDI ベースのシリアル番号を送信しません。したがって、サーバは認証とそれ以降の通信のためにプライマリ UDI を継続する必要があります。

メンバーハードウェアから SUDI ベースのシリアル番号の読み取りに使用できるメカニズムはなく、スタック または HA ユニットの他のメンバーからの UDI の読み取り方法に変更はありません。エージェントは引き続き、現在のようにすべてのハードウェアユニットから UDI を読み取ります。

SUDI ベースのデバイス認証

SUDI ベースのデバイス認証では、エージェントは起動時にデバイスに組み込みの SUDI 証明書があるかどうかを確認します。デバイスに SUDI 証明書がロードされている場合、エージェントは新しい PnP サービスを提供します。これにより、サーバがデバイスを識別できるようになります。この新しいサービスが利用できるかどうかは SUDI 証明書の存在によって異なり、エージェントの機能サービスのリストに表示されます。

上記の capability-service の変更に伴い、エージェントは device-info 応答の hardware-info セクションに新たなフィールドを追加し、SUDI 証明書がデバイスに組み込まれているかどうかを特定して確認します。

その後、エージェントはサーバとの HTTPS 接続を開始し、作業要求を送信します。サーバはデバイス認証サービスをチャレンジ要求/応答に使用できる必要があります。デバイス認証サービスでは、サーバが文字列を生成するために少なくとも 1 つのフィールドが必要です。オプションで、サーバはサポート可能な暗号化方式とハッシュ方式のリストを送信できます。エージェントは、サーバによって指定されたリストの暗号化方式のいずれかを使用する機能があるかどうかを確認し、暗号化方式を使用してサーバに通知を送信します。サーバで指定されたいずれの方法もエージェントが使用できない場合、エージェントはエラーメッセージで応答します。

サーバがデバイス認証サービス要求をエージェントに送信すると、エージェントは次の処理を実行します。

1. 指定された暗号化方式とハッシュ方式のいずれかを使用します。
2. 指定された暗号化方式およびハッシュ方式のいずれかを使用する機能がエージェントにない場合、エージェントはエラーメッセージで応答します。
3. PKI API を使用して、秘密キーを使用してサーバから提供されたチャレンジ文字列を暗号化します。
4. 次の応答を返します。
    1. 暗号テキスト
    2. 暗号に使用される方法
    3. 証明書（SUDI またはクライアントインストール証明書）

その後、サーバはデバイスから上記の応答を受信すると、次の処理を実行します。

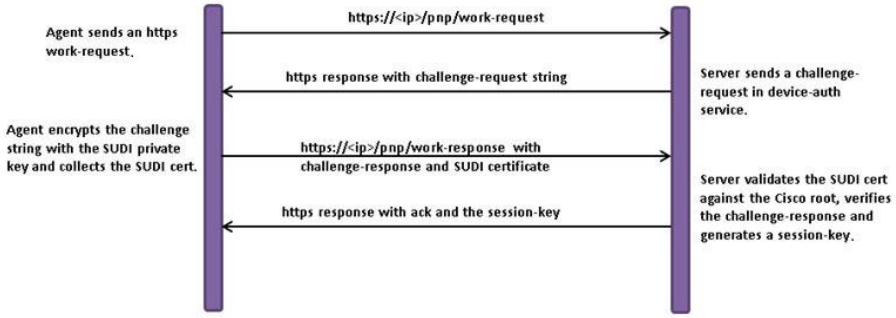
1. シスコまたはカスタマー CA に対して SUDI またはクライアント証明書を確認します。
2. SUDI またはクライアント証明書で使用可能な公開キーを使用して暗号文字列を復号します。
3. 復号された文字列が元のバージョンと一致するかどうかを確認します。
4. セッションキー（文字列）を生成し、確認応答としてデバイスに送り返します。

エージェントは、セッションキーを含む最終確認応答をサーバから受信すると、対応するプロファイルを提供されたセッションキーに関連付け、それをエージェントが送信する後続のすべてのメッセージのルート PnP セクションの属性としてサーバに送信します。

サーバは、デバイスからメッセージを送信する前にセッションキーを検証します。必要に応じて、サーバはセッションキーのタイマーを保持し、タイマーが期限切れになると無効ステータスに移行します。エージェントが期限切れのセッションキーを含むメッセージを送信すると、サーバはデバイス認証プロセスを繰り返し、新しいセッションキーを生成してから同じデバイスに再度送信します。デバイスがセッションキーを使用せずに要求を送信すると、サーバはデバイス認証プロセスを実行し、新しいセッションキーを生成してから同じデバイスに送信します。

次の図に、SUDI証明書を使用してデバイス認証を行うための、エージェントとサーバ間のメッセージシーケンスを示します。

図 *60 :* メッセージ シーケンス



Cisco Network Plug and Play エージェントの設定方法

Cisco Network Plug and Play エージェントのプロファイルの設定

Cisco Network Plug and Play エージェントのプロファイルを作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Network Plug and Play エージェントデバイスの設定

Cisco Network Plug and Play エージェントのデバイスを作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**device** {**username** *username* } {**password {0 | 7}** *password*} 例：	デバイス上に PnP エージェントを設定します。 • ユーザ名とパスワードに基づく認証システムを確立します。

	コマンドまたはアクション	目的
	`Device(config-pnp-init)# device username sjohn password 0 Tan123`	• *username*：ユーザ ID • *password*：ユーザが入力したパスワード • **0**：非暗号化パスワードまたは秘密キー（設定による）が後に続くことを指定します。 • **7**：暗号化パスワード（非表示）が後に続くことを指定します。
ステップ 5	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play の再接続要因の設定

固定インターバルバックオフ、指数バックオフ、ランダム指数バックオフのいずれかのモードでのセッション再接続を試みる前に、待機する時間を設定するために、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**reconnect** [*pause-time* [*exponential-backoff-factor* [**random**]]] 例：	PnP エージェント イニシエータ プロファイルがセッション再接続を試行するまでの待機時間を指定します。

	コマンドまたはアクション	目的
	`Device(config-pnp-init)# reconnect 100 2 random`	• pause-time 値は、接続が失われてから再接続するまで待機する時間（秒数）です。範囲は 1 ～ 2000000 です。デフォルトは 60 です。 • exponential-backoff-factor 値は、再接続試行を指数的にトリガーする値です。範囲は 2 ～ 9 です。
ステップ 5	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play の HTTP トランスポートプロファイルの設定

Cisco Plug and Play エージェントの HTTP トランスポートプロファイルをデバイス上に手動で作成するには、次のタスクを実行します。

PnP サーバ IP 設定には、IPv4 アドレスと IPv6 アドレスの両方を使用できます。また、PnP サーバに接続するため、設定の中でホスト名を使用することもできます。

どのプロファイルにも、1 つのプライマリ サーバと 1 つのバックアップ サーバの設定が可能です。Cisco PnP エージェントは、まずプライマリサーバとの接続の開始を試み、それが失敗した場合にはバックアップサーバを試します。バックアップサーバで障害が発生すると、Cisco PnP エージェントは再びプライマリサーバへの接続を試みます。サーバのうちの 1 つとの接続が確立されるまでこれが続行されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**pnp profile** *profile-name* 例：	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# pnp profile test-profile-1`	• PnP エージェントプロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**transport http host** *host-name* [**port** *port-number*] [**source** *interface-type*] 例： `Device(config-pnp-init)# transport http host hostname-1 port 1 source gigabitEthernet 0/0/0`	PnP エージェントの導入先サーバのホスト名に基づいて、PnP エージェント プロファイルの HTTP トランスポート設定を作成します。 • host の値はサーバのホスト名、ポート、および発信元を指定します。 • port-number の値は使用するポートを指定します。 • interface-type の値はエージェントのサーバへの接続に使用されるインターフェイスを指定します。
ステップ 5	**transport http ipv4** *ipv4-address* [**port** *port-number*] [**source** *interface-type*] 例： `Device(config-pnp-init)# transport http ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0`	PnP エージェントの導入先サーバの IPv4 アドレスに基づいて、PnP エージェント プロファイルの HTTP トランスポート設定を作成します。
ステップ 6	**transport http ipv6** *ipv6-address* [**port** *port-number*] [**source** *interface-type interface-number*] 例： `Device(config-pnp-init)# transport http ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1`	PnP エージェントの導入先サーバの IPv6 アドレスに基づいて、PnP エージェント プロファイルの HTTP トランスポート設定を作成します。
ステップ 7	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play の HTTPS トランスポートプロファイルの設定

Cisco Network Plug and Play エージェントの HTTP Secure（HTTPS）トランスポートプロファイルをデバイス上に手動で作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**transport https host** *host-name* [**port** *port-number*][**source** *interface-type*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# transport https host example.com port 231 source gigabitEthernet 0/0/0 localcert abc remotecert xyz`	PnP エージェントの導入先サーバのホスト名に基づいて、PnP エージェント プロファイルの HTTPS トランスポート設定を作成します。 • *localcert* の値は、Transport Layer Security（TLS）ハンドシェイク時にクライアント側の認証用に使用するトラストポイントを指定します。 • *remotecert* の値は、サーバ証明書の検証に使用されるトラストポイントを指定します。 （注） **crypto pki trustpoint** コマンドを使用した trustpoint-name の設定
ステップ 5	**transport https ipv4** *ipv4-address* [**port** *port-number*][**source** *interface-type*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# transport https ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0 localcert abc remotecert xyz`	PnP エージェントの導入先サーバの IPv4 アドレスに基づいて、PnP エージェント プロファイルの HTTPS トランスポート設定を作成します。
ステップ 6	**transport https ipv6** *ipv6-address* [**port** *port-number*][**source** *interface-type interface-number*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例：	PnP エージェントの導入先サーバの IPv6 アドレスに基づいて、PnP エージェント プロファイルの HTTPS トランスポート設定を作成します。

	コマンドまたはアクション	目的
	`Device(config-pnp-init)# transport https ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1 localcert abc remotecert xyz`	
ステップ 7	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play のバックアップデバイスの設定

バックアッププロファイルを作成し、デバイス上で Cisco Network Plug and Play エージェントを手動で有効または無効にするには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**backup device** {**username** *username* } {**password {0 | 7}** *password*} 例： `Device(config-pnp-init)# backup device username sjohn password 0 Tan123`	デバイス上に PnP エージェント バックアップ プロファイルを設定します。 • ユーザ名とパスワードに基づく認証システムを確立します。 • *username* - ユーザ ID • *password* - ユーザが入力するパスワード • 0：非暗号化パスワードまたは秘密キー（設定による）が後に続くことを指定します。

	コマンドまたはアクション	目的
		• 7 — 非表示パスワードが後に続くことを指定します。
ステップ 5	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play のバックアップ再接続要因の設定

固定インターバルバックオフ、指数バックオフ、またはランダム指数バックオフのいずれかの方法で、サーバに Cisco Network Plug and Play（PnP）エージェントのバックアップ再接続を設定するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**backup reconnect** [*pause-time* [*exponential-backoff-factor* [**random**]]] 例： `Device(config-pnp-init)# backup reconnect 100 2 random`	PnP エージェントイニシエータ プロファイルがセッション再接続を試行するまでの待機時間を指定します。 • pause-time 値は、接続が失われてから再接続するまで待機する時間（秒数）です。範囲は 1 ～ 2000000 です。デフォルトは 60 です。

	コマンドまたはアクション	目的
		• exponential-backoff-factor 値は、再接続試行を指数的にトリガーする値です。範囲は 2 ～ 9 です。
ステップ 5	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play のバックアップ HTTP トランスポートプロファイルの設定

Cisco Network Plug and Play エージェントのバックアップ HTTP トランスポートプロファイルをデバイス上に手動で作成するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**backup transport http host** *host-name* [**port** *port-number*] [**source** *interface-type*] 例： `Device(config-pnp-init)# backup transport http host hostname-1 port 1 source gigabitEthernet 0/0/0`	PnP エージェントの導入先サーバのホスト名に基づいて、PnP エージェント プロファイルのバックアップ HTTP トランスポート設定を作成します。 • host の値はサーバのホスト名、ポート、および発信元を指定します。 • port-number の値は使用するポートを指定します。

	コマンドまたはアクション	目的
		• interface-type の値はエージェントのサーバへの接続に使用されるインターフェイスを指定します。
ステップ 5	**backup transport http ipv4** *ipv4-address* [**port** *port-number*] [**source** *interface-type*] 例： `Device(config-pnp-init)# backup transport http ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0`	PnP エージェントの導入先サーバの IPv4 アドレスに基づいて、PnP エージェント プロファイルのバックアップ HTTP トランスポート設定を作成します。
ステップ 6	**backup transport http ipv6** *ipv6-address* [**port** *port-number*] [**source** *interface-type interface-number*] 例： `Device(config-pnp-init)# backup transport http ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1`	PnP エージェントの導入先サーバの IPv6 アドレスに基づいて、PnP エージェント プロファイルのバックアップ HTTP トランスポート設定を作成します。
ステップ 7	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play のバックアップ HTTPS トランスポートプロファイルの設定

Cisco Network Plug and Play エージェントのバックアップ HTTPS トランスポートプロファイルをデバイス上に手動で作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**pnp profile** *profile-name* 例： `Device(config)# pnp profile test-profile-1`	PnP エージェント プロファイルを作成し、PnP プロファイル初期設定モードを開始します。 • PnP エージェント プロファイルの名前を指定する英数字文字列。プロファイル名が重複していてはなりません。
ステップ 4	**backup transport https host** *host-name* [**port** *port-number*][**source** *interface-type*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# backup transport https host example.com port 231 source gigabitEthernet 0/0/0 localcert abc remotecert xyz`	PnP エージェントの導入先サーバのホスト名に基づいて、PnP エージェント プロファイルのバックアップ HTTPS トランスポート設定を作成します。 • *localcert* の値は、Transport Layer Security（TLS）ハンドシェイク時にクライアント側の認証用に使用するトラストポイントを指定します。 • *remotecert* の値は、サーバ証明書の検証に使用されるトラストポイントを指定します。
ステップ 5	**backup transport https ipv4** *ipv4-address* [**port** *port-number*][**source** *interface-type*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# backup transport https ipv4 10.0.1.0 port 221 source gigabitEthernet 0/0/0 localcert abc remotecert xyz`	PnP エージェントの導入先サーバの IPv4 アドレスに基づいて、PnP エージェント プロファイルのバックアップ HTTPS トランスポート設定を作成します。
ステップ 6	**backup transport https ipv6** *ipv6-address* [**port** *port-number*][**source** *interface-type interface-number*][**localcert** *trustpoint-name*][**remotecert** *trustpoint-name*] 例： `Device(config-pnp-init)# backup transport https ipv6 2001:DB8:1::1 port 331 source gigabitEthernet 0/0/1 localcert abc remotecert xyz`	PnP エージェントの導入先サーバの IPv6 アドレスに基づいて、PnP エージェント プロファイルのバックアップ HTTPS トランスポート設定を作成します。
ステップ 7	**end** 例： `Device(config-pnp-init)# end`	PnP プロファイル初期設定モードを終了し、特権 EXEC モードに戻ります。

Cisco Network Plug and Play エージェント タグの設定

Cisco Network Plug and Play エージェントのタグ情報を作成するには、次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**pnp tag** *tag-name* 例： `Device(config)# pnp tag xyz`	デバイスにタグを設定するには、**pnp tag** コマンドを使用します。Cisco のネイバー デバイスは Cisco Discovery Protocol（CDP）を通じてこのタグ情報を受信します。 （注） デバイスに既存のタグがある場合、タグ名を変更できるのは、タグ名の変更のために xml スキーマが PnP サーバにより送信される場合のみです。タグ名は上書きできません。 • PnP エージェント タグの名前を指定する英数字文字列。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラブルシューティングとデバッギング

Cisco Network Plug and Play サーバでデバッグを実行する（サーバを起動する）には、PnP プロファイルと PnP トランスポートを設定します。たとえば、PnP エージェントと PnP サーバ間でのサービスの連携動作を開始します。

debug pnp service コマンドを実行することでデバッグをキャプチャできます。問題を報告する場合は、ガイドに従って PnP エージェントフラッシュ内のすべての pnp を収集します。

（注） Cisco Plug and Play サーバのログを収集するには、『Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide』を参照してください。

デバイス、サーバ、および Cisco PnP エージェントのトラブルシューティングを行うには、次のコマンドを使用します。

表 *13*：デバイス、サーバ、および *Cisco PnP* エージェントのトラブルシューティング

コマンド	説明
dir nvram	デバイスに証明書が残っていないことを確認するには、このコマンドを使用します。
ping vrf interface-name *<controller_ip>*	デバイスがコントローラを ping できることを確認するには、このコマンドを使用します。
show auto install trace	自動インストールのトレースログを表示するには、このコマンドを使用します。
show boot	BOOTLDR 変数の現在の値を表示するには、このコマンドを使用します。
show cdp neighbor	すべての CDP ネイバーを表示するには、このコマンドを使用します。
Show crypto pki trustpoint	PKI トラストポイントを表示するには、このコマンドを使用します。
Show crypto pki trustful	信頼できる PKI を表示するには、このコマンドを使用します。
show ip interface brief	ルータインターフェイスの概要を表示するには、このコマンドを使用します。
show ipv6 interface brief	IPv6 インターフェイスを表示するには、このコマンドを使用します。
show run | inc pnp	1 つの PnP プロファイルのみがインストールされていることを確認するには、このコマンドを使用します。
show pnp trace	デバイスにスタートアップ コンフィギュレーションがないことを確認するには、このコマンドを使用します。
show pnp tech	Cisco Plug and Play IOS エージェントのアクティブな接続を表示するには、このコマンドを使用します。
show vlan	VLAN 情報を表示するには、このコマンドを使用します。

コマンド	説明
show ntp status	NTP ステータスを表示するには、このコマンドを使用します。
show version	デバイスが最新のCCOイメージを実行していることを確認するには、このコマンドを使用します。

用語集

PnP エージェント：展開プロセスを自動化するためのデバイス上の組み込みエージェント

PnP ヘルパーアプリケーション：スマートフォンやパーソナルコンピュータ上の展開を容易にするアプリケーション。PnP ヘルパーアプリケーションは、お客様またはデバイスに固有ではなく、どのような展開シナリオでも使用できます。限られたシナリオで必要になることがあります。

PnP プロトコル：PnP エージェントと PnP サーバ間のプロトコル。これは、PnP サーバのサードパーティ開発を可能にするオープンプロトコルです。

PnP サーバ：展開するデバイスの展開情報（イメージ、設定、ファイル、およびライセンス）を管理し、配布する中央サーバ。Cisco Network Plug and Play サーバは、管理アプリケーションにノース バウンド インターフェイスを提供し、PnP プロトコルを使用してデバイス上の PnP エージェントと通信します。

Open Plug-n-Play エージェントのその他の参考資料

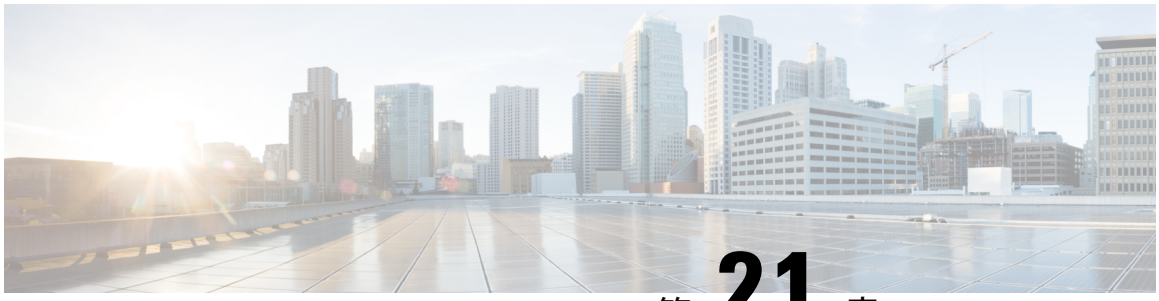
関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
PnP コマンド：コマンドシンタックスの詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	Cisco IOS PnP Command Reference
Cisco Network Plug and Play ソリューション	Solution Guide for Cisco Network Plug and Play
APIC-EM で Cisco Network Plug and Play を使用してシスコのネットワークデバイスを設定する方法	Configuration Guide for Cisco Network Plug and Play on Cisco APIC-EM

関連項目	マニュアル タイトル
APIC-EM の展開方法	Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide
APIC-EM を使用する前に	Cisco APIC-EM Quick Start Guide

MIB

MIB	MIB のリンク
• CISCO-BULK-FILE-MIB • CISCO-DATA-COLLECTION-MIB • CISCO-PROCESS-MIB • Expression-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs



第 21 章

ソフトウェア メンテナンス アップグレード（SMU）

この章は、次の項で構成されています。

ソフトウェアメンテナンスアップグレード（SMU）の概要

ソフトウェア メンテナンス アップグレード（SMU）は、システムにインストールできるパッケージであり、特定の不具合に対してパッチ修正やセキュリティの解決方法をリリースされたイメージに提供して問題を迅速に解決します。新しい機能は含まれていません。

次に、SMU の注意事項のいくつかを示します。

- リリースごと、コンポーネントごとに提供され、プラットフォームに固有です。SMU のバージョンは、アップグレードするパッケージのメジャー、マイナー、およびメンテナンス バージョンに同期されます。
- SMU は、メンテナンス リリースの代わりになるものではありません。SMU で修正されたすべての不具合は、次回のメンテナンスリリースに統合されます。
- Cisco IOS XE プラットフォームでは SMU の互換性を内部的に検証し、互換性のない SMU はインストールできません。これは、SMU 変更セットのルールまたは制限事項に基づいています。
- SMU はネットワークの問題に迅速に対応できるようにするとともに、必要なテストの時間と範囲を削減するため、従来の IOS ソフトウェアよりも大きなメリットがあります。
- SMU は既存のリリースのバグを修正するための方法であり、既存のリリースで PSIRT の修正を適用できます。

- SMU はリリース X からメンテナンスリリース X.1 へのアップグレードパスではありません。
- SMU はリリース X からリリース Y へのアップグレードパスではありません。

デバイスは「ホットパッチ」のみをサポートします。これは、以下を意味します。

- 実行中イメージがインプレースまたはインサービスで変更されます。
- これにより、サービスのダウンタイムと中断が回避されます。
- 不具合を修正するために更新されたコードは、別の場所に書き込まれ、パッチがプログラムの実行をリダイレクトします。

SMU のワークフローと基本要件

パッチのワークフローでは、EXEC モードで次の一連の操作を完了する必要があります。

1. ファイルシステムへの SMU の追加
2. システムでの SMU のアクティブ化
3. SMU 変更のコミット
4. SMU の削除とアンインストール

SMU の基本要件は次のとおりです。

- 不具合が検出された場合のイメージ
- 不具合の修正を含むパッチファイルは、ir1101-image_name.release_version.CSCxxyyyyy.SPA.smu.bin の形式にする必要がある

SMU の例

この項では、CDET CSCvk58743 のパッチの例を示します。

コマンドの例：

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface g0/0/0
Router(config-if)# ipv6 nd cache expire 770
Router(config-if)# end
Router#
 *Sep 25 12:00:29.978: %SYS-5-CONFIG_I: Configured from console by console
```

次の CDET が示すように、ND キャッシュの有効期限タイマーがコマンド出力に表示されませんでした。 **show ipv6 neighbors g0/0/0**

- **CSCvk58743**

Summary：Show ipv6 interface は「ND キャッシュの有効期限タイマー」を表示しない

Component：ipv6

Defective Image：ir1101-universalk9.16.11.01.SPA.bin

Patch Image：ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin

必要な設定出力は次のようになります。

```
Interface GigabitEthernet0/0/0
 no switchport
 no ip address
 ipv6 address FE80::1 link-local
 ipv6 address 2001::1/64
 ipv6 nd na glean

ipv6 nd cache expire 770

 end
```

上記の出力では、青のテキストで IPv6 ネイバー検出のキャッシュエントリの期限が切れるまでの時間を設定します。範囲は 1 ～ 65536 秒です。

パッチイメージのインストール

パッチイメージをインストールするには、次の手順を実行します。

ステップ 1 イメージを追加します。

```
Router# install add file flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
install_add: START Mon Dec 17 21:11:23 UTC 2018
install_add: Adding SMU
*Dec 17 21:11:26.241: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install add
flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin--- Starting SMU Add operation ---
Performing SMU_ADD on Active/Standby
  [R0] SMU_ADD package(s) on R0
  [R0] Finished SMU_ADD on R0
Checking status of SMU_ADD on [R0]
SMU_ADD: Passed on [R0]
Finished SMU Add operation
SUCCESS: install_add  Mon Dec 17 21:11:39 UTC 2018
```

ステップ 2 パッチイメージをアクティブにします。

```
Router# install activate file flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
install_activate: START Mon Dec 17 21:11:57 UTC 2018
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]y Building
configuration...
 [OK]Modified configuration has been saved
*Dec 17 21:12:02.086: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config
fileinstall_activate: Activating SMU
*Dec 17 21:12:05.339: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install activate
 flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
Executing pre scripts....
Executing pre scripts done.
--- Starting SMU Activate operation ---
```

```
Performing SMU_ACTIVATE on Active/Standby
 [R0] SMU_ACTIVATE package(s) on R0
  [R0] Finished SMU_ACTIVATE on R0
Checking status of SMU_ACTIVATE on [R0]
SMU_ACTIVATE: Passed on [R0]
Finished SMU Activate operation
SUCCESS: install_activate /flash1/ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin Mon Dec 17
21:12:26 UTC 2018
*Dec 17 21:12:25.463: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer: Install
auto abort timer will expire in 7200 seconds
*Dec 17 21:12:27.358: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install
activate SMU flash:ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
```

ステップ 3 インストールを確定します。

```
Router# install commit
install_commit: START Mon Dec 17 21:13:28 UTC 2018
install_commit: Committing SMU

*Dec 17 21:13:31.516: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install commit
Executing pre scripts....
Executing pre scripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on Active/Standby
  [R0] SMU_COMMIT package(s) on R0
  [R0] Finished SMU_COMMIT on R0
Checking status of SMU_COMMIT on [R0]
SMU_COMMIT: Passed on [R0]
Finished SMU Commit operation

SUCCESS: install_commit /flash1/ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin Mon Dec 17 21:13:47
 UTC 2018
```

ステップ 4 インストール手順のステータスの概要を表示します。

```
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,

C - Activated
 & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    /flash1/ir1101-universalk9.16.11.01.CSCvk58743.SPA.smu.bin
IMG   C    16.11.1.0.4

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

パッチイメージのアンインストール

パッチイメージを削除またはアンインストールする方法は 2 つあります。

- 次のコマンドを使用して、イメージを元のバージョンに復元します。

- **install rollback to base**

- 次のコマンドを順番に使用して、パッチを具体的に削除します。
  - **install deactivate file flash:ir1101-image_name.release_version.CSCxxyyyyy.SPA.smu.bin**
  - **install commit**
  - **install remove file flash:ir1101-image_name.release_version.CSCxxyyyyy.SPA.smu.bin**

ロールバックを使用したパッチイメージのアンインストール

この項では、ロールバック方式の使用例を示します。

インストールされているパッチを表示します。

```
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    /flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin
IMG   C    16.12.02.0.6
```

次のコマンドを使用できます。

```
Router# install ?
  abort              Abort the current install operation
  activate           Activate an installed package
  add                Install a package file to the system
  auto-abort-timer   Install auto-abort-timer
  commit             Commit the changes to the loadpath
  deactivate         Deactivate an install package
  label              Add a label name to any installation point
  prepare            Prepare package for operation
  remove             Remove installed packages
  rollback           Rollback to a previous installation point
Router# install rollback to ?
  base       Rollback to the base image
  committed  Rollback to the last committed installation point
  id         Rollback to a specific install point id
  label      Rollback to a specific install point label
```

install rollback to base コマンドはパッチ全体を削除し、検出された不具合を含む基本イメージのバージョンに戻します。

```
Router# install rollback to base
install_rollback: START Fri Apr 24 22:58:25 UTC 2020

*Apr 24 22:58:28.375: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 rollbackinstall_rollback: Rolling back SMU
Executing pre scripts....
Executing pre sripts done.

--- Starting SMU Rollback operation ---
Performing SMU_ROLLBACK on Active/Standby
  [R0] SMU_ROLLBACK package(s) on R0
  [R0] Finished SMU_ROLLBACK on R0
```

```
Checking status of SMU_ROLLBACK on [R0]
SMU_ROLLBACK: Passed on [R0]
Finished SMU Rollback operation

SUCCESS: install_rollback /flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin Fri
 Apr 24 22:58:54 UTC 2020

*Apr 24 22:58:55.368: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install rollback
```

インストールされているパッチを表示します。

```
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   C    16.12.02.0.6
```

（注） 上記のコマンド出力では、パッチは削除されており、デバイスはアップグレード前の基本イメージバージョンに戻ります。

Deactivate、Commit、および Remove を使用したパッチイメージのアンインストール

次のシーケンスでは、2 つのパッチがデバイスにインストールされています。削除されるのは 1 つのみです。

インストールされているパッチを表示します。

```
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    /flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin
SMU   C    /flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin
IMG   C    16.12.02.0.6
```

ステップ 1 パッチを非アクティブ化します。

```
Router# install deactivate file flash:ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin
install_deactivate: START Fri Apr 24 22:54:10 UTC 2020
install_deactivate: Deactivating SMU
Executing pre scripts....
Executing pre sripts done.

--- Starting SMU Deactivate operation ---
```

```
Performing SMU_DEACTIVATE on Active/Standby
  [R0] SMU_DEACTIVATE package(s) on R0
  [R0] Finished SMU_DEACTIVATE on R0
Checking status of SMU_DEACTIVATE on [R0]
SMU_DEACTIVATE: Passed on [R0]
Finished SMU Deactivate operation

SUCCESS: install_deactivate /flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin Fri Apr 24
22:54:49 UTC 2020
```

インストールされているパッチを表示します。

```
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    /flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin
SMU   D    /flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin
IMG   C    16.12.02.0.6
```

ステップ 2 アクションをコミットします。

```
Router# install commit
install_commit: START Fri Apr 24 22:56:11 UTC 2020
install_commit: Committing SMU

*Apr 24 22:56:15.169: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
commitExecuting pre scripts....
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on Active/Standby
  [R0] SMU_COMMIT package(s) on R0
  [R0] Finished SMU_COMMIT on R0
Checking status of SMU_COMMIT on [R0]
SMU_COMMIT: Passed on [R0]
Finished SMU Commit operation

SUCCESS: install_commit /flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin Fri Apr 24 22:56:32
 UTC 2020

*Apr 24 22:56:33.342: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install
commit SMU
```

インストールされているパッチを表示します。

```
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    /flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin
SMU   I    /flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin
IMG   C    16.12.02.0.6
```

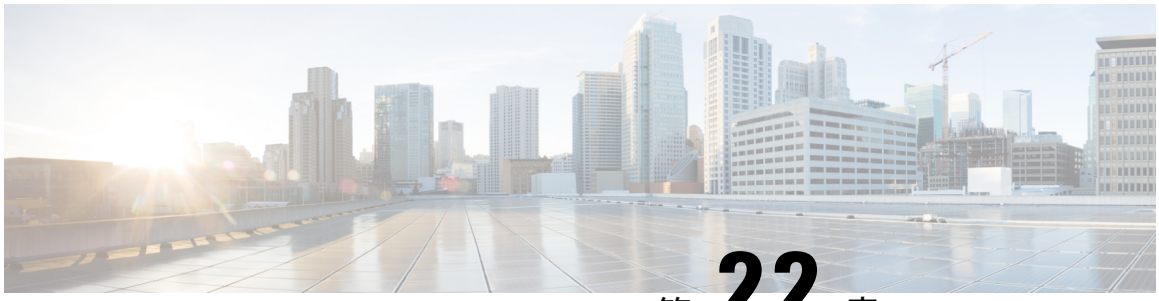
ステップ 3 パッチを削除します。

```
Router# install remove file flash:ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin
install_remove: START Fri Apr 24 22:57:17 UTC 2020

*Apr 24 22:57:20.775: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install remove
flash:ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bininstall_remove: Removing SMU
Executing pre scripts....
Executing pre scripts done.

--- Starting SMU Remove operation ---
Performing SMU_REMOVE on Active/Standby
  [R0] SMU_REMOVE package(s) on R0
  [R0] Finished SMU_REMOVE on R0
Checking status of SMU_REMOVE on [R0]
SMU_REMOVE: Passed on [R0]
Finished SMU Remove operation

SUCCESS: install_remove /flash1/ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin Fri Apr 24 22:57:34
 UTC 2020

*Apr 24 22:57:34.902: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install
remove flash:ir1101-universalk9.16.12.02.CSCvt63576.SPA.smu.bin
```

インストールされているパッチを表示します。

```
Router# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    /flash1/ir1101-universalk9.16.12.02.CSCvq74407.SPA.smu.bin
IMG   C    16.12.02.0.6
```

上記のコマンド出力では、CDET CSCvt63576 のパッチは削除されていますが、CDET CSCvq74407 のパッチは残っています。



第 22 章

Smart Licensing Using Policy（SLP）

この章は、次の項で構成されています。

SLP の概要

Smart Licensing Using Policy（SLP）は、IOS-XE リリース 17.3.2 以降のデフォルトモードで、以前は Smart Licensing Enhanced（SLE）と呼ばれていました。スマート ソフトウェア ライセンスは SLE に換わりました。IR1101 は SLP のみをサポートします。機能の違いの一部は次のとおりです。

- 輸出規制の要件にのみ認証コードが必要です。
- EVAL ライセンスがなくなりました。承認済みステータスが [In Use] または [Not In Use] と適用タイプクラスに変更されました。
- Cisco Smart Licensing Utility（CSLU）は、特定のカスタマートポロジでデバイスと Cisco Smart Software Manager（CSSM）との間をインターフェースする新しいツールです。
- スループットはデフォルトで 250 MB に制限されます。

重要 この項の残りの部分で使用される例は、ESR6300 ルータを示しています。IR1101 は、高スループットライセンスをサポートしていない点を除き、同じように機能します。

ライセンス執行（エンフォースメント）タイプ

所与のライセンスは、3 つの適用タイプのいずれかに属します。適用タイプは、ライセンスを使用する前に承認が必要かどうかを示します。

- 不適用または非適用

ライセンスの大半はこの適用タイプに属します。不適用ライセンスは、外部との接続がないネットワークで使用する前、または接続されたネットワークでの登録前に承認を必要としません。このようなライセンスの使用条件は、エンドユーザライセンス契約（EULA）に基づきます。

- 適用

この適用タイプに属するライセンスは、使用前に承認が必要です。必要な承認は承認コードの形式で行われ、対応する製品インスタンスにインストールする必要があります。

適用ライセンスの例としては、シスコのイーサネットスイッチで利用可能な Media Redundancy Protocol（MRP）クライアントライセンスがあります。

- 輸出規制

この適用タイプに属するライセンスは米国の取引規制法によって輸出が制限されており、これらのライセンスは使用前に承認が必要です。これらのライセンスの場合も、必要な承認コードは、対応する製品インスタンスにインストールする必要があります。シスコは、ハードウェア購入の際に発注がある場合、輸出規制ライセンスをプリインストールすることがあります。

輸出規制ライセンスの例としては、特定のシスコのルータで使用可能な高セキュリティ（HSEC）ライセンスがあります。

SLP アーキテクチャ

この項では、SLP の実装に含めることができるさまざまなコンポーネントについて説明します。

製品インスタンス

製品インスタンスとは、Unique Device Identifier（UDI）によって識別されるシスコ製品の単一インスタンスです。

製品インスタンスは、ライセンス使用状況（RUM レポート）を記録および報告し、期限切れのレポートや通信障害などに関するアラートとシステムメッセージを提供します。RUM レポートおよび使用状況データは、製品インスタンスに安全に保存されます。

リソース使用率測定レポート（RUM レポート）は、ポリシーで指定されたレポート要件を満たすためのライセンス使用状況レポートです。RUM レポートは製品インスタンスによって生成され、CSSMによって使用されます。製品インスタンスは、ライセンス使用状況情報とすべてのライセンス使用状況の変更を、開いている RUM レポートに記録します。システムが決定した間隔で、開いている RUM レポートが閉じられ、新しい RUM レポートが開かれて、ライセンスの使用状況の記録が継続されます。閉じられた RUM レポートは、いつでも CSSM に送信できます。

RUM確認応答（RUM ACK またはACK）はCSSMからの応答であり、RUM レポートのステータスに関する情報を提供します。レポートの ACK が製品インスタンスで使用可能になると、対応する RUM レポートが不要になり、削除できることが示されます。

CSSM は、最後に受信した RUM レポートに従ってライセンス使用状況情報を表示します。

Cisco Smart Software Manager（CSSM）

CSSM は一元化された場所からすべてのシスコ ソフトウェア ライセンスを管理できるポータルです。CSSMは、現在の要件を管理し、将来のライセンス要件を計画するための使用傾向を確認するのに役立ちます。

CSSM には https://software.cisco.com からアクセスできます。[License] タブで、[Smart Software Licensing] のリンクをクリックします。

CSSM では、次のことができます。

- バーチャルアカウントを作成、管理、または表示する。
- 製品インスタンスの登録トークンを作成および管理する。
- バーチャルアカウント間または表示ライセンス間でライセンスを転送する。
- 製品インスタンスを転送、削除、または表示する。
- バーチャルアカウントに関するレポートを実行する。
- 電子メール通知の設定を変更する。
- 仮想アカウント情報を表示する。

CSSM を使用する前に、次のポータルで使用方法に関する短いビデオをご覧ください。

https://www.cisco.com/c/ja_jp/buy/smart-accounts/software-manager.html

[**View Video**] ボタンをクリックします。

Cisco Smart Licensing Utility（CSLU）

CSLUは、集約ライセンスワークフローを提供するWindowsベースのレポートユーティリティです。これにより、CSSMに接続する代わりに、すべてのライセンスと関連する製品インスタンスを構内から管理できます。

このユーティリティが実行する主な機能は次のとおりです。

- ワークフローのトリガー方法に関するオプションを提供します。ワークフローはCSLUや製品インスタンスによってトリガーできます。
- 製品インスタンスから使用状況レポートを収集し、その使用状況レポートを対応するスマートアカウントやバーチャルアカウントにアップロードします。オンラインでもオフライン（ファイルを使用）でも可能です。同様に、RUM レポート ACK をオンラインまたはオフラインで収集して製品インスタンスに提供します。
- 承認コード要求を CSSM に送信し、CSSM から承認コードを受信します。

CSLU は次の方法で SLP トポロジに含めることができます。

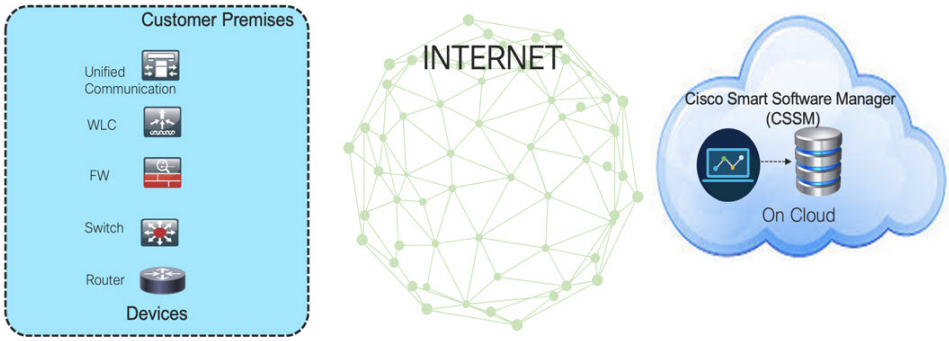
- スタンドアロンツールとして CSLU を使用し、CSSM に接続するには、Windows アプリケーションをインストールします。
- スタンドアロンツールとして CSLU を使用し、CSSM に接続しないようにするには、Windows アプリケーションをインストールします。このオプションを使用すると、必要な使用状況情報がファイルにダウンロードされ、CSSM にアップロードされます。これは、外部と接続していないネットワークに適しています。
- Cisco DNA Center などのコントローラに組み込みます。

カスタマートポロジ

IoT ルーティング プラットフォームは 2 つの異なるトポロジを使用します。

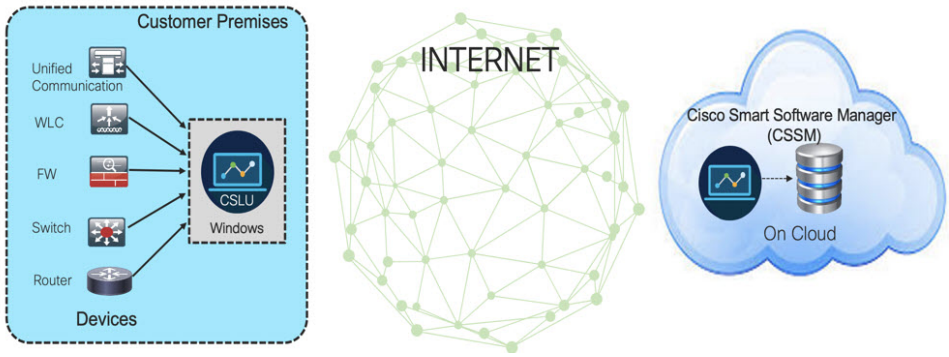
- フルオフラインアクセス
- CSLU に CSSM へのアクセスなし

次の図にフルオフラインアクセスを示します。



このトポロジでは、デバイスは CSSM（software.cisco.com）に接続できません。ユーザはシスコ製品と CSSM 間で情報をコピー/ペーストし、ライセンスのチェックイン/チェックアウトを手動で確認する必要があります。

次の図に、CSSM へのアクエスのない CSLU を示します。



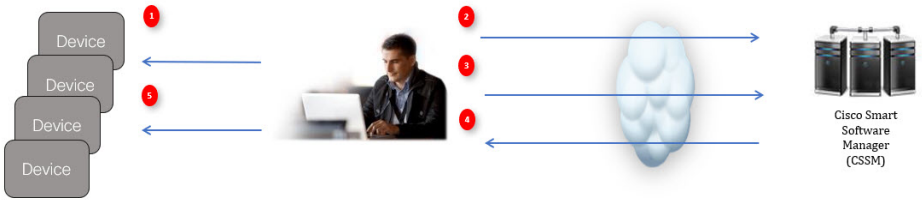
このトポロジでは、デバイスは CSLU コントローラに接続されていますが、CSLU と CSSM（Cisco Smart Software Manager – software.cisco.com）の間に接続はありません。

シスコのデバイスは、ローカルにインストールされた CSLU に使用状況情報を送信します。ユーザは、CSLU と CSSM の間で情報をコピー/ペーストして、ライセンスを手動でチェックイン/チェックアウトする必要があります。

ライセンスのインストール手順：フルオフラインアクセス トポロジ

この手順では、ルータと CSSM 間で必要な情報を手動で交換する必要があります。

情報のフローについては、次の図を参照してください。



1. ライセンス使用状況データファイルまたは AuthCode 要求を生成します。
2. CSSM にエクスポートします。
3. ライセンス使用状況データまたは AuthCode 要求をアップロードします。
4. ACK/AuthRequest ファイルをルータにエクスポートします。
5. ACK ファイルまたは AuthRequestAuthCode のアップロード

CSSM での製品インスタンスの登録手順

ステップ 1 ルータからライセンス使用状況ファイルを生成します。

EXEC モードで次の手順を実行します。

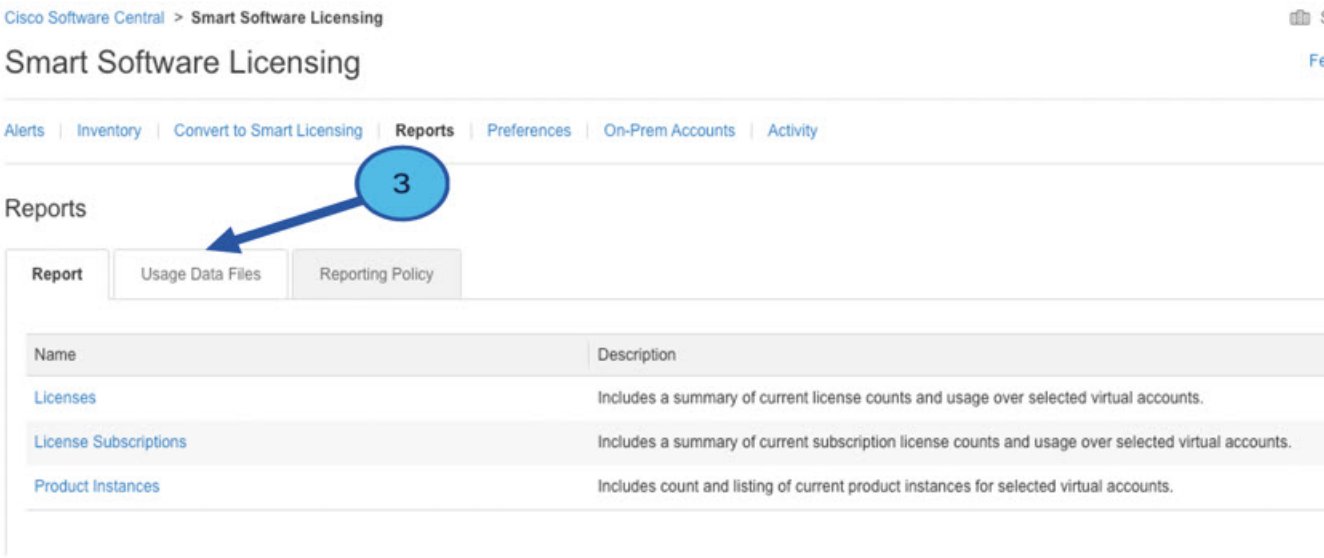
例：

```
Router# license smart save usage all file flash:slp
```

ステップ 2 ライセンス使用状況ファイル（slp）をホストのラップトップ/PC にエクスポートします。

ステップ 3 クラウド上の CSSM にライセンス使用状況ファイルをインポートします。[**Usage Data Files**] タブをクリックします。

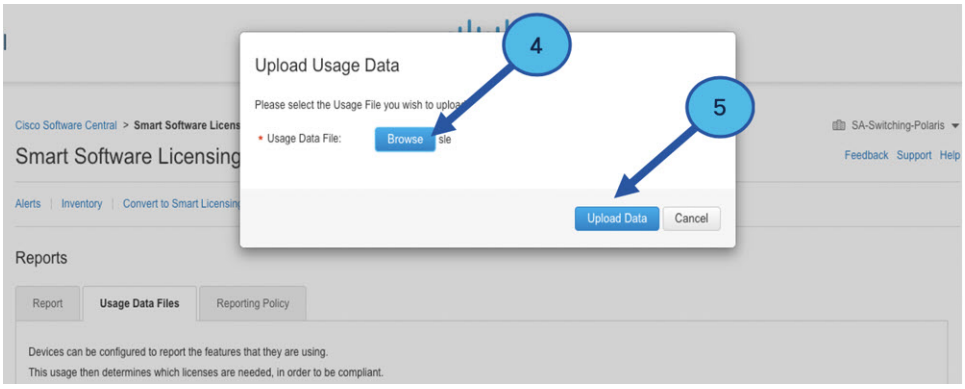
図 *61* : 使用状況データファイル



ステップ 4 [**Upload Usage Data**（SIP MWI notification mechanism）] ウィンドウが表示されます。[**Browse**] をクリックし、ファイルがある場所に移動します。

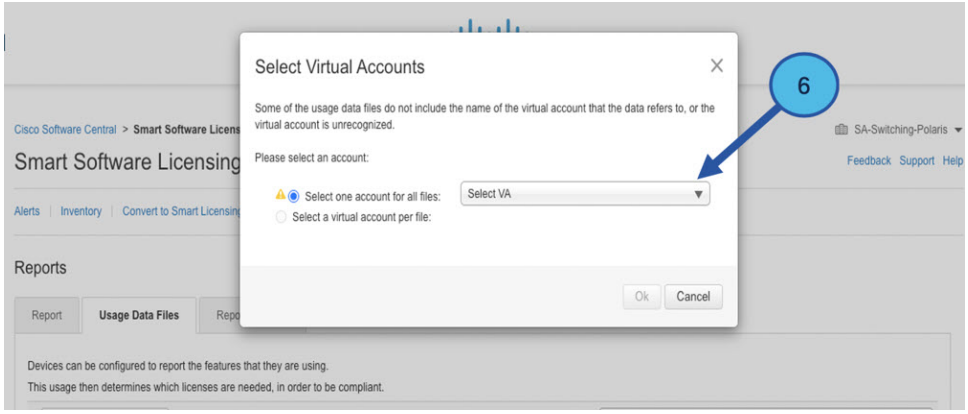
ステップ 5 [**Upload Data**] をクリックします。

図 *62* : 参照とアップロード



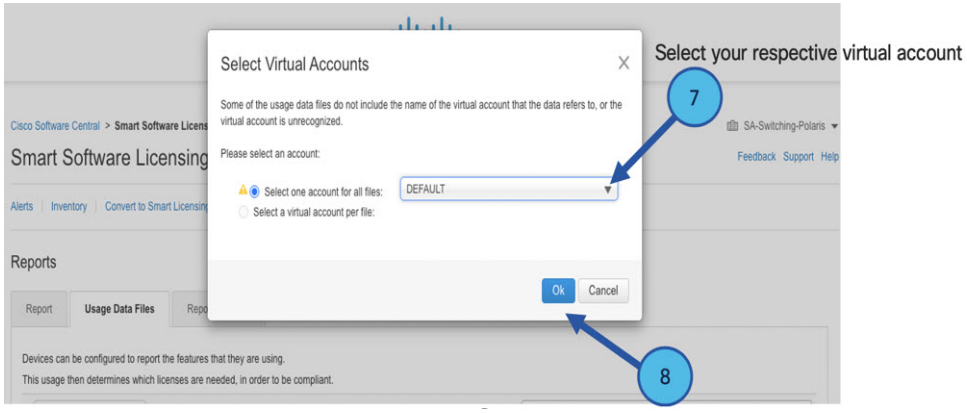
ステップ 6 バーチャルアカウントを選択します。

図 *63* : アカウントの選択



ステップ 7 プルダウンから、それぞれのバーチャルアカウントを選択します。

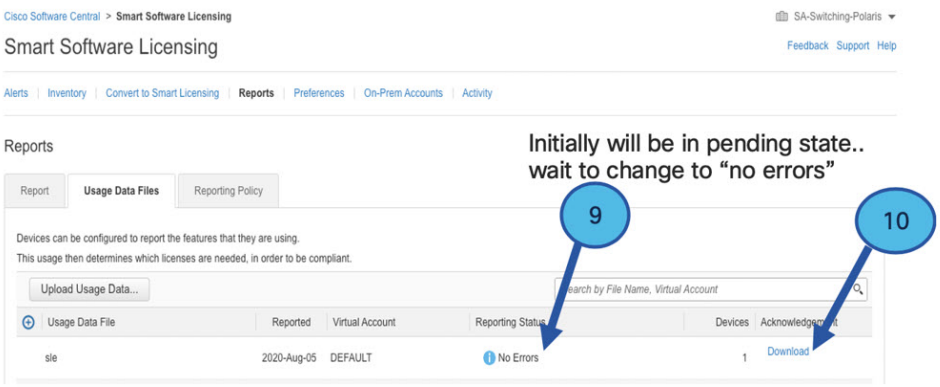
図 *64* : 自分のアカウントの選択



ステップ 8 [**Ok**] をクリックします。

ステップ 9 [Smart Software Licensing] ウィンドウを確認します。最初は、[Reporting Status] の状態が **Pending** になります。続行する前に、ウィンドウに **No Errors** が反映されるまで待ちます。

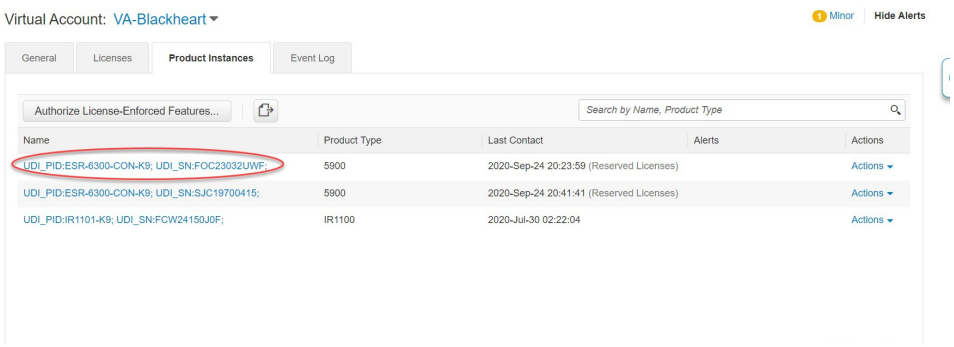
図 *65* : ステータスの表示



ステップ 10　[**Download**] をクリックして ACK ファイルをダウンロードします。

ステップ 11　[**Product Instances**] タブの下にデバイスがリストされていることを確認します。

図 *66* : 製品インスタンス



ステップ 12　コマンド ライン インターフェイスを使用して、CSSM からデバイスに ACK ファイルをインポートします。

CSSM からデバイスへの ACK ファイルのインポート

ステップ 1　CSSM からホストラップトップまたは usbflash デバイスに ACK ファイルをコピーします。次に、デバイスで exec モードを使用した場合の例を示します。

