Cisco 4000 シリーズ ISR ソフトウェア コンフィギュレーション ガイド、Cisco IOS XE 17

最終更新：2022 年 4 月 22 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/

Text Part Number: OL-29328-03

目 次

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.

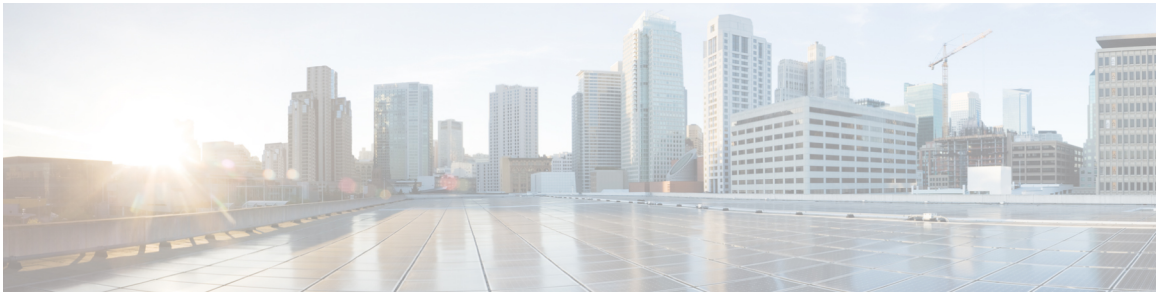
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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



はじめに

この項では、このマニュアルの目的について説明し、関連する製品とサービスの詳細情報へのリンクを示します。

はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

対象読者および適用範囲

このドキュメントは、Cisco Enterprise ルータの設定担当者を対象としています。このドキュメントの対象者は、主に次のとおりです。

- ネットワーキングに関する技術的な背景知識と経験を持つお客様。
- ルータベースのインターネットワーキングに関する基本的な知識に精通しているが、Cisco IOS ソフトウェアについては経験の浅いシステム管理者。
- インターネットワーキング装置のインストールと設定を担当しているシステム管理者、および Cisco IOS ソフトウェアに精通しているシステム管理者。

機能の互換性

コンフィギュレーション ガイドで説明されているデバイスで使用可能な機能などの Cisco IOS XE ソフトウェアの詳細については、それぞれのルータのドキュメントセットを参照してください。

特定の機能のサポートを確認するには、Cisco Feature Navigator ツールを使用します。これは、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。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または **Ctrl**	^ および **Ctrl** シンボルは、Ctrl キーを表します。たとえば、^**D** または **Ctrl**+**D** というキーの組み合わせは、**Ctrl** キーを押しながら **D** キーを押すことを意味します。キーは大文字で表記されていますが、大文字と小文字の区別はありません。
string	ストリングは、イタリックで示される引用符を付けない一組の文字です。たとえば、SNMP コミュニティ ストリングとして public を設定する場合、ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

コマンドシンタックスの説明には、次の表記法を使用しています。

表記法	説明
ボールド	ユーザが入力するコマンドおよびキーワードを示します。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
|	縦棒で区切られている場合、複数の任意または必須のキーワードまたは引数から、1 つを選択します。

表記法	説明
[x | y]	角カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、任意の選択肢です。
{x | y}	波カッコで囲まれ、縦棒で区切られたキーワードまたは引数は、必須の選択肢です。

省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。たとえば、次の表を参照してください。

表記法	説明
[x {y | z}]	角カッコ内の波カッコおよび縦棒は、任意の要素内の必須の選択肢です。

例では、次の表記法を使用しています。

表記法	説明
`screen`	画面に表示される情報の例は、Courier フォントで表します。
`bold screen`	ユーザの入力が必要なテキストの例は、太字の Courier フォントで表します。
< >	山カッコで囲まれたテキストは、パスワードなど、画面に出力されないテキストを表します。
!	行の先頭にある感嘆符（!）は、コメント行を表します。また、いくつかのプロセスでも、Cisco IOS XE ソフトウェアにより感嘆符が表示されることがあります。
[ ]	角カッコは、システム プロンプトに対するデフォルトの応答です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

シスコバグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

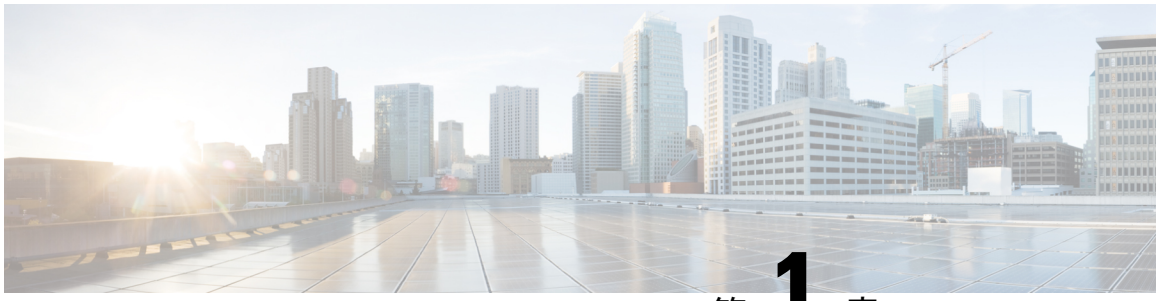
マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

トラブルシューティング

トラブルシューティングの最新の詳細情報については、
https://www.cisco.com/c/ja_jp/support/index.html にある Cisco TAC Web サイトを参照してください。

製品カテゴリに移動し、リストから製品を選択するか、製品の名前を入力します。発生している問題に関する情報を見つけるには、**トラブルシュートおよびアラート**を参照してください。



第 1 章

概要

このマニュアルでは、Cisco 4000 シリーズ サービス統合型ルータ（ISR）に固有のソフトウェア機能の概要を示します。

次の表に、Cisco 4000 シリーズ ISR に属するルータ モデルを示します。

表 *1 : Cisco 4000* シリーズ ルータのモデル

Cisco 4400 シリーズ ISR	Cisco 4300 シリーズ ISR	Cisco 4200 シリーズ ISR
• Cisco 4431 ISR • Cisco 4451 ISR • Cisco 4461 ISR	• Cisco 4321 ISR • Cisco 4331 ISR • Cisco 4351 ISR	Cisco 4221 ISR

（注） 特に明記されない限り、このマニュアルの情報は、Cisco 4400 シリーズ ルータ、Cisco 4300 シリーズ ルータ、および Cisco 4200 シリーズ ルータに適用されます。

この章で説明する内容は、次のとおりです。

はじめに

Cisco 4000 シリーズ ISR は、LAN および WAN 接続機能を搭載したモジュール型ルータであり、Cisco 拡張サービスモジュール（SM-X）およびネットワーク インターフェイス モジュール（NIM）などのインターフェイスモジュールを使用してこれを設定できます。NIM スロットでは、ホステッド アプリケーション用のリムーバブル ストレージもまたサポートされています。

エンタープライズ アプリケーションとサービス プロバイダー アプリケーション向けに次の機能が備わっています。

- エンタープライズ アプリケーション
  - ハイエンド ブランチ ゲートウェイ
  - 地域サイトの集約
  - キーサーバーまたは PfR プライマリ コントローラ
  - デバイス統合またはRack in a Box
- サービス プロバイダー アプリケーション
  - 顧客宅内機器（CPE）でのハイエンド マネージド サービス
  - サービス統合プラットフォーム
  - ルート リフレクタまたはシャドウ ルータ
  - 柔軟性のあるカスタマー エッジ ルータ

ルータは Cisco IOS XE ソフトウェアを実行し、多数の個別プロセスでソフトウェア コンポーネントを使用します。このモジュール型アーキテクチャにより、標準の Cisco IOS ソフトウェアと比べてネットワーク復元力が向上します。

プロセス

ルータの状態を確認し、トラブルシューティングを行う際に役立つバックグラウンドプロセスの一覧を次の表に示します。ただし、ほとんどのルータ動作を理解するうえで、これらのプロセスを理解しておく必要はありません。

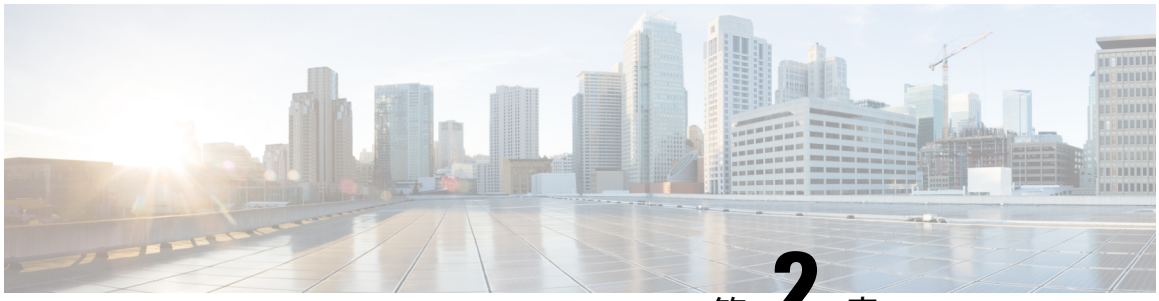
表 *2:* 個別のプロセス

プロセス	目的	影響される FRU	サブパッケージマッピング
Chassis Manager	ハイ アベイラビリティ（HA）ステート、環境モニタリング、および FRU ステート制御の管理など、シャーシ管理機能を制御します。	RP SIP ESP	RPControl SIPBase ESPBase

プロセス	目的	影響される FRU	サブパッケージマッピング
Host Manager	IOS プロセスと、基盤となるプラットフォームカーネルおよびオペレーティングシステムの多くの情報収集機能との間のインターフェイスを提供します。	RP SIP ESP	RPControl SIPBase ESPBase
ロガー	各 FRU で実行されるプロセスに対して、IOS ロギングサービスを提供します。	RP SIP ESP	RPControl SIPBase ESPBase
IOS	ルータのすべての転送およびルーティング機能を実装します。	RP	RPIOS
Forwarding Manager	ESP への設定の詳細のダウンロード、および IOS プロセスへのフォワーディングプレーン情報（統計情報など）の伝達を管理します。	RP ESP	RPControl ESPBase
Pluggable Services	認証などのプラットフォーム ポリシー アプリケーションと IOS プロセスを統合します。	RP	RPControl
Shell Manager	統合パッケージの非 IOS コンポーネントに関連するユーザ インターフェイス（UI）機能を提供します。これらの機能は、IOS プロセスに障害が発生したときに診断モードでも使用できます。	RP	RPControl

プロセス	目的	影響される FRU	サブパッケージマッピング
IO モジュール プロセス	NIM または拡張サービス モジュール（SM-X）との間で、設定およびその他の制御メッセージを交換します。	IO モジュール	SIPSPA
CPP ドライバプロセス	ESP での CPP ハードウェア フォワーディングエンジンを管理します。	ESP	ESPBase
CPP HA プロセス	CPP ハードウェア フォワーディングエンジンの HA ステートを管理します。	ESP	ESPBase
CPP SP プロセス	Forwarding Manager プロセスの ESP インスタンスで CPP 側機能への高遅延タスクを実行します。	ESP	ESPBase

ルータの機能およびモデルの詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』を参照してください。



第 2 章

Cisco 4000 シリーズ ISR での初期ルータ設定の指定

この章では、Cisco 4000 シリーズ サービス統合型ルータ（ISR）での初期設定の実行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。

Cisco 4000 シリーズ ISR での初期設定の実行

setup コマンド機能または Cisco IOS コマンド ライン インターフェイス（CLI）を使用して、Cisco 4000 シリーズ ISR で初期設定を実行できます。

シスコの setup コマンド機能の使用

setup コマンド機能では、ルータおよびネットワークの情報を入力するように要求されます。指示に従って、LANインターフェイスやWANインターフェイスなどの初期設定を行ってください。setup コマンド機能の一般的な詳細については、次のマニュアルを参照してください。

『*Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4』の「Part 2: Cisco IOS User Interfaces: Using AutoInstall and Setup」
（http://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-xe-3s/products-installation-and-configuration-guides-list.html）

ここでは、ルータのホスト名とパスワードを設定し、管理ネットワークと通信するためのインターフェイスを設定する方法について説明します。

（注） 表示されるメッセージは、ルータ モデル、装着されているインターフェイス モジュール、およびソフトウェア イメージによって変わります。次の例とユーザー入力（**bold**の部分）は、あくまでも例です。

（注） setup コマンド機能を間違って使用した場合は、setup コマンド機能を終了し、再度実行してください。**Ctrl-C** を押し、特権 EXEC モード（Router#）に **setup** コマンドを入力します。

setup コマンド機能を使用してルータを初期設定する手順は、次のとおりです。

手順の概要

1. Cisco IOS-XE CLI から、特権 EXEC モードで **setup** コマンドを次のように入力します。
2. setup コマンド機能を引き続き使用する場合は、 **yes** を入力します。
3. **yes** と入力して基本管理の設定に入ります。
4. ルータのホスト名を入力します（例では「myrouter」）。
5. イネーブル シークレット パスワードを入力します。このパスワードは暗号化される（安全性が高い）ので、設定を表示してもパスワードは表示されません。
6. イネーブル シークレット パスワードとは異なるイネーブル パスワードを入力します。このパスワードは暗号化されない（安全性が低い）ので、設定を表示するとパスワードも表示されます。
7. 仮想端末パスワードを入力します。このパスワードによって、コンソール ポート以外のポートからの不正アクセスを防止できます。
8. 次のプロンプトに対して、使用するネットワークに適した応答を入力します。
9. 次のプロンプトに対して、使用するネットワークに適した応答を入力します。
10. 次のプロンプトに応答します。[2] を選択して初期設定を保存します。

手順の詳細

ステップ 1 Cisco IOS-XE CLI から、特権 EXEC モードで **setup** コマンドを次のように入力します。

例：

```
Router> enable

Password: <password>

Router# setup

        --- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:
```

現在、setup 設定ユーティリティの実行中です。

setup コマンド機能のプロンプトは、ルータのモデル、組み込まれているインターフェイスモジュール、さらにソフトウェアイメージによって異なります。次の手順とユーザー入力（太字の部分）は、あくまでも例です。

（注） Cisco IOS XE ルータに起動した際に何も設定がない場合には、この setup コマンド機能が自動的に入力されます。

（注） setup コマンド機能を間違って使用した場合は、setup コマンド機能を終了し、再度実行してください。Ctrl+C を押し、特権 EXEC モードのプロンプト（Router#）に setup コマンドを入力します。setup コマンド機能の使用方法の詳細については、次の URL でアクセスできる『*Cisco IOS Configuration Fundamentals Command Reference*』の「*The Setup Command*」の章を参照してください：https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref.html

ステップ 2 setup コマンド機能を引き続き使用する場合は、 **yes** を入力します。

例：

```
Continue with configuration dialog? [yes/no]:
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 '[]'.
```

ステップ 3 **yes** と入力して基本管理の設定に入ります。

例：

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

ステップ 4 ルータのホスト名を入力します（例では「myrouter」）。

例：

```
Configuring global parameters:
Enter host name [Router]: myrouter
```

ステップ 5 イネーブル シークレット パスワードを入力します。このパスワードは暗号化される（安全性が高い）ので、設定を表示してもパスワードは表示されません。

例：

```
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: cisco
```

ステップ 6 イネーブル シークレット パスワードとは異なるイネーブル パスワードを入力します。このパスワードは暗号化されない（安全性が低い）ので、設定を表示するとパスワードも表示されます。

例：

```
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: cisco123
```

ステップ 7 仮想端末パスワードを入力します。このパスワードによって、コンソール ポート以外のポートからの不正アクセスを防止できます。

例：

```
The virtual terminal password is used to protect
```

```
access to the router over a network interface.
Enter virtual terminal password: cisco
```

ステップ 8 次のプロンプトに対して、使用するネットワークに適した応答を入力します。

例：

```
Configure SNMP Network Management? [no]: yes
    Community string [public]:
```

使用可能なインターフェイスの要約が表示されます。

（注） インターフェイスの概要には、インターフェイスのナンバリングが含まれます。これはルータ モデルおよびインストールされているモジュールとインターフェイス カードによって変わります。

例：

```
Current interface summary
Interface      IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0     unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1/0  10.10.10.12     YES DHCP   up                    up
GigabitEthernet0/2/0    unassigned      YES NVRAM  administratively down down
SSLVPN-VIF0               unassigned      NO  unset  up
Any interface listed with OK? value "NO" does not have a valid configuration
```

ステップ 9 次のプロンプトに対して、使用するネットワークに適した応答を入力します。

例：

```
Configuring interface GigabitEthernet0/1/0
:
  Configure IP on this interface? [yes]: yes
    IP address for this interface [10.10.10.12
]:
    Subnet mask for this interface [255.0.0.0] : 255.255.255.0
    Class A network is 10.0.0.0, 24 subnet bits; mask is /24
```

次のコンフィギュレーション コマンド スクリプトが作成されました。

例：

```
hostname myrouter
enable secret 5 $1$t/Dj$yAeGKviLLZNOBX0b9eifO0 enable password cisco123 line vty 0 4 password
cisco snmp-server community public !
no ip routing
!
interface GigabitEthernet0/0/0
shutdown
no ip address
!
interface GigabitEthernet0/1/0
no shutdown
ip address 10.10.10.12 255.255.255.0
!
interface GigabitEthernet0/2/0
shutdown
no ip address
!
end
```

ステップ 10 次のプロンプトに応答します。[2] を選択して初期設定を保存します。

例：

```
[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...
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started! RETURN
```

ユーザ プロンプトが表示されます。

例：

```
myrouter>
```

設定の完了

シスコ setup を使用するとき、および設備に必要なすべての情報を指定し終わると、最終的な設定が表示されます。ルータ設定を完了するには、次の手順を実行します。

手順の概要

1. 設定の保存を求めるプロンプトが表示されたら、設定の保存を選択します。
2. 画面にメッセージが表示されなくなったら、**Return** を押して Router> プロンプトを表示します。
3. 既存の設定の変更または別の設定の作成を選択します。Router> プロンプトは、コマンドライン インターフェイス（CLI）を実行中で、ルータの初期設定を完了したことを示します。それでも、これは設定の完了ではありません。この時点で 2 つの選択肢があります。

手順の詳細

ステップ 1 設定の保存を求めるプロンプトが表示されたら、設定の保存を選択します。

- 「no」と答えると、入力した設定情報は保存されません。また、ルータイネーブルプロンプト（Router#）に戻ります。setup と入力すると、System Configuration Dialog に戻ります。
- 「yes」と答えると、設定は保存され、ユーザー EXEC プロンプト（Router>）に戻ります。

例：

```
Use this configuration? {yes/no} : yes
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started!
%LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
%LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
%LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
%LINK-3-UPDOWN: Interface Serial0/0/1, changed state to down
%LINK-3-UPDOWN: Interface Serial0/2, changed state to down
```

```
%LINK-3-UPDOWN: Interface Serial1/0, changed state to up
%LINK-3-UPDOWN: Interface Serial1/1, changed state to down
%LINK-3-UPDOWN: Interface Serial1/2, changed state to down
<Additional messages omitted.>
```

ステップ 2 画面にメッセージが表示されなくなったら、**Return** を押して Router> プロンプトを表示します。

ステップ 3 既存の設定の変更または別の設定の作成を選択します。Router> プロンプトは、コマンドライン インターフェイス（CLI）を実行中で、ルータの初期設定を完了したことを示します。それでも、これは設定の完了ではありません。この時点で 2 つの選択肢があります。

- もう一度 setup コマンド機能を実行し、別の設定を作成します。

例：

```
Router> enable
Password: password
Router# setup
```

- CLI を使用して、既存の設定を変更するか、追加の機能を設定します。

例：

```
Router> enable
Password: password
Router# configure terminal
Router(config)#
```

Cisco IOS XE CLI の使用：手動設定

ここでは、コマンドラインインターフェイス（CLI）にアクセスしてルータで初期設定を実行する方法について説明します。

（注） Cisco IOS CLI でルータを初期設定する場合は、コンソール接続を確立する必要があります。

出荷前にルータにデフォルトの設定ファイルがインストールされていない場合、システム設定ダイアログメッセージが表示されません。デバイスを設定するには、次の手順に従います。

手順の概要

1. 次のシステムメッセージがルータに表示されたら、適切な答えを入力します。
2. Return を押して自動インストールを終了し、手動設定を続行します。
3. Return を押すと Router> プロンプトが表示されます。
4. enable と入力して特権 EXEC モードを開始します。

手順の詳細

ステップ 1 次のシステムメッセージがルータに表示されたら、適切な答えを入力します。

例：

```
--- System Configuration Dialog ---
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 '[]'.
Would you like to enter the initial configuration dialog? [yes/no]: no
```

ステップ 2 Return を押して自動インストールを終了し、手動設定を続行します。

例：

```
Would you like to terminate autoinstall? [yes]
 Return
```

いくつかのメッセージが表示され、次のような行で終わります。

例：

```
...
Copyright (c) 1986-2012 by cisco Systems, Inc.
Compiled <date
> <time
> by <person
>
```

ステップ 3 Return を押すと Router> プロンプトが表示されます。

例：

```
...
flashfs[4]: Initialization complete.
Router>
```

ステップ 4 enable と入力して特権 EXEC モードを開始します。

例：

```
Router> enable

Router#
```

Cisco 4000 シリーズ ISR のホスト名の設定

ホスト名はCLIプロンプトとデフォルトの設定ファイル名に使用されます。ルータのホスト名を設定しないと、出荷時のデフォルト ホスト名である「Router」が使用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **hostname** *name*
4. ルータ プロンプトに新しいホスト名が表示されることを確認します。
5. **end**

手順の詳細

	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： `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 3	**hostname** *name* 例： `Router(config)# hostname myrouter`	ネットワーク サーバのホスト名を指定または修正します。
ステップ 4	ルータ プロンプトに新しいホスト名が表示されることを確認します。 例： `myrouter(config)#`	—
ステップ 5	**end** 例： `myrouter# end`	（任意）特権 EXEC モードに戻ります。

イネーブルおよびイネーブル シークレット パスワードの設定

セキュリティのレイヤを追加するには、特にネットワークを経由するパスワードまたは TFTP サーバに保存されるパスワードの場合、**enable password** コマンドまたは **enable secret** コマンドを使用します。どちらのコマンドも同じ結果を達成します。つまり、特権 EXEC（イネーブル）モードにアクセスするために入力する必要がある、暗号化されたパスワードを設定できます。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。Cisco IOS XE ソフトウェアの古いイメージを起動する場合にのみ、**enable password** コマンドを使用します。

詳細については、『Cisco IOS Security Configuration Guide』の「Configuring Passwords and Privileges」を参照してください。また、『Cisco IOS Password Encryption Facts』テクニカルノートと『Improving Security on Cisco Routers』テクニカルノートも参照してください。

（注） **enable secret** コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **enable secret** *password*
5. **end**
6. **enable**
7. **end**

手順の詳細

	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： `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 3	**enable password** *password* 例： `Router(config)# enable password pswd2`	（任意）多様な特権レベルに対して、アクセスを制御するローカル パスワードを設定します。 • 推奨：この手順を実行するのは、**enable secret** コマンドを認識しない古いブート ROM をブートする場合、または Cisco IOS-XE ソフトウェアの古いイメージをブートする場合だけにしてください。
ステップ 4	**enable secret** *password* 例： `Router(config)# enable secret greentree`	**enable password** コマンドよりも強化したセキュリティ レイヤを指定します。 • 手順 3 で入力したものと同じパスワードを使用しないでください。
ステップ 5	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • 新しいイネーブルまたはイネーブル シークレット パスワードが機能していることを確認します。
ステップ 7	**end** 例： `Router(config)# end`	（任意）特権 EXEC モードに戻ります。

コンソールのアイドル特権 EXEC タイムアウトの設定

ここでは、コンソール回線のアイドル特権EXECタイムアウトを設定する方法について説明します。デフォルトでは、特権 EXEC コマンド インタープリタは、ユーザ入力の検出を 10 分間待ってからタイムアウトします。

コンソール回線を設定するとき、通信パラメータの設定、自動ボー接続の指定、および使用している端末の端末操作パラメータの設定を行うこともできます。コンソール回線の設定の詳細については、『*Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*』を参照してください。とくに「Configuring Operating Characteristics for Terminals」および「Troubleshooting and Fault Management」の章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **exec-timeout** *minutes* [*seconds*]
5. **end**
6. **show running-config**

手順の詳細

	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： `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。

	コマンドまたはアクション	目的
ステップ 3	**line console 0** 例： `Router(config)# line console 0`	コンソール回線を設定し、回線コンフィギュレーション コマンドのコレクション モードを開始します。
ステップ 4	**exec-timeout** *minutes* [*seconds*] 例： `Router(config-line)# exec-timeout 0 0`	アイドル特権 EXEC タイムアウトを設定します。これは特権 EXEC コマンドインタープリタがユーザの入力が検出されるまで待つ間隔です。 • 次に、タイムアウトなしを指定する例を示します。exec-timeout 値を 0 に設定すると、ルータへのログイン後にタイムアウトでログアウトすることがなくなります。この場合、disable コマンドを使用して手動でログアウトしないでコンソールを離れると、セキュリティ上の問題が発生する可能性があります。
ステップ 5	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Router(config)# show running-config`	実行コンフィギュレーション ファイルを表示します。 • アイドル特権 EXEC タイムアウトを適切に設定したことを確認します。

例

次に、コンソールのアイドル特権 EXEC タイムアウトを 2 分 30 秒に設定する例を示します。

```
line console
 exec-timeout 2 30
```

次に、コンソールのアイドル特権 EXEC タイムアウトを 30 秒に設定する例を示します。

```
line console
 exec-timeout 0 30
```

ギガビット イーサネット管理インターフェイスの概要

ルータには、GigabitEthernet0 という名前のイーサネット管理ポートがあります。

このインターフェイスの目的は、ユーザーがルータの管理タスクを実行できるようにすることです。これは、ネットワークトラフィックを転送すべきではない（多くの場合、転送できない）インターフェイスです。ただし、Telnet および SSH を介してルータにアクセスし、ルータ

で管理タスクを実行するために使用できます。このインターフェイスは、ルータがルーティングを開始する前か、またはその他の転送インターフェイスが非アクティブ時にトラブルシューティングを行う場合に有用な機能を提供します。

管理イーサネット インターフェイスでは、次の点に注意してください。

- ルータには、GigabitEthernet0 という名前の管理イーサネット インターフェイスが 1 つあります。
- インターフェイスでサポートされるルーテッド プロトコルは、IPv4、IPv6、および ARP だけです。
- インターフェイスは、転送インターフェイスが機能していないか、IOS プロセスがダウンしていても、ルータにアクセスする手段を提供します。
- 管理イーサネット インターフェイスは、自身の VRF の一部です。詳細については、『Software Configuration Guide for Cisco 4000 Series ISRs』の「Management Ethernet Interface VRF」を参照してください。

ギガビット イーサネットのデフォルト構成

デフォルトでは、転送 VRF は、「Mgmt-intf」という特殊なグループ名を持つインターフェイス用に設定されます。この設定を変更することはできません。これは、管理インターフェイスのトラフィックをフォワーディング プレーンから分離します。基本設定は他のインターフェイスと同様ですが、これらのインターフェイスでサポートされない多くの転送機能があります。GigabitEthernet0 インターフェイスは管理用にのみ使用されるため、ここでは転送機能を設定できません。

```
For example, the default configuration is as follows:
interface GigabitEthernet0
vrf forwarding Mgmt-intf
ip address 172.18.77.212 255.255.255.0
negotiation auto
```

ギガビット イーサネット ポートの番号

ギガビット イーサネット管理ポートは、常に GigabitEthernet0 です。

ポートには、コンフィギュレーション モードでアクセスできます。

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gigabitethernet0
Router(config-if)#
```

ギガビット イーサネット インターフェイスの設定

ここでは、IP アドレスおよびインターフェイスの説明をルータのイーサネット インターフェイスに割り当てる方法について説明します。

ギガビット イーサネット インターフェイスに関する総合的な設定情報については、『*Cisco IOS Interface and Hardware Component Configuration Guide*』

（http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflanin.html）の「Configuring LAN Interfaces」を参照してください。

インターフェイスのナンバリングについては、ルータのソフトウェア コンフィギュレーション ガイドを参照してください。

手順の概要

1. **enable**
2. **show ip interface brief**
3. **configure terminal**
4. **interface** {**fastethernet** | **gigabitethernet**} **0**/*port*
5. **description** 文字列
6. **ip address** *ip-address mask*
7. **no shutdown**
8. **end**
9. **show ip interface brief**

手順の詳細

	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	**show ip interface brief** 例： `Router# show ip interface brief`	IP に設定されているインターフェイスの簡単なステータスを表示します。 • ルータ上にあるイーサネットインターフェイスの種類がわかります。
ステップ 3	**configure terminal** 例： `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 4	**interface** {**fastethernet**	**gigabitethernet**} **0**/*port* 例： `Router(config)# interface gigabitethernet 0/0/0`	イーサネット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 モードを開始します。 （注） インターフェイスの番号付けについては、「Slots, Subslots (Bay), Ports, and Interfaces in Cisco 4000 Series ISRs」（1 ～ 38 ページ）を参照してください。
ステップ 5	**description** 文字列 例：	（任意）インターフェイス設定に説明を追加します。説明があると、そのインターフェイスに接続さ

	コマンドまたはアクション	目的
	`Router(config-if)# description GE int to 2nd floor south wing`	れているものを思い出しやすくなります。また、トラブルシューティングのために役立つこともあります。
ステップ 6	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 172.16.74.3 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 7	**no shutdown** 例： `Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 8	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show ip interface brief** 例： `Router# show ip interface brief`	IP に設定されているインターフェイスの簡単なステータスを表示します。イーサネットインターフェイスが起動し、正しく設定されていることを確認します。

設定例

ギガビット イーサネット インターフェイスの設定：例

```
!
interface GigabitEthernet0/0/0
 description GE int to HR group
 ip address 172.16.3.3 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
```

show ip interface brief コマンドの出力例

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/1   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/2   unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/3   unassigned      YES NVRAM  administratively down down
GigabitEthernet0       10.0.0.1        YES manual up                    up
```

デフォルトルートまたはラストリゾートゲートウェイの指定

ここでは、IP ルーティングをイネーブルにしてデフォルト ルートを指定する方法について説明します。デフォルトルートの指定の代替手段については、技術仕様ノートの『Configuring a Gateway of Last Resort Using IP Commands』を参照してください。

パケット用のより良いルートがなく、しかも宛先が接続先ネットワークではない場合、Cisco IOS-XE ソフトウェアは、そのゲートウェイ（ルータ）をラストリゾートゲートウェイとして使用します。ここでは、デフォルト ルート（ラスト リゾート ゲートウェイを計算するルート候補）としてネットワークを選択する方法について説明します。ルーティング プロトコルがデフォルト ルート情報を伝播する方法は、プロトコルによって異なります。

IP ルーティングおよび IP プロトコルの設定

IP ルーティングおよび IP ルーティングプロトコルに関する総合的な設定情報については、Cisco.com の『Configuring IP Routing Protocol-Independent Feature』を参照してください。

IP ルーティング

IP ルーティングは、Cisco ISO-XE ソフトウェアで自動的にイネーブルになります。IP ルーティングを設定すると、設定済みのデフォルト ルートなど、パケットの転送に設定済みまたは既存のルートが使用されます。

（注） このタスク セクションは、IP ルーティングをディセーブルにするときは適用されません。IP ルーティングをディセーブルにするときにデフォルトルートを指定するには、Cisco.com にある技術仕様ノートの『Configuring a Gateway of Last Resort Using IP Commands』を参照してください。

デフォルト ルート

ルータは他のすべてのネットワークに対してルートを決定できないこともあります。ルーティング機能を実現するための一般的な方法は、スマート ルータとして複数のルータを使用し、残りのルータのデフォルト ルータをスマート ルータに設定します（スマート ルータにはインターネットワーク全体のルーティング テーブルに関する情報が格納されます）。これらのデフォルト ルートをダイナミックに渡すことや、個々のルータに設定することができます。

ほとんどのダイナミックな内部ルーティング プロトコルには、スマート ルータがダイナミックなデフォルト情報を生成し、それを他のルータに渡す処理を発生させるメカニズムが含まれます。

デフォルト ネットワーク

指定したデフォルトネットワークに直接接続されているインターフェイスがルータにある場合、ルータで実行されるダイナミック ルーティング プロトコルによって、デフォルトルートが生成されるか、デフォルトルートが調達されます。RIP の場合、ルータは疑似ネットワーク

0.0.0.0 をアドバタイズします。IGRP の場合、ネットワーク自体がアドバタイズされ、外部ルートとしてフラグが付けられます。

ネットワークのデフォルトを生成しているルータには、そのルータ自身のデフォルトも指定する必要がある場合があります。ルータが自身のデフォルト ルートを生成する方法の 1 つは、適切なデバイスを経由してネットワーク 0.0.0.0 に至るスタティック ルートを指定することです。

ラスト リゾート ゲートウェイ

デフォルト情報をダイナミック ルーティング プロトコルを介して渡している場合、その他の設定は不要です。ルーティング テーブルは定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。RIP の場合、0.0.0.0 という唯一の選択肢しかありません。IGRP の場合、システム デフォルトの候補にすることができるネットワークが複数存在することもあります。Cisco IOS-XE ソフトウェアはアドミニストレーティブ ディスタンスおよびメトリック情報の両方を使用して、デフォルト ルート（ラスト リゾート ゲートウェイ）を判断します。選択したデフォルト ルートは、**show ip route** EXEC コマンドのラスト リゾート ゲートウェイの表示に示されます。

ダイナミックなデフォルト情報がソフトウェアに送信されない場合は、**ip default-network** グローバル コンフィギュレーション コマンドを使用し、デフォルト ルートの候補を指定します。この方法では、**ip default-network** コマンドは引数として未接続ネットワークを使用します。このネットワークが任意のソース（ダイナミックまたはスタティック）のルーティング テーブルに表示される場合、デフォルト ルート候補としてフラグが付けられ、デフォルト ルートの可能な選択肢になります。

ルータのデフォルト ネットワークにインターフェイスがなく、そのネットワークに対するルートはある場合、そのネットワークはデフォルト パス候補と見なされます。ルート候補は検査され、アドミニストレーティブ ディスタンスおよびメトリックに基づいて最適な候補が選択されます。最適なデフォルト パスに対するゲートウェイは、ラスト リゾート ゲートウェイになります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **ip route** *dest-prefix mask next-hop-ip-address* [*admin-distance*] [**permanent**]
5. 次のいずれかを実行します。
   - **ip default-network** *network-number*
   -
   - **ip route** *dest-prefix mask next-hop-ip-address*
6. **end**
7. **show ip route**

手順の詳細

	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： `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 3	**ip routing** 例： `Router(config)# ip routing`	IP ルーティングを有効にします。
ステップ 4	**ip route** *dest-prefix mask next-hop-ip-address* [*admin-distance*] [**permanent**] 例： `Router(config)# ip route 192.168.24.0 255.255.255.0 172.28.99.2`	スタティック ルートを確立します。

ステップ 5	次のいずれかを実行します。
	• **ip default-network** *network-number*
	•
	• **ip route** *dest-prefix mask next-hop-ip-address*
	例：
	`Router(config)# ip default-network 192.168.24.0`
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 172.28.99.1`
		ラスト リゾート ゲートウェイを計算するルート候補としてネットワークを選択します。
		ラスト リゾート ゲートウェイを計算するために、ネットワーク 0.0.0.0 0.0.0.0 に対するスタティック ルートを作成します。

ステップ 6	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show ip route** 例： `Router# show ip route`	現在のルーティング テーブル情報を表示します。ラスト リゾート ゲートウェイが設定されていることを確認します。

設定例

デフォルト ルートの指定：例

```
!
ip route 192.168.24.0 255.255.255.0 172.28.99.2
!
ip default-network 192.168.24.0
!
```

show ip route コマンドの出力例

```
Router# show ip route

Codes: L - local, 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, H - NHRP,
l - LISP a - application route + - replicated route, % - next hop override
Gateway of last resort is not set 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/24 is directly connected, Loopback1 L 10.0.0.1/32 is directly connected,
Loopback1 Router#
```

リモートコンソールアクセスのための仮想端末回線の設定

仮想端末（VTY）回線は、ルータに対してリモート アクセスするために使用されます。ここでは、電源があるユーザだけがルータをリモートアクセスできるように、パスワードを使用して仮想端末回線を設定する方法について説明します。

デフォルトで、ルータには5個の仮想端末回線があります。ただし、追加の仮想端末回線を作成できます。『Cisco IOS XE Dial Technologies Configuration Guide』（http://www.cisco.com/en/US/docs/ios/dial/configuration/guide/2_xe/dia_2_xe_book.html）を参照してください。

回線パスワードおよびパスワードの暗号化は、『Cisco IOS XE Security Configuration Guide: Secure Connectivity』（http://www.cisco.com/en/US/docs/ios/ios_xe/sec_secure_connectivity/configuration/guide/2_xe/sec_secure_connectivity_xe_book.html）に記載されています。「Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices」のセクションを参照してください。アクセスリストで仮想端末回線（VTY）のセキュリティを保護する場合、『Access Control Lists: Overview and Guidelines』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **line vty** *line-number* [*ending-line-number*]
4. **password** *password*
5. **login**

6. **end**
7. **show running-config**
8. 別のネットワーク デバイスから、ルータに対する Telnet セッションの開始を試行します。

手順の詳細

	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： `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 3	**line vty** *line-number* [*ending-line-number*] 例： `Router(config)# line vty 0 4`	リモート コンソール アクセスために、仮想端末回線（VTY）の回線コンフィギュレーション コマンドのコレクション モードを開始します。 • ルータ上のすべての VTY 回線を設定していることを確認します。 （注） ルータ上の VTY 回線の数を確認するには、**line vty ?** コマンドを使用します。
ステップ 4	**password** *password* 例： `Router(config-line)# password guessagain`	回線のパスワードを指定します。
ステップ 5	**login** 例： `Router(config-line)# login`	ログイン時のパスワードチェックをイネーブルにします。
ステップ 6	**end** 例： `Router(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Router# show running-config`	実行コンフィギュレーション ファイルを表示します。リモートアクセスのために仮想端末回線を適切に設定したことを確認します。