例：

```
Router#license smart import <flash: | usbflash0:> ACK_slp
Import Data Successful
Router#
*Sep  1 21:12:58.576: %SIP-1-LICENSING: SIP service is Up. License report acknowledged.
*Sep  1 21:12:58.616: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was successfully
 installed
```

ステップ 2 製品インスタンスがデータをインポートしたことを確認します。

例：

```
Router# show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (ESR6300_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M
  Feature Description: network-advantage_250M
  Enforcement type: NOT ENFORCED
```

ステップ 3 ライセンスが使用中であることを確認します。

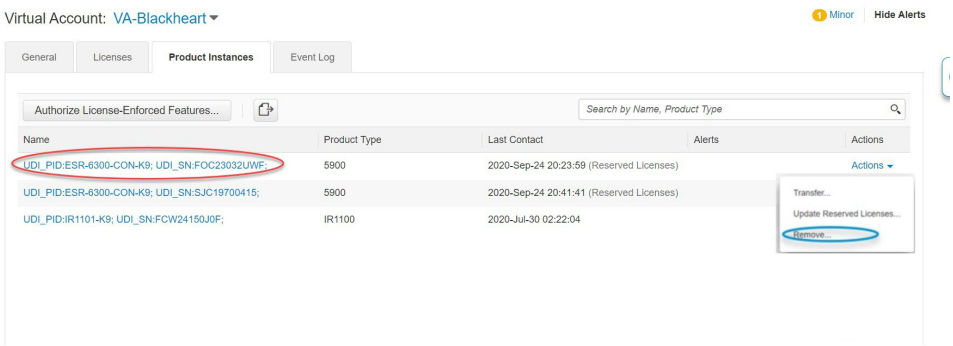
例：

```
Router# show license summary
License Usage:
  License                                          Entitlement tag               Count   Status
  -----------------------------------------------------------------------------------------
  network-advantage_250M  (ESR6300_P_250M_A)         1      IN USE

Router#
Router#show license all | beg Usage Reporting:
Usage Reporting:
  Last ACK received: Sep 01 21:12:58 2020 UTC
  Next ACK deadline: <none>
  Reporting Interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: Sep 01 00:28:48 2020 UTC
```

CSSM からのデバイスの削除

ステップ 1 [Product instances] タブに戻ります。デバイスを見つけます。

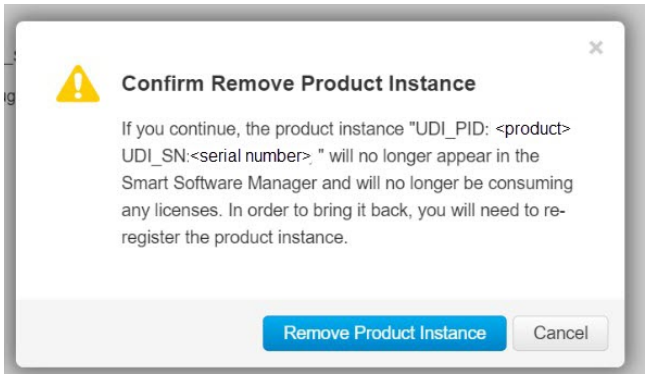
図 *67 :* 製品インスタンス



ステップ 2　デバイスの横にある [**Actions**] をクリックし、それらのオプションから [**Remove**] をクリックします。

[Confirm Remove Product Instance] ウィンドウが表示されます。

図 *68 :* 製品インスタンスの削除の確認

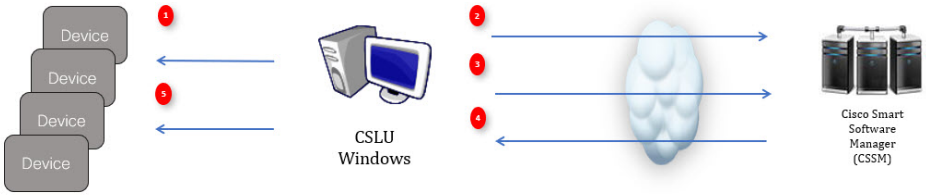


ステップ 3　[**Remove Product Instance**] をクリックします。

ライセンスのインストール手順：CSLU に CSSM へのアクセスなし

この手順では、ルータと CSLU 間で必要な情報をオンラインで交換します。

情報のフローについては、次の図を参照してください。



ステップ 1 CSLU で、AuthCode を必要とするデバイスを特定し、要求を開始します。AuthCode ファイルが作成されます。

ステップ 2 AuthCode ファイルを CSSM にエクスポートします。

ステップ 3 AuthCode を CSSM SA/VA アカウントにアップロードします。

ステップ 4 AuthRequestAuthcode ファイルを CSLU にエクスポートします。

ステップ 5 ACK ファイルまたは AuthRequestAuthCode のアップロード

デバイスが CSLU に接続されている場合の手順

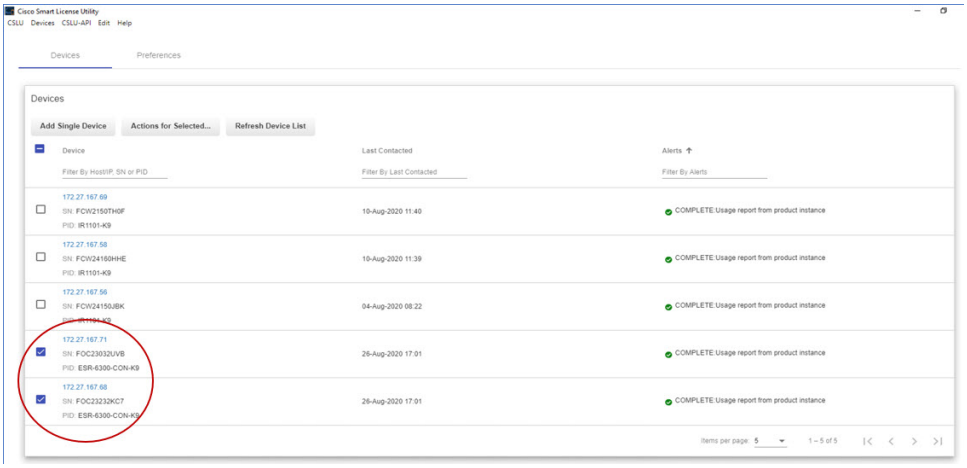
最初に、CLI を使用して次の手順をルータで実行してライセンス UDI を取得します。

```
Router#show license summary
License Reservation is ENABLED License Usage:
License Entitlement tag Count Status
network-advantage_250M (ESR6300 _P_250M_A) 1 IN USE

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#platform hardware throughput level 2G
% 2G throughput level requires hseck9 license!

Router(config)#end
Router#sh license udi
UDI: PID:ESR-6300-CON-K9,SN:FOC23032UVB
```

ステップ 1 Cisco Smart License Utility（CSLU）を開きます。

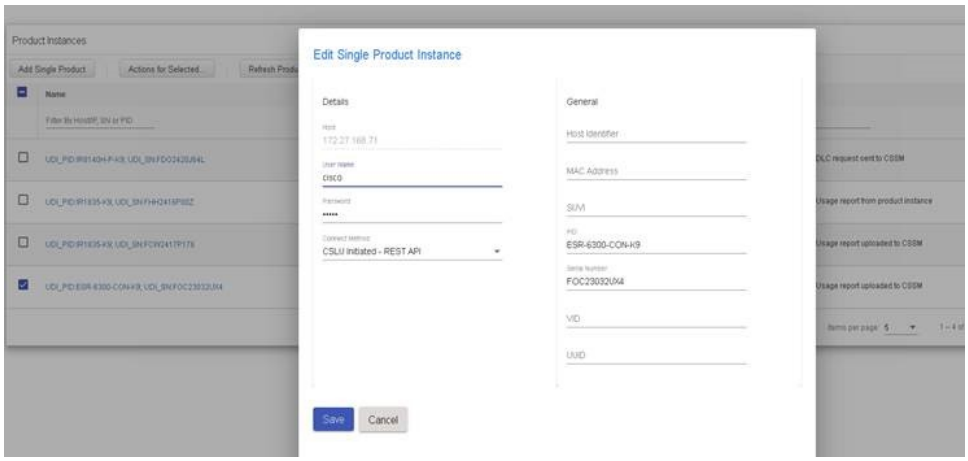
ステップ 2 [**Product Instances**] タブに移動し、[UDI] をクリックします。

図 *69 : UDI* の選択



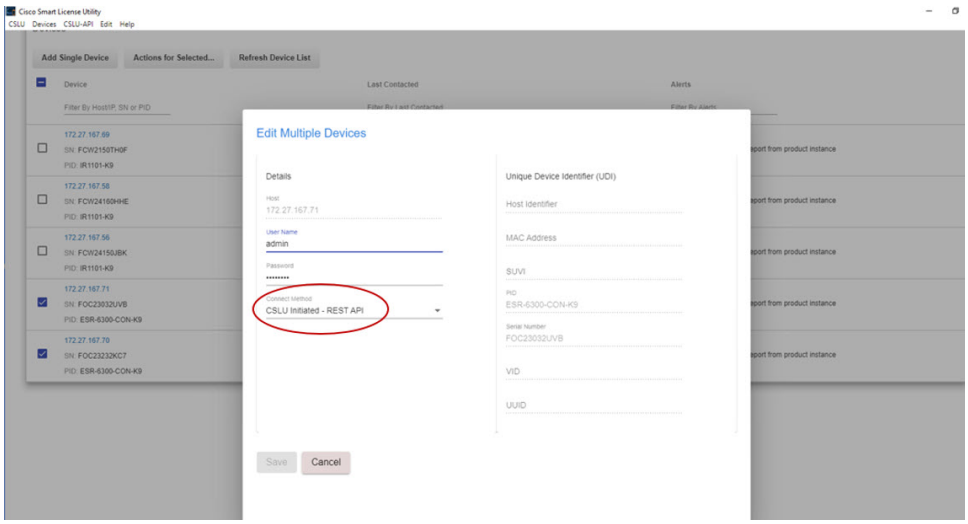
ステップ 3 [**Edit Single Product Instance**（SIP MWI notification mechanism）] ウィンドウが表示されます。

図 *70 : 1* つの製品インスタンスの編集



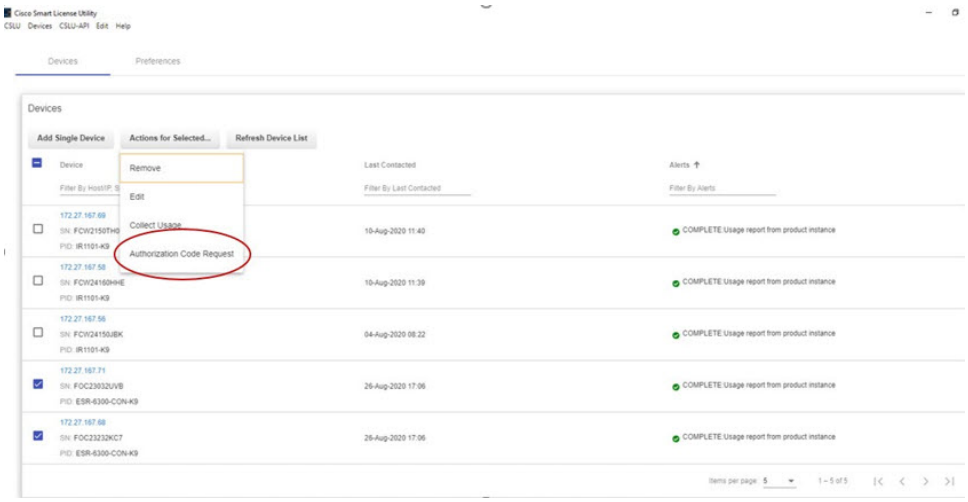
ステップ 4 [**Edit Multiple Devices**（SIP MWI notification mechanism）] ウィンドウが表示されます。アカウントのパスワードを入力して [**Save**] をクリックします。

図 *71 :* 複数のデバイスの編集



ステップ 5 [**Product Instances**] ウィンドウで、[**Actions for Selected Devices**] タブをクリックします。

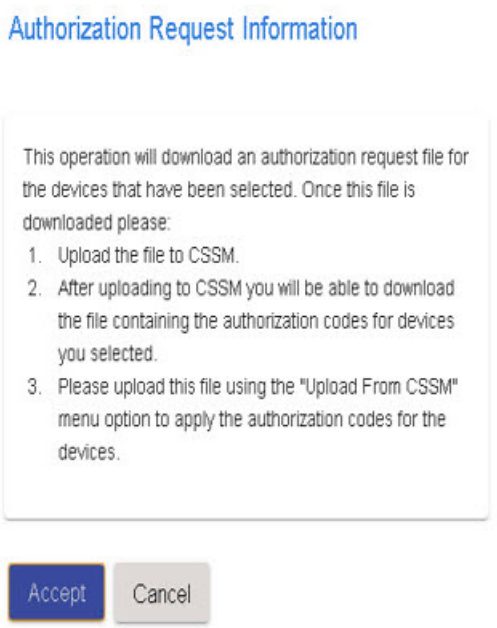
図 *72 :* 選択したデバイスに対するアクション



ステップ 6 **Authorization Code Request** を選択します。

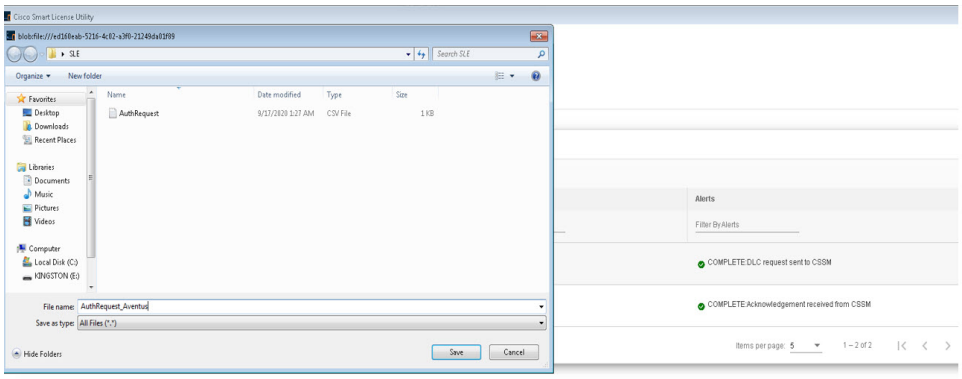
ステップ 7 [**Authorization Request Information**（SIP MWI notification mechanism）] ウィンドウが表示されます。内容を読んで [**Accept**] をクリックします。

図 *73 :* 承認要求情報



ステップ 8 CSLU がラップトップに承認要求ファイルをダウンロードします。[**Save**] をクリックします。

図 *74* : 承認要求ファイル



CSSM への AuthRequest ファイルのエクスポート

次の手順では、保存した認証要求ファイルを取得して、Cisco Smart Software Manager（CSSM）にエクスポートします。

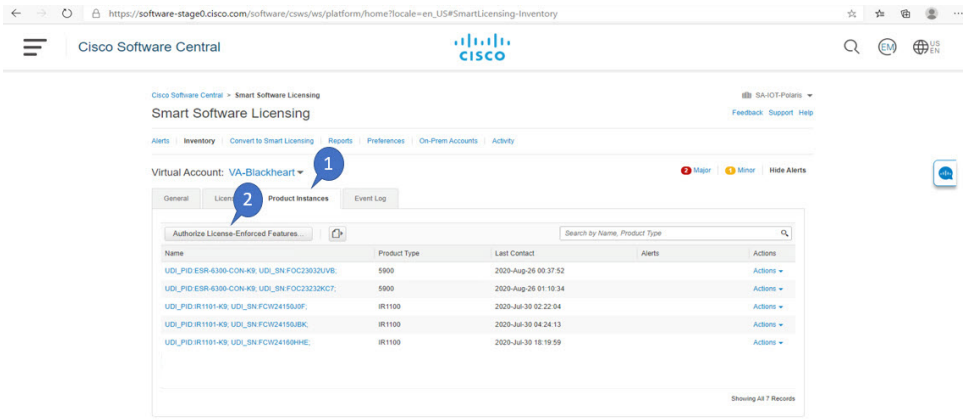
CSSM を起動します。

[**Inventory**] タブをクリックし、バーチャルアカウントを選択します。

ステップ 1　[**Product Instances**] タブをクリックします。

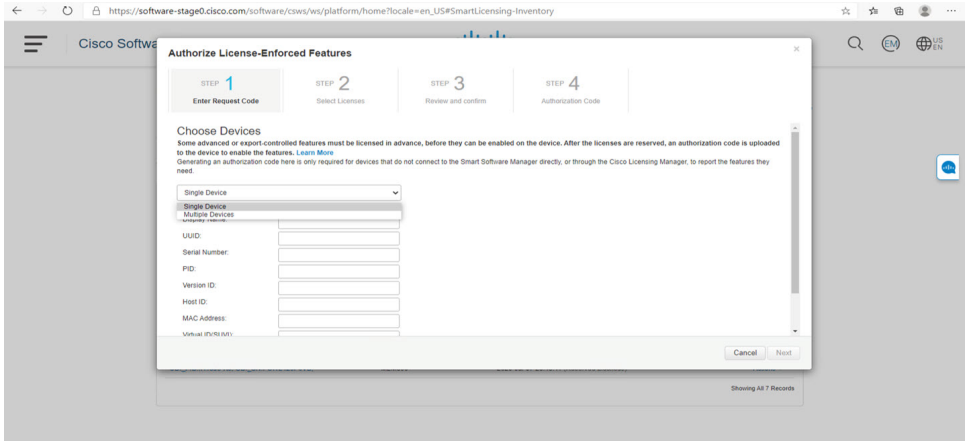
ステップ 2　[**Authorize License-Enforced Features**] をクリックします。

図 *75* : ライセンス適用機能の認証



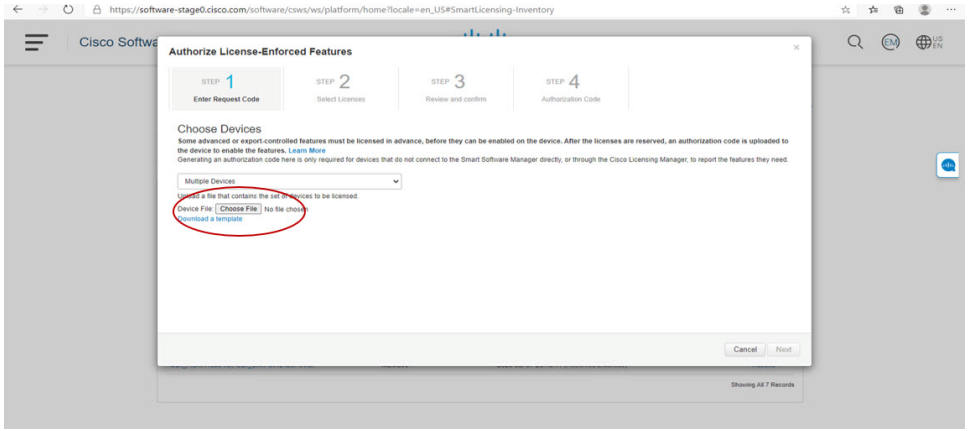
Authorize License-Enforced Features ウィンドウが表示されます.

図 *76 :* ライセンス適用機能の認証



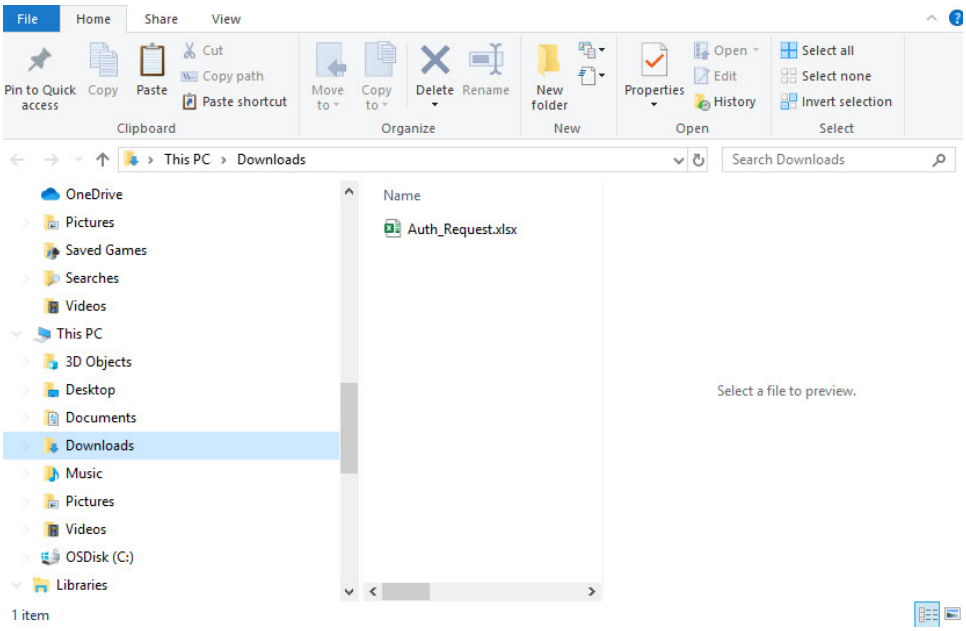
ステップ 3 プルダウンから **Multiple** または **Single** デバイスを選択します。

ステップ 4 ウィンドウが、デバイスファイルを選択するオプションに変わります。[**Choose File**] をクリックします。



ステップ 5 ラップトップで認証要求ファイルを保存した場所に移動するポップアップウィンドウが開きます。

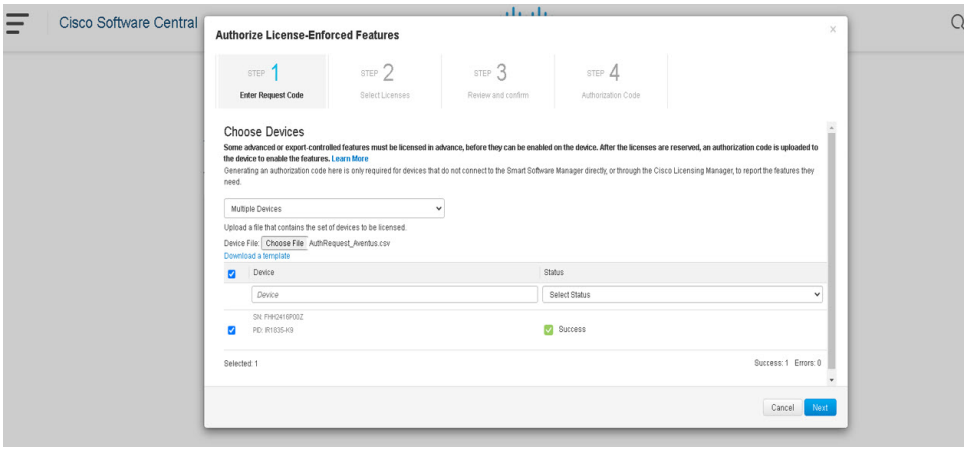
図 *77 : [File Navigation]* ウィンドウを開く



ステップ 6 ファイルを選択し、[**Open**] をクリックします。

ステップ 7 認証ファイルがロードされ、デバイスが表示されるウィンドウに変化します。

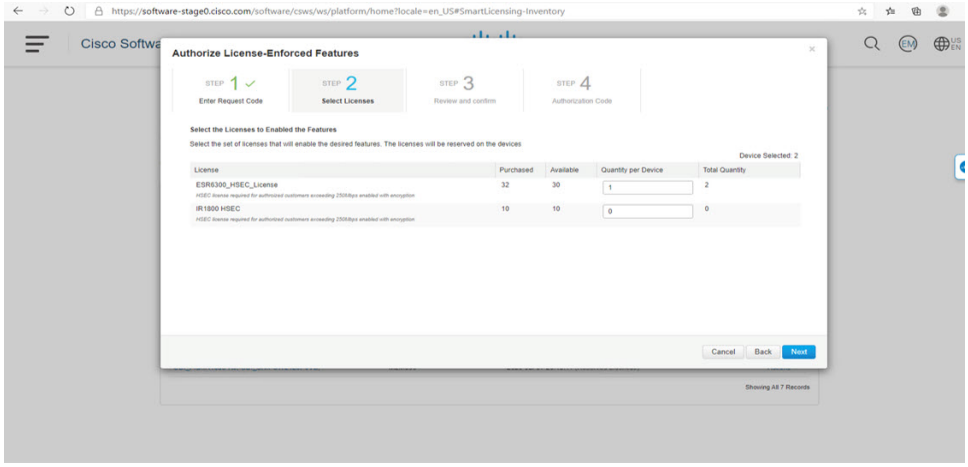
図 *78 :* デバイスの表示



ステップ 8 デバイスが表示されたら、[**Next**] をクリックします。

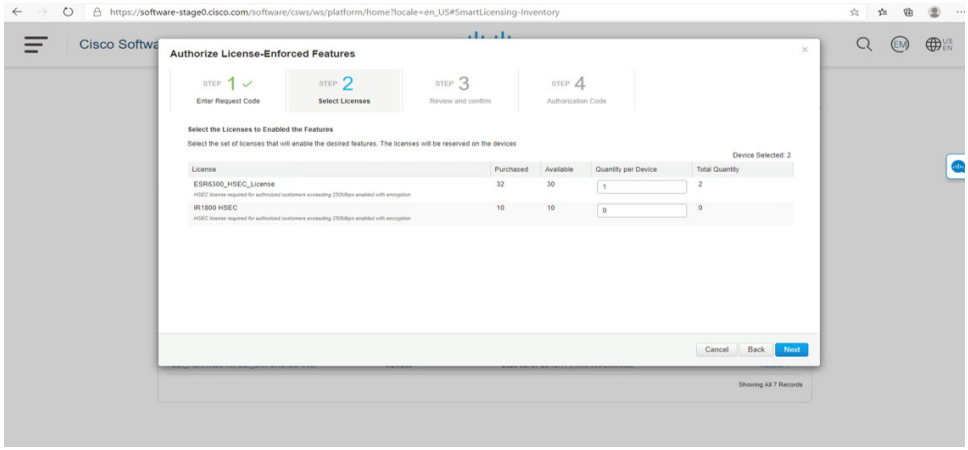
ステップ 9 [**Select Licenses**] タブが開きます。

図 *79* : ライセンスの選択



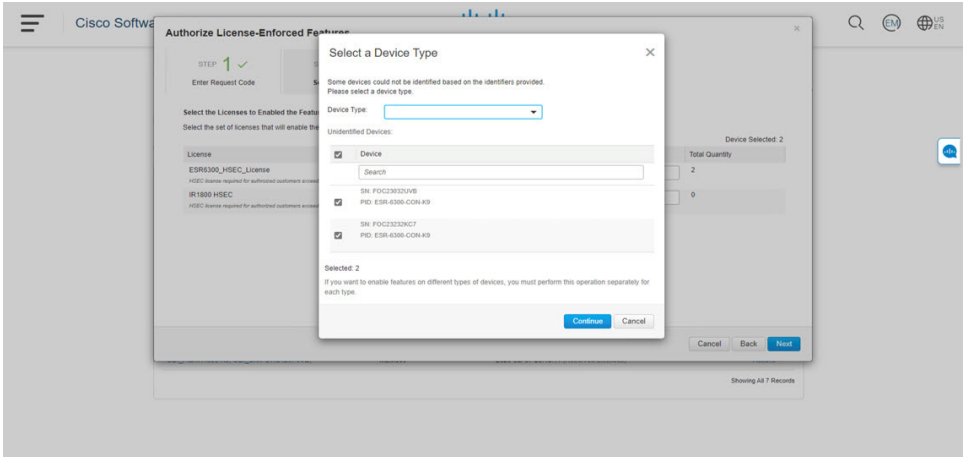
ステップ 10 **Quantity per Device** の下に、希望する数を入力します。

図 *80* : 数の入力



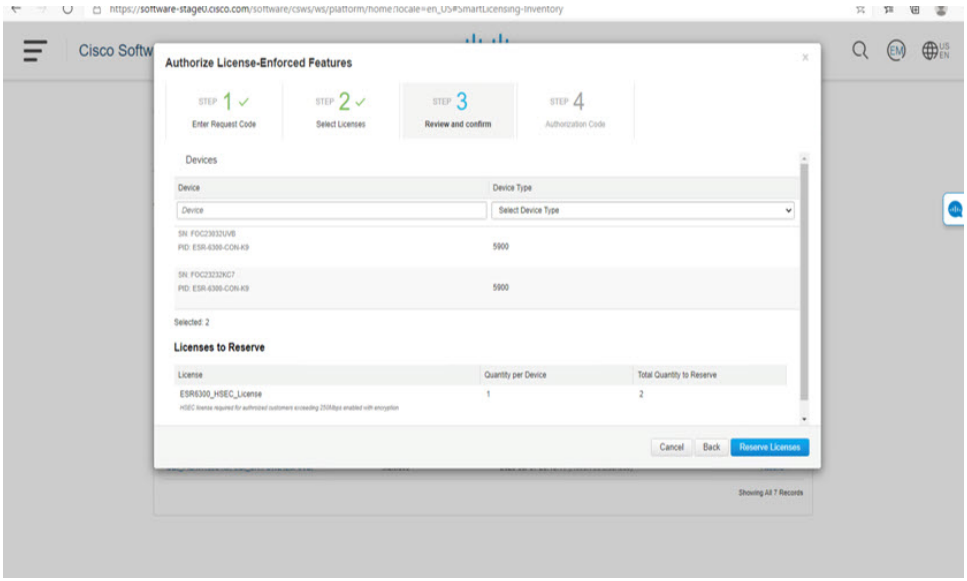
ステップ 11 CSSM が識別情報からデバイスを識別できない場合は、手動で選択できます。

図 *81* : デバイスタイプの選択



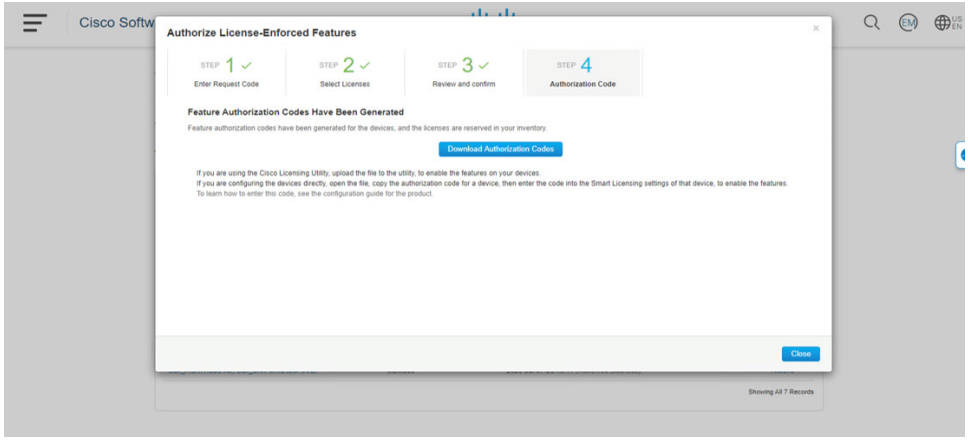
ステップ 12　[**Continue**] をクリックすると、ウィンドウが [**Review and Confirm**] に変わります。

図 *82* : 確認



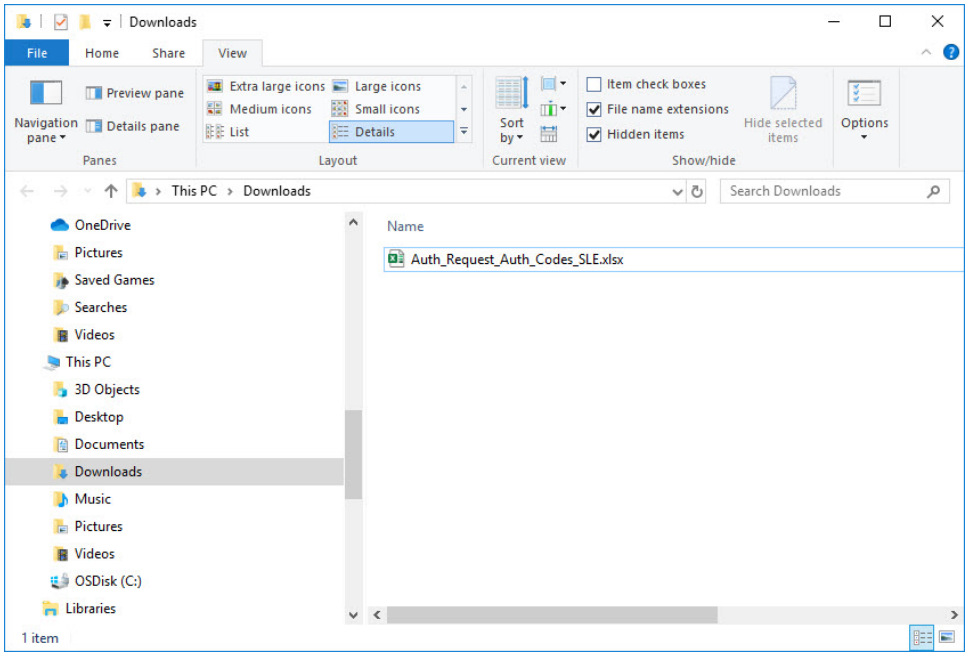
ステップ 13　**Reserve Licenses** をクリックすると、CSSM によって機能認証コードが生成されます。

図 *83* : 機能認証コード



ステップ 14 [**Download Authorization Codes**] をクリックすると、コードを保存する場所に移動するためのウィンドウが開きます。

図 *84* : 認証コードの保存



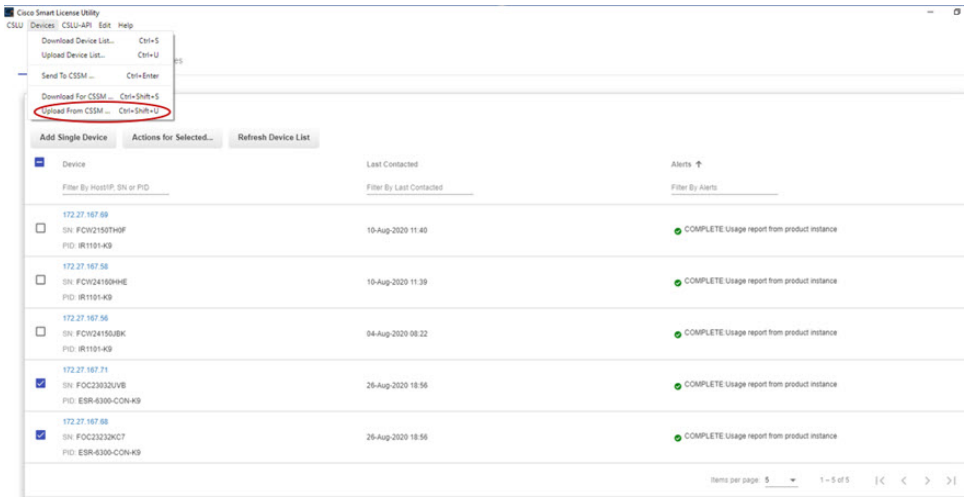
ステップ 15 [**Ok**] をクリックします。

CSLU への承認要求コードファイルのアップロード

ステップ 1 Cisco Smart License Utility（CSLU）を開きます。

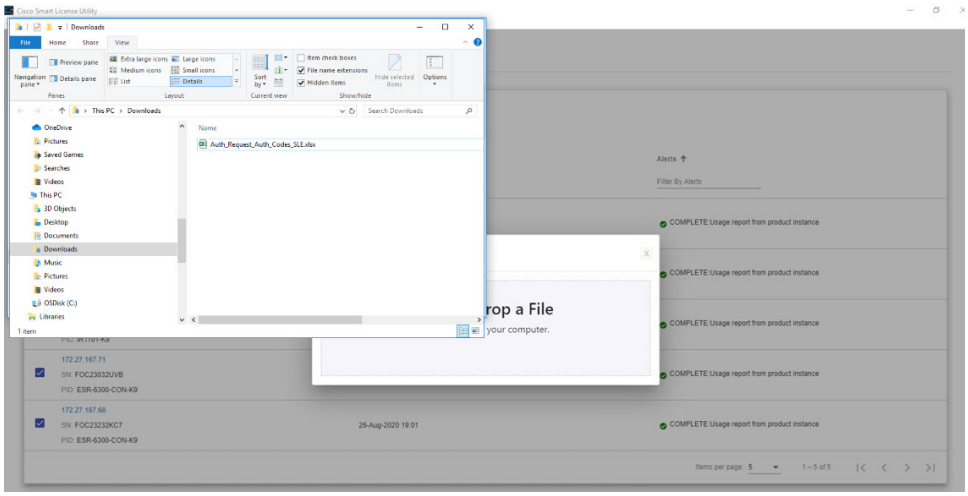
ステップ 2 **Product Instances** に移動し、**Upload From Cisco** を選択します。

図 *85 :* シスコからのアップロード



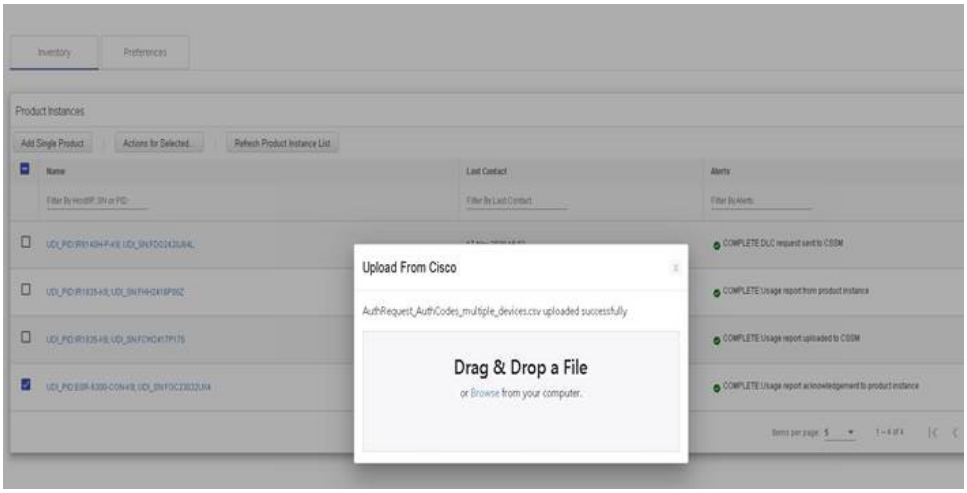
ステップ 3 ファイルをロードするオプションは 2 つあります。**Drag and Drop** するか、またはファイルを保存した場所を **Browse** します。次の例では、[Browse] を示します。

図 *86 :* ファイルの参照



ステップ 4 認証コードファイルを選択し、[**Open**] をクリックします。システムが認証コードファイルをアップロードすると、正常にアップロードされたことを示すメッセージが表示されます。

図 *87 :* 正常にアップロード



ルータでのライセンス インストール プロセス

コマンドライン インターフェイスから次の手順を実行します。

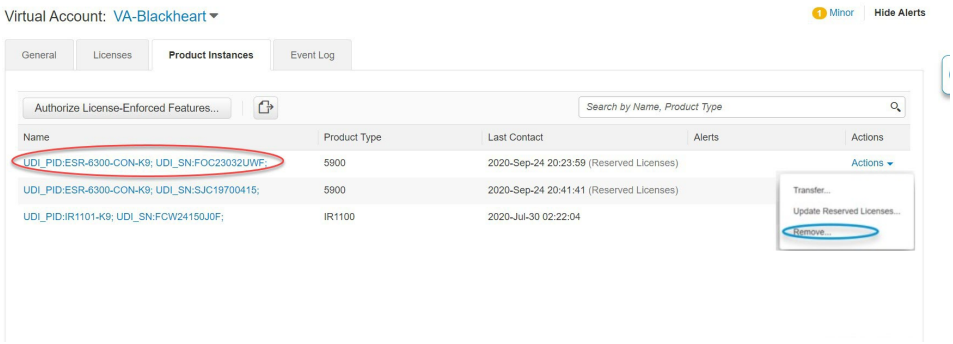
```
Router#show license summary
License Reservation is ENABLED
License Usage:
  License Entitlement tag Count Status
  network-advantage_250M (ESR6300_P_250M_E) 1 IN USE
  hseck9 (ESR6300_HSEC) 1 IN USE

Router#show license usage
License Authorization:
  Status: Not Applicable
network-advantage_250M (ESR6300_P_250M_A):
  Description: network-advantage_250M
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage_250M
  Feature Description: network-advantage_250M
  Enforcement type: NOT ENFORCED
hseck9 (ESR6300_HSEC_License):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED

Router(config)#platform hardware throughput level 2G
% Please write mem and reload
% The config will take effect on next reboot
```

```
Router(config)#end
Router#
*Sep 30 18:05:55.654: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#show license summary
License Reservation is ENABLED License Usage:
  License            Entitlement tag   Count   Status
  network-advantage_250M  (ESR6300_P_250M_A)       1      IN USE
  hseck9                  (ESR6300_HSEC_License)   1      IN USE
  network-advantage_2G    (ESR6300_P_2G_A)    1      IN USE
```

CSSM からのデバイスの削除

ステップ 1 [Product instances] タブに戻ります。デバイスを見つけます。

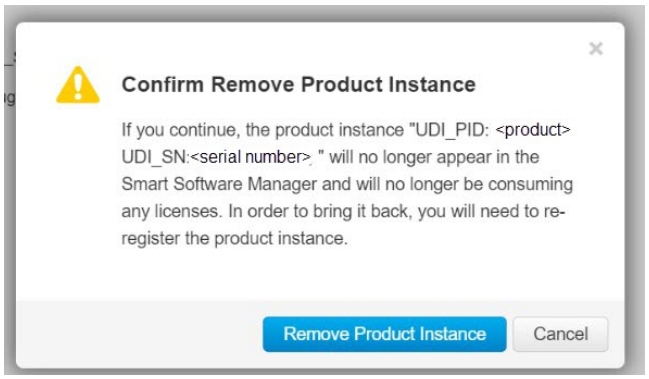
図 *88* : 製品インスタンス



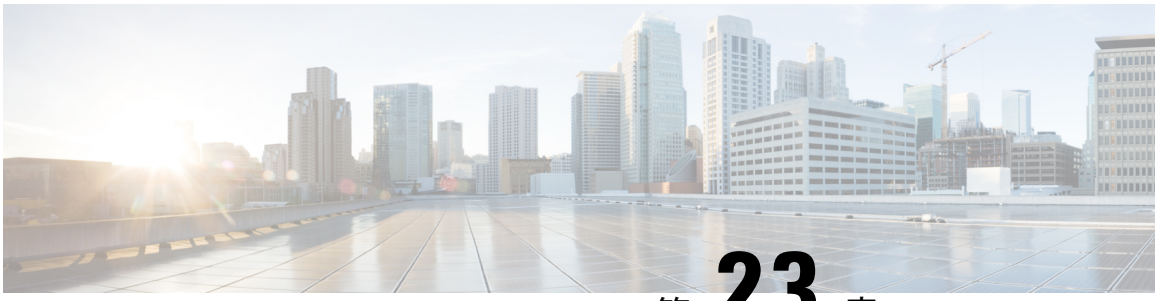
ステップ 2 デバイスの横にある [**Actions**] をクリックし、それらのオプションから [**Remove**] をクリックします。

[Confirm Remove Product Instance] ウィンドウが表示されます。

図 *89* : 製品インスタンスの削除の確認



ステップ 3 [**Remove Product Instance**] をクリックします。



第 23 章

イーサネット スイッチ ポートの設定

この章は、次の項で構成されています。

VLAN の設定

VLANは、ユーザーの物理的な位置に関係なく、機能またはアプリケーションなどで論理的に分割された、スイッチによるネットワークです。VLAN には、物理 LAN と同じ属性があります。ただし、同じ LAN セグメントに物理的に配置されていないエンドステーションもグループ化できます。どのようなデバイスポートでも VLAN に属することができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN 内のエンドステーションだけに転送またはフラッディングされます。各VLANは1つの論理ネットワークと見なされ、VLANに属さないステーション宛のパケットは、ルータまたはフォールバックブリッジングをサポートするデバイスを経由して伝送しなければなりません。デバイススタックでは、スタック全体にまたがる複数のポートで VLAN を形成できます。VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLANごとに独自のブリッジ管理情報ベース（MIB）情報があり、スパニングツリーの独自の実装をサポートできます。

VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるエンド ステーションはすべて同じ VLAN に属します。デバイス上のインターフェイスの VLAN メンバーシップは、インターフェイスごとに手動で割り当てます。この方法でデバイスインターフェイスを VLAN に割り当てた場合、これをインターフェイスベース（またはスタティック）VLAN メンバーシップと呼びます。

デバイスは、デバイス仮想インターフェイス（SVI）を使用して、VLAN 間でトラフィックをルーティングできます。VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。

アクセス ポート

アクセス ポートは（音声 VLAN ポートとして設定されている場合を除き）1 つの VLAN だけに所属し、その VLAN のトラフィックだけを伝送します。トラフィックは、VLAN タグが付いていないネイティブ形式で送受信されます。アクセス ポートに着信したトラフィックは、ポートに割り当てられている VLAN に所属すると見なされます。アクセスポートがタグ付きパケット（タグ付き IEEE 802.1Q）を受信した場合、そのパケットは廃棄され、送信元アドレスは学習されません。

トランク ポート

トランク ポートは複数の VLAN のトラフィックを伝送し、デフォルトで VLAN データベース内のすべての VLAN のメンバとなります。次のトランク ポート タイプはサポートされています。

- IEEE 802.1Q トランク ポートは、タグ付きとタグなしの両方のトラフィックを同時にサポートします。IEEE 802.1Q トランク ポートは、デフォルトのポート VLAN ID（PVID）に割り当てられ、すべてのタグなしトラフィックはポートのデフォルト PVID 上を流れます。NULL VLAN ID を備えたすべてのタグなしおよびタグ付きトラフィックは、ポートのデフォルト PVID に所属するものと見なされます。発信ポートのデフォルト PVID と等しい VLAN ID を持つパケットは、タグなしで送信されます。残りのトラフィックはすべて、VLAN タグ付きで送信されます。

デフォルトでは、トランク ポートは、VTP に認識されているすべての VLAN のメンバですが、トランク ポートごとに VLAN の許可リストを設定して、VLAN メンバーシップを制限できます。許可 VLAN のリストは、その他のポートには影響を与えませんが、対応トランク ポートには影響を与えます。デフォルトでは、使用可能なすべての VLAN（VLAN ID 1 ～ 4094）が許可リストに含まれます。トランクポートは、VTP が VLAN を認識し、VLAN が有効な状態にある場合に限り、VLAN のメンバーになることができます。VTP が新しい有効になっている VLAN を認識し、その VLAN がトランクポートの許可リストに登録されている場合、トランクポートは自動的にその VLAN のメンバになり、トラフィックはその VLAN のトランク ポート間で転送されます。VTP が、VLAN のトランクポートの許可リストに登録されていない、新しい有効な VLAN を認識した場合、ポートはその VLAN のメンバーにはならず、その VLAN のトラフィックはそのポート間で転送されません。

詳細については、『VLAN Configuration Guide, Cisco IOS XE Gibraltar 16.10.x』[英語] を参照してください。

VLAN トランキング プロトコル（VTP）

VTP は、レイヤ 2 のメッセージ プロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のスイッチ上で集中的に設定変更を行い、その変更を自動

的にネットワーク上の他のスイッチに伝達できます。VTPを使用しない場合、VLANに関する情報を他のスイッチに送信できません。VTP は、1 台のスイッチで行われた更新が VTP を介してドメイン内の他のスイッチに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のスイッチ上で同時に発生する環境の場合、VTP は適していません。VLAN データベースの不整合が生じます。

VTP の設定の詳細については、以下を参照してください。http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1046901

IEEE 802.1x ポートベースの認証の設定

IEEE 802.1x ポートベースの認証は、不正なデバイス（サプリカント）によるネットワーク アクセスを防止するためにデバイスに設定されます。デバイスでは、固定構成やインストールされているモジュールに基づいて、ルータ、スイッチ、およびアクセスポイントの機能を組み合わせることができます。スイッチ機能は、組み込みスイッチ ポートまたはスイッチ ポート付きプラグインモジュールのいずれかにより提供されます。この機能は、アクセスポートとトランクポートの両方をサポートします。802.1Xポートベース認証の詳細については、『Configuring IEEE 802.1X Port-Based Authentication Guide』[英語] を参照してください。

スパニングツリー プロトコルの設定

スパニングツリープロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ2リンク管理プロトコルです。レイヤ2イーサネットネットワークの正常な動作を実現するには、どの2つのステーション間でもアクティブパスを1つにする必要があります。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。また、スイッチも複数のレイヤ2インターフェイスのエンドステーション MAC アドレスを学習する可能性が出てきます。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンドステーション側で、単一 LAN セグメントに接続されているのか、複数セグメントからなるスイッチド LAN に接続されているのかを検出することはできません。

STPは、スパニングツリーアルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを1つ選択します。スパニングツリーアルゴリズムは、アクティブトポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチドレイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートが指定ポートの役割またはバックアップポートの役割にであるようなスイッチはルートスイッチです。少なくとも 1 つのポートが指定ポートの役割のスイッチは、指定スイッチと呼ばれます。スパニングツリーは、冗長データパスを強制的にスタンバイ（ブロック）ステートにします。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリー アルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、定期的にブリッジ プロトコルデータ ユニット（BPDU）と呼ばれるスパニングツリー フレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。BPDUには、送信側スイッチおよびそのポートについて、スイッチおよびMACアドレス、スイッチ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

スイッチの 2 つのポートがループの一部になっている場合、スパニングツリー ポート プライオリティとパス コストの設定値によって、どちらのポートをフォワーディング ステートにするか、どちらをブロッキング ステートにするかが制御されます。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。パス コストの値は、メディアの速度を表します。

STP の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4_8PortGENIM.html#pgfId-1079138

例：スパニングツリー プロトコルの設定

次に、ギガビット イーサネット インターフェイスのスパニングツリー ポート プライオリティの設定の例を示します。ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。

```
Router# configure terminal
Router(config)# interface FastEthernet 0/0/1
Router(config-if)# spanning-tree vlan 1 port-priority 64
Router(config-if)# end
```

ギガビット イーサネット インターフェイスのスパニングツリー ポート コストを変更する方法の例を示します。ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。

```
Router#configure terminal
Router(config)# interface FastEthernet 0/0/1
Router(config-if)# spanning-tree cost 18
Router(config-if)# end
```

VLAN 10 のブリッジ プライオリティを 33792 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 priority 33792
Router(config)# end
```

VLAN 10 の hello タイムを 7 秒に設定する例を示します。hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 hello-time 7
Router(config)# end
```

転送遅延時間を設定する例を示します。転送遅延時間は、スパニングツリー ラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 forward-time 21
Router(config)# end
```

スパニング ツリーの最大エージング インターバルの設定の例を示します。最大エージング タイムは、再設定を試行するまでにスイッチがスパニングツリー コンフィギュレーション メッセージを受信せずに待機する秒数です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 max-age 36
Router(config)# end
```

スイッチを VLAN 10 のルート ブリッジとして設定し、ネットワークの直径を 4 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# exit
```

MAC アドレス テーブル操作の設定

MAC アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス：スイッチが学習し、使用されなくなった時点でドロップされる送信元 MAC アドレス。エージング タイム設定を使用して、テーブル内で使用されていないアドレスをスイッチが保持する期間を定義します。
- スタティック アドレス：手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャスト アドレス。

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、アドレスに対応付けられたポート、およびタイプ（スタティックまたはダイナミック）のリストです。

セキュア MAC アドレスの有効化、スタティック エントリの作成、セキュア MAC アドレス最大数の設定、エージング タイムの設定の例については、「例：MAC アドレス テーブル操作」を参照してください。

MAC アドレス テーブルの操作の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1048223

例：MAC アドレス テーブル操作

次に、MAC アドレス テーブルにスタティック エントリを作成する例を示します。

```
Router# configure terminal
Router(config)# mac address-table static 0002.0003.0004 interface FastEthernet 0/0/1
vlan 3
Router(config)# end
```

次に、エージング タイマーを設定する例を示します。

```
Router# configure terminal
Router(config)# mac address-table aging-time 300
Router(config)# end
```

スイッチ ポート アナライザの設定

Cisco IR1101 がサポートしているのは、ローカル SPAN のみ、かつ最大 1 つの SPAN セッションです。ポートを通過するネットワーク トラフィックを解析するには、SPAN を使用して、そのスイッチ上の別のポート、またはネットワーク アナライザやその他のモニタ デバイスもしくはセキュリティ デバイスに接続されている別のスイッチ上のポートに、トラフィックのコピーを送信します。SPAN は送信元ポート上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は発信元ポート上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元に出入りするトラフィックだけです。送信元にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の送信元からルーティングされているトラフィックはモニタできません。ただし、送信元で受信し、別の送信元にルーティングされるトラフィックは、モニタできます。

スイッチド ポート アナライザ（SPAN）セッションの設定方法については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swspan.html

例：SPAN の設定

ギガビット イーサネット送信元インターフェイスからの双方向トラフィックをモニタするように SPAN セッションを設定する方法の例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 source FastEthernet 0/0/1
Router(config)# end
```