	コマンドまたはアクション	目的

ステップ 8	別のネットワーク デバイスから、ルータに対する Telnet セッションの開始を試行します。
	例：
	`Router# 172.16.74.3`
	例：
	`Password:`
		ルータにリモートアクセスできること、および仮想端末回線のパスワードが正しく設定されていることを確認します。

設定例

次に、パスワードを使用して仮想端末回線を設定する例を示します。

```
!
line vty 0 4
 password guessagain
 login
!
```

次の作業

VTY 回線を設定したら、次の手順を実行します。

- （任意）仮想端末回線のパスワードを暗号化するには、『Cisco IOS Security Configuration Guide』の「Configuring Passwords and Privileges」の章を参照してください。また、『Cisco IOS Password Encryption Facts』テクニカル ノートを参照してください。
- （任意）アクセスリストを使用して VTY 回線のセキュリティを確保するには、『Cisco IOS Security Configuration Guide』の「Part 3: Traffic Filtering and Firewalls」を参照してください。

補助回線の設定

ここでは、補助回線について回線コンフィギュレーション モードを開始する方法について説明します。補助回線の設定方法は、補助（AUX）ポートの具体的な実装によって異なります。補助回線の設定については、次のマニュアルを参照してください。

- 『*Configuring a Modem on the AUX Port for EXEC Dialin Connectivity*』（技術仕様ノート）
  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080094bbc.shtml
- 『*Configuring Dialout Using a Modem on the AUX Port*』（設定例）
  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_configuration_example09186a0080094579.shtml
- 『*Configuring AUX-to-AUX Port Async Backup with Dialer Watch*』（設定例）
  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_configuration_example09186a0080093d2b.shtml
- 『*Modem-Router Connection Guide*』（技術仕様ノート）
  http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a008009428b.shtml

手順の概要

1. **enable**
2. **configure terminal**
3. **line aux 0**
4. AUX ポートの特定の実装に合わせて回線を設定するには、技術仕様ノートと設定例を参照してください。

手順の詳細

	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： `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 3	**line aux 0** 例： `Router(config)# line aux 0`	補助回線について回線コンフィギュレーション コマンドのコレクション モードを開始します。
ステップ 4	AUX ポートの特定の実装に合わせて回線を設定するには、技術仕様ノートと設定例を参照してください。	—

ネットワーク接続の確認

ここでは、ルータのネットワーク接続を確認する方法について説明します。

始める前に

- この章で説明するすべての設定タスクを完了する必要があります。
- 適切に設定したネットワーク ホストにルータを接続する必要があります。

手順の概要

1. **enable**
2. **ping** [*ip-address* | *hostname*]
3. **telnet** {*ip-address* | *hostname*}

手順の詳細

	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	**ping** [*ip-address* | *hostname*] 例： `Router# ping 172.16.74.5`	初期ネットワーク接続を診断します。接続を確認するには、ネクストホップのルータ、または設定済みの各インターフェイスに接続しているホストに対して ping を実行します。
ステップ 3	**telnet** {*ip-address* | *hostname*} 例： `Router# telnet 10.20.30.40`	Telnet をサポートするホストにログインします。VTY 回線パスワードをテストする必要がある場合には、別のネットワークデバイスからこの手順を実行し、ルータの IP アドレスを使用します。

例

次の表示は、IP アドレス 192.168.7.27 に対して ping を実行したときの出力例です。

```
Router# ping

Protocol [ip]:
Target IP address: 192.168.7.27

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/2/4 ms
```

次の表示は、IP ホスト名 donald に対して ping を実行したときの出力例です。

```
Router# ping donald

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.27, timeout is 2 seconds:
!!!!!
Success rate is 100 percent, round-trip min/avg/max = 1/3/4 ms
```

デバイス設定の保存

ここでは、実行コンフィギュレーションを NVRAM のスタートアップ コンフィギュレーションに保存することで、次のシステム リロード時、または電源の再投入時に設定を失わない方法について説明します。NVRAM には、ルータ上に 256 KB のストレージがあります。

手順の概要

1. **enable**
2. **copy running-config startup-config**

手順の詳細

	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	**copy running-config startup-config** 例： `Router# copy running-config startup-config`	実行中の設定をスタートアップ コンフィギュレーションに保存します。

設定およびシステムイメージのバックアップコピーの保存

ファイルの破損時にファイルの回復を補助し、ダウンタイムを最小限に抑えるために、スタートアップ コンフィギュレーション ファイルおよびCisco IOS-XE ソフトウェア システム イメージ ファイルのバックアップ コピーをサーバに保存することを推奨します。

手順の概要

1. **enable**
2. **copy nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**}
3. **show {bootflash0|bootflash1}:**
4. **copy {bootflash0|bootflash1}:** {**ftp:** | **rcp:** | **tftp:**}

手順の詳細

	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）。

	コマンドまたはアクション	目的
ステップ 2	**copy nvram:startup-config** {**ftp:** | **rcp:** | **tftp:**} 例： `Router# copy nvram:startup-config ftp:`	スタートアップ コンフィギュレーション ファイルをサーバにコピーします。コンフィギュレーション ファイルのコピーはバックアップコピーとして使用できます。プロンプトが表示されたら、コピー先の URL を入力します。
ステップ 3	**show {bootflash0|bootflash1}:** 例： `Router# show {bootflash0|bootflash1}:`	フラッシュ メモリ ファイル システムのレイアウトとコンテンツを表示します。システムイメージファイルの名前を確認します。
ステップ 4	**copy {bootflash0|bootflash1}:** {**ftp:** | **rcp:** | **tftp:**} 例： `Router# copy {bootflash0|bootflash1}: ftp:`	フラッシュ メモリのファイルをサーバーにコピーします。 • システムイメージファイルをサーバーにコピーし、バックアップ コピーとして使用します。 • プロンプトが表示されたら、ファイル名とコピー先の URL を入力します。

設定例

スタートアップ コンフィギュレーションの TFTP サーバーへのコピー：例

次に、スタートアップ コンフィギュレーションを TFTP サーバーにコピーする例を示します。

```
Router# copy nvram:startup-config tftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [rtr2-confg]? <cr>

Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>

![OK]
```

フラッシュ メモリから TFTP サーバーへのコピー：例

次に、特権 EXEC で **show {flash0|flash1}:** コマンドを使用してシステムイメージファイルの名前を確認し、**copy {flash0|flash1}: tftp:** 特権 EXEC コマンドを使用して、システムイメージを TFTP サーバーにコピーする例を示します。このルータはデフォルトのユーザー名とパスワードを使用しています。

```
Router#Directory of bootflash:
11 drwx 16384 Jun 12 2012 17:31:45 +00:00 lost+found 64897 drwx 634880 Sep 6 2012 14:33:26
 +00:00 core 340705 drwx 4096 Oct 11 2012 19:28:27 +00:00 .prst_sync 81121 drwx 4096 Jun
 12 2012 17:32:39 +00:00 .rollback_timer 12 -rw- 0 Jun 12 2012 17:32:50 +00:00
tracelogs.336 713857 drwx 1347584 Oct 11 2012 20:24:26 +00:00 tracelogs 162241 drwx 4096
 Jun 12 2012 17:32:51 +00:00 .installer 48673 drwx 4096 Jul 2 2012 17:14:51 +00:00
vman_fdb 13 -rw- 420654048 Aug 28 2012 15:01:31 +00:00
```

```
crankshaft-universalk9.BLD_MCP_DEV_LATEST_20120826_083012.SSA.bin 14 -rw- 727035 Aug 29
 2012 21:03:25 +00:00 uut2_2000_ikev1.cfg 15 -rw- 420944032 Aug 29 2012 19:40:28 +00:00
 crankshaft-universalk9.BLD_MCP_DEV_LATEST_20120829_033026.SSA.bin 16 -rw- 1528 Aug 30
2012 14:24:38 +00:00 base.cfg 17 -rw- 360900 Aug 31 2012 19:10:02 +00:00
uut2_1000_ikev1.cfg 18 -rw- 421304160 Aug 31 2012 16:34:19 +00:00
crankshaft-universalk9.BLD_MCP_DEV_LATEST_20120821_193221.SSA.bin 19 -rw- 421072064 Aug
 31 2012 18:31:57 +00:00 crankshaft-universalk9.BLD_MCP_DEV_LATEST_20120830_110615.SSA.bin
 20 -rw- 453652 Sep 1 2012 01:48:15 +00:00 uut2_1000_ikev1_v2.cfg 21 -rw- 16452768 Sep
11 2012 20:36:20 +00:00 upgrade_stage_1_of_1.bin.2012-09-05-Delta 22 -rw- 417375456 Sep
 12 2012 20:28:23 +00:00 crankshaft-universalk9.2012-09-12_00.45_cveerapa.SSA.bin 23
-rw- 360879 Oct 8 2012 19:43:36 +00:00 old-config.conf 24 -rw- 390804800 Oct 11 2012
15:34:08 +00:00 _1010t.bin 7451738112 bytes total (4525948928 bytes free)
Router#show bootflash: -#- --length-- ---------date/time--------- path 1 4096 Oct 11
2012 20:22:19 +00:00 /bootflash/ 2 16384 Jun 12 2012 17:31:45 +00:00 /bootflash/lost+found
 3 634880 Sep 06 2012 14:33:26 +00:00 /bootflash/core 4 1028176 Sep 06 2012 14:31:17
+00:00 /bootflash/core/UUT2_RP_0_iomd_17360.core.gz 5 1023738 Sep 06 2012 14:31:24 +00:00
 /bootflash/core/UUT2_RP_0_iomd_23385.core.gz 6 1023942 Sep 06 2012 14:31:30 +00:00
/bootflash/core/UUT2_RP_0_iomd_24973.core.gz 7 1023757 Sep 06 2012 14:31:37 +00:00
/bootflash/core/UUT2_RP_0_iomd_26241.core.gz 8 1023726 Sep 06 2012 14:31:43 +00:00
/bootflash/core/UUT2_RP_0_iomd_27507.core.gz 9 1023979 Sep 06 2012 14:31:50 +00:00
/bootflash/core/UUT2_RP_0_iomd_28774.core.gz 10 1023680 Sep 06 2012 14:31:56 +00:00
/bootflash/core/UUT2_RP_0_iomd_30045.core.gz 11 1023950 Sep 06 2012 14:32:02 +00:00
/bootflash/core/UUT2_RP_0_iomd_31332.core.gz 12 1023722 Sep 06 2012 14:32:09 +00:00
/bootflash/core/UUT2_RP_0_iomd_5528.core.gz 13 1023852 Sep 06 2012 14:32:15 +00:00
/bootflash/core/UUT2_RP_0_iomd_7950.core.gz 14 1023916 Sep 06 2012 14:32:22 +00:00
/bootflash/core/UUT2_RP_0_iomd_9217.core.gz 15 1023875 Sep 06 2012 14:32:28 +00:00
/bootflash/core/UUT2_RP_0_iomd_10484.core.gz 16 1023907 Sep 06 2012 14:32:35 +00:00
/bootflash/core/UUT2_RP_0_iomd_11766.core.gz 17 1023707 Sep 06 2012 14:32:41 +00:00
/bootflash/core/UUT2_RP_0_iomd_13052.core.gz 18 1023963 Sep 06 2012 14:32:48 +00:00
/bootflash/core/UUT2_RP_0_iomd_14351.core.gz 19 1023915 Sep 06 2012 14:32:54 +00:00
/bootflash/core/UUT2_RP_0_iomd_15644.core.gz 20 1023866 Sep 06 2012 14:33:00 +00:00
/bootflash/core/UUT2_RP_0_iomd_17171.core.gz 21 1023518 Sep 06 2012 14:33:07 +00:00
/bootflash/core/UUT2_RP_0_iomd_18454.core.gz 22 1023938 Sep 06 2012 14:33:13 +00:00
/bootflash/core/UUT2_RP_0_iomd_19741.core.gz 23 1024017 Sep 06 2012 14:33:20 +00:00
/bootflash/core/UUT2_RP_0_iomd_21039.core.gz 24 1023701 Sep 06 2012 14:33:26 +00:00
/bootflash/core/UUT2_RP_0_iomd_22323.core.gz 25 4096 Oct 11 2012 19:28:27 +00:00
/bootflash/.prst_sync 26 4096 Jun 12 2012 17:32:39 +00:00 /bootflash/.rollback_timer 27
 0 Jun 12 2012 17:32:50 +00:00 /bootflash/tracelogs.336 28 1347584 Oct 11 2012 20:24:26
 +00:00 /bootflash/tracelogs 29 392 Oct 11 2012 20:22:19 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.gz 30 308 Oct 11 2012 18:39:43 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011183943.gz 31 308 Oct 11 2012
18:49:44 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011184944.gz 32
42853 Oct 04 2012 07:35:39 +00:00 /bootflash/tracelogs/hman_R0-0.log.0498.20121004073539.gz
 33 307 Oct 11 2012 18:59:45 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011185945.gz 34 308 Oct 11 2012
19:19:47 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011191947.gz 35 307
 Oct 11 2012 19:37:14 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011193714.gz 36 308 Oct 11 2012
19:47:15 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011194715.gz 37 308
 Oct 11 2012 19:57:16 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011195716.gz 38 308 Oct 11 2012
20:07:17 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011200717.gz 39 307
 Oct 11 2012 20:12:18 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011201218.gz 40 306 Oct 11 2012
20:17:18 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011201718.gz 41
44220 Oct 10 2012 11:47:42 +00:00
/bootflash/tracelogs/hman_R0-0.log.32016.20121010114742.gz 42 64241 Oct 09 2012 20:47:59
 +00:00 /bootflash/tracelogs/fman-fp_F0-0.log.12268.20121009204757.gz 43 177 Oct 11 2012
 19:27:03 +00:00 /bootflash/tracelogs/inst_compmatrix_R0-0.log.gz 44 307 Oct 11 2012
18:24:41 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011182441.gz 45 309
 Oct 11 2012 18:29:42 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011182942.gz 46 43748 Oct 06 2012
13:49:19 +00:00 /bootflash/tracelogs/hman_R0-0.log.0498.20121006134919.gz 47 309 Oct 11
 2012 18:44:43 +00:00 /bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011184443.gz
```

```
 48 309 Oct 11 2012 19:04:46 +00:00
/bootflash/tracelogs/inst_cleanup_R0-0.log.0000.20121011190446.gz 49 2729 Oct 09 2012
21:21:49 +00:00 /bootflash/tracelogs/IOSRP_R0-0.log.20011.20121009212149 50 116 Oct 08
2012 21:06:44 +00:00 /bootflash/tracelogs/binos_log_R0-0.log.20013.20121008210644
```

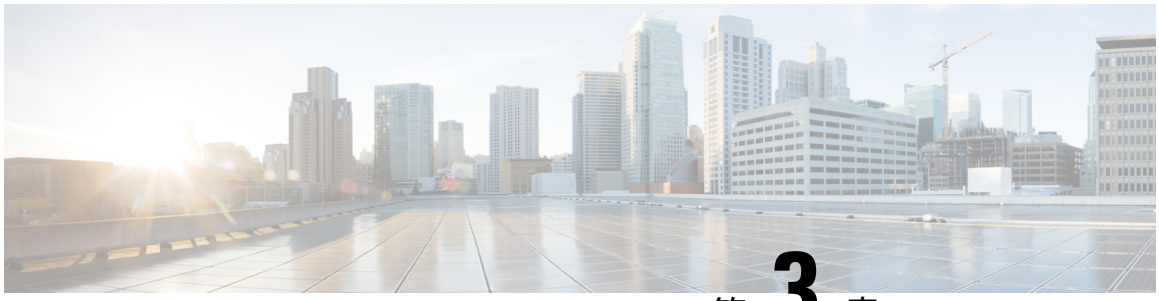
（注） 完了した作業内容を失わないために、進行に合わせてときどき設定を保存してください。**copy running-config startup-config** コマンドを入力し、NVRAM に設定を保存します。

Cisco 4000 シリーズ ISR での初期設定の確認

Cisco IOS-XE で次のコマンドを入力することで、ルータの初期設定を確認できます。

- **show version**—システムのハードウェア バージョン、インストールされているソフトウェア バージョン、コンフィギュレーション ファイルの名前とソース、ブート イメージ、搭載されている DRAM、NVRAM、およびフラッシュ メモリの容量を表示します。
- **show diag**：インストールされているコントローラ、インターフェイスプロセッサ、およびポートアダプタに関する診断情報を一覧表示します。
- **show interfaces**：インターフェイスが正常に機能しているかどうかと、インターフェイスおよび回線プロトコルが正しい状態（アップまたはダウンのいずれかの状態）にあるかどうかを示します。
- **show ip interface brief—** ：IP プロトコルに設定されているインターフェイスのステータスの概要を表示します。
- **show configuration—** ：正しいホスト名とパスワードが設定されているかどうかを確認します。
- **show platform—** ：ソフトウェア/ROMMON のバージョンなどを表示します。

初期設定を完了および確認したら、特定の特性と機能を設定できるようになります。『Software Configuration Guide for the Cisco 4400 and Cisco 4300 Series ISRs』を参照してください。



第 3 章

ルータの基本設定

ここでは、ルータの基本設定について説明します。次の項で構成されています。

デフォルト設定

ルータを起動すると、ルータはデフォルトのファイル名（ルータの PID）を検索します。たとえば、Cisco 4000 シリーズ サービス統合型ルータは、isr 4451.cfg という名前のファイルを検索します。Cisco 4000 シリーズ ISRは、このファイルを検索した後、標準の files-router-confg または ciscortr.cfg を検索します。

Cisco 4000 ISR は、ブートフラッシュで isr4451.cfg ファイルを検索します。ファイルがブートフラッシュで見つからない場合、ルータは標準の router-confg と ciscortr.cfg を検索します。すべてのファイルが見つからない場合、ルータは、同じ特定の順序で、これらのファイルを保存している可能性のある挿入済みの USB をチェックします。

（注） 挿入済みの USB に PID という名前の構成ファイルがある一方で、標準ファイルの 1 つがブートフラッシュにある場合、システムは標準ファイルを検索して使用します。

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 : 977 bytes
!
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
!
no aaa new-model
!
ipv6 multicast rpf use-bgp
!
!
multilink bundle-name authenticated
!
!
redundancy
mode none
!

interface GigabitEthernet0/0/0
no ip address
negotiation auto
!
interface GigabitEthernet0/0/1
no ip address
negotiation auto
!
interface GigabitEthernet0/0/2
no ip address
negotiation auto
!
interface GigabitEthernet0/0/3
no ip address
negotiation auto
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
negotiation auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!

!
control-plane
!
```

```
!
line con 0
stopbits 1
line vty 0 4
login
!
!
end
```

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。

手順の概要

1. **configure terminal**
2. **hostname** *name*
3. **enable secret** *password*
4. **no ip domain-lookup**

手順の詳細

	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 secret** *password* 例： `Router(config)# enable secret cr1ny5ho`	ルータへの不正なアクセスを防止するには、暗号化パスワードを指定します。
ステップ 4	**no ip domain-lookup** 例：	ルータが未知の単語（入力ミス）をIPアドレスに変換しないようにします。

	コマンドまたはアクション	目的
	`Router(config)# no ip domain-lookup`	グローバル パラメータ コマンドの詳細については、『Cisco IOS Release Configuration Guide』マニュアル セットを参照してください。

ギガビット イーサネット インターフェイスの設定

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。

手順の概要

1. **interface gigabitethernet** *slot/bay/port*
2. **ip address** *ip-address mask*
3. **ipv6 address** *ipv6-address/prefix*
4. **no shutdown**
5. **exit**

手順の詳細

	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 0/0/1`	ルータ上で ギガビット イーサネット 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`	指定したギガビット イーサネット 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`	指定したギガビット イーサネット 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。
ステップ 4	**no shutdown** 例： `Router(config-if)# no shutdown`	ギガビットイーサネットインターフェイスをイネーブルにし、その状態を管理上のダウンから管理上のアップに変更します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Router(config-if)# exit`	ギガビット イーサネット インターフェイスのコンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

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。

手順の概要

1. **interface** *type number*
2. （オプション 1）**ip address** *ip-address mask*
3. （オプション 2） **ipv6 address** *ipv6-address/prefix*
4. **exit**

手順の詳細

	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： `Router(config-if)# ip address 10.108.1.1 255.255.255.0`	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)# 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。

	コマンドまたはアクション	目的
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

このコンフィギュレーション例のループバック インターフェイスは、仮想テンプレート インターフェイス上の NAT をサポートするために使用されています。この設定例は、スタティック IP アドレスとして機能する IP アドレス 192.0.2.0/24 のギガビット イーサネット インターフェイス上に設定されるループバック インターフェイスを示しています。ループバック インターフェイスは、ネゴシエートされた IP アドレスを持つ virtual-template1 に紐付けられます。

```
!
interface loopback 0
ip address 192.0.2.0 255.255.255.0 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
```

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 203.0.113.1/24
  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
```

MAC フィルタのハードウェア制限

ここでは、Cisco 4000 シリーズ ISR でサポートされている仮想 MAC アドレスの数と分布について説明します。仮想 MAC アドレスフィルタは、次のインターフェイスでサポートされています。

- GigabitEthernet インターフェイスの MAC フィルタ
- TenGigabitEthernet インターフェイスの MAC フィルタ

GigabitEthernet インターフェイスの MAC アドレスフィルタ

このデバイスは、32 の MAC アドレスフィルタのセットをサポートしています。これらのフィルタは、4 つの GE ポートで使用できます。4 つの GE ポートのそれぞれが、プライマリ MAC アドレス（BIA）用に 1 つのエントリを予約します。残りの 28 の MAC フィルタは、Hot Standby Router Protocol（HSRP）などの機能に使用できます。

（注） 各ポートは、使用可能な機能フィルタをいくつでも使用できます。1 つのポートで最大 28 の機能フィルタを使用できます。4 つの GE ポートのすべてが均等にフィルタを使用する場合、各ポートは最大 7 つのフィルタを持つことができます。

TenGigabitEthernet インターフェイスの MAC アドレスフィルタ

このデバイスは、32 の MAC アドレスフィルタのセットをサポートしています。これらのフィルタは、2 つの 10GE ポートで使用できます。10GE ポートのそれぞれが、プライマリ MAC アドレス（BIA）用に 1 つのエントリを予約します。残りの 30 の MAC フィルタは、HSRP などの機能に使用できます。

（注） 各ポートは、使用可能な機能フィルタをいくつでも使用できます。1 つのポートで最大 30 の機能フィルタを使用できます。両方の GE ポートが均等にフィルタを使用する場合、各ポートは最大 15 のフィルタを持つことができます。

MAC フィルタの配布

次の表に、Cisco 4000 シリーズ ISR の MAC フィルタの配布を示します。

表 *3 : Cisco 4461 ISR* の *MAC* フィルタの配布

インターフェイス	フィルタの総数		プライマリ MAC アドレス（BIA）		機能フィルタ
Gigabit0/0/0	32	=	1	+	28
Gigabit0/0/1			1		
Gigabit0/0/2			1		
Gigabit0/0/3			1		
TenGigabit0/0/0	32	=	1	+	30
TenGigabit0/0/1			1		

表 *4 : Cisco 4451* および *4431 ISR* ギガビット イーサネット インターフェイスの *MAC* フィルタの配布

インターフェイス	フィルタの総数		プライマリ MAC アドレス（BIA）		機能フィルタ
Gigabit0/0/0	32	=	1	+	28
Gigabit0/0/1			1		
Gigabit0/0/2			1		
Gigabit0/0/3			1		

表 *5 : Cisco 4351* および *4331 ISR* の *MAC* フィルタの配布

インターフェイス	フィルタの総数		プライマリ MAC アドレス（BIA）		機能フィルタ
Gigabit0/0/0	16	=	1	+	15
Gigabit0/0/1	16		1		15
Gigabit0/0/2	16		1		15

表 *6 : Cisco 4321* および *4221 ISR* の *MAC* フィルタの配布

インターフェイス	フィルタの総数		プライマリ MAC アドレス（BIA）		機能フィルタ
Gigabit0/0/0	16	=	1	+	15

インターフェイス	フィルタの総数		プライマリ MAC アドレス（BIA）		機能フィルタ
Gigabit0/0/1	16	=	1	+	15

モジュール インターフェイスの設定

サービスモジュールの設定の詳細については、『Cisco SM-1T3/E3 Service Module Configuration Guide』の「Service Module Management」の項の「Service Modules」を参照してください。

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。

（注） Cisco アグリゲーション サービス ルータまたは Cisco CSR 1000v では、CDP はデフォルトでイネーブルに設定されていません。

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。

手順の概要

1. **line** [**aux** | **console** | **tty** | **vty**] *line-number*
2. **password** *password*
3. **login**
4. **exec-timeout** *minutes* [*seconds*]
5. **exit**
6. **line** [**aux** | **console** | **tty** | **vty**] *line-number*
7. **password** *password*
8. **login**
9. **end**

手順の詳細

	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。「**0 0**」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。

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。

	コマンドまたはアクション	目的
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。

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。

手順の概要

1. （オプション 1） **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. （オプション 2） **ipv6 route** *prefix/mask* {*ipv6-address* | *interface-type interface-number* [*ipv6-address*]}
3. **end**

手順の詳細

	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 192.168.1.0 255.255.0.0 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`	IP パケットのスタティック ルートを指定します。
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。

例

設定の確認

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 192.168.1.0 255.255.255.0
```

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

     10.10.10.2/24 is subnetted, 1 subnets
C       10.10.10.2 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。

ルータは、ルーティング情報プロトコル（RIP）または Enhanced Interior Gateway Routing Protocol（EIGRP）などの IP ルーティング プロトコルを使用して、ルートを動的に学習できます。

- Routing Information Protocol の設定 （43 ページ）
- Enhanced Interior Gateway Routing Protocol の設定 （46 ページ）

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。

手順の概要

1. **router rip**
2. **version** {**1** | **2**}
3. **network** *ip-address*
4. **no auto-summary**

5. **end**

手順の詳細

	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

次の設定例は、IP ネットワーク 10.0.0.0 および 192.168.1.0 でイネーブルにされる RIP version 2 を示します。この設定を表示するには、特権 EXEC モードで **show running-config** コマンドを使用します。

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

Current configuration : 1616 bytes
!
! Last configuration change at 03:17:14 EST Thu Sep 6 2012
!
version 15.3
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable password cisco
!
no aaa new-model
!
transport-map type console consolehandler
 banner wait ^C
Waiting for IOS vty line
^C
 banner diagnostic ^C
Welcome to diag mode
^C
!
clock timezone EST -4 0
!
!


ip domain name cisco.com
ip name-server vrf Mgmt-intf 203.0.113.1
ip name-server vrf Mgmt-intf 203.0.113.129

!
ipv6 multicast rpf use-bgp
!
!
multilink bundle-name authenticated
!
redundancy
 mode none
!
ip ftp source-interface GigabitEthernet0
ip tftp source-interface GigabitEthernet0
!
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3
```

```
 no ip address
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 172.18.77.212 255.255.255.240
 negotiation auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 172.18.77.209
!
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password cisco
 login
!
transport type console 0 input consolehandler
!
ntp server vrf Mgmt-intf 10.81.254.131
!
end
```

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    10.0.0.0/8 [120/1] via 10.2.2.1, 00:00:02, Ethernet0/0/0
```

Enhanced Interior Gateway Routing Protocol の設定

拡張インテリア ゲートウェイ ルーティング プロトコル（EIGRP）を設定するには、次の手順を実行します。

手順の概要

1. **router eigrp** *as-number*
2. **network** *ip-address*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**router eigrp** *as-number* 例： `Router(config)# router eigrp 109`	ルータ コンフィギュレーション モードを開始して、ルータ上でEIGRPをイネーブルにします。自律システム（AS）番号は、他の EIGRP ルータへのルートを識別します。また、EIGRP情報のタグ付けに使用されます。

ステップ 2	**network** *ip-address*
	例：
	`Router(config)# network 192.168.1.0`
	`Router(config)# network 10.10.12.115`
		EIGRPを適用するネットワークのリストを指定します（直接接続されているネットワークのIPアドレスを使用）。

ステップ 3	**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

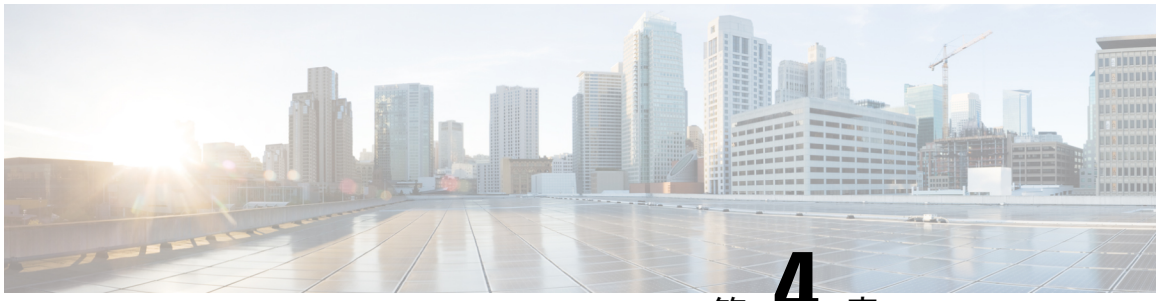
次の設定例は、IP ネットワーク 192.168.1.0 および 10.10.12.115 でイネーブルにされる EIGRP ルーティング プロトコルを示します。EIGRP の自律システム番号として、109 が割り当てられています。この設定を表示するには、**show running-config** コマンドを使用します。

```
Router# show running-config
.
.
.
!
router eigrp 109
 network 192.168.1.0
  network 10.10.12.115
!
.
.
.
```

IP EIGRP が正しく設定されたかどうかを確認するには、**show ip route** コマンドを入力し、文字Dで示されるEIGRPルートを探します。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
D     10.0.0.0/8 [90/409600] via 10.2.2.1, 00:00:02, Ethernet0/0
```



第 4 章

Cisco IOS XE ソフトウェアの使用

この章では、Cisco IOS XE ソフトウェアの基本的な使用方法について説明します。この章は次の項で構成されています。

ルータ コンソールを使用して CLI にアクセスする方法

始める前に

2 つのシリアル ポート（コンソール（CON）ポートおよび補助（AUX）ポート）があります。コマンドライン インターフェイス（CLI）に直接アクセスするか、または Telnet を使用する場合には、CON ポートを使用します。

ここでは、ルータへの主要なアクセス方法について説明します。

直接接続されたコンソールを使用して CLI にアクセスする方法

CON ポートは、no-flow 制御と RJ-45 コネクタを備えた EIA/TIA-232 非同期シリアル接続機能です。CON ポートは、シャーシの前面パネルにあります。

ここでは、制御インターフェイスにアクセスする手順について説明します。

コンソール ポートとの接続

ステップ 1 端末エミュレーション ソフトウェアを次のように設定します。

- 9,600 bps（ビット/秒）
- 8 データ ビット
- パリティなし
- フロー制御なし

ステップ 2 RJ-45/RJ-45 ケーブルと RJ-45/DB-25 DTE アダプタ、または RJ-45/DB-9 DTE アダプタ（「Terminal」のラベル付き）を使用して、CON ポートに接続します。

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 **setup** コマンドを入力する場合は、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』の「Initial Configuration」の項の「Using Cisco Setup Command Facility」を参照してください。

ステップ 4 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
```

SSH を使用したコンソールへのアクセス

Secure Shell（SSH）は、ネットワーク デバイスへのセキュアなリモート アクセス接続を提供するプロトコルです。デバイスで SSH サポートを有効にするには、次の手順を実行します。

ステップ 1 ホスト名を設定します。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname xxx_lab
```

ここで、*host name* は、ルータのホスト名または IP アドレスです。

ステップ 2 ルータの DNS ドメインを設定します。

```
xxx_lab(config)# xxx.cisco.com
```

ステップ 3 SSH で使用する SSH キーを生成します。

```
xxx_lab(config)#  crypto key generate rsa
The name for the keys will be: xxx_lab.xxx.cisco.com Choose the size of the key modulus in the range

of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a
few
minutes.
How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
xxx_lab(config)#
```

ステップ 4 デフォルトでは、vtys? transport は Telnet です。この場合、Telnet はディセーブルであり、SSH のみサポートされます。

```
xxx_lab(config)#line vty 0 4
xxx_lab(config-line)#transport input SSH
```

ステップ 5 SSH 認証用のユーザ名を作成し、ログイン認証をイネーブルにします。

```
xxx_lab(config)# username jsmith privilege 15 secret 0 p@ss3456
xxx_lab(config)#line vty 0 4
xxx_lab(config-line)# login local
```

ステップ 6 SSH を使用してデバイスへのリモート接続を確認します。

Telnet を使用してリモート コンソールから CLI にアクセスする方法

ここでは、Telnet を使用してリモート 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 （51 ページ）
- 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 （52 ページ）

Telnet を使用してルータ コンソールに接続するための準備

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』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
```

USB シリアル コンソール ポートから CLI にアクセスする方法

ルータに備わっている追加のシステム設定メカニズムであるタイプ B ミニポート USB シリアル コンソールは、タイプ B USB 対応ケーブルを使用したルータのリモート管理をサポートします。『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』の「Connecting to a Console Terminal or Modem」の項を参照してください。

キーボード ショートカットの使用方法

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 7: 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。

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 *8:* 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 *9*: 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。

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。

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 *10*：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`
`<0-2> GigabitEthernet interface number`
 	
`Router(config)# interface GigabitEthernet 1/?`
 	
`<0-4> Port Adapter number`
 	
`Router (config)# interface GigabitEthernet 1/3/?`
`<0-15> GigabitEthernet interface number`
 	
`Router (config)# interface GigabitEthernet 1/3/8?`
`. <0-3>`
`Router (config)# interface GigabitEthernet 1/3/8.0`
 	
`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。

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。

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。

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。

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。

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
     0 unknown protocol drops
GigabitEthernet0/0/1 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/2 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/3 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0 is up, line protocol is up
     0 unknown protocol drops
Loopback0 is up, line protocol is up
     0 unknown protocol drops
```

ルータの電源切断

ルータの電源スイッチをオフの位置にすることで、ルータをいつでも安全にオフにできます。ただし、NVRAM に対する設定の最後の WRITE 処理以降に加えた実行コンフィギュレーションへの変更は失われます。

ルータの電源をオフにする前に、スタートアップ後に必要な設定が保存されていることを確認します。copy running-config startup-config コマンドは、設定を NVRAM に保存します。ルータの電源を入れると、保存された設定でルータが開始されます。

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。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ソフトウェア イメージのセットを確認したり、ある機能が特定の Cisco IOS XE ソフトウェア イメージで使用可能かどうかを確認したりするには、Cisco Feature Navigator を使用するか、『Release Notes for Cisco IOS XE』を参照してください。

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。

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

以下の事項については、Cisco 4000 シリーズ ISR の『Release Notes』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。

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 タイムアウトの変更 （65 ページ）
- CLI セッションのロック （66 ページ）

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

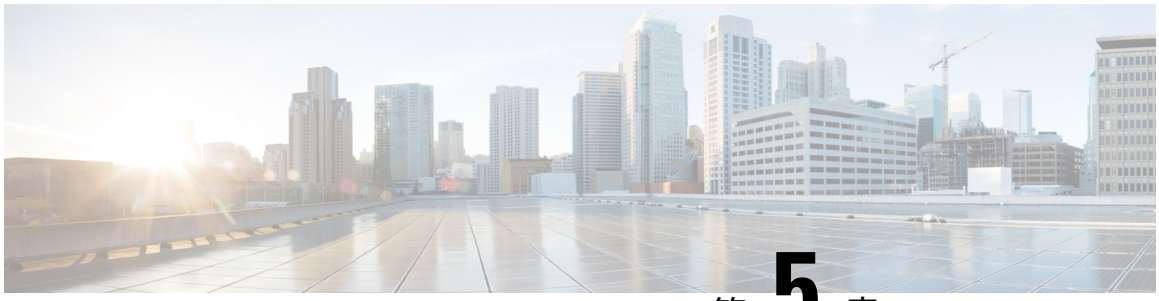
ステップ 3 **Router(config)# lockable**

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 5 章

スマートライセンス

この章では、Cisco スマート ライセンス クライアント機能の概要について説明し、製品の登録と承認を完了するために必要な複数のツールとプロセスについても説明します。

この章は、次の項で構成されています。

スマートライセンシングの概要

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- 簡単なアクティベーション：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- 管理の統合：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供します。
- ライセンスの柔軟性：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（http://software.cisco.com/）。

シスコライセンスの詳細な概要については、https://cisco.com/go/licensingguide を参照してください。

アクセスルータとエッジルータのスマートライセンス設定については、https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/smart-licensing/qsg/b_Smart_Licensing_QuickStart/b_Smart_Licensing_QuickStart_chapter_01.html を参照してください。

Cisco Smart Licensing クライアントの前提条件

- Smart Licensing クライアント機能を使用する前に、Call Home が有効になっていることを確認します。
- デバイスが Smart Licensing モードをサポートする Cisco IOS XE Everest 16.6.1 バージョンを実行していることを確認します。

Cisco Smart Licensing クライアントの制約事項

- Cisco 4000 シリーズ ISR プラットフォームでは、Cisco IOS XE リリース 16.6.1 以降、Cisco スマートライセンスの Cisco ONE スイートライセンス、テクノロジー パッケージ ライセンス、スループットライセンス、および HSECK9 ライセンスがサポートされます。

Cisco Smart Licensing クライアントの情報

Cisco Smart Licensing：概要

Smart Licensing には、お客様の注文をキャプチャし、Smart Call Home トランスポートゲートウェイを介してCisco Cloud License Service と通信する機能があります。さらに、Smart Call Home トランスポートゲートウェイは、目的とするシスコ製品のパフォーマンスとテクノロジーレベルに基づいて、製品の登録と承認を完了するのに役立ちます。Call Home の詳細については、*Call Home* を参照してください。