ギガビット イーサネット インターフェイスを SPAN セッションの宛先として設定する方法の例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 destination FastEthernet 0/0/1
Router(config)# end
```

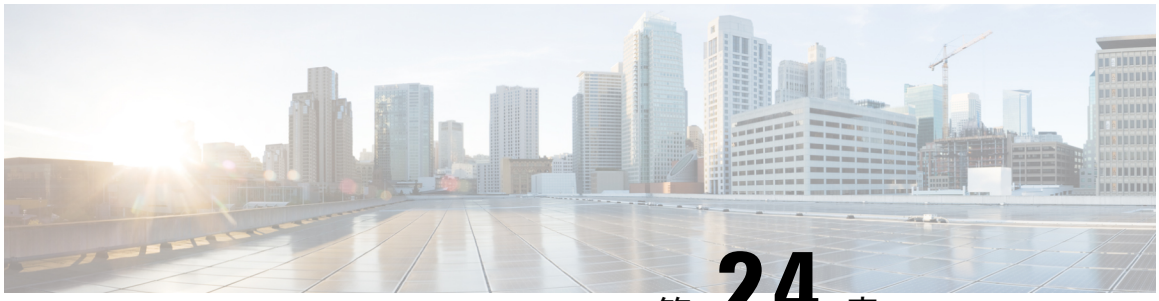
SPAN セッション 1 の SPAN 送信元としてのギガビット イーサネットを削除する方法の例を示します。

```
Router# configure terminal
Router(config)# no monitor session 1 source FastEthernet 0/0/1
Router(config)# end
```

IPv4 用 IGMP スヌーピング

IGMP スヌーピングにより、スイッチで IGMP パケットを調べたり、パケットの内容に基づいて転送先を決定したりできます。IGMP または IGMP スヌーピング クエリアからの IGMP クエリーを受信するサブネットで、IGMP スヌーピングを使用するように、スイッチを設定できます。IGMP スヌーピングは、IPv4 マルチキャスト トラフィックを受信するポートだけにそのトラフィックをダイナミックに転送するように、レイヤ 2 LAN ポートを設定することにより、レイヤ 2 で IPv4 マルチキャスト トラフィックを抑制します。

レイヤ 2 スイッチは IGMP スヌーピングを使用して、レイヤ 2 インターフェイスを動的に設定し、マルチキャスト トラフィックが IP マルチキャスト デバイスと対応付けられたインターフェイスにのみ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを制限できます。名称が示すとおり、IGMP スヌーピングの場合は、LAN スイッチでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャスト グループとメンバ ポートを追跡する必要があります。特定のマルチキャスト グループについて、ホストから IGMP レポートを受信したスイッチは、ホストのポート番号を転送テーブル エントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブル エントリからホスト ポートを削除します。マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。この機能の詳細については、https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/snooigmp.html [英語] を参照してください。



第 24 章

セルラー プラガブル インターフェイス モジュール設定ガイド

「Cisco 4G LTE-Advanced Configuration」の章は『Cellular Pluggable Interface Module Configuration Guide』という新しい独立したガイドに置き換えられました。このガイドには、Cisco Cellular PIM の使用に関するあらゆる最新情報が含まれています。

第 25 章

SCADA に関する情報

この章は、次の項で構成されています。

SCADA の概要

SCADA は、水管理、電力、製造業などの業界で採用されている制御システムおよび管理システムを意味します。SCADA システムは、システム内のさまざまなタイプの機器からデータを収集し、その情報をコントロール センターに転送して分析します。一般に、コントロール センターの担当者が、SCADA システムのアクティビティをモニタし、必要に応じて介入します。

リモート端末ユニット（RTU）は、SCADA システム内のプライマリ制御システムとして機能します。RTU は、SCADA システム内の特定の機能を制御するように設定されています。これは、ユーザ インターフェイスを使って必要に応じて変更できます。

IR1101 では、回線は非同期インターフェイスと同じ 0/2/0 です。

IR1101 の役割

ネットワークでは、コントロール センターは常に、IR1101 との通信時にネットワーク内のマスターとして機能します。IR1101 は、RTU と通信するときにコントロール センターのプロキシ マスターステーションとして機能します。

IR1101 は、次を実行するために SCADA ゲートウェイとして機能するプロトコル変換を提供します。

- RTU からデータを受信し、コントロール センターから RTU に設定コマンドを中継する。
- コントロールセンターから設定コマンドを受信し、RTUデータをコントロールセンターに中継する。
- RTU がオフラインのときは、コントロール センターから受信する要求を終端する。

IR1101 は、次のプロトコルに対してプロトコル変換を実行します。

- IEC 60870 T101 と IEC 60870 T104 の送受信。
- DNP3 シリアルから DNP3 IP へ

主な用語

IR1101 で T101 および T104 プロトコル スタックを設定する場合は、次の用語が関係します。

- チャネル：各 IR1101 シリアル ポート インターフェイスでチャネルが設定されており、リモート コントロール センターへの各 IP 接続に単一の RTU への接続が提供されます。各接続は、単一の T101（RTU）または T104（コントロール センター）プロトコル スタックを転送します。
- リンク アドレス：デバイスまたはステーションのアドレスです。
- リンク モード（平衡型および非平衡型）：データ転送のモードです。
  - 非平衡型の設定とは、マスターから開始されたデータ転送を指します。
  - 平衡型の設定は、マスターまたはスレーブが開始したデータ転送のいずれかを指します。
- セクター： リモート サイト内の単一の RTU を指します。
- セッション：リモート サイトへの単一の接続を表します。

IR1101 で DNP3 プロトコル スタックを設定する場合は、次の用語が関係します。

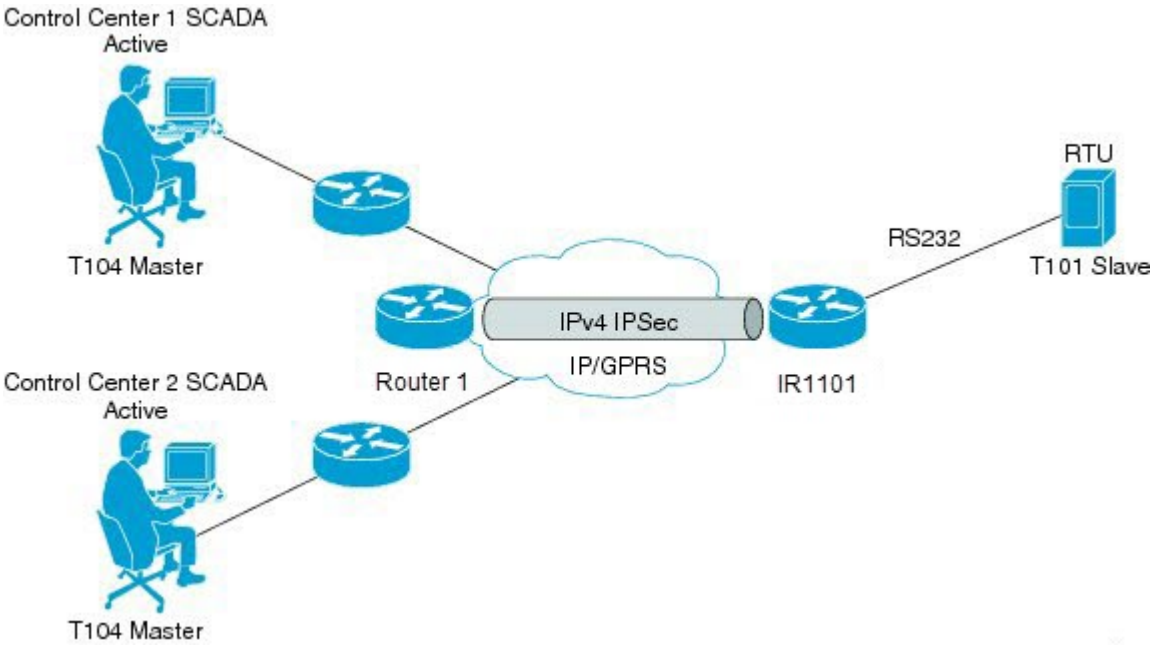
- チャネル：IR1101 シリアル ポート インターフェイスでチャネルが設定されており、リモート コントロール センターへの各 IP 接続に単一の RTU への接続が提供されます。各接続は、単一の DNP3 シリアル（RTU）または DNP3 IP（コントロール センター）プロトコル スタックを転送します。
- リンク アドレス：デバイスまたはステーションのアドレスです。
- セッション：リモート サイトへの単一の接続を表します。

プロトコル変換アプリケーション

図 90 : SCADA システム内のルータ （269 ページ） では、（配電ネットワークの二次変電所内にインストールされた）IR1101 は、プロトコル変換を使用して、SCADA システム内のコントロール センターと RTU 間のセキュアなエンドツーエンド接続を提供しています。

IR1101 は、RS232 接続を介して RTU（スレーブ）に接続します。パブリック インフラストラクチャ（セルラーなど）を介して転送されたトラフィックを保護するため、IR1101 は、RTU から SCADA データを、IPSec トンネル（FlexVPN サイト間またはハブ アンド スポーク）を介して SCADA システムのコントロール センターに転送します。IPSec トンネルは、IR1101 とヘッドエンドアグリゲーション ルータ間のすべてのトラフィックを保護します。SCADA トラフィックは、適切なコントロール センターに転送される前に、SCADA トラフィックのパスに配置された IPS デバイスで点検できます。

図 *90 : SCADA* システム内のルータ



前提条件

RTU がネットワークで設定され、動作している必要があります。

IR1101 に接続する RTU ごとに、T101/T104 に関する次の情報が必要になります。

- チャネル情報
  - チャネル名
  - 接続タイプ：シリアル
  - リンク送信手順の設定：平衡型または非平衡型

- リンクのアドレス フィールド（オクテットで表される番号）

- セッション情報
  - セッション名
  - アプリケーション サービス データ ユニット（ASDU）の共通アドレスのサイズ （オクテットで表される数値）
  - 送信原因（COT）のサイズ（オクテットで表される数値）
  - Information Object Address（IOA）のサイズ（オクテットで表される数値）
- セクター情報
  - セクター名
  - ASDU アドレス（オクテットで表される番号）

IR1101 に接続する RTU ごとに、DNP3 に関する次の情報が必要になります。

- チャネル情報
  - チャネル名
  - 接続タイプ：シリアル
  - リンク アドレス
- セッション情報
  - セッション名

注意事項と制約事項

各チャネルは 1 つのセッションのみをサポートします。

各セッションは 1 つのセクターのみをサポートします。

デフォルト設定

T101/T104 パラメータ	デフォルト
T101 の役割	マスター
T104 の役割	スレーブ

DNP3 パラメータ	デフォルト
未承認応答（DNP3-serial）	有効になっていません
未承認メッセージの送信（DNP3-IP）	有効

プロトコル変換の設定

この項では、次のトピックについて取り上げます。

（注） プロトコル変換で動作する IR1101 の設定を変更する前に、プロトコル変換エンジンの開始と停止 （286 ページ） のセクションを参照してください。

IR1101 シリアル ポートと SCADA カプセル化の有効化

IR1101 でプロトコル変換を有効にして設定するには、その前に IR1101 のシリアルポートを有効にし、そのポートで SCADA カプセル化を有効にする必要があります。

始める前に

IR1101 のシリアル ポートの可用性を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**interface async** *slot/port/interface*	async slot/port/interface のコマンド モードを開始します。 *slot*：値 0 *port*：値 2 *interface*：値 0
ステップ 3	**no shutdown**	管理上ポートを稼働させます。
ステップ 4	encapsulation scada	プロトコル変換およびその他の SCADA プロトコルのシリアルポートでのカプセル化を有効にします。

例

次の例は、シリアル ポート 0/2/0 を有効にし、そのインターフェイスでカプセル化を有効にして SCADA プロトコルをサポートする方法を示しています。

```
router# configure terminal
router(config)# interface async 0/2/0
router (config-if)# no shutdown
router (config-if)# encapsulation scada
```

T101 および T104 プロトコル スタックの設定

scada システム内のコントロールセンター（T104）と RTU（T101）間のエンドツーエンド通信を可能にする T101 および T104 プロトコル スタックを設定できます。

- T101 プロトコル スタックの設定 （272 ページ）
- T104 プロトコル スタックの設定 （275 ページ）
- プロトコル変換エンジンの開始と停止 （286 ページ）

前提条件

すべての必要な設定情報が収集されていることを確認します。

シリアル ポートと SCADA カプセル化を有効にします。

T101 プロトコル スタックの設定

T101 プロトコル スタックのチャネル、セッション、およびセクター パラメータを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**scada-gw protocol t101**	T101 プロトコルのコンフィギュレーション モードを開始します。
ステップ 3	**channel** *channel_name*	T101 プロトコルのチャネル コンフィギュレーション モードを開始します。 *channel_name*：IR1101 のシリアル ポートと RTU とが通信するチャネルを示します。 （注） 入力したチャネル名が存在しない場合、ルータは新しいチャネルを作成します。 このコマンド **no** の形式を入力すると、既存のチャネルが削除されます。ただし、チャネルを削除するには、すべてのセッションを削除する必要があります。
ステップ 4	**role master**	マスター ロールを T101 プロトコル チャネルに割り当てます（デフォルト）。
ステップ 5	link-mode {balanced | unbalanced}	リンク モードを平衡型または非平衡型のいずれかに設定します。

	コマンドまたはアクション	目的
		非平衡型：マスターから開始されたデータ転送を意味します。 平衡型：マスターまたはスレーブのいずれかのデータ転送を意味します。
ステップ 6	**link-addr-size {none | one | two}**	リンク アドレス サイズをオクテット単位で定義します。
ステップ 7	**bind-to-interface async** *slot/port/interface*	システムが T101 プロトコル トラフィックを送信する IR1101 シリアル インターフェイスを定義します。 *slot*：値 0 *port*：値 2 *interface*：値 0
ステップ 8	**exit**	チャネルの設定を終了し、チャネル コンフィギュレーション モードを終了します。すべての設定を保存します。
ステップ 9	**session** *session_name*	セッション コンフィギュレーション モードを開始し、セッションに名前を割り当てます。
ステップ 10	**attach-to-channel** *channel_name*	セッションをチャネルに接続します。 ステップ 3 で入力したのと同じチャネル名を使用します。 *channel_name*：チャネルを識別します。
ステップ 11	common-addr-size **{one | two | three}**	共通アドレス サイズをオクテット単位で定義します。
ステップ 12	cot size **{one | two | three}**	自発的または巡回データ スキームなどの送信原因をオクテット単位で定義します。
ステップ 13	info-obj-addr-size **{one | two | three}**	情報オブジェクト要素のアドレスサイズをオクテット単位で定義します。
ステップ 14	**link-addr-size {one | two | three}**	リンク アドレス サイズをオクテット単位で定義します。
ステップ 15	**link-addr** *link_address*	RTU のリンク アドレスを意味します。

	コマンドまたはアクション	目的
		（注） ここで入力したリンク アドレスは、シリアル ポートが接続する RTU で設定された値と一致している必要があります。 *link_address*：0 ～ 65535 の範囲。
ステップ 16	**exit**	セッション コンフィギュレーション モードを終了します。
ステップ 17	**sector** *sector_name*	セクターコンフィギュレーションモードを開始し、RTU のセクターに名前を割り当てます。 *sector_name*：セクターを識別します。
ステップ 18	**attach-to-session** *session_name*	RTU セクターをセッションに接続します。 ステップ 9 で入力したのと同じセッション名を使用します。 *session_name*：セッションを識別します。
ステップ 19	**asdu-addr** *asdu_address*	RTU の ASDU 構造アドレスを意味します。
ステップ 20	**exit**	セクター コンフィギュレーション モードを終了します。
ステップ 21	**exit**	プロトコル コンフィギュレーション モードを終了します。

例

次の例は、*RTU_10* の T101 プロトコル スタックのパラメータを設定する方法を示しています。

```
router# configure terminal
router(config)# scada-gw protocol t101
router(config-t101)# channel rtu_channel
router(config-t101-channel)# role master
router(config-t101-channel)# link-mode unbalanced
router(config-t101-channel)# link-addr-size
 one
router(config-t101-channel)# bind-to-interface async 0/2/0
router(config-t101-channel)# exit
router(config-t101)# session rtu_session
router(config-t101-session)# attach-to-channel rtu_channel
router(config-t101-session)# common-addr-size two
router(config-t101-session)# cot-size one
router(config-t101-session)# info-obj-addr-size two
router(config-t101-session)# link-addr 3
router(config-t101-session)# exit
router(config-t101)# sector rtu_sector
router(config-t101-sector)# attach-to-session rtu_session
```

```
router(config-t101-sector)# asdu-addr 3
router(config-t101-sector)# exit
router(config-t101)# exit
router(config)#
```

T104 プロトコル スタックの設定

T104 プロトコルを介して接続するコントロール センターごとに、次の手順を実行します。

始める前に

すべての必要な設定情報が収集されていることを確認します。（「前提条件 （269 ページ）」を参照）。

シリアル ポートと SCADA カプセル化を有効にします。（「IR1101 シリアル ポートと SCADA カプセル化の有効化 （271 ページ）」を参照）。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	**scada-gw protocol t104**	T104 プロトコルのコンフィギュレーション モードを開始します。
ステップ 3	**channel** *channel_name*	T104 プロトコルのチャネル コンフィギュレーション モードを開始します。 *channel_name*：ルータがコントロール センターと通信するチャネルを識別します。 （注） 入力したチャネル名が存在しない場合、ルータは新しいチャネルを作成します。 このコマンド **no** の形式を入力すると、既存のチャネルが削除されます。ただし、チャネルを削除するには、すべてのセッションを削除する必要があります。
ステップ 4	**k-value** *value*	チャネルの未処理のアプリケーション プロトコル データ ユニット（APDU）の最大数を設定します。 （注） APDU には、APDU とコントロール ヘッダーが組み込まれています。 *value*：値の範囲は 1 ～ 32767 です。デフォルト値は 12 APDU です。
ステップ 5	**w-value** *value*	チャネルの APDU の最大数を設定します。

	コマンドまたはアクション	目的
		value：値の範囲は 1 ～ 32767 です。デフォルト値は 8 APDU です。
ステップ 6	**t0-timeout** *value*	T104 チャネルの接続確立の t0-timeout 値を定義します。
ステップ 7	**t1-timeout** *value*	T104 チャネルの送信またはテスト APDU の t1-timeout 値を定義します。
ステップ 8	**t2-timeout** *value*	ルータがデータ メッセージを受信しない場合の確認応答のための t2-timeout 値を定義します。 （注） t2 値には、常に T104 チャネルの t1 値よりも小さい値を設定する必要があります。
ステップ 9	**t3-timeout** *value*	T104 チャネルが長いアイドル状態の場合に、S フレームを送信する t3-timeout 値を定義します。 （注） t3 値は、常に T104 チャネルの t1 値よりも高い値に設定する必要があります。
ステップ 10	**tcp-connection {0|1} local-port** {*port_number* | **default**} **remote-ip** {*A.B.C.D* | *A.B.C.D/LEN* | **any**} **[vrf** *WORD***]**	冗長コントロール センターが存在する設定では、プライマリ コントロール センターで定義されたようにセカンダリ コントロール センターの接続値を設定します。 *port-number*：2000 ～ 65535 の間の値。 デフォルト値 2404。 *A.B.C.D*：単一ホスト。 *A.B.C.D/nn*：サブネット A.B.C.D/LEN。 any：任意のリモート ホスト 0.0.0.0/0。 WORD：VRF 名。
ステップ 11	**exit**	チャネル コンフィギュレーション モードを終了します。
ステップ 12	**session** *session_name*	セッション コンフィギュレーション モードを開始し、セッションに名前を割り当てます。 *session_name*：ステップ 3 でチャネルに割り当てたのと同じ名前を使用します。
ステップ 13	**attach-to-channel** *channel_name*	セッション トラフィックを転送するチャネルの名前を定義します。

	コマンドまたはアクション	目的
ステップ 14	cot size **{one | two | three}**	自発的または巡回データ スキームなどの送信原因（cot）をオクテット単位で定義します。
ステップ 15	**exit**	セッション コンフィギュレーション モードを終了します。
ステップ 16	**sector** *sector_name*	セクターコンフィギュレーションモードを開始し、コントロール センターのセクターに名前を割り当てます。
ステップ 17	**attach-to-session** *session_name*	コントロール センターのセクターをチャネルに接続します。 *session_name*：ステップ 3 でチャネルに割り当てたのと同じ名前を使用します。
ステップ 18	**asdu-addr** *asdu_address*	ASDU構造アドレスを意味します。ここで入力した値は、RTUのASDU値と一致する必要があります。 *asdu_address –asdu_address*：値は 1 または 2。
ステップ 19	**map-to-sector** *sector_name*	コントロール センター（T104）のセクターを RTU（T101）セクターにマッピングします。
ステップ 20	ステップ 1 に戻ります。	ネットワーク内でアクティブになっているコントロール センターごとに、このセクションのすべての手順を繰り返します。

例

次の例は、コントロール センター *1* とコントロール センター *2*（どちらもマスターとして設定）で T104 プロトコル スタックのパラメータを設定し、T104 セクターを T101 セクターにマッピングする方法を示しています。

コントロール センター 1（*cc_master1*）を設定するには、次のコマンドを入力します。

```
router# configure terminal
router(config)# scada-gw protocol t104
router(config-t104)# channel cc_master1
router(config-t104-channel)# k-value 12
router(config-t104-channel)# w-value 8
router(config-t104-channel)# t0-timeout 30
router(config-t104-channel)# t1-timeout 15
router(config-t104-channel)# t2-timeout 10
router(config-t104-channel)# t3-timeout 30
router(config-t104-channel)# tcp-connection 0 local-port 2050 remote-ip 209.165.200.225
router(config-t104-channel)# tcp-connection 1 local-port 2051 remote-ip 209.165.201.25
router(config-t104-channel)# exit
router(config-t104)# session
 cc_master1
```

```
router(config-t104-session)# attach-to-channel cc_master1
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master1-sector
router(config-t104-sector)# attach-to-session cc_master1
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104)# exit
router(config)#
```

コントロール センター 2（*cc_master2*）を設定するには、次のコマンドを入力します。

```
router(config)# scada-gw protocol t104
router(config-t104)# channel cc_master2
router(config-t104-channel)# k-value 12
router(config-t104-channel)# w-value 8
router(config-t104-channel)# t0-timeout 30
router(config-t104-channel)# t1-timeout 15
router(config-t104-channel)# t2-timeout 10
router(config-t104-channel)# t3-timeout 30
router(config-t104-channel)# tcp-connection 0 local-port 2060 remote-ip 209.165.201.237
router(config-t104-channel)# tcp-connection 1 local-port 2061 remote-ip 209.165.200.27
router(config-t104-channel)# exit
router(config-t104)# session
 cc_master2
router(config-t104-session)# attach-to-channel cc_master2
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master2-sector
router(config-t104-sector)# attach-to-session cc_master2
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104-sector)# exit
router(config-t104)# exit
router(config)#
```

設定例

次の例は、T101 接続用のシリアル ポート インターフェイスの設定、T101 および T104 プロトコル スタックの設定、および IR1101 でプロトコル変換エンジンを開始する方法を示しています。

```
router# configure terminal
router(config)# interface async 0/2/0
router (config-if)# no shutdown
router (config-if)# encapsulation scada
router (config-if)# exit
router(config)# scada-gw protocol t101
router(config-t101)# channel rtu_channel
router(config-t101-channel)# role master
router(config-t101-channel)# link-mode unbalanced
router(config-t101-channel)# link-addr-size
 one
router(config-t101-channel)# bind-to-interface async 0/2/0
router(config-t101-channel)# exit
router(config-t101)# session rtu_session
router(config-t101-session)# attach-to-channel rtu_channel
```

```
router(config-t101-session)# common-addr-size two
router(config-t101-session)# cot-size one
router(config-t101-session)# info-obj-addr-size two
router(config-t101-session)# link-addr 3
router(config-t101-session)# exit
router(config-t101)# sector rtu_sector
router(config-t101-sector)# attach-to-session rtu_session
router(config-t101-sector)# asdu-addr 3
router(config-t101-sector)# exit
router(config-t101)# exit
router(config)# scada-gw protocol t104
router(config-t104)# channel cc_master1
router(config-t104-channel)# k-value 12
router(config-t104-channel)# w-value 8
router(config-t104-channel)# t0-timeout 30
router(config-t104-channel)# t1-timeout 15
router(config-t104-channel)# t2-timeout 10
router(config-t104-channel)# t3-timeout 30
router(config-t104-channel)# tcp-connection 0 local-port 2050 remote-ip any
router(config-t104-channel)# tcp-connection 1 local-port 2051 remote-ip any
router(config-t104-channel)# exit
router(config-t104)# session
 cc_master1
router(config-t104-session)# attach-to-channel cc_master1
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master1-sector
router(config-t104-sector)# attach-to-session cc_master1
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104)# exit

router(config-t104)# session
 cc_master2
router(config-t104-session)# attach-to-channel cc_master2
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master2-sector
router(config-t104-sector)# attach-to-session cc_master2
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104-sector)# exit
router(config-t104)# exit
router(config)# scada-gw enable
```

次の例は、DNP3 プロトコル スタックを使用して SCADA システム内のコントロール センターと RTU 間のエンドツーエンド通信を設定し、IR1101 でプロトコル変換エンジンを開始する方法を示しています。

```
router# configure terminal
router(config)# interface async 0/2/0
router (config-if)# no shutdown
router (config-if)# encapsulation scada
router (config-if)# exit
router(config)# scada-gw protocol dnp3-serial
router(config-dnp3s)# channel rtu_channel
router(config-dnp3s-channel)# bind-to-interface async 0/2/0
router(config-dnp3s-channel)# link-addr source 3
router(config-dnp3s-channel)# unsolicited-response enable
router(config-dnp3s-channel)# exit
router(config-dnp3s)# session rtu_session
```

```
router(config-dnp3s-session)# attach-to-channel rtu_channel
router(config-dnp3s-session)# link-addr dest 3
router(config-dnp3s-session)# exit
router(config-dnp3s)# exit
router(config)# scada-gw protocol dnp3-ip
router(config-dnp3n)# channel cc_channel
router(config-dnp3n-channel)# link-addr dest 3
router(config-dnp3n-channel)# tcp-connection local-port default remote-ip any
router(config-dnp3n-channel)# exit
router(config-dnp3n)# session cc_session
router(config-dnp3n-session)# attach-to-channel cc_channel
router(config-dnp3n-session)# link-addr source 3
router(config-dnp3n-session)# map-to-session rtu_session
router(config-dnp3n)# exit
router(config)# exit
router(config)# scada-gw enable
```

（注） T101 側から取得した IOA アドレスは、SCADA ゲートウェイによる変更なしで T104 側に送信されます。

SCADA に対する YANG データモデルのサポート

Cisco IOS XE 17.1.1 には、SCADA システム向けの Cisco IOS XE YANG モデルのサポートが導入されています。他の領域においては、以前のリリースで YANG モデルが提供されていました。

https://github.com/YangModels/yang/tree/master/vendor/cisco/xe/17111

SCADA YANG モデル

メインの Cisco-IOS-XE ネイティブモデルに属する 2 つの機能モジュールを SCADA で使用できます。

- Cisco-IOS-XE-scada-gw.yang

このモジュールには SCADA ゲートウェイのコンフィギュレーション コマンドの YANG 定義のコレクションが含まれています。

- Cisco-IOS-XE-scada-gw-oper.yang

このモジュールには SCADA ゲートウェイの運用データの YANG 定義のコレクションが含まれています。

SCADA モデルを機能させるには、8 つの依存モジュール（メインの Cisco-IOS-XE ネイティブモデルに属する）をインポートする必要があります。次の項では、SCADA YANG モデルのリスト、設定CLI コマンド、および各機能モジュールが対象とする依存モジュールを示します。

Cisco-IOS-XE-scada-gw

次に、このモジュールに対応する CLI コマンドを示します。

```
(config)# scada-gw protocol t101
(config-t101)# channel <
channel-name>
(config-t101)# bind-to-interface
<interface-name>
(config-t101)# link-mode
<link-mode>
(config-t101)# link-addr-size
<size>
(config-t101)# day-of-week <enable>
(config-t101)# session
<session_name>
(config-t101)# attach-to-channel
<channel-name>
(config-t101)# cot-size
<size>
(config-t101)# common-addr-size
<size>
(config-t101)# info-obj-addr-size
<size>
(config-t101)# link-addr
<addr>
(config-t101)# request
(config-t101)# sector <sector_name
>
(config-t101)# attach-to-session <
session-name>
(config-t101)# asdu-addr
<addr>
(config-t101)# request
(config)# scada-gw protocol t104
(config-t104)# channel <channel-name>
(config-t104)# tcp connection

(config-t104)# to-timeout
<value>
(config-t104)# t1-timeout
<value>

(config-t104)# t2-timeout
<value>

(config-t104)# t3-timeout
<value>

(config-t104)# k-value
<value>

(config-t104)# w-value
<value>

(config-t101)# day-of-week
<enable>
(config-t101)# send-ei <
enable>
(config-t104)# session
<session_name>
(config-t104)# attach-to-channel
<channel_name>
(config-t104)# sector
<sector_name>
(config-t104)# attach-to-session
```

```
<session-name>
config-t104)# map-to-sector
<sector-name>
(config) scada-gw enable
```

Cisco-IOS-XE-scada-gw モジュールには、次の依存モジュールがあります。

- Cisco-IOS-XE-native
- Cisco-IOS-XE-features
- ietf-inet-types
- Cisco-IOS-XE-interfaces
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @（すべてのリビジョン）
- cisco-semver

Cisco-IOS-XE-scada-gw-oper

次に、このモジュールに対応する CLI コマンドを示します。

```
# show scada statistics
# show scada tcp
```

次に、Cisco-IOS-XE-scada-gw-oper モジュールの依存モジュールを示します。

- Cisco-IOS-XE-native
- Cisco-IOS-XE-features
- ietf-inet-types
- Cisco-IOS-XE-interfaces
- Cisco-IOS-XE-ip
- Cisco-IOS-XE-vlan
- ietf-yang-types @（すべてのリビジョン）
- cisco-semver

DNP3 プロトコル スタックの設定

SCADA システム内のコントロール センターと RTU 間のエンドツーエンド通信を可能にする DNP3 シリアルおよび DNP3 IP プロトコル スタックを設定できます。

DNP3 シリアルの設定

RTU との DNP シリアル通信用のチャネルおよびセッション パラメータを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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。

	コマンドまたはアクション	目的
ステップ 2	**scada-gw protocol dnp3-serial**	DNP3 シリアルプロトコルのコンフィギュレーション モードを開始します。
ステップ 3	**channel** *channel_name*	DNP3 シリアルプロトコルのチャネル コンフィギュレーション モードを開始します。 *channel_name*：ルータのシリアル ポートと RTU とが通信するチャネルを識別します。 注：入力したチャネル名が存在しない場合、ルータは新しいチャネルを作成します。 このコマンド **no** の形式を入力すると、既存のチャネルが削除されます。ただし、チャネルを削除するには、すべてのセッションを削除する必要があります。
ステップ 4	**bind-to-interface async0/2/0**	システムが DNP3 プロトコル トラフィックを送信するルータの非同期インターフェイスを定義します。
ステップ 5	**link-addr source** *source_address*	マスターのリンク アドレスです。 *source_address*：1 ～ 65535 の範囲の値。
ステップ 6	**unsolicited-response enable**	（任意）未承認応答を許可します。 このコマンドの **no** 形式を入力すると、未承認応答が無効になります。 デフォルトでは無効です。
ステップ 7	**exit**	チャネルの設定を終了し、チャネル コンフィギュレーション モードを終了します。すべての設定を保存します。
ステップ 8	**session** *session_name*	セッション コンフィギュレーションモードを開始し、セッションに名前を割り当てます。 注：入力したセッション名が存在しない場合、ルータは新しいセッションを作成します。 このコマンドの **no** 形式を入力すると、既存のセッションが削除されます。
ステップ 9	**attach-to-channel** *channel_name*	セッションをチャネルに接続します。 注：ステップ 3 で入力したのと同じチャネル名を使用します。 *channel_name*：チャネルを識別します。

	コマンドまたはアクション	目的
ステップ 10	**link-addr dest** *destination_address*	スレーブのリンク アドレスです。 *destination_address*：1 ～ 65535 の範囲の値。
ステップ 11	**exit**	セッション コンフィギュレーション モードを終了します。
ステップ 12	**exit**	プロトコル コンフィギュレーション モードを終了します。

例

次の例は、DPN3 シリアル プロトコル スタックのパラメータを設定する方法を示しています。

```
router# configure terminal
router(config)# scada-gw protocol dnp3-serial
router(config-dnp3s)# channel rtu_channel
router(config-dnp3s-channel)# bind-to-interface async 0/2/0
router(config-dnp3s-channel)# link-addr source 3
router(config-dnp3s-channel)# unsolicited-response enable
router(config-dnp3s-channel)# exit
router(config-dnp3s)# session rtu_session
router(config-dnp3s-session)# attach-to-channel rtu_channel
router(config-dnp3s-session)# link-addr dest 3
router(config-dnp3s-session)# exit
router(config-dnp3s)# exit
router(config)#
```

DNP3 IP の設定

DNP3 IP を介して接続するコントロール センターに対して、次の手順を実行します。冗長性を確保するために、同じセッション設定を共有する複数の接続を同じセッション下に作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	**scada-gw protocol dnp3-ip**	DNP-IP プロトコルのコンフィギュレーション モードを開始します。
ステップ 3	**channel** *channel_name*	DNP-IP プロトコルのチャネル コンフィギュレーション モードを開始します。 *channel_name*：ルータがコントロール センターと通信するチャネルを識別します。

	コマンドまたはアクション	目的
		注：入力したチャネル名が存在しない場合、ルータは新しいチャネルを作成します。 このコマンド **no** の形式を入力すると、既存のチャネルが削除されます。ただし、チャネルを削除するには、すべてのセッションを削除する必要があります。
ステップ 4	**link-addr dest** *destination_address*	マスターのリンク アドレスです。 *destination_address*：1 ～ 65535 の範囲の値。
ステップ 5	**send-unsolicited-msg enable**	（任意）未承認メッセージを許可します。 デフォルトでは有効です。
ステップ 6	**tcp-connection local-port** [**default** | *local_port*] **remote-ip** [**any** | *remote_ip* | *remote_subnet*]	TCP 接続のローカル ポート番号とリモート IP アドレスを設定します。 • **default**–20000. • *local_port*：2000 ～ 65535 の値の範囲。 • any–Any remote hosts 0.0.0.0/0 • *remote_ip*：単一ホスト：a. B. C. D • *remote_subnet*：サブネット：A. C. D/LEN remote_subnet が指定されている場合、2 つのチャネルに同じローカル ポートがあると、リモート サブネットは相互にオーバーラップできません。 注：<local-port, remote-ip> はすべてチャネルごとに一意である必要があります。remote_subnet が指定されている場合、2 つのチャネルに同じローカル ポートがあると、リモートサブネットは相互にオーバーラップできません。
ステップ 7	**exit**	チャネル コンフィギュレーション モードを終了します。
ステップ 8	**session** *session_name*	セッション コンフィギュレーションモードを開始し、セッションに名前を割り当てます。 注：入力したセッション名が存在しない場合、ルータは新しいセッションを作成します。 このコマンドの **no** 形式を入力すると、既存のセッションが削除されます。
ステップ 9	**attach-to-channel** *channel_name*	セッションをチャネルに接続します。

	コマンドまたはアクション	目的
		ステップ 3 で入力したのと同じチャネル名を使用します。 *channel_name*：チャネルを識別します。
ステップ 10	**link-addr source** *source_address*	スレーブのリンク アドレスです。 *source_address*：1 ～ 65535 の値。
ステップ 11	map-to-session *session_name*	dnp3-ip セッションを既存の dnp3-serial セッションにマッピングします。 注：1 つの dnp3-ip セッションは、1 つの dnp3 シリアル セッションにのみマッピングできます。
ステップ 12	**exit**	セッション コンフィギュレーション モードを終了します。
ステップ 13	**exit**	プロトコル コンフィギュレーション モードを終了します。

例

次の例は、DNP3 IP パラメータの設定例を示しています。

```
router# configure terminal
router(config)# scada-gw protocol dnp3-ip
router(config-dnp3n)# channel cc_channel
router(config-dnp3n-channel)# link-addr dest 3
router(config-dnp3n-channel)# tcp-connection local-port default remote-ip any
router(config-dnp3n-channel)# exit
router(config-dnp3n)# session cc_session
router(config-dnp3n-session)# attach-to-channel cc_channel
router(config-dnp3n-session)# link-addr source 4
router(config-dnp3n-session)# map-to-session rtu_session
router(config-dnp3n)# exit
router(config)# exit
```

プロトコル変換エンジンの開始と停止

IR1101 でプロトコル変換を使用するには、プロトコル変換エンジンを開始する必要があります。

Starting：IR1101 シリアル ポートで SCADA カプセル化を有効にし、IR1101 で T101 および T104 プロトコルを設定した後、プロトコル変換エンジンを開始できます。

Stopping：アクティブなプロトコル変換エンジンを使用して IR1101 でプロトコル変換に対する設定変更を行う前に、エンジンを停止する必要があります。

始める前に

firsttimeのルータ上のプロトコル変換エンジンの**starting**前に、次の項目が完了していることを確認してください。

IR1101 シリアル ポートと SCADA カプセル化の有効化 （271 ページ）

T101 および T104 プロトコル スタックの設定 （272 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**[no] scada-gw enable**	IR1101 でプロトコル変換エンジンを開始（**scada-gw enable**）または停止（**no scada-gw enable**）します。

例

ルータでプロトコル変換エンジンを起動するには、次のコマンドを入力します。

```
router# configure terminal
router(config)# scada-gw enable
```

ルータのプロトコル変換エンジンを停止するには、次のコマンドを入力します。

```
router# configure terminal
router(config)# no
 scada-gw enable
```

設定の確認

コマンド	目的
show running-config	アクティブな機能とその設定を含むルータの設定を示します。
scada データベースの表示	SCADA データベースの詳細の表示
show scada statistics	SCADA ゲートウェイの統計情報を表示します。これには、送受信されたメッセージ数、タイムアウト、およびエラーが含まれます。
scada tcp の表示	SCADA ゲートウェイに関連付けられている TCP 接続を表示します。

次の例は、show scada tcp および show scada statistics コマンドの出力を示しています。

```
router# show scada tcp
```

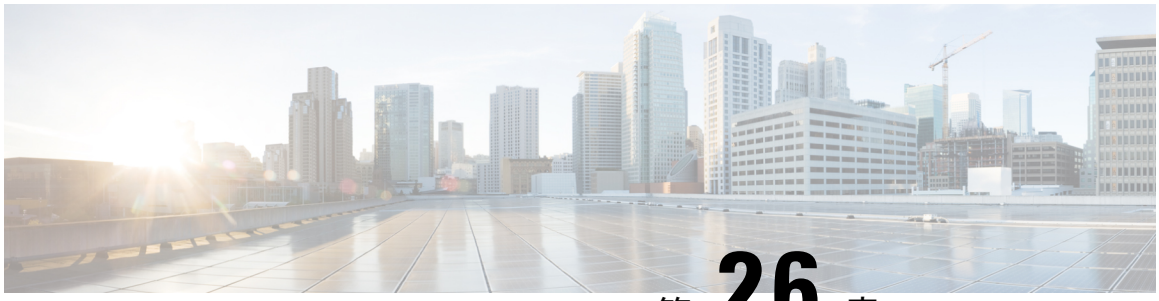
```
DNP3 network channel [test]: 4 max simultaneous connections
conn: local-ip: 3.3.3.21       local-port 20000       remote-ip 3.3.3.15     data-socket
 1
Total:
  1 current client connections
  0 total closed connections
router# show scada statistics
DNP3 network Channel [test]:
  5 messages sent, 2 messages received
  0 timeouts, 0 aborts, 0 rejections
  2 protocol errors, 2 link errors, 0 address errors
DNP3 serial Channel [test]:
  152 messages sent, 152 messages received
  1 timeouts, 0 aborts, 0 rejections
  0 protocol errors, 0 link errors, 0 address errors
```

debug コマンド

このセクションでは、トラブルシューティングに役立ついくつかのデバッグ コマンドを示します。

表 *14 : SCADA* 機能レベルのデバッグ コマンド

コマンド	目的
debug scada function config	設定トレース
debug scada function control	コントロール トレース
debug scada function file	ファイル トレース
debug scada function freeze	フリーズ トレース
debug scada function physical	物理トレース
debug scada function poll	ポーリング トレース
debug scada function stack	スタック トレース
debug scada function umode	Umode トレース



第 26 章

raw ソケット トランスポート

この章は、次の項で構成されています。

raw ソケット トランスポート

raw ソケットトランスポートは、ライフラインアプリケーションの IP ネットワークを介して、1 つのシリアルインターフェイスから別のシリアルインターフェイスに文字のストリームを転送します。

このドキュメントでは、IR1101 の raw ソケット トランスポートについて解説し、raw ソケット トランスポート コマンドに関する参照セクションを示します。

このマニュアルの構成は、次のとおりです。

raw ソケット トランスポートに関する情報

raw ソケットは、IP ネットワークを介してシリアルデータを転送するための方法です。この機能は、リモート ターミナルの単位（RTU）から遠隔監視制御・情報取得（SCADA）データを転送するのに使用できます。このメソッドは、ブロック シリアル トンネル（BSTUN）プロトコルに代わるものです。

raw ソケット トランスポートは、トランスポート プロトコルとして TCP または UDP をサポートします。インターフェイスはいずれかのプロトコルを使用するように設定できますが、両方を同時に使用することはできません。TCP トランスポートは、データの確認応答と連続配信を

必要とする制御アプリケーションなどのアプリケーションに適しています。回線 SEL リレーなど、遅延の影響を受けやすいアプリケーションに対して、UDP トランスポートは TCP よりも高速なシリアル データ転送を提供します。

raw ソケット トランスポートでは、非同期シリアルインターフェイスに対して以下がサポートされています。

- 組み込みの自動 TCP 接続再試行メカニズムを装備したトランスポート プロトコルとしての TCP。
- 最大 32 の TCP セッション。
- サーバ、クライアント、またはその両方の組み合わせとしてのインターフェイス設定。
- サーバ インターフェイス 1 つ、ただし複数のクライアントあり。
- VRF 認識。ルータは、バーチャル プライベート ネットワーク（VPN）仮想ルーティングおよび転送 （VRF）インターフェイスを介して接続されたサーバ ホストに raw ソケット トランスポート トラフィックを送信できるようになります。

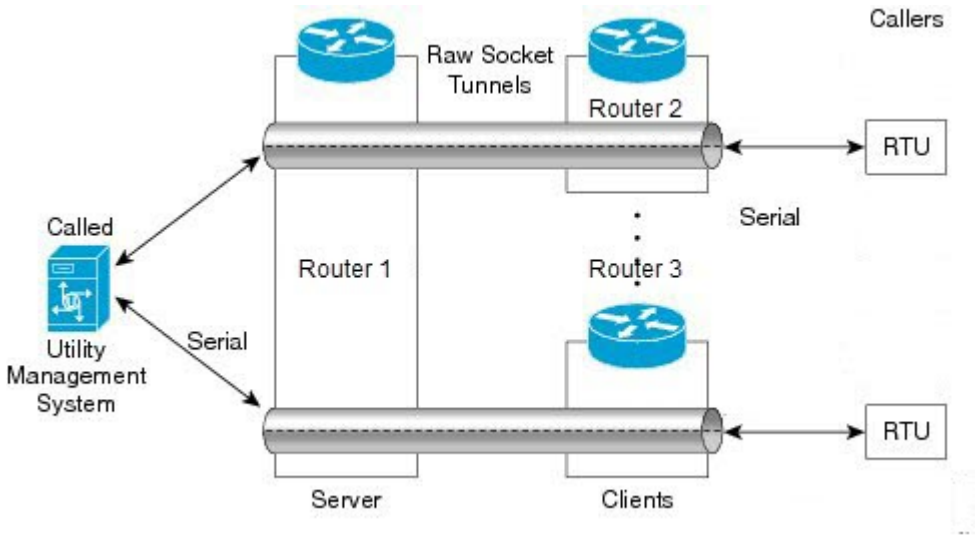
この項では、次のトピックについて取り上げます。

TCP トランスポート

TCP raw ソケット トランスポートは、クライアント/サーバモデルを使用します。1 つの非同期シリアル回線で、最大 1 つのサーバと複数のクライアントを設定できます。クライアント モードでは、IR1101 は raw ソケット サーバ（他の IR1101 ルータまたはサードパーティ製デバイスが可能）に対して最大 32 の TCP セッションを開始できます。

図 1 は、raw ソケット TCP 設定の例を示しています。この例では、複数の IR1101 ルータを含む IP ネットワークを介して、RTU とライフライン管理システムの間でシリアルデータが転送されています。1 つの IR1101 ルータ（ルータ 1）は raw ソケット サーバとして機能し、raw ソケット クライアントとして設定された他の IR1101 ルータ（ルータ 2 とルータ 3）からの TCP 接続要求をリッスンします。

raw ソケット クライアントは RTU からシリアル データのストリームを受信し、そのバッファにこのデータを蓄積してから、ユーザ指定のパケット化基準に基づいてデータをパケットに格納します。raw ソケット クライアントは、raw ソケット サーバとの TCP 接続を開始し、IP ネットワークを介してパケット化データを raw ソケット サーバに送信します。これにより、パケットからシリアルデータが取得され、それがシリアルインターフェイスに送信され、ライフライン管理システムに送信されます。



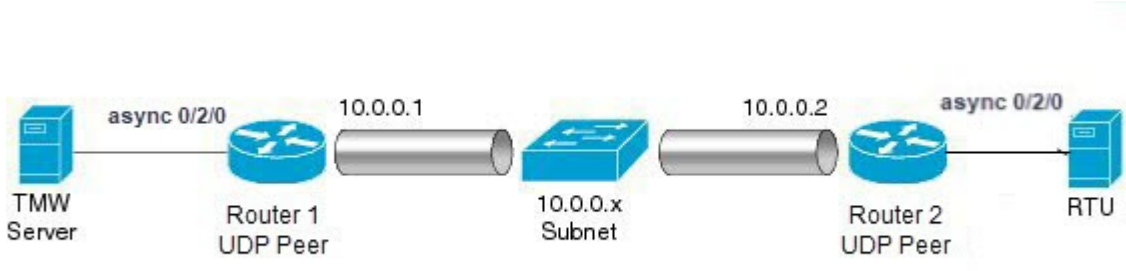
（注） ルータのシリアル リンク インターフェイスをサーバとして設定する場合、インターフェイスのピアはクライアントルータのシリアルリンクインターフェイスであり、その逆も同様です。

UDP トランスポート

UDP トランスポートは、ピアツーピア モデルを使用しています。非同期シリアル回線には複数の UDP 接続を設定できます。

図 2 は、raw ソケットの UDP 設定の例を示しています。この例では、シリアルデータは、raw ソケット UDP 対向として設定されている 2 つのルータ（ルータ 1 は IR1101、ルータ 2 は IR807）を含む IP ネットワークを介して RTU とライフライン管理システム間で転送されています。

この例では、raw ソケット UDP 対向は RTU からシリアル データのストリームを受信し、そのバッファにこのデータを蓄積してから、ユーザ指定のパケット化基準に基づいてデータをパケットに格納します。raw ソケット UDP 対向は、IP ネットワークを介してパケット化データをもう一方の終端の raw ソケット ピアに送信します。これにより、パケットからシリアルデータが取得され、それがシリアルインターフェイスに送信され、ライフライン管理システムに送信されます。



シリアル データ処理

デフォルトのシリアルプロトコル、非同期通信プロトコルが使用されている場合、raw ソケット対向が受信するシリアル データ ストリームは、次の基準に基づいてパケット化されます。

- **Packet length**：IR1101 がシリアルデータを対向に送信する引き金となるパケット長を指定できます。IR1101 がバッファ内にこの量のデータを収集すると、蓄積されたデータをパケット化して raw ソケット対向に転送します。
- **Packet-timer value**：パケット タイマーは、IR1101 がストリーム内の次の文字を受信するまで待機する時間を指定します。パケット タイマーの期限終了までに文字が受信されない場合、IR1101 がバッファ内で累積したデータはパケット化され、raw ソケット対向に転送されます。
- **Special character**：IR1101 がバッファに蓄積されたデータをパケット化して raw ソケット対向に送信する引き金となる文字を指定することができます。特殊文字（CR/LF など）を受信すると、IR1101 は蓄積されたデータをパケット化して raw ソケット 対向に送信します。

処理オプションの設定については、6 ページの「共通の raw ソケット ライン オプションの設定」の手順を参照してください。

VRF 対応 raw ソケット

VRF 対応 raw ソケットトランスポート機能を使用すると、VRF を使用して raw ソケットトラフィックを分離し、シリアル データを効率的に管理および制御することができます。VRF を設定したら、raw ソケットトランスポート用に設定されたシリアル インターフェイスを VRF に関連付けることができます。設定例については、raw ソケット VRF （302 ページ）を参照してください。

前提条件

使用するネットワーク デバイスとインターフェイスを含め、ネットワーク内で raw ソケット トラフィックが転送される方法、ルータがシリアル データをパケット化する方法、VRF を使用するかどうかを決定します。

注意事項と制約事項

通常、UDP トラフィックはネットワーク内のファイアウォールによってブロックされます。ネットワークにこうしたファイアウォールがある場合は、raw ソケット UDP トラフィックを許可するようにピンホールを設定してください。

デフォルト設定

機能	デフォルト設定
raw ソケット トランスポート	無効
パケット長	パケット長は設定されていません。
シリアル プロトコル	非同期通信プロトコル
パケット タイムアウト	15 ミリ秒
特殊文字	特殊文字は設定されていません。
raw ソケット モード	Best-effort モードはオフになっており、IR1101 ではサポートされていません。
TCP アイドル タイムアウト	5 分

raw ソケット トランスポートの設定

この項では、次のトピックについて取り上げます。

シリアルインターフェイスで raw ソケットトランスポートを有効化

IR1101 ルータで raw ソケットトランスポートを有効にするには、最初に非同期シリアル ポートを有効にし、そのポートに対して raw ソケット TCP または UDP カプセル化を有効にする必要があります。

始める前に

IR1101 のシリアル ポートが使用可能かどうかを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**interface async0**/*slot* /*port*	async slot/port のインターフェースのコマンド モードを開始します。
ステップ 3	**no ip address**	インターフェイスで IP 処理を無効にします。

	コマンドまたはアクション	目的
ステップ 4	次のいずれかを実行します。 • **encapsulation raw-tcp** • • **encapsulation raw-udp**	シリアル ポートの raw ソケット TCP カプセル化または UDP カプセル化を有効にします。

例

次に、シリアルポート 0/2/0 を有効にし、そのポートで raw ソケット TCP カプセル化を有効にする例を示します。

```
router# configure terminal
router(config)# interface async0/2/0
router(config-if)# no ip address
router(config-if)# encapsulation raw-tcp
router(config-if)# exit
```

共通の raw ソケット ライン オプションの設定

回線上のすべての接続に共通するオプションを設定できます。共通のオプションは、TCP と UDP の両方に適用されます。

始める前に

シリアルインターフェイスで raw ソケットトランスポートを有効化 （293 ページ） の説明に従って、raw ソケットトランスポートを有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**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	**line 0**/*slot* /*port*	シリアル スロット / ポートのライン コマンド モードを開始します。
ステップ 3	**raw-socket packet-length** *length*	IR1101 がシリアル データを対向に送信する引き金となるパケット長を指定します。IR1101 がバッファ内にこの大量のデータを蓄積すると、蓄積されたデータをパケット化して raw ソケット対向に転送します。 *length*：2 ～ 1400 バイト。 デフォルトでは、パケット長トリガーは無効になっています。

	コマンドまたはアクション	目的
ステップ 4	**raw-socket packet-timer** *timeout*	IR1101 がストリーム内の次の文字を受信するまで待機する最大時間をミリ秒単位で指定します。パケットタイマーの期限終了までに文字が受信されない場合、累積したデータはパケット化され、raw ソケット対向に転送されます。 *timeout*：3 ～ 1000 ミリ秒。 デフォルトは 15 ミリ秒です。
ステップ 5	**raw-socket spec-char** *ascii_char*	バッファに蓄積されたデータをパケット化して raw ソケット対向に送信するように IR1101 をトリガーする文字を指定します。 *ascii_char*：0 ～ 255。 デフォルトでは、特殊文字トリガーは無効になっています。

次のタスク

デフォルト値に戻すには、これらのコマンドの **no** 形式を使用します。

例

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket packet-length 32
router(config-line)# raw-socket packet-timer 500
router(config-line)# raw-socket special-char 3
```

raw ソケット TCP の設定

raw ソケット TCP カプセル化を有効にした後、TCP サーバまたはクライアントを設定します。

raw ソケット TCP サーバの設定

始める前に

シリアルインターフェイスで raw ソケットトランスポートを有効化（293 ページ）の説明に従って、そのポートのシリアル ポートおよび raw ソケット TCP カプセル化を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	**line 0**/*slot* /*port*	シリアル スロット / ポートのライン コマンド モードを開始します。
ステップ 3	**raw-socket tcp server** *port* [*ip_address*]	非同期回線インターフェイスの raw ソケット トランスポート TCP サーバを起動します。raw ソケット サーバ モードでは、IR1101 は raw ソケット クライアントからの着信接続要求をリッスンします。 *port*：サーバがリッスンするポート番号。 *ip_address*：（任意）サーバが接続要求をリッスンするローカル IP アドレス。
ステップ 4	**raw-socket tcp idle-timeout** *session_timeout*	非同期回線インターフェイスの raw ソケット トランスポート TCP セッション タイムアウトを設定します。この間隔でクライアントとサーバの間でデータが転送されない場合、TCP セッションは終了します。その後、クライアントはサーバとの TCP セッションの再確立を自動的に試みます。 このタイムアウト設定は、この特定の回線のすべての raw ソケット トランスポート TCP セッションに適用されます。 *session_timeout*：設定されているセッション アイドル タイムアウト（分）。デフォルトは 5 分です。

次のタスク

raw ソケット TCP サーバを削除するには、**no raw-socket tcp server** コマンドを使用します。

例

次の例は、非同期シリアル回線の raw ソケット TCP サーバを設定する方法を示しています。TCP サーバは、ローカル ポート 4000 およびローカル IP アドレス 10.0.0.1 で TCP クライアント接続要求を待ち受けます。raw ソケット TCP サーバと TCP クライアントのいずれかの間で 10 分間データが交換されない場合、TCP セッションが終了し、raw ソケット クライアントは raw ソケット サーバとのセッションの再確立を試行します。

```
router# configure terminal

router(config)# line 0/2/0
router(config-line)# raw-socket tcp server 4000 10.0.0.1
router(config-line)# raw-socket tcp idle-timeout 10
router(config-line)# exit
router(config)#
```

raw ソケット TCP クライアントの設定

始める前に

シリアルインターフェイスでrawソケットトランスポートを有効化（293ページ）の説明に従って、そのポートのシリアル ポートおよびraw ソケット TCP カプセル化を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	**line 0**/*slot* /*port*	シリアル スロット / ポートのライン コマンド モードを開始します。
ステップ 3	**raw-socket tcp client** *dest_ip_address dest_port* [*local_ip_address*] [*local_port*]	raw ソケット トランスポート TCP クライアント セッションの設定を指定します。 *dest_ip_address*：リモート raw ソケット サーバの宛先 IP アドレス。 *dest_port*：リモート サーバへの TCP 接続に使用する宛先ポート番号。 *local_ip_address*：（任意）クライアントがバインドできるローカル IP アドレス。 *local_port*：（任意）クライアントがバインドできるローカル ポート番号。
ステップ 4	**raw-socket tcp idle-timeout** *session_timeout*	非同期回線インターフェイスの raw ソケット トランスポート TCP セッション タイムアウトを設定します。この間隔でクライアントとサーバの間でデータが転送されない場合は、TCP セッションが閉じられます。その後、クライアントはサーバとの TCP セッションの再確立を自動的に試みます。 このタイムアウト設定は、この特定の回線のすべての raw ソケット トランスポート TCP セッションに適用されます。 *session_timeout*：設定されているセッション アイドル タイムアウト（分）。デフォルトは 5 分です。
ステップ 5	**raw-socket tcp keepalive** *interval*	非同期回線インターフェイスの raw ソケット トランスポート TCP セッションのキープアライブ インターバルを設定します。ルータは、設定された間隔に基づいてキープアライブ メッセージを送信します。たとえば、セルラー インターフェイスを介して raw

	コマンドまたはアクション	目的
		TCP トラフィックを送信するとき、この間隔の設定が必要な場合があります。 *interval*：現在設定されているキープアライブ インターバル（秒単位）。範囲は 1 ～ 864000 秒です。デフォルト値は 1 秒です。

次のタスク

raw ソケット TCP クライアントを削除するには、**no raw-socket tcp client** コマンドを使用します。

例

次の例は、非同期シリアル回線の raw ソケット TCP クライアントを設定する方法を示しています。raw ソケット クライアントとして機能する IR1101（ルータ）は、raw ソケット サーバとの TCP セッションを開始し、パケット化されたシリアル データをそのサーバに転送します。ルータは、バッファ内のシリアルデータのストリームを収集します。バッファに 827 バイト蓄積されると、ルータはデータをパケット化して raw ソケット サーバに転送します。ルータと raw ソケット サーバの間で 10 分間データが交換がされないと、raw ソケット サーバとの TCP セッションが終了し、ルータは raw ソケット サーバとのセッションの再確立を試みます。

```
router# configure terminal

router(config)# line 0/2/0
router(config-line)# raw-socket tcp client 10.0.0.1 4000
router(config-line)# raw-socket packet-length 827
router(config-line)# raw-socket tcp idle-timeout 10
router(config-line)# exit
router(config)#
```

raw ソケット UDP ピアツーピア接続の設定

raw ソケット UDP カプセル化および共通回線オプションを有効にした後、raw ソケット UDP ピアツーピア接続を設定します。接続の一端のローカル ポートは、もう一方の端の宛先ポートである必要があります。

始める前に

シリアルインターフェイスでraw ソケットトランスポートを有効化（293 ページ）の説明に従って、そのポートのシリアル ポートおよび raw ソケット UDP カプセル化を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	**line 0**/*slot* /*port*	シリアル スロット / ポートのライン コマンド モードを開始します。
ステップ 3	**raw-socket udp connection** *dest_ip_address dest_port local_port* [*local_ip_address*]	raw ソケット トランスポート UDP 接続を指定します。 *dest_ip_address*：UDP 接続に使用する宛先 IP アドレス *dest_port*：UDP 接続に使用する宛先ポート番号。 *local_port*：UDP 接続のローカル ポート番号。 *local_ip_address*：（任意）UDP 接続のローカル IP アドレス。

次のタスク

raw ソケット UDP 接続を削除するには、**no raw-socket udp connection** コマンドを使用します。

例

以下は、ルータ A（ローカル IP アドレス 192.168.0.8）とルータ B（ローカル IP アドレス 192.168.0.2）との間に raw ソケット UDP 接続を設定する方法を示しています。

ルータ A

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket udp connection 192.168.0.2 5000 7000
router(config-line)# exit
router(config)#
```

ルータ B

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket udp connection 192.168.0.8 7000 5000
router(config-line)# exit
router(config)#
```

設定の確認

コマンド	目的
show running-config	アクティブな機能とその設定を含む IR1101 の設定を表示します。

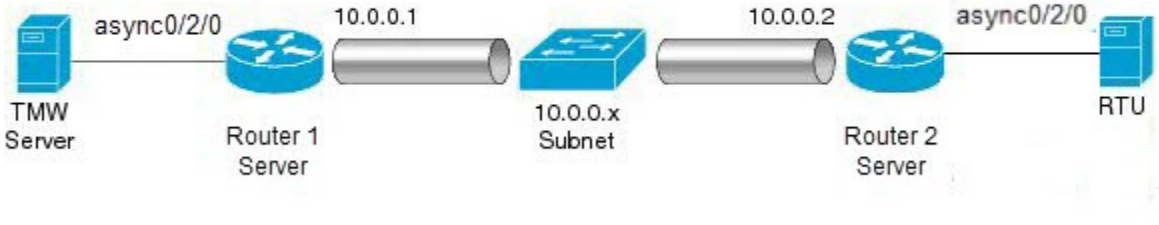
コマンド	目的
show raw-socket tcp detail	raw ソケット トランスポート TCP アクティビティに関する情報を表示します。
show raw-socket tcp sessions	raw ソケット トランスポート TCP セッションに関する情報を表示します。
show raw-socket tcp statistics	各非同期シリアル回線の raw ソケット トランスポート TCP 統計情報を表示します。
show raw-socket udp detail	raw ソケット トランスポート UDP アクティビティに関する情報を表示します。
show raw-socket udp sessions	raw ソケット トランスポート UDP セッションに関する情報を表示します。
show raw-socket udp statistics	各非同期シリアル回線の raw ソケット トランスポート UDP 統計情報を表示します。
clear raw-socket statistics	特定の TTY インターフェイスまたはすべての非同期シリアル回線の raw ソケット トランスポート統計情報をクリアします。

設定例

次のセクションでは、raw ソケットトランスポートの設定例を示します。

raw ソケット TCP

次の例は、ある IR1101 ルータ（ルータ 1）がサーバとして機能し、別の IR809（ルータ 2）がクライアントとして機能する raw ソケット トランスポートの設定を示しています。



次の表は、図 3 で強調表示されているサーバとクライアント IR1101 の設定を示しています。

IR1101 サーバ設定	IR807 クライアント設定
... interface async0/2/0 no ip address **encapsulation raw-tcp** ! ... line 0/2/0 **raw-socket tcp server 5000 10.0.0.1** **raw-socket packet-timer 3** **raw-socket tcp idle-timeout 5** ...	... interface async0 no ip address **encapsulation raw-tcp** ! interface async1 no ip address **encapsulation raw-tcp** ! ... line 1 **raw-socket tcp client 10.0.0.1 5000 10.0.0.2 9000** **raw-socket packet-length 32** **raw-socket tcp idle-timeout 5** line 2 **raw-socket tcp client 10.0.0.1 5000 10.0.0.2 9001** **raw-socket packet-length 32** **raw-socket tcp idle-timeout 5**

raw ソケット UDP

次の例は、2 つの IR1101 ルータ間の raw ソケット UDP 接続の設定例を示しています。

Router1 から

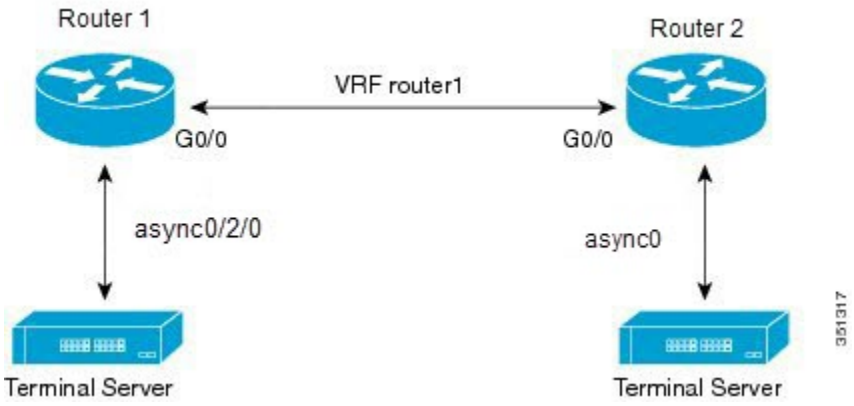
```
interface GigabitEthernet0/1
ip address 192.168.0.8 255.255.255.0
duplex auto
speed auto
interface async0/2/0
no ip address
encapsulation raw-udp
line 0/2/0
raw-socket udp connection 192.168.0.2 2 2
```

Router2 から

```
interface GigabitEthernet0/1
ip address 192.168.0.2 255.255.255.0
load-interval 60
duplex auto
speed auto
no keepalive
interface async0/2/0
no ip address
encapsulation raw-udp
line 0/2/0
raw-socket udp connection 192.168.0.8 2 2
```

raw ソケット VRF

次の例は、raw ソケット トランスポート用に設定された 2 台のルータが VRF を介して接続する raw ソケット VRF の設定を示しています。Router1 は raw ソケット TCP サーバとして機能する IR1101 で、Router2 は raw ソケット TCP クライアントとして機能する IR807 です。



以下は図 4 に示す Router1 と Router2 の設定です。

Router1 の設定

ルータに VRF を定義：

```
vrf definition router1
 rd 100:1
 route-target export 100:3
 route-target import 100:3
 !
 address-family ipv4
 exit-address-family
```

インターフェイスに VRF 設定を適用：

```
interface GigabitEthernet0/0
 vrf forwarding router1
 ip address 100.100.100.2 255.255.255.0
 duplex auto
 speed auto
```

シリアル インターフェイスに raw TCP を適用：

```
interface async0/2/0
 vrf forwarding router1
 no ip address
 encapsulation raw-tcp
```

回線に raw TCP を適用：

```
line 0/2/0
 raw-socket tcp server 5000 4.4.4.4
```

Router2 の設定

ルータに VRF を定義：

```
vrf definition router1
 rd 100:1
 route-target export 100:3
 route-target import 100:3
 !
 address-family ipv4
 exit-address-family
```

インターフェイスに VRF 設定を適用：

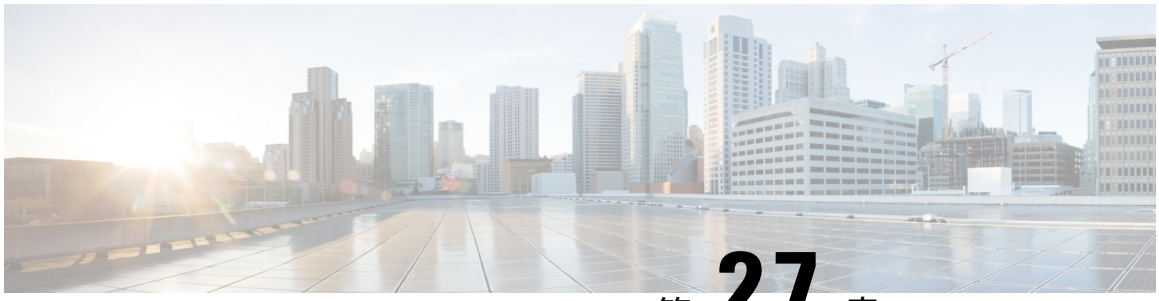
```
interface GigabitEthernet0/0
 vrf forwarding router1
 ip address 100.100.100.1 255.255.255.0
 duplex auto
 speed auto
```

シリアル インターフェイスに raw TCP を適用：

```
interface async0
 vrf forwarding router1
 no ip address
 encapsulation raw-tcp
```

回線に raw-tcp を適用：

```
line 1
  raw-socket tcp client 4.4.4.4 5000
```



第 27 章

IRM-1101 拡張モジュール

ここでは、次の内容について説明します。

IRM-1100 拡張モジュールの概要

IR1101 ルータには、デュアル LTE プラガブル、mSATA SSD FRU、SFP、およびデジタル GPIO 接続などの重要な機能を追加する拡張モジュールが用意されています。

拡張モジュールには、次の 2 つのタイプがあります。

- IRM-1100-SPMI
- IRM-1100-SP

警告 ベース IR1101 と同様に、活性挿抜（OIR）は拡張モジュールではサポートされないことに注意してください。デバイスの電源が入っているときに 4G モジュール（または mSATA）を挿入または取り外すと、モジュールが損傷することがあります。

次の図は、IRM-1100-SPMI の前面パネルを示し、その機能の一部を強調表示しています。

図 *91 : IRM-1100-SPMI* 拡張モジュールの詳細

項目	説明
1	4 GPIO + 1 リターン（デジタル I/O） （注）　機能はCisco IOS-XE リリース 16.12.1 以降で使用できます。
2	SFP コネクタ
3	プラガブルモジュール
4	mSATA SSD スロット
5	デジタル I/O LED

サポートされているハードウェアインターフェイスとその命名規則は、次の表に記載されています。

ハードウェア インターフェイス	命名ルール
拡張モジュール上のギガビットイーサネット SFP ポート	gigabitethernet 0/0/5
拡張モジュールのセルラー インターフェイス	cellular 0/3/0 and 0/3/1
拡張モジュール上の GPIO	alarm contact 1-4

mSATA の概要

エンドユーザがアプリケーションをホストできる IOx/ Guest-OS レガシーシステムには、通常、ユーザデータを保存するための 4 GB のディスクストレージが付属していました。シスコがサポートするプラガブル mSATA SSD PID で 50 GB の使用可能なストレージを追加できる機能が追加されました。100 GB mSATA SSD に対するサポートには次の制限があります。

- **show inventory** コマンドはサポートされていません。
- 55 GB（アプリケーションとパッケージに対する IOx 割り当ては同様）、32B（ストレージに対する IOS アプリケーションは IOS の「dir msata」に表示可能）をサポートしています。

警告 活性挿抜（OID）はサポートされていないことに注意してください。デバイスの電源が入っている状態で mSATA SSD を挿入または取り外すと、モジュールが損傷することがあります。

（注） すべての IoT プラットフォームと同様に、IOx の場合は Fog Director、ローカルマネージャ、またはアプリケーション ホスティング CLI を使用してアプリケーションをインストールし、指定された新しい mSATA ディスクストレージにアクセスします。

50 GB mSATA パーティショニング

IOS-XE は mSATA SSD を 2 つのパーティションに分割します。1 つは IOS-XE 用、もう 1 つは IOx 用です。使用率は次のとおりです。

- IOS：33.33%
- IOx：66.66%

これらのパーセンテージを使用すると、領域の割り当ては次のように分類されます。

50 GB mSATA：

- IOS：16.51 GB
- IOx：31.43 GB

mSATA SSD の使用

機能的には、mSATA の有無にかかわらず、IOS または IOx のエンドユーザに対する設定とトラブルシューティングに違いはありません。システムは追加ストレージを認識するだけです。mSATA ストレージに関連する情報を表示する CLI コマンドがいくつかあります。たとえば、show inventory、show platform msata などです。

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

```
Router#show platform hardware msata lifetime
SSD Lifetime Remaining: 99% -> 99% of the net disk read/write lifetime is remaining
```

```
Router#show platform hardware msata status
SSD is present
```

```
Router#show platform hardware msata
SSD Lifetime remaining(%): 99
```

mSATA のパーティショニングを表示します。

IOS-XE で mSATA のパーティション 1 を表示します。

```
Router#dir msata:
Directory of msata:/
11 drwx 16384 Jun 4 2019 17:59:45 +00:00 lost+found
33820622848 bytes total (32052379648 bytes free)
```

mSATA パーティションとの間でコンテンツをコピーします。

```
Router#copy bootflash: msata:
Source filename []? ir1101-uefi-rommon.SSA
Destination filename [ir1101-uefi-rommon.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
2097152 bytes copied in 0.164 secs (12787512 bytes/sec)
```

mSATA によって IOx に割り当てられたディスク領域を表示します。

```
Router#show app-hosting resource
CPU:
Quota: 1000(Units)
Available: 1000(Units)
Memory:
Quota: 862(MB)
Available: 862(MB)
Storage space:
Total: 58313(MB)
Available: 58313(MB)
```

mSATA SSD のウェアレベリングデータの表示

IOx Local Manager/Fog Director は、IR1101 上の mSATA SSD のウェアレベリングデータを表示できるようになりました。

IOx Local Manager では、**System > Storage** を選択することで確認できます。

IOS コマンドラインから、**show platform hardware msata** コマンドを使用してライフタイムをモニタできます。

```
Router#show platform hardware msata lifetime
SSD Lifetime remaining(%): 98
```

ルータのリロード後、このデータが再度入力されるまでに数分（約 5 分）かかります。

SSD のライフタイムがライフタイム制限の 15% と 5% に低下すると、エラーが syslog に報告され始めます。

次に例を示します。

```
*Jan 30 19:03:00.257: %IOX-4-IOX_SSD_LIFETIME_WARN: SSD Lifetime remaining in module:15
*Jan 30 19:02:30.157: %IOX-2-IOX_SSD_LIFETIME_CRITICAL: SSD Lifetime remaining in module:5
```

mSATA 摩耗率の MIB サポートと使用方法

IOx アプリケーション用のストレージを追加するために、mSATA 機能がルータに追加されました。次の表に、OID を持つルータを示します。

表 *15 : mSATA OID*

SKU	OID
IR1100-SSD-100G	1.3.6.1.4.1.9.12.3.1.9.96.176

この拡張の一部として、ルータの次の mSATA パラメータに対する SNMP サポートが追加されました。

- lifetime remaining（ウェアレベリング）
- mSATA SSD のメモリ使用量

show platform hardware msata コマンドは、この MIB に関する情報を提供します。

関連資料：

https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html

https://developer.cisco.com/docs/iox/

例：実際の OID と OID での SNMP get/walk の出力

<OID> = STRING: "Lifetime Remaining: 99%, Usage: 30%"

機能の詳細

ルータで SNMP 要求を実行する前に、次の条件を満たしている必要があります。

- アクティブ mSATA モジュールをルータ内に設定する必要があります。
- インテグレータは、サポートされているプラガブル mSATA を設計に組み込む必要があります。
- これを確認するには、**show platform hardware msata CLI** を使用します。

機能の前提条件

- ルータのリロード後、mSATA データが再度入力されるまでに約 5 分かかります。SNMP get のみが OID で許可されており、読み取り専用としてマークされます。値を設定することはできません。
- MIB 値を取得するには、ルータで SNMP を有効にする設定が必要です。

デジタル IO

IR1101 には、IRM-1100-SP と IRM-1100-SPMI の 2 つの異なる拡張モジュールがあります。IRM-1100-SPMI には、4 つの GPIO 接続と 1 つのリターン接続を持つデジタル I/O コネクタが搭載されています。ドライとウェットの両方の接点を 60 V までサポートしています。

- ドライ接点は、電圧源から分離されており（つまり「無電圧」）、組み込みリレー機能を持ち（NPN トランジスタ）、通常はイベントを示すために使用されます（開/閉、アラームなど）。
- ウェット接点は、外部電源（+3.3V ～ +60V、高電圧で許可されている電流は 150mA まで）による接点で、通常は何かを通電するために使用されます（ソレノイド、照明など）。

デジタル IO は、IR800 シリーズルータでサポートされているアラーム入力やアラーム出力に似ています。違いは、IR800 シリーズでは、アラーム入力は入力専用で、アラーム出力は専用出力になっていることです。デジタル IO では、入力または出力になります。アラーム出力には、ノーマルオープン（NO）端子またはノーマルクローズ（NC）端子を提供するリレーが含まれています。デジタル IO にはリレーは含まれていません。

GPIO にはアラームのトラップはありません。

デジタル IO ハードウェア機能の詳細については、『Cisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide』[英語] を参照してください。

コンフィギュレーション コマンド

アラーム重大度は critical、major、minor、または none に設定できます。この重大度は、アラームがトリガーされたときにアラームメッセージに表示されます。

IR1101 でアラームを設定し、表示するには、コマンド ライン インターフェイス（CLI）を使用します。

コマンド	目的
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。

コマンド	目的
alarm contact *contact-number***enable**	アラームコンタクト番号を有効にします。contact-number の値は 0 ー 4 です。<0-4> ：アラームコンタクト番号（0：アラームポート、1-4：デジタル I/O）。 アラームコンタクト 0 はベースユニット（ピン 3 と 4）にあり、常に出力モードになっています。アラーム 0 のその他の設定には、*severity*、*threshold*、および *trigger* があります。 アラームコンタクト 1 ー 4（ピン 1 ー 4）は IRM-1100 拡張モジュールにあり、入力モードにも、出力モードにもできます。ピン 5 はアース用です。アラーム 1 ー 4 のその他の設定には、*application*、*output*、*severity*、*threshold*、および *trigger* があります。
alarm contact {*contact-number* {**application** {dry | wet} | **description** | **enable** | {**output** {1 for High | 0 for Low} | **severity** {critical | major | minor | none} | **threshold** {1600-2700} | **trigger** {closed | open}}	• 設定する *contact number*（0 ～ 4）を入力します。 • **description** 文字列は最大 80 文字の英数字で指定し、生成されるすべてのシステムメッセージに表示されます。 • **application** には、dry（デフォルト）または wet を選択します。デジタル I/O ポート 1 ー 4 にのみ適用されます。 • **enable** は、アラームポートを有効にします。no alarm contact contact-number x は、アラームポートを無効にします。 • **output** は、High の場合は 1、Low の場合は 0 です。デジタル I/O ポート 1 ー 4 にのみ適用されます。 • **severity** には *critical*、*major*、*minor*、または *none* を入力します。重大度を設定しない場合、デフォルトは minor となります。 • **threshold** には 1600 ～ 2700 の値を選択します。デフォルト値は 1600 mv です。 • **trigger** には *open* または *closed* を入力します。トリガーを設定しない場合、回路が closed のときにアラームがトリガーされます。
end	特権 EXEC モードに戻ります。
show alarm	設定したアラーム接点を表示ます。
copy running-config startup-config	（任意）コンフィギュレーションファイルに設定を保存します。

CLI を使用してアラームコンタクトを確認します。

```
Router(config)#alarm contact ?
<0-4> Alarm contact number (0: Alarm port, 1-4: Digital I/O)
```

設定例

アラームを設定します。

```
ir1101#conf term
Enter configuration commands, one per line.   End with CNTL/Z.
ir1101(config)#alarm contact 1 description

Your Descriptive Text Here
ir1101(config)#alarm contact 1 severity critical

ir1101(config)#alarm contact 1 trigger closed

ir1101#
```

アラームステータスを表示するには、次の手順を実行します。

```
ir1101#show alarm
Alarm contact 0:
Enabled: Yes
Status: Not Asserted
Application: Dry
Description: test
Severity: Critical
Trigger: Open
Threshold: 2000
```

生成されるアラームの例：

```
ir1101# !
*Nov 27 14:54:52.573: %IR1101_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External
alarm asserted, Severity: Critical
```

イベント中のアラームステータスを表示するには、次の手順を実行します。

```
ir1101#show alarm
ALARM CONTACT
Enabled: Yes
Status: Asserted
Application: Dry
Description: test
Severity: Critical
Trigger: Open
Threshold: 2000
Digital I/O 1:
Enabled: No
Status: Not Asserted
Application: Dry
Description: External digital I/O port 1
Severity: Minor
Trigger: Closed
Threshold: 1600
Digital I/O 2:
Enabled: No
Status: Not Asserted
Application: Dry
```

```
Description: External digital I/O port 2
Severity: Minor
Trigger: Closed
Threshold: 1600
Digital I/O 3:
Enabled: No
Status: Not Asserted
Application: Dry
Description: External digital I/O port 3
Severity: Minor
Trigger: Closed
Threshold: 1600
Digital I/O 4:
Enabled: Yes
Status: Not Asserted
Description: External digital I/O port 4
Mode: Output
Router#
```

クリアされるアラームの例：

```
ir1101# !
*Nov 27 14:55:02.573: %IR1101_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_CLEAR: External
alarm cleared
ir1101#
```

新しいセルラー プラガブル モジュール

リリース16.12.1は、新しいプラガブルモジュール/モデムをサポートしています。拡張モジュールを搭載したIR1101は、デュアルLTE（アクティブ/アクティブ）、デュアルSIM、およびデュアル無線をサポートします。

- デュアルLTE（アクティブ/アクティブまたはアクティブ/バックアップ）は、拡張モジュールと2つのLTEプラガブルインターフェイスを備えたIR1101でサポートされます。1つはベースユニットにあり、もう1つは拡張モジュールにあります。
- デュアルSIMでは、2つのSIMが単一のLTEプラガブルモジュールでアクティブ/バックアップモードで動作します。デュアル無線では、2つのLTEプラガブルモジュールがアクティブ/アクティブモードで動作し、2つのSIMのそれぞれがデュアル無線の特定のセルラー無線に割り当てられます。

新しいSKUの詳細については、次の表を参照してください。

SKU ID	使用されるモデム	説明	サポートされている技術
P-LTE-VZ	WP7601-G	米国（Verizon社）製シングルマイクロSIM	LTE CAT4：B4、B13
P-LTE-US	WP7603-G	北米（AT&T社）製デュアルマイクロSIM	LTE CAT4：B2、B4、B5、B12HSPA+、UMTS：B2、B4、B5

SKU ID	使用されるモデム	説明	サポートされている技術
P-LTE-GB	WP7607-G	欧州向けデュアルマイクロ SIM	LTE CAT4：B3、B5、B8、B20、B28 HSPA +：B1、B5、B8 EDGE：900/1800
P-LTEA-LA	EM7430	APAC	**LTE 帯域**：B1、B3、B5、B7、B8、B18、B19、B21、B28、B38、B39、B40、B41 **非 LTE 帯域**： B87：WCDMA（欧州、日本、中国）2100 帯域 B91：WCDMA 米国 850 帯域 B92：WCDMA 日本 800 帯域 B114：WCDMA 欧州および日本 900 帯域 B115：WCDMA 日本 1700 帯域 B125：WCDMA 日本 850 帯域
P-LTEA-EA	EM7455	米国、カナダ、ヨーロッパ、中南米	**LTE 帯域**：帯域 B2、B4、B5、B13 **非 LTE 帯域**： B87：WCDMA（欧州、日本、中国）2100 帯域 B88：WCDMA 米国 PCS 1900 帯域 B89：WCDMA（欧州および中国）DCS 1800 帯域 B90：WCDMA 米国 1700 帯域 B91：WCDMA 米国 850 帯域 B114：WCDMA 欧州および日本 900 帯域

SFP のサポート

拡張モジュールの SFP インターフェイスは、ベースユニットとは動作が異なります。IR1101 ベースモジュールの SFP インターフェイスは、GigabitEthernet0/0/0 のコンボポート（SFP/RJ45）に組み込まれています。レイヤ 3（デフォルト）またはレイヤ 2 のインターフェイスとして設定できます。

拡張モジュールの SFP インターフェイスは SFP インターフェイスのみです。これは GigabitEthernet0/0/5 という名前のレイヤ 2 インターフェイスです。レイヤ 3 の機能セットの場合は、VLAN インターフェイスに割り当てる必要があります。

SFP インターフェイスに関する詳細は、次の例に示すように **show interfaces wireless detail** CLI を使用して表示できます。

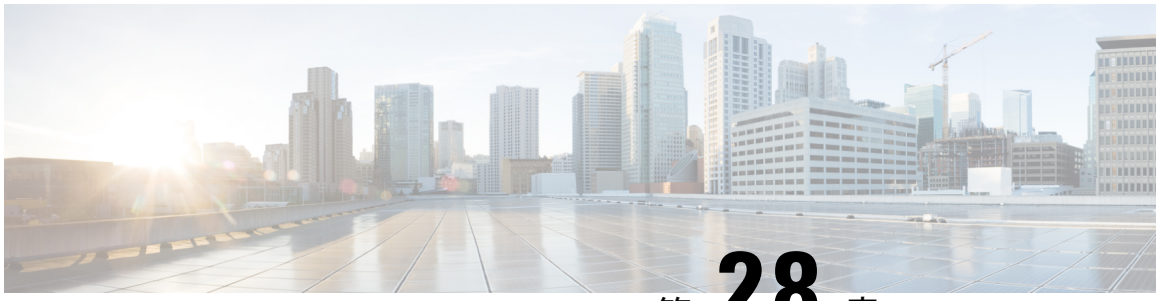
```
Router#show interfaces transceiver detail
IDPROM for transceiver Gigabitethernet0/0/0:
  Description                               = SFP or SFP+ optics (type 3)
  Transceiver Type:                         = GE T (26)
  Product Identifier (PID)                  = ABCU-5710RZ-CS4
  Vendor Revision                           =
  Serial Number (SN)                        = AGM151124J4
  Vendor Name                               = CISCO-AVAGO
  Vendor OUI (IEEE company ID)              = 00.17.6A (5994)
  CLEI code                                 =
  Cisco part number                         =
  Device State                              = Enabled.
  Date code (yy/mm/dd)                      = 11/03/21
  Connector type                            = Unknown.
  Encoding                                  = 8B10B (1)
  Nominal bitrate                           = GE (1300 Mbits/s)
  Minimum bit rate as % of nominal bit rate = not specified
  Maximum bit rate as % of nominal bit rate = not specified

Socket Verification

  SFP IDPROM Page 0xA0:
        000:        03 04 00 08 00 00 00 00 00 00
        010:        00 01 0D 00 00 00 00 00 64 00
        020:        43 49 53 43 4F 2D 41 56 41 47
        030:        4F 20 20 20 20 20 01 00 17 6A
        040:        41 42 43 55 2D 35 37 31 30 52
        050:        5A 2D 43 53 34 20 20 20 20 20
        060:        41 0C C1 15 00 10 00 00 41 47
        070:        4D 31 35 31 31 32 34 4A 34 20
        080:        20 20 20 20 31 31 30 33 32 31
        090:        20 20 00 00 00 99 00 00 06 17
        100:        C5 44 22 B7 DE 02 63 0F 59 73
        110:        64 EC A5 37 19 00 00 00 00 00
        120:        00 00 00 00 0F 2C 6D 22 FF FF
        130:        FF FF FF FF FF FF FF FF FF FF
        140:        FF FF FF FF FF FF FF FF FF FF
        150:        FF FF FF FF FF FF FF FF FF FF
        160:        FF FF FF FF FF FF FF FF FF FF
        170:        FF FF FF FF FF FF FF FF FF FF
        180:        FF FF FF FF FF FF FF FF FF FF
        190:        FF FF FF FF FF FF FF FF FF FF
        200:        FF FF FF FF FF FF FF FF FF FF
        210:        FF FF FF FF FF FF FF FF FF FF
        220:        FF FF FF FF

  SFP IDPROM Page 0xA2:
        000:        00 00 00 00 00 00 00 00 00 00
        010:        00 00 00 00 00 00 00 00 00 00
        020:        00 00 00 00 00 00 00 00 00 00
        030:        00 00 00 00 00 00 00 00 00 00
        040:        00 00 00 00 00 00 00 00 00 00
        050:        00 00 00 00 00 00 00 00 00 00
        060:        00 00 00 00 00 00 00 00 00 00
        070:        00 00 00 00 00 00 00 00 00 00
        080:        00 00 00 00 00 00 00 00 00 00
```

```
        090:        00 00 00 00 00 00 00 00 00 00
        100:        00 00 00 00 00 00 00 00 00 00
        110:        00 00 00 00 00 00 00 00 00 00
        120:        00 00 00 00 00 00 00 00 00 00
        130:        00 00 00 00 00 00 00 00 00 00
        140:        00 00 00 00 00 00 00 00 00 00
        150:        00 00 00 00 00 00 00 00 00 00
        160:        00 00 00 00 00 00 00 00 00 00
        170:        00 00 00 00 00 00 00 00 00 00
        180:        00 00 00 00 00 00 00 00 00 00
        190:        00 00 00 00 00 00 00 00 00 00
        200:        00 00 00 00 00 00 00 00 00 00
        210:        00 00 00 00 00 00 00 00 00 00
        220:        00 00 00 00 00 00 00 00 00 00
        230:        00 00 00 00 00 00 00 00 00 00
        240:        00 00 00 00 00 00 00 00 00 00
        250:        00 00 00 00 00 00
  Link reach for 9u fiber (km)                  = SX(550/270m) (0)
                                                  1xFC-MM(500/300m) (0)
                                                  2xFC-MM(300/150m) (0)
                                                  ESCON-MM(2km) (0)
  Link reach for 9u fiber (m)                   = SX(550/270m) (0)
                                                  1xFC-MM(500/300m) (0)
                                                  2xFC-MM(300/150m) (0)
                                                  ESCON-MM(2km) (0)
  Link reach for 50u fiber (m)                  = SR(2km) (0)
                                                  IR-1(15km) (0)
                                                  IR-2(40km) (0)
                                                  LR-1(40km) (0)
                                                  LR-2(80km) (0)
                                                  LR-3(80km) (0)
                                                  DX(40KM) (0)
                                                  HX(40km) (0)
                                                  ZX(80km) (0)
                                                  VX(100km) (0)
                                                  1xFC, 2xFC-SM(10km) (0)
                                                  ESCON-SM(20km) (0)
  Link reach for 62.5u fiber (m)                = SR(2km) (0)
                                                  IR-1(15km) (0)
                                                  IR-2(40km) (0)
                                                  LR-1(40km) (0)
                                                  LR-2(80km) (0)
                                                  LR-3(80km) (0)
                                                  DX(40KM) (0)
                                                  HX(40km) (0)
                                                  ZX(80km) (0)
                                                  VX(100km) (0)
                                                  1xFC, 2xFC-SM(10km) (0)
                                                  ESCON-SM(20km) (0)
  Nominal laser wavelength                  = 16652 nm.
  DWDM wavelength fraction                  = 16652.193 nm.
  Supported options                          = Tx disable
```

IP アドレスを持つ L3 SVI を拡張モジュール GE 0/0/5 SFP インターフェイスに割り当てます。

```
IR1101#config t
IR1101(config)#interface g0/0/5
IR1101(config-if)#switchport access vlan 2
IR1101(config-if)#no shut
IR1101(config-if)#interface vlan2
IR1101(config-if)#ip address 192.168.1.2 255.255.255.0
IR1101(config-if)#no shut
```

『CCisco Catalyst IR1101 Rugged Series Router Hardware Installation Guide』には、サポートされているすべての SFP インターフェイスが記載されています。



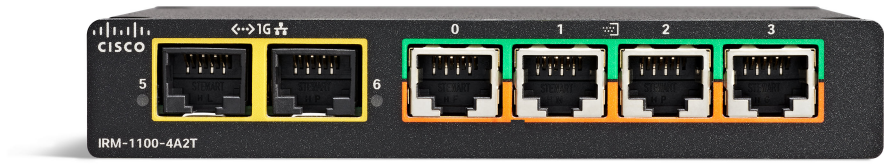
第 28 章

IRM-1100-4A2T 拡張モジュール

この章は、次の項で構成されています。

IRM-1100-4A2T の概要

IRM-1100-4A2T は、IR1101 に取り付けることのできる拡張モジュールです。IR1101 への追加の 4 つの非同期シリアルポートと 2 つのイーサネット インターフェイスを提供します。次の図は、IRM-1100-4A2T を示しています。



IRM-1100-4A2T イーサネット インターフェイスは、レイヤ 2 RJ45 10/100/1000 Mbps ポートです。

IRM-1100-4A2T シリアルポートは、RJ45 コンボポート（RS232/RS485/RS422）です。

IR1101 には、拡張モジュールを取り付けられる側面が 2 つあります。上部は拡張側、下部はコンピューティング側と呼ばれます。追加モジュールが上部に接続されている場合は、拡張モジュール（EM）側として参照されます。追加モジュールが下部に接続されている場合は、コンピューティング モジュール（CM）側として参照されます。機能は、拡張モジュールがどちら側に取り付けられているか、および使用されている拡張モジュールの数と種類によって異なります。

（注） 詳細については『Cisco Catalyst IR1101 Rugged Series Router Software Configuration Guide』をご覧ください

IRM-1100-4A2T は、次のツールから管理できます。

- Cisco DNA Center
- WebUI

ルータスイッチパス

プラットフォームで検出されるスイッチパスは、拡張モジュール（EM）側に接続されている追加モジュールのタイプに基づいています。次の表を参照してください。

追加モジュール	スイッチパス
モジュール未接続	IR1101-ES-5
IRM-1100-SPMI	IR1101-ES-6S
IRM-IR1100-4A2T	IR1101-ES-7G

（注） IRM-IR1100-4A2T が IR1101-K9 の両側に接続されている場合、列挙できる非同期インターフェイスは最大 9 つあります。IR1101-K9 のスイッチパスは IR1101-ES-7G になります。

シリアルポートのピン割り当てと特性

シリアルポートは、RS232 および RS485 の両方に対応する DCE ポートとして使用されます。RS485 は、全二重または半二重をサポートできます。

RJ45 のピン割り当てを次の図と表に示します。

図 *92 :* ピン配置

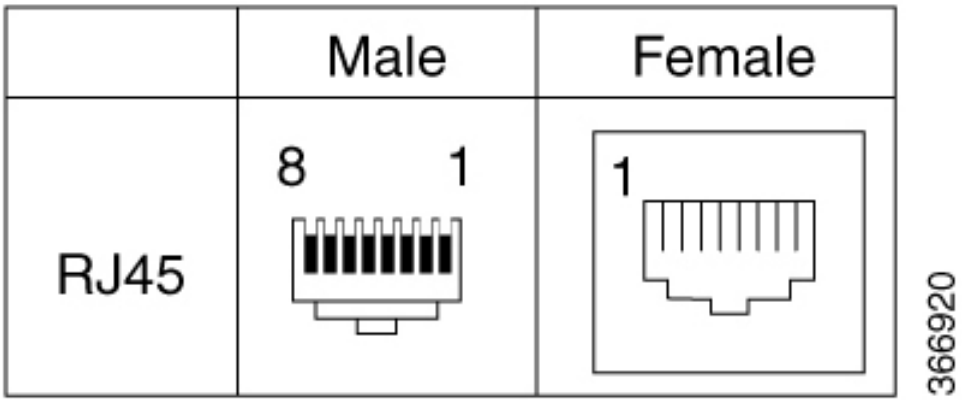


表 *16 :* シリアル ポートの特性

RS232					**RS485** 全二重		**RS485** 半二重	
ピン番号	**信号の説明**	**略称**	**S0（DTE）**	**S1（DCE）**	**信号**	**DIR**	**信号**	**DIR**
1	DCE レディ。 Cisco IOS では DSR として使用。	DSR/RI	入力	出力	TX-	出力	TX/RX+	<->
2	受信回線信号検出器	DCD	入力	出力	TX+	出力	TX/RX-	<->
3	DTE レディ	DTR	出力	入力	RX-	入力	—	—
4	信号用接地	COM	—	—	COM	—	COM	—
5	受信データ	RxD	入力	出力	—	—	—	—
6	送信データ	TxD	出力	入力	RX+	入力	—	—
7	送信可	CTS	入力	出力	—	—	—	—
8	送信要求	RTS	出力	入力	—	—	—	—

注意事項と制約事項

IRM-1100-4A2T には、次のガイドラインと制限事項があります。

- IOS-XE リリース 17.7.1 で利用可能
- 4 つの展開シナリオをサポート
- OIR のサポートなし

- イーサネットポートは L2 スイッチポートのみ
- コンピューティングモジュール側（下部）に何かが接続されている場合、スイッチポートは機能しません

IRM-1100-SPMI 拡張モジュールと IRM-1100-4A2T 拡張モジュールには、次のガイドラインと制限事項があります。

- CAT18 LTE モジュールはコンピューティング モジュール側（下部）ではサポートされていません
- コンピューティング モジュール側に接続されている場合、MSATA および GPIO ピンはサポートされません。
- IR1101 は、最大 2 つの LTE インターフェイスのみをサポートできます。これは、EM 側と CM 側の両方で拡張モジュールを LTE インターフェイスに接続することはサポートされていないことを意味します。接続すると EM 側のみアクティブになります。

展開シナリオ

IRM-1100-4A2T は、4 つの異なる展開シナリオをサポートしています。このセクションでは、この 4 つの機能の違いについて説明します。

インターフェイスの番号付けは、IRM-1100-4A2T モジュールの展開に基づいて列挙されます。

シナリオ 1

このシナリオでは、IRM-1100-4A2T は拡張側または上部に取り付けられています。次の図を参照してください。

この設定では、シリアルポートとイーサネットポートのすべての機能を利用できます。

4 つの追加の非同期インターフェイスと 2 つのギガビットイーサネットインターフェイスがサポートされています。

このシナリオでのインターフェイスの番号付けは次のとおりです。

- async 0/3/0（対応する回線：line 0/3/0）[シリアル]
- async 0/3/1（対応する回線：line 0/3/1）[シリアル]
- async 0/3/2（対応する回線：line 0/3/2）[シリアル]
- async 0/3/3（対応する回線：line 0/3/3）[シリアル]
- gigabitetherenet 0/0/5 [レイヤ 2]
- gigabitetherenet 0/0/6 [レイヤ 2]

シナリオ 2

このシナリオでは、IRM-1100-4A2T はコンピューティング側または下部に取り付けられています。さらに、このソリューションには、IRM-1100-SPMI 拡張モジュールが拡張側または上部に取り付けられています。次の図を参照してください。

この設定では、IRM-1100-4A2T のイーサネットポートは機能しません。シリアルポートは完全に機能します。

4 つの非同期インターフェイスがサポートされていますが、追加のレイヤ 2 インターフェイスはサポートされていません。

このシナリオでのインターフェイスの番号付けは次のとおりです。

- async 0/4/0（対応する回線：line 0/4/0）[シリアル]
- async 0/4/1（対応する回線：line 0/4/1）[シリアル]
- async 0/4/2（対応する回線：line 0/4/2）[シリアル]
- async 0/4/3（対応する回線：line 0/4/3）[シリアル]

シナリオ 3

このシナリオでは、IRM-1100-4A2T は拡張側または上部に取り付けられています。さらに、この設定では、IRM-1100-SPMI 拡張モジュールがコンピューティング側または下部に取り付けられています。次の図を参照してください。

この設定では、IRM-1100-4A2T は拡張側または上部に取り付けられ、完全に機能します。コンピューティング側または下部に取り付けられた IRM-1100-SPMI の SFP ポートは機能しません。

このシナリオでのインターフェイスの番号付けは次のとおりです。

- Async 0/3/0 – 0/3/3 [EM 側で接続]
- Async 0/4/0 – 0/4/3 [CM 側で接続]
- Gi0/0/5 および Gi0/0/6 [EM 側からのレイヤ 2 インターフェイス]
- CM 側の LTE インターフェイス、cellular 0/4/0 および cellular 0/4/1

シナリオ 4

このシナリオでは、拡張側とコンピューティング側の両方に 2 つの IRM-1100-4A2T 拡張モジュールが取り付けられています。次の図を参照してください。

この設定では、拡張側または上部に取り付けられた IRM-1100-4A2T がすべての機能を備えています。コンピューティング側または下部に取り付けられた IRM-1100-4A2T のイーサネットポートは機能しません。

8 つの非同期インターフェイスと 2 つのギガビットイーサネットインターフェイスがサポートされています。

このシナリオでのインターフェイスの番号付けは次のとおりです。

- Async 0/3/0 – 0/3/3 [EM 側で接続]
- Async 0/4/0 – 0/4/3 [CM 側で接続]
- Gi0/0/5 および Gi0/0/6 [EM 側からのレイヤ 2 インターフェイス]

配置に基づくインベントリの詳細

show inventory コマンドの出力には、IR1101 ベースユニットのどちら側に接続されているかに基づいて、さまざまな詳細が表示されます。

```
Router#sh inv
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9          , VID: V03  , SN: FCW2452P561
```

```
NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9          , VID: V03  , SN: FOC245126XR

NAME: "module subslot 0/0", DESCR: "IR1101-ES-7G"
PID: IR1101-ES-7G       , VID: V01  , SN:

NAME: "module subslot 0/4", DESCR: "P-LTE-MNA Module"
PID: P-LTE-MNA          , VID: V01  , SN: FOC24230U79

NAME: "Modem on Cellular0/4/0", DESCR: "Sierra Wireless WP7610"
PID: WP7610             , VID: 10000, SN: 356307100162618

NAME: "Module 2 - Compute Module", DESCR: "IR1100 expansion module with Pluggable slot,
 SFP, mSATA SSD slot and Digital GPIO"
PID: IRM-1100-SPMI      , VID: V02  , SN: FCW2502PAP0

NAME: "Module 3 - Expansion Module", DESCR: "IR1100 expansion module with 4 Async ports
 and 2 copper ports"
PID: IRM-1100-4A2T      , VID: V00  , SN: FOC25150ZRJ

Router# sh ip int bri
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  administratively down down
FastEthernet0/0/1      unassigned      YES unset  administratively down down
FastEthernet0/0/2      unassigned      YES unset  administratively down down
FastEthernet0/0/3      unassigned      YES unset  administratively down down
FastEthernet0/0/4      unassigned      YES unset  down                  down
GigabitEthernet0/0/5   unassigned      YES unset  administratively down down
GigabitEthernet0/0/6   unassigned      YES unset  down                  down
Cellular0/1/0          unassigned      YES NVRAM  administratively down down
Cellular0/1/1          unassigned      YES NVRAM  administratively down down
Async0/2/0             unassigned      YES unset  up up
Async0/3/0             unassigned      YES unset  up ip
Async0/4/0             unassigned      YES unset  administratively down down
Async0/3/1             unassigned      YES unset  administratively down down
Async0/4/1             unassigned      YES unset  administratively down down
Async0/3/2             unassigned      YES unset  administratively down down
Async0/4/2             unassigned      YES unset  administratively down down
Async0/3/3             unassigned      YES unset  administratively down down
Async0/4/3             unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  up                    down
```

ギガビット イーサネット スイッチ ポート

イーサネットポートは、レイヤ 2 RJ45 10/100/1000 Mbps ポートです。

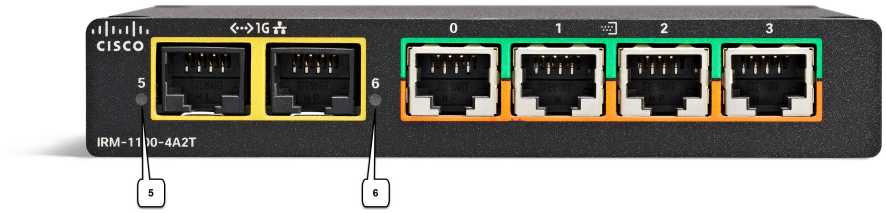
ベースルータ（IR1101）の GE ポートは、gigabitethernet 0/0/0 という名前です。IRM-1100-4A2T が拡張側または上部に取り付けられている場合、2 つの追加ポートを使用できます。

- gigabitethernet 0/0/5
- gigabitethernet 0/0/6

LED

前面には、2 つのイーサネットポート（5 と 6）に関連付けられた 2 つの LED があります。次の図を参照してください。

図 *93 :* イーサネット ポートの *LED*



LED の機能については、次の表を参照してください。

色/状態	説明
緑	ポートリンク、アクティビティなし
緑の点滅	アクティビティのある正常なリンク
消灯	リンクなし

LED ステータスは、コマンドラインからも使用できます。

```
Router# show led

 SYSTEM LED : Green

 Custom LED : Off

 VPN LED : Off

 ALARM LED : Off

 GigabitEthernet0/0/0 LED : On
 FastEthernet0/0/1    LED : On
 FastEthernet0/0/2    LED : Off
 FastEthernet0/0/3    LED : Off
 FastEthernet0/0/4    LED : Off
 GigabitEthernet0/0/5 LED : On
 GigabitEthernet0/0/6 LED : Off

 *Cellular 0/1*
 LTE module Enable LED : Green
 LTE module SIM 0 LED  : Off
 LTE module SIM 1 LED  : Off
 LTE module GPS LED    : Off
 LTE module RSSI 0 LED : Off
 LTE module RSSI 1 LED : Off
```

```
LTE module RSSI 2 LED : Off
LTE module RSSI 3 LED : Off
```

非同期ポート

IOS-XE リリース 17.7.1 ソフトウェアは、4 つの非同期ポートと 2 つのギガビット イーサネットインターフェイスを持つ追加モジュール（IRM-1100-4A2T）をサポートします。このソフトウェアは、ベースIR1101の拡張モジュールが取り付けられている側面に応じて、インターフェイス番号を列挙します。

ベースルータ（IR1101）の非同期ポートは async 0/2/0 であり、帯域外管理ポートは async 0/2/1 です。

IRM-1100-4A2Tが拡張側または上部に取り付けられている場合、非同期ポートは次のように番号付けされます。

- async 0/3/0（対応する回線：line 0/3/0）
- async 0/3/1（対応する回線：line 0/3/1）
- async 0/3/2（対応する回線：line 0/3/2）
- async 0/3/3（対応する回線：line 0/3/3）

IRM-1100-4A2Tがコンピューティング側または下部に取り付けられている場合、非同期ポートは次のように番号付けされます。

- async 0/4/0（対応する回線：line 0/4/0）
- async 0/4/1（対応する回線：line 0/4/1）
- async 0/4/2（対応する回線：line 0/4/2）
- async 0/4/3（対応する回線：line 0/4/3）

IRM-1100-4A2T の非同期ポートは以下をサポートします。

- メディアタイプ RS232（DCE）および RS485（RS422 と RS485 は同じ設定を共有します）
- 全二重/半二重

シリアル RJ45 のピン割り当て

すべてのシリアルポートは、次の 3 つの動作モードにすることができます。

- RS232
- RS485 全二重
- RS485 半二重

すべてのポートはRS232信号規格に準拠し、サポートされる最大ボーレートは115Kbpsです。次の表は、4 つのポートのピン割り当てを示しています。

ピン番号	説明	モード	方向
1	データ セット レディ	DCE	OUT
2	DCD/リング	DCE	OUT
3	データ端末レディ	DCE	IN
4	信号用接地	—	—
5	受信データ	DCE	OUT
6	送信データ	DCE	IN
7	送信可	DCE	OUT
8	送信要求	DCE	IN

DCE インターフェイスの設定手順

シリアル拡張モジュールのすべてのポートのデフォルトのインターフェイス設定は、RS232です。インターフェイスがメディアタイプRS485に設定されている場合、デフォルト設定は全二重モードです。

- GI0/0/5 および Gi0/0/6 の設定は、IR1101 ベースユニットの L2 ポートと同様です。
- 非同期ポートは、RS232 および RS485 の全二重と半二重の両方をサポートします。さらに、IR1101 ベースユニットの async 0/2/0 と比較して、拡張モジュールでは「メディアタイプ」、「全二重」、および「半二重」がサポートされます。

デフォルト設定

シリアル拡張モジュールのすべてのポートのデフォルト設定は、RS232 です。

```
Router#sh run int Async0/3/0
Building configuration...

Current configuration : 92 bytes

interface Async0/3/0
no ip address
encapsulation scada
shutdown
media-type rs232
```

メディアタイプ RS232 の設定例

CLI **media-type ?** は rs232 と rs485 が利用可能であることを示しています。

```
Router(config)#int Async0/3/3
Router(config-if)#media
Router(config-if)#media-type ?
 rs232 Set RS232 media type
 rs485 Set RS485 media type
```

RS232 のメディアタイプを設定します。

```
Router(config-if)#media-type rs232
Router(config-if)#no shut
Router(config-if)#end

Router#sh run int Async0/3/3
Building configuration...
!
Current configuration : 82 bytes
!
interface Async0/3/3
 no ip address
 encapsulation scada
 media-type rs232
 end
```