Smart Licensing のメリットは次のとおりです。

- Foundation スイートおよび Active Directory ユーザーとコンピュータ（ADUC）スイートを含む、Cisco IOS ソフトウェアライセンス（CISL）およびスマートラインセスモードでの CiscoONE スイートのサポート。
- 従来のライセンス（CSL）とスマートライセンスモードを切り替える機能。
- 4 つのソフトウェア ユニバーサル イメージ（NPE、NO-LI、NPE-NO-LI、および非 NPE イメージ）のサポート。

CSL から Smart Licensing への移行

Cisco Smart Licensing モデルでは、特別なソフトウェア キーまたはアップグレード ライセンス ファイルを使用せずに、ライセンス付き機能をアクティベートできます。新しい機能をアクティベートするには、適切な製品コマンドおよび設定を使用します。機能がアクティベートされます。 ソフトウェアのリブートは、製品の機能と要件によって変わるので必要だとは限りません。

同様に、高度な機能、パフォーマンス、および機能のダウングレードまたは削除を行うには、設定やコマンドを削除する必要があります。

上記アクションのいずれかが実行されると、ライセンスの状態の変更は次回同期時に Smart Software Manager で示され、適切なアクションが実行されます。

Cisco ONE スイート

Cisco ONE スイートは、お客様がインフラストラクチャ ソフトウェアを購入するための新しい方法です。Cisco ONE はデータセンター、ワイドエリア ネットワーク、およびローカルアクセス ネットワークに共通のお客様のシナリオに集中化された、簡素な購買モデルを提供します。

スマートライセンスによって、スマートライセンスの Cisco ONE スイートレベルのライセンス、IP ベース、拡張 IP サービス（AIS）、高度なエンタープライズサービス（AES）、機能ライセンスなどのイメージライセンス、およびスループットパフォーマンス、暗号化スループット、およびポートのライセンスがサポートされます。

Cisco ONE スイートについての詳細は、『Cisco ONE Suite』を参照してください。

Cisco Smart Licensing クライアントをアクティベートする方法

スマート ライセンスのイネーブル化

手順の概要

1. **enable**
2. **configure terminal**
3. **license smart enable**
4. **exit**
5. **write memory**
6. **show license all**

手順の詳細

	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	**license smart enable** 例：	デバイス上の Smart Licensing を有効にします。

	コマンドまたはアクション	目的
	`Device# license smart enable`	（注） スマート ライセンスを有効にすると、シスコ ソフトウェア ライセンス（CSL）およびすべてのライセンス コールは、スマート エージェントを通過します。 [no] でスマート ライセンスがすでに登録されている場合、スマート エージェントは 「license smart deregister」の操作を実行して Smart Licensing を無効化します。デバイスの CSL をアクティブにするには、デバイスをリロードします。
ステップ 4	**exit** 例： `Device# exit`	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。
ステップ 5	**write memory** 例： `Device# write memory`	NVRAM に実行コンフィギュレーションを保存します。
ステップ 6	**show license all** 例： `Device# show license all`	（任意）すべてのライセンスに関するサマリー情報を表示します。

スマートライセンスの無効化

手順の概要

1. **enable**
2. **configure terminal**
3. **no license smart enable**
4. **exit**
5. **write memory**
6. **reload**
7. **show license all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	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）。

	コマンドまたはアクション	目的
	`Device> enable`	
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	**no license smart enable** 例： `Device(config)# no license smart enable`	デバイス上の Smart Licensing を無効化します。 （注） スマート ライセンスを有効にすると、シスコ ソフトウェア ライセンス（CSL）およびすべてのライセンス コールは、スマート エージェントを通過します。[no] でスマート ライセンスがすでに登録されている場合、スマート エージェントは 「license smart deregister」 の操作を実行して Smart Licensing を無効化します。デバイスの CSL をアクティブにするには、デバイスをリロードします。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**write memory** 例： `Device# write memory`	NVRAM に実行コンフィギュレーションを保存します。
ステップ 6	**reload** 例： `Device# reload`	（任意）デバイスを再起動して、新しいフィーチャ セットをイネーブルにします。 （注） Cisco ONE スイートを設定した後でデバイスをリロードしていない場合はデバイスをリロードします。
ステップ 7	**show license all** 例： `Device# show license all`	（任意）すべてのライセンスに関するサマリー情報を表示します。

デバイス登録

手順の概要

1. **enable**
2. **license smart register idtoken** *idtoken* [**force**]
3. **license smart deregister**
4. **license smart renew** [**ID** | **auth**]

手順の詳細

	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	**license smart register idtoken** *idtoken* [**force**] 例： `Device# license smart register idtoken 123`	バックエンドのサーバーとデバイスと登録します。トークン ID は Smart Licensing サーバーの仮想 a/c から取得できます。 • **force**：デバイスが登録されているかどうかに関わらずデバイスを強制的に登録します。 （注） デバイスは Cisco サーバーにトークン ID を提供し、365 日間有効な「デバイス証明書」が返送されます。
ステップ 3	**license smart deregister** 例： `Device# license smart deregister`	バックエンドのサーバーからデバイスを登録解除します。
ステップ 4	**license smart renew** [**ID**	**auth**] 例： `Device# license smart renew ID`	（任意）手動で ID 認定または承認を更新します。 ライセンスブートレベル、ライセンス機能 hseck9、およびプラットフォーム ハードウェア スループット レベルの詳細については、『Smart Licensing Guide for Access and Edge Routers』を参照してください。

Cisco Smart Licensing クライアントのトラブルシューティング

Smart Licensing の有効化の問題をトラブルシューティングするにはデバイスで次のコマンドを使用します。

- **show version**
- **show running-config**

- **show license summary**
- **show license all**
- **show license tech support**
- **debug smart_lic error**
- **debug smart_lic trace**

Cisco Smart Licensing クライアントの設定例

例：すべてのライセンスに関するサマリー情報の表示

次に **show license all** コマンドを使用して、すべてのライセンスについての要約情報を表示する例を示します。

```
Device#show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
Status: REGISTERED
Smart Account: BU Production Test
Virtual Account: ISR4K
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Sep 04 15:40:03 2015 PDT
Last Renewal Attempt: None
Next Renewal Attempt: Mar 02 15:40:02 2016 PDT
Registration Expires: Sep 03 15:34:53 2016 PDT

License Authorization:
Status: AUTHORIZED on Sep 04 15:40:09 2015 PDT
Last Communication Attempt: SUCCEEDED on Sep 04 15:40:09 2015 PDT
Next Communication Attempt: Oct 04 15:40:08 2015 PDT
Communication Deadline: Dec 03 15:35:01 2015 PDT

License Usage
==============

ISR_4400_FoundationSuite (ISR_4400_FoundationSuite):
Description: Cisco ONE Foundation Perpetual License ISR 4400
Count: 1
Version: 1.0
Status: AUTHORIZED

ISR_4400_AdvancedUCSuite (ISR_4400_AdvancedUCSuite):
Description: Cisco ONE Advanced UC Perpetual License ISR 4400
Count: 1
Version: 1.0
Status: AUTHORIZED

ISR_4451_2G_Performance (ISR_4451_2G_Performance):
Description: Performance on Demand License for 4450 Series
Count: 1
Version: 1.0
Status: AUTHORIZED
```

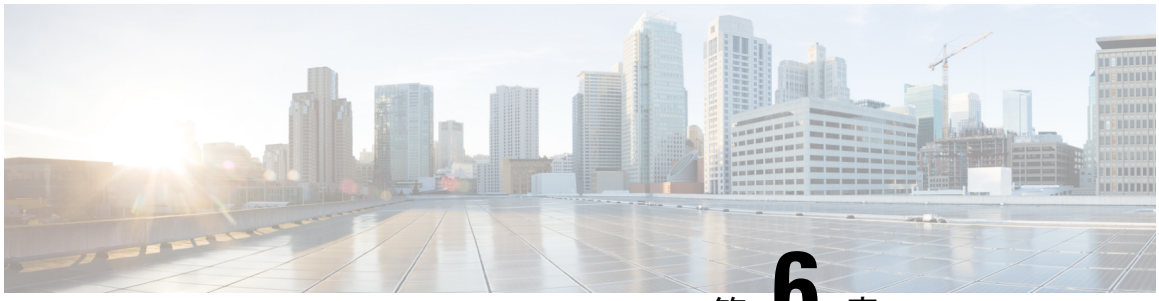
```
Product Information
====================
UDI: PID:ISR4451-X/K9,SN:FOC17042FJ9

Agent Version
=============
Smart Agent for Licensing: 1.4.0_rel/16
Component Versions: SA:(1_4_rel)1.0.15, SI:(dev22)1.2.6, CH:(dev5)1.0.32, PK:(dev18)1.0.17


Device#
```

例：Smart Licensing の有効化

次に、Cisco ONE スイートが有効になっているかどうかを確認するために **license smart enable** コマンドを使用する方法の例を示します。

（注） 次の例で表示される警告メッセージは、Cisco ISR G2 プラットフォームにのみ適用されます。Cisco 4000 シリーズ ISR プラットフォームの場合は、スマートライセンスを有効にしても警告メッセージは表示されません。

```
Device# license smart enable
Currently only Cisco ONE license suites are supported by Smart Licensing.
Please make sure your Cisco ONE suites are enabled before turning on Smart Licensing.
Any other licenses outside of Cisco ONE suites would be disabled and made unusable in
Smart Licensing.
If you have any questions, please get in touch with your Cisco representative before
using this mmode.
Please confirm Cisco ONE suites are enabled? [yes/no]: yes
```



第 6 章

Web ユーザーインターフェイスを使用したデバイスの管理

Web ユーザーインターフェイス（Web UI）は、組み込み GUI ベースのデバイス管理ツールです。デバイスをプロビジョニングしたり、デバイスの導入および管理性を簡素化したり、ユーザーエクスペリエンスを向上したりする機能を提供します。デフォルトのイメージが用意されているため、何かを有効化したりデバイスにライセンスをインストールしたりする必要はありません。Web UI を使用すれば、CLI の専門知識がなくても、設定を構築し、デバイスのモニタリングとトラブルシューティングを行うことができます。この章は、次の項で構成されています。

Web UI を使用した工場出荷時のデフォルト状態であるデバイスの設定

クイック セットアップ ウィザードを使用して、基本的なルータ設定を実行できます。ルータを設定するには、以下の手順を実行します。

始める前に

- Web UI にアクセスする前に、デバイスで基本設定を行う必要があります。

ステップ 1 シリアルケーブルの RJ-45 側をルータの RJ-45 コンソールポートに接続します。

ステップ 2 デバイスの初期設定ウィザードが表示された後、次のシステムメッセージがルータに表示されたら、「**No**」と入力してデバイスプロンプトを表示します。

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

ステップ 3 コンフィギュレーション モードで、次の設定パラメータを入力します。

```
!
ip dhcp pool WEBUIPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
username webui privilege 15 password cisco
!
interface gig 0/0/1
ip address 192.168.1.1 255.255.255.0
!
```

ステップ 4 イーサネットケーブルでデバイスとルータを接続し、gig 0/0/1 インターフェイスに接続します。

ステップ 5 システムを DHCP クライアントとして設定し、ルータの IP アドレスを自動的に取得します。

ステップ 6 ブラウザを起動し、ブラウザのアドレス行にデバイスの IP アドレスを入力します。セキュアな接続の場合は、「https://192.168.1.1/#/dayZeroRouting」と入力します。あまりセキュアではない接続の場合は、「http://192.168.1.1/#/dayZeroRouting」と入力します。

ステップ 7 デフォルトのユーザー名（webui）とデフォルトのパスワード（cisco）を入力します。

基本または詳細モード セットアップ ウィザードの使用

基本モードまたは詳細モードのセットアップを使用してルータを設定するには、次の手順を実行します。

ステップ 1 [Basic Mode] または [Advanced Mode] を選択し、[Go To Account Creation Page] をクリックします。

ステップ 2 ユーザ名とパスワードを入力します。確認のためにパスワードを再入力します。

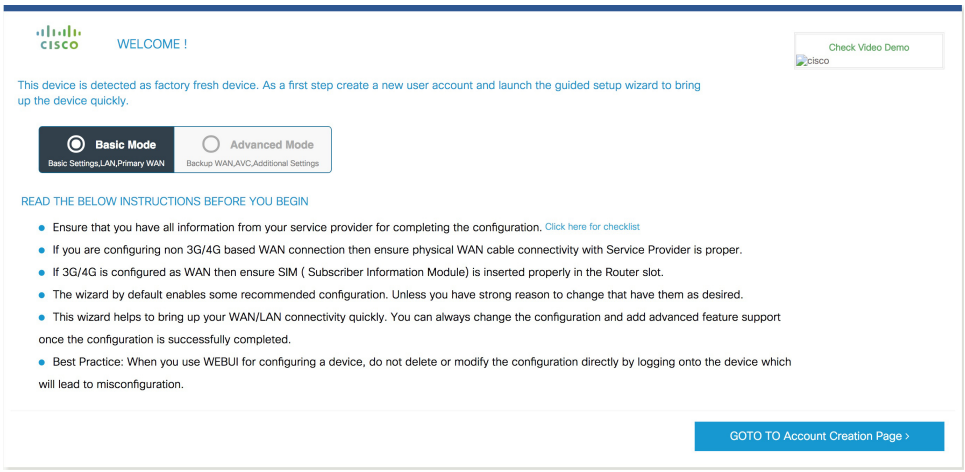
ステップ 3 [Create and Launch Wizard] をクリックします。

ステップ 4 デバイス名とドメイン名を入力します。

ステップ 5 [Time Zone] ドロップダウンリストから、適切なタイムゾーンを選択します。

ステップ 6 [Date and Time] ドロップダウンリストから、適切な日時モードを選択します。

ステップ 7 [LAN Settings] をクリックします。



LAN 設定を行います。

ステップ 1 [Web DHCP Pool/DHCP Pool] 名または [Create and Associate Access VLAN] オプションを選択します。

a) [Web DHCP Pool] を選択した場合は、次を指定します。

[Pool Name]：DGCP プール名を入力します。

[Network]：ネットワークアドレスおよびサブネットマスクを入力します。

b) [Create and Associate Access VLAN] オプションを選択した場合は、次を指定します。

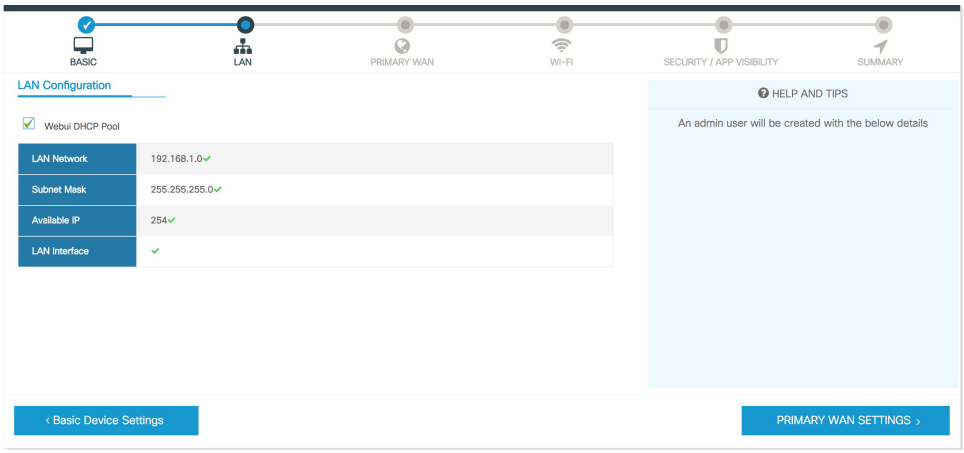
[Access VLAN]：アクセス VLAN の識別番号を入力します。指定できる範囲は 1 ～ 4094 です。

[Network]：VLAN の IP アドレスを入力します。

[Management Interfaces]：インターフェイスを選択し、右矢印と左矢印を使用して選択したリストボックスに移動します。ダブルクリックするかドラッグアンドドロップして、選択したリストボックスにインターフェイスを移動することもできます。

ステップ 2 [**Primary WAN Settings**] をクリックします。

プライマリ WAN 設定を行います。



プライマリ WAN 設定を行います。

ステップ 1 プライマリ WAN タイプを選択します。プライマリ WAN は、ルータがサポートする WAN のタイプに応じて、シリアル、3G/4G、イーサネット、またはブロードバンド（xDSL）を設定できます。

ステップ 2 ドロップダウン リストからインターフェイスを選択します。

ステップ 3 サービス プロバイダーから DNS サーバ情報を直接取得するには、[**Get DNS Server info directly from ISP**] チェックボックスをオンにします。プライマリ DNS とセカンダリ DNS は手動で入力することもできます。

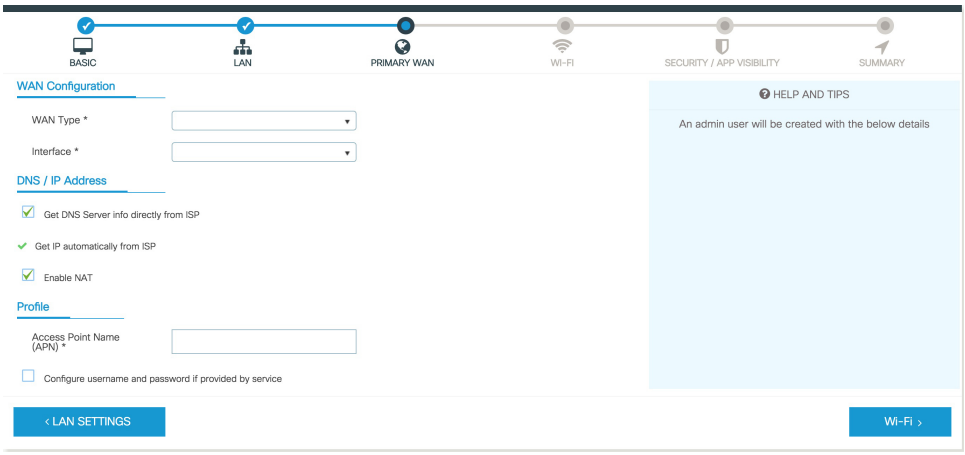
ステップ 4 [**Get IP automatically from ISP**] チェックボックスをオンにして、サービスプロバイダーから IP アドレス情報を直接取得します。IP アドレスおよびサブネット マスクを入力します。

ステップ 5 [**Enable NAT**] チェックボックスをオンにして、NAT を有効にします。NAT を有効にすることをお勧めします。

ステップ 6 [Enable PPPoE] チェックボックスをオンにして、PPPoE を有効にします。PPPoE を有効にする場合は、必要な認証モードを選択します。オプションは **PAP** と **CHAP** です。

ステップ 7 サービスプロバイダーから提供されたユーザー名とパスワードを入力します。

ステップ 8 [**Security/APP Visibility WAN Settings**] をクリックします。



セカンダリ WAN 設定を行います。

詳細設定では、セカンダリ WAN 接続を設定する必要があります。

ステップ 1 セカンダリ WAN タイプを選択します。ルータがサポートする WAN のタイプに応じて、シリアル、3G/4G、イーサネット、またはブロードバンド（xDSL）をセカンダリ WAN として設定できます。

ステップ 2 ドロップダウン リストからインターフェイスを選択します。

ステップ 3 サービス プロバイダーから DNS サーバ情報を直接取得するには、[**Get DNS Server info directly from ISP**] チェックボックスをオンにします。プライマリ DNS とセカンダリ DNS は手動で入力することもできます。

ステップ 4 [**Get IP automatically from ISP**] チェックボックスをオンにして、サービス プロバイダーから IP アドレス情報を直接取得します。IP アドレスおよびサブネット マスクを入力します。

ステップ 5 [**Enable NAT**] チェックボックスをオンにして、NAT を有効にします。NAT を有効にすることをお勧めします。

ステップ 6 [Enable PPPoE] チェックボックスをオンにして、PPPoE を有効にします。PPPoE を有効にする場合は、必要な認証モードを選択します。オプションは **PAP** と **CHAP** です。

ステップ 7 サービスプロバイダーから提供されたユーザー名とパスワードを入力します。

ステップ 8 [**Security/APP Visibility WAN Settings**] をクリックします。

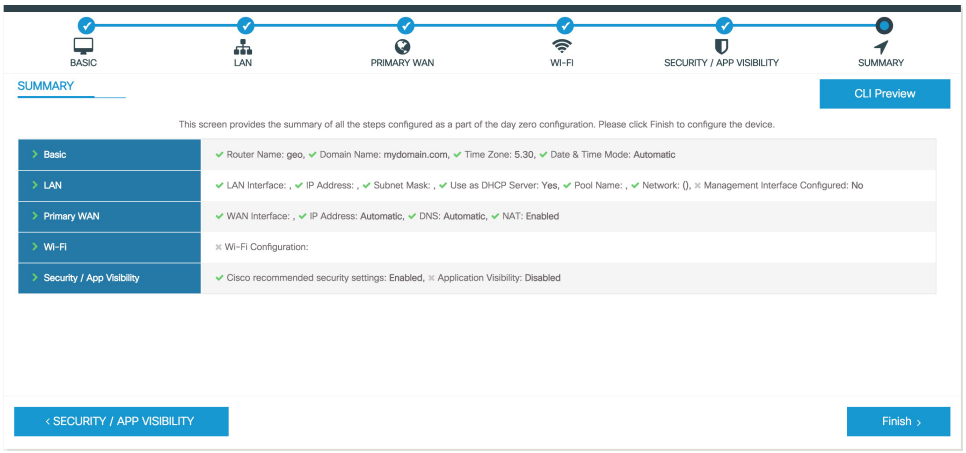
セキュリティ設定の構成

ステップ 1 すべてのパスワードがプレーンテキストで表示されないようにするには、[**Enable Recommended Settings**)] チェックボックスをオンにします。パスワードは暗号化されます。

ステップ 2 [**Day 0 Config Summary**] をクリックします。

ステップ 3 設定をプレビューするには、[CLI preview] をクリックします。

ステップ 4 [Finish] をクリックして、デイゼロセットアップを完了します。



Day One 設定に Web ユーザ インターフェースを使用

Web ユーザ インターフェイスの設定：

始める前に

- Web UI 情報をエラーなしで表示するには、デバイスに少なくとも 30 の VTY 回線を設定する必要があります。
- Web UI の設定画面にアクセスするには、権限 15 を持つユーザが必要です。権限が 15 未満の場合は、Web UI でダッシュボードとモニタリング画面にのみアクセスできます。

  ユーザアカウントを作成するには、**username** <username> **privilege** <privilege> **password 0** <passwordtext> を使用します。

```
Device #configure terminal
Device (config)# username <username> privilege <privilege> password 0
<passwordtext>
```

ステップ 1 HTTP サーバを設定します。デフォルトでは、HTTP サーバの設定がデバイス上に存在する必要があります。**ip http server** コマンドと **ip http secure-server** コマンドが実行コンフィギュレーションに存在するかをチェックして、設定を確認します。

```
Device #configure terminal
Device (config)#ip http server
Device (config)#ip http secure-server
```

ステップ 2 Web UI にログインするための認証オプションを設定します。次のいずれかの認証方式を使用できます。

a) ローカル データベースを使用して認証できます。Web UI 認証にローカル データベースを使用するには、**ip http authentication local** コマンドが実行コンフィギュレーションに含まれていることを確認しま

す。このコマンドは、デバイスで事前に設定されています。コマンドが存在しない場合は、次の例に示すようにデバイスを設定します。

```
Device #configure terminal
 Device (config)#ip http authentication local
```

b) AAA オプションを使用して認証します。Web UI に AAA 認証を使用するには、デバイスで「ip http authentication aaa」を設定していることを確認します。また、必要な AAA サーバ設定がデバイスに存在することを確認します。

```
Device #configure terminal
Device (config)#ip http authentication local
```

ステップ 3 ブラウザを起動します。アドレス バーに、デバイスの IP アドレスを入力します。セキュアな接続の場合は、「https://ip-address」と入力します。

ステップ 4 デフォルトのユーザー名（webui）とデフォルトのパスワード（cisco）を入力します。

ステップ 5 [Log In] をクリックします。

WebUIを使用したデバイスのプラグアンドプレイ（PnP）導入準備の監視とトラブルシューティング

表 *11 :* 機能の履歴

機能名	リリース情報	説明
WebUI を使用したデバイスの PnP 導入準備の監視とトラブルシューティング	Cisco IOS XE リリース 17.5.1a	PnP 導入準備で WebUI を使用して、デイゼロデバイスの導入準備を監視およびトラブルシューティングできるようになりました。自動 PnP 導入準備が失敗した場合は、デバイスの導入準備を手動で実行できます。

ゼロタッチプロビジョニング（ZTP）またはプラグアンドプレイ（PnP）プロセスを使用して、Cisco vManage に対するデバイスの導入準備を自動的に実行できます。このセクションでは、PnP メソッドを使用してデバイスの導入準備をモニタおよびトラブルシューティングする手順について説明します。WebUI のこの機能を使用すると、PnP 導入準備プロセスをモニタおよびトラブルシューティングしたり、そのリアルタイムステータスを確認したりすることもできます。この導入準備が停止または失敗した場合は、プロセスを終了し、デバイスの導入準備を手動で行うことができます。

前提条件

- WebUI を実行しているデバイス（Web ブラウザを実行できるコンピュータ）と導入準備しているデバイスは、デバイスの L2 スイッチポート（NIM）経由で接続する必要があります。
- デバイスの DHCP クライアント ID を文字列「webui」に設定する必要があります。
- デバイスが WebUI での Cisco SD-WAN デイゼロデバイスの導入準備をサポートしている必要があります。

デバイスの PnP 導入準備のトラブルシューティング

コントローラモードでの PnP によるデバイスの導入準備をトラブルシューティングするには、次の手順を実行します。

1. WebUI でコントローラモードを開始します。

   - 自律モードからコントローラモードへの切り替え：

     通常、デバイスを初めて起動したときは、自律モードになります。URL https://192.168.1.1/webui/ に移動し、デフォルトのログイン情報（webui/cisco）を使用してログインします。デバイスが WebUI での Cisco SD-WAN デイゼロデバイスの導入準備をサポートしている場合は、[Controller Mode] を選択してコントローラモードに切り替えることができます。続行するかどうかを確認するダイアログボックスが表示されます。**[はい（Yes）]**をクリックします。デバイスがリロードされ、コントローラモードに切り替えられます。

   - コントローラモードでのデバイスの起動：

     デバイスがすでにコントローラモードになっている場合は、モードを変更する必要はありません。https://192.168.1.1 または https://192.168.1.1/webui に移動します。デバイスが WebUI での Cisco SD-WAN デイゼロデバイスの導入準備をサポートしている場合、URL は https://192.168.1.1/ciscosdwan/ にリダイレクトされ、Cisco IOS XE SD-WAN デバイスのデフォルトのログイン情報（admin/admin）を使用してログインできます。

（注） PnP 導入準備の時点で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場合、WebUI はサポートされるデバイスにおいてデフォルトで有効になります。

2. [Welcome to Cisco SDWAN Onboarding Wizard] ページで、[Reset Default Password] をクリックします。

（注） デイゼロデバイスのデフォルトパスワードが脆弱です。したがって、安全なログインのため、WebUI でデバイスに初めてログインするときにパスワードをリセットする必要があります。デバイスが正常に導入準備されると、WebUI 設定は自動的に削除されます。Cisco vManage 上のデバイスのテンプレート設定に WebUI 設定があるまれなケースでは、デバイスの導入準備が成功した後でも削除されません。

3. デバイスのハードウェアとソフトウェアの詳細情報ページにリダイレクトされます。パスワードを入力して [Submit] をクリックします。

4. 次のページには、導入準備の進行状況が表示され、PnP Connect ポータルおよび Cisco SD-WAN コントローラのさまざまなコンポーネントのステータスが一覧表示されます。PnP IPv4 コンポーネントに障害が発生した場合、この障害は、デバイスの PnP 導入準備が失敗したことを示しています。

   導入準備プロセスのログを表示およびダウンロードするには、[SDWAN Onboarding Progress] バーの右側にある情報アイコンをクリックします。

5. 自動 PnP 導入準備が失敗した場合は、[Terminate Automated Onboarding] をクリックします。この操作により、デバイスを手動で導入準備できるようになります。

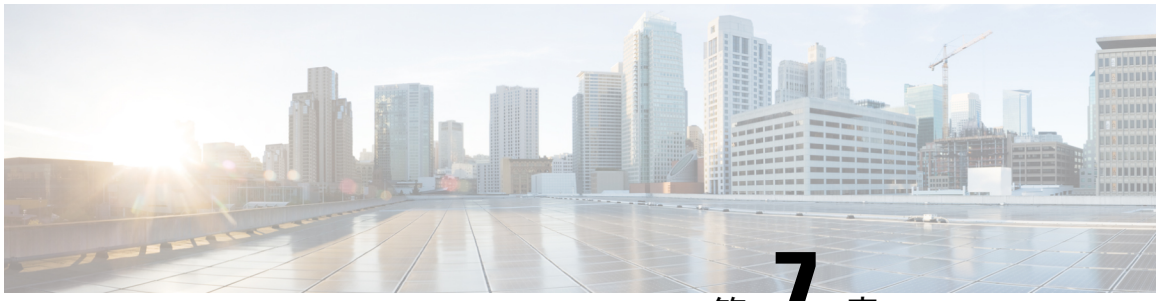
6. ダイアログボックスが表示されます。終了を続行するには、[Yes] をクリックします。終了の完了までに数分かかる場合があります。

7. [Bootstrap Configuration] ページで、[Select File] をクリックし、デバイスのブートストラップファイルを選択します。このファイルは、一般的なブートストラップファイル（共通プラットフォーム固有のファイル）と、Cisco vManage からダウンロード可能なフル設定ブートストラップファイルのいずれかです。このファイルには、vBond 番号、UUID、WAN インターフェイス、ルート CA、設定などの詳細情報が含まれている必要があります。

8. [Upload] をクリックします。

9. ファイルが正常にアップロードされたら、[Submit] をクリックします。

10. [SDWAN Onboarding Progress] ページに、Cisco SD-WAN コントローラのステータスが再度表示されます。[Controller Connection History] テーブルを開くには、[SDWAN Control Connections] バーの右側にある情報アイコンをクリックします。このテーブルでは、導入準備対象デバイスの状態を確認できます。導入準備が完了すると、デバイスの状態が [connect] に変わります。



第 7 章

コンソール ポート、Telnet、および SSH の処理

この章は、次の項で構成されています。

コンソール ポート、Telnet、および SSH に関する注意事項と制約事項

- トランスポートマップがイーサネット管理インターフェイスに適用されるとき、トランスポート マップでの Telnet および Secure Shell（SSH）設定は、他のすべての Telnet および SSH 設定をオーバーライドします。
- イーサネット管理インターフェイスを開始するユーザの認証には、ローカルユーザ名とパスワードだけを使用できます。持続性 Telnet または持続性 SSH を使用してイーサネット管理インターフェイス経由でルータにアクセスするユーザは、AAA 認証を使用できません。
- アクティブな Telnet または SSH セッションがあるイーサネット管理インターフェイスにトランスポート マップを適用すると、アクティブ セッションが切断される可能性があります。しかし、インターフェイスからトランスポートマップを削除すると、アクティブな Telnet セッションまたは SSH セッションの接続は切断されません。

- 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。

コンソール ポートの概要

ルータ上のコンソール ポートは、EIA/TIA-232 非同期、フロー制御なしのシリアル接続で、コネクタは RJ-45 コネクタを使用します。コンソール ポートはルータへのアクセスに使用され、ルート プロセッサの前面パネルに位置しています。

コンソール ポートを使用したルータへのアクセスについては、Cisco IOS XE ソフトウェアの使用 （49 ページ）を参照してください。

コンソール ポートの処理について

コンソール ポートを使用してルータにアクセスする場合は、自動的に Cisco IOS Command-Line Interface （CLI）へ誘導されます。

コンソールポートを介したルータへのアクセス試行で、CLI に接続する前にブレーク信号を送った場合（**Ctrl-C** または **Ctrl-Shift-6** を押すか、Telnet プロンプトで **send break** コマンドを入力）、非 RPIOS サブパッケージにアクセス可能であれば、診断モードに誘導されます。これらの設定を変更するには、コンソール ポートに設定したトランスポート マップをコンソール インターフェイスに適用します。

Telnet および SSH の概要

ルータ上の Telnet および SSH を、他のシスコ プラットフォームの Telnet および SSH と同様に設定して操作することができます。従来の Telnet については、『Cisco IOS Terminal Services Command Reference, Release 12.2』の回線コマンドを参照してください。AAA 認証方式の詳細については、「Authentication Commands」の章の回線コマンドを参照してください。

従来の SSH の設定については、『Cisco IOS Terminal Services Command Reference, Release 12.2』の「Configuring Secure Shell」の章を参照してください。

ルータでは、持続性 Telnet および持続性 SSH を使用することで、ユーザが Telnet や SSH を使って管理イーサネット ポート経由でルータにアクセスするとき、ネットワーク管理者は着信トラフィックの処理をより明確に定義できます。特に、持続性 Telnet および持続性 SSH では、Cisco IOS プロセスに障害が発生しても、Telnet または SSH を使用してイーサネット管理ポート経由でアクセスできるようにルータを設定できるため、より安定したネットワーク アクセスが実現します。

持続性 Telnet および持続性 SSH の概要

従来のシスコ ルータでは、Cisco IOS ソフトウェアに障害が発生した場合、Telnet または SSH を使用してルータにアクセスすることは不可能でした。従来のシスコ ルータで Cisco IOS の障害が発生した場合、ルータにアクセスする方法はコンソール ポートを介する方法しかありません。同様に、持続性 Telnet や持続性 SSH を使用しないルータ上のすべてのアクティブな Cisco IOS プロセスで障害が発生した場合は、コンソール ポート経由でしかルータにアクセスできません。

ただし、持続性 Telnet や持続性 SSH を使用すると、イーサネット管理インターフェイスの着信 Telnet トラフィックまたは SSH トラフィックの処理を定義するトランスポート マップを設定できます。多くの設定オプションがある中で、トランスポートマップを設定することで、すべてのトラフィックを Cisco IOS CLI や診断モードに転送できます。あるいは、Cisco IOS VTY 回線が使用可能になるのを待っているユーザがブレーク信号を送信した場合に、IOS VTY 回線が使用可能になるまで待機してからユーザを診断モードに転送することもできます。ユーザが Telnet または SSH を使って診断モードにアクセスする場合、アクティブな Cisco IOS プロセスがなくても、この Telnet 接続または SSH 接続は使用可能です。つまり、持続性 Telnet および持続性 SSH には、Cisco IOS プロセスが非アクティブな場合に診断モード経由でルータにアクセスできる機能が導入されています。診断モードについては、「Cisco IOS XE ソフトウェアの使用」を参照してください。持続性 Telnet または持続性 SSH トランスポート マップを使用して設定できるオプションについては、持続性 Telnet の設定 （89 ページ）および持続性 SSH の設定 （92 ページ）を参照してください。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **transport-map type console** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. （任意） **banner** [**diagnostic** | **wait**] *banner-message*
6. **exit**
7. **transport type console** *console-line-number* **input** *transport-map-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	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）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**configure terminal** 例： `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 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。

	コマンドまたはアクション	目的
		• *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。
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
```

持続性 Telnet の設定

ルータ上の Cisco IOS vty 回線にアクセスする持続性 Telnet の場合、vty 回線用にローカルログイン認証が設定されている必要があります（回線コンフィギュレーション モードの **login** コマンド）。ローカル ログイン認証が設定されていない場合、ユーザは、トランスポート マップが適用された管理イーサネット インターフェイス への Telnet 接続を使用して Cisco IOS にアクセスできません。ただし、この場合でも、診断モードにはアクセスできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **transport-map type persistent telnet** *transport-map-name*

4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. （任意） **banner** [**diagnostic** | **wait**] *banner-message*
6. **transport interface gigabitethernet 0**
7. **exit**
8. **transport type persistent telnetinput** *transport-map-name*

手順の詳細

	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： `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 3	**transport-map type persistent telnet** *transport-map-name* 例： `Router(config)# transport-map type persistent telnet telnethandler`	持続性 Telnet 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`	このトランスポート マップを使用して持続性 Telnet 接続を処理する方法を指定します。 • **allow**：Telnet 接続は、Cisco IOS vty 回線が使用可能になるのを待機し、割り込みがあるとルータとの接続を終了します。 • **allow interruptible**：Telnet 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、ユーザーは Cisco IOS vty 回線が使用可能になるのを待機している Telnet 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**：Telnet 接続はただちに診断モードを開始します。

	コマンドまたはアクション	目的
		• **none disconnect**：Telnet 接続は Cisco IOS vty 回線を待機せず、診断モードを開始しません。そのため、Cisco IOS ソフトウェアで vty 回線が即時に使用可能にならなければ、すべての Telnet 接続が拒否されます。

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)#`
		（任意）診断モードを開始しているユーザ、または持続性 Telnet 設定によって 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**：持続性 Telnet 設定により、診断モードに導かれたユーザー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**：vty 回線が使用可能になるのを待機しているユーザー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。

ステップ 6	**transport interface gigabitethernet 0** 例： `Router(config-tmap)# transport interface gigabitethernet 0`	管理イーサネットインターフェイス（インターフェイス gigabitethernet 0）に、トランスポート マップ設定を適用します。 持続性 Telnet は、ルータ上の管理イーサネットインターフェイスだけに適用可能です。管理イーサネット インターフェイスにトランスポート マップを適用する前に、この手順を実行する必要があります。
ステップ 7	**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 8	**transport type persistent telnetinput** *transport-map-name* 例： `Router(config)# transport type persistent telnet input telnethandler`	トランスポートマップで定義された設定を管理イーサネット 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 persistent telnet** 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

次の例では、トランスポートマップの設定によって、すべての Telnet 接続は Cisco IOS XE vty 回線が使用可能になるまで待機した後でルータに接続します。その間、ユーザーはこのプロセスに割り込みを行って、診断モードを開始できます。このような設定が管理イーサネット インターフェイス（**interface gigabitethernet 0**）に適用されます。

また、診断バナーと待機バナーも設定されます。

transport type persistent telnet input コマンドが入力され、持続性 Telnet がイネーブルになると、トランスポートマップがインターフェイスに適用されます。