メディアタイプ RS485 の設定例

RS485 のメディアタイプを設定します。

```
Router#conf t
Enter configuration commands, one per line.
Router(config)#int Asyn0/3/0
Router(config-if)#media
Router(config-if)#media-type rs485
Router(config-if)#end

Router# sh run int Async0/3/0

Building configuration...

Current configuration : 105 bytes
!
interface Async0/3/0
 no ip address
 encapsulation scada
 shutdown
 media-type rs485
 full-duplex
end
```

メディアタイプ RS485（半二重）の設定例

半二重を実行している RS485 のメディアタイプを設定します。

```
Router(config)#int Async0/4/2
Router(config-if)#media
Router(config-if)#media-type rs485
Router(config-if)#half-duplex
Router(config-if)#end

Router#sh run int Async0/4/2
Building configuration...

Current configuration : 105 bytes
!
```

```
interface Async0/4/2
 no ip address
 encapsulation scada
 shutdown
 media-type rs485
 half-duplex
```

GPIO 設定ピン

IRM-1100-4A2T には、GPIO ピンを使用してハードウェアに信号を送信する 4 つの非同期ポートがあり、メディアタイプとデュプレックスの設定が設定されます。以下は、GPIO ピンが RS232 として設定された「6」、RS485 全二重として設定された「4」、および RS485 半二重として設定された「C」に設定されている場合の標準的な信号の例です。

```
Router#sh controllers Async0/3/0
Line: 0/3/0(74) Interface:Async0/3/0
State=6 encapsulation=95 speed=9600 maxmtu=1500
Duplex=0 ACCM_TX=0xFFFFFFFF ACCM_RX=0xFFFFFFFF
Max_idle=10 frame_size=100
Buffered bytes=0 tty capabilities=0x8 tty statbits=0x40 databits=8
TX packet cnt:0 Scattered: 0 Particle cnt:0 Request cnt:0
PPP in total:0
PPP Rx head:0x0 tail:0x0
GPIO read: 6666
```

（注） 上記の出力では、すべての非同期ポート 0/3/0 ～ 0/3/3 は、デフォルトのメディアタイプ RS232 で設定されています。

```
Router#sh controllers Async0/4/2
Line: 0/4/2(100) Interface:Async0/4/2
State=6 encapsulation=95 speed=9600 maxmtu=1500
Duplex=0 ACCM_TX=0xFFFFFFFF ACCM_RX=0xFFFFFFFF
Max_idle=10 frame_size=100
Buffered bytes=0 tty capabilities=0x8 tty statbits=0x40 databits=8
TX packet cnt:0 Scattered: 0 Particle cnt:0 Request cnt:0
PPP in total:0
PPP Rx head:0x0 tail:0x0
GPIO read: 6C66
```

（注） 上記の出力では、非同期ポート 0/4/2 は RS485 半二重で設定され、残りのポートの Async0/4/0、0/4/1 および 0/4/3 はデフォルトのメディアタイプ RS232 で設定されます。

```
Router# sh controllers Async0/3/3
Line: 0/3/3(77) Interface:Async0/3/3
State=4 encapsulation=97 speed=9600 maxmtu=1500
Duplex=0 ACCM_TX=0xFFFFFFFF ACCM_RX=0xFFFFFFFF
Max_idle=10 frame_size=100
Buffered bytes=0 tty capabilities=0x8 tty statbits=0x440 databits=8
TX packet cnt:0 Scattered: 0 Particle cnt:0 Request cnt:0
PPP in total:0
```

```
PPP Rx head:0x0 tail:0x0
GPIO read: 4666
```

（注） 上記の出力では、非同期ポート 0/3/3 は RS485 全二重で設定され、残りのポートの Asyn0/3/0、Async0/3/1、および Async0/3/2 はデフォルトのメディアタイプ RS232 で設定されます。

debug コマンド

GPIO 設定のトラブルシューティングに使用できるデバッグコマンドがあります。

```
Router# debug condition interface <ASYNC_INTERFACE_SLOT> event
```

（注） このコマンドは、Async 0/2/0 インターフェイスではサポートされていません。

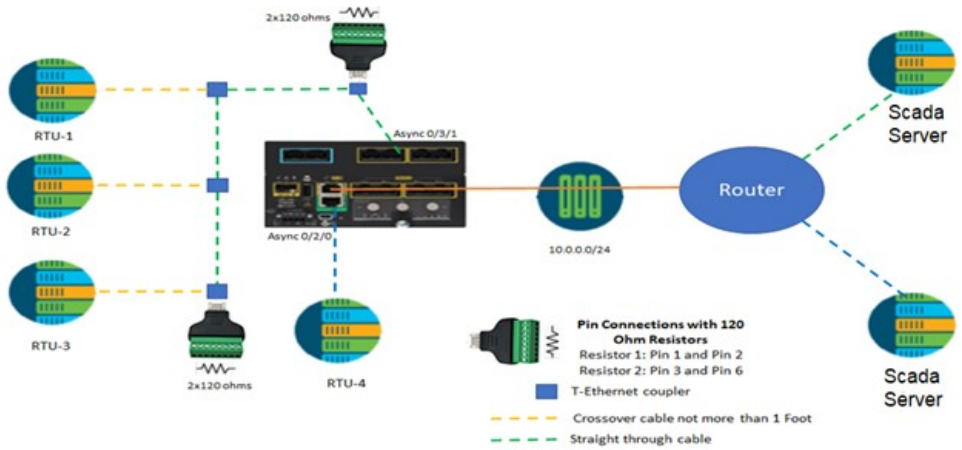
追加の非同期インターフェイスの設定例

詳細については、『IR1101 Rugged Series Router Software Configuration Guide』の「Raw Socket Transport」 の章を参照してください

Raw-TCP マルチホップ（デイジーチェーン）

raw-tcp の場合、ユーザーは raw-tcp カプセル化を非同期インターフェイスで設定し、関連するラインインターフェイスをサーバーまたはクライアントとして設定する必要があります。サーバーあたりのセッションの最大数は 32 です。

図 *94 : Raw-TCP* マルチホップの例

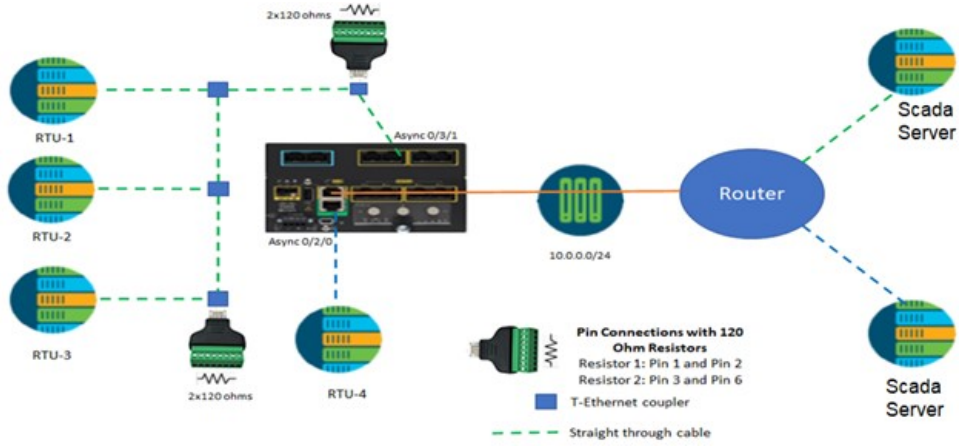


以下に、上記の 2 台のルータの設定例を示します。

IR1101	その他のルータ （注） 少なくとも 2 つのシリアルインターフェイスをサポートする IOS-XE ルータまたは IOS ルータを設定できます。
int Async0/2/0 encapsulation raw-tcp no shut int Async 0/3/1 encapsulation raw-tcp media-type rs485 full-duplex no shut line 0/2/0 raw-socket tcp client 10.0.0.2 6000 10.0.0.1 6001 line 0/3/1 raw-socket tcp client 10.0.0.2 5000 10.0.0.1 5001	int Async 0/2/0 encapsulation raw-tcp no shut int Async 0/2/1 encapsulation raw-tcp no shut line 0/2/0 raw-socket tcp server 6000 line 0/2/1 raw-socket tcp server 5000

Raw-UDP マルチホップ（デイジーチェーン）

図 *95 : Raw-UDP* マルチホップの例



以下に、上記の 2 台のルータの設定例を示します。

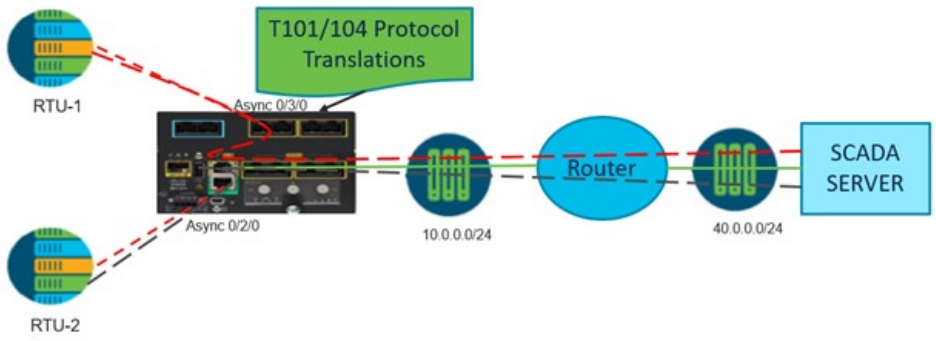
IR1101	その他のルータ （注） 少なくとも 2 つのシリアルインターフェイスをサポートする IOS-XE ルータまたは IOS ルータを設定できます。
int Async0/2/0 encapsulation raw-udp no shut int Async 0/3/1 encapsulation raw-udp media-type rs485 half-duplex no shut line 0/2/0 raw-socket udp connection 10.0.0.2 6001 6000 10.0.0.1 line 0/3/1 raw-socket udp connection 10.0.0.2 5001 5000 10.0.0.1	int Async 0/2/0 encapsulation raw-udp no shut int Async 0/2/1 encapsulation raw-udp no shut line 0/2/0 raw-socket udp connection 10.0.0.1 6000 6001 10.0.0.2 line 0/2/1 raw-socket udp connection 10.0.0.1 5000 5001 10.0.0.2

SCADA プロトコル変換

詳細については、『IR1101 Rugged Series Router Software Configuration Guide』の「Information About SCADA」の章を参照してください

T101/T104

図 *96 : T101/T104* 設定例



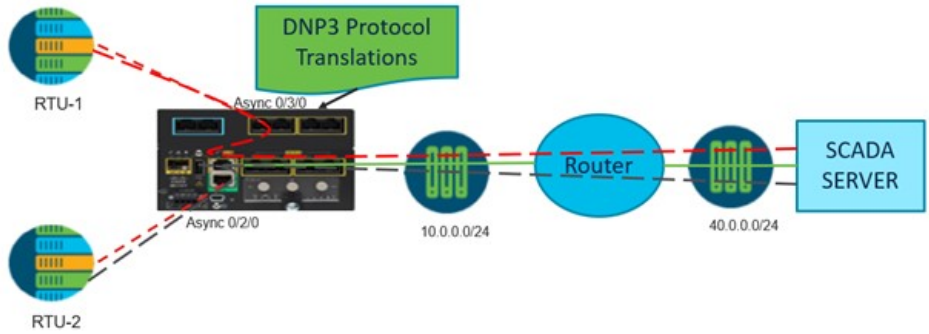
次に、上記の図の設定例を示します。

表 *17 : T101/T104* 設定例

int Async0/2/0 encapsulation scada no shut	scada-gw protocol t101 channel rt-chan-1 link-mode balanced bind-to-interface Async0/2/0 session rt-sess-1 attach-to-channel rt-chan-1 common-addr-size one cot-size two info-obj-addr-size three link-addr 31 sector rt-sec-1 attach-to-session rt-sess-1 asdu-addr 100	Scada-gw protocol t104 channel mt-chan-1 t3-timeout 20 tcp-connection 0 local-port 5000 remote-ip any session mt-sess-1 attach-to-channel mt-chan-1 sector mt-sec-1 attach-to-session mt-sess-1 asdu-addr 120 map-to-sector rt-sec-1
int Async0/3/0 encapsulation scada media-type rs485 half-duplex no shut	channel rt-chan-2 link-mode balanced bind-to-interface Async0/3/0 session rt-sess-2 attach-to-channel rt-chan-2 common-addr-size one cot-size two info-obj-addr-size three link-addr 32 sector rt-sec-2 attach-to-session rt-sess-2 asdu-addr 101	channel mt-chan-2 t3-timeout 20 tcp-connection 0 local-port 6000 remote-ip any session mt-sess-2 attach-to-channel mt-chan-2 sector mt-sec-2 attach-to-session mt-sess-2 asdu-addr 121 map-to-sector rt-sec-2 scada-gw enable

DNP3 IP/シリアル

図 *97 : DNP3 IP/*シリアル設定例



次に、上記の図の設定例を示します。

表 *18 : DNP3 IP*/シリアル設定例

int Async0/2/0 encapsulation scada no shut	scada-gw protocol dnp3-serial channel dnp3_serial_channel_1 link-addr source 5 request-timeout 60 link-timeout 6 unsolicited-response enable bind-to-interface Async0/2/0 no protocol test-link session dnp3_serial_session_1 attach-to-channel dnp3_serial_channel_1 link-addr dest 1	scada-gw protocol dnp3-ip channel dnp3_ip_channel_1 link-addr dest 3 send-unsolicited-msg enable tcp-connection local-port 5000 remote-ip any session dnp3_ip_session_1 attach-to-channel dnp3_ip_channel_1 link-addr source 7 map-to-session dnp3_serial_session_1
int Async0/3/0 encapsulation scada media-type rs485 half-duplex no shut	channel dnp3_serial_channel_2 link-addr source 6 request-timeout 60 link-timeout 6 unsolicited-response enable bind-to-interface Async0/3/0 no protocol test-link session dnp3_serial_session_2 attach-to-channel dnp3_serial_channel_2 link-addr dest 2	channel dnp3_ip_channel_2 link-addr dest 5 send-unsolicited-msg enable tcp-connection local-port 6000 remote-ip any session dnp3_ip_session_2 attach-to-channel dnp3_ip_channel_2 link-addr source 8 map-to-session dnp3_serial_session_2 scada-gw protocol ignore direction scada-gw enable

シリアルリレー

シリアルリレーは、IRM-1100-4A2T のすべての非同期ポートでサポートできます。任意の順序でマッピングできます。インターフェイスで設定された「カプセル化リレーライン」を使用した非同期インターフェイスのマッピング。例：

- relay line 0/0/0 0/2/0
- relay line 0/0/1 0/3/2
- relay line 0/0/2 0/3/0
- relay line 0/0/3 0/3/1
- relay line 0/0/4 0/4/0

詳細については、『IR1101 Configuration Guide』の「Serial Relay Service」の章を参照してください。

WebUI を使用して非同期ポートを設定

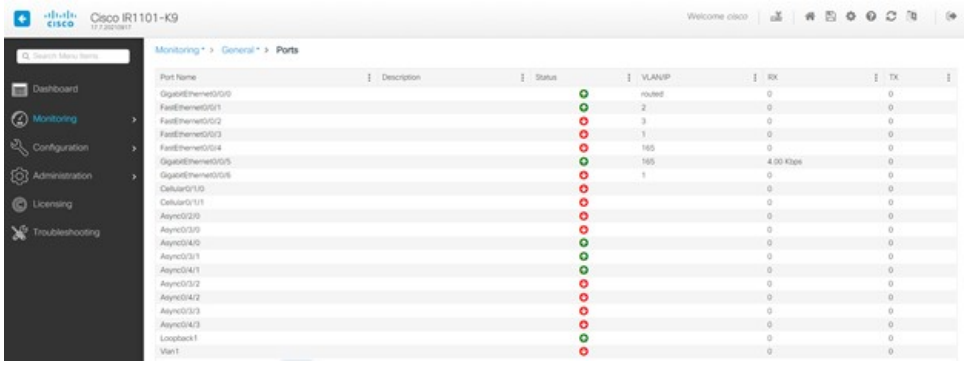
次の手順を使用して、WebUI を介して非同期ポートを設定します。

始める前に

Cisco IOS XE リリースは、非同期インターフェイスの設定および検証の基本テンプレートとして WebUI サポート（Day-1）をサポートします。

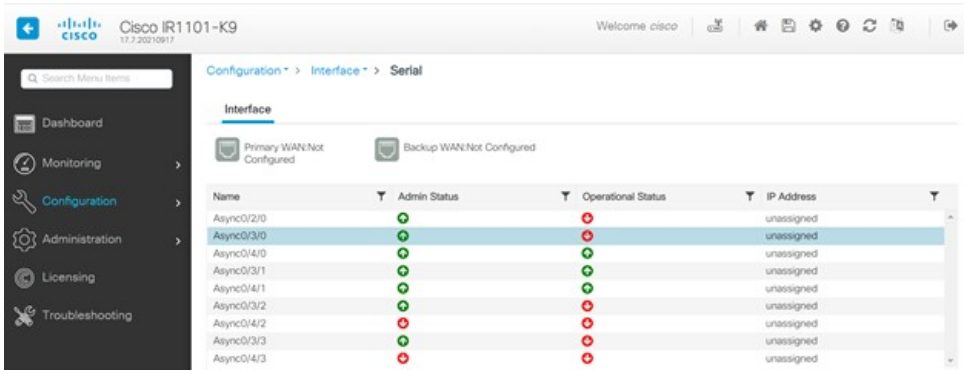
[Monitoring] > [General] > [Ports] に移動して、ポートを監視できます。

図 *98 :* モニター ポート（***Monitor Ports***）



ステップ 1 [Configuration] > [Interface] > [Interface] に移動します。

図 *99 :* シリアル ポート



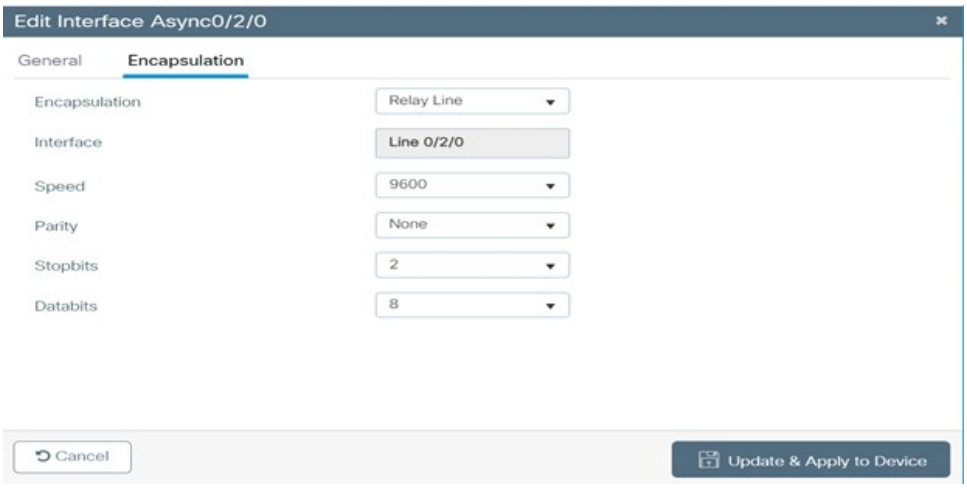
ステップ 2 編集するインターフェイスをダブルクリックします。**Edit Interface** [Interface Number] ウィンドウが表示されます。

図 *100* : インターフェイスの編集

ベース IR1101 の Async0/2/0 インターフェイスは、デフォルトでメディアタイプの RS232 をサポートします。このインターフェイスに関連付けられているメディアタイプを変更することはできません。

ステップ 3 [Edit Interface] ウィンドウの [Encapsulation] タブをクリックします。

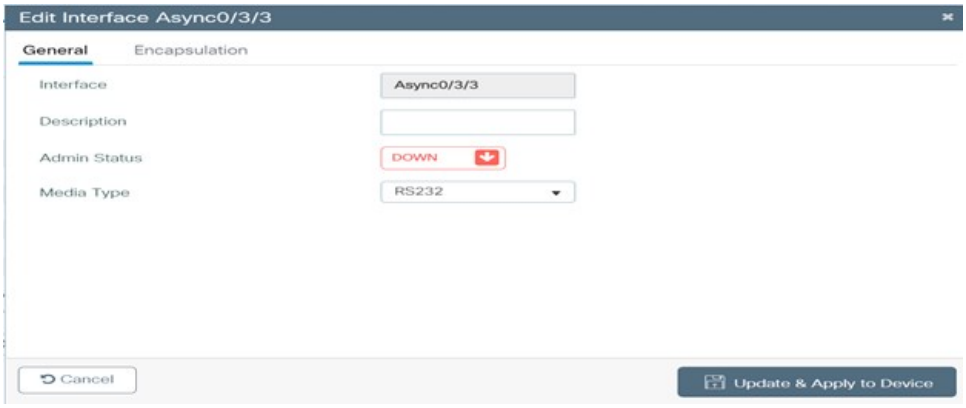
図 *101 : [Edit Interface]*（*[Encapsulation]*）



必要に応じて、Async0/2/0 インターフェイスおよび関連するラインインターフェイスのカプセル化を変更できます。ドロップダウンリストから、IR1101 の非同期インターフェイスでサポートされている値を選択します。

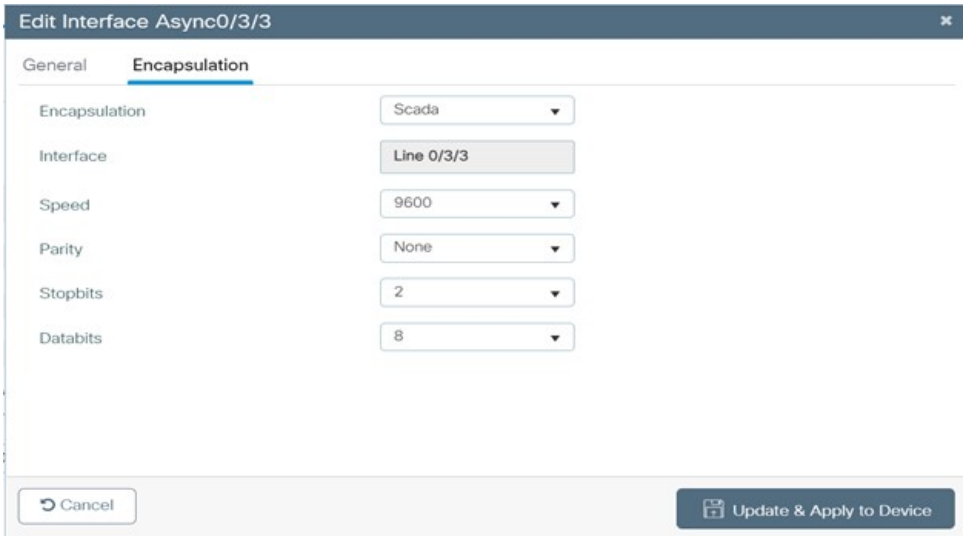
ステップ 4 同じ手順を実行して [Edit Interface] ウィンドウに移動し、IRM-1100-4A2T の非同期ポートを設定します。たとえば、Async0/3/3 インターフェイスを編集します。

図 *102 : Async0/3/3* インターフェイスの編集

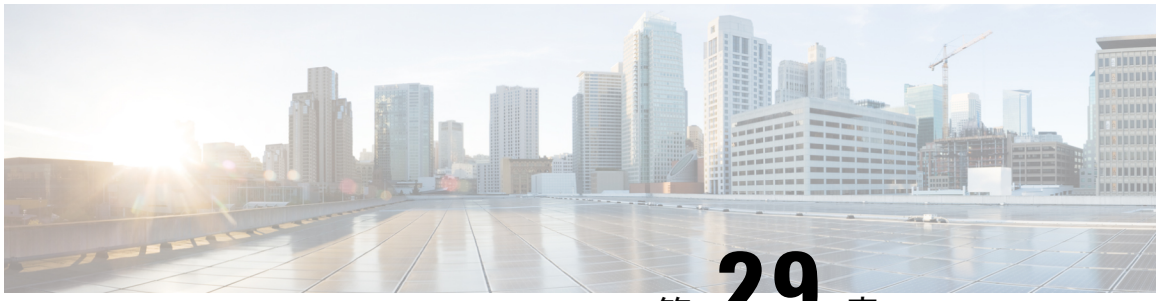


IRM-1100-4A2T のポートでは、ドロップダウンボックスからメディアタイプを変更できます。RS485 を選択した場合は、全二重または半二重を選択できます。

図 *103 : Async0/3/3* インターフェイスの編集（*[Encapsulation]* タブ）



ステップ 5 選択に問題がなければ、**Update & Apply to Device** をクリックします。



第 29 章

システム メッセージ

この章は、次の項で構成されています。

プロセス管理について

Telnet プロトコルを使ってコンソールにログインし、Telnet プロトコルをサポートする任意のワークステーションからシステム コンポーネントを監視することで、システム メッセージを確認できます。

ソフトウェアの開始と監視は、プロセス管理と呼ばれます。ルータのプロセス管理インフラストラクチャはプラットフォームに依存しないため、Cisco IOS XE が稼働するプラットフォーム全体でエラー メッセージが一貫しています。ユーザがプロセス管理に直接関与する必要はありませんが、プロセス障害などの問題を示すシステム メッセージを確認することをお勧めします。

エラー メッセージの詳細の検索方法

プロセス管理または syslog エラー メッセージについての詳細を表示するには、エラー メッセージ デコーダ ツール（https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi）でエラー メッセージを入力します。

たとえば、`%PMAN-0-PROCESS_NOTIFICATION` というメッセージをこのツールに入力すると、このエラー メッセージの説明と推奨処置が表示されます。

いくつかのエラー メッセージに関して、エラー メッセージ デコーダ ツールで表示される説明と推奨処置の例を以下に示します。

エラー メッセージ：`%PMAN-0-PROCESS_NOTIFICATION : The process lifecycle notification component failed because [chars]`

説明	推奨処置

プロセス ライフサイクル通知コンポーネントで障害が発生し、これが原因でプロセスの開始と停止を適切に検出できません。この問題は、ソフトウェア サブパッケージでのソフトウェアの不具合が原因で発生する可能性があります。	メッセージの時刻を書きとめ、カーネルエラーメッセージログを調べて問題の詳細を理解し、エラーが修正可能かどうかを確認してください。問題を解決できない場合、またはログが有用ではない場合は、コンソールに出力されたエラーメッセージ全体と、**show tech-support** コマンドの出力をそのままコピーし、収集した情報をシスコのテクニカル サポートに提出してください。

エラー メッセージ：`%PMAN-0-PROCFAILCRIT A critical process [chars] has failed (rc [dec])`

説明	推奨処置
ルータが機能するために必要な、重要なプロセスが失敗しました。	メッセージの時刻を書きとめ、エラーメッセージ ログを調査して、問題の詳細について理解してください。問題が解消されない場合は、コンソールまたはシステム ログに出力されたメッセージをそのままコピーします。http://www.cisco.com/tac で提供されているツールやユーティリティを使用して問題を調べ、解決してください。ツールやユーティリティのメッセージによって明確な情報が得られます。解決済みのソフトウェアの問題を検索するには、Bug Search Tool（http://www.cisco.com/cisco/psn/bssprt/bss）を使用します。さらに支援が必要な場合は、http://tools.cisco.com/ServiceRequestTool/create/ にアクセスして Technical Assistance Center でケースをオープンするか、シスコのテクニカルサポート担当者に問い合わせて、収集した情報を提出してください。**show logging** コマンドおよび **show tech-support** コマンドの出力結果および関連するトラブルシューティング ログを、提出する情報に、プレーンテキスト（.txt）形式で圧縮せずに添付してください。

エラー メッセージ：`%PMAN-3-PROCFAILOPT An optional process [chars] has failed (rc [dec])`

説明	推奨処置

トラフィックの転送に影響しないプロセスで、障害が発生しました。	メッセージの時刻を書きとめ、カーネルエラー メッセージ ログを調査して、問題の詳細について理解してください。このメッセージの受信後もトラフィックは引き続き転送されますが、このメッセージが原因でルータの一部の機能が無効になる可能性があるため、エラーを調査する必要があります。ログが有用ではないか、そこに示されている問題を解決できない場合は、コンソールまたはシステム ログに出力されたメッセージをそのままコピーします。http://www.cisco.com/tac で提供されているツールやユーティリティを使用して問題を調べ、解決してください。ツールやユーティリティのメッセージによって明確な情報が得られます。解決済みのソフトウェアの問題を検索するには、Bug Search Tool（http://www.cisco.com/cisco/psn/bssprt/bss）を使用します。さらに支援が必要な場合は、http://tools.cisco.com/ServiceRequestTool/create/ にアクセスして Technical Assistance Center でケースをオープンするか、シスコのテクニカルサポート担当者に問い合わせて、収集した情報を提出してください。**show logging** コマンドおよび **show tech-support** コマンドの出力結果および関連するトラブルシューティング ログを、提出する情報に、プレーンテキスト（.txt）形式で圧縮せずに添付してください。

エラー メッセージ：`%PMAN-3-PROCFAIL The process [chars] has failed (rc [dec])`

説明	推奨処置

エラーが発生したためにプロセスが失敗しました。	このメッセージは、プロセスに関連する他のメッセージとともに表示されます。他のメッセージを調べて失敗の理由を判別し、修正処置を実行できるかどうかを確認します。問題が解消されない場合は、コンソールまたはシステム ログに出力されたメッセージをそのままコピーします。http://www.cisco.com/tac で提供されているツールやユーティリティを使用して問題を調べ、解決してください。ツールやユーティリティのメッセージによって明確な情報が得られます。解決済みのソフトウェアの問題を検索するには、Bug Search Tool（http://www.cisco.com/cisco/psn/bssprt/bss）を使用します。さらに支援が必要な場合は、http://tools.cisco.com/ServiceRequestTool/create/ にアクセスして Technical Assistance Center でケースをオープンするか、シスコのテクニカルサポート担当者に問い合わせて、収集した情報を提出してください。**show logging** コマンドおよび **show tech-support** コマンドの出力結果および関連するトラブルシューティング ログを、提出する情報に、プレーンテキスト（.txt）形式で圧縮せずに添付してください。

エラー メッセージ：`%PMAN-3-PROCFAIL_IGNORE [chars] process exits and failures are being ignored due to debug settings. Normal router functionality will be affected. Critical router functions like RP switchover, router reload, FRU resets, etc. may not function properly.`

説明	推奨処置
ユーザにより設定されたデバッグ設定のため、プロセス障害は無視されます。	この動作が意図されたものであり、ユーザの設定に基づいてデバッグ設定が行われている場合、対処は不要です。このメッセージが表示されることが問題であると判断される場合は、デバッグ設定を変更します。このデバッグ設定では通常、ルータは正常に動作しません。SSO スイッチオーバー、ルータのリロード、FRU リセットなどの機能が影響を受けます。この設定は、デバッグを実行する場合にだけ使用してください。通常は、この設定でルータを動作させることはありません。

エラー メッセージ：`%PMAN-3-PROCHOLDDOWN The process [chars] has been helddown (rc [dec])`

説明	推奨処置

繰り返し発生する障害に伴って行われたプロセス再起動の回数が多すぎるため、ホールドダウン状態になりました。	このメッセージは、プロセスに関連する他のメッセージとともに表示されます。他のメッセージを調べて失敗の理由を判別し、修正処置を実行できるかどうかを確認します。問題が解消されない場合は、コンソールまたはシステム ログに出力されたメッセージをそのままコピーします。http://www.cisco.com/tac で提供されているツールやユーティリティを使用して問題を調べ、解決してください。ツールやユーティリティのメッセージによって明確な情報が得られます。解決済みのソフトウェアの問題を検索するには、Bug Search Tool（http://www.cisco.com/cisco/psn/bssprt/bss）を使用します。さらに支援が必要な場合は、http://tools.cisco.com/ServiceRequestTool/create/ にアクセスして Technical Assistance Center でケースをオープンするか、シスコのテクニカルサポート担当者に問い合わせて、収集した情報を提出してください。**show logging** コマンドおよび **show tech-support** コマンドの出力結果および関連するトラブルシューティング ログを、提出する情報に、プレーンテキスト（.txt）形式で圧縮せずに添付してください。

エラー メッセージ：`%PMAN-3-RELOAD_RP_SB_NOT_READY : Reloading: [chars]`

説明	推奨処置
準備のできたスタンバイ インスタンスがないため、ルート プロセッサがリロードされています。	リロードが、エラー状態に起因するものではないことを確認してください。

エラー メッセージ：`%PMAN-3-RELOAD_RP : Reloading: [chars]`

説明	推奨処置
RP がリロードされています。	リロードが、エラー状態に起因するものではないことを確認してください。エラー状態に起因している場合は、他のログ メッセージで要求されている情報を収集します。

エラー メッセージ：`%PMAN-3-RELOAD_SYSTEM : Reloading: [chars]`

説明	推奨処置

システムがリロードされています。	リロードが、エラー状態に起因するものではないことを確認してください。エラー状態に起因している場合は、他のログ メッセージで要求されている情報を収集します。

エラー メッセージ：`%PMAN-3-PROC_BAD_EXECUTABLE : Bad executable or permission problem with process [chars]`

説明	推奨処置
プロセスで使用される実行可能ファイルに問題があるか、またはアクセス許可に関する問題があります。	示されている実行可能ファイルを正しい実行可能ファイルに置き換えます。

エラー メッセージ：`%PMAN-3-PROC_BAD_COMMAND:Non-existent executable or bad library used for process <process name>`

説明	推奨処置
プロセスで使用される実行可能ファイルが存在していないか、または依存ライブラリに問題があります。	示されている実行可能ファイルが存在しており、依存ライブラリに問題がないことを確認します。

エラー メッセージ：`%PMAN-3-PROC_EMPTY_EXEC_FILE : Empty executable used for process [chars]`

説明	推奨処置
プロセスで使用される実行可能ファイルが空です。	示されている実行可能ファイルのサイズがゼロではないことを確認します。

エラー メッセージ：`%PMAN-5-EXITACTION : Process manager is exiting: [chars]`

説明	推奨処置
プロセス マネージャを終了します。	プロセス マネージャの終了が、エラー状態に起因するものではないことを確認します。エラー状態に起因している場合は、他のログメッセージで要求されている情報を収集します。

エラー メッセージ：`%PMAN-6-PROCSHUT : The process [chars] has shutdown`

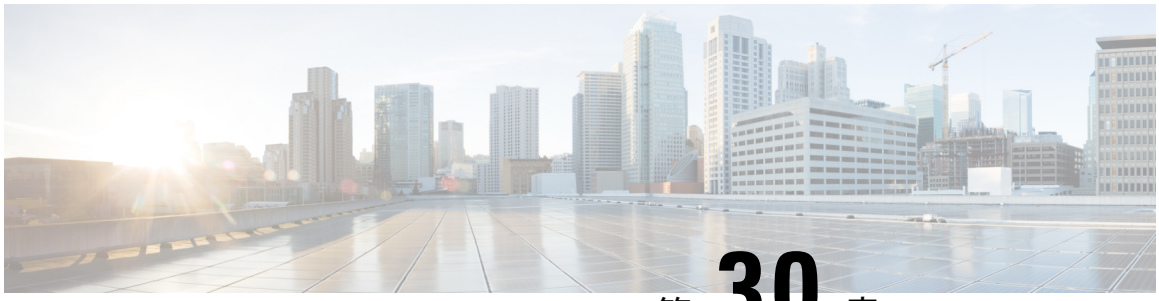
説明	推奨処置
プロセスのグレースフル シャットダウンが完了しました。	ユーザによる操作は必要ありません。このメッセージは、通知目的で示されます。

エラー メッセージ： `%PMAN-6-PROCSTART : The process [chars] has started`

説明	推奨処置
プロセスが正常に起動され、正常に稼働しています。	ユーザによる操作は必要ありません。このメッセージは、通知目的で示されます。

エラー メッセージ：`%PMAN-6-PROCSTATELESS : The process [chars] is restarting stateless`

説明	推奨処置
プロセスがステートレス再起動を要求しました。	ユーザによる操作は必要ありません。このメッセージは、通知目的で示されます。



第 30 章

環境モニタ

環境モニタ

ルータには、システム温度を監視する複数のセンサーを備えた強力な環境モニタ システムがあります。環境モニタ システムの主要な機能の一部を以下に示します。

- CPU およびマザーボードの温度監視
- 異常なイベントの記録と通知の生成
- 簡易ネットワーク管理プロトコル（SNMP）トラップの監視
- オンボード障害ロギング（OBFL）データの生成と収集
- Call Home イベント通知の送信
- システム エラー メッセージの記録
- 現在の設定およびステータスの表示

環境モニタおよびリポート機能

モニタおよびリポート機能により、環境状態が悪化する前に状態を特定し、解決することができるので、システムの正常な稼働を維持できます。

- 環境モニタ機能 （350 ページ）
- 環境レポート機能 （351 ページ）

環境モニタ機能

環境モニタ機能では、センサーを使用して、シャーシ内部を流れる冷却空気の温度を監視します。

ルータの環境動作条件は、次を満たしている必要があります

- 非動作時温度：-40 ～ 70 °C（-40 ～ 158 °F）
- 非動作時湿度：5 ～ 95% 相対湿度（結露しないこと）
- 動作温度：

  -40 ～ 60 °C（-40 ～ 140 °F）：エアーフローなしの密閉型 NEMA キャビネット内

  -40 ～ 70 °C（-40 ～ 158 °F）：エアーフロー 40 lfm の自然通気型キャビネット内

  -40 ～ 75 °C（-40 ～ 167 °F）：エアーフロー 200 lfm の強制通気型キャビネット内
- 動作時湿度：10 ～ 95% 相対湿度（結露しないこと）
- 動作時の高度：–500 ～ 5,000 フィート。304.8 m（1,000 フィート）ごとに最大動作温度が 1.5 °C ずつ低下。

次の表に、環境モニタリング システムで使用されるステータス状態のレベルを示します。

表 *19*：環境モニタリング システムで使用されるステータス状態のレベル

ステータス レベル	説明
標準	監視対象のすべてのパラメータが通常の許容範囲内にあります。
警告	システムが特定のしきい値を超えています。システムは稼働し続けますが、オペレータが操作してシステムをノーマル ステートに戻すことを推奨します。
重大	温度または電圧条件が許容値を超えています。システムは引き続き動作しますが、やがてシャットダウンします。ただちにオペレータが操作する必要があります。

たとえば以下に示す状態が発生した場合、環境モニタリング システムからコンソールにメッセージが送信されます。

温度および電圧が最大または最小しきい値を超えている

温度または電圧の最大しきい値と最小しきい値を示す警告メッセージを次の例に示します。

```
Warnings :
--------
For all the temperature sensors (name starting with “Temp:”) above,
the critical warning threshold is 100C (100C and higher)
the warning threshold is 80C (range from 80C to 99C)
the low warning threshold is 1C (range from -inf to 1C).
```

```
For all voltage sensors (names starting with "V:"),
the high warning threshold starts at that voltage +10%. (voltage + 10% is warning)
the low warning threshold starts at the voltage -10%. (voltage - 10% is warning)
```

環境レポート機能

次のコマンドを使用して、環境ステータス レポートを取得および表示できます。

- **show diag all eeprom**
- **show environment**
- **show environment all**
- **show inventory**
- **show platform**
- **show platform diag**
- **show platform software status control-processor**
- **show diag slot R0 eeprom detail**
- **show version**
- **show power**

これらのコマンドは、温度や電圧などのパラメータの現在値を表示します。

環境モニタリング システムにより、これらのパラメータの値が 60 秒ごとに更新されます。これらのコマンドの簡単な例を以下に示します。

show diag all eeprom：例

```
Router# show diag all eepromMIDPLANE EEPROM data:

Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
Asset ID :
CLEI Code : UNASSIGNED
Power/Fan Module P0 EEPROM data is not initialized

Power/Fan Module P1 EEPROM data is not initialized

Slot R0 EEPROM data:

Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
```

```
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
CLEI Code : UNASSIGNED
Slot F0 EEPROM data:

Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
CLEI Code : UNASSIGNED
Slot 0 EEPROM data:

Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
CLEI Code : UNASSIGNED
SPA EEPROM data for subslot 0/0:

Product Identifier (PID) : IR1101-ES-5
Version Identifier (VID) : V01
PCB Serial Number :
Top Assy. Part Number : 68-2236-01
Top Assy. Revision : A0
Hardware Revision : 2.2
CLEI Code : CNUIAHSAAA
SPA EEPROM data for subslot 0/1 is not available

SPA EEPROM data for subslot 0/2 is not available

SPA EEPROM data for subslot 0/3 is not available

SPA EEPROM data for subslot 0/4 is not available

SPA EEPROM data for subslot 0/5 is not available

Router#
```

show environment：例

```
Router# show environment
Number of Critical alarms: 0
Number of Major alarms: 0
Number of Minor alarms: 0

Slot Sensor Current State Reading Threshold(Minor,Major,Critical,Shutdown)
---------- -------------- --------------- ------------
---------------------------------------
R0 Temp: LM75BXXX Normal 43 Celsius (75 ,80 ,90 ,na )(Celsius)
```

```
Router#
```

show environment all：例

```
Router# show environment all
Sensor List: Environmental Monitoring
Sensor Location State Reading
Temp: LM75BXXX R0 Normal 48 Celsius
```

show inventory：例

```
Router# show inventory
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9 , VID: V00 , SN: FCW2132TH0Z

NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9 , VID: , SN:

NAME: "module subslot 0/0", DESCR: "IR1101-ES-5"
PID: IR1101-ES-5 , VID: V01 , SN:

NAME: "subslot 0/0 transceiver 0", DESCR: "GE SX"
PID: GLC-SX-MM-RGD , VID: V01 , SN: FNS16370HL4

NAME: "module subslot 0/1", DESCR: "P-LTE-US Module"
PID: P-LTE-US , VID: V01 , SN: FOC21333R92

NAME: "Modem 0 on Cellular0/1/0", DESCR: "Sierra Wireless WP7603"
PID: WP7603 , VID: 10000, SN: 359528080000794
```

show platform：例

```
Router# show platform
Chassis type: IR1101-K9

Slot Type State Insert time (ago)
--------- ------------------- ---------------------- -----------------
0 IR1101-K9 ok 01:52:41
0/0 IR1101-ES-5 ok 01:51:35
R0 IR1101-K9 ok, active 01:52:41
F0 IR1101-K9 init, active 01:52:41
Router#
```

show platform diag：例

```
Router# show platform diag
Chassis type: IR1101-K9
```

```
Slot: 0, IR1101-K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:25 (5d02h ago)
Software declared up time : 00:01:07 (5d02h ago)
CPLD version :
Firmware version : 1.3

Sub-slot: 0/0, IR1101-ES-5
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:02:21 (5d02h ago)
Logical insert detect time : 00:02:21 (5d02h ago)

Sub-slot: 0/1, P-LTE-US
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:02:21 (5d02h ago)
Logical insert detect time : 00:02:21 (5d02h ago)

Slot: R0, IR1101-K9
Running state : ok, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:25 (5d02h ago)
Software declared up time : 00:00:25 (5d02h ago)
CPLD version : 00000000
Firmware version : 1.2

Slot: F0, IR1101-K9
Running state : init, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:25 (5d02h ago)
Software declared up time : 00:01:10 (5d02h ago)
Hardware ready signal time : 00:00:00 (never ago)
Packet ready signal time : 00:00:00 (never ago)
CPLD version : 00000000
Firmware version : 1.2

Router#
```

show platform software status control-processor：例

```
Router# show platform software status control-processor
RP0: online, statistics updated 9 seconds ago
Load Average: healthy
1-Min: 0.32, status: healthy, under 5.00
5-Min: 0.33, status: healthy, under 5.00
15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
Total: 3959840
Used: 2894588 (73%), status: healthy
Free: 1065252 (27%)
Committed: 2435656 (62%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 0.50, System: 0.91, Nice: 0.00, Idle: 98.07
```

```
IRQ: 0.40, SIRQ: 0.10, IOwait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 0.81, System: 0.30, Nice: 0.00, Idle: 98.48
IRQ: 0.20, SIRQ: 0.20, IOwait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 0.81, System: 2.65, Nice: 0.00, Idle: 95.41
IRQ: 1.12, SIRQ: 0.00, IOwait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 7.66, System: 17.05, Nice: 0.00, Idle: 70.58
IRQ: 4.59, SIRQ: 0.10, IOwait: 0.00


Router#
```

show diag slot R0 eeprom detail：例

```
Router# show diag slot R0 eeprom detail
Slot R0 EEPROM data:

EEPROM version : 4
Compatible Type : 0xFF
Controller Type : 3457
Hardware Revision : 0.2
PCB Part Number : 73-18820-03
Board Revision : 02
Deviation Number : 0
Fab Version : 02
PCB Serial Number : FOC22106KKH
Top Assy. Part Number : 68-6479-03
Top Assy. Revision : 04
Chassis Serial Number : FCW2213TH07
Deviation Number : 0
RMA Test History : 00
RMA Number : 0-0-0-0
RMA History : 00
Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
CLEI Code : UNASSIGNED
Manufacturing Test Data : 00 00 00 00 00 00 00 00
Field Diagnostics Data : 00 00 00 00 00 00 00 00
Chassis MAC Address : 682c.7b4d.7880
MAC Address block size : 128
Asset ID :
Asset Alias :
PCB Part Number : 73-18821-03
Board Revision : 03
Deviation Number : 0
Fab Version : 02
PCB Serial Number : FOC22106KHD
PCB Part Number : 73-19117-02
Board Revision : 02
Deviation Number : 0
Fab Version : 01
PCB Serial Number : FOC22106KJ9
Asset ID :
Router#
```

show version：例

```
Router# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version
 16.10.1prd7, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 31-Oct-18 23:27 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 1 hour, 53 minutes
Uptime for this control processor is 1 hour, 54 minutes
System returned to ROM by reload
System image file is "usb0:ir1101-universalk9.16.10.01prd7.SPA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package Technology-package
Current Type Next reboot
------------------------------------------------------------------------------
network-advantage Smart License network-advantage


Smart Licensing Status: UNREGISTERED/EVAL EXPIRED

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 711867K/6147K bytes of memory.
Processor board ID FCW2150TH0F
1 Virtual Ethernet interface
4 FastEthernet interfaces
```

```
1 Gigabit Ethernet interface
1 Serial interface
1 terminal line
32768K bytes of non-volatile configuration memory.
4038072K bytes of physical memory.
3110864K bytes of Bootflash at bootflash:.
0K bytes of WebUI ODM Files at webui:.
30670832K bytes of USB Flash at usbflash0:.

Configuration register is 0x0 (will be 0x2102 at next reload)

Router#
```

show power：例

```
Router# show power
Main PSU :
Total Power Consumed: 8.16 Watts
Router#
```

その他の参考資料

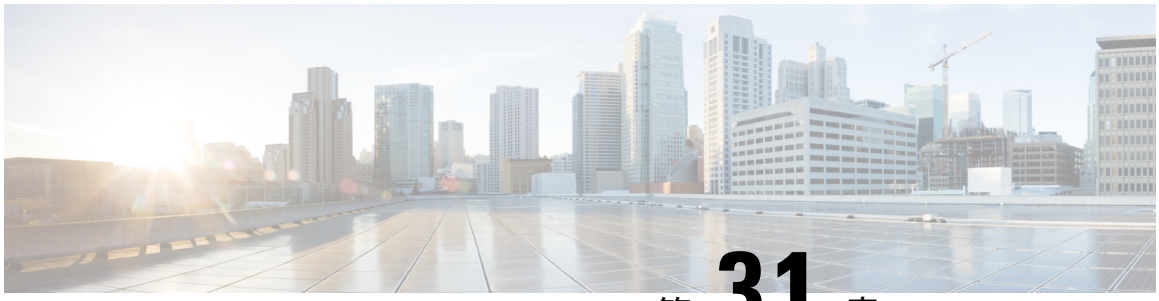
以降のセクションで、電力効率管理機能に関連した参考資料について説明します。

MIB

MIB	MIB のリンク
CISCO-ENTITY-FRU-CONTROL-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を検索およびダウンロードするには、http://www.cisco.com/go/mibs にある Cisco MIB Locator を使用してください。

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html



第 31 章

IOx アプリケーション ホスティング

この章は、次の項で構成されています。

アプリケーション ホスティング

ホスト アプリケーションは、サービス ソリューションとしてのソフトウェアであり、コマンドを使用してリモートで実行できます。アプリケーションのホスティングによって、管理者には独自のツールやユーティリティを利用するためのプラットフォームが与えられます。

このモジュールでは、アプリケーション ホスティング機能とその有効化の方法について説明します。

アプリケーション ホスティングに関する情報

アプリケーション ホスティングの必要性

仮想環境への移行により、再利用可能なポータブルかつスケーラブルなアプリケーションを構築する必要性が高まりました。アプリケーションのホスティングによって、管理者には独自のツールやユーティリティを利用するためのプラットフォームが与えられます。ネットワーク デバイスでホスティングされているアプリケーションは、さまざまな用途に利用できます。これは、既存のツールのチェーンによる自動化から、設定管理のモニタリング、統合に及びます。

Cisco のデバイスは Linux ツール チェーンを使用して構築されたサードパーティ製の市販アプリケーションをサポートしています。ユーザは、シスコが提供するソフトウェア開発キットと相互にコンパイルされたカスタム アプリケーションを実行できます。

IOx の概要

IOx は Cisco が開発したエンド ツー エンド アプリケーション フレームワークであり、Cisco ネットワーク プラットフォーム上のさまざまなタイプのアプリケーションに対し、アプリケーション ホスティング機能を提供します。

IR1101 向けの IOx アーキテクチャは、ハイパーバイザ アプローチを使用する他のシスコ プラットフォームとは異なります。他のプラットフォームでは、IOx は仮想マシンとして動作します。一方 IR1101 では、IOx はプロセスとして動作しています。

シスコ アプリケーションのホスティングの概要

IR1101 では、ユーザは、アプリケーション ホスティング CLI を使用してアプリケーションを展開できます。アプリケーション ホスティング CLI は、他の古いプラットフォームでは利用できません。アプリケーションを展開する方法は他に Local Manager または Fog Director を使用する方法があります。

アプリケーション ホスティングは、次のサービスを提供します。

- コンテナ内の指定されたアプリケーションを起動する。
- 使用可能なリソース（メモリ、CPU、およびストレージ）を確認し、それらを割り当て、管理する。
- コンソール ロギングのサポートを提供する。
- REST API を介してサービスへのアクセスを提供する。
- CLI エンドポイントを提供する。
- Cisco Application Framework（CAF）と呼ばれるアプリケーション ホスティング インフラストラクチャを提供する。
- VirtualPortGroup および管理インターフェイスを介したプラットフォーム固有のネットワーキング（パケットパス）のセットアップを支援する。

コンテナは、ホスト オペレーティング システムでゲスト アプリケーションを実行するために提供される仮想環境と呼ばれています。Cisco IOS XE 仮想化サービスは、ゲスト アプリケーションを実行するための管理性とネットワーキング モデルを提供します。仮想化インフラストラクチャにより、管理者はホストとゲスト間の接続を指定する論理インターフェイスを定義できます。IOx は、論理インターフェイスをゲスト アプリケーションが使用する仮想ネットワーク インターフェイス カード（vNIC）にマッピングします。

コンテナに展開されるアプリケーションは、TAR ファイルとしてパッケージ化されます。これらのアプリケーションに固有の設定は、TAR ファイルの一部としてもパッケージ化されています。

デバイス上の管理インターフェイスは、アプリケーション ホスティング ネットワークを IOS 管理インターフェイスに接続します。アプリケーションのレイヤ 3 インターフェイスは、IOS

管理インターフェイスからレイヤ2ブリッジ トラフィックを受信します。管理インターフェイスは、管理ブリッジを使用してコンテナ/アプリケーション インターフェイスに接続します。IPアドレスは、管理インターフェイスIPアドレスと同じサブネット上にある必要があります。

IOXMAN

IOXMANは、シリアルデバイスをエミュレートするLibvirtを除く、ゲスト アプリケーションのロギングまたはトレース サービスを提供するトレース インフラストラクチャを確立するプロセスです。IOXMAN は、ゲスト アプリケーションのライフサイクルに基づいて、トレース サービスを有効または無効にし、ロギング データを IOS syslog に送信し、トレース データを IOx トレース ログに保存し、各ゲスト アプリケーションの IOx トレースロ グを維持します。

IR1101 ルータでのアプリケーション ホスティング

ここでは、IR1101産業向けルータに固有のアプリケーションホスティングの特性について説明します。

（注） IR1101 CPU は、他のルータのように x86 アーキテクチャに基づいていません。したがって、アプリケーションが ARM 64 ビット アーキテクチャに準拠している必要があります。