```
Router(config)# transport-map type persistent telnet telnethandler
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 IOS Process--
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

持続性 SSH の設定

このタスクでは、ルータで持続性 SSH を設定する方法を説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **transport-map type persistent ssh** *transport-map-name*
4. **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]
5. **rsa keypair-name** *rsa-keypair-name*
6. （任意） **authentication-retries** *number-of-retries*
7. （任意） **banner** [**diagnostic** | **wait**] *banner-message*
8. （任意） **time-out** *timeout-interval*
9. **transport interface gigabitethernet 0**
10. **exit**
11. **transport type persistent ssh input** *transport-map-name*

手順の詳細

	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： `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 3	**transport-map type persistent ssh** *transport-map-name* 例： `Router(config)# transport-map type persistent telnet telnethandler`	持続性 SSH 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 interruptible`	持続性 SSH 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**：SSH 接続は、Cisco IOS VTY 回線が使用可能になるのを待機し、割り込みがあるとルータとの接続を終了します。 • **allow interruptible**：SSH 接続は VTY 回線が使用可能になるのを待機します。また、ユーザーは、VTY 回線が使用可能になるのを待機しているSSH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**：SSH 接続はただちに診断モードを開始します。 • **none disconnect**：SSH 接続は VTY 回線を待機せず、診断モードを開始しません。したがって、VTY 回線が即時に利用可能にならない場合、すべての SSH 接続が拒否されます。

	コマンドまたはアクション	目的
ステップ 5	**rsa keypair-name** *rsa-keypair-name* 例： `Router(config)# rsa keypair-name sshkeys`	持続性 SSH 接続に使用される Rivest, Shamir, Adelman（RSA）キーペアに名前を付けます。 持続性 SSH 接続では、トランスポート マップ コンフィギュレーション モードでこのコマンドを使用して、RSA キーペアの名前を定義する必要があります。ルータの他のコマンド（**ip ssh rsa keypair-name** コマンドを使用するなど）で定義された RSA キーペアの定義は、持続性 SSH 接続に適用されません。 デフォルトでは *rsa-keypair-name* は定義されていません。
ステップ 6	（任意） **authentication-retries** *number-of-retries* 例： `Router(config-tmap)# authentication-retries 4`	（任意）接続をドロップするまでの認証リトライ数を指定します。 デフォルトの *number-of-retries* は、3 です。

ステップ 7	（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)#`
		（任意）診断モードを開始しているユーザ、または持続性 SSH 設定によって 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**：持続性 SSH 設定によって診断モードに誘導されたユーザーに表示されるバナーメッセージを作成します。
		• **wait**：VTY 回線が使用可能になるのを待機しているユーザー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。

ステップ 8	（任意） **time-out** *timeout-interval* 例： `Router(config-tmap)# time-out 30`	（任意）SSH タイムアウト インターバル（秒）を指定します。 デフォルトの *timeout-interval* は、120 秒です。
ステップ 9	**transport interface gigabitethernet 0** 例： `Router(config-tmap)# transport interface gigabitethernet 0`	イーサネット管理インターフェイス（interface gigabitethernet 0）に、トランスポート マップ設定を適用します。 持続性 SSH は、ルータのイーサネット管理インターフェイスだけに適用可能です。

	コマンドまたはアクション	目的
ステップ 10	**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 11	**transport type persistent ssh input** *transport-map-name* 例： `Router(config)# transport type persistent ssh input sshhandler`	トランスポート マップで定義された設定をイーサネット管理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 persistent ssh** 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

次の例では、トランスポート マップの設定によってすべての SSH 接続が VTY 回線のアクティブ化を待機した後で、設定対象のルータに接続します。このトランスポート マップ設定はイーサネット管理インターフェイス（インターフェイス gigabitethernet 0）に適用されます。RSA キーペアには、`sshkeys` という名前が付けられています。

この例では、持続性 SSH の設定に必要なコマンドだけを使用しています。

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
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 IOS Process--
X
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent telnet input telnethandler
```

次の例では、トランスポート マップの設定により、SSH 経由でイーサネット管理ポートへのアクセスを試みるユーザに次の設定が適用されます。

- SSH ユーザは VTY 回線がアクティブになるのを待機しますが、VTY 回線を介した Cisco IOS ソフトウェアへのアクセス試行が中断されると、診断モードを開始します。
- RSA キー ペアの名前は sshkeys です。
- この接続により、1 回の認証リトライが許可されます。
- このトランスポートマップによる SSH 処理の結果として診断モードが開始されると、バナー `--Welcome to Diagnostic Mode--` が表示されます。

- 接続が VTY 回線のアクティブ化を待機している場合、バナー `--Waiting for vty line--` が表示されます。
- **transport type persistent ssh input** コマンドが入力され、持続性 SSH が有効になると、トランスポートマップがインターフェイスに適用されます。

```
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# authentication-retries 1
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 vty line--
X
Router(config-tmap)# time-out 30
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
```

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** | **persistent** [**ssh** | **telnet**]]]

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`）、持続性 SSH（`sshhandler`）、持続性 Telnet トランスポート（`telnethandler`））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


Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:
Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: telnethandling1
Type: Persistent Telnet Transport

Connection:
Wait option: Wait Allow


Router# show transport-map type console
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 persistent ssh
Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Router# show transport-map type persistent telnet
Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: telnethandling1
Type: Persistent Telnet Transport

Connection:
Wait option: Wait Allow


Router# show transport-map name telnethandler
Transport Map:
Name: telnethandler
Type: Persistent Telnet Transport

Interface:
GigabitEthernet0
```

```
Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS process

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map name consolehandler
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 name sshhandler
Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys

Router#
```

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

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait
Shell banner:
Wait banner :

Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :
```

例

次に、SSH 用の新しいトランスポートマップが設定される前と後の両方で発行される **platform software configuration access policy** コマンドの例を示します。設定時に、持続性 SSH トランスポート マップの接続ポリシーとバナーが設定され、SSH のトランスポート マップがイネーブル化されます。

```
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 :

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
```

```
Enter TEXT message. End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 0
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
Router(config)# exit

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 with interrupt
Shell banner:
Welcome to Diag Mode

Wait banner :
Waiting for IOS


Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :
```

モデム接続用の補助ポートの設定

Cisco 4000 シリーズ ISR では、ルータの補助ポートにモデムを接続して、EXEC ダイヤルイン接続を使用できます。モデムを補助ポートに接続すると、リモートユーザはルータにダイヤルインして設定できます。補助ポートでモデムを設定するには、次の手順を実行します。

ステップ 1 アダプタ ケーブルの RJ-45 側をルータの黒い AUX ポートに接続します

ステップ 2 AUX ポートの非同期インターフェイスを確認するには、**show line** コマンドを使用します。

```
Router# show  line

 Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*     0 CTY              -    -    -  - -   0   0   0/0    -
      1 AUX   9600/9600 -    -    -  - -   0   0   0/0    -
      2 VTY              -    -    -  - -   0   0   0/0    -
      3 VTY              -    -    -  - -   0   0   0/0    -
      4 VTY              -    -    -  - -   0   0   0/0    -
      5 VTY              -     -   -  - -   0   0   0/0    -
```

```
   6 VTY              -    -  -  - -   0   0   0/0    -
```

ステップ 3 ルータの AUX 回線を設定するには、次のコマンドを使用します。

```
Router(config)# line 1

Router(config-line)#modem inOut
Router(config-line)#modem autoconfigure type usr_sportster
Router(config-line)#speed 115200  [Speed to be set according to the modem manual]
Router(config-line)#stopbits 1 [Stopbits to be set according to the modem manual]
Router(config-line)#transport input all
Router(config-line)#flowcontrol hardware [flowcontrol to be set according to the modem manual]
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#end
Router(config)#enable password lab
```

ステップ 4 モデムでリバース Telnet 方式を使用して、モデムの接続と設定文字列を確認します。

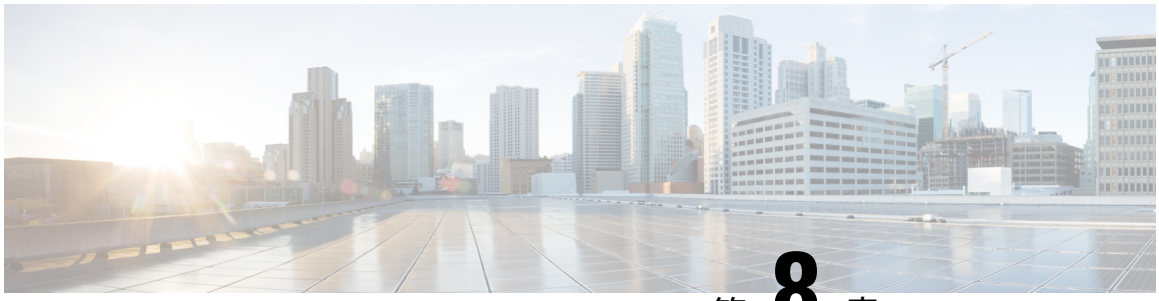
```
Router(config)#int loopback 0
Router(config-if)#ip add 192.0.2.1 255.255.255.0
Router(config-if)#end
Router#telnet 192.0.2.1 2001
Trying 192.0.2.1, 2001 ... Open

User Access Verification

Password: <enter the password given under line configuration>

at    <<<=== Modem command
OK  <<<=== This OK indicates that the modem is connected successully to the AUX port.
```

ステップ 5 アナログ電話を使用して、電話回線がアクティブで、正常に機能していることを確認します。次に、アナログ電話回線をモデムに接続します。

ステップ 6 別のデバイス（PC）からルータへの EXEC モデムコールを開始して、モデム接続をテストします。

ステップ 7 接続が確立されると、ダイヤルインクライアントにパスワードの入力が求められます。正しいパスワードを入力してください。

注：このパスワードは、補助ポート回線で設定されているパスワードと一致する必要があります。



第 8 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。

概要

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。

- 統合パッケージで実行するルータの管理および設定 （121 ページ） ：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 （126ページ） ：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。

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。ROMMONの詳細については、『Upgrading Field-Programmable Hardware Devices for Cisco 4000 Series ISRs』ガイドの「ROM Monitor Overview and Basic Procedures」セクションを参照してください。

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。

ROMMONの互換性マトリクス

次の表に、各 ROMMON リリースでサポートされている Cisco 4000 シリーズ サービス統合型ルータに関する情報を示します。

表 *12 : Cisco 4000* シリーズ サービス統合型ルータでサポートされている *ROMMON* リリース

プラットフォーム	16.2(1r)	16.2(2r)	16.4(3r)	16.7(3r)	16.7(4r)	16.7(5r)	16.8(1r)	16.9(1r)	16.12(1r)	16.12(2r)	17.6.1
Cisco 4221 ISR	—	—	対応	対応	対応	対応	—	対応	対応	対応	対応
Cisco 4321 ISR	対応	対応	対応	対応	対応	対応	—	対応	対応	対応	対応
Cisco 4331 ISR	対応	対応	対応	対応	対応	対応	—	対応	対応	対応	対応
Cisco 4351 ISR	対応	対応	対応	対応	対応	対応	—	対応	対応	対応	対応

プラットフォーム	16.2(1r)	16.2(2r)	16.4(3r)	16.7(3r)	16.7(4r)	16.7(5r)	16.8(1r)	16.9(1r)	16.12(1r)	16.12(2r)	17.6.1
Cisco 4431 ISR	あり	—	—	—	対応	対応	—	—	—	対応	対応
Cisco 4451 ISR	あり	—	—	—	対応	対応	—	—	—	対応	対応
Cisco 4461 ISR	—	—	—	—	—	—	—	対応	対応	対応	対応

（注） Cisco IOS XE 3.x から 16.x イメージにアップグレードする場合は、最初に ROMMON リリースを 16.7(5r) ROMMON リリースにアップグレードする必要があります。IOS XE 16.x イメージに基づいて 16.7(5r) ROMMON リリースにアップグレードした後、ROMMON リリースを以降の ROMMON リリースに自動アップグレードできます。

（注） ROMMON リリース 16.9(1r) は、Cisco BIOS Protection をサポートしている最初のリリースです。デバイスが 16.9(1r) ROMMON リリースにアップグレードされた後、ROMMON リリースを 16.9(1r) より前のリリースにダウングレードすることはできません。今後の ROMMON リリースはすべて、16.9(1r) リリースにダウングレードできます。また、プラットフォームに 16.9(1r) 以降のリリースがインストールされている場合は、IOS XE 16.9.1 以降のリリースまたは SD-WAN 16.11.1 以降のリリースをアップグレードに使用する必要があります。

（注） IOS XE リリース 17.1.x ～ 17.5.x の ROMMON イメージは、リリース 16.12(2r) に対応しています。

（注） Cisco IOS XE リリース 17.6.1 以降、ROMMON イメージは、スタンドアロンパッケージとしてリリースされず、IOS XE イメージとともにパッケージ化されます。17.6.1 ROMMON は、製造日が 2535 以降のデバイスでのみ使用されます。デバイスの製造日は、CLI コマンドの **show license udi** を使用して表示できます。次に例を示します。

```
elixir_p1b_11#show  license udi
 UDI: PID:C1131X-8PWB, SN: FGL2451L5MJ
```

この例のデバイスの製造日は 2451 です。

サポートされている最小 ROMMON リリース

次の表に、Cisco IOS XE 16.x..x リリースでサポートされている最小 ROMMON リリースを示します。

表 *13 : Cisco IOS XE 16.xx* リリースでサポートされている最小 *ROMMON* リリース

Cisco IOS XE リリース	Cisco 4321 ISR	Cisco 4321 ISR	Cisco 4331 ISR	Cisco 4351 ISR	Cisco 4431 ISR	Cisco 4451 ISR	Cisco 4461 ISR
Cisco IOS XE 16.3.x	—	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	—
Cisco IOS XE 16.4.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	—
Cisco IOS XE 16.5.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	—
Cisco IOS XE 16.6.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	—
Cisco IOS XE 16.7.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	—
Cisco IOS XE 16.8.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	—
Cisco IOS XE 16.9.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	16.9(1r)
Cisco IOS XE 16.10.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	16.9(1r)
Cisco IOS XE 16.11.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	16.9(1r)
Cisco IOS XE 16.12.x	16.7(4r)	16.7(3r)	16.7(3r)	16.7(3r)	16.7(4r)	16.7(4r)	16.9(1r)

Cisco IOS XE リリース	Cisco 4321 ISR	Cisco 4321 ISR	Cisco 4331 ISR	Cisco 4351 ISR	Cisco 4431 ISR	Cisco 4451 ISR	Cisco 4461 ISR
Cisco IOS XE 17.1.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.2.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.3.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.4.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.5.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.6.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)

（注） 製造日が2535以降のデバイスの場合、サポートされている最小ROMMONバージョンは17.6.1です。これらのデバイスは、それより古いROMMONバージョンにダウングレードできません。

推奨 ROMMON リリース

次の表に、各 Cisco IOS XE 16.xx リリースのルーティング プラットフォームに推奨される ROMMON リリースを示します。

表 *14 : Cisco IOS XE 16.xx* リリースの推奨 *ROMMON* リリース

Cisco IOS XE リリース	Cisco 4321 ISR	Cisco 4321 ISR	Cisco 4331 ISR	Cisco 4351 ISR	Cisco 4431 ISR	Cisco 4451 ISR	Cisco 4461 ISR
Cisco IOS XE 16.3.x	—	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	—
Cisco IOS XE 16.4.x	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	—
Cisco IOS XE 16.5.x	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	—
Cisco IOS XE 16.6.x	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	—

Cisco IOS XE リリース	Cisco 4321 ISR	Cisco 4321 ISR	Cisco 4331 ISR	Cisco 4351 ISR	Cisco 4431 ISR	Cisco 4451 ISR	Cisco 4461 ISR
Cisco IOS XE 16.7.x	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	—
Cisco IOS XE 16.8.x	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	—
Cisco IOS XE 16.9.x	16.9(1r)	16.9(1r)	16.9(1r)	16.9(1r)	16.12(2r)	16.12(2r)	16.9(1r)
Cisco IOS XE 16.10.x	16.9(1r)	16.9(1r)	16.9(1r)	16.9(1r)	16.12(2r)	16.12(2r)	16.9(1r)
Cisco IOS XE 16.11.x	16.9(1r)	16.9(1r)	16.9(1r)	16.9(1r)	16.12(2r)	16.12(2r)	16.9(1r)
Cisco IOS XE 16.12.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.1.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.2.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.3.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.4.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.5.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)
Cisco IOS XE 17.6.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)

（注） 製造日が2535以降のデバイスの場合、サポートされている最小ROMMONバージョンは17.6.1です。これらのデバイスは、それより古いROMMONバージョンにダウングレードできません。IOS XE 16.12を搭載し、ROMMON 17.6.1rがプリインストールされたデバイスの場合、サポートされている最小ROMMONバージョンは17.6.1rです。ROMMONを16.12(2r)にダウングレードしないでください。これらのデバイスは、それより古いROMMONバージョンにダウングレードできません。

プロビジョニング ファイル

ここでは、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（126ページ）で使用されるファイルとプロセスに関する背景情報を提供します。

ルータの統合パッケージは、一連のサブパッケージと、packages.conf という名前のプロビジョニングファイルで設定されます。ソフトウェアを実行する一般的な方法は、統合パッケージを起動する方法です。統合パッケージはメモリーにコピーされ、展開/マウントされて、メモリー内で実行されます。プロビジョニング ファイルの名前は変更可能ですが、サブパッケージファイルの名前は変更できません。プロビジョニング ファイルとサブパッケージ ファイルは、同じディレクトリに保管される必要があります。個々のサブパッケージファイルが異なるディレクトリに保管されている場合、プロビジョニング ファイルは適切に機能しません。

（注） 例外として、新規またはアップグレードされたモジュール ファームウェア パッケージが後でインストールされる場合は、プロビジョニング ファイルと同じディレクトリに含まれている必要はありません。

プロビジョニング ファイル packages.conf を使って起動するようルータを設定すると、Cisco IOS XE ソフトウェアのアップグレード後に boot ステートメントを変更する必要がないため、便利です。

ファイル システム

次の表に、Cisco 4000 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 *15*：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。
harddisk:	（NIM-SSD、NIM-HDD、または内部 mSATA フラッシュ デバイスがルータに実装されている場合）ハード ディスク ファイル システム。 （注） 内部 mSATA フラッシュ デバイスは Cisco ISR4300 シリーズ ルータでのみサポートされています。
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。

ファイルシステム	説明
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。
usb0: usb1:	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 ドライブが usb0: または usb1: ポートに装着されている場合にのみ表示されます。

? ヘルプ オプションを使用するか、またはコマンド リファレンス ガイドの **copy** コマンドを使用します。

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 *16 :* 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。
lost+found 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。

ファイルまたはディレクトリ	説明
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。

- crashinfo ファイル、core ファイル、trace 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。

自動ブートのコンフィギュレーション レジスタの設定

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。

コンフィギュレーション レジスタの詳細については、「Use of the Configuration Register on All Cisco Routers」と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 （123 ページ）を参照してください。

（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。

（注） **confreg** を 0x2102 または 0x0 に変更した後、コンソールのボーレートが 9600 に設定されます。**confreg** を設定した後にコンソールセッションを確立できない場合、または意味のない出力が表示される場合は、端末エミュレーション ソフトウェアで設定を 9600 に変更してください。

ライセンス

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。

評価ライセンスは 60 日後に使用権ライセンスに自動的に変換され、使用権ライセンスは無期限に有効です。永久ライセンスへの変換は、評価ライセンスだけに適用されます。ルータでサポートされている他の機能については、永久ライセンスを購入する必要があります。

『Software Activation Configuration Guide, Cisco IOS XE Release 3S』の「Configuring the Cisco IOS Software Activation Feature」の章を参照してください。

統合パッケージ

次の 2 つの統合パッケージ（イメージ）のいずれか 1 つがルータにプリインストールされています。

- **universalk9**：これには **ipbasek9** ベースパッケージと、**securityk9**、**uck9**、および **appxk9** テクノロジーパッケージが含まれています。
- **universalk9_npe**：これには **ipbasek9** ベースパッケージと、**securityk9_npe**、**uck9**、および **appxk9** テクノロジーパッケージが含まれています。このイメージの暗号化機能は限定されています。

（注） 「npe」はNo Payload Encryption（ペイロード暗号化なし）を意味します。

（注） 統合パッケージは「スーパー パッケージ」および「イメージ」とも呼ばれます。

ルータのソフトウェア イメージを取得するには、http://software.cisco.com/download/navigator.html にアクセスしてください。

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。

universalk9 および **universalk9_npe** イメージとは別個に、Boot ROMMON イメージを使用できます。詳細については、「*ROMMON* イメージ」のセクションを参照してください。

デジタル署名付きのシスコ ソフトウェアの確認と、イメージファイルのデジタル署名情報の表示方法については、『Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S』の「Digitally Signed Cisco Software」の項を参照してください。

次の例では、パッケージのソフトウェアの真正性に関する情報と内部詳細情報を取得する方法を示します。

- 「デジタル署名付き *Cisco* ソフトウェア署名情報の表示」のセクション
- 「モジュールまたは統合パッケージの説明を取得する」のセクション

統合パッケージの機能の多くは **ipbasek9** ベースパッケージに含まれています。**ipbasek9** パッケージのライセンスキーは、デフォルトでアクティベートされます。

テクノロジー パッケージ

テクノロジーパッケージには、統合パッケージ内のソフトウェア機能が含まれています。異なる機能セットを使用するには、選択したテクノロジーパッケージライセンスをイネーブル（有効）にします。テクノロジーパッケージを任意に組み合わせてライセンスをイネーブルにできます。

各テクノロジー パッケージには評価ライセンスがあります。評価ライセンスは 60 日後に使用権（RTU）ライセンスに変換され、その後は無期限に有効となります。

テクノロジー パッケージのリストを次に示します。

（注） Cisco 1000 シリーズ サービス統合型ルータでは、L2TPv2 セッションは appxk9 なしで起動しますが、トラフィックがセッションを通過するには appxk9 ライセンスが必要です。L2TPv2 セッションに QoS ポリシーを適用する場合も appxk9 ライセンスが必要です。

securityk9

securityk9 テクノロジーパッケージには、IPsec、SSL/SSH、ファイアウォール、セキュア VPN など、すべての暗号化機能が含まれています。

securityk9_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 **securityk9** 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。**securityk9_npe** パッケージは **universalk9_npe** イメージでのみ使用可能です。したがって、**securityk9** パッケージと **securityk9_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。

uck9

Cisco Unified Border Element（Cisco UBE）機能を有効にするには、Unified Communications テクノロジーパッケージが必要です。Cisco UBE 機能を使用するには、セッションライセンスと、メディアを保護するためのセキュリティ テクノロジー パッケージが必要です。

appxk9

appxk9 テクノロジーパッケージにはアプリケーション エクスペリエンス機能が含まれています。これは、Cisco 第 2 世代サービス統合型ルータの DATA パッケージの機能に似ています。詳細については、http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/software-activation-on-integrated-services-routers-isr/white_paper_c11_556985.html#wp9000791を参照してください。

appxk9 パッケージには、MPLS、PfR、L2/L3 VPN、ブロードバンド、AVC などの多数の機能が含まれています。

機能ライセンス

次の各機能を使用するには、対応する機能ライセンスを有効にします。以降の項でこれについて説明します。

HSECK9

完全な暗号化機能を実装するには **HSECK9** ライセンスが必要です。**HSECK9** ライセンスがない場合、225 個のセキュアトンネルおよび 85 Mbps の暗号化帯域幅だけを使用できます。**HSECK9** ライセンスにより、**securityk9** テクノロジーパッケージ内の機能は、最大限のセキュアトンネルおよび暗号化帯域幅を使用できます。**HSECK9** ライセンスを有効にするには、Cisco.com から **FL-44-HSEC-K9** ライセンスを購入し、**license install** *license-files* コマンドを使ってそれをインストールします。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。

（注） **HSECK9** 機能には、60 日後に RTU ライセンスに変換される評価ライセンスは含まれないため、機能ライセンスを取得する必要があります。

輸出規制機能を有効にしない場合は、デバイスで HSECK9 ライセンス機能が設定されていても、デバイスは HSECK9 ライセンス要求をスマートライセンスサーバーに送信しません。

（注） IOS XE Fuji 16.8.1 以降、トンネル数と暗号スループットに関する制限が拡張されています。HSEC がない場合、新しいスループット制限は各方向で 250 Mbps であり、トンネルの数は 1000 です。

また、**HSECK9** 機能のライセンスを有効にするには、**securityk9** テクノロジーパッケージも必要です。**securityk9** テクノロジーパッケージの詳細については、securityk9 （114 ページ）を参照してください。

HSECK9 機能ライセンスの削除

デバイスから HSECK9 機能のライセンスを削除するには、次の手順に従ってライセンスを正常に削除する必要があります。ユーザーは、必要に応じて、後でこのライセンスを復活させることができます。これらの手順に従わないと、機能ライセンスは、リロード後に認可された状態に戻ります。

HSECK9 機能のライセンスを削除するには、次の手順を実行します。

ステップ 1 デバイスの登録を解除します。
ステップ 2 **no license featurehseck9** コマンドを使用して、HSEC ライセンスの設定を解除します。
ステップ 3 **write memory** コマンドを使用して、実行コンフィギュレーションを保存します。
ステップ 4 （任意）登録解除後もデバイスが表示される場合は、ライセンスポータルからデバイスを削除します。
ステップ 5 デバイスをリロードします。
ステップ 6 **show license detail** コマンドを使用して、ライセンスが削除されたことを確認します。

パフォーマンス

スループットの向上を可能にするパフォーマンス機能は、パフォーマンス ライセンスによってイネーブルになります。この機能は **ipbasek9** テクノロジーパッケージに含まれています。この機能をイネーブルにするには、パフォーマンス ライセンス（製品番号 FL-44-PERF-K9）をご注文ください。このライセンスはスループット ライセンスとして表示されます。

使用ライセンスをアクティブにしてからルータをリロードすることによって、2.5 Gbps から 5 Gbps に ESP のスループットをアップグレードできます。使用ライセンスのアクティブ化の詳細については、『**Configuring Cisco Right-To-Use License Configuration Guide**』を参照してください。ESP の現在のスループット レベルを決定するには、show platform hardware throughput

level コマンドを実行します。次に、このコマンドの出力例を示します（パフォーマンス アップグレード ライセンス適用前）。

スループットレベルを設定するには、次の手順を実行します。また、スループットレベルをアップグレードするには、`platform hardware throughput level { 2500000 | 5000000}` コマンドを使用します。

1. ユーザー EXEC コンフィギュレーション モードで、`enable` コマンドを入力します。
2. グローバル コンフィギュレーション モードを開始するには、`configure terminal` コマンドを入力します。
3. スループットレベルをアップグレードするには、`platform hardware throughput level{2500000|5000000}` コマンドを入力します。
4. グローバル コンフィギュレーション モードを終了するために、exit を入力します
5. 設定を保存するには、`copy running-config startup-config` コマンドを入力します。
6. ルータをリロードするには、reload を入力します。リロードは、スループット レベルをアクティブ化するために必要な措置です。

```
show platform hardware throughput level
The current throughput level is 2500000 kb/s
```

スループットレベルを設定するには、次の手順を実行します。また、スループットレベルをアップグレードするには、`platform hardware throughput level { 2500000 | 5000000}` コマンドを使用します。

1. ユーザー EXEC コンフィギュレーション モードで、`enable` コマンドを入力します。
2. グローバル コンフィギュレーション モードを開始するには、`configure terminal` コマンドを入力します。
3. スループットレベルをアップグレードするには、`platform hardware throughput level{2500000|5000000}` コマンドを入力します。
4. グローバル コンフィギュレーション モードを終了するために、exit を入力します
5. 設定を保存するには、`copy running-config startup-config` コマンドを入力します。
6. ルータをリロードするには、reload を入力します。リロードは、スループット レベルをアクティブ化するために必要な措置です。

次に、スループット レベルをアップグレードする例を示します。

```
Router>enable
Router#configure terminal
Router(config)#platform hardware throughput level 5000000
% The config will take effect on next reboot
Router(config)#exit
Router#copy running-config startup-config
Router#reload
```

ブースト パフォーマンス ライセンス

Cisco ブート パフォーマンス ライセンスを使用すると、スループット帯域幅を増やすことができます。次のモードでブート パフォーマンス ライセンスを有効にできます。

（注） ブースト パフォーマンス ライセンスを使用するには、デバイスで Cisco IOS XE ソフトウェア バージョン 16.07.01 以降が実行されている必要があります。また、ライセンスがライセンス CSSM リポジトリに追加される前にデバイスが CSSM に登録されている場合、ブーストライセンスコマンドは使用できません。ブーストライセンスコマンドを実行するには、CSSM からデバイスの登録を解除して登録しなおす必要があります。

（注） Cisco 4000 シリーズ ISR でブーストライセンスを有効にした場合、Snort IPS および ISR-WAAS の仮想サービスコンテナを設定できません。

CSL モードでのブート パフォーマンス ライセンスのアクティブ化

ブースト パフォーマンス ライセンスを Cisco ソフトウェアライセンス（CSL）モードでアクティブ化するには、次の手順を実行します。

1. この例に示すように、**license install bootflash:xxx** コマンドでデバイスを設定します。

```
Device#license install bootflash:FDO203520HU_201804090203446350.lic
Installing licenses from "bootflash:FDO203520HU_201804090203446350.lic"
Installing...Feature:booster_performance...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install

Building configuration...
[OK]
% Throughput boost is configured, it will take effect after reload
```

2. ログに次のメッセージが表示されます。

```
*Apr  9 07:40:11.674: %LICENSE-6-INSTALL: Feature booster_performance 1.0 was installed
 in this device.
 UDI=ISR4331/K9:FDO203520HU; StoreIndex=2:Primary License Storage
```

3. **platform hardware throughput level boost** が設定に自動的に追加されます。

```
Device#show running-config | include throughput

platform hardware throughput level boost
```

4. 設定を保存し、デバイスをリロードして、ブースト パフォーマンス ライセンスを有効にします。この例に示すように、リロード後にブーストパフォーマンスがアクティブになります。

```
Device#show platform hardware throughput level

The current throughput level is unthrottled
```

```
Device#show license

<output omitted>

Index 11 Feature: booster_performance
 Period left: Life time
 License Type: Permanent
 License State: Active, In Use
 License Count: Non-Counted
 License Priority: Medium
```

5. グローバル コンフィギュレーション モードを終了するために、exit を入力します
6. 設定を保存するには、`copy running-config startup-config` コマンドを入力します。

スマートライセンスモードでのブート パフォーマンス ライセンス

ここでは、2つのユースケースにより、デバイスからブート パフォーマンス ライセンスをアクティブ化および非アクティブ化するプロセスについて説明します。

ブースト パフォーマンス ライセンスの有効化：

- デバイスをスマートライセンスモードで起動します。ブースト パフォーマンス コマンドは、スマートポータルに登録しないと表示されません。
- スマートポータルに正常に登録したら、スマートアカウントでブースト パフォーマンス ライセンスが使用可能かどうかをチェックします。
- この機能を有効にするには、**platform hardware throughput level boost** コマンドを使用します。設定を保存する必要があります。スマートアカウントで有効なライセンスがまだ使用可能である場合、デバイスのリロード後にブートパフォーマンス機能が有効になります。
- プラットフォーム ハードウェア スループット レベルをチェックするには、**show platform hardware throughput level boost** コマンドを使用します。十分なライセンスがない場合は、コンプライアンス違反（OOC）メッセージが表示され、スループットレベルの変更はデバイスがリロードされても有効になりません。

ライセンスの返却：

- デバイスは、**boost performance** コマンドが設定されたスマートライセンスモードになっています。
- **show running-config** コマンドおよび **show license summary** コマンドを使用して、スマートアカウントからのブーストパフォーマンス情報を表示します。
- **no platform hardware throughput level boost** コマンドを使用して機能を無効にします。

（注） コマンドは設定から削除されますが、ライセンスはデバイスがリロードされた後にのみリリースされます。

スループットレベルは、デバイスがリロードされるまで有効になりません。

ライセンスの可視性は、デバイスがリロードされるまで利用できます。

使用プールからブースト パフォーマンス ライセンスが 1 カウント削減され、1 つのライセンスが元のプールに戻されます。

Cisco ソフトウェアライセンスのスマートライセンスへの移行

ここでは、Cisco ソフトウェアライセンス（CSL）に**boost performance license**がある場合にデバイスが CSL からスマートライセンスに移行するときのユースケースについて説明します。ブーストパフォーマンスの動作は、CSL でブーストパフォーマンスがアクティブ化されている場合、スマートアカウントのライセンスの可用性によって決定されます。

スループットレベルを設定するには、次の手順を実行します。また、スループットレベルをアップグレードするには、次を使用します：

1. **platform hardware throughput level boost** コマンドを使用してデバイスを設定し、**show running-config** を使用して、ブースト パフォーマンス ライセンスがアクティブ化されているかどうかをチェックします。
2. **show license** を使用して、ブーストパフォーマンスが使用中であり、永久ライセンスモードであるかどうかを確認します。
3. `license smart enable` コマンドを使用してスマートライセンスを有効にします。登録が成功すると、ライセンス要求が、検証のためにスマートポータルに送信されます。成功した場合、ブーストパフォーマンスは有効であり、リロードは必要ありません。それ以外の場合、**platform hardware throughput level boost** は設定から排除されます。ブーストパフォーマンス機能は、リロード後に無効になります。
4. 移行中の登録前にライセンスが存在する場合は、後で余分なリロードを避けるために、ライセンスの評価モードを維持する必要があります。
5. グローバル コンフィギュレーション モードを終了するために、exit を入力します
6. 設定を保存するには、`copy running-config startup-config` コマンドを入力します。
7. ルータをリロードするには、reload を入力します。リロードは、スループット レベルをアクティブ化するために必要な措置です。

スマートライセンスの Cisco ソフトウェアライセンスへの移行

このセクションには、スマートライセンスから Cisco ソフトウェアライセンスへの移行中に何が起こるのかを説明する次の 2 つのユースケースが含まれています。

ブーストパフォーマンスが使用されている場合：

- Device# **platform hardware throughput level boost**
- Device# **show license**で、スマートライセンスとブースト パフォーマンス ライセンスが有効になっていることを確認します。
- 対応するデバイスからブースト パフォーマンス ライセンスが消費されている場合は、スマート ライセンス アカウントをチェックします。
- スマートライセンスを削除します。
- Device# **no license smart enable**
- ブースト パフォーマンス ライセンスが使用可能かどうかをチェックし、ブーストコマンドを保持することを決定できます。
- 追加のリロードは必要ありません。

ブーストパフォーマンスが使用されていない場合：

- show running-configuration で **no platform hardware throughput level boost** を使用します。
- スマートライセンスが有効になっているもののブースト パフォーマンス ライセンスがリストにない場合は、Device# **show license** でチェックします。
- スマート ライセンス アカウントをチェックします。対応するデバイスからブースト パフォーマンス ライセンスが使用されていません。
- スマートライセンスを削除するには、**no license smart enable** を使用します。
- **boost permanent license** が使用可能かどうかをチェックし、**boost** キーワードを追加します。
- ブートパフォーマンスがアクティブ化され、リロード後に「使用中」状態になります。

（注） 使用可能な永久ライセンスがないと、多くの場合、**no boost performance** コマンドおよび機能が変更されます。

- **ハイブリッドの Cisco IOS XE リリースが使用されている場合:**
- ハイブリッドの Cisco IOS XE リリース（IOS XE 16.9.x）を使用しており、スマートライセンスから使用権（RTU）ライセンスにロールバックする場合は、ルータを 2 回リロードして、ライセンスを「アクティブ、使用中」状態にします。
- Device# **configuration terminal**
- スマートライセンスを削除するには、**no license smart enable** を使用します。
- Device# **no license smart enable**
- Device# **exist**
- スマートライセンスを削除するには、ルータをリロードします。

- Device# **configure terminal**
- **yes** と入力してエンドユーザーライセンス契約書に同意します。
- Device# **exist**
- RTU ライセンスを「使用中」状態にするには、ルータをリロードします。

LED インジケータ

ルータの LED の詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』の「Overview」の項の「LED Indicators」を参照してください。

SSD キャリアカード NIM の LED の詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』の「Installing and Upgrading Internal Modules and FRUs」の項の「Overview of the SSD Carrier Card NIM（NIM-SSD）」を参照してください。

関連資料

ソフトウェアライセンスの詳細については、『Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2』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。

ソフトウェアのインストール方法とアップグレード方法

ソフトウェアをインストールまたはアップグレードするには、統合パッケージまたは個別パッケージのソフトウェアを使用する以下のいずれかの方法に従います。概要の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 （121 ページ）
- 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 （126 ページ）

統合パッケージで実行するルータの管理および設定

（注） オプションのサブパッケージもまたインストールする必要がある場合、または個別のサブパッケージをアップグレードする予定の場合は、この手順を使用しないでください。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 （126 ページ）を参照してください。

- 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 （122 ページ）
- 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 （123 ページ）

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、**copy** コマンドを使用してルータの **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、TFTP を使用して **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、**boot system** 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。

```
Router# dir bootflash:
Directory of bootflash:/
11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer

928862208 bytes total (712273920 bytes free)

Router# copy tftp: bootflash:
Address or name of remote host []? 172.17.16.81
Source filename []?
/auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
Destination filename [isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin]?
Accessing
tftp://172.17.16.81//auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
...
Loading /auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin from
172.17.16.81 (via GigabitEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
[OK - 208904396 bytes]
208904396 bytes copied in 330.453 secs (632176 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/
11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 28 2008 16:17:34 -07:00
isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
928862208 bytes total (503156736 bytes free)
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash
bootflash:isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
Router(config)# config-reg 0x2102
Router(config)# exit
Router# show run | include boot
boot-start-marker
boot system flash bootflash:isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
boot-end-marker
Router# copy run start
Destination filename [startup-config]?
```

```
Building configuration...
[OK]
Router# reload
```

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

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router# show run | include boot
boot-start-marker
boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
boot-end-marker
license boot level adventerprise
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 17:42:54.445 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit
with
reload chassis code


Initializing Hardware ...

System integrity status: c0000600
Failures detected:
Boot FPGA corrupt


Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
```

```
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 424317088 (0x194a90a0) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
expected 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 5116 msec
Image validated
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (local/local): load_modules took: 2 seconds,
expected max time 2 seconds

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
 15.4(20140527:095327)
[v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ios 156]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 27-May-14 21:28 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2014 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.
```

```
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.


Warning: the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.


Press RETURN to get started!


Router>
Router>
Router>enable
Router# show version
Cisco IOS XE Software, Version BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ext
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
 15.4(20140527:095327)
v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ios 156]

IOS XE Version: BLD_V154_3_S_XE313_THROTTLE_LATEST

Cisco IOS-XE software, Copyright (c) 2005-2014 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 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp://10.81.116.4/rtp-isr4400-54/isr4400.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.

License Level: adventerprise
License Type: EvalRightToUse
--More-- Next reload license Level: adventerprise

cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Configuration register is 0x2102
```

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

個別のパッケージの実行と統合パッケージの実行のどちらを選択するかについては、「ソフトウェアのインストール：概要」のセクションを参照してください。

この項では、次の項目について説明します。

- 統合パッケージからのサブパッケージのインストール （126 ページ）
- ファームウェア サブパッケージのインストール （138 ページ）
- フラッシュ ドライブの統合パッケージからサブパッケージをインストールする （132 ページ）

統合パッケージからのサブパッケージのインストール

TFTP サーバから統合パッケージを取得するには、次の手順を実行します。

この手順のバリエーションとして、USB フラッシュ ドライブから統合パッケージを取得することもできます。この方法は、「フラッシュドライブの統合パッケージからサブパッケージをインストールする」で説明されています。

始める前に

TFTP サーバに統合パッケージをコピーします。

手順の概要

1. **show version**

2. **dir bootflash:**
3. **show platform**
4. **mkdir bootflash:** *URL-to-directory-name*
5. **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*
6. **reload**
7. **boot** *URL-to-directory-name*/**packages.conf**
8. **show version installed**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show version**
	例：
	`Router# show version`
	`Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version 15.3(20120627:221639) [build_151722 111]`
	`Copyright (c) 1986-2012 by Cisco Systems, Inc.`
	`Compiled Thu 28-Jun-12 15:17 by mcpre`
	`.`
	`.`
	`.`
		ルータで実行されているソフトウェアのバージョンを表示します。後で、インストールするソフトウェア バージョンとこのバージョンを比較できます。

ステップ 2	**dir bootflash:** 例： `Router# dir bootflash:`	ソフトウェアの旧バージョンを表示し、パッケージが存在していることを示します。

ステップ 3	**show platform**
	例：
	`Router# show platform`
	`Chassis type: ISR4451/K9`
		インベントリを表示します。

ステップ 4	**mkdir bootflash:** *URL-to-directory-name* 例： `Router# mkdir bootflash:mydir`	展開したソフトウェアイメージの保存先ディレクトリを作成します。 ディレクトリにはイメージと同じ名前を指定できます。
ステップ 5	**request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name* 例： `Router# request platform software package expand file bootflash:isr4400-universalk9-NIM.bin to bootflash:mydir`	ステップ 4 で作成したイメージ保存用ディレクトリ（*URL-to-directory-name*）の中に、TFTP サーバーからのソフトウェアイメージ（*URL-to-consolidated-package*）を展開します。

	コマンドまたはアクション	目的

ステップ 6	**reload**
	例：
	`Router# reload`
	`rommon >`
		ROMMON モードをイネーブルにします。このモードで、統合ファイル内のソフトウェアをアクティブ化できます。

ステップ 7	**boot** *URL-to-directory-name*/**packages.conf** 例： `rommon 1 > boot bootflash:mydir/packages.conf`	プロビジョニング ファイル（packages.conf）のパスと名前を指定して、統合パッケージを起動します。

ステップ 8	**show version installed**
	例：
	`Router# show version installed`
	`Package: Provisioning File, version: n/a, status: active`
		新しくインストールされたソフトウェアのバージョンを表示します。

例

この例の最初の部分では、統合パッケージ isr4400-universalk9.164422SSA.bin が TFTP サーバにコピーされます。これは必須のステップです。例のそれ以降の部分では、統合ファイル packages.conf が起動されます。

```
Router# copy tftp:isr4400/isr4400-universalk9.164422SSA.bin bootflash:
Address or name of remote host []? 192.0.2.1
Destination filename [isr4400-universalk9.164422SSA.bin]?
Accessing tftp://192.0.2.1/isr4400/isr4400-universalk9.164422SSA.bin...
Loading isr4400/isr4400-universalk9.164422SSA.bin from 192.0.2.1 (via GigabitEthernet0):
 !!!!!!!!
[OK - 410506248 bytes]

410506248 bytes copied in 338.556 secs (1212521 bytes/sec)


Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental
Version
15.3(20120627:221639) [build_151722 111]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 28-Jun-12 15:17 by mcpre

IOS XE Version: 2012-06-28_15.31_mcpre

Cisco IOS-XE software, Copyright (c) 2005-2012 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 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp:isr4400/isr4400.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.

License Level: adventerprise
License Type: EvalRightToUse
Next reload license Level: adventerprise
cisco ISR4451/K9 (2RU) processor with 1136676K/6147K bytes of memory.
Processor board ID FGL161611AB
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.

Configuration register is 0x8000

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 May 3 2012 19:58:37 +00:00 lost+found
178465 drwx 4096 Jun 6 2012 15:20:20 +00:00 core
584065 drwx 4096 Jul 13 2012 19:19:00 +00:00 .prst_sync
405601 drwx 4096 May 3 2012 19:59:30 +00:00 .rollback_timer
113569 drwx 40960 Jul 13 2012 19:19:32 +00:00 tracelogs
64897 drwx 4096 May 3 2012 19:59:42 +00:00 .installer
13 -rw- 1305 May 7 2012 17:43:42 +00:00 startup-config
14 -rw- 1305 May 7 2012 17:43:55 +00:00 running-config
15 -r-- 1541 Jun 4 2012 18:32:41 +00:00 debug.conf
16 -rw- 1252 May 22 2012 19:58:39 +00:00 running-config-20120522
519169 drwx 4096 Jun 4 2012 15:29:01 +00:00 vman_fdb

7451738112 bytes total (7067635712 bytes free)



Router# show platform
Chassis type: ISR4451/K9

Slot         Type                State                 Insert time (ago)
---------    ------------------- --------------------- -----------------
0            ISR4451/K9          ok                    15:57:33
 0/0         ISR4451-6X1GE       ok                    15:55:24
1            ISR4451/K9          ok                    15:57:33
 1/0         SM-1T3/E3           ok                    15:55:24
2            ISR4451/K9          ok                    15:57:33
 2/0         SM-1T3/E3           ok                    15:55:24
```

```
R0          ISR4451/K9          ok, active            15:57:33
F0          ISR4451-FP          ok, active            15:57:33
P0          Unknown             ps, fail              never
P1          XXX-XXXX-XX         ok                    15:56:58
P2          ACS-4450-FANASSY    ok                    15:56:58

Slot        CPLD Version        Firmware Version
---------   ------------------- ----------------------------------------
0           12090323            15.3(01r)S [ciscouser-ISRRO...
1           12090323            15.3(01r)S [ciscouser-ISRRO...
2           12090323            15.3(01r)S [ciscouser-ISRRO...
R0          12090323            15.3(01r)S [ciscouser-ISRRO...
F0          12090323            15.3(01r)S [ciscouser-ISRRO...

Router# mkdir bootflash:isr4400-universalk9.dir1
Create directory filename [isr4400-universalk9.dir1]?
Created dir bootflash:/isr4400-universalk9.dir1
Router# request platform software package expand file bootflash:isr4400-universalk9.NIM.bin

to bootflash:isr4400-universalk9.dir1
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# reload
Proceed with reload? [confirm]

*Jul 13 19:39:06.354: %SYS-5-RELOAD: Reload requested by console.Reload Reason: Reload
Command.

rommon 1 > boot bootflash:isr4400-universalk9.dir1/packages.conf

File size is 0x00002836
Located isr4400-universalk9.dir1/packages.conf
Image size 10294 inode num 324484, bks cnt 3 blk size 8*512
#
File is comprised of 1 fragments (33%)

is_valid_sha1hash: SHA-1 hash:
calculated 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
expected 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
File size is 0x04b3dc00
Located isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg
Image size 78896128 inode num 324491, bks cnt 19262 blk size 8*512
###############################################################################################
File is comprised of 21 fragments (0%)
.....



Router# show version installed
Package: Provisioning File, version: n/a, status: active
File: bootflash:isr4400-universalk9.dir1/packages.conf, on: RP0
Built: n/a, by: n/a
File SHA1 checksum: ad09affd3f8820f4844f27acc1add502e0b8f459

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg,
on: RP0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: active
```

```
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
 RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e
Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: dir1, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb
Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
 RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
File:
bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge-BLD-BLD_MCP_DEV_LATEST_20120710
_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpcontrol-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
```

```
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: 2012-07-10_16.23_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpios-universalk9-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb

Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpaccess-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpbase-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes-BLD-BLD_MCP_DEV_LATEST
_20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File:
bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_sp2700-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
```

フラッシュ ドライブの統合パッケージからサブパッケージをインストールする

USB フラッシュドライブの統合パッケージからサブパッケージをインストールする手順は、「統合パッケージからのサブパッケージのインストール」で説明されている手順に似ています。

ステップ 1 **show version**

ステップ 2 **dir usb***n***:**

ステップ 3 **show platform**

ステップ 4 **mkdir bootflash:***URL-to-directory-name*

ステップ 5 **request platform software package expand fileusb***n***:** ***package-name to URL-to-directory-name***

ステップ 6 **reload**

ステップ 7 **boot** *URL-to-directory-name/***packages.conf**

ステップ 8 **show version installed**

Cisco IOS XE Denali リリース 16.3 のソフトウェアのインストールおよびアップグレード方法

ソフトウェアをインストールまたはアップグレードするには、統合パッケージまたは個別パッケージのソフトウェアを使用する以下のいずれかの方法に従います。「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 Denali* リリース *16.3* へのアップグレード」セクション

Cisco IOS XE Denali リリース 16.3 へのアップグレード

デバイスを初めて Cisco IOS XE Denali リリース 16.3 にアップグレードする場合は、前のセクションに示されている手順を使用します。さらに、Cisco IOS XE Denali リリース 16.3 には、最小 ROMMON バージョンが必要です。デバイスは Cisco IOS XE Denali 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
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router# show run | include boot
boot-start-marker
boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
boot-end-marker
license boot level adventerprise
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 17:42:54.445 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit
with
reload chassis code
```

```
Initializing Hardware ...

System integrity status: c0000600


Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 504063931 (0x1e0b67bb) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
expected 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 5116 msec
Image validated
```

```
Detected old ROMMON version 12.2(20150910:184432), upgrade required
Upgrading to newer ROMMON version required by this version of IOS-XE, do not power cycle
 the system.  A reboot will automatically occur for the new ROMMON to take effect.
selected : 1
Booted : 1
Reset Reason: 1

Info: Upgrading entire flash from the rommon package
Switching to ROM 0
Upgrade image MD5 signature is b702a0a59a46a20a4924f9b17b8f0887
Upgrade image MD5 signature verification is b702a0a59a46a20a4924f9b17b8f0887
Switching back to ROM 1
ROMMON upgrade complete.

To make the new ROMMON permanent, you must restart the RP.
ROMMON upgrade successful.  Rebooting for upgrade to take effect.


Initializing Hardware ...

System integrity status: 00300610
Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed

Expected hash:
ddaf35a193617abacc417349ae204131
12e6fa4e89a97ea20a9eeee64b55d39a
2192992a274fc1a836ba3c23a3feebbd
454d4423643ce80e2a9ac94fa54ca49f

Obtained hash:
ddaf35a193617abacc417349ae204131
12e6fa4e89a97ea20a9eeee64b55d39a
2192992a274fc1a836ba3c23a3feebbd
454d4423643ce80e2a9ac94fa54ca49f
ROM:Sha512 Self Test Passed
Self Tests Latency: 418 msec
Rom image verified correctly


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username

CPLD Version: 33 (MM/DD/YY): 06/23/14 Cisco ISR4351/K9 Slot:0

Current image running: Boot ROM1

Last reset cause: ResetRequest
Reading confreg 0x2102

Reading monitor variables from NVRAM
Enabling interrupts...done

Checking for PCIe device presence...done
Cisco ISR4351/K9 platform with 16777216 Kbytes of main memory

autoboot entry: NVRAM VALUES: bootconf: 0x0, autobootstate: 0
autobootcount: 0, autobootsptr: 0x0
Rommon upgrade requested
Flash upgrade reset 0 in progress
```

```
.......
Initializing Hardware ...

Checking for PCIe device presence...done
Reading confreg 2102
System integrity status: 0x300610
Key Sectors:(Primary, GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 288
RSA Self Test Passed

Expected hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F

Obtained hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F
Sha512 Self Test Passed
Rom image verified correctly


System Bootstrap, Version 16.2(1r), RELEASE SOFTWARE
Copyright (c) 1994-2016  by cisco Systems, Inc.


Current image running: *Upgrade in progress* Boot ROM0

Last reset cause: BootRomUpgrade
ISR4351/K9 platform with 16777216 Kbytes of main memory

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 504063931 (0x1e0b67bb) bytes


Image Base is: 0x56834018
Image Size is: 0x1E089706
Package header rev 1 structure detected
Package type:30000, flags:0x0
IsoSize = 503874534
Parsing package TLV info:
000: 000000090000001D4B45595F544C565F -         KEY_TLV_
```

```
010: 5041434B4147455F434F4D5041544942 - PACKAGE_COMPATIB
020: 494C49545900000000000090000000B - ILITY
030: 4652555F52505F545950450000000009 - FRU_RP_TYPE
040: 000000184B45595F544C565F5041434B -     KEY_TLV_PACK
050: 4147455F424F4F544152434800000009 - AGE_BOOTARCH
060: 0000000E415243485F693638365F5459 -     ARCH_i686_TY
070: 5045000000000009000000144B45595F - PE          KEY_
080: 544C565F424F4152445F434F4D504154 - TLV_BOARD_COMPAT
090: 0000000900000012424F4152445F6973 -         BOARD_is
0A0: 72343330305F545950450000000000009 - r4300_TYPE
0B0: 000000184B45595F544C565F43525950 -     KEY_TLV_CRYP
0C0: 544F5F4B4559535452494E4700000009 - TO_KEYSTRING

TLV: T=9, L=29, V=KEY_TLV_PACKAGE_COMPATIBILITY
TLV: T=9, L=11, V=FRU_RP_TYPE
TLV: T=9, L=24, V=KEY_TLV_PACKAGE_BOOTARCH
TLV: T=9, L=14, V=ARCH_i686_TYPE
TLV: T=9, L=20, V=KEY_TLV_BOARD_COMPAT
TLV: T=9, L=18, V=BOARD_isr4300_TYPE
TLV: T=9, L=24, V=KEY_TLV_CRYPTO_KEYSTRING
TLV: T=9, L=10, V=EnCrYpTiOn
TLV: T=9, L=11, V=CW_BEGIN=$$
TLV: T=9, L=19, V=CW_FAMILY=$isr4300$
TLV: T=9, L=59, V=CW_IMAGE=$isr4300-universalk9.2016-06-29_23.31_paj.SSA.bin$
TLV: T=9, L=19, V=CW_VERSION=$16.3.1$
TLV: T=9, L=52, V=CW_DESCRIPTION=$Cisco IOS Software, IOS-XE Software$
TLV: T=9, L=9, V=CW_END=$$
Found DIGISIGN TLV type 12 length = 392
RSA Self Test Passed

Expected hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F

Obtained hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F
Sha512 Self Test Passed
Found package arch type ARCH_i686_TYPE
Found package FRU type FRU_RP_TYPE
Calculating SHA-1 hash...Validate package: SHA-1 hash:
 calculated 8B082C48:35C23C9E:8A091441:D6FACEE6:B5111533
 expected   8B082C48:35C23C9E:8A091441:D6FACEE6:B5111533

Image validated

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
```

```
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
 16.3(20160527:095327)
[v163_throttle]
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 27-May-16 21:28 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2016 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.



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.


Warning: the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.


Press RETURN to get started!
```

ファームウェア サブパッケージのインストール

始める前に

必要なファームウェアパッケージを含む統合パッケージを入手し、パッケージを展開します。（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（126ページ）を参照）。ファームウェアパッケージの場所と名前を書きとめ、以下の手順でその情報を *URL-to-package-name* に使用します。

たとえば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（126ページ）などを使ってルータがすでに設定されている場合、ファームウェア サブパッケージをインストールできます。

ファームウェア サブパッケージは個別にはリリースされません。統合パッケージを展開した後で、統合パッケージ内のファームウェア パッケージを選択できます。その後、次の手順に従ってファームウェア パッケージをインストールできます。

（注） 統合パッケージに関するリリース ノートを参照して、統合パッケージ内のファームウェアと、ルータに現在インストールされている Cisco IOS XE ソフトウェア バージョンとの互換性があることを確認してください。

手順の概要

1. **show version**
2. **dir bootflash:**
3. **show platform**
4. **mkdir bootflash:** *URL-to-directory-name*
5. **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*
6. **reload**
7. **boot** *URL-to-directory-name* **/packages.conf**
8. **show version installed**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**show version**
	例：
	`Router# show version`
	`Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version 15.3(20120627:221639) [build_151722 111]`
	`Copyright (c) 1986-2012 by Cisco Systems, Inc.`
	`Compiled Thu 28-Jun-12 15:17 by mcpre`
	`.`
	`.`
	`.`
		ルータで実行されているソフトウェアのバージョンを表示します。後で、インストールするソフトウェア バージョンとこのバージョンを比較できます。

ステップ 2	**dir bootflash:** 例： `Router# dir bootflash:`	ソフトウェアの旧バージョンを表示し、パッケージが存在していることを示します。

ステップ 3	**show platform**
	例：
	`Router# show platform`
	`Chassis type: ISR4451/K9`
		インベントリを確認します。
		「統合パッケージからのサブパッケージのインストール」セクションの例を参照してください。

ステップ 4	**mkdir bootflash:** *URL-to-directory-name* 例：	展開したソフトウェアイメージの保存先ディレクトリを作成します。

	コマンドまたはアクション	目的
	`Router# mkdir bootflash:mydir`	ディレクトリにはイメージと同じ名前を指定できます。
ステップ 5	**request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name* 例： `Router# request platform software package expand file bootflash:isr4400-universalk9-NIM.bin to bootflash:mydir`	ステップ 4 で作成したイメージ保存用ディレクトリ（*URL-to-directory-name*）の中に、TFTP サーバーからのソフトウェアイメージ（*URL-to-consolidated-package*）を展開します。

ステップ 6	**reload**
	例：
	`Router# reload`
	`rommon >`
		ROMMON モードをイネーブルにします。このモードで、統合ファイル内のソフトウェアをアクティブ化できます。

ステップ 7	**boot** *URL-to-directory-name* **/packages.conf** 例： `rommon 1 > boot bootflash:mydir/packages.conf`	プロビジョニング ファイル（packages.conf）のパスと名前を指定して、統合パッケージを起動します。

ステップ 8	**show version installed**
	例：
	`Router# show version installed`
	`Package: Provisioning File, version: n/a, status: active`
		新しくインストールされたソフトウェアのバージョンを表示します。

例

次の例の最初の部分では、TFTP サーバにコピーされる統合パッケージ isr4400-universalk9.164422SSA.bin が示されます。これは必須のステップです。例のそれ以降の部分では、統合ファイル packages.conf が起動されます。

```
Router# tftp:isr4400/isr4400-universalk9.164422SSA.bin bootflash:
Address or name of remote host []? 192.0.2.1
Destination filename [isr4400-universalk9.164422SSA.bin]?
Accessing tftp://192.0.2.1/isr4400/isr4400-universalk9.164422SSA.bin...
Loading isr4400/isr4400-universalk9.164422SSA.bin from 192.0.2.1 (via GigabitEthernet0):
 !!!!!!!!
[OK - 410506248 bytes]

410506248 bytes copied in 338.556 secs (1212521 bytes/sec)


Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental
Version
15.3(20120627:221639) [build_151722 111]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 28-Jun-12 15:17 by mcpre

IOS XE Version: 2012-06-28_15.31_mcpre
```

```
Cisco IOS-XE software, Copyright (c) 2005-2012 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 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp:isr4400/isr4400.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.

License Level: adventerprise
License Type: EvalRightToUse
Next reload license Level: adventerprise
cisco ISR4451/K9 (2RU) processor with 1136676K/6147K bytes of memory.
Processor board ID FGL161611AB
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.

Configuration register is 0x8000

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 May 3 2012 19:58:37 +00:00 lost+found
178465 drwx 4096 Jun 6 2012 15:20:20 +00:00 core
584065 drwx 4096 Jul 13 2012 19:19:00 +00:00 .prst_sync
405601 drwx 4096 May 3 2012 19:59:30 +00:00 .rollback_timer
113569 drwx 40960 Jul 13 2012 19:19:32 +00:00 tracelogs
64897 drwx 4096 May 3 2012 19:59:42 +00:00 .installer
13 -rw- 1305 May 7 2012 17:43:42 +00:00 startup-config
14 -rw- 1305 May 7 2012 17:43:55 +00:00 running-config
15 -r-- 1541 Jun 4 2012 18:32:41 +00:00 debug.conf
16 -rw- 1252 May 22 2012 19:58:39 +00:00 running-config-20120522
519169 drwx 4096 Jun 4 2012 15:29:01 +00:00 vman_fdb

7451738112 bytes total (7067635712 bytes free)
```

```
Router# show platform
Chassis type: ISR4451/K9

Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0 ISR4451/K9 ok 15:57:33
0/0 ISR4451-6X1GE ok 15:55:24
1 ISR4451/K9 ok 15:57:33
1/0 SM-1T3/E3 ok 15:55:24
2 ISR4451/K9 ok 15:57:33
2/0 SM-1T3/E3 ok 15:55:24
R0 ISR4451/K9 ok, active 15:57:33
F0 ISR4451-FP ok, active 15:57:33
P0 Unknown ps, fail never
P1 XXX-XXXX-XX ok 15:56:58
P2 ACS-4450-FANASSY ok 15:56:58

Slot CPLD Version Firmware Version
--------- ------------------- ----------------------------------------
0 12090323 15.3(01r)S [ciscouser-ISRRO...
1 12090323 15.3(01r)S [ciscouser-ISRRO...
2 12090323 15.3(01r)S [ciscouser-ISRRO...
R0 12090323 15.3(01r)S [ciscouser-ISRRO...
F0 12090323 15.3(01r)S [ciscouser-ISRRO...

Router# mkdir bootflash:isr4400-universalk9.dir1
Create directory filename [isr4400-universalk9.dir1]?
Created dir bootflash:/isr4400-universalk9.dir1
Router# request platform software package expand file bootflash:isr4400-universalk9.NIM.bin
 to
 bootflash:isr4400-universalk9.dir1
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# reload
Proceed with reload? [confirm]

*Jul 13 19:39:06.354: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
 Command.

rommon 1 > boot bootflash:isr4400-universalk9.dir1/packages.conf

File size is 0x00002836
Located isr4400-universalk9.dir1/packages.conf
Image size 10294 inode num 324484, bks cnt 3 blk size 8*512
#
File is comprised of 1 fragments (33%)

is_valid_sha1hash: SHA-1 hash:
calculated 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
expected 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
File size is 0x04b3dc00
Located isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg
Image size 78896128 inode num 324491, bks cnt 19262 blk size 8*512
###########################################################################################
File is comprised of 21 fragments (0%)
.....
```

```
Router# show version installed
Package: Provisioning File, version: n/a, status: active
File: bootflash:isr4400-universalk9.dir1/packages.conf, on: RP0
Built: n/a, by: n/a
File SHA1 checksum: ad09affd3f8820f4844f27acc1add502e0b8f459

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg,
on: RP0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
 RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e
Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: dir1, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb
Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
 RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
```

```
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpcontrol-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: 2012-07-10_16.23_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpios-universalk9-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb

Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpaccess-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpbase-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File:
bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File:
bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_sp2700-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
```

xDSL NIM でのファームウェアのアップグレード

xDSL ネットワーク インターフェイス モジュール（NIM）のファームウェアをアップグレードするには、次の手順を実行します。

始める前に

インストール期間中に Cisco IOS XE イメージ（スーパーパッケージ）を使用してパッケージを packages.conf モードで起動すると、ルータをリロードせずにファームウェアをアップグレードまたはダウングレードできます。ファームウェアのアップグレードに進む前に、「ファーム

ウェアサブパッケージのインストール」のセクションに記載されている手順に従う必要があります。

Cisco IOS XE イメージを使用して、packages.conf モードでルータを起動しない場合は、ファームウェアのアップグレードを進める前に、次の前提条件を満たしておく必要があります。

- ファームウェア サブパッケージ（NIM ファームウェア）を bootflash:/mydir にコピーします。
- プラットフォーム ソフトウェア パッケージ展開ファイル *boot flash:/mydir/<IOS-XE image>* に要求を送信し、スーパーパッケージを展開します。
- ハードウェアモジュールのサブスロットをリロードして、新しいファームウェアでモジュールを起動します。
- **show platform software subslot x/y module firmware** コマンドを使用して、モジュールが新しいファームウェアで起動したことを確認します。

手順の概要

1. Cisco IOS XE イメージをブートフラッシュ **mydir** にコピーします。
2. **request platform software package expand file** *bootflash:/mydir /<IOS-XE image* を使用して、スーパーパッケージを展開します。
3. **reload**。
4. **boot bootflash:mydir/ /packages.conf**。
5. **copy** NIM ファームウェア サブパッケージを **bootflash:mydir/** フォルダにコピーします。
6. **request platform software package install** *rp 0 file bootflash:/mydir/<firmware subpackage>*
7. **hw-module subslot x/y reload** を使用して、新しいファームウェアでモジュールを起動します。
8. **show platform software subslot 0/2 module firmware** を使用して、モジュールが新しいファームウェアで起動したことを確認します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Cisco IOS XE イメージをブートフラッシュ **mydir** にコピーします。 例： `Router# mkdir bootflash:mydir`	展開したソフトウェアイメージの保存先ディレクトリを作成します。 ディレクトリにはイメージと同じ名前を指定できます。
ステップ 2	**request platform software package expand file** *bootflash:/mydir /<IOS-XE image* を使用して、スーパーパッケージを展開します。 例： `Router# request platform software package expand file bootflash:/mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin`	プラットフォーム ソフトウェア パッケージをスーパーパッケージに展開します。

	コマンドまたはアクション	目的

ステップ 3	**reload**。
	例：
	`Router# reload`
	`rommon >`
		ROMMON モードを有効にします。このモードで、スーパーパッケージファイル内のソフトウェアをアクティブ化できます。

ステップ 4	**boot bootflash:mydir/ /packages.conf**。 例： `rommon 1 > boot bootflash:mydir/packages.conf`	プロビジョニングファイル（packages.conf）のパスと名前を指定して、スーパーパッケージを起動します。
ステップ 5	**copy** NIM ファームウェア サブパッケージを **bootflash:mydir/** フォルダにコピーします。 例： `Router#copy bootflash:isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg bootflash:mydir/`	NIM ファームウェア サブパッケージを bootflash:mydir にコピーします。
ステップ 6	**request platform software package install** *rp 0 file bootflash:/mydir/<firmware subpackage>* 例： `Router#equest platform software package install rp 0 file bootflash:mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg`	ソフトウェアパッケージがインストールされます。
ステップ 7	**hw-module subslot x/y reload** を使用して、新しいファームウェアでモジュールを起動します。 例： `Router#hw-module subslot 0/2 reload`	ハードウェアモジュールのサブスロットをリロードして、新しいファームウェアでモジュールを起動します。

ステップ 8	**show platform software subslot 0/2 module firmware** を使用して、モジュールが新しいファームウェアで起動したことを確認します。
	例：
	`Router# show platform software subslot 0/2 module firmware`
	`Pe`
		新しくインストールされたファームウェアのバージョンを表示します。

例

次に、ルータモジュールでファームウェアをアップグレードする例を示します。

```
Routermkdir bootflash:mydir
Create directory filename [mydir]?
Created dir bootflash:/mydir
Router#c
Router#copy bootflash:isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin bootflash:mydir/
```

```
Destination filename [mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCC
425288648 bytes copied in 44.826 secs (9487544 bytes/sec)
Router#
Router#
Router#dir bootflash:mydir
Directory of bootflash:/mydir/

632738  -rw-        425288648  Dec 12 2014 09:16:42 +00:00
isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin

7451738112 bytes total (474025984 bytes free)
Router#

Router#request platform software package
expand file bootflash:/mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router#reload
Proceed with reload? [confirm]

*Dec 12 09:26:09.874: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.Dec 12 09:26:25.156 R0/0: %PMAN-5-EXITACTION: Process manager is exiting:
process exit with reload chassis code


Initializing Hardware ...

System integrity status: 00000610
 Rom image verified correctly
 System Bootstrap, Version 15.3(3r)S1, RELEASE SOFTWARE
Copyright (c) 1994-2013  by cisco Systems, Inc.

 Current image running: Boot ROM0

Last reset cause: LocalSoft
 Cisco ISR4451-X/K9 platform with 4194304 Kbytes of main memory


rommon 1  boot bootflash:mydir/packages.conf

 File size is 0x000028f1
 Located mydir/packages.conf
 Image size
10481 inode num 632741, bks cnt 3 blk size 8*512

#
 File size is 0x150ae3cc
 Located mydir/isr4400-mono-universalk9.03.14.00.S.155-1.S-std.SPA.pkg
 Image size 353035212 inode num 356929, bks cnt 86191 blk size 8*512
 ###################################################################
######################################################################
 Boot image size = 353035212 (0x150ae3cc) bytes

 Package header rev 1 structure detected
 Calculating SHA-1 hash...done
 validate_package: SHA-1 hash:
```

```
  calculated 8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3
  expected   8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3

 RSA Signed RELEASE Image Signature Verification Successful.
 Package Load Test Latency : 3799 msec
 Image validated
 Dec 12 09:28:50.338 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 61864 kB] - Please clean up files on bootflash.

             Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(1)S,
RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Nov-14 18:28 by mcpre



Cisco IOS-XE software, Copyright (c) 2005-2014 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.



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.

cisco ISR4451-X/K9 (2RU) processor with 1681388K/6147K bytes of memory.
Processor board ID FTX1736AJUT
2 Ethernet interfaces
4 Gigabit Ethernet interfaces
2 ATM interfaces
```

```
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of flash memory at bootflash:.

Press RETURN to get started!

*Dec 12 09:28:58.922:
%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = esg Next reboot level = appxk9 and License = appxk9
*Dec 12 09:28:58.943:
%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = esg Next reboot level = ipbasek9 and License = ipbasek9
*Dec 12 09:28:58.981:
 %ISR_THROUGHPUT-6-LEVEL: Throughput level has been set to 1000000 kbps
*Dec 12 09:29:13.302: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*Dec 12 09:28:51.438: %CMRP-3-PFU_MISSING:cmand:  The platform does not detect a power
supply in slot 1
*Dec 12 09:29:01.256: %CMLIB-6-THROUGHPUT_VALUE:cmand:  Throughput license found,
throughput set to 1000000 kbps
*Dec 12 09:29:03.223: %CPPHA-7-START:cpp_ha:  CPP 0 preparing ucode
*Dec 12 09:29:03.238: %CPPHA-7-START:cpp_ha:  CPP 0 startup init
*Dec 12 09:29:11.335: %CPPHA-7-START:cpp_ha:  CPP 0 running init
*Dec 12 09:29:11.645: %CPPHA-7-READY:cpp_ha:  CPP 0 loading and initialization complete
*Dec 12 09:29:11.711: %IOSXE-6-PLATFORM:cpp_cp:
Process CPP_PFILTER_EA_EVENT__API_CALL__REGISTER
*Dec 12 09:29:16.280:
%IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO:
Management vrf Mgmt-intf created with ID 1, ipv4 table-id 0x1, ipv6 table-id 0x1E000001
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state to up
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state to up
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to down
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state to up
*Dec 12 09:29:17.521: %SYS-5-LOG_CONFIG_CHANGE: Buffer logging disabled
*Dec 12 09:29:18.867: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 12 09:29:18.870:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled
*Dec 12 09:29:18.870:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*Dec 12 09:29:18.871:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/2, interfaces disabled
*Dec 12 09:29:18.873:
%SPA_OIR-6-OFFLINECARD: SPA (ISR4451-X-4x1GE) offline in subslot 0/0
*Dec 12 09:29:18.874: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VA-B) offline in subslot 0/1
*Dec 12 09:29:18.874: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
*Dec 12 09:29:18.876: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F0
*Dec 12 09:29:18.876: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0
*Dec 12 09:29:18.882: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0
*Dec 12 09:29:18.884: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/1
*Dec 12 09:29:18.884: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/2
*Dec 12 09:29:18.935: %SYS-5-RESTART: System restarted --
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(1)S,
RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Nov-14 18:28 by mcpre
*Dec 12 09:29:18.895: %SPA-3-ENVMON_NOT_MONITORED:iomd:  Environmental monitoring
```

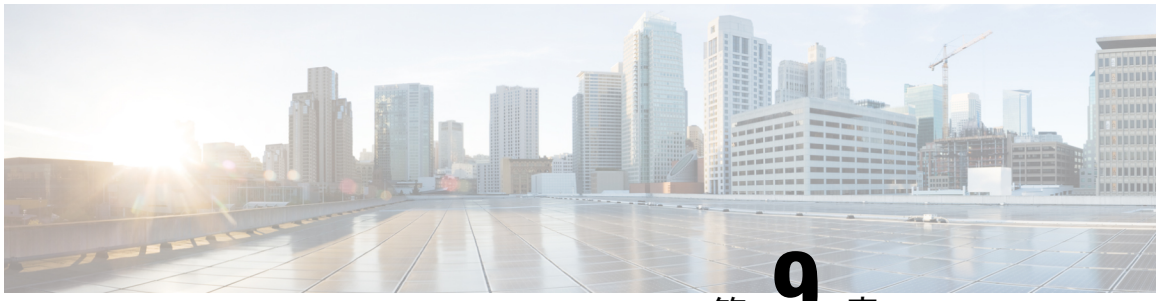
```
is not enabled for ISR4451-X-4x1GE[0/0]
*Dec 12 09:29:19.878: %LINK-5-CHANGED: Interface GigabitEthernet0,

changed state to administratively down
*Dec 12 09:29:22.419: %SPA_OIR-6-ONLINECARD: SPA (ISR4451-X-4x1GE) online in subslot 0/0
*Dec 12 09:29:22.610: %SYS-6-BOOTTIME: Time taken to reboot after reload =  194 seconds
*Dec 12 09:29:24.354: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to down
*Dec 12 09:29:24.415: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/2,
changed state to down
*Dec 12 09:29:24.417: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/3,
changed state to down
*Dec 12 09:29:30.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to up
*Dec 12 09:29:30.925: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/2,
 changed state to up
*Dec 12 09:29:30.936: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/3,
 changed state to up
*Dec 12 09:29:31.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
*Dec 12 09:29:31.930: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0/2, changed state to up
*Dec 12 09:29:31.936: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0/3, changed state to up
*Dec 12 09:29:34.147: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 12 09:30:29.152: %SPA_OIR-6-ONLINECARD: SPA (NIM-VA-B) online in subslot 0/1
*Dec 12 09:30:29.470: %SPA_OIR-6-ONLINECARD: SPA (NIM-VAB-A) online in subslot 0/2
*Dec 12 09:30:31.152: %LINK-3-UPDOWN: Interface Ethernet0/1/0, changed state to down
*Dec 12 09:30:31.152: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to down
*Dec 12 09:30:31.470: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to down
*Dec 12 09:30:31.470: %LINK-3-UPDOWN: Interface ATM0/2/0, changed state to down
*Dec 12 09:31:03.074: %CONTROLLER-5-UPDOWN: Controller VDSL 0/2/0, changed state to up
*Dec 12 09:31:05.075: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to up
*Dec 12 09:31:06.076: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2/0,
changed state to up
*Dec 12 09:31:12.559: %CONTROLLER-5-UPDOWN: Controller VDSL 0/1/0, changed state to up
*Dec 12 09:31:20.188: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to up
*Dec 12 09:31:21.188: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/1/0,
changed state to up
Router>
Router>en
Password:
Router#
Router#show controller vdsl 0/2/0
Controller VDSL 0/2/0 is UP

Daemon Status:  UP

   XTU-R (DS)  XTU-C (US)
Chip Vendor ID:  'BDCM'    'BDCM'
Chip Vendor Specific:   0x0000    0xA41B
Chip Vendor Country:    0xB500    0xB500
Modem Vendor ID: 'CSCO'    '    '
Modem Vendor Specific:  0x4602    0x0000
Modem Vendor Country:   0xB500    0x0000
Serial Number Near:     FOC18426DQ8 4451-X/K15.5(1)S
Serial Number Far:
Modem Version Near:     15.5(1)S
Modem Version Far:      0xa41b

Modem Status(L1): TC Sync (Showtime!)
DSL Config Mode: VDSL2
Trained Mode(L1): G.993.2 (VDSL2) Profile 30a
```

```
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: 4.14L.04
Modem PHY Version: A2pv6F039h.d24o_rc1

Line 1:

   XTU-R (DS)  XTU-C (US)
Trellis:   ON    ON
SRA:     disabled   disabled
SRA count:    0    0
Bit swap:    enabled   enabled
Bit swap count:   9    0
Profile 30a:    enabled
Line Attenuation:   3.5 dB    0.0 dB
Signal Attenuation:   0.0 dB    0.0 dB
Noise Margin:   30.9 dB  12.4 dB
Attainable Rate: 200000 kbits/s   121186 kbits/s
Actual Power:  13.3 dBm   7.2 dBm
Per Band Status:        D1  D2  D3  U0  U1  U2  U3
Line Attenuation(dB):   0.9 1.5 5.5 N/A 0.1 0.9 3.8
Signal Attenuation(dB): 0.8 1.5 5.5 N/A 0.0 0.2 3.2
Noise Margin(dB):       31.1 31.0 30.9 N/A 12.3 12.4 12.5
Total FECC:  0    0
Total ES:  0    0
Total SES:  0    0
Total LOSS:  0    0
Total UAS:  51    51
Total LPRS:  0    0
Total LOFS:  0    0
Total LOLS:  0    0