アプリケーション ホスティングは、アプリケーション ホスティング CLI、Local Manager および Fog Director を使用して実現できます。

IOx URL アクセス方法

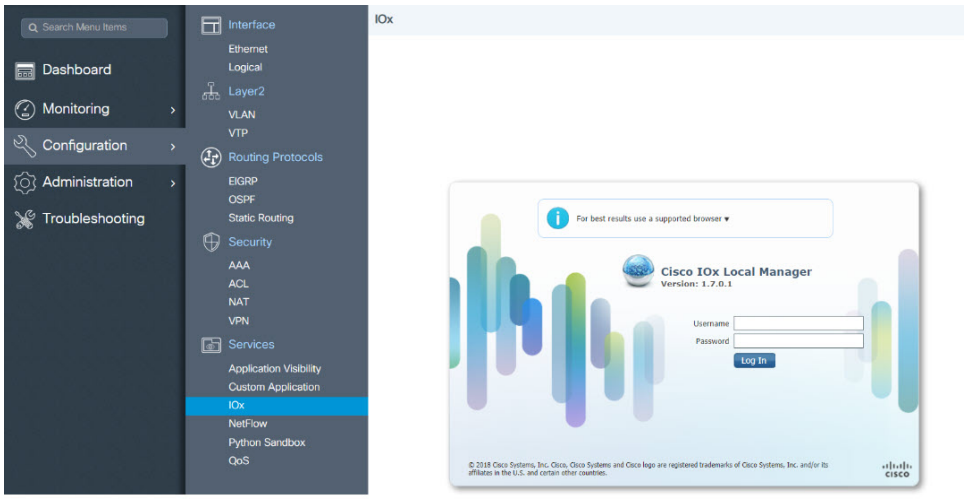
IOx URL には、2 つの異なる方法でアクセスできます。

1. IOx ログインへの直接 URL を使用します。
2. Web ユーザーインターフェイス（WebUI）を介して IOx ログインに移動します。

1 番目の方法の構文は、**https://***IR1101-IP-ADDRESS***/iox/login** です。

2 番目の方法の構文は、**https://***IR1101-IP-ADDRESS* で、その後、次に示すように IOx に移動します。

図 *104 : Local Manager*



1. WebUI から、**[Configuration] > [Services] > [IOx]** をクリックします。

2. 設定されたユーザ名とパスワードを使用してログインします。

3. 『Cisco IOx Local Manager Reference Guide』のアプリケーション ライフサイクルの手順を実行します。

IOX URL ユーザー制限

2 番目の方法では、IOx ユーザーがルータ全体の設定を使用できるようにします。一部の組織では、IOx ユーザーはルータを管理するユーザーとは異なります。この場合、IOx ユーザーのアクセスをルータの WebUI 全体ではなく、IOx ローカルマネージャ WebUI のみに制限する必要があります。

現在、IOx ユーザーは権限 15 ユーザーとして設定されています。IOx ユーザーをローカルマネージャのみに制限するために、次のコマンドを使用できます。

```
Router(conf)# no ip http server
Router(conf)# ip http secure-server
Router(conf)# ip http session-module-list list2 OPENRESTY_PKI,NG_WEBUI
Router(conf)# ip http secure-active-session-modules list2
```

コマンド **no ip http server** は、https のない Web サーバーをオフにします。次のコマンド **ip http secure-server** は https モードをオンにします。

OPENRESTY_PKI と NG_WEBUI のみを含めると、IOX ローカル マネージャ モジュールのみが有効になるため、すべてのユーザーは、権限 15、https://IR1101-IP-ADDRESS/iox/login がある場合にのみ IOX ローカルマネージャにアクセスできます。

さらに、すべてのユーザーに対して、WebUI アクセス、**https://***IR1101-IP-ADDRESS* が無効になります。

（注） この方法は、すべてのユーザーに対してメイン Web ページ **https://***IR1101-IP-ADDRESS* を無効にし、すべてのユーザーに対して **https://***IR1101-IP-ADDRESS***/iox/login** のみを有効にします。一般的な管理と設定に IR1101 メインルータ WebUI を使用しない場合は、この方法を使用します。

VirtualPortGroup

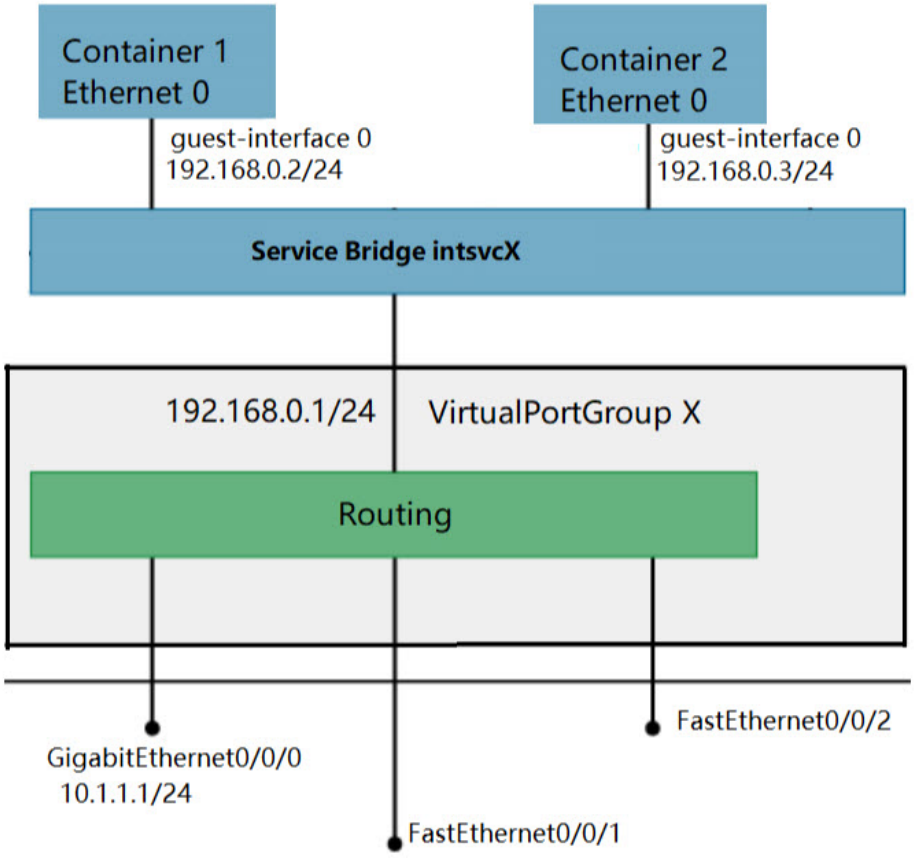
VirtualPortGroup は、Linux ブリッジ IP アドレスにマッピングする Cisco IOS 上のソフトウェア構成要素です。そのため、VirtualPortGroup は、Linux コンテナのスイッチ仮想インターフェイス（SVI）を表します。各ブリッジには、複数のインターフェイスを含めることができ、それぞれ異なるコンテナにマッピングされます。各コンテナには、複数のインターフェイスを含めることもできます。

VirtualPortGroup インターフェイスは、interface virtualportgroup コマンドを使用して設定します。これらのインターフェイスが作成されると、IP アドレスとその他のリソースが割り当てられます。

VirtualPortGroup インターフェイスは、アプリケーション ホスティング ネットワークを IOS ルーティング ドメインに接続します。アプリケーションのレイヤ 3 インターフェイスは、IOS からルーティングされたトラフィックを受信します。VirtualPortGroup インターフェイスは、SVC ブリッジを介してコンテナ/アプリケーション インターフェイスに接続します。

IR8x9 ルータとは異なるため、次の図は VirtualPortGroup とその他のインターフェイス間の関係を理解する上で役に立ちます。

図 *105* : 仮想ポート グループ マッピング



vNIC

コンテナのライフサイクル管理には、内部論理インターフェイスごとに 1 つのコンテナをサポートするレイヤ 3 ルーティング モデルが使用されます。これは、各アプリケーションに対して仮想イーサネットペアが作成されることを意味します。このペアのうち vNIC と呼ばれるインターフェイスは、アプリケーション コンテナの一部です。vpgX と呼ばれるもう 1 つのインターフェイスは、ホスト システムの一部です。

NIC は、コンテナ内の標準イーサネットインターフェイスで、プラットフォームデータプレーンに接続してパケットを送受信します。IOx は、コンテナ内の各 vNIC について、ゲートウェイ（VirtualPortGroup インターフェイス）、IP アドレス、および一意の MAC アドレス割り当てを行います。

コンテナ/アプリケーション内の vNIC は、標準のイーサネットインターフェイスと見なされています。

アプリケーション ホスティングの設定方法

IOx の有効化

IOx Local Manager へのアクセスを有効にするには、次の作業を実行します。IOx Local Manager を使用することで、ホスト システム上のアプリケーションの管理、制御、モニタ、トラブルシューティング、および関連するさまざまなアクティビティを実行できます。

（注） 次の手順では、IP HTTP コマンドは IOX を有効にしませんが、ユーザは WebUI にアクセスして IOX Local Manager に接続できるようになります。

手順の詳細

手順	コマンド	目的
1.	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
2.	**configure terminal** 例： `Device#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。
3.	**iox** 例： `Device(config)#iox`	IOx を有効にします

手順	コマンド	目的
4.	**ip http server** 例： `Device(config)#ip http server`	IP または IPv6 システム上の HTTP サーバを有効化します。
5.	**ip http secure-server** 例： `Device(config)#ip http secure-server`	セキュア HTTP（HTTPS）サーバを有効にします。
6.	**username** *name* **privilege** *level* **password** {**0** | **7** | *user-password* }*encrypted-password* 例： `Device(config)#username cisco privilege 15 password 0 cisco`	ユーザー名ベースの認証システムとユーザーの権限レベルを確立します。 ユーザー名の特権レベルは 15 に設定する必要があります。
7.	**end** 例： `Device(config-if)#end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 3 データ ポートへの VirtualPortGroup の設定

複数のレイヤ 3 データポートを 1 つ以上の VirtualPortGroup またはコンテナにルーティングできます。VirutalPortGroups とレイヤ 3 のデータポートは、異なるサブネット上にある必要があります。

レイヤ 3 データポートで外部ルーティングを許可するには、**ip routing** コマンドを有効にします。

手順の詳細

ステップ	コマンド
1.	**enable** 例： `Device>enable`
2.	**configure terminal** 例： `Device#configure terminal`
3.	**ip routing** 例： `Device(config)#ip routing`
4.	**interface type number** 例： `Device(config)#interface gigabitethernet 0/0/0`
5.	**no switchport** 例： `Device(config-if)#no switchport`

ステップ	コマンド
6.	**ip address ip-address mask** 例： `Device(config-if)#ip address 10.1.1.1 255.255.255.0`
7.	**exit** 例： `Device(config-if)#exit`
8.	**interface type number** 例： `Device(config)#interface virtualportgroup 0`
9.	**ip address ip-address mask** 例： `Device(config-if)#ip address 192.168.0.1 255.255.255.0`
10.	**end** 例： `Device(config-if)#end`
11.	**configure terminal** Enter configuration commands, one per line. CNTL/Z で終了します。 例： `Device#configure terminal`
12.	**app-hosting appid app1** 例： `Device(config)#app-hosting appid app1`

ステップ	コマンド
13.	**app-vnic gateway0 virtualportgroup 0 guest-interface 0** 例： `Device(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0`
14.	**guest-ipaddress 192.168.0.2 netmask 255.255.255.0** 例： `Device(config-app-hosting-gateway0)#guest-ipaddress 192.168.0.2 netmask 255.255.255`
15.	**app-default-gateway 192.168.0.1 guest-interface 0** 例： `Device(config-app-hosting-gateway0)#app-default-gateway 192.168.0.1 guest-interface`
16.	**end** 例： `Device#end`

アプリケーションのインストールとアンインストール

手順の詳細

ステップ	コマンド
1.	**enable** 例： `Device>enable`

ステップ	コマンド
2.	**app-hosting install appid** *application-name* **package** *package-path* 例： `Device#app-hosting install appid lxc_app package flash:my_iox_app.tar`
3.	**app-hosting activate appid** *application-name* 例： `Device#app-hosting activate appid app1`

ステップ	コマンド
4.	**app-hosting start appid** *application-name* 例： `Device#app-hosting start appid app1`
5.	**app-hosting stop appid** *application-name* 例： `Device#app-hosting stop appid app1`
6.	**app-hosting deactivate appid** *application-name* 例： `Device#app-hosting deactivate appid app1`
7.	**app-hosting uninstall appid** *application-name* 例： `Device#app-hosting uninstall appid app1`

アプリケーションのリソース設定の上書き

リソースの変更は、app-hosting activate コマンドが設定された後にのみ有効になります。

手順の詳細

ステップ	コマンド
1.	**enable** 例： `Device>enable`
2.	**configure terminal** 例： `Device#configure terminal`
3.	**app-hosting appid** *name* 例： `Device(config)#app-hosting appid app1`
4.	**app-resource profile** *name* 例： `Device(config-app-hosting)#app-resource profile custom`
5.	**cpu** *unit* 例： `Device(config-app-resource-profile-custom)# cpu 800`

ステップ	コマンド
6.	**memory** *memory* 例： `Device(config-app-resource-profile-custom)# memory 512`
7.	**vcpu** *number* 例： `Device(config-app-resource-profile-custom)# vcpu 2`
8.	**end** 例： `Device(config-app-resource-profile-custom)# end`

アプリケーションホスティングコンフィギュレーションの確認

手順の詳細

1. **enable**

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

Example:

```
Device>enable
```

2. show iox-service

すべての IOx サービスのステータスを表示します。

Example:

```
Device# show iox-service
IOx Infrastructure Summary:
---------------------------------------
IOx service (CAF) 1.8.0.2 : Running
IOx service (HA) : Not Supported
IOx service (IOxman) : Running
Libvirtd 1.3.4 : Running
Device#
```

3. show app-hosting detail

アプリケーションに関する詳細情報を表示します。

Example:

```
Device#show app-hosting detail
App id                 : app1
Owner                  : iox
State                  : RUNNING
Application
  Type                 : lxc
  Name                 : nt08-stress
  Version              : 0.1
  Description          : Stress Testing Application
  Path                 : usbflash0: my_iox_app.tar
Activated profile name : custom
Resource reservation
  Memory               : 64 MB
  Disk                 : 2 MB
  CPU                  : 500 units
Attached devices
  Type              Name               Alias
  ---------------------------------------------
  serial/shell     iox_console_shell   serial0
  serial/aux       iox_console_aux     serial1
  serial/syslog    iox_syslog          serial2
  serial/trace     iox_trace           serial3

Network interfaces
   ---------------------------------------
eth0:
   MAC address         : 52:54:dd:fa:25:ee
```

4. show app-hosting list

アプリケーションとそれらのステータスの一覧を表示します。

Example:

```
Device#show app-hosting list
App id                           State
---------------------------------------------------------
app1                             RUNNING
```

アプリケーション ホスティングの設定例

次の例を参照してください。

例：IOx の有効化

```
Device> enable
Device# configure terminal
Device(config)# iox
Device(config)# ip http server
Device(config)# ip http secure-server
Device(config)# username cisco privilege 15 password 0 cisco
Device(config)# end
```

例：レイヤ 3 データ ポートへの VirtualPortGroup の設定

```
Device> enable
Device# configure terminal
Device(config)# ip routing
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no switchport
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface virtualportgroup 0
Device(config-if)# ip address 192.168.0.1 255.255.255.0
Device(config-if)# end
```

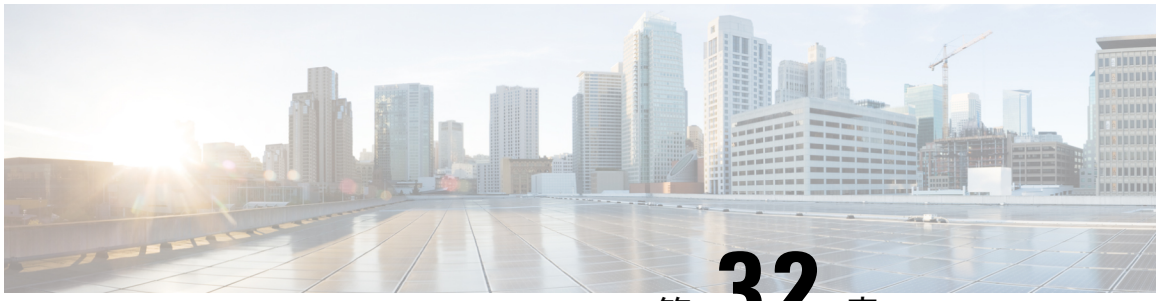
例：アプリケーションのインストールとアンインストール

```
Device> enable
Device# app-hosting install appid app1 package flash:my_iox_app.tar
Device# app-hosting activate appid app1
Device# app-hosting start appid app1
Device# app-hosting stop appid app1
Device# app-hosting deactivate appid app1
Device# app-hosting uninstall appid app1
```

例：アプリケーションのリソース設定の上書き

```
Device# configure terminal
Device(config)# app-hosting appid app1
Device(config-app-hosting)# app-resource profile custom
Device(config-app-resource-profile-custom)# cpu 800
Device(config-app-resource-profile-custom)# memory 512
Device(config-app-resource-profile-custom)# vcpu 2
Device(config-app-resource-profile-custom)# end
```

例：アプリケーションのリソース設定の上書き



第 32 章

シリアルリレーサービス

この章は、次の項で構成されています。

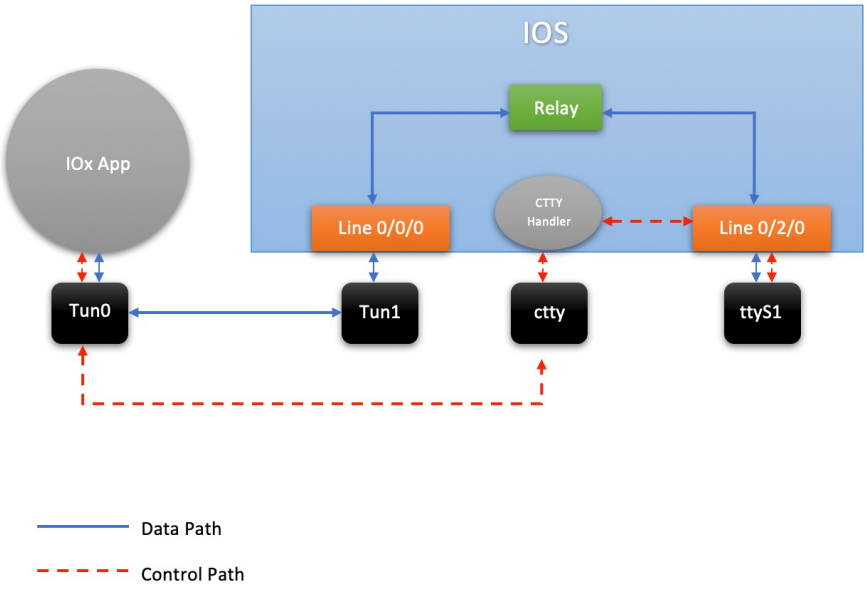
シリアルリレーサービス

IR1101 のシリアルリレーサービスは、IOx アプリケーションが非同期シリアルポート（IOS-XE では /dev/ttyS1）と通信できるようにします。シリアルリレーサービスの設定は、IR800 の設定と同様です。

データパス

IR1101 では、IOS-XE が非同期シリアルポートのデータパスと制御パスを完全に制御します。これは、PPP、raw ソケット、SCADA などの非同期ポートでサポートされている他のカプセル化にとっては不可欠です。IOx アプリケーションは、デバイスを完全に制御することはできません。すべてのデータと設定は、IOS-XE を介してデバイスに渡されます。実際のシリアルポートを IOx アプリケーションに公開する代わりに、シリアルリレーサービスは、/dev/ttyTun0 として列挙されるソフトウェアによってエミュレートされたシリアル tty デバイスを作成します（以下を参照）。デバイスのペア /dev/ttyTun0 と /dev/ttyTun1 はデータトンネルを表し、データ転送中にパススルーゲートウェイとして機能します。/dev/ ttyTun1 は IOS-XE によって開かれ、IOS からアプリケーションへのすべての入出力データはデータ転送中にこのデバイスを使用します。回線 0/0/0 は、/dev/ttyTun1 との通信に使用されます。シリアルリレーサービスは、2 本の回線間の接続を許可するように事前に設定しておく必要があります。

図 *106* : データパス



データパス：

1. IOx アプリケーションが /dev/ttyTun0 に文字を送信すると、トンネルドライバは自動的にデータを /dev/ttyTun1 にプッシュします。
2. IOS はデータを読み取り、シリアルリレーサービスに渡します。
3. シリアルリレーサービスは、リレーサービスのもう一方の端（この場合は回線 0/2/0）に関する情報を取得し、回線のバッファにデータを転送します。
4. ラインドライバは、バッファにデータがあると、実際のシリアルデバイス（/dev/ttyS1）にデータをアクティブにプッシュします。
5. リバースパスは、/dev/ttyS1 と /dev/tun0 の役割を入れ替えても同様に機能します。

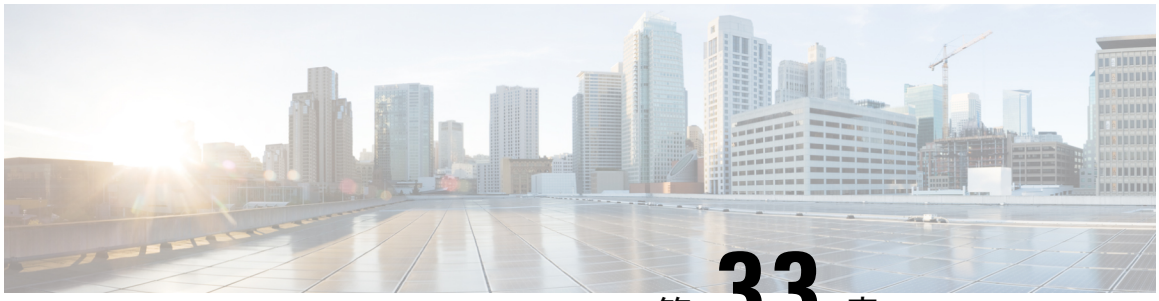
制御パス：

1. IOx アプリケーションが /dev/ttyTun0 で TCGETS ioctl コールを実行すると、トンネルドライバは /dev/cttyTun を使用して、IOS で実行されている CTTY ハンドラサービスに要求を送信します。
2. CTTY ハンドラサービスとカーネルドライバは、クライアント/サーバアーキテクチャを使用して設定オブジェクトと通信します。
3. TCGETS に関する要求を /dev/cttyTun から受信すると、CTTY ハンドラは要求を調べ、必要なデータを制御データ構造に入力するようにラインドライバに要求します。
4. 制御データ構造を受信すると、CTTY ハンドラは /dev/cttyTun に応答を送信し、最終的に /dev/ttyTun0 に戻ります。
5. /dev/ttyTun0 は要求どおりに IOx アプリケーションに制御データを渡します。

6. 同様のパスを TCSETS に当てはめると、CTTY ハンドラが下部の /dev/ttyS1 ドライバの設定を更新するようにラインドライバに要求します。
7. 回線 0/2/0 のラインドライバと /dev/ttyTun0 のドライバ設定は、常に相互に同期しています。ボーレートの変更などの設定変更は、設定のオーバーヘッドを増加させずにラインドライバに透過的に伝達されます。これは、仮想シリアルポートが実際のシリアルポートのパラメータを設定できる IR800 シリーズのシリアルリレーの伝達機能をエミュレートしています。

コンフィギュレーション コマンド

```
IR1101#configure terminal
IR1101(config)#interface async 0/2/0
IR1101(config-if)#encapsulation relay-line
IR1101(config-if)#exit
IR1101(config)#relay line 0/2/0 0/0/0
IR1101(config)#exit
IR1101#
```



第 33 章

Cisco SD-WAN のサポート

この章は、次の項で構成されています。

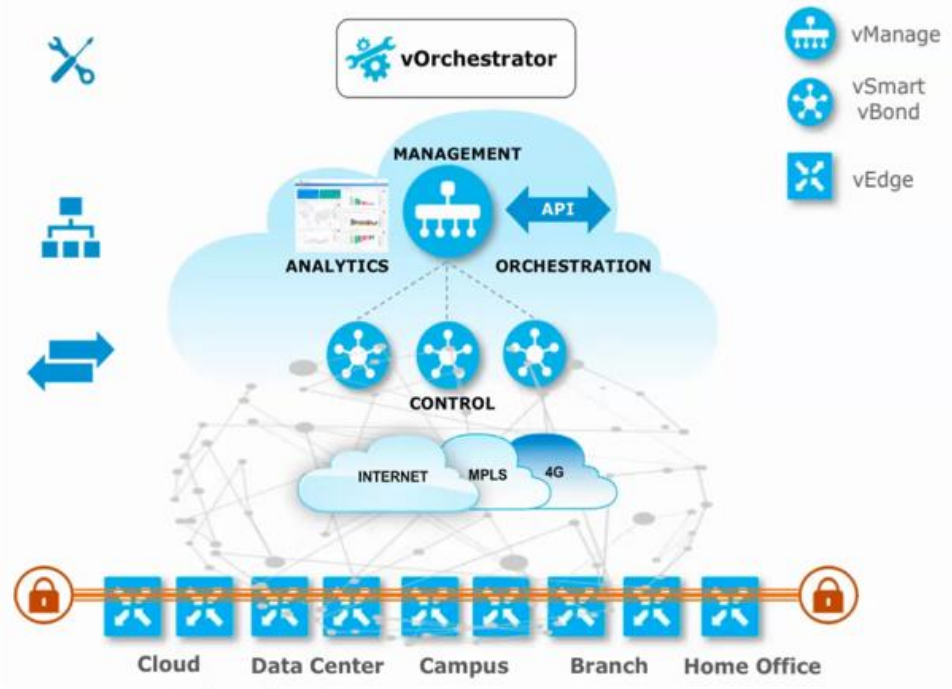
Cisco SD-WAN の概要

Cisco SD-WAN はクラウドファーストのアーキテクチャです。データプレーンとコントロールプレーンを分離して Cisco vManage コンソールから管理します。SD-WAN オーバーレイファブリックをすぐに構成でき、データセンター、ブランチ、キャンパス、コロケーション施設に接続してネットワーク速度、セキュリティ、効率性を改善できます。

Cisco SDWAN はクラウドベースのソリューションを採用しており、vOrchestrator、vManage、vSmart、vEdge で構成されています。

- vOrchestrator は、クラウド内のすべてのコントローラ VM を起動します。
- vManage は、SDWAN ソリューション全体の管理プレーンです。netconf/YANG を使用して vEdge デバイスと通信します。
- vSmart は、SDWAN ソリューション全体のコントロールプレーンです。vEdge デバイスと通信し、ルートリフレクタ、キーリフレクタ、およびポリシーエンジンとして機能します。
- vEdge は、SDWAN ソリューション全体のデータプレーンです。IR1101 プラットフォームは、SDWAN ネットワークの一部として vSmart、vManage と通信します。

次の図に、SDWAN のハイレベルアーキテクチャを示します。



Cisco SD-WAN はクラウドファースト アーキテクチャですが、一部のコンポーネントはオンプレミスで展開できます。SD-WAN の機能の詳細については、Cisco SD-WAN のランディング ページを参照してください。

IOS XE リリース 17.3.2 以降、IOS XE イメージは SD-WAN を実行するコントローラモードとして設定できます。Cisco IOS XE SD-WAN と Cisco IOS XE 機能の展開には、単一の universalk9 イメージが使用されます。この universalk9 イメージは、自律モード（Cisco IOS XE 機能の場合）とコントローラモード（Cisco SD-WAN 機能の場合）の 2 つをサポートしています。

Cisco IOS XE と Cisco IOS XE の SD-WAN 機能には、それぞれ自律モードとコントローラ実行モードでアクセスします。自律モードはルータのデフォルトモードで、Cisco IOS XE 機能が含まれています。Cisco IOS XE SD-WAN 機能にアクセスするには、コントローラモードに切り替えます。既存のプラグアンドプレイ ワークフローを使用してデバイスのモードを決定できます。

（注） PnP プロセスは、Gi0/0/0 またはセルラーで動作します。

詳細については、『Cisco SD-WAN Getting Started Guide』を参照してください。

関連資料

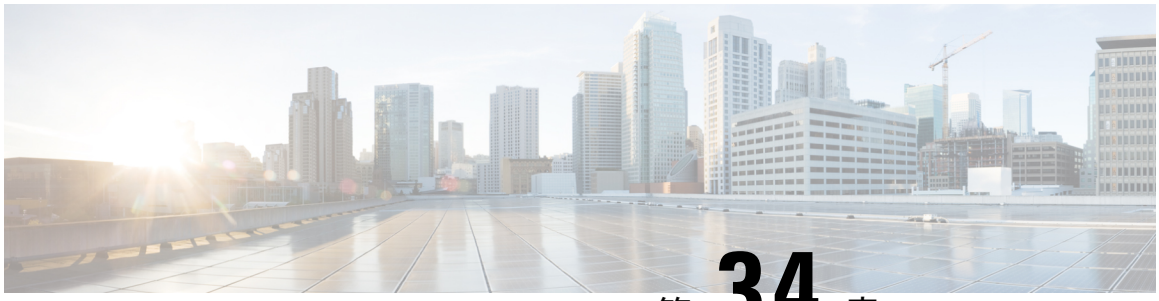
Cisco SDWAN のマニュアルは、次の場所から入手できます。

https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html

https://sdwan-docs.cisco.com/Product_Documentation/Software_Features

Cisco SD-WAN に関するすべての技術資料は、次の URL から入手できます。

https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html



第 34 章

ROM モニタ概要

この章は、次の項で構成されています。

ROM モニタ概要

ROM モニタは、ルータの電源を投入またはリロードしたときに、ハードウェアを初期化して Cisco IOS XE ソフトウェアをブートするブートストラップ プログラムです。ROM モニタ モードのルータに端末を接続すると、ROM モニタ（rommon 1>）の Command-Line Interface（CLI）プロンプトが表示されます。

通常の動作中は ROM モニタ モードを使用しません。ROM モニタ モードは、ソフトウェア セット全体の再インストール、ルータのパスワードのリセット、または起動時に使用するコンフィギュレーション ファイルの指定などの、特殊な場合だけ使用されます。

ROM モニタ ソフトウェアは多くの名前で呼ばれます。ROM モニタ モードの CLI プロンプトにちなんで *ROMMON* と呼ばれることもあります。また、ROM モニタ ソフトウェアはブート ソフトウェア、ブート イメージ、ブート ヘルパーと呼ばれることもあります。Cisco IOS XE ソフトウェアを使用するルータで配布されますが、ROM モニタは、Cisco IOS XE ソフトウェアとは別のプログラムです。通常の起動中に、ROM モニタによってルータを初期化し、Cisco IOS XE ソフトウェアに制御が渡ります。Cisco IOS XE ソフトウェアが引き継いだ後、ROM モニタはもう使用中でありません。

環境変数およびコンフィギュレーション レジスタ

2 つのプライマリ接続が ROM モニタと Cisco IOS XE ソフトウェアの間にあります。これは ROM モニタ環境変数およびコンフィギュレーション レジスタです。

ROM モニタ環境変数は、Cisco IOS XE ソフトウェアの場所を定義し、それをロードする方法について説明します。ROM モニタがルータを初期化したら、Cisco IOS XE ソフトウェアを検出し、ロードするために環境変数を使用します。

コンフィギュレーション レジスタは、ルータの起動方法を制御するソフトウェア設定です。コンフィギュレーション レジスタの主な用途の 1 つは、ルータを ROM モニタ モードで開始するか、それとも管理EXECモードで開始するかを制御することです。必要に応じて、コンフィギュレーション レジスタは ROM モニタ モードまたは管理 EXEC モードに設定されます。通常、ROM モニタ モードを使用する必要がある場合、Cisco IOS XE ソフトウェア プロンプトを使用してコンフィギュレーション レジスタを設定します。ROM モニタ モードのメンテナンスが完了したら、Cisco IOS XE ソフトウェアでルータがリブートするように、コンフィギュレーション レジスタを変更します。

端末接続での ROM モニタ モードへのアクセス

ルータが ROM モニタ モードになっている場合、カードのコンソール ポートに直接接続された端末からだけ ROM モニタ ソフトウェアにアクセスできます。Cisco IOS XE ソフトウェア（EXECモード）が動作していないため、nonmanagementインターフェイスを利用できません。基本的には、すべての Cisco IOS XE ソフトウェア リソースが利用不可です。ハードウェアが存在しますが、ハードウェアを使用できるようにするコンフィギュレーションはありません。

ネットワーク管理アクセスおよび ROM モニタ モード

ROM モニタ モードは、Cisco IOS XE ソフトウェア内のモードではなく、ルータ モードであることを認識しておくことが重要です。ROM モニタ ソフトウェアおよび Cisco IOS XE ソフトウェアは同じルータで動作する2つの別個のプログラムであることを覚えておくことを推奨します。ルータは、いつでも、これらのプログラムのうちの 1 つのみを実行します。

ROM モニタおよび Cisco IOS XE ソフトウェアを使用する場合に混乱を招く可能性のある 1 つの領域は、管理イーサネットインターフェイスのIP設定を定義する領域です。ほとんどのユーザは、CiscoIOS XE ソフトウェアでの管理イーサネットインターフェイスの設定に慣れています。ルータが ROM モニタモードになっていると、しかしながら、ルータは Cisco IOS XE ソフトウェアを実行していないため、管理イーサネット インターフェイスの設定を使用できません。

ルータで ROM モニタ モードになっているときに TFTP サーバなどの他のデバイスにアクセスするには、IP アクセス情報を使って ROM モニタ変数を設定する必要があります。

（注） TFTP アクセス変数は、IR1101 プラットフォームでは現在サポートされていません。

ROM モニタ モードの利用

ここでは、ROMMONモードに入る方法について説明します。次のセクションが含まれています。

現在の ROMMON バージョンの確認

ルータで実行中の ROMmon のバージョンを表示するには、**show rom-monitor** コマンドを使用します。ROMmon で設定されているすべての変数を表示するには、show romvar を使用します。

```
Router#show rom-monitor r0
System Bootstrap, Version 1.2, RELEASE SOFTWARE
Copyright (c) 1994-2018  by cisco Systems, Inc.

Router# show romvar
ROMMON variables:
 PS1 = rommon ! >
 MCP_STARTUP_TRACEFLAGS = 00000000:00000000
 LICENSE_SUITE =
 RET_2_RTS =
 Diagnostic = 1
 THRPUT =
 USER_BOOT_PARAM =  DEBUG_CONF=/bootflash/debug.conf
 EULA_ACCEPTED = TRUE
 BOOT_WDOG = DISABLE
 LICENSE_BOOT_LEVEL =
 BOOT = bootflash:ir1101_crashkernel.bin,1;
 CRASHINFO = bootflash:crashinfo_RP_00_00_20180619-204307-UTC
 RET_2_RCALTS =
 BSI = 0
 RANDOM_NUM = 1662155698

Router# reload
```

コンフィギュレーション レジスタが hex value 0x0 または 0x1820 に設定されている場合、リロード操作すると ROMmon モード コマンド プロンプト（rommon 1 >）が表示されます。プロンプトで set コマンドを呼び出すと（rommon 1 > set）、IOS/XE exec モードで上記の「show romvar」と同じ情報が表示されます。

```
rommon 1 > set
PS1=rommon ! >
MCP_STARTUP_TRACEFLAGS = 00000000:00000000
 LICENSE_SUITE =
 RET_2_RTS =
 Diagnostic = 1
 THRPUT =
 USER_BOOT_PARAM =  DEBUG_CONF=/bootflash/debug.conf
 EULA_ACCEPTED = TRUE
 BOOT_WDOG = DISABLE
 LICENSE_BOOT_LEVEL =
 BOOT = bootflash:ir1101_crashkernel.bin,1;
 CRASHINFO = bootflash:crashinfo_RP_00_00_20180619-204307-UTC
 RET_2_RCALTS =
 BSI = 0
 RANDOM_NUM = 1662155698
```

一般的な ROM モニタ コマンド

次の表は、ROM モニタ モードで一般的に使用されるコマンドの要約を示します。これらのコマンドの使用に関する詳細については、このマニュアルの該当する手順を参照してください。

表 *20 :* 一般的な *ROM* モニタ コマンド

ROMMON コマンド	説明
boot image	手動で仮想 Cisco IOS XE ソフトウェア イメージをブートします。
boot image –o config-file-path	手動で一時的な代替管理コンフィギュレーション ファイルにより Cisco IOS XE ソフトウェアをブートします。
confreg	config-register 設定を変更します。
dev	使用可能なローカル ストレージ デバイスを表示します。
dir	ストレージ デバイス内のファイルを表示します。
reset	ノードをリセットします。
set	現在設定されている ROM モニタ環境設定を表示します。
sync	新しい ROM モニタ環境設定を保存します。
unset	環境変数の設定を削除します。

例

次の例は、ルータで **?** コマンドを入力すると表示される結果を示しています。

```
rommon 1 > ?
alias               set and display aliases command
boot                boot up an external process
confreg             configuration register utility
dev                 list the device table
dir                 list files in file system
help                monitor builtin command help
history             monitor command history
meminfo             main memory information
repeat              repeat a monitor command
reset               system reset
set                 display the monitor variables
showmon             display currently selected ROM monitor
sync                write monitor environment to NVRAM
token               display board's unique token identifier
unalias             unset an alias
unset               unset a monitor variable
```

ROM モニタ プロンプトの変更

次の例に示すように **PS1=** コマンドを使用して、ROM モニタ モードのプロンプトを変更できます。

```
rommon 8 > PS1="IR1101 rommon ! > "
IR1101 rommon 9 >
```

プロンプトを変更すると、ROM モニタの複数のルータを同時に処理する場合に役立ちます。この例は、プロンプトが「IR1101 rommo」で、次に行番号、さらに「>」が続くことを示しています。

コンフィギュレーション レジスタ設定の表示

現在のコンフィギュレーション レジスタ設定を表示するには、次のようにパラメータを使用せずに **confreg** コマンドを入力します。

```
rommon > confreg
   Configuration Summary
   (Virtual Configuration Register: )
enabled are:
[ 0 ] break/abort has effect
[ 1 ] console baud: 9600
 boot:...... the ROM Monitor
do you wish to change the configuration? y/n  [n]:
```

コンフィギュレーション レジスタ設定には、仮想コンフィギュレーション レジスタのラベルが付いています。コンフィギュレーション レジスタ設定の変更を回避するには、**no** コマンドを入力します。

環境変数の設定

ROM モニタ 環境変数は、ROM モニタの属性を定義します。環境変数は、コマンドのように入力し、常にその後に等号（=）が続きます。環境変数の設定は大文字で入力し、その後に定義を続けます。次に例を示します。

```
IP_ADDRESS=10.0.0.2
```

正常な動作状態では、これらの変数を変更する必要はありません。ROM モニタの動作方法を変更する必要がある場合だけ、クリアまたは設定します。

この項では、次のトピックについて取り上げます。

頻繁に使用される環境変数

次の表は、主要な ROM モニタ環境変数を示します。これらの変数を使用する方法については、このマニュアルの関連する手順を参照してください。IR1101 ブート ローダはネットブートをサポートしていないため、環境変数の IP_ADDRESS、IP_SUBNET_MASK、DEFAULT_GATEWAY、TFTP_SERVER、TFTP_FILE などの設定は使用されません。

表 *21 :* 頻繁に使用される *ROM* モニタ環境変数

環境変数	説明
BOOT=path/file	ノードのブート ソフトウェアを識別します。この変数は通常、ルータのブート時に自動的に設定されます。

環境変数の設定の表示

現在の環境変数の設定を表示するには、**set** コマンドを入力します。

```
rommon 1 > showmon
System Bootstrap, Version 1.3(REL), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

IR1101-K9 platform with 4188160 Kbytes of main memory

MCU Version - Bootloader: 4, App: 4
MCU is in application mode.
```

環境変数の設定の入力

環境変数の設定は大文字で入力し、その後に定義を続けます。次に、ROMmon モードで設定できる環境変数の例を示します。

```
rommon 1 > confreg 0x0
rommon 1> BOOT_WDOG = DISABLE
rommon 1> BOOT = IR1101-K9_image_name
```

環境変数の設定の保存

現在の環境変数の設定を保存するには、**sync** コマンドを入力します。

```
rommon > sync
```

（注） **sync** コマンドを使用して保存されていない環境値は、システムがリセットされる、またはブートされるたびに廃棄されます。

ROM モニタ モードの終了

ROM モニタ モードを終了するには、コンフィギュレーション レジスタを変更し、ルータをリセットする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**confreg** 例： `rommon 1> confreg`	コンフィギュレーション レジスタのコンフィギュレーション プロンプトが開始します。
ステップ 2	指示されたとおりにプロンプトに応答します。	詳しくは、この手順の後の例を参照してください。
ステップ 3	**reset** 例： `rommon 2> reset`	ルータをリセットして初期化します。

設定例

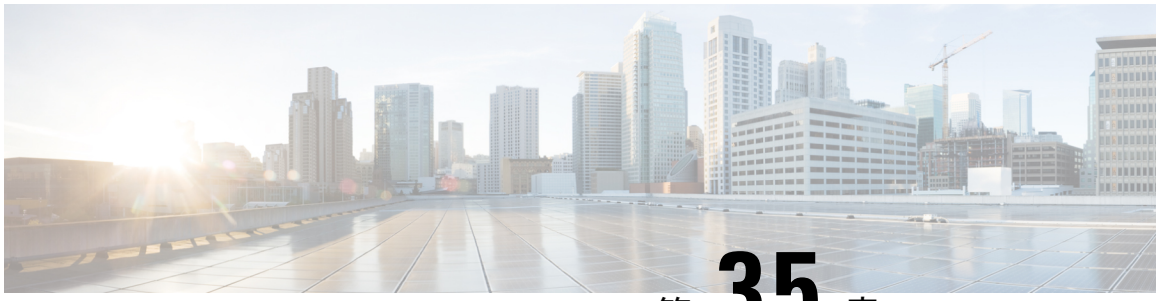
```
rommon 3 > confreg
           Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
 boot: ...... the ROM Monitor
do you wish to change the configuration? y/n  [n]:  y
 enable  "diagnostic mode"? y/n  [n]:
 enable  "use net in IP bcast address"? y/n  [n]:
 enable  "load rom after netboot fails"? y/n  [n]:
 enable  "use all zero broadcast"? y/n  [n]:
 disable "break/abort has effect"? y/n  [n]:
 enable  "ignore system config info"? y/n  [n]:
 change console baud rate? y/n  [n]:
change the boot characteristics? y/n  [n]:
           Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
 boot: ...... the ROM Monitor
do you wish to change the configuration? y/n  [n]:
```

ルータ用 ROMmon のアップグレード

IR1101-K9 ルータの ROMmon アップグレードは、イメージが起動すると自動的に実行されます。ROMmon の最新バージョンは、IOSXE イメージにバンドルされています。アルゴリズムは、現在の実行中のバージョンがバンドルされているバージョンよりも古いかどうかを検出します。古い場合は、自動的にアップグレードされます。現在実行中のバージョンがバンドルされているバージョンと同じ場合、アップグレードは実行されません。正常にアップグレードされると、ルータは自動的に再起動して新しいバージョンをロードして実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意）ハードウェア上の ROMmon の現在のリリース番号を表示するには、ルータで **show rom-monitor** *slot* コマンドを実行します。実行するコマンドの出力の解釈については、現在の ROMMON バージョンの確認 （387 ページ）を参照してください。	
ステップ 2	**config-register 0x2102** コマンドを使用しても自動ブートが有効にならない場合、ROMmon プロンプトで **boot** *filesystem:/file-location* コマンドを実行して Cisco IOS XE イメージをブートします。*filesystem:/file-location* は、統合パッケージ ファイルへのパスです。ROMmon のアップグレードは、Cisco IOS XE イメージが起動されるまで、いずれのハードウェアにとっても永続的なものではありません。	
ステップ 3	起動が完了したら、ユーザ プロンプトに **enable** コマンドを実行して特権 EXEC モードを開始します。	
ステップ 4	ROMmon がアップグレードされたかどうかを確認するには、**show rom-monitor** *slot* コマンドを実行します。	



第 35 章

WAN モニタリング

この章は、次の項で構成されています。

WANMon について

WANMon は、次の製品とインターフェイスの WAN リンクのリカバリ要件に対応する柔軟なソリューションです。

- 物理ネットワーク：4G LTE とイーサネット（WAN ポート）
- 仮想リンク：非暗号マップベースの IPSec トンネル（レガシーまたは FlexVPN）。つまり、インターフェイスとして設定する任意の IPSec トンネルです。

WANMon を有効にして、WAN リンクをモニタし、リンク障害トリガーの受信時にリンクリカバリアクションを開始します。

組み込みの復旧動作

次に、リンクタイプに固有の組み込みリカバリプロセスの 3 つのレベルを示します。

リンクタイプ	リカバリ アクション		
	レベル 0（即時）	レベル1（アクティブ）	レベル 2（最終手段）
4G LTE	インターフェイスをクリアしてから shut/no-shut	モジュールのリロード	システム リロード

リンクタイプ	リカバリ アクション		
	レベル 0（即時）	**レベル1（アクティブ）**	**レベル 2（最終手段）**
イーサネット	インターフェイスをクリアしてから shut/no-shut	アクションなし	システム リロード
トンネル	Shut/no-shut	アクションなし	システム リロード

各レベルには、実行される組み込みリカバリアクションに基づく 2 つの時間ベースのしきい値があります。次に、各レベルのデフォルト設定を示します。

- *threshold* は、リンク障害トリガーを受信してから、指定されたレベルで設定されたリカバリアクションを開始するまでの待機時間です（分単位）。
- *mintime* は、リンクがダウンしたままの場合にリカバリアクションを実行する頻度です。

次に、組み込み値を示します。

レベル	threshold	mintime	説明
レベル 0	10 分	10 分	リンクがダウンしてから 10 分後にレベル 0 のアクションをトリガーします。10 分以下の間隔で繰り返します。
レベル 1	60 分	60 分	リンクがダウンしてから 10 分後にレベル 1 のアクションをトリガーします。60 分以下の間隔で繰り返します。
レベル 2	480 分	60 分	リンクがダウンした 480 分後にレベル 2 のアクションをトリガーします。60 分以下の間隔で繰り返します。

（注） しきい値を 0 に指定すると、そのレベルのリカバリアクションは実行されません。これを使用すると、他の WAN リンクが動作している可能性がある中でリンク障害トリガーを受信したときに、システムのリロード（組み込みのレベル 2 のリカバリアクション）を回避できます。

前提条件

WANMon モジュールが使用可能であることを確認します。WANMon モジュールは、*tm_w3316anmon.tcl* ポリシーファイルとして IOS-XE イメージに含まれています。

注意事項と制約事項

- WANMon は、セルラーインターフェイスに必要な IP アドレスチェック（ユーザ設定なし）を自動的に実行します。

- 他のすべてのインターフェイスでは、WANMon は IP アドレスチェックを実行しません。
- WANMon は、リンクリセッタアプレットがモニタするアプリケーションイベントを生成することによって、ユーザ指定のアクションを間接的にトリガーします。
- 本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

WANMon の設定

ルータで WANMon を有効にして特定のインターフェイスに WAMMon サポートを割り当てることができます。必要に応じて、組み込みリカバリアクションのオーバーライド、カスタムリカバリリンクの定義、およびトラックオブジェクト値を設定して IP アドレスチェックを無効にするためのイベントマネージャの環境ポリシーの定義を実行できます。デフォルトでは、WANMon は無効になっています。

手順

	コマンドまたはアクション	目的
ステップ 1	**event manager policy** *tm_wanmon.tcl* **authorization bypass**	WANMon リンクのリカバリモジュールを有効にします。 このポリシーによって呼び出される CLI の許可を回避するには、**authorization bypass** を使用します。
ステップ 2	**event manager environment wanmon_if_list** <*instance*> {*interface name* { **ipsla** <*instance*>}}	WAN のインターフェイスに WANMon を設定し、これがインターフェイス コンフィギュレーション コマンドであることを示します。 （注） プレフィックス wanmon_if_list を持つ環境変数でインターフェイス設定を構成します。 インスタンスを指定することで、複数のインターフェイスを使用できます。 必ず、完全なインターフェイス名（cellular0/1/0 または cellular0/3/0）を指定します。 必要に応じて、IP SLA icmp-echo トリガーを設定できます。インスタンスを指定することで、複数の IP SLA トリガー を使用できます。 （注） WANMon は SLA ID のステータスのみを確認します。*icmp-echo* が最も一般的ですが、必要に応じて、他のタイプの SLA プローブ（*udp-echo* など）も代わりに使用できます。

	コマンドまたはアクション	目的
ステップ 3	**event manager environment wanmon_if_listx** {*interface name* { **recovery** *Level0* {*Level1* } *Level2*}}	（任意）組み込みしきい値をオーバーライドします。
ステップ 4	**publish-event sub-system 798 type 2000 arg1** <*interface name*> **arg2** <*level* >	（任意）リンクリセットアプレットを使用してカスタムリカバリアクションを設定します。 <*interface* > は完全なインターフェイス名です（cellular0/1/0 や cellular0/3/0 など）。 <*level* > は、目的のリンクリカバリアクションに一致するように、0、1、または 2 になります。
ステップ 5	**{stub** <*track-stub-id* > **}**	（任意）イベントマネージャの環境ポリシーを使用してトラックオブジェクト値を設定できます。WANMon は、外部アプレットがスタブオブジェクトを追跡できるように、リンク状態を反映するための track-stub-object 値を設定できます。
ステップ 6	**event manager environment wanmon_if_listx** {<*interface name* > { **checkip** <*instance* >}}	（任意）IP アドレスチェックを無効にします。

次のタスク

例

```
event manager policy tm_wanmon.tcl authorization bypass
```

次に、セルラーおよびイーサネットのインターフェイスを設定するイベントマネージャコマンドの例を示します。

```
event manager environment wanmon_if_list1 {cellular0/1/0 {ipsla 1}}
event manager environment wanmon_if_list2 {GigabitEthernet0/0/0 {ipsla 2}}
```

この例では、カスタムリカバリのしきい値を設定します。

```
event manager environment wanmon_if_list {cellular0/1/0 {recovery 20 {90 75} 600}
```

引数の説明

- レベル 0 のしきい値は、リンク障害トリガーの 20 分後に設定されます。レベル 0 のリカバリアクションは、セルラーインターフェイスに対して実行されます。10 分以下の間隔（デフォルト）で無期限に繰り返します。
- レベル 1 のしきい値は 90 分に設定されます。レベル 1 のリカバリアクションは、セルラーインターフェイスに対して実行されます。75 分以下の間隔で繰り返します。
- レベル 2 のしきい値は 600 分（10 時間）に設定されます。

次は、track-stub-object 値を 21 に設定します。

```
conf t
track 21 stub-object
event manager environment wanmon_if_list {cellular0/1/0 {ipsla 1} {stub 21}
```

WANMon 設定の確認

WANMon 設定を確認するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**show event manager policy registered**	WAN モニタリングポリシーを表示します。
ステップ 2	**show event manager environment**	インターフェイスの設定時に設定されたインターフェイス環境変数を表示します。

次のタスク

例

```
show event manager policy registered
1    script    system  multiple   Off   Thu Jan 16 18:44:29 2014  tm_wanmon.tcl
show event manager environment
1 wanmon_if_list   {cell0/1/0 {ipsla 1}}
```

設定例

ここでは、次の例を示します。

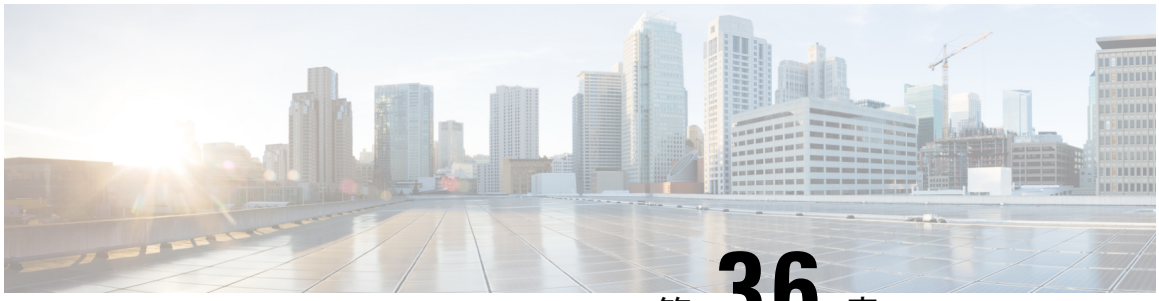
WANMon セルラーインターフェイスの設定例

```
track 1 ip sla 1
ip sla 1
 icmp-echo 172.27.166.250
 timeout 6000
 frequency 300
ip sla schedule 1 life forever start-time now
event manager environment wanmon_if_list {cellular0/1/0 {ipsla 1}}
event manager policy tm_wanmon.tcl authorization bypass
```

複数 WAN リンクのモニタリング例

```
track 1 ip sla 1
```

```
track 21 stub-object
ip sla 1
 icmp-echo 172.27.166.250
 timeout 6000
 frequency 300
ip sla schedule 1 life forever start-time now
track 2 ip sla 2
track 22 stub-object
ip sla 2
 icmp-echo 10.27.16.25
 timeout 6000
 frequency 300
ip sla schedule 2 life forever start-time now
event manager environment wanmon_if_list1 {cellular0/1/0 {ipsla 1} {stub 21}}
event manager policy tm_wanmon.tcl authorization bypass
```



第 36 章

デジタル加入者線（DSL）の設定

この章は、次の項で構成されています。

概要

ルータは Small Form-Factor Pluggable（SFP）ネットワーク インターフェイス モジュールを使用して DSL 機能を追加します。DSL ソリューションは、次の Annex をサポートしています。