     DS Channel1   DS Channel0 US Channel1   US Channel0
Speed (kbps):    NA       100014  NA       100014
SRA Previous Speed:   NA            0  NA            0
Previous Speed:    NA            0  NA            0
Reed-Solomon EC:   NA            0  NA            0
CRC Errors:    NA            0  NA            0
Header Errors:    NA            0  NA            0
Interleave (ms):   NA         9.00  NA         0.00
Actual INP:    NA         4.00  NA         0.00

Training Log : Stopped
Training Log Filename : flash:vdsllog.bin

Router#
Router#

Router#copy bootflash:isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
 bootflash:mydir/
Destination filename [mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
6640604 bytes copied in 1.365 secs (4864911 bytes/sec)
Router#
```

```
Router#request platform software package install rp 0 file
bootflash:mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatiblity verficiation ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatiblity verficiation

--- Starting impact testing ---
Checking operational impact of change
Finished impact testing

--- Starting list of software package changes ---
Old files list:
  Removed isr4400-firmware_nim_xdsl.03.14.00.S.155-1.S-std.SPA.pkg
New files list:
  Added isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
```

```
Skipping soft links for firmware upgrade
Skipping soft links for firmware upgrade
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19
/release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]

  Replacing running software
  Replacing CLI software
  Restarting software
  Applying final IPC and database definitions
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.
Router#
Router#show platform software subslot 0/2 module firmware
Avg Load info
-----------------------------------------
1.83 1.78 1.44 3/45 607

Kernel distribution info
-----------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2
(Buildroot 2011.11) ) #3 SMP PREEMPT Fri Nov 7 09:26:19 IST 2014

Module firmware versions
-----------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039h.d24o_rc1

Boot Loader: Secondry
-----------------------------------------
Version: 1.1

Modem Up time
-----------------------------------------
0D 0H 25M 38S

Router#

Router#hw-module subslot 0/2 reload
Proceed with reload of module? [confirm]
Router#
*Dec 12 09:55:59.645: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-VAB-A)
reloaded on subslot 0/2
*Dec 12 09:55:59.646: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
*Dec 12 09:55:59.647: %CONTROLLER-5-UPDOWN: Controller VDSL 0/2/0, changed state to down
*Dec 12 09:57:22.514: new extended attributes received from iomd(slot 0 bay 2 board 0)
*Dec 12 09:57:22.514: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-VAB-A)
```

```
 reloaded on subslot 0/2
*Dec 12 09:57:22.515: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
Router#
Router#
*Dec 12 09:58:35.471: %SPA_OIR-6-ONLINECARD: SPA (NIM-VAB-A) online in subslot 0/2
*Dec 12 09:58:37.470: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to down
*Dec 12 09:58:37.470: %LINK-3-UPDOWN: Interface ATM0/2/0, changed state to down
Router#

Router#show platform software subslot 0/2 module firmware
Avg Load info
-----------------------------------------
0.84 0.23 0.08 1/45 598

Kernel distribution info
-----------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2 (Buildroot 2011.11)
 ) #6 SMP PREEMPT Mon Nov 17 10:51:41 IST 2014

Module firmware versions
-----------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039n.d24o_rc1

Boot Loader: Secondry
-----------------------------------------
Version: 1.1

Modem Up time
-----------------------------------------
0D 0H 0M 42S

Router#
```



第 9 章

スロットおよびサブスロットの設定

この章では、スロットとサブスロットについて説明します。スロットはルータのシャーシ スロット番号を示し、サブスロットはサービス モジュールが装着されているスロットを示します。

スロットおよびサブスロットの詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』の「About Slots and Interfaces」の項を参照してください。

この章で説明する内容は、次のとおりです。

インターフェイスの設定

ここでは、ギガビットインターフェイスを設定する方法について説明し、ルータ インターフェイスの設定例も示します。

ギガビット イーサネット インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *slot/subslot/port*
4. **ip address** *ip-address mask* [**secondary**] **dhcp pool**
5. **negotiation auto**
6. **end**

手順の詳細

	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： `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 3	**interface GigabitEthernet** *slot/subslot/port* 例： `Router(config)# interface GigabitEthernet 0/0/1`	GigabitEthernet インターフェイスを設定します。 • **GigabitEthernet**：インターフェイスのタイプ。 • *slot*：シャーシのスロット番号。 • */subslot*：セカンダリスロット番号。スラッシュ（/）が必要です。 • /port：ポートまたはインターフェイス番号。スラッシュ（/）が必要です。
ステップ 4	**ip address** *ip-address mask* [**secondary**] **dhcp pool** 例： `Router(config-if)# ip address 10.0.0.1 255.255.255.0 dhcp pool`	GigabitEthernet に IP アドレスを割り当てます。 • **ip address** *ip-address*：インターフェイスの IP アドレス。 • *mask*：関連付けられている IP サブネットのマスク。 • **secondary**（任意）：設定されたアドレスをセカンダリ IP アドレスとして指定します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。 • **dhcp**：DHCP を介してネゴシエートされる IP アドレス。 • **pool**：ローカル DHCP プールから自動的に設定される IP アドレス。
ステップ 5	**negotiation auto** 例： `Router(config-if)# negotiation auto`	ネゴシエーション モードを選択します。 • **auto**：リンクの自動ネゴシエーションを実行します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-if)# end`	現在のコンフィギュレーションセッションを終了して、特権 EXEC モードに戻ります。

インターフェイスの設定：例

次に、**interface gigabitEthernet** コマンドを使用してインターフェイスを追加し、IP アドレスを設定する例を示します。**0/0/0** はスロット/サブスロット/ポートを示します。ポートには 0 ～ 3 の番号が付いています。

```
Router# show running-config interface gigabitEthernet 0/0/0
Building configuration...
Current configuration : 71 bytes
!
interface gigabitEthernet0/0/0
no ip address
negotiation auto
end

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitEthernet 0/0/0
```

すべてのインターフェイスのリストの表示：例

この例では、**show platform software interface summary** コマンドおよび **show interfaces summary** コマンドを使用して、すべてのインターフェイスを表示します。

```
Router# show platform software interface summary
  Interface                 IHQ  IQD  OHQ  OQD  RXBS  RXPS  TXBS  TXPS  TRTL
------------------------------------------------------------------------------
* GigabitEthernet0/0/0        0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/1        0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/2        0    0    0    0     0     0     0     0     0
* GigabitEthernet0/0/3        0    0    0    0     0     0     0     0     0
* GigabitEthernet0            0    0    0    0     0     0     0     0     0


Router# show interfaces summary
   *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

Interface             IHQ  IQD    OHQ    OQD    RXBS    RXPS    TXBS    TXPS    TRTL
------------------------------------------------------------------------------------

* GigabitEthernet0/0/0 0    0      0      0      0       0       0       0       0
* GigabitEthernet0/0/1 0    0      0      0      0       0       0       0       0
* GigabitEthernet0/0/2 0    0      0      0      0       0       0       0       0
```

```
* GigabitEthernet0/0/3 0    0      0      0      0       0       0       0       0
* GigabitEthernet      0    0      0      0      0       0       0       0       0
```

インターフェイスに関する情報の表示：例

次に、**show ip interface brief** コマンドを使用して、インターフェイスの IP 情報とステータスの要約（仮想インターフェイスバンドル情報を含む）を表示する例を示します。

```
Router# show ip interface brief
Interface              IP-Address      OK?  Method  Status                 Protocol
GigabitEthernet0/0/0    10.0.0.1       YES  manual  down                   down
GigabitEthernet0/0/1    unassigned     YES  NVRAM   administratively down  down
GigabitEthernet0/0/2    10.10.10.1     YES  NVRAM   up                     up
GigabitEthernet0/0/3    10.8.8.1       YES  NVRAM   up                     up
GigabitEthernet0        172.18.42.33   YES  NVRAM   up                     up
```

第 10 章

Cisco Thousand Eyes エンタープライズ エージェント アプリケーションのホスティング

この章では Cisco Thousand Eyes エンタープライズ エージェント アプリケーションのホスティングについて説明します。この章で説明する内容は、次のとおりです。

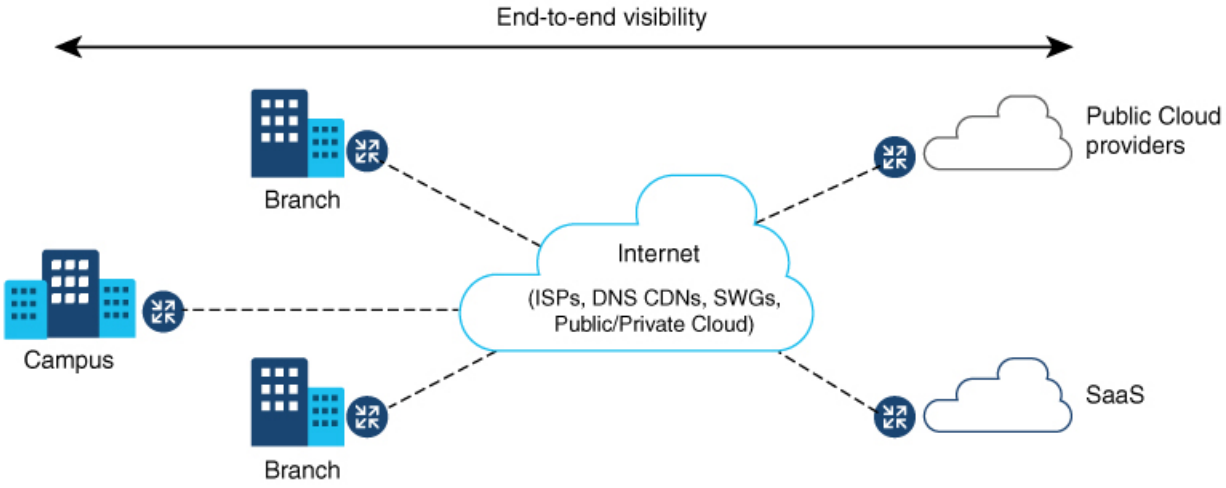
Cisco ThousandEyes エンタープライズ エージェント アプリケーションのホスティング

Cisco ThousandEyes は、ネットワーク インテリジェンス プラットフォームであり、エージェントを使用してさまざまなテストを実行し、ネットワークとアプリケーションのパフォーマンスをモニタできます。このアプリケーションを使用して、ビジネスに影響を及ぼすネットワークおよびサービス全体のエンドツーエンドパスを表示できます。Cisco ThousandEyes アプリケーションは、内部、外部、およびインターネットネットワークのネットワーク トラフィック パスをリアルタイムでアクティブにモニターし、ネットワークパフォーマンスの分析を支援します。また、Cisco ThousandEyes アプリケーションはルーティングおよびデバイスデータで強化されたアプリケーション可用性に関する分析情報を提供し、デジタルエクスペリエンスの多面的な表示を可能にします。

Cisco IOS XE リリース 17.6.1 以降、アプリケーション ホスティング機能を使用して、Cisco ThousandEyes Enterprise Agent をコンテナアプリケーションとして Cisco 4000 シリーズ サービス統合型ルータ（ISR）に展開できます。このエージェント アプリケーションは、Cisco IOx

docker-type オプションを使用して docker イメージとして実行されます。コントローラモードで Cisco ThousandEyes を設定する方法の詳細については、『Cisco SD-WAN Systems and Interfaces Configuration Guide』を参照してください。

図 *1 : ThousandEyes* アプリケーションによるネットワークの表示



Cisco ThousandEyes Enterprise エージェント アプリケーションの機能情報

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

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

表 *17 : Cisco ThousandEyes Enterprise* エージェント アプリケーションの機能情報

機能名	リリース	機能情報
Cisco ThousandEyes Enterprise Agent アプリケーションのホスティング	Cisco IOS XE 17.7.1a	Cisco ThousandEyes Enterprise Agent アプリケーションには、デバイスからドメインネームサーバー（DNS）情報を継承する機能が導入されています。この機能強化により、vManage ThousandEyes 機能テンプレートの DNS フィールドはオプションのパラメータになりました。

機能名	リリース	機能情報
Cisco ThousandEyes Enterprise Agent アプリケーションのホスティング	Cisco IOS XE 17.6.1	アプリケーション ホスティング機能をコンテナとして使用して、ルーティング プラットフォームで実行される ThousandEyes エージェント アプリケーションを統合することで、インターネット、クラウドプロバイダー、およびエンタープライズ ネットワークに関する詳細な分析情報を用いてアプリケーション エクスペリエンスを可視化できます。

サポートされるプラットフォームとシステム要件

次の表に、サポートされるプラットフォームとシステム要件を示します。

表 *18*：サポートされるプラットフォームとシステム要件

プラットフォーム	ブートフラッシュ	FRU ストレージ	DRAM
Cisco ISR 4000 シリーズ			
ISR446x	8 GB	NIM-SSD（外部）	8 GB、16 GB、32 GB
ISR4451	8 GB	NIM-SSD（外部）	8 GB、16 GB
ISR4351/31	16 GB	NIM-SSD（外部）	8 GB、16 GB
ISR4321	8 GB	NIM-SSD（外部）	8 GB
ISR4221X	8 GB	NIM-SSD（外部）	8 GB

（注） Cisco ThousandEyes Enterprise Agent を実行するための最小 DRAM およびストレージの要件は 8 GB です。デバイスに十分なメモリまたはストレージがない場合は、DRAM をアップグレードするか、または M.2 USB などの外部ストレージを追加することをお勧めします。使用可能なリソースが他のアプリケーションを実行するのに十分でない場合、Cisco IOx はエラーメッセージを生成します。

Cisco ThousandEyes アプリケーションのインストールと実行のワークフロー

デバイスに Cisco ThousandEyes イメージをインストールして実行するには、次の手順を実行します。

ステップ 1 Cisco ThousandEyes ポータルで新しいアカウントを作成します。

ステップ 2 ソフトウェアのダウンロードページから Cisco ThousandEyes アプリケーションパッケージをダウンロードし、エージェントバージョン 4.0.2 を使用していることを確認します。

ステップ 3 デバイスでイメージをコピーします。

ステップ 4 イメージをインストールして起動します。

ステップ 5 エージェントをコントローラに接続します。

（注） Cisco IOS XE 17.6.1 ソフトウェアとともに Cisco ThousandEyes アプリケーションパッケージをサポートするプラットフォームを注文した場合、Cisco ThousandEyes アプリケーションパッケージはデバイスのブートフラッシュで使用できます。

Cisco ThousandEyes アプリケーションをホストするワークフロー

アプリケーションをインストールして起動するには、次の手順を実行します。

始める前に

Cisco ThousandEyes ポータルで新しいアカウントを作成し、トークンを生成します。Cisco ThousandEyes エージェント アプリケーションは、このトークンを使用して、正しい Cisco ThousandEyes アカウントを認証し、チェックインします。トークンが無効であるというメッセージが表示された場合に、その問題のトラブルシューティングを行うには、Cisco ThousandEyes アプリケーションのトラブルシューティング（166 ページ）のセクションを参照してください。

（注） 正しいトークンとドメインネームサーバー（DNS）情報を設定すると、デバイスが自動的に検出されます。

ステップ 1 デバイスで Cisco IOX アプリケーション環境を有効にします。

- 非 SD-WAN（自立モード）イメージには次のコマンドを使用します。

```
config terminal
 iox
end
write
```

- SD-WAN（コントローラモード）イメージには次のコマンドを使用します。

```
config-transaction
iox
commit
```

ステップ 2 IOx コマンドが受け入れられる場合は、数秒間待機してから、**show iox** コマンドを使用して IOx プロセスが動作しているかどうかを確認します。出力に、show IOxman プロセスが実行中であると表示される必要があります。

```
Device #show iox

IOx Infrastructure Summary:
---------------------------
IOx service (CAF) 10.11.0.0     : Running
IOx service (HA)               : Not Supported
IOx service (IOxman)           : Running
IOx service (Sec storage)      : Not Supported
Libvirtd 1.3.4                 : Running
```

ステップ 3 ThousandEyes アプリケーション LXC tarball がデバイスの *bootflash:* で使用可能であることを確認します。

ステップ 4 仮想ポート グループ インターフェイスを作成して、Cisco ThousandEyes アプリケーションへのトラフィックパスを有効にします。

```
interface VirtualPortGroup 0
          ip address 192.168.35.1 255.255.255.0
        exit
```

ステップ 5 生成されたトークンを使用して、アプリケーション ホスティング アプリケーションを設定します。

```
app-hosting appid te
          app-vnic gateway1 virtualportgroup 0 guest-interface 0
          guest-ipaddress 192.168.35.2 netmask 255.255.255.0
          app-default-gateway 192.168.35.1 guest-interface 0
          app-resource docker
                  prepend-pkg-opts □ Required to get the default run-time options from package.yaml

                   run-opts 1 "--hostname thousandeyes"
              run-opts 2 "-e TEAGENT_ACCOUNT_TOKEN=<ThousandEyes token>"
        run-opts 3 "-e TEAGENT_PROXY_TYPE=STATIC -e TEAGENT_PROXY_LOCATION=proxy.something.other:80"

          name-server0 10.75.75.75 □ ISP's DNS server
        end

app-hosting appid te
 app-resource docker
  prepend-pkg-opts
  run-opts 2 "--hostname
```

（注） プロキシ設定は、Cisco ThousandEyes エージェントがプロキシなしでインターネットにアクセスできない場合にのみ使用できます。また、ホスト名はオプションです。インストール時にホスト名を指定しない場合、デバイスのホスト名が Cisco ThousandEyes エージェントのホスト名として使用されます。デバイスのホスト名が Cisco ThousandEyes ポータルに表示されます。DNS ネームサーバー情報はオプションです。Cisco ThousandEyes エージェントがプライベート IP アドレスを使用する場合は、NAT 経由でデバイスへの接続を確立します。

ステップ 6 **install** コマンドを使用してアプリケーションがデバイスにインストールされたときに、アプリケーションを自動的に実行するように **start** コマンドを設定します。

```
app-hosting appid te
         start
```

ステップ 7 ThousandEyes アプリケーションをインストールします。

```
app-hosting install appid <appid> package [bootflash: | harddisk: | https:]
```

次のオプションから ThousandEyes アプリケーションをインストールする場所を選択します。

```
Device# app-hosting install appid te package ?
          bootflash:  Package path □ ISR4K case if image is locally available in bootflash:
          harddisk:   Package path □ Cat8K case if image is locally available in M.2 USB
          https:      Package path □ Download over the internet if image is not locally present in
 router. URL to ThousandEyes site hosting agent image to be provided here
```

ステップ 8 アプリケーションが動作しているかどうかを確認します。

```
Device#show app-hosting list
 App id                                   State
---------------------------------------------------------
  te                                       RUNNING
```

（注） これらの手順のいずれかに失敗した場合は、**show logging** コマンドを使用して IOx エラーメッセージを確認します。ディスク容量が不足しているというエラーメッセージが表示される場合は、ストレージメディア（ブートフラッシュまたはハードディスク）をクリーンアップして空き容量を増やします。**show app-hosting resource** コマンドを使用して、CPU とディスクメモリを確認します。

デバイスへのイメージのダウンロードとコピー

イメージをダウンロードしてブートフラッシュにコピーするには、次の手順を実行します。

ステップ 1 Cisco ThousandEyes イメージが bootflash:/<directory name> に事前にコピーされているかどうかを確認します。

ステップ 2 デバイスのディレクトリにイメージがない場合は、次の手順を実行します。

a) デバイスがインターネットに直接アクセスできる場合は、**application install command.** コマンドで https:. オプションを使用します。このオプションにより、Cisco ThousandEyes ソフトウェアのダウンロードページから bootflash:/apps にイメージがダウンロードされ、アプリケーションがインストールされます。

```
Device# app-hosting install appid <appid string> package [bootflash: | flash | http | https://
  | ftp | ] URL to image location hosted on ThousandEyes portal

Device# app-hosting install appid te1000 package
https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar

Installing package
'https://downloads.thousandeyes.com/enterprise-agent/thousandeyes-enterprise-agent-4.0.2.cisco.tar'
 for 'te1000'.

Use 'show app-hosting list' for progress.
*Jun 29 23:43:29.244: %IOSXE-6-PLATFORM: R0/0: IOx:  App verification successful
*Jun 29 23:45:00.449: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install succeeded: te1000
installed successfully Current state is DEPLOYED
```

```
*Jun 29 23:45:01.801: %IOSXE-6-PLATFORM: R0/0: IOx:  App verification successful
*Jun 29 23:45:51.054: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succeeded: te1000 started
 successfully Current state is RUNNING

Device#show app-hosting detail appid te1000  ( Details of Application)
App id                 : te1000
Owner                  : iox
State                  : RUNNING
Application
  Type                 : docker
  Name                 : ThousandEyes Enterprise Agent
  Version              : 4.0
  Author               : ThousandEyes <support@thousandeyes.com>
  Path                 : bootflash:thousandeyes-enterprise-agent-4.0-22.cisco.tar
Resource reservation
  Memory               : 500 MB
  Disk                 : 1 MB
  CPU                  : 1500 units
  CPU-percent          : 70 %
```

b) デバイスにプロキシサーバーがある場合は、イメージを bootflash:/apps に手動でコピーします。

c) ソフトウェアのダウンロードページから Cisco ThousandEyes アプリケーションパッケージをダウンロードし、エージェントバージョン 4.0.2 を使用していることを確認します。

d) bootflash: にアプリケーション ディレクトリを作成し、イメージをコピーします。

```
Device# mkdir bootflash:apps
Create directory filename [apps]?
Created dir bootflash:/apps
```

e) Cisco ThousandEyes イメージを *bootflash:apps* ディレクトリにコピーします。

f) **verify** コマンドを使用してイメージを検証します。

```
verify /md5 bootflash:apps/<file name>
```

Cisco ThousandEyes エージェントとコントローラの接続

始める前に

エージェントをコントローラに接続する前に、インターネットに接続していることを確認します。

Cisco ThousandEyes アプリケーションが稼働状態になると、エージェント（ThousandEyes エージェント）プロセスがクラウド環境で実行されているコントローラに接続します。

（注） 接続に関連する問題がある場合、関連するエラーメッセージがアプリケーション固有のログ（*/var/logs*）に記録されます。

エージェントのパラメータの変更

エージェントのパラメータを変更するには、次のアクションを実行します。

ステップ 1 **app-hosting stop appid appid** コマンドを使用して、アプリケーションを停止します。
ステップ 2 **app-hosting deactivate appid appid** コマンドを使用して、アプリケーションを非アクティブ化します。
ステップ 3 アプリケーション ホスティングの設定に必要な変更を加えます。
ステップ 4 **app-hosting activate appid appid** コマンドを使用して、アプリケーションをアクティブ化します。
ステップ 5 **app-hosting start appid appid**コマンドを使用して、アプリケーションを起動します。

アプリケーションのアンインストール

アプリケーションをアン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 **app-hosting stop appid te** コマンドを使用して、アプリケーションを停止します。
ステップ 2 **show app-hosting list** コマンドを使用して、アプリケーションがアクティブ状態であるかどうかを確認します。
ステップ 3 **app-hosting deactivate appid te** コマンドを使用して、アプリケーションを非アクティブ化します。
ステップ 4 アプリケーションがアクティブ状態でないことを確認します。**show app-hosting list** コマンドを使用して、アプリケーションのステータスを確認します。
ステップ 5 **app-hosting install appid te** コマンドを使用して、アプリケーションをアンインストールします。
ステップ 6 アンインストールプロセスが完了したら、**show app-hosting list** コマンドを使用して、アプリケーションが正常にアンインストールされたかどうかを確認します。

Cisco ThousandEyes アプリケーションのトラブルシューティング

Cisco ThousandEyes アプリケーションをトラブルシューティングするには、次の手順を実行します。

1. **app-hosting connect appid appid session /bin/bash** コマンドを使用して、Cisco ThousandEyes エージェント アプリケーションに接続します。
2. */etc/te-agent.cfg* でアプリケーションに適用されている設定を確認します。

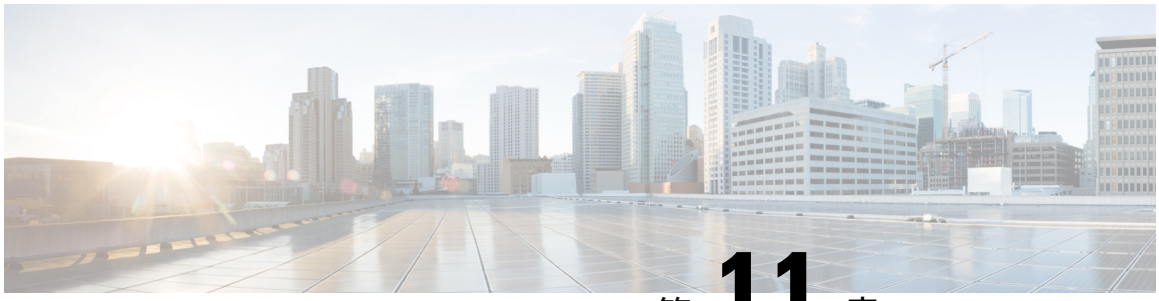
3. */var/log/agent/te-agent.log* のログを表示します。これらのログを使用して、設定のトラブルシューティングを行うことができます。

ThousandEyes アプリケーションのステータスの確認

Cisco ThousandEyes アプリケーションが実行状態の場合、ThousandEyes ポータルに登録されます。エージェントが実行状態になってから数分後にアプリケーションが表示されない場合は、**app-hosting connect appid thousandeyes_enterprise_agent session** コマンドを使用して次の点を確認してください。

```
Device#app-hosting connect appid thousandeyes_enterprise_agent session
Device# cat /var/log/agent/te-agent.log
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.AptPackageInterface] {} Initialized
APT package interface
2021-02-04 08:59:29.642 INFO  [e4736a40] [te.agent.main] {} Agent version 1.103.0 starting.
  Max core size is 0 and max open files is 1024
2021-02-04 08:59:29.642 DEBUG [e4736a40] [te.agent.db] {} Vacuuming database
2021-02-04 08:59:29.643 INFO  [e4736a40] [te.agent.db] {} Found version 0, expected
version 50
2021-02-04 08:59:29.672 INFO  [e4708700] [te.probe.ServerTaskExecutor] {} ProbeTaskExecutor
 started with 2 threads.
2021-02-04 08:59:29.673 INFO  [e2f05700] [te.probe.ProbeTaskExecutor.bandwidth] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO  [e2704700] [te.probe.ProbeTaskExecutor.realtime] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.673 INFO  [e1f03700] [te.probe.ProbeTaskExecutor.throughput] {}
ProbeTaskExecutor started with 1 threads.
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.agent.DnssecTaskProceessor] {} Agent is not
 running bind
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised
SNMP++ session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised
SNMP++ session
2021-02-04 08:59:29.674 DEBUG [e4736a40] [te.snmp.RequestDispatcher] {} Initialised
SNMP++ session
2021-02-04 08:59:29.674 INFO  [e4736a40] [te.agent.main] {} Agent starting up
2021-02-04 08:59:29.675 INFO  [e4736a40] [te.agent.main] {} No agent id found, attempting
 to obtain one
2021-02-04 08:59:29.675 INFO  [e4736a40] [te.agent.ClusterMasterAdapter] {} Attempting
to get agent id from sc1.thousandeyes.com
2021-02-04 08:59:29.679 ERROR [e4736a40] [te.agent.main] {} Error calling create_agent:
 Curl error - Couldn't resolve host name
2021-02-04 08:59:29.680 INFO  [e4736a40] [te.agent.main] {} Sleeping for 30 seconds
Note :
```

（注） DNS サーバーの接続を確認します。Cisco ThousandEyes エージェントがプライベート IP アドレスに割り当てられている場合は、NAT 設定を確認します。



第 11 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。次に、定期的な監視のメリットを示します。

- 数年にわたって稼働しているラインカードのメモリ不足が原因で、大規模な停止が発生する可能性があります。メモリの使用状況を監視することで、ラインカードのメモリの問題を特定でき、停止を防止できます。

- 定期的な監視によって、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。たとえば、8 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が表示されます。

```
Router# show memory
           Head            Total(b)     Used(b)     Free(b)      Lowest(b)    Largest(b)
Processor  2ABEA4316010   4489061884   314474916   4174586968   3580216380   3512323496
lsmpi_io   2ABFAFF471A8   6295128      6294212     916          916          916
Critical   2ABEB7C72EB0   1024004      92          1023912      1023912      1023912
```

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
   1         583     48054         12  0.00%  0.00%  0.00%   0 Chunk Manager
   2         991    176805          5  0.00%  0.00%  0.00%   0 Load Meter
   3           0         2          0  0.00%  0.00%  0.00%   0 IFCOM Msg Hdlr
   4           0        11          0  0.00%  0.00%  0.00%   0 Retransmission o
   5           0         3          0  0.00%  0.00%  0.00%   0 IPC ISSU Dispatc
   6      230385    119697       1924  0.00%  0.01%  0.00%   0 Check heaps
   7          49        28       1750  0.00%  0.00%  0.00%   0 Pool Manager
   8           0         2          0  0.00%  0.00%  0.00%   0 Timers
   9       17268    644656         26  0.00%  0.00%  0.00%   0 ARP Input
  10         197    922201          0  0.00%  0.00%  0.00%   0 ARP Background
  11           0         2          0  0.00%  0.00%  0.00%   0 ATM Idle Timer
  12           0         1          0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
  13           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  14           0         1          0  0.00%  0.00%  0.00%   0 Policy Manager
  15           0         2          0  0.00%  0.00%  0.00%   0 DDR Timers
  16           1        15         66  0.00%  0.00%  0.00%   0 Entity MIB API
  17          13      1195         10  0.00%  0.00%  0.00%   0 EEM ED Syslog
  18          93        46       2021  0.00%  0.00%  0.00%   0 PrstVbl
  19           0         1          0  0.00%  0.00%  0.00%   0 RO Notify Timers
```

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：ラインカードの合計メモリ
- 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-processor
RP0: online, statistics updated 5 seconds ago
Load Average: healthy
  1-Min: 0.07, status: healthy, under 5.00
  5-Min: 0.11, status: healthy, under 5.00
  15-Min: 0.09, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3971216
  Used: 3415976 (86%)
  Free: 555240 (14%)
  Committed: 2594412 (65%), status: healthy, under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.40, System:  1.20, Nice:  0.00, Idle: 97.39
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  0.89, System:  0.79, Nice:  0.00, Idle: 98.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  0.80, System:  2.50, Nice:  0.00, Idle: 96.70
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  3.09, System:  6.19, Nice:  0.00, Idle: 90.60
  IRQ:  0.00, SIRQ:  0.09, IOwait:  0.00
CPU4: CPU Utilization (percentage of time spent)
  User:  0.10, System:  0.30, Nice:  0.00, Idle: 99.60
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU5: CPU Utilization (percentage of time spent)
  User:  0.89, System:  1.59, Nice:  0.00, Idle: 97.50
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU6: CPU Utilization (percentage of time spent)
  User:  0.80, System:  1.10, Nice:  0.00, Idle: 98.10
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU7: CPU Utilization (percentage of time spent)
  User:  0.20, System:  3.40, Nice:  0.00, Idle: 96.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00


Router# show platform software status control-processor brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.09   0.10   0.09

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  3971216  3426452 (86%)   544764 (14%)   2595212 (65%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   1.60   0.90   0.00  97.30   0.10   0.10   0.00
         1   0.09   1.29   0.00  98.60   0.00   0.00   0.00
         2   0.10   0.10   0.00  99.79   0.00   0.00   0.00
         3   0.00   0.00   0.00 100.00   0.00   0.00   0.00
```

```
4    0.60    4.90    0.00   94.50    0.00    0.00    0.00
5    0.70    1.30    0.00   98.00    0.00    0.00    0.00
6    0.10    0.00    0.00   99.90    0.00    0.00    0.00
7    1.39    0.49    0.00   98.10    0.00    0.00    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。

```
Aug 22 13:40:41.038 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 7084440 kB] - Please clean up files on bootflash.
```

ブートフラッシュディスクのサイズは、少なくともルータに搭載されている物理メモリと同じサイズでなければなりません。この条件を満たしていない場合、次の例に示すようなsyslogアラームが生成されます。

```
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Flash capacity (8 GB) is insufficient for fault
analysis based on
installed memory of RP (16 GB)
%IOSXEBOOT-2-FLASH_SIZE_CHECK: (rp/0): Please increase the size of installed flash to
at least 16 GB (same as
physical memory size)
```

ハードウェア アラームの監視方法

• 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 （177 ページ）

オンサイトのネットワーク管理者が可聴アラームまたは可視アラームに対応する

• 可聴アラームと可視アラームについて （174 ページ）
• 可聴アラームのクリア （174 ページ）
• 可視アラームのクリア （174 ページ）

可聴アラームと可視アラームについて

電源モジュールの DB-25 アラーム コネクタを使用することにより、外部デバイスを電源モジュールに接続できます。外部デバイスは視覚アラーム用 DC 電球または聴覚アラーム用ベルです。

ルータの前面プレートにある CRIT、MIN、または MAJ のいずれかの LED がアラームによって点灯する場合、可視アラームまたは可聴アラームが有線接続されていると、アラームによって電源 DB-25 コネクタのアラーム リレーも作動し、ベルが鳴るか、または電球が点滅します。

可聴アラームのクリア

可聴アラームを解除するには、次のいずれかの作業を行います。

• 前面プレートの **Audible Cut Off** ボタンを押す
• **clear facility-alarm** コマンドを入力する

可視アラームのクリア

視覚アラームを解除するには、アラーム条件を解決する必要があります。**clear facility-alarm** コマンドを入力しても、前面プレートのアラーム LED の解除や DC 電球の消灯はできません。たとえば、アクティブなモジュールをグレースフルに非アクティブ化せずに取り外したためにクリティカル アラーム LED が点灯した場合、このアラームを解決する唯一の方法はモジュールを再度取り付けることです。

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 （175 ページ）
• アラーム メッセージの例 （175 ページ）
• アラーム メッセージの確認と分析 （177 ページ）

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。

アラーム メッセージの例

正しい非アクティブ化の実行前にモジュールが取り外された場合にコンソールに送信されるアラーム メッセージの例を、次に示します。モジュールを再び装着すると、アラームは消去されます。

モジュールが取り外された場合

```
*Aug 22 13:27:33.774: %ISR4451-X_OIR-6-REMSPA: Module removed from subslot 1/1, interfaces
 disabled
*Aug 22 13:27:33.775: %SPA_OIR-6-OFFLINECARD: Module (SPA-4XT-SERIAL) offline in subslot
 1/1
```

モジュールが再び装着された場合

```
*Aug 22 13:32:29.447: %ISR4451-X_OIR-6-INSSPA: Module inserted in subslot 1/1
*Aug 22 13:32:34.916: %SPA_OIR-6-ONLINECARD: Module (SPA-4XT-SERIAL) online in subslot
1/1
*Aug 22 13:32:35.523: %LINK-3-UPDOWN: SIP1/1: Interface EOBC1/1, changed state to up
```

アラーム

アラームを表示するには、**show facility-alarm status** コマンドを使用します。電源のクリティカル アラームの例を次に示します。

```
Router# show facility-alarm status
System Totals  Critical: 5  Major: 0  Minor: 0

Source                    Severity      Description [Index]
------                    --------      -------------------
Power Supply Bay 0        CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/1      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/2      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/3      INFO          Physical Port Link Down [1]
xcvr container 0/0/0      INFO          Transceiver Missing [0]
xcvr container 0/0/1      INFO          Transceiver Missing [0]
xcvr container 0/0/2      INFO          Transceiver Missing [0]
xcvr container 0/0/3      INFO          Transceiver Missing [0]
```

クリティカルアラームを表示するには、次の例に示すように **show facility-alarm status critical** コマンドを使用します。

```
Router# show facility-alarm status critical
System Totals  Critical: 5  Major: 0  Minor: 0

Source                    Severity      Description [Index]
------                    --------      -------------------
Power Supply Bay 0        CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/1      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/2      INFO          Physical Port Link Down [1]
GigabitEthernet0/0/3      INFO          Physical Port Link Down [1]
```

ルータの主要ハードウェアコンポーネントの動作状態を表示するには、**show platform diag** コマンドを使用します。次の例は、電源 P0 で障害が発生したことを示します。

```
Router# show platform diag
Chassis type: ISR4451/K9

Slot: 0, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:42 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA
101]

Sub-slot: 0/0, ISR4451-4X1GE
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:02:48 (1w0d ago)
  Logical insert detect time  : 00:02:48 (1w0d ago)

Slot: 1, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:43 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA
101]

Slot: 2, ISR4451-NGSM
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:44 (1w0d ago)
  CPLD version                : 12061320
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA
101]

Slot: R0, ISR4451/K9
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:09 (1w0d ago)
  CPLD version                : 12061320
```

```
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA
101]

Slot: F0, ISR4451-FP
  Running state               : init, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:09 (1w0d ago)
  Software declared up time   : 00:01:37 (1w0d ago)
  Hardware ready signal time  : 00:00:00 (never ago)
  Packet ready signal time    : 00:00:00 (never ago)
  CPLD version                :
  Firmware version            : 12.2(20120618:163328)[ciscouser-ESGROM_20120618_GAMMA
101]

Slot: P0, Unknown
  State                       : ps, fail
  Physical insert detect time : 00:00:00 (never ago)

Slot: P1, XXX-XXXX-XX
  State                       : ok
  Physical insert detect time : 00:01:26 (1w0d ago)

Slot: P2, ACS-4450-FANASSY
  State                       : ok
  Physical insert detect time : 00:01:26 (1w0d ago)
```

アラーム メッセージの確認と分析

アラームメッセージの確認を容易にするために、コンソールまたはsyslogに送信されたアラームメッセージを分析するスクリプトを作成できます。スクリプトは、アラーム、セキュリティの警告、インターフェイスのステータスなどのイベントに関するレポートを表示できます。

syslog メッセージも、CISCO-SYSLOG-MIB に定義されている履歴表を使用して、簡易ネットワーク管理プロトコル（SNMP）経由でアクセスできます。

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

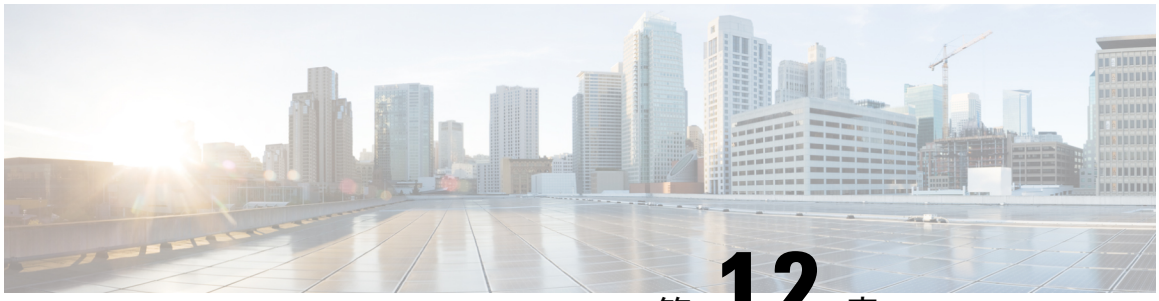
アプリケーション層プロトコルであるSNMPは、ネットワーク内のデバイスを監視および管理するための、標準化されたフレームワークと共通の言語を提供します。アラームを監視するすべての方法の中で、SNMPは、エンタープライズとサービスプロバイダのセットアップで複数のルータを監視するための最適な方法です。

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, RFC 4133（CISCO-ENTITY-ALARM-MIB および CISCO-ENTITY-SENSOR-MIB の稼働に必要）
- CISCO-ENTITY-ALARM-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 12 章

システム メッセージ

システム メッセージは、ログ ファイルに保存されるか、またはルータで実行中のソフトウェアから他のデバイスに転送されます。これらのメッセージは syslog メッセージとも呼ばれます。システム メッセージは、監視およびトラブルシューティングのためのロギング情報を提供します。

この章で説明する内容は、次のとおりです。

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`

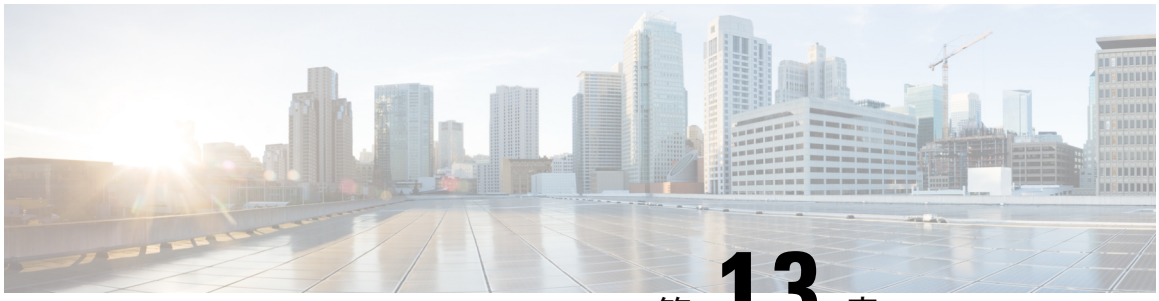
説明	推奨処置
プロセスのグレースフル シャットダウンが完了しました。	ユーザによる操作は必要ありません。このメッセージは、通知目的で示されます。

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 13 章

トレース管理

この章で説明する内容は、次のとおりです。

トレースの概要

トレースは、内部イベントをログする機能です。トレース メッセージを含むトレース ファイルが自動的に作成され、ルータの hard disk: ファイル システムの tracelogs ディレクトリに保存されます（ブートフラッシュにトレース ファイルが保存されます）。

トレースファイルのデータは、次の処理を行う場合に役立ちます。

- トラブルシューティング：ルータの問題を特定して解決するのに役立ちます。システムで他の問題が同時に発生している場合でも、診断モードでトレースファイルにアクセスできます。
- デバッグ：システム アクションと操作の詳細を取得するのに役立ちます。

トレースの機能

トレースは、ルータの内部イベントの内容を記録します。モジュールに関するすべてのトレース出力を含むトレース ファイルが定期的に作成および更新され、tracelog ディレクトリに保存されます。トレースファイルは、システムパフォーマンスに影響を及ぼすことなく、このディレクトリから消去して、ファイルシステムのスペースを回復することができます。ファイル転送機能（FTP、TFTP など）を使用してこれらのファイルを他の宛先にコピーできます。また、プレーン テキスト エディタで開くことができます。

（注） ルータでトレースをディセーブルにすることはできません。

トレース情報を表示し、トレース レベルを設定するには、次のコマンドを使用します。

- **show platform software trace message**：特定のモジュールに関する最新のトレース情報を表示します。このコマンドは特権EXECモードおよび診断モードで使用可能です。診断モードでこのコマンドを使用すると、Cisco IOS XEの障害発生時にトレース ログ情報を収集できます。
- **set platform software trace**：出力に保存されるメッセージのタイプを決定するトレースレベルを設定します。トレース レベルの詳細については、トレースレベル （188ページ）を参照してください。

トレースレベル

トレースレベルは、トレースバッファまたはトレースファイルに保存する必要のあるモジュール情報の量を決定します。

次の表に、使用可能なすべてのトレース レベルと、各トレース レベルで表示されるメッセージのタイプについて説明します。

表 *19*：トレースレベルとその内容

トレースレベル	レベル番号	説明
Emergency	0	システムが使用不能になる問題のメッセージです。
[Alert]	1	ただちに対応する必要のある動作についてのメッセージです。
クリティカル	2	クリティカルな状態についてのメッセージです。これは、ルータ上のすべてのモジュールに関するデフォルト設定です。
Error	3	システムエラーについてのメッセージです。
Warning	4	システム警告についてのメッセージです。

トレースレベル	レベル番号	説明
Notice	5	重大な問題に関するメッセージです。ただし、ルータは通常どおり動作しています。
Informational	6	単に情報を提供するだけのメッセージです。
Debug	7	デバッグレベルの出力を提供するメッセージです。
Verbose	8	生成可能なすべてのトレースメッセージが送信されます。
Noise	—	モジュールについて生成可能なすべてのトレース メッセージが記録されます。 ノイズレベルは常に最上位のトレースレベルに相当します。トレース機能の今後の拡張によって、Verbose レベルよりも高いトレース レベルが導入される場合でも、Noise レベルは新規に導入されるトレース レベルと同等になります。

トレース レベルが設定されている場合、設定されているトレース レベル自体と、それより低いすべてのトレース レベルの両方のメッセージが収集されます。

たとえば、トレース レベルを 3（エラー）に設定すると、トレース ファイルにはレベル 0（緊急）、1（アラート）、2（重要）、および 3（エラー）のメッセージが出力されます。

トレース レベルを 4（警告）に設定すると、レベル 0（緊急）、1（アラート）、2（重要）、3（エラー）、および 4（警告）のメッセージが出力されます。

ルータのすべてのモジュールのデフォルト トレース レベルは 5（通知）です。

トレース レベルは、コンフィギュレーション モードでは設定されません。このため、ルータのリロード後にトレース レベル設定がデフォルト値に戻ります。

⚠

注意 モジュールのトレース レベルをデバッグ レベル以上に設定すると、パフォーマンスに悪影響を及ぼす可能性があります。

注意 多数のモジュールで高いトレース レベルを設定すると、パフォーマンスが大幅に低下する可能性があります。特定の状況で高いトレース レベルが必要な場合は、複数のモジュールで高いレベルを設定する代わりに、常に1つのモジュールのトレース レベルを高く設定することをお勧めします。

トレース レベルの表示

デフォルトでは、ルータ上のすべてのモジュールが 5（通知）に設定されます。ユーザが変更しないかぎり、この設定はそのまま維持されます。

ルータのモジュールのトレースレベルを表示するには、特権EXECモードまたは診断モードで **show platform software trace level** コマンドを入力します。

次の例では、**show platform software trace level** コマンドを使用して、アクティブなRP上のフォワーディング マネージャ プロセスのトレースレベルを表示します。

```
Router# show platform software trace level forwarding-manager rp active
Module Name                      Trace Level
-------------------------------------------------
acl                              Notice
binos                            Notice
binos/brand                      Notice
bipc                             Notice
bsignal                          Notice
btrace                           Notice
cce                              Notice
cdllib                           Notice
cef                              Notice
chasfs                           Notice
chasutil                         Notice
erspan                           Notice
ess                              Notice
ether-channel                    Notice
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
fman_rp                          Notice
fpm                              Notice
fw                               Notice
icmp                             Notice
interfaces                       Notice
iosd                             Notice
ipc                              Notice
ipclog                           Notice
iphc                             Notice
IPsec                            Notice
mgmte-acl                        Notice
mlp                              Notice
mqipc                            Notice
nat                              Notice
nbar                             Notice
netflow                          Notice
om                               Notice
peer                             Notice
qos                              Notice
```

```
route-map                       Notice
sbc                             Notice
services                        Notice
sw_wdog                         Notice
tdl_acl_config_type             Notice
tdl_acl_db_type                 Notice
tdl_cdlcore_message             Notice
tdl_cef_config_common_type      Notice
tdl_cef_config_type             Notice
tdl_dpidb_config_type           Notice
tdl_fman_rp_comm_type           Notice
tdl_fman_rp_message             Notice
tdl_fw_config_type              Notice
tdl_hapi_tdl_type               Notice
tdl_icmp_type                   Notice
tdl_ip_options_type             Notice
tdl_ipc_ack_type                Notice
tdl_IPsec_db_type               Notice
tdl_mcp_comm_type               Notice
tdl_mlp_config_type             Notice
tdl_mlp_db_type                 Notice
tdl_om_type                     Notice
tdl_ui_message                  Notice
tdl_ui_type                     Notice
tdl_urpf_config_type            Notice
tdllib                          Notice
trans_avl                       Notice
uihandler                       Notice
uipeer                          Notice
uistatus                        Notice
urpf                            Notice
vista                           Notice
wccp                            Notice
```

トレース レベルの設定

ルータに含まれる1つのモジュールのトレースレベル、またはルータにおける特定プロセスに含まれるすべてのモジュールのトレースレベルを設定するには、特権EXECモードまたは診断モードで **set platform software trace** コマンドを入力します。

次の例では、スロット 0 の ESP プロセッサの Forwarding Manager で ACL モジュールに関するトレースレベルを `info` に設定します。

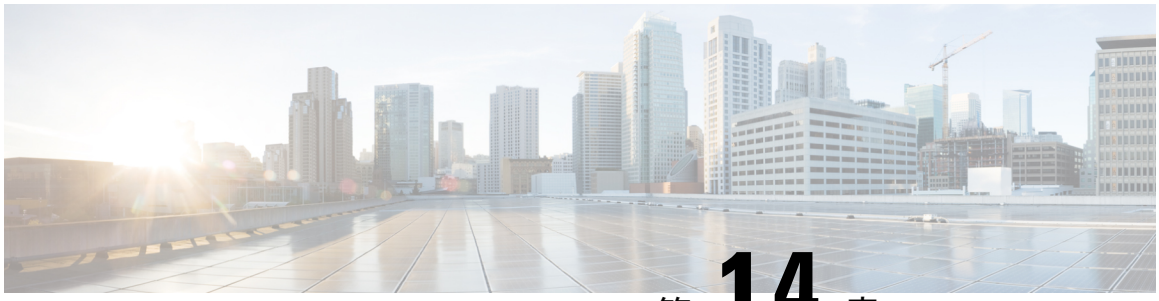
```
set platform software trace forwarding-manager F0 acl info
```

トレース バッファのデータの表示

トレースバッファ内またはファイル内のトレースメッセージを表示するには、特権EXECモードまたは診断モードで **show platform software trace message** コマンドを入力します。次の例では、**show platform software trace message** コマンドを使用して、RP スロット 0 の Host Manager プロセスのトレースメッセージを表示します。

```
Router# show platform software trace message host-manager R0
08/23 12:09:14.408 [uipeer]: (info): Looking for a ui_req msg
08/23 12:09:14.408 [uipeer]: (info): Start of request handling for con 0x100a61c8
```

```
08/23 12:09:14.399 [uipeer]: (info): Accepted connection for 14 as 0x100a61c8
08/23 12:09:14.399 [uipeer]: (info): Received new connection 0x100a61c8 on descriptor
14
08/23 12:09:14.398 [uipeer]: (info): Accepting command connection on listen fd 7
08/23 11:53:57.440 [uipeer]: (info): Going to send a status update to the shell manager
 in slot 0
08/23 11:53:47.417 [uipeer]: (info): Going to send a status update to the shell manager
 in slot 0
```



第 14 章

パケットトレース

初版：2016 年 8 月 3 日

パケットトレース機能は、Cisco IOS XE プラットフォームによってデータパケットがどのように処理されているのかを詳細に理解できます。これは、ユーザーが問題を診断し、より効率的にトラブルシューティングするために役立ちます。このモジュールは、パケットトレース機能の使用方法に関する情報を提供します。

パケットトレースについて

パケットトレース機能は、アカウンティング、サマリー、パスデータという 3 つのレベルのパケット検査を提供します。各レベルは、一部のパケット処理機能を犠牲にして、パケット処理の詳細なビューを提供します。ただし、パケットトレースは、debug platform condition ステートメントに一致するパケットの検査を制限し、大量のトラフィックが発生する環境下でも実行可能なオプションです。

次の表で、パケットトレースによって提供される 3 つのレベルの検査について説明します。

表 *20 :* パケットトレースレベル

パケットトレースレベル	説明
アカウンティング	パケットトレースのアカウンティングでは、ネットワークプロセッサに出入りするパケット数が示されます。パケットトレースのアカウンティングは負荷の軽いパフォーマンス アクティビティであり、無効化されるまで継続的に実行されます。
サマリー	パケットトレースのサマリーレベルでは、限られた数のパケットデータが収集されます。パケットトレースのサマリーは、入力インターフェイスと出力インターフェイス、最終的なパケットの状態、およびパケットのパント、ドロップ、インジェクションを随時追跡します。サマリーデータの収集は、通常のパケット処理と比較してパフォーマンスが高く、問題のあるインターフェイスを分離するのに役立ちます。
パスデータ	パケットトレースのパスデータレベルでは、パケットトレースが最も詳細なレベルで実行されます。限られた数のパケットを対象にデータが収集されます。パケットトレースのパスデータでは、条件付きデバッグIDを含むデータがキャプチャされます。このデータは、機能デバッグ、タイムスタンプ、および機能固有のパストレースデータと関連付ける際に役立ちます。 パスデータには、パケットコピーと Feature Invocation Array（FIA）トレースという 2 つのオプション機能もあります。パケットコピーオプションを使用すると、パケットの各種レイヤ（レイヤ 2、レイヤ 3、レイヤ 4）で入力パケットや出力パケットをコピーできます。FIA トレースオプションは、パケット処理中に呼び出されたすべての機能エントリを追跡します。このオプションは、パケット処理中に何が起こっているかを把握する際に役立ちます。 （注） パスデータの収集では、多くのパケット処理リソースが消費されます。また、オプション機能はパケットパフォーマンスに徐々に影響を及ぼします。そのため、パスデータレベルは限定的なキャパシティで使用するか、パケットパフォーマンスの変化が許容できる状況で使用してください。

パケットトレースの設定に関する使用上のガイドライン

パケットトレース機能を設定する際は、次のベストプラクティスを考慮してください。

- パケットをより包括的に表示するには、パケットトレース機能を使用する際に入力条件を使用することを推奨します。
- パケットトレースの設定には、データプレーンメモリが必要です。データプレーンメモリが制限されているシステムでは、パケットトレース値をどのように選択するかを慎重に検討してください。パケットトレースによって消費されるメモリ量の概算値は、次の式で求められます。

必要なメモリ＝（統計オーバーヘッド）＋（パケット数）＊（サマリーサイズ＋データサイズ＋パケットコピーサイズ）。

パケットトレース機能を有効にすると、統計用に少量の固定メモリが割り当てられます。同様に、パケットごとのデータをキャプチャする場合、サマリーデータ用に各パケットに少量の固定メモリが必要です。ただし、式が示すように、トレース対象に選択したパケット数や、パスデータとパケットのコピーを収集するかどうかによって、消費されるメモリ量が大きく影響される可能性があります。

パケットトレースの設定

パケットトレース機能を設定するには、次の手順を実行します。

（注） パケットトレース機能によって消費されるメモリの量は、パケットトレース設定の影響を受けます。通常のサービスの中断を避けるために、パケットごとのパスデータとコピーバッファのサイズ、およびトレースするパケット数を慎重に選択する必要があります。**show platform hardware qfp active infrastructure exmem statistics** コマンドを使用すると、現在のデータプレーンの DRAM メモリ消費量をチェックできます。

手順の概要

1. **enable**
2. **debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]**
3. **debug platform packet-trace {punt |inject|copy|drop|packet|statistics}**
4. **debug platform condition [ipv4 | ipv6] [interface** *interface***][access-list** *access-list -name* **|** *ipv4-address / subnet-mask* **|** *ipv6-address / subnet-mask***] [ingress | egress |both]**
5. **debug platform condition start**
6. **debug platform condition stop**
7. **show platform packet-trace {configuration | statistics | summary | packet {all |** *pkt-num***}}**
8. **clear platform condition all**
9. **exit**

手順の詳細

	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 モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]** 例： `Router# debug platform packet-trace packets 2048 summary-only`	指定した数のパケットのサマリーデータを収集します。デフォルトでは機能パスデータをキャプチャし、必要に応じて FIA トレースを実行します。 *pkt-num*：所定の時間に維持されるパケットの最大数を指定します。 **fia-trace**：サマリーデータ、機能固有のデータなど、詳細なレベルのデータキャプチャを実行します。また、パケット処理中にアクセスされた各機能エントリも表示します。 **summary-only**：詳細情報を最小限にしたサマリーデータのキャプチャを有効にします。 **circular**：最近トレースされたパケットのデータを保存します。 *data-size*：各パケットの機能データと FIA トレースデータを保存するデータバッファのサイズをバイト単位で指定します。パケットで非常に重いパケット処理が実行された場合、ユーザーは必要に応じてデータバッファのサイズを増やすことができます。デフォルト値は 2048 です。
ステップ 3	**debug platform packet-trace {punt |inject|copy|drop|packet|statistics}** 例： `Router# debug platform packet-trace punt`	データからコントロールプレーンへパントされたパケットのトレースを有効にします。
ステップ 4	**debug platform condition [ipv4 | ipv6] [interface** *interface***][access-list** *access-list -name* **|** *ipv4-address / subnet-mask* **|** *ipv6-address / subnet-mask***] [ingress | egress |both]** 例： `Router# debug platform condition interface g0/0/0 ingress`	パケットをトレースするための一致基準を指定します。プロトコル、IP アドレスおよびサブネットマスク、アクセス制御リスト（ACL）、インターフェイス、方向によるフィルタリング機能を提供します。
ステップ 5	**debug platform condition start** 例： `Router# debug platform condition start`	指定した位置基準を有効にしてパケットトレースを開始します。
ステップ 6	**debug platform condition stop** 例：	条件を非アクティブにして、パケットのトレースを停止します。

	コマンドまたはアクション	目的
	`Router# debug platform condition start`	
ステップ 7	**show platform packet-trace {configuration | statistics | summary | packet {all | *pkt-num*}}** 例： `Router# show platform packet-trace 14`	指定されたオプションに従って、パケットトレースデータを表示します。**show** コマンドのオプションの詳細については、{start cross reference} 表 21-1 {end cross reference} を参照してください。
ステップ 8	**clear platform condition all** 例： `Router(config)# clear platform condition all`	**debug platform condition** コマンドおよび **debug platform packet-trace** コマンドによって提供された設定を削除します。
ステップ 9	**exit** 例： `Router# exit`	特権 EXEC モードを終了します。

UDF オフセットを使用したパケットトレーサの設定

オフセットを使用してパケットトレース UDF を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **udf** *udf name* **header** {**inner | outer**} {**13**|**14**} **offset** *offset-in-bytes* **length** *length-in-bytes*
4. **udf** *udf name* {**header | packet-start**} *offset-base offset length*
5. **ip access-list extended** {*acl-name* |*acl-num*}
6. **ip access-list extended { deny | permit } udf udf-name value mask**
7. **debug platform condition [ipv4 | ipv6] [interface** *interface***] [access-list** *access-list -name* **|** *ipv4-address / subnet-mask* **|** *ipv6-address / subnet-mask***] [ingress | egress |both]**
8. **debug platform condition start**
9. **debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]**
10. **debug platform packet-trace {punt | inject|copy | drop |packet | statistics}**
11. **debug platform condition stop**
12. **exit**

手順の詳細

	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	**udf** *udf name* **header** {**inner** | **outer**} {**13**|**14**} **offset** *offset-in-bytes* **length** *length-in-bytes*
	例：
	`Router(config)# udf TEST_UDF_NAME_1 header inner l3 64 1`
	`Router(config)# udf TEST_UDF_NAME_2 header inner l4 77 2`
	`Router(config)# udf TEST_UDF_NAME_3 header outer l3 65 1`
	`Router(config)# udf TEST_UDF_NAME_4 header outer l4 67 1`
		個々の UDF 定義を設定します。UDF の名前、オフセット元のネットワーキングヘッダー、抽出するデータの長さを指定できます。
		inner キーワードまたは **outer** キーワードは、カプセル化されていないレイヤ 3 またはレイヤ 4 のヘッダーからのオフセットの開始を指定するか、またはカプセル化されたパケットがある場合は内部 L3/L4 からのオフセットの開始を指定します。
		length キーワードはオフセットからの長さをバイト単位で指定します。有効な範囲は 1 ～ 2 です。

ステップ 4	**udf** *udf name* {**header** | **packet-start**} *offset-base offset length* 例： `Router(config)# udf TEST_UDF_NAME_5 packet-start 120 1`	• header：オフセットの基本設定を指定します。 • packet-start：packet-start からのオフセットベースを指定します。packet-start は、パケットトレースがインバウンドパケット用かアウトバウンドパケット用かによって異なります。パケットトレースがインバウンドパケット用である場合、パケット開始はレイヤ 2 になります。アウトバウンドの場合は、packet-start はレイヤ 3 になります。 • offset：オフセット ベースからオフセットさせるバイト数を指定します。オフセット ベース（レイヤ 3/レイヤ 4 ヘッダー）からの先頭バイトに一致させるには、オフセットを 0 に設定します。 • length：オフセットからのバイト数を指定します。1 バイトまたは 2 バイトだけがサポートされます。追加のバイト数に一致させるには、複数の UDF の定義が必要です。

	コマンドまたはアクション	目的
ステップ 5	**ip access-list extended** {*acl-name* |*acl-num*} 例： `Router(config)# ip access-list extended acl2`	拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。拡張 ACL は、IP パケットの送信元アドレスおよび宛先アドレスを ACL に設定されているアドレスと比較して、トラフィックを制御します。
ステップ 6	**ip access-list extended { deny | permit } udf udf-name value mask** 例： `Router(config-acl)# permit ip any any udf TEST_UDF_NAME_5 0xD3 0xFF`	現在のアクセス制御エントリ（ACE）と併せて、UDF で一致するように ACL を設定します。ACL で定義されているバイトは 0xD3 です。マスクは、許可および拒否するトラフィックを指定するように、IP ACL で IP アドレスとともに使用します。
ステップ 7	**debug platform condition [ipv4 | ipv6] [interface** *interface***] [access-list** *access-list -name* **|** *ipv4-address / subnet-mask* **|** *ipv6-address / subnet-mask***] [ingress | egress |both]** 例： `Router# debug platform condition interface gi0/0/0 ipv4 access-list acl2 both`	パケットをトレースするための一致基準を指定します。プロトコル、IP アドレスおよびサブネットマスク、アクセス制御リスト（ACL）、インターフェイス、方向によるフィルタリング機能を提供します。
ステップ 8	**debug platform condition start** 例： `Router# debug platform condition start`	指定した位置基準を有効にしてパケットトレースを開始します。
ステップ 9	**debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]** 例： `Router# debug platform packet-trace packet 1024 fia-trace data-size 2048`	指定した数のパケットのサマリーデータを収集します。デフォルトでは機能パスデータをキャプチャし、必要に応じて FIA トレースを実行します。 *pkt-num*：所定の時間に維持されるパケットの最大数を指定します。 **fia-trace**：サマリーデータ、機能固有のデータなど、詳細なレベルのデータキャプチャを実行します。また、パケット処理中にアクセスされた各機能エントリも表示します。 **summary-only**：詳細情報を最小限にしたサマリーデータのキャプチャを有効にします。 **circular**：最近トレースされたパケットのデータを保存します。

	コマンドまたはアクション	目的
		data-size：各パケットの機能データとFIAトレースデータを保存するデータバッファのサイズをバイト単位で指定します。パケットで非常に重いパケット処理が実行された場合、ユーザーは必要に応じてデータバッファのサイズを増やすことができます。デフォルト値は2048です。
ステップ10	**debug platform packet-trace {punt | inject|copy | drop |packet | statistics}** 例： `Router# debug platform packet-trace punt`	データからコントロールプレーンへパントされたパケットのトレースを有効にします。
ステップ11	**debug platform condition stop** 例： `Router# debug platform condition start`	条件を非アクティブにして、パケットのトレースを停止します。
ステップ12	**exit** 例： `Router# exit`	特権EXECモードを終了します。

パケットトレース情報の表示

パケットトレース情報を表示するには、次の **show** コマンドを使用します。

表 *21 : show* コマンド

コマンド	説明
show platform packet-trace configuration	デフォルトを含むパケットトレース設定が表示されます。
show platform packet-trace statistics	トレースされたすべてのパケットのアカウンティングデータが表示されます。
show platform packet-trace summary	指定した数のパケットのサマリーデータが表示されます。
show platform packet-trace {all | *pkt-num*} [decode]	すべてのパケットまたは指定したパケットのパスデータが表示されます。**decode** オプションを使用すると、バイナリパケットのより人間が判読しやすい形式へのデコードが試みられます。

パケットトレースデータの削除

パケットトレースデータをクリアするには、次のコマンドを使用します。

表 *22 : clear* コマンド

コマンド	説明
clear platform packet-trace statistics	収集されたパケットトレースデータと統計をクリアします。
clear platform packet-trace configuration	パケットトレース設定と統計をクリアします。

パケットトレースの設定例

ここでは、次の設定例について説明します。

例：パケットトレースの設定

この例では、パケットトレースを設定し、結果を表示する方法について説明します。この例では、ギガビットイーサネットインターフェイス 0/0/1 への着信パケットがトレースされ、最初の 128 パケットの FIA トレースデータがキャプチャされます。また、入力パケットがコピーされます。**show platform packet-trace packet 0** コマンドにより、パケット 0 について、概要データと、パケット処理中にアクセスされた各機能エントリが表示されます。

```
Router>
enable
Router# debug platform packet-trace packet 128 fia-trace
Router# debug platform packet-trace punt
Router# debug platform condition interface g0/0/1 ingress
Router# debug platform condition start
Router#! ping to UUT
Router# debug platform condition stop
Router# show platform packet-trace packet 0
Packet: 0           CBUG ID: 9
Summary
  Input     : GigabitEthernet0/0/1
  Output    : GigabitEthernet0/0/0
  State     : FWD
  Timestamp
    Start   : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
    Stop    : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
  Feature: IPV4
    Source      : 192.0.2.1
    Destination : 192.0.2.2
    Protocol    : 1 (ICMP)
  Feature: FIA_TRACE
    Entry     : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
    Timestamp : 3685243309297
```

```
  Feature: FIA_TRACE
    Entry     : 0x82011a00 - IPV4_INPUT_DST_LOOKUP_CONSUME
    Timestamp : 3685243311450
  Feature: FIA_TRACE
    Entry     : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
    Timestamp : 3685243312427
  Feature: FIA_TRACE
    Entry     : 0x82004b68 - IPV4_OUTPUT_LOOKUP_PROCESS
    Timestamp : 3685243313230
  Feature: FIA_TRACE
    Entry     : 0x8034f210 - IPV4_INPUT_IPOPTIONS_PROCESS
    Timestamp : 3685243315033
  Feature: FIA_TRACE
    Entry     : 0x82013200 - IPV4_OUTPUT_GOTO_OUTPUT_FEATURE
    Timestamp : 3685243315787
  Feature: FIA_TRACE
    Entry     : 0x80321450 - IPV4_VFR_REFRAG
    Timestamp : 3685243316980
  Feature: FIA_TRACE
    Entry     : 0x82014700 - IPV6_INPUT_L2_REWRITE
    Timestamp : 3685243317713
  Feature: FIA_TRACE
    Entry     : 0x82000080 - IPV4_OUTPUT_FRAG
    Timestamp : 3685243319223
  Feature: FIA_TRACE
    Entry     : 0x8200e500 - IPV4_OUTPUT_DROP_POLICY
    Timestamp : 3685243319950
  Feature: FIA_TRACE
    Entry     : 0x8059aff4 - PACTRAC_OUTPUT_STATS
    Timestamp : 3685243323603
  Feature: FIA_TRACE
    Entry     : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
    Timestamp : 3685243326183

Router# clear platform condition all
Router# exit
```

LFTS（Linux Forwarding Transport Service）は、CPP からパントされたパケットを IOSd 以外のアプリケーションに転送するトランスポートメカニズムです。この例では、インターセプトされた binos アプリケーション宛ての LFTS ベースのパケットが表示されてます。

```
Router# show platform packet-trace packet 10
Packet: 10     CBUG ID: 52
Summary
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  State  : PUNT 55 (For-us control)
  Timestamp
    Start : 597718358383 ns (06/06/2016 09:00:13.643341 UTC)
    Stop : 597718409650 ns (06/06/2016 09:00:13.643392 UTC)
Path Trace
  Feature: IPV4
    Input  : GigabitEthernet0/0/0
    Output : <unknown>
    Source : 10.64.68.2
    Destination : 10.0.0.102
    Protocol : 17 (UDP)
      SrcPort : 1985
      DstPort : 1985
  Feature: FIA_TRACE
    Input  : GigabitEthernet0/0/0
    Output : <unknown>
    Entry  : 0x8a0177bc - DEBUG_COND_INPUT_PKT
    Lapsed time : 426 ns
```

```
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : <unknown>
  Entry  : 0x8a017788 - IPV4_INPUT_DST_LOOKUP_CONSUME
  Lapsed time : 386 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : <unknown>
  Entry  : 0x8a01778c - IPV4_INPUT_FOR_US_MARTIAN
  Lapsed time : 13653 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017730 - IPV4_INPUT_LOOKUP_PROCESS_EXT
  Lapsed time : 2360 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017be0 - IPV4_INPUT_IPOPTIONS_PROCESS_EXT
  Lapsed time : 66 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017bfc - IPV4_INPUT_GOTO_OUTPUT_FEATURE_EXT
  Lapsed time : 680 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017d60 - IPV4_INTERNAL_ARL_SANITY_EXT
  Lapsed time : 320 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017a40 - IPV4_VFR_REFRAG_EXT
  Lapsed time : 106 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017d2c - IPV4_OUTPUT_DROP_POLICY_EXT
  Lapsed time : 1173 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017940 - INTERNAL_TRANSMIT_PKT_EXT
  Lapsed time : 20173 ns
LFTS Path Flow: Packet: 10    CBUG ID: 52
  Feature: LFTS
  Pkt Direction: IN
  Punt Cause  : 55
       subCause : 0
```

例：パケットトレースの使用

次に、パケットトレースを使用して Cisco デバイスの NAT 設定でパケットドロップのトラブルシューティングを行うシナリオの例を示します。この例には、パケットトレース機能によって提供される詳細レベルを効果的に利用して問題に関する情報を収集し、問題を切り分けて、解決策を見つける方法が示されています。

このシナリオでは、問題があることはわかりますが、どこからトラブルシューティングを開始すればよいかはわかりません。したがって、多数の着信パケットのパケットトレースのサマリーにアクセスすることを検討する必要があります。

```
Router# debug platform condition ingress
Router# debug platform packet-trace packet 2048 summary-only
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Pkt   Input             Output            State  Reason
0     Gi0/0/0           Gi0/0/0           DROP   402 (NoStatsUpdate)
1     internal0/0/rp:0  internal0/0/rp:0  PUNT   21  (RP<->QFP keepalive)
2     internal0/0/recycle:0  Gi0/0/0      FWD
```

この出力には、ギガビット イーサネット インターフェイス 0/0/0 の NAT 設定が原因でパケットがドロップされていることが示されています。これによって、問題は特定のインターフェイスで発生していることがわかります。この情報を使用して、トレースするパケットを制限し、データキャプチャのパケット数を減らし、検査レベルを上げることができます。

```
Router# debug platform packet-trace packet 256
Router# debug platform packet-trace punt
Router# debug platform condition interface Gi0/0/0
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Router# show platform packet-trace 15
Packet: 15          CBUG ID: 238
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:1
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 1166288346725 ns (06/06/2016 09:09:42.202734 UTC)
    Stop    : 1166288383210 ns (06/06/2016 09:09:42.202770 UTC)
Path Trace
  Feature: IPV4
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.64.68.3
    Destination : 10.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985
IOSd Path Flow: Packet: 15    CBUG ID: 238
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From CPP
  Feature: IP
    Pkt Direction: IN
    Source      : 10.64.68.122
    Destination : 10.64.68.255
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.64.68.122
    Destination : 10.64.68.255
    Interface   : GigabitEthernet0/0/0
  Feature: UDP
    Pkt Direction: IN
    src         : 10.64.68.122(1053)
```

```
    dst         : 10.64.68.255(1947)
    length      : 48

Router#show platform packet-trace packet 10
Packet: 10          CBUG ID: 10
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:0
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 274777907351 ns (01/10/2020 10:56:47.918494 UTC)
    Stop    : 274777922664 ns (01/10/2020 10:56:47.918509 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.78.106.2
    Destination : 10.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985

IOSd Path Flow: Packet: 10    CBUG ID: 10
  Feature: INFRA
    Pkt Direction: IN
Packet Rcvd From DATAPLANE
 Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.78.106.2
    Destination : 10.0.0.102
    Interface   : GigabitEthernet0/0/0

  Feature: UDP
    Pkt Direction: IN DROP
    Pkt : DROPPED
    UDP: Discarding silently
    src        : 881 10.78.106.2(1985)
    dst         : 10.0.0.102(1985)
    length      : 60

Router#show platform packet-trace packet  12
Packet: 12          CBUG ID: 767
Summary
  Input     : GigabitEthernet3
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 16120990774814 ns (01/20/2020 12:38:02.816435 UTC)
    Stop    : 16120990801840 ns (01/20/2020 12:38:02.816462 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 10.1.1.1
    Destination : 10.1.1.2
    Protocol    : 6 (TCP)
      SrcPort   : 46593
      DstPort   : 23
IOSd Path Flow: Packet: 12    CBUG ID: 767
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From DATAPLANE
```

```
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.1.1.1
    Destination : 10.1.1.2
    Interface   : GigabitEthernet3

  Feature: IP
    Pkt Direction: IN
    FORWARDEDTo transport layer
    Source        : 10.1.1.1
    Destination   : 10.1.1.2
    Interface     : GigabitEthernet3

  Feature: TCP
    Pkt Direction: IN
    tcp0: I NoTCB 10.1.1.1:46593 10.1.1.2:23 seq 1925377975 OPTS 4 SYN  WIN 4128
```

```
Router# show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
0     INJ.2                     Gi1                       FWD
1     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
2     INJ.2                     Gi1                       FWD
3     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
4     INJ.2                     Gi1                       FWD
5     INJ.2                     Gi1                       FWD
6     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
7     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
8     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
9     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
10    INJ.2                     Gi1                       FWD
11    INJ.2                     Gi1                       FWD
12    INJ.2                     Gi1                       FWD
13    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
14    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
15    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
16    INJ.2                     Gi1                       FWD
```

次に、パケットトレースデータの統計を表示する例を示します。

```
Router#show platform packet-trace statistics
Packets Summary
  Matched  3
  Traced   3
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     3
    Count       Code  Cause
    3           56    RP injected for-us control
  Drop     0
  Consume  0

          PKT_DIR_IN
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              0
IP               0              0              0
IPV6             0              0              0
ARP              0              0              0

         PKT_DIR_OUT
```

```
              Dropped       Consumed       Forwarded
INFRA             0              0              0
TCP               0              0              0
UDP               0              0              0
IP                0              0              0
IPV6              0              0              0
ARP               0              0              0
```

次に、コントロールプレーンからフォワーディングプロセッサに挿入およびパントされるパケットを表示する例を示します。

```
Router#debug platform condition ipv4 10.118.74.53/32 both
 Router#Router#debug platform condition start
Router#debug platform packet-trace packet 200
Packet count rounded up from 200 to 256

Router#show platform packet-tracer packet 0
show plat pack pa 0
Packet: 0           CBUG ID: 674
Summary
  Input     : GigabitEthernet1
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 17756544435656 ns (06/29/2020 18:19:17.326313 UTC)
    Stop    : 17756544469451 ns (06/29/2020 18:19:17.326346 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      : <unknown>
    Source      : 10.118.74.53
    Destination : 172.18.124.38
    Protocol    : 17 (UDP)
      SrcPort   : 2640
      DstPort   : 500

IOSd Path Flow: Packet: 0    CBUG ID: 674
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
  Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.118.74.53
    Destination : 172.18.124.38
    Interface   : GigabitEthernet1

  Feature: IP
  Pkt Direction: IN
  FORWARDED To transport layer
    Source        : 10.118.74.53
    Destination   : 172.18.124.38
    Interface     : GigabitEthernet1

  Feature: UDP
  Pkt Direction: IN
  DROPPED
 UDP: Checksum error: dropping
 Source      : 10.118.74.53(2640)
 Destination : 172.18.124.38(500)

Router#show platform packet-tracer packet 2
Packet: 2           CBUG ID: 2
```

```
IOSd Path Flow:
  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 172.18.124.38:22 172.18.124.55:52774 seq 3052140910
 OPTS 4 ACK 2346709419 SYN  WIN 4128

  Feature: TCP
  Pkt Direction: OUT
  FORWARDED
 TCP: Connection is in SYNRCVD state
 ACK         : 2346709419
 SEQ         : 3052140910
 Source      : 172.18.124.38(22)
 Destination : 172.18.124.55(52774)


  Feature: IP
  Pkt Direction: OUTRoute out the generated packet.srcaddr: 172.18.124.38, dstaddr:
172.18.124.55

  Feature: IP
  Pkt Direction: OUTInject and forward successful srcaddr: 172.18.124.38, dstaddr:
172.18.124.55

  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 172.18.124.38:22 172.18.124.55:52774 seq 3052140910
 OPTS 4 ACK 2346709419 SYN  WIN 4128
Summary
  Input     : INJ.2
  Output    : GigabitEthernet1
  State     : FWD
  Timestamp
    Start   : 490928006866 ns (06/29/2020 13:31:30.807879 UTC)
    Stop    : 490928038567 ns (06/29/2020 13:31:30.807911 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : internal0/0/rp:0
    Output      : <unknown>
    Source      : 172.18.124.38
    Destination : 172.18.124.55
    Protocol    : 6 (TCP)
      SrcPort   : 22
      DstPort   : 52774
  Feature: IPSec
    Result    : IPSEC_RESULT_DENY
    Action    : SEND_CLEAR
    SA Handle : 0
    Peer Addr : 10.124.18.172
    Local Addr: 10.124.18.172


Router#
```