ADSL2（A）、ADSL2 +（A、J、J は 17.5.1 リリースでのみサポート）。VDSL2 は Annex A、B をサポートしています。すべて TR100、TR105、TR114、TR115 に準拠しています。

IOS-XE リリース 17.5.1 では、コントローラインターフェイスで Annex-J 設定のサポートが追加されています。

（注） ADSL2+ J はサポートされていますが、ADSL2 J は 17.5.1 ではまだサポートされていません。

Annex-J を有効にするには、次の手順を実行します。

```
router#config term
router(conf)#controller vdsl 0/0/0
router(conf-if)#capability annex-j
router#(conf-if)#exit
router#
```

Annex-J を削除するには、次の手順を実行します。

```
router#config term
router(conf)#controller vdsl 0/0/0
router(conf-if)#no capability annex-j
router#(conf-if)#exit
router#
```

17.5.1 では、新しいコマンド **rx-padding** が追加されています。このコマンドは、MTU が 64 バイト未満のパケットに使用されます。

（注） サービスプロバイダからのダウンストリームで64mtu未満のフレームが想定される場合、VLAN設定は vlan 96 である必要があります。サービスプロバイダからのダウンストリームで 64mtu 未満のフレームが想定される場合、単一の PVC（つまり、Vlan96）でサポートされるのは単一の VLAN だけです。今後のリリースでは、VLAN サポートの範囲を Vlan44 ー 1024、single-vlanin single-pvc に拡張する予定です。

コマンドの例は次のとおりです。

```
router#config term
router#controller vdsl 0/0/0
router(conf-if)#rx-padding
router(conf-if)#end
router#write mem
```

機能に関する警告

この項では、サポートされている機能とサポートされていない機能のリストを示します。

- DSL SFP は IR1101 ベースユニットに挿入されている場合にのみ動作します。IRM-1100 拡張ユニットではサポートされていません。IR1101 は GI0/0/0 で 1 つの DSL SFP のみをサポートできます。
- VDSL2 はプロファイル 8a ー 17a のみをサポートし、30a はサポートしていません。
- SFP は現在、Yang をサポートしていません。これは将来のリリースで提供される予定です。
- DSL ユーザの認証および設定時に、RADIUS と AAA をサポートします。
- DSL インターフェイスには DSL サービスに依存する最小限の設定が必要であるため、DSL インターフェイスでは Plug and Play（PnP）機能を使用できません。
- ゼロタッチ展開（ZTD）は、IIoT Field Network Director を介してのみサポートされます。FND では、cgna wsma ベースの ZTD のみを使用します。DSL インターフェイスでは PnP ベースの ZTD はサポートされていません。ZTD では、サービスプロバイダーの要件に応じて、基本的な最小設定とパラメータを使用してステージングします。

DSL をサポートするには、IR1101 が IOS-XE 17.4.1 以降で動作している必要があります。

- show controller vdsl 0/0/0 コマンドは、c111x プラットフォームと同様に、すべての DSL（VDSL2/ADSL2/ADSL2+）コントローラ情報を表示するために使用されます。controller コマンドは VDSL ですが、これは実際には DSL を意味し、ADSL と VDSL に使用されます。
- ADSL2/2+ 設定では、c111x プラットフォームのように ATM インターフェイスはありません。すべての設定は DSL SFP WAN g0/0/0 インターフェイス、そのサブインターフェイスオプション、およびコントローラ vdsl0/0/0 上にあります。ATM パケットは DSL SFP によって処理され、イーサネットパケットとして再構成されます。Annex A、L がサポートされています。
- WebUI を使用して、interface g0/0/0 を通常どおり設定/モニタできます。リリース 17.4.1 の Controller vdsl 0/0/0 のモニタ/設定オプションに固有のオプションはありません。
- VDSL2 および ADSL2+ の各種 MIB は、17.5.1 以降のリリースでのみトリクルをサポートします。MIB の情報については、このセクションで後述します。
- ADSL2/2+ ATM の設定において、シナリオでサービスプロバイダからのダウンストリームが 64 バイト MTU 未満であると想定している場合は、次のステップを確認してください。
  1. rx-padding cli が有効になっている。
  2. Vlan96 の値がインターフェイス コンフィギュレーションで使用される。
  3. この特定のシナリオで、単一 PVC でのマルチ VLAN サポートがない。

DSL 機能の仕様

表 *22 : DSL* 機能の仕様

マルチモード DSL（VDSL2 と ADSL2/2+）	• DSL SFP を介して提供 • SFP は 1 つの RJ-45 インターフェイスを搭載 • 両端回線テスト（DELT）診断モードをサポート（VDSL2 のみ）

表 *23 : VDSL2* 機能の仕様

VDSL2	• VDSL2 993.2 Annex A と Annex B • 997 および 998 のバンドプラン • G.994.1 ITU G.hs • VDSL2 のプロファイル：8a、8b、8c、8d、12a、12b、および 17a • ベクタリング • U0 帯域対応（25 ～ 276 kHz） • IEEE 802.3ah 64/65 オクテットカプセル化のみに基づくイーサネットパケット転送モード（PTM） • Dying Gasp

表 *24 : ADSL2/2+* 機能の仕様

ADSL2/2+	• ADSL2 の Annex A と L • ADSL2+ の Annex A • ADSL2+ の Annex J（17.5.1 で使用可能） • G.994.1 ITU G.hs • 電話局からの距離が 16,000 フィートを超えるループ長でのパフォーマンスを強化するために範囲拡張 ADSL2（G.922.3）Annex L を採用 • T1.413 ANSI ADSL2/2+ DMT Issue 2 に準拠 • DSL Forum TR-067 と TR-100 に準拠 • インパルスノイズ保護（INP）と拡張 INP • ダウンストリーム電源バックオフ（DPBO） • Dying Gasp

Dying Gasp は、ルータがコンデンサの残存電力の一部を使用して DSLAM に機能停止メッセージを送信する機能です。**show controller vdsl 0/0/0 local** コマンドを使用して、ルータが Dying Gasp メッセージを送信する準備ができていることを確認できます。

```
Router#show controllers vdsl 0/0/0 local
SFP Vendor PID: SFPV5311TR
SFP Vendor SN: V021932028C
Firmware embedded in IOS-XE: 1_62_8463
Running Firmware Version: 1_62_8455
Management Link: up
DSL Status: showtime
Dumping internal info: idle
Dying Gasp: armed
Dumping DELT info:  idle
```

（注） Dying Gasp が無効になっている場合、出力には **Dying gasp: disarmed** と表示されます。

Dying Gasp の設定はありません。実装に対しソフトウェアによって内部的に処理されます。SFP shut/no shut がトリガーされると、1 ー 2 の通知が 50 ns 以内に送信されます。

DSL SFP の取り付け

DSL SFP の挿入手順については、 製品のハードウェア設置ガイドを参照してください。

警告 取り付け作業者がこれらの指示を理解すること、およびSFPの挿入および取り外しの正しい方法に精通していることが重要です。そうでない場合は、SFP に損傷を与える可能性があります。

DSL SFP をサポートするための IOS-XE の最小リリースは、IR1101 では 17.4.1 です。

基本設定

SFP を取り付けたら、起動するための基本設定が必要です。手順は次のとおりです。

```
configure t
Router(conf)#interface g0/0/0
Router(conf-if)#media-type sfp
Router(conf-if)#no shut
Router(conf-if)#exit
```

この時点で、SFP 挿入の syslog メッセージが表示されます。

SFP の確認

SFP を安全に取り付けたら、**show inventory** コマンドでそのステータスを確認できます。

```
Router#show inventory

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

NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9 , VID: V03 , SN: FCW23500H5X

NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9 , VID: V03 , SN: FOC23473SRK

NAME: "module subslot 0/0", DESCR: "IR1101-ES-5"
PID: IR1101-ES-5 , VID: V01 , SN:

NAME: "subslot 0/0 transceiver 0", DESCR: "GE T"
PID: SFP-VADSL2+-I , VID: V01 , SN: MET2023000A
Ignore the description, it will always reflect GE T for all IR1101 SFPs
PID and S/N are what matter
```

次に示す出力では、説明とビットレートは無視してください。PID/シリアル番号情報はSFPの情報です。

```
Router#show interfaces transceiver detail
IDPROM for transceiver Gigabitethernet0/0/0:
Description = SFP or SFP+ optics (type 3)
Transceiver Type: = GE T (26)
Product Identifier (PID) = SFP-VADSL2+-I
Vendor Revision = V5.1
Serial Number (SN) = MET2023000A
Vendor Name = CISCO-METANOIA
Vendor OUI (IEEE company ID) = 00.00.00 (0)
CLEI code =
Cisco part number = 74-124941
Device State = Enabled.
Date code (yy/mm/dd) = 20/23/
Connector type = .
Encoding = 8B10B (1)
Nominal bitrate = GE (1300 Mbits/s)
Minimum bit rate as % of nominal bit rate = not specified
Maximum bit rate as % of nominal bit rate = not specified

Socket Verification


SFP IDPROM Page 0xA0:
000: 03 04 22 08 00 00 00 00 00 00
010: 00 01 0D 00 00 00 00 00 FF 00
020: 43 49 53 43 4F 2D 4D 45 54 41
030: 4E 4F 49 41 20 20 00 00 00 00
040: 53 46 50 56 35 33 31 31 54 52
050: 35 31 43 53 20 20 56 35 2E 31
060: 00 00 00 00 3F 08 00 00 00 4D 45
070: 54 32 30 32 33 30 30 30 41 20
080: 20 20 20 20 32 30 32 33 20 20
090: 20 20 00 00 00 6D 63 00 30 60
100: FE 53 E4 C1 54 F1 F1 C1 FA 1A
110: 98 EC 6B E0 7F 00 00 00 00 00
120: 00 00 00 00 8C D0 5C F7 00 00
130: 00 00 00 00 00 00 00 00 37 34
140: 2D 31 32 34 39 34 31 20 56 30
150: 31 20 CF EC 55 00 00 00 00 D4
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: 00 00 53 46 50 2D 56 41 44 53
200: 4C 32 2B 2D 49 20 20 20 20 20
210: 20 20 00 00 17 00 00 00 00 00
220: 00 00 00 5A

SFP IDPROM Page 0xA2:
000: 00 00 00 00 00 00 00 00 00 00
010: 00 00 00 00 00 00 00 00 00 00
020: 00 00 00 00 00 00 00 00 00 00
030: 00 00 00 00 00 00 00 00 00 00
040: 00 00 00 00 00 00 00 00 00 00
050: 00 00 00 00 00 00 00 00 00 00
060: 00 00 00 00 00 00 00 00 00 00
070: 00 00 00 00 00 00 00 00 00 00
080: 00 00 00 00 00 00 00 00 00 00
090: 00 00 00 00 00 00 00 00 00 00
100: 00 00 00 00 00 00 00 00 00 00
110: 00 00 00 00 00 00 00 00 00 00
120: 00 00 00 00 00 00 00 00 00 00
```

```
130: 00 00 00 00 00 00 00 00 00 00
140: 00 00 00 00 00 00 00 00 00 00
150: 00 00 00 00 00 00 00 00 00 00
160: 00 00 00 00 00 00 00 00 00 00
170: 00 00 00 00 00 00 00 00 00 00
180: 00 00 00 00 00 00 00 00 00 00
190: 00 00 00 00 00 00 00 00 00 00
200: 00 00 00 00 00 00 00 00 00 00
210: 00 00 00 00 00 00 00 00 00 00
220: 00 00 00 00 00 00 00 00 00 00
230: 00 00 00 00 00 00 00 00 00 00
240: 00 00 00 00 00 00 00 00 00 00
250: 00 00 00 00 00 00
Link reach for 9u fiber (km) = SX(550/270m) (0)
1xFC-MM(500/300m) (0)
2xFC-MM(300/150m) (0)
ESCON-MM(2km) (0)
Link reach for 9u fiber (m) = SX(550/270m) (0)
1xFC-MM(500/300m) (0)
2xFC-MM(300/150m) (0)
ESCON-MM(2km) (0)
Link reach for 50u fiber (m) = SR(2km) (0)
IR-1(15km) (0)
IR-2(40km) (0)
LR-1(40km) (0)
LR-2(80km) (0)
LR-3(80km) (0)
DX(40KM) (0)
HX(40km) (0)
ZX(80km) (0)
VX(100km) (0)
1xFC, 2xFC-SM(10km) (0)
ESCON-SM(20km) (0)
Link reach for 62.5u fiber (m) = SR(2km) (0)
IR-1(15km) (0)
IR-2(40km) (0)
LR-1(40km) (0)
LR-2(80km) (0)
LR-3(80km) (0)
DX(40KM) (0)
HX(40km) (0)
ZX(80km) (0)
VX(100km) (0)
1xFC, 2xFC-SM(10km) (0)
ESCON-SM(20km) (0)
Nominal laser wavelength = 0 nm.
DWDM wavelength fraction = 0.0 nm.

No transceiver present
```

SFP 上の LED 表示

DSL SFP には 2 つの LED インジケータが組み込まれています。この LED は、ルータのパネルにある LED とは無関係に動作します。

（注） **show platform led** は SFP LED を対象としていません。DSL リンクステータスには、**show controller vdsl 0/0/0 local** コマンドを使用します。

LED 表示

次の表で SFP LED の表示について説明します。

インジケータ LED	LED カラー	状態	説明
LED 1	橙色	点灯	CPE 側（IR ルータで使用する場合はオンになることを予期）
LED 1	橙色	消灯	セントラルオフィス側（サポート対象外）
xDSL ステータス LED	緑	低速の点滅	アイドル
xDSL ステータス LED	緑	高速の点滅	トレーニング
xDSL ステータス LED	緑	点灯	稼働中
xDSL ステータス LED	緑	超高速の点滅	パケット送信

SFP LED のワークフロー

次の表に、ブートアップ時の SFP LED の表示を示します。

SFP 挿入前	消灯
SFP 起動中	低速で緑の点滅
自動ネゴシエーション完了後	緑の点灯
CLI からトリガーされた SFP シャットダウン	消灯
CLI からトリガーされた SFP no shut	点滅後に緑の点灯
SFP トラフィック	緑の点滅

自動ネゴシエーション

SFP の LED に基づいて、自動ネゴシエーションのステータスを確認できます。shut/no shut 時または自動ネゴシエーション中は、次のシーケンスが確認されます。

低速で緑の点滅	アイドル
高速で緑の点滅	トレーニング
緑の点灯	ハンドシェイク成功、通信開始

SFP LED が緑色にゆっくり点滅してから緑色に速く点滅する場合、通常は自動ネゴシエーションモードであることを意味します。これが長時間続く場合は、DSLAM およびルータ DSL SFP

のパラメータを再確認する必要があります。次の章では、ルータ xDSL 設定について詳しく説明します。

DSL SFP ファームウェアのアップグレード

DSL SFP にファームウェアがロードされている。SFP にロードされているバージョンを確認し、ルータイメージで使用可能なバージョンと比較する必要があります。お客様は、ISP との契約に応じてアップグレードを決定する必要があります。

SFP をアップグレードするには SFP の最小設定が必要です。

```
configure t
Router(conf)#interface g0/0/0
Router(conf-if)#media-type sfp
Router(conf-if)#no shut
Router(conf-if)#exit
```

show controller vdsl 0/0/0 local コマンドを実行して、ファームウェアレベルを確認します。

```
Router#show controllers vdsl 0/0/0 local
SFP Vendor PID: SFPV5311TR
SFP Vendor SN: V021932028C
Firmware embedded in IOS-XE: 1_62_8463
Running Firmware Version: 1_62_8455
Management Link: up
DSL Status: showtime
Dumping internal info: idle
Dying Gasp: armed
Dumping DELT info:  idle
```

SFP をアップグレードするには、次のコマンドを使用します。

```
Router#upgrade hw-module subslot 0/0 sfp 0
Upgrade SFP firmware on interface GigabitEthernet0/0/0 from 1_62_8455 to 1_62_8463
Connection will be disrupted, Continue(Y/N)?y
Start ebm upgrade!!
..................................................
..................................................
................
firmware update success!!
```

このコマンドは新しいファームウェアをロードしてから、インターフェイスで shut/no shut を実行して SFP をリセットします。

（注） 17.5.1 以降では、IOS イメージにバンドルされている SFP ファームウェアに加えて、スタンドアロン SFP ファームウェアをアップグレードする機能があります。次に例を示します。

```
Router#upgrade hw-module subslot 0/0 sfp 0 {flash|usbflash0|msata}:sfp_fw_image
```

MTU の制限

SFP データシートの仕様により、MTU の制限は次のとおりです。

- VDSL では、DSL SFP インターフェイスの MTU 範囲は 64 ー 1800 バイト

- ADSL2/2+ では、DSL SFP インターフェイスの MTU 範囲は 64 ー 1700 バイト

ADSL2/2+

ADSL2/2+ の概要

この項では、ADSL2/2+ の概要を示します。

重要 ルータ SFP ベースの DSL サポートは、他の ISR DSL プラットフォームと比べると、設定とトラブルシューティングの点で異なります。ATM インターフェイスはなく、イーサネットと ATM 間のパケット変換は Adaption Layer5（AAL5）を介して内部的に処理されます。すべての設定は、コントローラ vdsl 0/0/0 および g0/0/0 のインターフェイス/サブインターフェイスにあります。AAL5 よりも UBR が推奨されています。

詳細については、以降の章を参照してください。

ADSL2/2+ は auto モードで動作します（DSL コントローラとの DSLAM 自動ネゴシエーションの設定）。Annex A は ADSL2+ でサポートされています。Annex A と reach-extended Annex L mode-1 は ADSL2 でサポートされています。これは TR-100/TR-105 に準拠しています。

- 自動ネゴシエーション ハンドシェイク手順では SFP は ITU-T G.994.1 DSL TRx に準拠しており、物理層管理では ITU-T G.997.1 for DSL TRx に準拠しています。
- DSL SFP は AVD2 CPE モードのみをサポートする ITU-T G.99x 標準に準拠しています。
- LLC/SNAP および VCMux イーサネット ブリッジド カプセル化オプションをサポートしています。
- すべての PPPoX カプセル化は、PPPoE を介してのみ設定されます。内部的にはパケット変換は ATM を介して処理されます。c111x ISR の場合のような PPPoA 設定はありません。
- ADSL-PVC はコントローラ VDSL 0/0/0 で設定できます。各 SFP は 8 つの PVC をサポートしています。
- 各 PVC は、802.1q VLAN タギングとのマッピングをサポートしています。
- VPI の範囲は 0 ー 255、VCI の範囲は 32 ー 65535 です。

show controller vdsl 0/0/0 に反映される「mode」は、常に PTM（パケット転送モード）です。内部的に ATM へのパケット変換が処理されます（AAL5）。

ADSL2/2+ の設定

ルータは、非対称デジタル加入者線（ADSL）2/2+ をサポートしています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `router> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `router# configure terminal`	グローバル設定モードを開始します。
ステップ 3	**controller vdsl <port>** 例： `router(config)# controller vdsl 0/0/0`	ADSL2/2+ コントローラに対してコンフィギュレーションモードを開始します。
ステップ 4	**adsl-pvc <vpi/vci>** 例： `router(config-controller)#adsl-pvc 0/35`	PVC の VPI と VCI パラメータを設定します。詳細なサブコマンドについては、ADSL2/2+PVC サブモード （412 ページ）を参照してください。
ステップ 5	**bridge-dot1q <1-4094>** 例： `router(config-controller-adsl-pvc)#bridge-dot1q 2`	PVC の bridge-dot1q パラメータを設定します。
ステップ 6	**encapsulation llcsnap|vcmux** 例： `router(config-controller-adsl-pvc)#encapsulation llcsnap`	デフォルトでは、無効です。llcsnap または vcmux のいずれかです。この例は、LLCSNAP としての PVC のカプセル化を示しています。
ステップ 7	**exit** 例： router(config-controller-adsl-pvc)# **exit**	新しい設定を有効にします。
ステップ 8	**end** 例： `router(config-controller)# end`	コンフィギュレーション モードを終了します。

ADSL2/2+ コントローラ設定コマンド

ここでは、コントローラ設定に固有の CLI コマンドの一部について説明します。

簡易（Brief）	書式	コマンド デフォルト	説明	他の IOS-XE ISR との違い
adsl-pvc	**adsl-pvc** *[name] {<vpi>/<vci>}* **adsl-pvc 0/35** **adsl-pvc PVC1 0/35**	なし	ADSL2/2+ PVC サブモード VPI/VCI 値 0 ～ 255 VCI 値 32 ～ 65535 ADSL2/2+ サブモードの詳細については、次を参照してください。ADSL2/2+ PVC サブモード （412 ページ）	VPI：0 ～ 31 VCI：1 ～ 1023
bitswap		デフォルトは [有効（Enabled）] です。	ビットスワップ	
carrier-set	**carrier-set** *[a43 a43c b43]*	a43 a43c b43	DSL SFP キャリアセット	c111x は modem vdsl オプションでこれらのトーンを定義します。たとえば、CLI を使用して v43 を無効にする必要があります。ルータでは、トーン v43 はデフォルトで無効になっています。
default			コマンドをデフォルト値に設定します。	
description			コントローラ固有の説明	

簡易（Brief）	書式	コマンド デフォルト	説明	他の IOS-XE ISR との違い
exit			コントローラ コンフィギュレーション モードを終了します。 これは、設定を有効にするために必須です。	
help			インタラクティブなヘルプ システムの説明	
mac-address	**mac-address** *<MAC address>*	デフォルトでは、MAC は事前に設定されています。	DSL SFP MAC アドレス。コントローラを動作させるために何も設定する必要はありません。	
modem vdsl			ルータには適用されません。c111x から継承されます。	c111x でのみ適用されます。
mpls			ルータには適用されません。c111x から継承されます。	c111x でのみ適用されます。
no			コマンドを無効にするか、またはデフォルト値を設定します	
shutdown			VDSL コントローラをシャットダウンします。	
sra		デフォルトは [有効（Enabled）] です。	シームレスなレート適応	

ADSL2/2+ PVC サブモード

次の表に、関連するコマンドを示します。

簡易（Brief）	書式	デフォルト	説明	他の IOS-XE ISR との違い
adsl-pvc	adsl-pvc vpi/vci	なし	DSL インターフェイスでは、最大 8 つの PVC をサポートできます。 VCI の範囲は 32 ー 65535 VPI の範囲は 0 〜 255	VPI/VCI 値 0ー31 VCI 値は 1 ー 1023
bridge-dot1q	**bridge-dot1q** *<1-4094>*	なし	802.1Q VLAN ID から PVC へのマッピング	
cbr	**cbr** *<peak cell rate>* CBP PCR の範囲は 0 ー 5500	非対応	固定ビットレート（CBR）サービスの設定 AAL5 よりも UBR が推奨されています。	48 ー 1408（Kbps 単位）
default-pvc	**default-pvc**	最初に作成された PVC	デフォルト PVC として PVC を設定 adsl-pvc の default-pvc コマンドは、DSL SFP で使用できるオプションです。アクティブな PVC が 2 つ以上ある場合に、DSL SFP がデフォルトとして処理する PVC を選択します。	
encapsulation	**encapsulation** *<llcsnap|vcmux>*	なし	ADSL2/2+ PVC カプセル化の設定	

簡易（Brief）	書式	デフォルト	説明	他の IOS-XE ISR との違い
exit			adsl-pvc サブコマンドの終了	
ubr	**ubr** <*peak cell rate*> UBR のピークセルレートの範囲は 0 ー 5500	対応	未指定ビットレート（UBR）サービスの設定	48 ー 1408（Kbps 単位）
vbr-nrt	**vbr-nrt** <*peak cell rate*> <*sustainable cell rate*> PCR の範囲は 0 ー 5500 SCR の範囲は 0 ー 5500	非対応	非リアルタイム可変ビットレートサービスの設定 AAL5 よりも UBR が推奨されています。	48 ー 1408（Kbps 単位）
vbr-rt	**vbr-rt** <*peak cell rate*> <*sustainable cell rate*> PCR の範囲は 0 ー 5500 SCR の範囲は 0 ー 5500	非対応	リアルタイム可変ビットレートサービスの設定 AAL5 よりも UBR が推奨されています。	48 ー 1408（Kbps 単位）
vlanid-rx	**vlanid-rx** *<1-4094>*	bridge-dot1q に応じる	DSL SFP が受信したイーサネットパケットの VLAN ID がルータに送信されるようにセットするよう DSL SFP を設定します。 DSL SFP VLAN 動作 vlanop-rx と組み合わせて使用し、イーサネットパケットから VLAN ID を削除するか、または置換します。	IoT ルータのみ

簡易（**Brief**）	書式	デフォルト	説明	他の **IOS-XE ISR** との違い
vlanid-tx	**vlanid-tx** *<1-4094>*	bridge-dot1q に応じる	ネットワークに送信するイーサネットパケットの VLAN ID を設定するように DSL SFP を設定します。 DSL SFP VLAN 動作 vlanop-tx と組み合わせて使用し、ネットワークにパケットを送信する前にイーサネットパケットから VLAN ID を削除または置換します。	IoT ルータのみ
vlanop-rx	**vlanop-rx** *<pass-through|remove|replace>*	Remove	DSL SFP が受信したイーサネットパケットに対する DSL SFP の VLAN ID 動作をルータに送信するように設定します。 VLAN の削除または置換動作は、vlanid-rx とともに使用されます。 パススルーオプションは、イーサネットパケットの既存の VLAN ID を保持します。	IoT ルータのみ

簡易（Brief）	書式	デフォルト	説明	他の IOS-XE ISR との違い
vlanop-tx	**vlanop-tx** <*pass-through*|*remove*|*replace*>	Replace	DSL SFP のイーサネットパケットに対する VLAN ID 動作をネットワークに送信するように設定します。 VLAN の削除または置換動作は、vlanid-tx とともに使用されます。 パススルーオプションは、イーサネットパケットの既存の VLAN ID を保持します。	IoT ルータのみ

ADSL2+ の例

次に、ADSL2+ 設定の例を示します。

（注） いくつかの主要な出力メッセージの説明については、コントローラ ステータス メッセージ（432 ページ）を参照してください。

```
Router#show controller vdsl 0/0/0
Controller VDSL 0/0/0 is UP

Daemon Status: UP

XTU-R (DS) XTU-C (US)
Chip Vendor ID: 'META' 'BDCM'.
Chip Vendor Specific: 0x0000 0x0762
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'META' ' '
Modem Vendor Specific: 0x0000 0x0000
Modem Vendor Country: 0xB500 0x0000
Serial Number Near: MET2023000A V5311TR 1_62_8463
Serial Number Far:
Modem Version Near: 1_62_8463 MT5311.
Modem Version Far: <value>

Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.992.3 (ADSL2) Annex A

TC Mode: PTM
```

```
Selftest Result: 0x00
DELT configuration: disabled
DELT state: not running

Failed full inits: 0
Short inits: 0
Failed short inits: 0

Modem FW Version:
Modem PHY Version:
Modem PHY Source: System

Line 0:

XTU-R (DS) XTU-C (US)
Trellis: ON ON
SRA: enabled enabled.
SRA count: 0 0.
Bit swap: enabled enabled.
Bit swap count: 0 0
Line Attenuation: 2.4 dB dB
Signal Attenuation: 5.0 dB 0.0 dB
Noise Margin: 8.2 dB 6.5 dB
Attainable Rate: 12491 kbits/s 1153 kbits/s
Actual Power: 0.0 dBm 10.2 dBm
Total FECC: 0 0
Total ES: 0 399
Total SES: 0 188
Total LOSS: 0 177
Total UAS: 103 6325
Total LPRS: 0 0
Total LOFS: 0 0
Total LOLS: 0 0


DS Channel1 DS Channel0 US Channel1 US Channel0
Speed (kbps): NA 12491 NA 1093
SRA Previous Speed: NA 0 NA 0
Previous Speed: NA 12583 NA 1097
Reed-Solomon EC: NA 0 NA 0
CRC Errors: NA 209 NA 0
Header Errors: NA 0 NA 0
Interleave (ms): NA 1.00 NA 1.00
Actual INP: NA 0.00 NA 0.00
```

ADSL2 Annex A の例

次に、ADSL2 Annex A 設定の例を示します。

（注） いくつかの主要な出力メッセージの説明については、コントローラ ステータス メッセージ（432 ページ）を参照してください。

```
show controller vdsl 0/0/0
Controller VDSL 0/0/0 is UP
Daemon Status: UP
XTU-R (DS) XTU-C (US)
```

```
Chip Vendor ID: 'META' 'BDCM'
Chip Vendor Specific: 0x0000 0x0762
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'META' ' '
Modem Vendor Specific: 0x0000 0x0000
Modem Vendor Country: 0xB500 0x0000
Serial Number Near: MET2023000A V5311TR 1_62_8463
Serial Number Far:

Modem Version Near: 1_62_8463 MT5311
Modem Version Far:
Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.992.5 (ADSL2+) Annex A
TC Mode: PTM
Selftest Result: 0x00
DELT configuration: disabled
DELT state: not running

Failed full inits: 0
Short inits: 0
Failed short inits: 0

Modem FW Version:
Modem PHY Version:
Modem PHY Source: System

Line 0:
XTU-R (DS) XTU-C (US)

Trellis: ON ON
SRA: enabled enabled
SRA count: 0 0
Bit swap: enabled enabled
Bit swap count: 0 0
Line Attenuation: 1.4 dB dB
Signal Attenuation: 2.4 dB 0.0 dB
Noise Margin: 9.5 dB 6.3 dB
Attainable Rate: 23550 kbits/s 1105 kbits/s
Actual Power: 0.0 dBm 12.2 dBm
Total FECC: 1 0
Total ES: 1 396
Total SES: 0 317
Total LOSS: 0 287
Total UAS: 57 3344
Total LPRS: 0 0
Total LOFS: 0 0
Total LOLS: 0 0
DS Channel1 DS Channel0 US Channel1 US Channel0

Speed (kbps): NA 23550 NA 1105
SRA Previous Speed: NA 0 NA 0
Previous Speed: NA 23580 NA 1109
Reed-Solomon EC: NA 0 NA 0
CRC Errors: NA 95 NA 4
Header Errors: NA 0 NA 0
Interleave (ms): NA 1.00 NA 1.00
Actual INP: NA 0.00 NA 0.00
Training Log : Stopped
Training Log Filename : flash:vdsllog.bin
```

ADSL2 Annex L の例

次に、ADSL2 Annex L 設定の例を示します。

（注） いくつかの主要な出力メッセージの説明については、コントローラ ステータス メッセージ（432 ページ）を参照してください。

```
show controller vdsl 0/0/0
Controller VDSL 0/0/0 is UP
Daemon Status: UP
XTU-R (DS) XTU-C (US)

Chip Vendor ID: 'META' 'BDCM'
Chip Vendor Specific: 0x0000 0x0762
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'META' ' '
Modem Vendor Specific: 0x0000 0x0000
Modem Vendor Country: 0xB500 0x0000
Serial Number Near: V0219320270 V5311TR 1_62_8463
Serial Number Far:

Modem Version Near: 1_62_8463 MT5311
Modem Version Far:
Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.992.3 (ADSL2) Annex L
TC Mode: PTM
Selftest Result: 0x00
DELT configuration: disabled
DELT state: not running
Failed full inits: 0
Short inits: 0
Failed short inits: 0
Modem FW Version:
Modem PHY Version:
Modem PHY Source: System
Line 0:
XTU-R (DS) XTU-C (US)

Trellis: ON ON
SRA: enabled enabled
SRA count: 0 0
Bit swap: enabled enabled
Bit swap count: 0 0
Line Attenuation: 2.5 dB dB
Signal Attenuation: 5.7 dB 0.0 dB
Noise Margin: 7.0 dB 6.2 dB
Attainable Rate: 10164 kbits/s 288 kbits/s
Actual Power: 0.0 dBm 8.4 dBm
Total FECC: 0 0
Total ES: 6 0
Total SES: 6 0
Total LOSS: 6 0
Total UAS: 54 31
Total LPRS: 0 0
Total LOFS: 6 0
Total LOLS: 0 0
DS Channel1 DS Channel0 US Channel1 US Channel0
```

```
Speed (kbps): NA 10164 NA 243
SRA Previous Speed: NA 0 NA 0
Previous Speed: NA 12495 NA 1089
Reed-Solomon EC: NA 0 NA 0
CRC Errors: NA 0 NA 0
Header Errors: NA 0 NA 0
Interleave (ms): NA 1.00 NA 1.00
Actual INP: NA 0.00 NA 0.00
Training Log : Stopped
Training Log Filename : flash:vdsllog.bin
```

VDSL2

VDSL2 の概要

この項では、VDSL2 の概要を示します。

ルータ DSL SFP-VADSL2+-I は、ITU-T 標準 G.993.2（VDSL2）に準拠して VDSL2 Annex A、B のサポートを提供します。この xDSL SFP は、TR-114（VDSL2 Annex A および B のパフォーマンス）と TR-115（University of New Hampshire による VDSL2 機能検証テスト）にも準拠します。SFP は、AVD2 CPE モードのみをサポートする ITU-T G.99x 標準に準拠します。

- 設定可能なバンドプラン。3072/4096 と 8 バンド/4 通過帯域制約に従う北米の Annex A（G.998）と欧州の Annex B（G.997、998）バンドプランに準拠
- すべての VDSL2 プロファイル（8a/b/c/d、12a / b、17a、30a）をサポート
- EU タイプのアップストリームバンド 0（US0）をサポート
- DSL TRx の ITU-T G.994.1 ハンドシェイク手順に準拠
- DSL TRx の ITU-T G.997.1 物理層管理に準拠
- CPE モードの ITU-T G.993.5 Self-FEXT キャンセル（ベクトル化）に準拠
- 堅牢なオーバーヘッドチャネル（ROC）をサポート
- D/L の変更とビットスワッピングによるシームレスレート適応（SRA）を含むオンライン再設定（OLR）をサポート
- アップストリーム/ダウンストリーム電源バックオフ（UPBO / DPBO）をサポート
- DELT をサポート
- VDSL2 でサポートされている最大 MTU サイズは 1,800 バイト
- 標準準拠の VDSL2 モードは PTM（パケット転送モード）
- VDSL2 のベクトル化をサポート

設定および表示用のコマンドについては、以下の詳細な項を参照してください。**show controller vdsl 0/0/0** は検証のための基本的なコマンドです。

VDSL2 の設定

ルータは Very-High-Bit-Rate デジタル加入者線（VDSL2）をサポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `router> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 例： `router# configure terminal`	グローバル設定モードを開始します。
ステップ 3	**controller vdsl 0/0/0** 例： `router(config-controller)# controller vdsl 0/0/0`	VDSL2 コントローラに対してコンフィギュレーション モードを開始します。
ステップ 4	**carrier-set** *a43 a43c b43* 例： `router(config-controller)# carrier-set a43|a43c|b43`	キャリアセットを設定します。複数選択可能。デフォルトは a43、a43c、b43 です。 v43 はデフォルトで無効になっています。
ステップ 5	**end** 例： `router(config-controller)# end`	コントローラ コンフィギュレーション モードを終了します。

VDSL2 コントローラ設定コマンド

ここでは、コントローラ設定に固有の CLI コマンドの一部について説明します。

簡易（Brief）	書式	コマンド デフォルト	説明
bitswap		デフォルトは [有効（Enabled）] です。	ビットスワップ
capability	**capability** *[annex-j]*	なし	DSL SFP 機能の設定
carrier-set	**carrier-set** *[a43 b43 a43c]*	a43 b43 a43c	DSL SFP キャリアセット
default			コマンドをデフォルト値に設定します。

簡易（Brief）	書式	コマンド デフォルト	説明
description			コントローラ固有の説明
exit			コントローラ コンフィギュレーションモードを終了します。
help			インタラクティブなヘルプ システムの説明
mac-address	**mac-address** <*MAC address*>	デフォルトでは、MAC は事前に設定されています。	DSL SFP MAC アドレス。コントローラを動作させるために何も設定する必要はありません。
modem vdsl		該当なし	モデムの設定
mpls			IoT ルータには適用されません。c111x から継承されます。
no			コマンドを無効にするか、またはデフォルト値を設定します
shutdown			VDSL コントローラをシャットダウンします。
sra		デフォルトは [有効（Enabled）] です。	シームレスなレート適応

VDSL の例

次に、VDSL 設定の例を示します。

```
show controllers vdsl 0/0/0
Controller VDSL 0/0/0 is UP
Daemon Status: UP
XTU-R (DS) XTU-C (US)

Chip Vendor ID: 'META' 'IKNS'
Chip Vendor Specific: 0x0000 0x0101
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'META' ' '
Modem Vendor Specific: 0x0000 0x2AB0
Modem Vendor Country: 0xB500 0x37A0
Serial Number Near: E80462D1B001 SFP-V5311-T-R 8431
```

```
Serial Number Far: ^A5u
Modem Version Near: 1_62_8431 MT5311
Modem Version Far: 6.7.0.15IK005010

Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.993.2 (VDSL2) Profile 17a

TC Mode: PTM
Selftest Result: 0x00
DELT configuration: disabled
DELT state: not running

Failed full inits: 0
Short inits: 0
Failed short inits: 0

Modem FW Version:
Modem PHY Version:
Modem PHY Source: System

Line 0:
XTU-R (DS) XTU-C (US)

Trellis: ON ON
SRA: enabled enabled
SRA count: 0 0
Bit swap: enabled enabled
Bit swap count: 0 0
Line Attenuation: 2.7 dB dB
Signal Attenuation: 3.9 dB dB
Noise Margin: 7.2 dB 24.8 dB
Attainable Rate: 113289 kbits/s 86904 kbits/s
Actual Power: 9.3 dBm 8.1 dBm
Per Band Status: D1 D2 D3 U0 U1 U2 U3
Line Attenuation(dB): 0.0 1.5 2.5 N/A 0.2 0.2 0.6
Signal Attenuation(dB): 0.0 2.0 4.0 N/A 0.0 0.0 0.0
Noise Margin(dB): 0.0 7.2 7.2 0.0 24.7 24.8 24.8
Total FECC: 0 2203
Total ES: 1 2280
Total SES: 0 2199
Total LOSS: 0 2199
Total UAS: 81 2199
Total LPRS: 0 0
Total LOFS: 0 0
Total LOLS: 0 0
DS Channel1 DS Channel0 US Channel1 US Channel0

Speed (kbps): NA 103985 NA 50219
SRA Previous Speed: NA 0 NA 0
Previous Speed: NA 103985 NA 50219
Reed-Solomon EC: NA 0 NA 0
CRC Errors: NA 117 NA 1
Header Errors: NA 0 NA 0
Interleave (ms): NA 0.00 NA 0.02
Actual INP: NA 0.00 NA 0.00
Training Log : Stopped
Training Log Filename : flash:vdsllog.bin
```

いくつかの主要な出力メッセージの説明については、コントローラ ステータス メッセージ（432 ページ）を参照してください。

トラブルシューティングと L1 トレーニングログ

トラブルシューティング

この項では、DSL 制御やデータパスが稼働していない場合のトラブルシューティングとデバッグについて説明します。

問題：WAN インターフェイス g0/0/0 がダウンしている場合：

回避策：次を試します。

- L1 のケーブル配線、ネットワーキングを確認し、別の SFP で確認する
- **show int g0/0/0**、**show run all**、および **show version** の出力をキャプチャする
- g0/0/0 に **media-type sfp** 設定があり、インターフェイスがシャットダウンされているかどうかを確認する
- 別の SFP を試して検出されるかどうかを確認する
- SFP の LED ステータスを確認する。SFP 上の LED 表示 （405 ページ）を参照してください。

問題：コントローラの状態が DOWN の場合：

次に例を示します。

```
Router#show controllers vdsl 0/0/0
Controller VDSL 0/0/0 is DOWN
```

回避策：次を試します。

- L1 ケーブル配線を確認する
- RJ11 オスと RJ45 メスのコネクタに RJ11 ケーブルを差し込んで、位置が合うかどうかを確認する
- 実行中の FW がシステム FW と同じであることを確認する。そうでない場合は、SFP FW をアップグレードします。DSL SFP ファームウェアのアップグレード （407 ページ）を参照してください。
- すべての L1 トレーニングログの出力を収集する。フォルダ内の L1 デバッグログが Cisco TAC に送信されること、およびサービス内部コマンド **test vdsl option 0x0 6** の出力と **show controller 0/0/0 local** の出力を確認します。L1 トレーニングログ （434 ページ）を参照してください。

- 考えられる回避策：上記のログを収集した後、ルータが再起動して回復するかどうかを確認します。それでも動作しない場合は、SFP を再度ホットリムーブまたは挿入してみます。

問題：コントローラが稼働していても **show controller vdsl 0/0/0** に DSL リンクアイドルが表示されます。

回避策：次を試します。

- **show controller vdsl 0/0/0 local** が Running FW = System FW を表示することを確認する。そうでない場合は、FW をアップグレードし、shut/no shut g0/0/0 を実行します。DSL SFP ファームウェアのアップグレード （407 ページ）を参照してください。
- DSLAM でキャリアセットが（コントローラ vdsl 0/0/0 で）一致することを確認する
- 設定が変更された場合は、DSLAM インターフェイスを再起動する
- DSLAM 側のパワースペクトル密度、周波数帯域計画、プロファイル、動作モード、VLAN などを微調整する。ルータ DSL コントローラ側では、auto モードがデフォルトであり、キャリアセットを除き、設定は必要ありません。例：DSLAM が POTS のみをサポートする場合、キャリアセットを a43 に設定することを推奨します。デフォルトでは、a43、a43c、b43 が許可されています。
- DSLAM プロファイルには、VDSL2/ADSL2/2+ により、サポートされるプロファイル、帯域などのみが含まれていることを確認します。DSL 機能の仕様（401 ページ）の表を参照してください。
- service internal コマンドの **test vdsl rawcli "basic show summary 1"** を連続して使用すると、ステータスが Idle/Handshake/Training から Idle に戻るか、または Idle でスタックすることがあります。Idle に戻る場合は、DSLAM プロファイルの設定を再確認します。スタックする場合は、L1 デバッグログを共有します。
- DSLAM の設定が以前機能していたものと同じであり、イメージのアップグレード後、または新しい SFP の変更後にコントローラが稼働していてもネゴシエーションが実行されない場合は、次の情報をシスコに提供してください。
  - SFP LED ステータス
  - Capture **show version**, **show running-config**, **show run all | sec controller**, **show interface gigabitethernet 0/0/0**, and **show controller vdsl 0/0/0 local**.
- 考えられる回避策：シスコにログを提供した後、write erase を試し、ルータをリロードします。また、このデバイスに接続されている DSLAM インターフェイスを shut/no shut し、SFP とケーブルを再度取り外します。

問題：コントローラは稼働しているのにデーモンがダウンしている。

回避策：次を試します。

- debug vdsl を有効にしてデバッグし、Cisco TAC と共有する。
- 既知の最新の動作設定とソフトウェアバージョンを提供する。
- 考えられる回避策：シスコにログを提供した後、write erase を試し、ルータをリロードします。また、このデバイスに接続されているDSLAMインターフェイスをshut/no shutし、SFP とケーブルを再度取り外します。
- 適切なdatak9、securityk9、およびnetwork-advantageライセンスがピアとクライアントの両方で有効になっているかどうかを確認します。

問題：**show controller vdsl 0/0/0** で DSLAM up のプロファイルがありコントローラは稼働しているが、ダイヤラは IP を取得していない

回避策：次を試します。

- ルートの確認
- **debug dialer** の出力を調べて、情報が提供されているかどうかを確認します。ダイヤラのアイドル時間がすぐにリセットされる場合は、ダイヤラのアイドルタイムアウトを変更します（デフォルトは 120 秒で、十分最適な値です）。
  - PPPoEサーバとPPPoEクライアント/CPEの両方にSWライセンス（datak9、securityk9、およびnetwork-advantage）があることを確認します。
  - 次に、機能する基本的なダイヤラ設定を示します。

```
interface Dialer1
ip address negotiated
no ip redirects
encapsulation ppp
dialer pool 1
dialer-group 1
no cdp enable
ppp authentication chap callin
ppp chap hostname WORD
ppp chap password 0 WORD
ppp ipcp route default
!
ip route 0.0.0.0 0.0.0.0 Dialer1 (or any route that works in user environment)
```

- PPPoE サーバの認証クレデンシャルが PPPoE クライアントと一致していることを確認します。
- DHCPを使用する場合は、サーバにリースするための十分なアドレスがあることを確認します。

- パケットを受信した場合にデバッグするには、ヘッドエンド/ピアルータで debug ppp session と debug ip dhcp server packet detail を有効にします。ルータで debug ppp session を有効にする。
- 上記の手順で問題を解決できなかった場合は、上記のすべてのデバッグ情報を次の情報とともに Cisco TAC に提供してください。
  - **show version**、**show running**、**show run all | sec controller**、**show controller vdsl 0/0/0**、および **show controller vdsl 0/0/0 local** の出力
  - service internal コマンドの **test vdsl rawcli "basic show summary 1"**、**basic show summary 1**、および **test vdsl option 0x0 6** の出力
  - DSLAM の設定
  - L1 トレーニングログL1 トレーニングログ （434 ページ）を参照してください。
- 考えられる回避策：上記のログをシスコに提出するために順番に収集した後、write erase を試し、ピアとルータをリロードします。具体的には、PPP設定でダイヤラインターフェイスを削除してからもう一度適用します。最後の手段としては、このルータ DSL SFP インターフェイスに接続されている DSLAM インターフェイスの shut/no shut を試します。さらに、動作を切り分けるため、別のルータ（使用可能な場合）でこの SFP を検証します。動作する場合は、同じルータで複数の SFP を検証します（SFP またはルータの問題の場合は絞り込みます）。

問題：コントローラが動作しておりダイヤラが起動しているが、ダイヤラが IP を取得していない場合、認証は PAP でのみ機能し、CHAP では機能しません。

解決策：次のようなシナリオがあるとします。

show controller vdsl 0/0/0 が showtime を表示

show pppoe session が確立された PPP セッションを表示。

次に、仮想アクセスがダイヤラにバインドされていることがわかりますが、それでもダイヤラはダイヤラの PAP 設定で IP を取得しませんでした。しかし、PPPoE サーバー側では CHAP が機能しません。CHAP認証に成功し、デバイス ack も表示されましたが、PPPoE クライアント/デバイス側で IP をまだ取得していません。

debug ppp packet はすべてが正常であることを示しましたが、IP をまだ取得していません。このような場合は、次のように有効にして監視します。**debugppp authentication** を有効にすると、chap ハンドシェイクが成功した後、ルータクライント（または任意の IOS ルータ）で chap にデフォルトのローカルホスト名が設定されている場合、無効にする必要があるルータ CLI で設定されたローカルホスト名に基づいて検証するデバイス/クライアントによって、別の試行があったことに気づくことがあります。

```
config t
service internal
Int Dialer1
```

```
no ppp chap ignoreus
no shut
exit
```

詳細については、PPP CHAP 認証の理解および設定のリンクを参照してください。
https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html

問題：コントローラが稼働している場合にダイヤラはIPを取得しましたが、ダイヤラをself-pingしたり、PPPoE サーバーを ping したりできません。

回避策：次を試します。

- 適切な SW ライセンス（datak9、securityk9、および network-advantage）が PPPoe サーバとクライアントの両方で有効になっていることを確認します。
- PPPoE クライアントセッションで icmp が有効になっているかどうかを確認します（アクセスリスト経由で有効にします）。
- **debug pppoe session** で pap/chap 認証と一致していることを確認します。
- show pppoe session should reflect session（ダイヤラとの仮想アクセスバインディング）
- PPPoEセッションのデバッグの場合、次の項はすべてのIOSプラットフォームに共通します。 https://www.cisco.com/c/en/us/td/docs/routers/ir910/software/release/1_0/configuration/guide/ir910scg/swpppoe.pdf
- g0/0/0 DSL インターフェイスにスタティック IP を適用し、DSLAM とピアを ping できるかどうかを確認します（DSL SFP の問題を特定するため）
- 次に、基本的な PPPoE サーバと PPPoE クライアントの設定を示します。PPPoE サーバもCisco IOS デバイスであることが前提です。

```
PPPoE Server
ip dhcp excluded-address 41.41.41.1 41.41.41.9
!
ip dhcp pool 41-41-41-pool
network 41.41.41.0 255.255.255.0
default-router 41.41.41.1
 lease 2
!
username dslpeer password 0 dslpeerpass
!!
bba-group pppoe global
virtual-template 1
!
interface GigabitEthernet0/0/0
no ip address
media-type sfp
!
interface GigabitEthernet0/0/0.1
encapsulation dot1Q 1 native
ip address 41.41.41.1 255.255.255.0
pppoe enable group global
!
interface Virtual-Template1
```

```
ip unnumbered GigabitEthernet0/0/0.1
peer default ip address dhcp-pool 41-41-41-pool
ppp authentication pap chap
!
 >>>>>> Add routes as relevant, next hop being the IP that Router Dialer acquires
!
ip route 10.0.0.0 255.255.255.0 41.41.41.3 >> dialer ip, change as necessary

PPPoE Client:
controller VDSL 0/0/0
Carrier-set a43 >>> Can set to whichever [a43, b43, a43c, v43 depending on DSLAM
support]
interface GigabitEthernet0/0/0
no ip address
media-type sfp
!
interface GigabitEthernet0/0/0.1
encapsulation dot1Q 1 native
pppoe enable group global
pppoe-client dial-pool-number 1
!
interface Dialer1
ip address negotiated
no ip redirects
encapsulation ppp
dialer pool 1
dialer-group 1
no cdp enable
ppp authentication chap callin
ppp chap hostname dslpeer
ppp chap password 0 dslpeerpass
ppp ipcp route default
!
ip route 0.0.0.0 0.0.0.0 Dialer1
```

問題：DSL トラフィックがしばらくの間は通過していましたが、そのうちに帯域幅が低くなります。

回避策：次を試します。

- DSLAM プロファイルの PSD、バンドプランの設定が微調整されていることを確認します（このような場合、理想としてはルータ DSL SFP とは無関係であることです）。
- Cisco ルータ DSL インターフェイス、ダイヤラインターフェイスで ip arp タイムアウトが引き上げられていることを確認します（これは、トラフィックが集中している場合や輻輳時に特に役立ちます）。

（注） 次のコマンドは、トラブルシューティングに役立つ場合があります。

インターフェイスのステータス：

```
Router#show ip interface brief
Use this command to validate if Dialer acquired an IP address
```

インベントリのステータス：

```
Router#show inventory

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

NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9 , VID: V03 , SN: FCW23500H5X

NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9 , VID: V03 , SN: FOC23473SRK

NAME: "module subslot 0/0", DESCR: "IR1101-ES-5"
PID: IR1101-ES-5 , VID: V01 , SN:

NAME: "subslot 0/0 transceiver 0", DESCR: "GE T"
PID: SFP-VADSL2+-I , VID: V01 , SN: MET2023000A
Ignore the description, it will always reflect GE T for all ISR Router SFPs
PID and S/N are what matter
```

実行中のソフトウェアの詳細を表示するコマンド：

```
Router#show running-config all
Router#dir flash:
Router#dir nvram:
Router#show version
```

次に、自動ネゴシエーションのステータスも反映するデバッグコマンドのいくつかを示します。

```
Router#configure terminal
Router#service internal
Router#exit
The following test command will reflect auto-negotiation status:
Router#test vdsl rawcli "basic show summary 1"
Link time Rate US/DS Mode Status Annex TxPkts/RxPkts
4 1097/12491 ADSL2 Showtime AnnexA 0/0
```

よく寄せられる質問

この項では、よく寄せられるいくつかの質問に対する回答を示します。

質問：コントローラで特定の Annex とプロファイルに VDSL2 または ADSL2/2+ を設定するにはどうすればよいですか。

回答：ルータ DSL SFP は auto モードでのみ動作します。SFP コントローラ側で設定するオプションはありません。変更は DSLAM 側でのみ行うことができます。

質問：設定するコントローラ ADSL オプションがありません。

回答：Controller vdsl 0/0/0 は、Cisco IOS-XE 製品全体で共通の名称です。同じ CLI がすべての DSL プロトコル（VDSL2、ADSL2、ADSL2+）に有効です。

質問：設定する ATM インターフェイスがありません。

回答：ユーザ設定用の ATM インターフェイスはありません。Controller vdsl 0/0/0 と DSL SFP WAN インターフェイス g0/0/0 のすべての設定オプションとそのサブインターフェイス オプションでは、ATM パケットは DSL SFP によって処理され、イーサネットパケットとして再構築されます。Annex A、L がサポートされています。

質問：show controller vdsl 0/0/0 のトレーニングログが機能していません。開始/停止するオプションがありません。

回答：このオプションは、c111x プラットフォーム専用であり、ルータ DSL SFP ではありません。ルータプラットフォーム L1 のデバッグについては、次を参照してください。L1 トレーニングログ （434 ページ）

質問：DSL SFP ファームウェアはどこでダウンロードできますか。

回答：

17.5.1 以降では、スタンドアロン FW は IOS の Flash:、mSATA、および usbflash0: を介してアップグレードできます。DSL ファームウェアをアップグレードするには、次を参照してください。DSL SFP ファームウェアのアップグレード （407 ページ）

質問：ADSL2 Annex L が動作していません。

回答：DSLAM プロファイル設定のビットレートが許可された正しいレートであることを確認します。ルータ DSL SFP は自動モードであるため、最も高いビットレートのプロファイルとネゴシエートします（そのため、これは主に DSLAM 設定の微調整によって決まります）。

質問：Annex-L Mode1 はサポートされていますが、Mode2 はサポートされていません。

回答：DSLAM 設定でサポートされていないモード/プロファイル/帯域が無効になっていることを確認します。サポートされている仕様については、DSL 機能の仕様 （401 ページ）を参照してください。

質問：ADSL2/2+ で、バーストサイズ（ピークセルレートと持続セルレート）が最大 5500 に設定されている場合、ダイヤラがフラッピングし続けます。

回答：ダイヤラがフラッピングしている場合、ピアのアップストリームを受信している可能性があり、高レートのダウンストリーム トラフィックを処理できませんでした。ダイヤラ設定で **ip keepalive** を無効にするか、デフォルトの keepalive を最大値に引き上げます。

質問：PVC の許可数

回答：8

質問：コントローラの設定が有効になりません。

回答：設定を有効にするには、コントローラ コンフィギュレーション モードを終了します。回避策として、コントローラ インターフェイスを shut/no shut を実行します。理想としては、これはコントローラ設定モードから「終了」した時点を反映する必要があります。DSLAM がプロファイル基準と一致していることを確認します。サポートされていない帯域/プロファイルはハンドシェイクを遅延させる可能性があるため、削除する必要があります。

質問：ADSL2/2+ コントローラの設定で、最大バーストサイズの設定が有効になりません。

回答：nrt-VBR または rt-VBR を設定する場合、ピークセルレート（PCR）と持続可能セルレート（SCR）の設定のみがサポートされています。オプションの最大バーストサイズ（MBS）はサポートされていません。

質問：L1 デバッグログのキャプチャ時にシステムがハングし、かなりの時間がかかります。show コマンドは機能しません。

回答：**debug vdsl controller 0/0/0 dump** *internal folder_name* を実行すると、ほとんどのシステム リソースが消費されます。そのための警告 syslog も表示されます。これは、コントローラの状態によっては完了するまでに約 10 分かかります。プロセスの実行時に複数回にわたってコントローラが shut/no shut を繰り返します。このアクティビティ中は介入しないでください。完

了したら、syslog で「DONE」を確認し、shut/no shut g0/0/0 のプロンプトが表示されることを確認します。

質問：新しい SNMP MIB は追加されていますか。

回答：リリース 17.5.1 では、次の ADSL2+ MIBS が導入されました。

- 1.3.6.1.2.1.10.94.1.1.4.1.2 ADSL-LINE MIB:adslAtucChanCurrTxRate
- 1.3.6.1.2.1.10.94.1.1.5.1.2 ADSL-LINE MIB:adslAturChanCurrTxRate
- 1.3.6.1.2.1.10.94.1.1.2.1.8 ADSL-LINE MIB:adslAtucCurrAttainableRate
- 1.3.6.1.2.1.10.94.1.1.3.1.8 ADSL-LINE MIB:adslAturCurrAttainableRate

質問：SFP がルータでスタックしています。

回答：これは IR1101 の古いモデルで発生する可能性があります。前面プレートが変更されました。

SFP ラッチを（すべての SFP と同様に）慎重に取り扱うには、次の手順に従います。SFP のホットリムーブを実行する場合は、次の手順を実行します。

- ラッチを外し（カチッと音がする）、45 ー 90 度に傾けます。押し付けたり、無理に倒したりしないでください。
- ケーブルを取り外します。
- SFP を取り外します。

⚠

注意 SFPを挿入するときは、ロックされたことを音で確認します。ケーブルを差し込みし、ラッチを閉じます。もう一度クリック音が聞こえます。ラッチを無理に押し込むと破損し、ルータから SFP が抜けなくなります。回避策としては、前面プレートを取り外して SFP を取り外します。

コントローラ ステータス メッセージ

この項では、**show controller vdsl 0/0/0** コマンドの主要な出力メッセージについて説明します。

次の表を参照してください。

出力メッセージ	説明
Controller VDSL 0/0/0 is UP	コントローラの状態

出力メッセージ	説明
Daemon Status: UP	内部 IOS DSL デーモンの状態
Chip Vendor ID: 'META' 'BDCM'.	SFP Metanoia チップ情報
Chip Vendor Specific: 0x0000 0x0762	EEPROM プログラミングで SFP Metanoia チップ情報が書き込まれる
Chip Vendor Country: 0xB500 0xB500	SFP Metanoia チップ情報
Modem Vendor ID: 'META'	SFP Metanoia チップ情報
Modem Vendor Specific: 0x0000 0x0000	SFP Metanoia チップ情報
Modem Vendor Country: 0xB500 0x0000	SFP Metanoia チップ情報
Serial Number Near: MET2023000A V5311TR 1_62_8463	SFP Metanoia チップ情報
Serial Number Far:	SFP Metanoia チップ情報、空の場合は無視、Serial Number Near は必要な値
Modem Version Near: 1_62_8463 MT5311	モデムファームウェア情報
Modem Version Far: <value>	空の場合は無視。上記の Near バージョンが重要
Modem Status: TC Sync (Showtime!)	L1 SFP 自動ネゴシエーションステータスを表示 SFP が shut/no shut の場合、次の自動ネゴシエーション シーケンスが表示されます。 Idle、Handshake、Training、Showtime! Showtime は自動ネゴシエーションが完了したことを示します。
DSL Config Mode: AUTO	常に AUTO モード、ADSL2/2+、VDSL2 用 に設定する特定の CLI なし
Trained Mode: G.992.3 (ADSL2) Annex A	ITU と Annex タイプを明示
TC Mode: PTM	ADSL2/+ の場合でも、常にパケット転送モード。SFP はすでに ATM をイーサネットフレームに変換している。
SRA: enabled enabled.	デフォルトでは有効
Bit swap: enabled enabled.	デフォルトでは有効

L1 トレーニングログ

デバイスを設定するには、次の手順を実行します。

```
Router#configure terminal
Router#service internal
Router#logging console
Router#exit
```

デバッグを設定するには、次の手順を実行します。

```
Router#debug vdsl sfp debug | error | event | info | packet For SFP level debuging
```

```
Router#debug vdsl controller 0/0/0 dump internal {dir} For L1 debugging
```

L1 デバッグダンプが開始されると、次のように表示されます。

```
%VDSL_SFP_MGR-5-DUMP_START: Dump internal info started on interface GigabitEthernet0/0/0
```

重要 **この時点ではデバイスを使用できません。完了するまで約 10 分待ちます。**

その時点で、次のように表示されます。

```
%VDSL_SFP_MGR-4-DUMP_DONE: Dump internal info done, please shut/no shut on interface
GigabitEthernet0/0/0 to recover
```

デバイスを通常の動作モードに回復するには、次の手順を実行します。

```
Router#configure terminal
Router#interface g0/0/0
Router#shut
Router#no shut
Router#exit
```

bootflash: に保存されたディレクトリログをシスコに提供します。

（注） 新しいログまたはデバッグを開始するたびに、既存の情報に追加するのではなく、新しいディレクトリに保存することを推奨します。

Metanoia SFP デバッグコマンドを有効にするには、次の手順を実行します。

```
Router#configure terminal
Router#service internal
Router#exit
Router#test vdsl rawcli “basic show summary 1” This command shows the L1 auto-negotiation
 status
Link time Rate US/DS Mode Status Annex TxPkts/RxPkts
773 1089/23628 ADSL2+ Showtime AnnexA 470/338

Router#test vdsl option 6 0x0 If functional, State = 2 should display. This command shows
 basic L1 bringup of DSL SFP and it's states. Provide to Cisco for L1 troubleshooting.
Debug flags: 0x8000
Seq 0: slot=0 slot_port=0 bay=0 port=0 Name:MetaMgr0_0_0
MetanoiaPort=0 SFP type: 1 State: 2 cnt=855
MAC:00:00:00:00:00:00 Choice:0
```

```
hw interface:GigabitEthernet0/0/0 sw interface:GigabitEthernet0/0/0
Firmware file: /etc/SFP_V5311-T-R_CSP.b, size=491520, version=1_62_8463
SFP version: 1_62_8463
Notification Seq: 0x1 cnt: 0xB3 Stat Cycle:255
VDSL State: 5
EBM Tx: 21039 Rx: 21031
EBM Wait Timeout: 8 Rx Loss: 0
G994 vid CO: BDCM CPE: META
Serial No CO: CPE: MET2023000A V5311TR 1_62_8463
Version CO: CPE: 1_62_8463 MT5311
Capability CO: 000000000001000000 CPE: 000000000001000000
Line Attn: UP: 65535 DOWN: 13
```

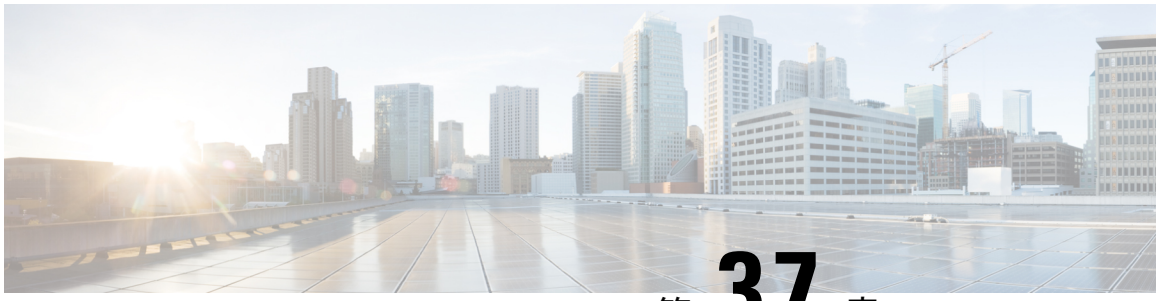
SFP をリセットするためのヒント：

- 理想的には、g0/0/0 shut/no shut はほとんどの場合に動作します（たとえば、ファームウェアアップグレード後、ホット OIR など）。

SFP をハードリロードするには、次の手順を実行します。

```
Router#hw-module subslot 0/0 reload
```

このオプションは、ソフトウェアモジュールを含むサブスロット全体を強制的にリロードします。したがって、接続が telnet/ssh 経由の場合、1 ー 2 分間アクセスできなくなり、バッファされたすべての messages/syslog が出力されます。



第 37 章

アウトオブバンド管理（OOB）

この章は、次の項で構成されています。

アウトオブバンド管理（OOB）

4G に障害が発生した場合に備えてさらに冗長性を確保するため、OOB には 2 台のルータをまとめて 1 本の USB ケーブルで接続する方法が用意されています。これにより、ルータ A の USB ポートをルータ B の USB コンソールに接続してルータ A からルータ B のコンソールポートにアクセスできるため、アウトオブバンド接続を維持できます。

この機能は IOS CLI で実装する必要があります。ユーザは別のルータの USB コンソールに tty 回線（/dev/ttyUSB）経由でリバース telnet を実行できる必要があります。

OOB トポロジ

次の図に、2 台の IR1101 ルータ間の物理的な接続を示します。

図 *107* : トポロジ

上の青い線は、USB 2.0 タイプ A から USB 2.0 ミニ USB タイプ B へのケーブルです。次の設定については、このトポロジを参照してください。

機能に関する警告

各ルータを設定する前に、両方のルータの基本的なシリアル設定を確認します。

```
line con 0
 stopbits 1
 speed 9600
```

（注） IR1101 の古さに応じて、デフォルトのボーレートは 9600 または 115200 になります。

- Plug and Play はサポートされていません。設定前にケーブルを取り付ける必要があります。
- OOB は、USB ポートである async0/2/1 でのみ機能します。Async0/2/0 は IR1101 のシリアルインターフェイスです。
- この機能を終了するには、「Ctrl-Shift-6」、「x」、「disconnect」の順に押します。

OOB の設定

ルータ A とルータ B の例については前の図を参照してください。ルータ A からルータ B のコンソールにアクセスするには、次の手順を実行します。

ルータ A の電源を投入し、次の設定を行います。

```
interface Async0/2/1
 ip address 20.0.0.1 255.0.0.0
```

```
 encapsulation relay-line
!
line 0/2/1
 transport input all
 transport output all
```

回線 51 の速度がルータ B のコンソールと同じであることを確認します。

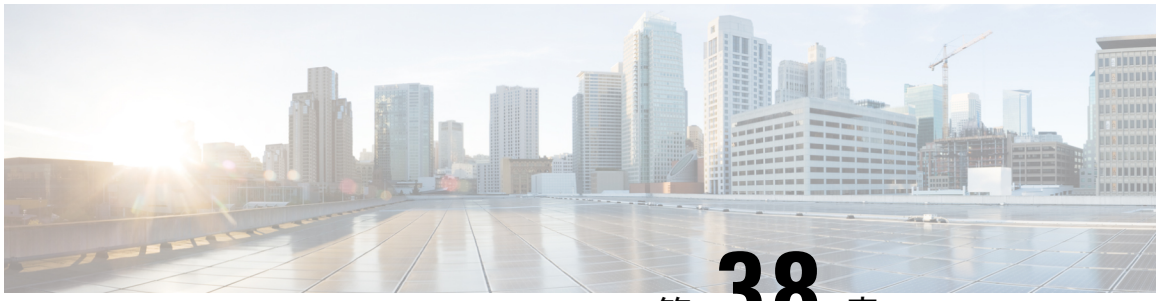
```
IR1101-A#show line

   Tty Line Typ     Tx/Rx    A Modem  Roty AccO AccI  Uses  Noise Overruns  Int
*     0    0 CTY              -    -      -    -    -     4      0    0/0       -
  0/0/0    2 TTY      0/0     -    -      -    -    -     0      0    0/0       -
  0/2/0   50 TTY   9600/9600  -    -      -    -    -     4      0    0/0       -
  0/2/1   51 TTY   9600/9600  -    -      -    -    -     4      0    0/0       -
     74   74 VTY              -    -      -    -    -     3      0    0/0       -
     75   75 VTY              -    -      -    -    -     1      0    0/0       -
     76   76 VTY              -    -      -    -    -     0      0    0/0       -
     77   77 VTY              -    -      -    -    -     0      0    0/0       -
     78   78 VTY              -    -      -    -    -     0      0    0/0       -
     79   79 VTY              -    -      -    -    -     0      0    0/0       -
     80   80 VTY              -    -      -    -    -     0      0    0/0       -
     81   81 VTY              -    -      -    -    -     0      0    0/0       -
     82   82 VTY              -    -      -    -    -     0      0    0/0       -
     83   83 VTY              -    -      -    -    -     0      0    0/0       -
     84   84 VTY              -    -      -    -    -     0      0    0/0       -
     85   85 VTY              -    -      -    -    -     0      0    0/0       -
     86   86 VTY              -    -      -    -    -     0      0    0/0       -
     87   87 VTY              -    -      -    -    -     0      0    0/0       -
     88   88 VTY              -    -      -    -    -     0      0    0/0       -

 Line(s) not in async mode -or- with no hardware support:
1, 3-49, 52-73, 89-735
```

ルータ A で回線 0/2/1 を設定します。

```
IR1101-A#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
IR1101-A(config)#line 0/2/1
IR1101-A(config-line)#speed 9600
IR1101-A(config-line)#
```

ルータ A の IP（ポート 2051）を介してルータ B に Telnet で接続します。

```
IR1101-A#telnet 20.0.0.1 2051
Trying 20.0.0.1, 2051 ... Open


IR1101-B#

IR1101-B#   <== to exit, press “Ctrl-Shift-6”, then “x”, then “disconnect”

IR1101-A#disconnect
Closing connection to 20.0.0.1 [confirm]
```



第 38 章

プロセス ヘルス モニタリング

この章では、ルータの各種コンポーネントの正常性を管理および監視する方法について説明します。ここで説明する内容は、次のとおりです。

コントロール プレーンのリソースの監視

ここでは、Cisco IOS プロセスとコントロール プレーン全体の観点から見たメモリおよび CPU の監視について説明します。

定期的な監視による問題の回避

プロセスを正しく動作させるには、プロセスのステータス/正常性を監視して通知する機能が必要です。プロセスに障害が発生すると、syslogエラーメッセージが表示され、プロセスの再起動またはルータのリブートが実行されます。プロセスがスタックしているかクラッシュしたことをモニターが検出すると、syslogエラーメッセージが表示されます。プロセスが再起動可能な場合は再起動され、それ以外の場合はルータが再起動されます。

システム リソースの監視によって、起こり得る問題を発生前に検出できるため、システムの停止を回避できます。また、正常なシステム負荷の基準が確立されます。ハードウェアやソフトウェアをアップグレードした時に、この情報を比較の根拠として使用し、アップグレードがリソースの使用率に影響を与えたかどうかを確認できます。

Cisco IOS プロセスのリソース

アクティブ プロセスの CPU 使用率統計情報を表示し、これらのプロセスで使用されているメモリの容量を確認するには、**show memory** コマンドと **show process cpu** コマンドを使用できます。これらのコマンドは、Cisco IOS プロセスのみのメモリと CPU の使用状況を示します。プラットフォーム全体のリソースに関する情報は含まれません。4 GB RAM を搭載し、1 つの Cisco IOS プロセスを実行しているシステムで **show memory** コマンドを実行すると、次のメモリ使用状況情報が表示されます。

```
Router# show memory
Tracekey : 1#33e0077971693714bd2b0bc347d77489
Address Bytes Prev Next Ref PrevF NextF what Alloc PC

Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 7F68ECD010 728952276 281540188 447412088 445683380 234766720
lsmpi_io 7F6852A1A8 6295128 6294304 824 824 412
Dynamic heap limit(MB) 200 Use(MB) 0



Processor memory

Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F68ECD010 0000000568 00000000 7F68ECD2A0 001 -------- -------- *Init* :400000+60E37C4
7F68ECD2A0 0000032776 7F68ECD010 7F68ED5300 001 -------- -------- Managed Chunk Q
:400000+60D12A8
7F68ED5300 0000000056 7F68ECD2A0 7F68ED5390 001 -------- -------- *Init* :400000+3B0C610
7F68ED5390 0000012808 7F68ED5300 7F68ED85F0 001 -------- -------- *Init* :400000+B8A5D64
Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F68ED85F0 0000032776 7F68ED5390 7F68EE0650 001 -------- -------- List Elements
:400000+60A4A9C
7F68EE0650 0000032776 7F68ED85F0 7F68EE86B0 001 -------- -------- List Headers
:400000+60A4AD8
7F68EE86B0 0000032776 7F68EE0650 7F68EF0710 001 -------- -------- IOSXE Process S
:400000+11924CC
7F68EF0710 0000032776 7F68EE86B0 7F68EF8770 001 -------- -------- IOSXE Queue Pro
:400000+1192510
7F68EF8770 0000065544 7F68EF0710 7F68F087D0 001 -------- -------- IOSXE Queue Bal
:400000+1192554
7F68F087D0 0000000328 7F68EF8770 7F68F08970 001 -------- -------- *Init* :400000+B89E1D8
7F68F08970 0000000328 7F68F087D0 7F68F08B10 001 -------- -------- *Init* :400000+B89E1D8
7F68F08B10 0000000328 7F68F08970 7F68F08CB0 001 -------- -------- *Init* :400000+B89E1D8
7F68F08CB0 0000000360 7F68F08B10 7F68F08E70 001 -------- -------- Process Events
:400000+60F9CD4
7F68F08E70 0000000056 7F68F08CB0 7F68F08F00 001 -------- -------- SDB String
:400000+605981C
7F68F08F00 0000000080 7F68F08E70 7F68F08FA8 001 -------- -------- Init :400000+60599E4
Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F68F08FA8 0000036872 7F68F08F00 7F68F12008 001 -------- -------- *Init* :400000+11891E8
7F68F12008 0000010008 7F68F08FA8 7F68F14778 001 -------- -------- Platform VM Pag
:400000+11AD244
7F68F14778 0000002008 7F68F12008 7F68F14FA8 001 -------- -------- *Init*
iosd_crb_ir1101_unix:7F8EB59000+5CC1C
7F68F14FA8 0000200712 7F68F14778 7F68F46008 001 -------- -------- Interrupt Stack
:400000+11891E8
7F68F46008 0000003008 7F68F14FA8 7F68F46C20 001 -------- -------- Watched Semapho
:400000+60FE448
7F68F46C20 0000000328 7F68F46008 7F68F46DC0 001 -------- -------- *Init* :400000+B89E1D8
7F68F46DC0 0000000096 7F68F46C20 7F68F46E78 001 -------- -------- Init :400000+60599E4
7F68F46E78 0000000216 7F68F46DC0 7F68F46FA8 001 -------- -------- *Init* :400000+60ED228
```

```
7F68F46FA8 0000036872 7F68F46E78 7F68F50008 001 -------- -------- *Init* :400000+11891E8
7F68F50008 0000000896 7F68F46FA8 7F68F503E0 001 -------- -------- Watched Message
:400000+60FE4A8
7F68F503E0 0000002008 7F68F50008 7F68F50C10 001 -------- -------- Watcher Message
:400000+60FE4D8
Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F68F50C10 0000000360 7F68F503E0 7F68F50DD0 001 -------- -------- Process Events
:400000+60F9CD4
7F68F50DD0 0000000184 7F68F50C10 7F68F50EE0 001 -------- -------- *Init* :400000+60ED918
7F68F50EE0 0000000112 7F68F50DD0 7F68F50FA8 001 -------- -------- *Init* :400000+60B57CC
7F68F50FA8 0000036872 7F68F50EE0 7F68F5A008 001 -------- -------- *Init* :400000+11891E8
7F68F5A008 0000002336 7F68F50FA8 7F68F5A980 001 -------- -------- Process Array
:400000+6102A4C
7F68F5A980 0000000184 7F68F5A008 7F68F5AA90 001 -------- -------- *Init* :400000+60ED918
7F68F5AA90 0000000184 7F68F5A980 7F68F5ABA0 001 -------- -------- *Init* :400000+60ED918
7F68F5ABA0 0000000184 7F68F5AA90 7F68F5ACB0 001 -------- -------- *Init* :400000+60ED918
7F68F5ACB0 0000000184 7F68F5ABA0 7F68F5ADC0 001 -------- -------- *Init* :400000+60ED918
7F68F5ADC0 0000000184 7F68F5ACB0 7F68F5AED0 001 -------- -------- *Init* :400000+60ED918
```

show process cpu コマンドは、Cisco IOS CPU の平均使用率を次のように表示します。

```
Router# show process cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 0 17 0 0.00% 0.00% 0.00% 0 Chunk Manager
2 552 1205 458 0.00% 0.00% 0.00% 0 Load Meter
3 0 1 0 0.00% 0.00% 0.00% 0 PKI Trustpool
4 0 1 0 0.00% 0.00% 0.00% 0 Retransmission o
5 0 1 0 0.00% 0.00% 0.00% 0 IPC ISSU Dispatc
6 36 13 2769 0.00% 0.00% 0.00% 0 RF Slave Main Th
7 0 1 0 0.00% 0.00% 0.00% 0 EDDRI_MAIN
8 0 1 0 0.00% 0.00% 0.00% 0 RO Notify Timers
9 4052 920 4404 0.23% 0.09% 0.06% 0 Check heaps
10 12 101 118 0.00% 0.00% 0.00% 0 Pool Manager
11 0 1 0 0.00% 0.00% 0.00% 0 DiscardQ Backgro
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
12 0 2 0 0.00% 0.00% 0.00% 0 Timers
13 0 163 0 0.00% 0.00% 0.00% 0 WATCH_AFS
14 0 2 0 0.00% 0.00% 0.00% 0 ATM AutoVC Perio
15 0 2 0 0.00% 0.00% 0.00% 0 ATM VC Auto Crea
16 76 3024 25 0.00% 0.00% 0.00% 0 IOSXE heartbeat
17 0 13 0 0.00% 0.00% 0.00% 0 DB Lock Manager
18 0 1 0 0.00% 0.00% 0.00% 0 DB Notification
19 0 1 0 0.00% 0.00% 0.00% 0 IPC Apps Task
20 0 1 0 0.00% 0.00% 0.00% 0 ifIndex Receive
21 36 1210 29 0.00% 0.00% 0.00% 0 IPC Event Notifi
22 72 5904 12 0.00% 0.00% 0.00% 0 IPC Mcast Pendin
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
23 0 1 0 0.00% 0.00% 0.00% 0 Platform appsess
24 0 101 0 0.00% 0.00% 0.00% 0 IPC Dynamic Cach
25 16 1210 13 0.00% 0.00% 0.00% 0 IPC Service NonC
26 0 1 0 0.00% 0.00% 0.00% 0 IPC Zone Manager
27 64 5904 10 0.00% 0.00% 0.00% 0 IPC Periodic Tim
28 76 5904 12 0.00% 0.00% 0.00% 0 IPC Deferred Por
29 0 1 0 0.00% 0.00% 0.00% 0 IPC Process leve
30 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat Manager
31 8 346 23 0.00% 0.00% 0.00% 0 IPC Check Queue
32 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat RX Cont
33 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat TX Cont
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
34 48 606 79 0.00% 0.00% 0.00% 0 IPC Keep Alive M
```

```
35 28 1210 23 0.00% 0.00% 0.00% 0 IPC Loadometer
36 0 1 0 0.00% 0.00% 0.00% 0 IPC Session Deta
37 0 1 0 0.00% 0.00% 0.00% 0 SENSOR-MGR event
38 4 606 6 0.00% 0.00% 0.00% 0 Compute SRP rate
39 0 1 0 0.00% 0.00% 0.00% 0 MEMLEAK PROCESS
40 0 1 0 0.00% 0.00% 0.00% 0 ARP Input
41 112 6331 17 0.00% 0.00% 0.00% 0 ARP Background
42 0 2 0 0.00% 0.00% 0.00% 0 ATM Idle Timer
43 0 1 0 0.00% 0.00% 0.00% 0 ATM ASYNC PROC
44 0 1 0 0.00% 0.00% 0.00% 0 CEF MIB API
--More--
...
show process cpu platform sorted

CPU utilization for five seconds: 11%, one minute: 12%, five minutes: 12%
Core 0: CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 3%
Core 1: CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 3%
Core 2: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 3: CPU utilization for five seconds: 42%, one minute: 42%, five minutes: 42%
Pid PPid 5Sec 1Min 5Min Status Size Name
------------------------------------------------------------------------------
18246 17700 34% 34% 34% S 272500 qfp-ucode-sparr
18297 16477 1% 1% 1% S 165768 fman_fp_image
9992 9121 1% 1% 1% S 743608 linux_iosd-imag
27122 26048 0% 0% 0% S 8460 nginx
26048 25864 0% 0% 0% S 19252 nginx
25928 1 0% 0% 0% S 2960 rotee
25864 1 0% 0% 0% S 3532 pman.sh
24212 2 0% 0% 0% S 0 kworker/u8:0
19648 8282 0% 0% 0% S 220 sleep
19635 10903 0% 0% 0% S 212 sleep
18121 17675 0% 0% 0% S 10968 ngiolite
17979 1 0% 0% 0% S 1660 rotee
17863 2 0% 0% 0% S 0 kworker/1:0
17859 1 0% 0% 0% S 2836 rotee
17737 17095 0% 0% 0% S 56828 iomd
17700 13380 0% 0% 0% S 3556 pman.sh
17675 12798 0% 0% 0% S 3524 pman.sh
17518 16854 0% 0% 0% S 15024 hman
17312 1 0% 0% 0% S 2828 rotee
17095 12798 0% 0% 0% S 3568 pman.sh
17085 1 0% 0% 0% S 2876 rotee
16942 2 0% 0% 0% S 0 kworker/0:1
16892 14768 0% 0% 0% S 108952 cpp_cp_svr
16854 13380 0% 0% 0% S 3568 pman.sh
16716 1 0% 0% 0% S 2996 rotee
16664 15963 0% 0% 0% S 51096 cpp_sp_svr
16477 13380 0% 0% 0% S 3540 pman.sh
16326 15536 0% 0% 0% S 39852 cpp_ha_top_leve
16270 1 0% 0% 0% S 2972 rotee
15963 13380 0% 0% 0% S 3528 pman.sh
15779 15163 0% 0% 0% S 55208 cpp_driver
15730 1 0% 0% 0% S 1640 rotee
15536 13380 0% 0% 0% S 3528 pman.sh
15412 1 0% 0% 0% S 1716 rotee
15274 14681 0% 0% 0% S 15004 hman
15163 13380 0% 0% 0% S 3624 pman.sh
15083 14361 0% 0% 0% S 26792 cman_fp
15057 1 0% 0% 0% S 1660 rotee
14891 1 0% 0% 0% S 2868 rotee
14768 13380 0% 0% 0% S 3568 pman.sh
14722 14127 0% 0% 0% S 27536 cmcc
14717 14108 0% 0% 0% S 15220 btman
14681 12798 0% 0% 0% S 3572 pman.sh
```

```
14627 1 0% 0% 0% S 2996 rotee
14361 13380 0% 0% 0% S 3596 pman.sh
14338 1 0% 0% 0% S 2984 rotee
14314 1 0% 0% 0% S 2824 rotee
14155 13577 0% 0% 0% S 15128 btman
14127 12798 0% 0% 0% S 3612 pman.sh
14108 13380 0% 0% 0% S 3572 pman.sh
13813 13380 0% 0% 0% S 252 inotifywait
--More--
```

コントロール プレーン全体のリソース

各コントロール プロセッサのコントロール プレーンのメモリおよびCPUの使用状況により、コントロールプレーン全体のリソースを管理できます。コントロールプレーンのメモリとCPUの使用状況の情報を表示するには、**show platform software status control-processor brief** コマンド（サマリー ビュー）または **show platform software status control-processor** コマンド（詳細ビュー）を使用できます。

すべてのコントロール プロセッサのステータスとして [Healthy] が表示されるのが正常です。他に表示されうるステータスの値は、[Warning] と [Critical] です。[Warning] は、ルータが動作中であるものの、動作レベルの確認が必要であることを示しています。[Critical] は、ルータで障害が発生する可能性が高いことを示しています。

[Warning] または [Critical] ステータスが表示されたら、次の対処方法に従ってください。

- 設定内の要素の数を減らすか、動的なサービスの容量を制限して、システムに対する静的および動的な負荷を減らします。
- ルータと隣接機器の数を減らしたり、ACLなどのルールの数を制限したり、VLANの数を減らしたりなどの対処を行います。

ここでは、**show platform software status control-processor** コマンドの出力のフィールドについて説明します。

Load Average

[Load Average] は、CPU リソースのプロセス キューまたはプロセス コンテンションを示します。たとえば、シングルコアプロセッサで瞬間的な負荷が 7 の場合は、7 つのプロセスが実行可能な状態になっていて、そのうちの 1 つが現在実行中という意味です。デュアルコアプロセッサで負荷が 7 となっている場合、7 つのプロセスが実行可能な状態になっていて、そのうちの 2 つが現在実行中であることを示します。

Memory Utilization

[Memory Utilization] は次のフィールドで示されます。

- Total：システムメモリの合計
- Used：使用済みメモリ
- Free：使用可能なメモリ
- Committed：プロセスに割り当てられている仮想メモリ

CPU Utilization

[CPU Utilization] は CPU が使用されている時間の割合を表すもので、次のフィールドで示されます。

- CPU：割り当て済みプロセッサ
- User：Linux カーネル以外のプロセス
- System：Linux カーネルのプロセス
- Nice：プライオリティの低いプロセス
- Idle：CPU が非アクティブだった時間の割合
- IRQ：割り込み
- SIRQ：システムの割り込み
- IOwait：CPU が入出力を待っていた時間の割合

例：show platform software status control-processor コマンド

次に **show platform software status control-processor** コマンドのいくつかの使用例を示します。

```
Router# show platform software status control-processorRP0: online, statistics updated
4 seconds ago
Load Average: healthy
1-Min: 0.29, status: healthy, under 5.00
5-Min: 0.51, status: healthy, under 5.00
15-Min: 0.54, status: healthy, under 5.00
Memory (kb): healthy
Total: 4038072
Used: 2872136 (71%), status: healthy
Free: 1165936 (29%)
Committed: 2347228 (58%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 1.00, System: 0.70, Nice: 0.00, Idle: 97.88
IRQ: 0.30, SIRQ: 0.10, IOwait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 0.70, System: 0.30, Nice: 0.00, Idle: 98.48
IRQ: 0.30, SIRQ: 0.20, IOwait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 0.20, System: 1.11, Nice: 0.00, Idle: 98.27
IRQ: 0.40, SIRQ: 0.00, IOwait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 8.23, System: 24.37, Nice: 0.00, Idle: 58.00
IRQ: 9.26, SIRQ: 0.11, IOwait: 0.00
```

```
Router# show platform software status control-processor briefLoad Average
Slot Status 1-Min 5-Min 15-Min
RP0 Healthy 0.28 0.46 0.52

Memory (kB)
Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
```

```
RP0 Healthy 4038072 2872672 (71%) 1165400 (29%) 2349820 (58%)

CPU Utilization
Slot CPU User System Nice Idle IRQ SIRQ IOwait
RP0 0 0.70 0.20 0.00 98.58 0.30 0.20 0.00
1 1.10 0.90 0.00 97.59 0.30 0.10 0.00
2 0.40 1.31 0.00 97.87 0.40 0.00 0.00
3 8.00 26.55 0.00 56.33 8.99 0.11 0.00
```

アラームを使用したハードウェアの監視

ルータの設計とハードウェアの監視

問題が検出されるとルータからアラーム通知が送信されます。これにより、ネットワークをリモートで監視できます。**show** コマンドを使用してデバイスを定期的にポーリングする必要はありませんが、必要に応じてオンサイト モニタリングを実行できます。

ブートフラッシュ ディスクの監視

ブートフラッシュ ディスクには、2 つのコア ダンプを保存できる十分な空き領域が必要です。この条件が監視されて、ブートフラッシュ ディスクが 2 つのコア ダンプを保存するには小さすぎる場合には、次の例に示すような syslog アラームが生成されます。

```
Oct  6 14:10:56.292: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota
exceeded
[free space is 1429020 kB] - Please clean up files on bootflash.
```

ハードウェア アラームの監視方法

コンソールまたは **syslog** でのアラーム メッセージの確認

ネットワーク管理者は、システム コンソールまたはシステム メッセージ ログ（syslog）に送信されるアラーム メッセージを確認することにより、アラーム メッセージを監視できます。

logging alarm コマンドの有効化

アラーム メッセージをコンソールや syslog などのロギング デバイスに送信するには、**logging alarm** コマンドを有効にする必要があります。このコマンドはデフォルトでは無効になっています。

ログに記録されるアラームの重大度レベルを指定できます。指定したしきい値以上のアラームが発生するたびに、アラーム メッセージが生成されます。たとえば、次のコマンドではクリティカル アラーム メッセージだけがロギング デバイスに送信されます。

```
Router(config)# logging alarm critical
```

アラームの重大度を指定しない場合、すべての重大度のレベルのアラーム メッセージがロギング デバイスに送信されます。

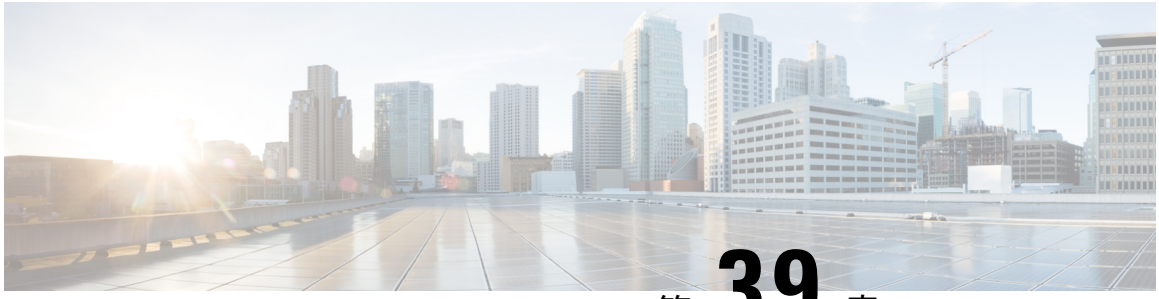
SNMP 経由でアラームが報告された場合のネットワーク管理システムによるネットワーク管理者への警告

アプリケーション層プロトコルである SNMP は、ネットワーク内のデバイスを監視および管理するための、標準化されたフレームワークと共通の言語を提供します。

SNMP は、サービスに影響を及ぼす可能性のある障害、アラーム、状況を通知します。これにより、ネットワーク管理者は、ログの確認、デバイスのポーリング、ログ レポートの確認を行う代わりに、ネットワーク管理システム（NMS）経由でルータ情報を入手できます。

SNMP を使用してアラーム通知を取得するには、次の MIB を使用します。

- ENTITY-MIB、RFC4133（CISCO-ENTITY-ALARM-MIB、ENTITY-STATE-MIB および CISCO-ENTITY-SENSOR-MIB の稼働に必須）
- CISCO-ENTITY-ALARM-MIB
- ENTITY-STATE-MIB
- CISCO-ENTITY-SENSOR-MIB（トランシーバ環境アラーム情報用。この情報は CISCO-ENTITY-ALARM-MIB では提供されません）



第 39 章

トラブルシューティング

ここでは、トラブルシューティングのシナリオについて説明します。

ソフトウェアに関する不具合のトラブルシューティングを行う前に、コンソールポートを使用して PC をルータに接続してください接続した PC を使用してルータのステータス メッセージを表示し、コマンドを入力して問題のトラブルシューティングを実行できます。

また、Telnet を使用してリモートから各インターフェイスにアクセスすることもできます。Telnet オプションを使用する方法では、インターフェイスが稼働していることが前提になります。

診断モードの概要

ルータは、次のような場合に、診断モードを開始するか、または診断モードにアクセスします。

- IOS プロセスの障害が原因の場合があります。あるいは、IOS プロセスで障害が発生したときにシステムがリセットすることがあります。
- **transport-map** コマンドを使ってユーザ設定のアクセス ポリシーが設定されると、ユーザは診断モードに誘導されます。
- ルータにアクセスしている間に送信ブレーク信号（**Ctrl-C** または **Ctrl-Shift-6**）が入力されると、ブレーク信号を受信したルータが診断モードを開始するように設定されている場合があります。

診断モードでは、ユーザ EXEC モードで使用可能なコマンドのサブセットを使用できます。このコマンドは、次のような場合に使用できます。

- IOS ステートなど、ルータ上のさまざまなステートを検査する。
- コンフィギュレーションの置き換えまたはロールバック。
- IOS またはその他のプロセスの再開方法を提供する。
- ルータ全体、モジュール、またはその他のハードウェア コンポーネントなどのハードウェアをリブートします。
- FTP、TFTP、および SCP などのリモート アクセス方式を使用した、ルータに対するファイル転送、またはルータからのファイル転送。

以前のルータでは、障害時に ROMMON などの制限付きアクセス方式を使用して Cisco IOS 問題を診断し、トラブルシューティングを行っていましたが、診断モードを使用すると、より広範なユーザインターフェイスを使用してトラブルシューティングできるようになります。診断モードコマンドは、Cisco IOS プロセスが正常に動作していないときでも動作可能です。また、ルータが正常に動作しているときに、ルータの特権 EXEC モードでもこれらのコマンドを使用できます。

代理店に連絡する前に

問題の原因が見つからない場合は、製品を購入した代理店に連絡し、指示を求めてください。代理店に連絡する前に、次の情報を用意してください。

- シャーシのタイプとシリアル番号
- メンテナンス契約書または保証情報
- ソフトウェアのタイプとバージョン番号
- ハードウェアを受け取った日付
- 問題点の要約
- 問題箇所を特定するために行った手順の概要

show interfaces トラブルシューティング コマンド

すべての物理ポートとルータ上の論理インターフェイスの状態を表示するには、**show interfaces** コマンドを使用します。#unique_500 unique_500_Connect_42_tab_1055127 はコマンド出力のメッセージについて説明しています。

IR1101 は次のインターフェイスをサポートしています。

GigabitEthernet 0/0/0

Cellular 0/1/0

FastEthernet 0/0/1 ～ 0/0/4

Async 0/2/0

ソフトウェア アップグレード方法

Cisco IR1101 ルータのソフトウェアは、次の方法でアップグレードできます。

- 既存の Cisco IOS ソフトウェア イメージの使用中に、LAN または WAN 経由で新しいソフトウェア イメージをフラッシュ メモリにコピーします。
- ブート イメージ（ROM モニタ）の実行中に、LAN 経由で新しいソフトウェア イメージをフラッシュ メモリにコピーします。
- ROM モニタ モードで新しいソフトウェア イメージをコンソール ポート経由でコピーします。
- ROM モニタ モードで、TFTP サーバにロードされたソフトウェア イメージからルータを起動します。この方法を使用するには、TFTP サーバがルータと同じ LAN 上にある必要があります。

コンフィギュレーション レジスタの変更

コンフィギュレーション レジスタを変更する手順は、次のとおりです。

ステップ 1 PC をルータのコンソール ポートに接続します。

ステップ 2 特権 EXEC プロンプト（*router_name* #）で **show version** コマンドを入力すると、既存のコンフィギュレーション レジスタ値が表示されます（次の出力例の末尾の太字部分を参照）。

例：

```
Router# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.10.1,
RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 09-Nov-18 18:08 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON
```

```
Router uptime is 14 hours, 36 minutes
Uptime for this control processor is 14 hours, 37 minutes
System returned to ROM by reload
System restarted at 08:47:04 GMT Mon Nov 12 2018
System image file is "bootflash:ir1101-universalk9.16.10.01.SPA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                      Technology-package
Current                       Type                         Next reboot
------------------------------------------------------------------------------
network-essentials     Smart License                  network-essentials


Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 711861K/6147K bytes of memory.
Processor board ID FCW222700MY
3 Virtual Ethernet interfaces
4 FastEthernet interfaces
1 Gigabit Ethernet interface
1 Serial interface
1 terminal line
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4038072K bytes of physical memory.
3110864K bytes of Bootflash at bootflash:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x1821


Router#
```

ステップ 3 コンフィギュレーション レジスタの設定値を記録します。

ステップ 4 ブレークの設定（コンフィギュレーション レジスタのビット 8 の値で示されます）を有効にするには、特権 EXEC モードから **config-register 0x01** コマンドを入力します。

- ブレーク有効：ビット 8 が 0 に設定されています。
- ブレーク無効（デフォルトの設定）：ビット 8 が 1 に設定されています。

自動ブートのコンフィギュレーション レジスタの設定

（注） コンフィギュレーション レジスタの変更は、高度なトラブルシューティングのみを対象としており、シスコのサポートからガイダンスがある場合にのみ行うようにしてください。

コンフィギュレーション レジスタを使用して、ルータの動作を変更できます。これには、ルータの起動方法の制御が含まれます。次のいずれかのコマンドを使用して、ROM で起動するようにコンフィギュレーション レジスタを 0x0 に設定します。

- Cisco IOS コンフィギュレーション モードで **config-reg** 0x0 コマンドを使用します。
- ROMMON プロンプトで **confreg** 0x0 コマンドを使用します。

（注） コンフィギュレーション レジスタを 0x2102 に設定すると、Cisco IOS XE ソフトウェアを自動ブートするようにルータが設定されます。

ルータのリセット

ルータをリセットする手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	ブレークが無効になっている場合は、ルータの電源をオフ（O）にしてから 5 秒後に再びオン（|）にします。その後 60 秒以内に、**Break**キーを押します。端末に ROM モニタ プロンプトが表示されます。	（注） 一部の端末では、キーボードに *Break* というラベルの付いたキーがあります。使用するキーボードに Break キーがない場合は、端末に付属のマニュアルを参照して、ブレーク信号の送信方法を確認してください。
ステップ 2	break を押します。端末に次のプロンプトが表示されます。 **例**： `rommon 2>`	
ステップ 3	**confreg 0x142** を入力して、コンフィギュレーション レジスタをリセットします。 **例**： `rommon 2> confreg 0x142`	

	コマンドまたはアクション	目的

ステップ 4	**reset** コマンドを入力して、ルータを初期化します。
	例：
	`rommon 2> reset`
	例：
	`--- System Configuration Dialog ---`
		ルータの電源が一度オフになってからオンになり、コンフィギュレーション レジスタが 0x142 に設定されます。ルータはブート ROM システム イメージを使用します。その状況はシステム コンフィギュレーション ダイアログで示されます。

ステップ 5	次のメッセージが表示されるまで、プロンプトに **no** で応答します。 例： `Press RETURN to get started!`	
ステップ 6	**Return** を押します。次のプロンプトが表示されます。 例： `Router>`	

ステップ 7	enable コマンドを入力して、イネーブル モードを開始します。コンフィギュレーション変更は、イネーブル モードでだけ行うことができます。
	例：
	`Router> enable`
	例：
	`Router#`
		プロンプトが特権 EXEC プロンプトに変わります。

ステップ 8	**show startup-config** コマンドを入力すると、コンフィギュレーション ファイルに保存されているイネーブル パスワードが表示されます。 例： `Router# show startup-config`	

次のタスク

イネーブル パスワードを回復する場合には、「変更を保存」のセクションに示す手順は実行しないでください。代わりに、「コンフィギュレーション レジスタ値」のセクションに記載されている手順を実行して、パスワード回復作業を行ってください。

イネーブル シークレット パスワードを回復する場合、**show startup-config** コマンド出力には表示されません。「パスワードのリセットと変更の保存」セクションに記載されている手順を実行して、パスワード回復作業を完了させてください。

失われたパスワードの復旧

失われたイネーブルパスワードまたはイネーブルシークレットを回復するには、次の作業を行います。

1. コンフィギュレーション レジスタの変更
2. ルータのリセット
3. パスワードをリセットし、変更を保存します（イネーブル シークレット パスワードを忘れた場合のみ）。
4. コンフィギュレーション レジスタ値をリセットします。

   5.write erase を実行した場合、またはリセット ボタンを使用した場合は、ライセンスを追加する必要があります。

```
IR1101#config term
IR1101#license smart reservation
```

（注） パスワードを回復できるのは、コンソール ポートを使用してルータに接続している場合だけです。Telnet セッション経由では実行できません。

ヒント イネーブル シークレット パスワードの変更方法のさらに詳しい情報については、Cisco.com の「Hot Tips」を参照してください。

パスワードのリセットと変更の保存

パスワードをリセットして、変更を保存するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** コマンドを入力して、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。 例： `Router# configure terminal`	

	コマンドまたはアクション	目的
ステップ 2	**enable secret** コマンドを入力して、ルータのイネーブル シークレット パスワードをリセットします。 例： `Router(config)# enable secret password`	
ステップ 3	**exit** を入力して、グローバル コンフィギュレーション モードを終了します。 例： `Router(config)# exit`	
ステップ 4	設定変更を保存します。 例： `Router# copy running-config startup-config`	

パスワードリカバリの無効化

No Service Password-Recovery は、Cisco IOS プラットフォームに依存しない機能/CLI で、Cisco IOS-XE デバイスで使用できます。No Service Password-Recovery セキュリティ機能を有効にすると、コンソールアクセス権を持つすべてのユーザが、ブートアップ時にブレークシーケンス（Control+C）を使用して rommon を開始できなくなります。

（注） この機能を有効にする前に、フラッシュ内に有効な Cisco IOS イメージが存在することを確認します。これを行わないと、ルータがブートループに入ります。システムに **no service password recovery** がない場合は、ハード電源リセットボタンが無効になります。

次のイベントにより、ルータは標準の IOS-XE 動作として rommon モードになります。

- config-reg 設定は手動起動
- ユーザが工場出荷時のデフォルトオプションにリセットすることを選択

詳細情報と設定手順については、次を参照してください。https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-sy/sec-usr-cfg-15-sy-book/sec-no-svc-pw-recvry.html

サービス パスワード リカバリ アップデートでのコンフィグレジスタの変更の問題

サービスパスワードリカバリが無効になっている場合、コンフィグレジスタを変更できず、0x01 でスタックされます。この問題は、IR1101 ルータで見つかりました。詳細については、テクニカルノート『Understand Configuration Register Usage on all Routers』を参照してください。

コンフィギュレーション レジスタ値のリセット

パスワードの回復または再設定を行った後にコンフィギュレーション レジスタをリセットするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** コマンドを入力して、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。 **例**： `Router# configure terminal`	
ステップ 2	**configure register** コマンドと、記録しておいた元のコンフィギュレーション レジスタ値を入力します。 **例**： `Router(config)# config-reg value`	
ステップ 3	**exit** を入力して、コンフィギュレーション モードを終了します。 **例**： `Router(config)# exit`	**（注）** 忘れたイネーブル パスワードを回復する前に使用していたコンフィギュレーションに戻るには、コンフィギュレーションの変更を保存せずに、ルータを再起動してください。
ステップ 4	ルータを再起動し、回復したパスワードを入力します。	

コンソール ポートのトランスポート マップの設定

このタスクでは、ルータ上のコンソール ポート インターフェイスにトランスポート マップを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Router> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例**：	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。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 3	**transport-map type console** *transport-map-name* 例： `Router(config)# transport-map type console consolehandler`	コンソール接続を処理するためのトランスポート マップを作成して名前を付け、トランスポートマップ コンフィギュレーション モードを開始します。
ステップ 4	**connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]] 例： `Router(config-tmap)# connection wait none`	コンソール接続を処理する方法を、このトランスポート マップで指定します。 • **allow interruptible**：コンソール接続はCisco IOS VTY回線が使用可能になるのを待機します。また、ユーザはCisco IOS VTY 回線が使用可能になるのを待機しているコンソール接続に割り込むことにより、診断モードを開始できます。これがデフォルト設定です。 （注） **Ctrl+C** キーまたは **Ctrl+Shift+6** キーを入力すると、ユーザは待機中の接続に割り込むことができます。 • **none**：コンソール接続はただちに診断モードを開始します。

ステップ 5	（任意） **banner** [**diagnostic** | **wait**] *banner-message*
	例：
	`Router(config-tmap)# banner diagnostic X`
	`Enter TEXT message. End with the character 'X'.`
	`--Welcome to Diagnostic Mode--`
	`X`
	`Router(config-tmap)#`
		（オプション）診断モードを開始しているユーザ、またはコンソール トランスポート マップ設定のために Cisco IOS VTY 回線を待機しているユーザに表示されるバナー メッセージを作成します。
		• **diagnostic**：コンソール トランスポート マップ設定のために診断モードに誘導されたユーザに表示されるバナー メッセージを作成します。
		（注） **Ctrl+C** キーまたは **Ctrl+Shift+6** キーを入力すると、ユーザは待機中の接続に割り込むことができます。
		• **wait**：Cisco IOS VTY が使用可能になるのを待機しているユーザに表示されるバナー メッセージを作成します。
		• *banner-message*：同じデリミタで開始および終了するバナー メッセージ。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-tmap)# exit`	トランスポートマップ コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを再開します。
ステップ 7	**transport type console** *console-line-number* **input** *transport-map-name* 例： `Router(config)# transport type console 0 input consolehandler`	トランスポートマップで定義された設定をコンソール インターフェイスに適用します。 このコマンドの *transport-map-name* は、**transport-map type console** コマンドで定義された *transport-map-name* と一致する必要があります。

例

次に、コンソール ポートのアクセス ポリシーを設定し、コンソール ポート 0 に接続するためにトランスポート マップを作成する例を示します。

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

コンソール ポート、SSH、および Telnet の処理設定の表示

コンソール ポート、SSH、および Telnet の処理設定を表示するには、次のコマンドを使用します。

- **show transport-map**
- **show platform software configuration access policy**

トランスポート マップ設定を表示するには、**show transport-map** コマンドを使用します。

show transport-map [**all** | **name** *transport-map-name* | **type** [**console**]]

このコマンドは、ユーザ EXEC モードまたは特権 EXEC モードで使用可能です。

例

次に、ルータで設定されたトランスポートマップの例（コンソールポート（`consolehandler`）を示します。

```
Router# show transport-map all
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode


Router# show transport-map type console
Transport Map:
Name: consolehandler


REVIEW DRAFT - CISCO CONFIDENTIAL

Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode


Router# show transport-map type persistent ssh
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

着信コンソール ポート、SSH、および Telnet 接続の処理に関する現行設定を表示するには、**show platform software configuration access policy** コマンドを使用します。このコマンドの出力には、各接続タイプ（Telnet、SSH、およびコンソール）の現在の待機ポリシーと、現在設定されているバナーの情報が示されます。

show transport-map コマンドとは異なり、**show platform software configuration access policy** コマンドは診断モードで使用可能です。このため、トランスポートマップ設定情報が必要であるにもかかわらず Cisco IOS CLI にアクセスできない場合に、このコマンドを入力できます。

例

次に、**show platform software configuration access policy** コマンドの例を示します。

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt Shell banner:
Welcome to Diagnostic Mode
```

```
Wait banner :
Waiting for IOS Process

Method : ssh Rule : wait Shell banner: Wait banner :

Method : console
Rule : wait with interrupt Shell banner:
Wait banner :
```

factory reset コマンドの使用

コマンド **factory reset** は、追加されたルータまたはスイッチ上の特定の顧客のデータをすべて削除するために使用されます。設定、ログ ファイル、ブート変数、およびコア ファイル形式のデータが対象です。

コマンド **factory-reset all** は、bootflash、nvram、rommon 変数、ライセンス、およびログを消去します。

```
Router#factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
 *Enter*

*May 12 09:55:45.831: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory
Reset.

***Return to ROMMON Prompt
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。