例：パケットトレースの使用

次に、パケットトレースを使用して Cisco ASR 1006 ルータの NAT 設定でパケットドロップのトラブルシューティングを行うシナリオの例を示します。この例には、パケットトレース機能によって提供される詳細レベルを効果的に利用して問題に関する情報を収集し、問題を切り分けて、解決策を見つける方法が示されています。

このシナリオでは、問題があることはわかりますが、どこからトラブルシューティングを開始すればよいかはわかりません。したがって、多数の着信パケットのパケットトレースのサマリーにアクセスすることを検討する必要があります。

```
Router# debug platform condition ingress
Router# debug platform packet-trace packet 2048 summary-only
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Pkt   Input             Output            State  Reason
0     Gi0/0/0           Gi0/0/0           DROP   402 (NoStatsUpdate)
1     internal0/0/rp:0  internal0/0/rp:0  PUNT   21  (RP<->QFP keepalive)
2     internal0/0/recycle:0  Gi0/0/0      FWD
```

この出力には、ギガビット イーサネット インターフェイス 0/0/0 の NAT 設定が原因でパケットがドロップされていることが示されています。これによって、問題は特定のインターフェイスで発生していることがわかります。この情報を使用して、トレースするパケットを制限し、データキャプチャのパケット数を減らし、検査レベルを上げることができます。

```
Router# debug platform packet-trace packet 256
Router# debug platform packet-trace punt
Router# debug platform condition interface Gi0/0/0
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Router# show platform packet-trace 15
Packet: 15          CBUG ID: 238
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:1
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 1166288346725 ns (06/06/2016 09:09:42.202734 UTC)
    Stop    : 1166288383210 ns (06/06/2016 09:09:42.202770 UTC)
Path Trace
  Feature: IPV4
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.64.68.3
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985
IOSd Path Flow: Packet: 15    CBUG ID: 238
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From CPP
  Feature: IP
    Pkt Direction: IN
    Source      : 10.64.68.122
    Destination : 10.64.68.255
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.64.68.122
    Destination : 10.64.68.255
    Interface   : GigabitEthernet0/0/0
  Feature: UDP
    Pkt Direction: IN
    src         : 10.64.68.122(1053)
```

```
    dst         : 10.64.68.255(1947)
    length      : 48

Router#show platform packet-trace packet 10
Packet: 10          CBUG ID: 10
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:0
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 274777907351 ns (01/10/2020 10:56:47.918494 UTC)
    Stop    : 274777922664 ns (01/10/2020 10:56:47.918509 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.78.106.2
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985

IOSd Path Flow: Packet: 10    CBUG ID: 10
  Feature: INFRA
    Pkt Direction: IN
Packet Rcvd From DATAPLANE
 Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.78.106.2
    Destination : 224.0.0.102
    Interface   : GigabitEthernet0/0/0

  Feature: UDP
    Pkt Direction: IN DROP
    Pkt : DROPPED
    UDP: Discarding silently
    src        : 881 10.78.106.2(1985)
    dst         : 224.0.0.102(1985)
    length      : 60

Router#show platform packet-trace packet  12
Packet: 12          CBUG ID: 767
Summary
  Input     : GigabitEthernet3
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 16120990774814 ns (01/20/2020 12:38:02.816435 UTC)
    Stop    : 16120990801840 ns (01/20/2020 12:38:02.816462 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 12.1.1.1
    Destination : 12.1.1.2
    Protocol    : 6 (TCP)
      SrcPort   : 46593
      DstPort   : 23
IOSd Path Flow: Packet: 12    CBUG ID: 767
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From DATAPLANE
```

```
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 12.1.1.1
    Destination : 12.1.1.2
    Interface   : GigabitEthernet3

  Feature: IP
    Pkt Direction: IN
    FORWARDEDTo transport layer
    Source        : 12.1.1.1
    Destination   : 12.1.1.2
    Interface     : GigabitEthernet3

  Feature: TCP
    Pkt Direction: IN
    tcp0: I NoTCB 12.1.1.1:46593 12.1.1.2:23 seq 1925377975 OPTS 4 SYN  WIN 4128
```

```
Router# show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
0     INJ.2                     Gi1                       FWD
1     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
2     INJ.2                     Gi1                       FWD
3     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
4     INJ.2                     Gi1                       FWD
5     INJ.2                     Gi1                       FWD
6     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
7     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
8     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
9     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
10    INJ.2                     Gi1                       FWD
11    INJ.2                     Gi1                       FWD
12    INJ.2                     Gi1                       FWD
13    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
14    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
15    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
16    INJ.2                     Gi1                       FWD
```

次に、パケットトレースデータの統計を表示する例を示します。

```
Router#show platform packet-trace statistics
Packets Summary
  Matched  3
  Traced   3
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     3
    Count       Code  Cause
    3           56    RP injected for-us control
  Drop     0
  Consume  0

          PKT_DIR_IN
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              0
IP               0              0              0
IPV6             0              0              0
ARP              0              0              0

         PKT_DIR_OUT
```

```
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              0
IP               0              0              0
IPV6             0              0              0
ARP              0              0              0
```

次に、コントロールプレーンからフォワーディングプロセッサに挿入およびパントされるパケットを表示する例を示します。

```
Router#debug platform condition ipv4 10.118.74.53/32 both
 Router#Router#debug platform condition start
Router#debug platform packet-trace packet 200
Packet count rounded up from 200 to 256

Router#show platform packet-tracer packet 0
show plat pack pa 0
Packet: 0           CBUG ID: 674
Summary
  Input     : GigabitEthernet1
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 17756544435656 ns (06/29/2020 18:19:17.326313 UTC)
    Stop    : 17756544469451 ns (06/29/2020 18:19:17.326346 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      : <unknown>
    Source      : 10.118.74.53
    Destination : 198.51.100.38
    Protocol    : 17 (UDP)
      SrcPort   : 2640
      DstPort   : 500

IOSd Path Flow: Packet: 0    CBUG ID: 674
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
  Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.118.74.53
    Destination : 198.51.100.38
    Interface   : GigabitEthernet1

  Feature: IP
  Pkt Direction: IN
  FORWARDED To transport layer
    Source        : 10.118.74.53
    Destination   : 198.51.100.38
    Interface     : GigabitEthernet1

  Feature: UDP
  Pkt Direction: IN
  DROPPED
 UDP: Checksum error: dropping
 Source      : 10.118.74.53(2640)
 Destination : 198.51.100.38(500)

Router#show platform packet-tracer packet 2
Packet: 2           CBUG ID: 2
```

```
IOSd Path Flow:
  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
 OPTS 4 ACK 2346709419 SYN  WIN 4128

  Feature: TCP
  Pkt Direction: OUT
  FORWARDED
 TCP: Connection is in SYNRCVD state
 ACK         : 2346709419
 SEQ         : 3052140910
 Source      : 198.51.100.38(22)
 Destination : 198.51.100.55(52774)


  Feature: IP
  Pkt Direction: OUTRoute out the generated packet.srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

  Feature: IP
  Pkt Direction: OUTInject and forward successful srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
 OPTS 4 ACK 2346709419 SYN  WIN 4128
Summary
  Input     : INJ.2
  Output    : GigabitEthernet1
  State     : FWD
  Timestamp
    Start   : 490928006866 ns (06/29/2020 13:31:30.807879 UTC)
    Stop    : 490928038567 ns (06/29/2020 13:31:30.807911 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : internal0/0/rp:0
    Output      : <unknown>
    Source      : 172.18.124.38
    Destination : 172.18.124.55
    Protocol    : 6 (TCP)
      SrcPort   : 22
      DstPort   : 52774
  Feature: IPSec
    Result    : IPSEC_RESULT_DENY
    Action    : SEND_CLEAR
    SA Handle : 0
    Peer Addr : 55.124.18.172
    Local Addr: 38.124.18.172


Router#
```

その他の参考資料

標準

標準	タイトル
なし	—

MIB

MIB	MIB のリンク
なし	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 を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 {start hypertext}http://www.cisco.com/go/mibs{end hypertext}

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	{start hypertext}http://www.cisco.com/cisco/web/support/index.html{end hypertext}

パケットトレースの機能情報

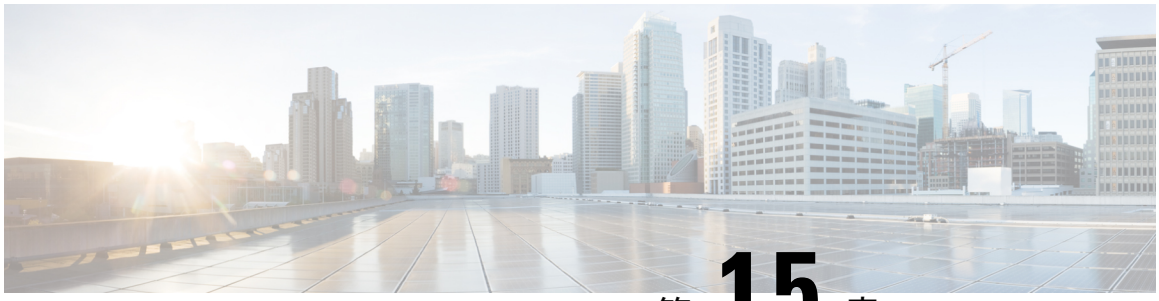
{start cross reference}表 21-4{end cross reference} に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

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 を使用すると、ソフトウェア イメージがサポートする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確認できます。Cisco Feature Navigator にアクセスするには、{start hypertext} http://www.cisco.com/go/cfn{end hypertext} に進みます。Cisco.com のアカウントは必要ありません。

（注） {start cross reference}表 21-4{end cross reference} には、特定のソフトウェア リリース トレインで各機能をサポートするソフトウェアリリースだけが示されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *23 :* パケットトレースの機能情報

機能名	リリース	機能情報
パケットトレース	Cisco IOS XE 3.10S	パケットトレース機能は、Cisco IOS XE ソフトウェアによるデータパケットの処理方法に関する情報を提供します。 Cisco IOS XE リリース 3.10S で、この機能が導入されました。 次のコマンドが導入または変更されました。 • **debug platform packet-trace packet** *pkt-num* [**fia-trace** | **summary-only**] [**data-size** *data-size*] [**circular**] • **debug platform packet-trace copy packet** {**input** | **output** | **both**} [**size** *num-bytes*] [**L2** | **L3** | **L4**] • **show platform packet-trace** {**configuration** | **statistics** | **summary** | **packet** {**all** | *pkt-num*}}
	Cisco IOS XE 3.11S	Cisco IOS XE リリース 3.11S で、この機能が拡張され、次の機能が含まれるようになりました。 • 一致した統計と追跡された統計。 • トレース開始タイムスタンプに加えて、トレース停止タイムスタンプ。 次のコマンドが導入または変更されました。 • **debug platform packet-trace drop** [**code** *drop-num*] • **show platform packet-trace packet** {**all** | *pkt-num*} [*decode*]
	Cisco IOS XE Denali 16.3.1	Cisco IOS XE Denali 16.3.1 で、この機能が拡張され、IOSd とともにレイヤ 3 パケットトレースが含まれるようになりました。 次のコマンドが導入または変更されました。**debug platform packet-trace punt**.
	Cisco IOS XE Amsterdam 17.3.1	**show platform packet-trace** コマンドの出力に、IOSd から発信されたパケットか、IOSd または他の BinOS プロセス宛のパケットに関する追加のトレース情報が含まれるようになりました。



第 15 章

環境モニタリングおよび PoE 管理

Cisco 4000 シリーズ サービス統合型ルータには、ルータの環境を定期的に監視するハードウェアおよびソフトウェア機能があります。詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』を参照してください。

この章では、ルータの環境モニタリング機能について説明します。この機能により、重大なイベントを監視し、さまざまなルータ コンポーネントのステータスに関する統計レポートを生成できます。この章は次の項で構成されています。

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。重大なイベントが発生すると、マイクロプロセッサは HOST CPU への割り込みを生成し、定期的なステータスおよび統計情報レポートを生成します。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、マザーボード、ミッドプレーンの温度の監視
- ファン回転速度の監視
- 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 （218 ページ）
• 環境レポート機能 （220 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。

ローカル電源モジュールで監視できるものは、次のとおりです。

- 入出力電流
- 出力電圧
- 入出力電力
- 温度
- ファン回転速度

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。

- 動作温度（公称）：0°C ～ 40°C（32°F ～ 104°F）
- 動作湿度（公称）：10% ～ 85% RH（結露しないこと）
- 動作湿度（短期）：10% ～ 85% RH（結露しないこと）
- 動作高度：海抜高度 0 m ～ 3000 m （0 ～ 10,000 フィート）
- AC 入力範囲：85 ～ 264 VAC

また、各電源はそれぞれの内部温度と電圧を監視します。電源モジュールの状態は、許容範囲内（ノーマル）または許容範囲外（クリティカル）のどちらかです。内部電源の温度または電圧がクリティカル レベルに達すると、電源はシステム プロセッサと相互作用することなくシャットダウンします。

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 *24*：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。

ステータス レベル	説明
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。

ファン障害

システム電源がオンである場合、すべてのファンが作動するはずです。1 つのファンに障害が発生してもシステムは引き続き稼働しますが、次のメッセージが表示されます。

```
%IOSXE_PEM-3-FANFAIL: The fan in slot 2/0 is encountering a failure condition
```

センサーが許容範囲外

センサーが許容範囲外になると、次のメッセージが表示されます。

```
%ENVIRONMENTAL-1-ALERT: V: 1.0v PCH, Location: R0, State: Warning, Reading: 1102 mV

%ENVIRONMENTAL-1-ALERT: V: PEM Out, Location: P1, State: Warning, Reading: 0 mV

%ENVIRONMENTAL-1-ALERT: Temp: Temp 3, Location R0, State : Warning, Reading : 90C
```

ファン トレイ（スロット P2）の取り外し

ファン トレイ（スロット P2）が取り外されると、次のメッセージが表示されます。

```
%IOSXE_PEM-6-REMPEM_FM: PEM/FM slot P2 removed
```

ファン トレイ（スロット P2）の再挿入

ファン トレイ（スロット P2）が再び挿入されると、次のメッセージが表示されます。

```
%IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P2 inserted
```

ファン トレイ（スロット 2）が正常稼働している

スロット 2 のファン トレイが正常に稼働している場合は、次のメッセージが表示されます。

```
%IOSXE_PEM-6-PEMOK: The PEM in slot P2 is functioning properly
```

スロット 2（ファン トレイ）のファン 0 が動作していない

スロット 2 のファン トレイのファン 0 が正常に動作していない場合は、次のメッセージが表示されます。

```
%IOSXE_PEM-3-FANFAIL: The fan in slot 2/0 is encountering a failure condition
```

スロット 2（ファン トレイ）のファン 0 が正常に動作しいる

スロット 2 のファン トレイのファン 0 が正常に動作している場合は、次のメッセージが表示されます。

```
%IOSXE_PEM-6-FANOK: The fan in slot 2/0 is functioning properly
```

スロット 1 の主電源モジュールがオフになっている

スロット 1 の主電源モジュールに電源がオフになると、次のメッセージが表示されます。

```
%IOSXE_PEM-3-PEMFAIL: The PEM in slot 1 is switched off or encountering a
failure condition.
```

スロット 1 に主電源モジュールが装着された

スロット 1 に主電源モジュールに電源が装着されると、次のメッセージが表示されます。

```
%IOSXE_PEM-6-INSPEM_FM: PEM/FM slot P1 inserted
%IOSXE_PEM-6-PEMOK: The PEM in slot 1 is functioning properly
```

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。

- **debug environment**
- **debug platform software cman env monitor polling**
- **debug ilpower**
- **debug power** [**inline** | **main**]
- **show diag all eeprom**
- **show diag slot R0 eeprom detail**
- **show environment**
- **show environment all**
- **show inventory**
- **show platform all**

- **show platform diag**
- **show platform software status control-processor**
- **show version**
- **show power**
- **show power inline**

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。

debug environment：例

```
Router# debug environment location P0
Environmental sensor Temp: Temp 1 P0 debugging is on
Environmental sensor Temp: Temp 2 P0 debugging is on
Environmental sensor Temp: Temp 3 P0 debugging is on
Environmental sensor V: PEM Out P0 debugging is on
Environmental sensor I: PEM In P0 debugging is on
Environmental sensor I: PEM Out P0 debugging is on
Environmental sensor W: In pwr P0 debugging is on
Environmental sensor W: Out pwr P0 debugging is on
Environmental sensor RPM: fan0 P0 debugging is on

*Sep 12 00:45:13.956: Sensor: Temp: Temp 1 P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=29
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: Temp: Temp 1 P0 State=Normal Reading=29
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: Temp: Temp 2 P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=33
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: Temp: Temp 2 P0 State=Normal Reading=34
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: Temp: Temp 3 P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=34
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: Temp: Temp 3 P0 State=Normal Reading=35
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: V: PEM Out P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=12709
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: V: PEM Out P0 State=Normal Reading=12724
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: I: PEM In P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=1
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: I: PEM In P0 State=Normal Reading=1
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: I: PEM Out P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=4
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
```

```
*Sep 12 00:45:13.956: Sensor: I: PEM Out P0 State=Normal Reading=4
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: W: In pwr P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=92
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: W: In pwr P0 State=Normal Reading=92
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: W: Out pwr P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=46
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: W: Out pwr P0 State=Normal Reading=46
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
*Sep 12 00:45:13.956: Sensor: RPM: fan0 P0, In queue 1
*Sep 12 00:45:13.956: State=Normal Reading=3192
*Sep 12 00:45:13.956: Rotation count=0 Poll period=60000
*Sep 12 00:45:13.956: Sensor: RPM: fan0 P0 State=Normal Reading=3180
*Sep 12 00:45:13.956: Inserting into queue 1 on spoke 173.
*Sep 12 00:45:13.956: Rotation count=60 Displacement=0
```

debug platform software cman env monitor polling：例

```
Router# debug platform software cman env monitor polling
platform software cman env monitor polling debugging is on
Router#
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 1, P0, 29
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 2, P0, 34
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 3, P0, 35
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback V: PEM Out, P0, 12709
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback I: PEM In, P0, 1
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback I: PEM Out, P0, 4
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback W: In pwr, P0, 93
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback W: Out pwr, P0, 48
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P0, 3192
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 1, P1, 33
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 2, P1, 32
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback Temp: Temp 3, P1, 36
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback V: PEM Out, P1, 12666
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback I: PEM In, P1, 1
*Sep 12 00:46:13.962: IOS-RP-ENVMON: sensor READ callback I: PEM Out, P1, 4
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback W: In pwr, P1, 55
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback W: Out pwr, P1, 46
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P1, 2892
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan0, P2, 4894
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan1, P2, 4790
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan2, P2, 5025
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback RPM: fan3, P2, 5001
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback W: fan pwr, P2, 8
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback Temp: Inlet 1, R0, 25
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback Temp: Inlet 2, R0, 28
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback Temp: Outlet 1, R0, 30
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback Temp: Outlet 2, R0, 35
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 12v, R0, 12735
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 5v, R0, 5125
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 3.3v, R0, 3352
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.05v, R0, 1052
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 2.5v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.8v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.2v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.15v, R0, 0
```

```
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.1v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.0v, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.8v PCH, R0, 1787
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.5v PCH, R0, 1516
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.5v CPUC, R0, 1526
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.5v CPUI, R0, 1529
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.0v PCH, R0, 1009
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 1.5v QLM, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: VCore, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: VTT, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 0.75v CPUI, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback V: 0.75v CPUC, R0, 0
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback I: 12v, R0, 7
*Sep 12 00:46:13.963: IOS-RP-ENVMON: sensor READ callback W: pwr, R0, 81
```

debug ilpower：例

```
Router# debug ilpower ?
cdp ILPOWER CDP messages
controller ILPOWER controller
event ILPOWER event
ha ILPOWER High-Availability
port ILPOWER port management
powerman ILPOWER powerman
registries ILPOWER registries
scp ILPOWER SCP messages
```

debug power [inline|main]：例

この例では、1 台の 1000 W 電源と 1 台の 450 W 電源があります。インラインパワーおよび主電源の出力を示します。

```
Router# debug power ?
inline ILPM inline power related
main Main power related
<cr>
Router# debug power
POWER all debug debugging is on

Router# show debugging | include POWER
POWER:
POWER main debugging is on
POWER inline debugging is on
Router#
..
*Jan 21 01:29:40.786: %ENVIRONMENTAL-6-NOTICE: V: PEM Out, Location: P1, State: Warning,
 Reading: 0 mV
*Jan 21 01:29:43.968: %IOSXE_PEM-6-PEMOK: The PEM in slot P1 is functioning properly
*Jan 21 01:29:43.968: %PLATFORM_POWER-6-MODEMATCH: Main power is in Boost mode
*Jan 21 01:29:43.968: Power M: Received Msg for 12V/Main, total power 1450, Run same as
 cfg Yes
*Jan 21 01:29:43.968: Power M: Received Msg for POE/ILPM, total power 500, Run same as
cfg No
*Jan 21 01:29:43.968: Power I: Updating pool power is 500 watts
*Jan 21 01:29:43.968: Power I: Intimating modules of total power 500 watts
*Jan 21 01:29:46.488: Power M: Received Msg for 12V/Main, total power 1450, Run same as
 cfg Yes
*Jan 21 01:29:46.488: Power M: Received Msg for POE/ILPM, total power 500, Run same as
cfg No
*Jan 21 01:29:46.488: Power I: Updating pool power is 500 watts
```

```
*Jan 21 01:29:46.488: Power I: Intimating modules of total power 500 watts
Router#
```

show diag all eeprom：例

```
Router# show diag all eeprom
MIDPLANE EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
Asset ID : P1B-R2C-CP1.0
CLEI Code : TDBTDBTDBT
Power/Fan Module P0 EEPROM data:

Product Identifier (PID) : XXX-XXXX-XX
Version Identifier (VID) : XXX
PCB Serial Number : DCA1547X047
CLEI Code : 0000000000
Power/Fan Module P1 EEPROM data:

Product Identifier (PID) : XXX-XXXX-XX
Version Identifier (VID) : XXX
PCB Serial Number : DCA1533X022
CLEI Code : 0000000000
Power/Fan Module P2 EEPROM data is not initialized

Internal PoE is not present
Slot R0 EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
CLEI Code : TDBTDBTDBT
Slot F0 EEPROM data:

Product Identifier (PID) : ISR4451-FP
Version Identifier (VID) : V00
PCB Serial Number : FP123456789
Hardware Revision : 4.1
Slot 0 EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
CLEI Code : TDBTDBTDBT
Slot 1 EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
CLEI Code : TDBTDBTDBT
Slot 2 EEPROM data:

Product Identifier (PID) : ISR4451/K9
Version Identifier (VID) : V01
PCB Serial Number : FOC15507S9K
Hardware Revision : 1.0
```

```
CLEI Code : TDBTDBTDBT
SPA EEPROM data for subslot 0/0:

Product Identifier (PID) : ISR441-4X1GE
Version Identifier (VID) : V01
PCB Serial Number : JAB092709EL
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 1/0 is not available

SPA EEPROM data for subslot 1/1 is not available

SPA EEPROM data for subslot 1/2 is not available

SPA EEPROM data for subslot 1/3 is not available

SPA EEPROM data for subslot 1/4 is not available

SPA EEPROM data for subslot 2/0 is not available

SPA EEPROM data for subslot 2/1 is not available

SPA EEPROM data for subslot 2/2 is not available

SPA EEPROM data for subslot 2/3 is not available
SPA EEPROM data for subslot 2/4 is not available
```

show environment：例

この例で、スロット POE0 および POE1 の出力に注目してください。Cisco IOS XE 3.10 以降では、外部 PoE モジュールがサポートされています。

```
Router# show environment

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

Slot Sensor Current State Reading
---- ------ ------------ -------
P0 Temp: Temp 1 Normal 28 Celsius
P0 Temp: Temp 2 Normal 43 Celsius
P0 Temp: Temp 3 Normal 44 Celsius
P0 V: PEM Out Normal 12404 mV
P0 I: PEM In Normal 1 A
P0 I: PEM Out Normal 7 A
P0 P: In pwr Normal 106 Watts
P0 P: Out pwr Normal 87 Watts
P0 RPM: fan0 Normal 2952 RPM
P2 RPM: fan0 Normal 4421 RPM
P2 RPM: fan1 Normal 4394 RPM
```

```
P2 RPM: fan2 Normal 4433 RPM
P2 RPM: fan3 Normal 4410 RPM
P2 P: pwr Normal 6 Watts
POE0 Temp: Temp 1 Normal 44 Celsius
POE0 I: 12v In Normal 2 A
POE0 V: 12v In Normal 12473 mV
POE0 P: In pwr Normal 25 Watts
POE1 Temp: Temp 1 Normal 40 Celsius
POE1 I: 12v In Normal 2 mA
POE1 V: 12v In Normal 12473 mV
POE1 P: In pwr Normal 20 Watts
R0 Temp: Inlet 1 Normal 24 Celsius
R0 Temp: Inlet 2 Normal 26 Celsius
R0 Temp: Outlet 1 Normal 33 Celsius
R0 Temp: Outlet 2 Normal 32 Celsius
R0 Temp: core-B Normal 43 Celsius
R0 Temp: core-C Normal 38 Celsius
R0 V: 12v Normal 12355 mV
R0 V: 5v Normal 5090 mV
R0 V: 3.3v Normal 3331 mV
R0 V: 3.0v Normal 2998 mV
R0 V: 2.5v Normal 2436 mV
R0 V: 1.05v Normal 1049 mV
R0 V: 1.8v Normal 1798 mV
R0 V: 1.2v Normal 1234 mV
R0 V: Vcore-C Normal 1155 mV
R0 V: 1.1v Normal 1104 mV
R0 V: 1.0v Normal 1012 mV
R0 V: 1.8v-A Normal 1782 mV
R0 V: 1.5v-A Normal 1505 mV
R0 V: 1.5v-C1 Normal 1516 mV
R0 V: 1.5v-B Normal 1511 mV
R0 V: Vcore-A Normal 1099 mV
R0 V: 1.5v-C2 Normal 1492 mV
R0 V: Vcore-B1 Normal 891 mV
R0 V: Vcore-B2 Normal 904 mV
R0 V: 0.75v-B Normal 754 mV
R0 V: 0.75v-C Normal 759 mV
R0 I: 12v Normal 8 A
R0 P: pwr Normal 86 Watts
0/1 P: pwr Normal 5 Watts
P1 Temp: Temp 1 Normal 30 Celsius
P1 Temp: Temp 2 Normal 38 Celsius
P1 Temp: Temp 3 Normal 39 Celsius
P1 V: PEM Out Normal 12404 mV
P1 I: PEM In Normal 1 A
P1 I: PEM Out Normal 6 A
P1 P: In pwr Normal 86 Watts
P1 P: Out pwr Normal 68 Watts
P1 RPM: fan0 Normal 2940 RPM
```

show environment all：例

```
Router# show environment all
Sensor List: Environmental Monitoring
Sensor Location State Reading
Temp: Temp 1 P0 Normal 29 Celsius
Temp: Temp 2 P0 Normal 43 Celsius
Temp: Temp 3 P0 Normal 44 Celsius
V: PEM Out P0 Normal 12404 mV
I: PEM In P0 Normal 1 A
```

```
I: PEM Out P0 Normal 8 A
P: In pwr P0 Normal 111 Watts
P: Out pwr P0 Normal 91 Watts
RPM: fan0 P0 Normal 2940 RPM
RPM: fan0 P2 Normal 4419 RPM
RPM: fan1 P2 Normal 4395 RPM
RPM: fan2 P2 Normal 4426 RPM
RPM: fan3 P2 Normal 4412 RPM
P: pwr P2 Normal 6 Watts
Temp: Temp 1 POE0 Normal 44 Celsius
I: 12v In POE0 Normal 2 A
V: 12v In POE0 Normal 12473 mV
P: In pwr POE0 Normal 25 Watts
Temp: Temp 1 POE1 Normal 40 Celsius
I: 12v In POE1 Normal 2 mA
V: 12v In POE1 Normal 12473 mV
P: In pwr POE1 Normal 20 Watts
Temp: Inlet 1 R0 Normal 24 Celsius
Temp: Inlet 2 R0 Normal 27 Celsius
Temp: Outlet 1 R0 Normal 33 Celsius
Temp: Outlet 2 R0 Normal 32 Celsius
Temp: core-B R0 Normal 49 Celsius
Temp: core-C R0 Normal 37 Celsius
V: 12v R0 Normal 12355 mV
V: 5v R0 Normal 5084 mV
V: 3.3v R0 Normal 3331 mV
V: 3.0v R0 Normal 2998 mV
V: 2.5v R0 Normal 2433 mV
V: 1.05v R0 Normal 1052 mV
V: 1.8v R0 Normal 1798 mV
V: 1.2v R0 Normal 1226 mV
V: Vcore-C R0 Normal 1155 mV
V: 1.1v R0 Normal 1104 mV
V: 1.0v R0 Normal 1015 mV
V: 1.8v-A R0 Normal 1782 mV
V: 1.5v-A R0 Normal 1508 mV
V: 1.5v-C1 R0 Normal 1513 mV
V: 1.5v-B R0 Normal 1516 mV
V: Vcore-A R0 Normal 1099 mV
V: 1.5v-C2 R0 Normal 1492 mV
V: Vcore-B1 R0 Normal 1031 mV
V: Vcore-B2 R0 Normal 901 mV
V: 0.75v-B R0 Normal 754 mV
V: 0.75v-C R0 Normal 754 mV
I: 12v R0 Normal 8 A
P: pwr R0 Normal 97 Watts
P: pwr 0/1 Normal 5 Watts
Temp: Temp 1 P1 Normal 30 Celsius
Temp: Temp 2 P1 Normal 39 Celsius
Temp: Temp 3 P1 Normal 39 Celsius
V: PEM Out P1 Normal 12404 mV
I: PEM In P1 Normal 1 A
I: PEM Out P1 Normal 6 A
P: In pwr P1 Normal 87 Watts
P: Out pwr P1 Normal 66 Watts
RPM: fan0 P1 Normal 2940 RPM
```

show inventory：例

```
Router# show inventory
NAME: "Chassis", DESCR: "Cisco ISR4451 Chassis"
```

```
PID: ISR4451/K9 , VID: V01, SN: FGL160110QZ

NAME: "Power Supply Module 0", DESCR: "450W AC Power Supply for Cisco ISR4450"
PID: XXX-XXXX-XX , VID: XXX, SN: DCA1547X047

NAME: "Power Supply Module 1", DESCR: "450W AC Power Supply for Cisco ISR4450"
PID: XXX-XXXX-XX , VID: XXX, SN: DCA1614Y022

NAME: "Fan Tray", DESCR: "Cisco ISR4450 Fan Assembly"
PID: ACS-4450-FANASSY , VID: , SN:

NAME: "POE Module 0", DESCR: "Single POE for Cisco ISR4451"
PID: PWR-POE-4400 , VID: , SN: FHH1638P00E

NAME: "POE Module 1", DESCR: "Single POE for Cisco ISR4451"
PID: PWR-POE-4400 , VID: , SN: FHH1638P00G

NAME: "GE-POE Module", DESCR: "POE Module for On Board GE for Cisco ISR4400"
PID: 800G2-POE-2 , VID: V01, SN: FOC151849W9

NAME: "module 0", DESCR: "Cisco ISR4451 Built-In NIM controller"
PID: ISR4451/K9 , VID: , SN:
NAME: "NIM subslot 0/2", DESCR: " NIM-4MFT-T1/E1 - T1/E1 Serial Module"
PID: NIM-4MFT-T1/E1 , VID: V01, SN: FOC16254E6W

NAME: "NIM subslot 0/3", DESCR: "NIM SSD Module"
PID: NIM-SSD , VID: V01, SN: FHH16510032

NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
PID: ISR4451-X-4x1GE , VID: V01, SN: JAB092709EL

NAME: "module 1", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451/K9 , VID: , SN:

NAME: "SM subslot 1/0", DESCR: "SM-X-1T3/E3 - Clear T3/E3 Serial Module"
PID: SM-X-1T3/E3 , VID: V01, SN: FOC164750RG

NAME: "module 2", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451/K9 , VID: , SN:

NAME: "SM subslot 2/0", DESCR: "SM-ES3X-24-P: EtherSwitch SM L3 + PoEPlus + MACSec + 24
 10/100/1000"
PID: SM-ES3X-24-P , VID: V01, SN: FHH1629007C

NAME: "module R0", DESCR: "Cisco ISR4451 Route Processor"
PID: ISR4451/K9 , VID: V01, SN: FOC15507S95

NAME: "module F0", DESCR: "Cisco ISR4451 Forwarding Processor"
PID: ISR4451/K9 , VID: , SN:
```

（注） Cisco ISR 4321 では、**show inventory** コマンドで電源およびファントレイのシリアル番号は表示されません。

show platform：例

```
Router# show platform
Chassis type: ISR4451/K9
```

```
Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0 ISR4451/K9 ok 3d11h
0/0 ISR4451-X-4x1GE ok 3d11h
0/2 NIM-4MFT-T1/E1 ok 3d11h
0/3 NIM-SSD ok 3d11h
1 ISR4451/K9 ok 3d11h
1/0 SM-X-1T3/E3 ok 3d11h
2 ISR4451/K9 ok 3d11h
2/0 SM-ES3X-24-P ok 3d11h
R0 ISR4451/K9 ok, active 3d11h
F0 ISR4451/K9 ok, active 3d11h
P0 XXX-XXXX-XX ok 3d11h
P1 XXX-XXXX-XX ok 3d11h
P2 ACS-4450-FANASSY ok 3d11h
POE0 PWR-POE-4400 ok 3d11h
POE1 PWR-POE-4400 ok 3d11h
GE-POE 800G2-POE-2 ok 3d11h
```

show platform diag：例

```
Router# show platform diag
Chassis type: ISR4451/K9

Slot: 0, ISR4451/K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:01:43 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Sub-slot: 0/0, ISR4451-X-4x1GE
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Sub-slot: 0/2, NIM-4MFT-T1/E1
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Sub-slot: 0/3, NIM-SSD
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Slot: 1, ISR4451/K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:01:44 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S
```

```
Sub-slot: 1/0, SM-X-1T3/E3
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Slot: 2, ISR4451/K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:01:45 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Sub-slot: 2/0, SM-ES3X-24-P
Operational status : ok
Internal state : inserted
Physical insert detect time : 00:03:03 (3d10h ago)
Logical insert detect time : 00:03:03 (3d10h ago)

Slot: R0, ISR4451/K9
Running state : ok, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:01:04 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Slot: F0, ISR4451/K9
Running state : ok, active
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:01:04 (3d10h ago)
Software declared up time : 00:02:39 (3d10h ago)
Hardware ready signal time : 00:00:00 (never ago)
Packet ready signal time : 00:02:48 (3d10h ago)
CPLD version : 12121625
Firmware version : 15.3(1r)S

Slot: P0, XXX-XXXX-XX
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: P1, XXX-XXXX-XX
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: P2, ACS-4450-FANASSY
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: POE0, PWR-POE-4451
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: POE1, PWR-POE-4451
State : ok
Physical insert detect time : 00:01:29 (3d10h ago)

Slot: GE-POE, 800G2-POE-2
State : ok
```

```
Physical insert detect time : 00:01:29 (3d10h ago)
```

show platform software status control-processor：例

```
Router# show platform software status control-processor
RP0: online, statistics updated 2 seconds ago
Load Average: health unknown
1-Min: 0.13, status: health unknown, under
5-Min: 0.07, status: health unknown, under
15-Min: 0.06, status: health unknown, under
Memory (kb): healthy
Total: 3971244
Used: 2965856 (75%)
Free: 1005388 (25%)
Committed: 2460492 (62%), status: health unknown, under 0%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 1.00, System: 2.90, Nice: 0.00, Idle: 96.00
IRQ: 0.10, SIRQ: 0.00, IOwait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 10.71, System: 29.22, Nice: 0.00, Idle: 60.06
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 0.80, System: 1.30, Nice: 0.00, Idle: 97.90
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 10.61, System: 34.03, Nice: 0.00, Idle: 55.25
IRQ: 0.00, SIRQ: 0.10, IOwait: 0.00
CPU4: CPU Utilization (percentage of time spent)
User: 0.60, System: 1.20, Nice: 0.00, Idle: 98.20
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU5: CPU Utilization (percentage of time spent)
User: 13.18, System: 35.46, Nice: 0.00, Idle: 51.24
IRQ: 0.00, SIRQ: 0.09, IOwait: 0.00
CPU6: CPU Utilization (percentage of time spent)
User: 0.80, System: 2.40, Nice: 0.00, Idle: 96.80
IRQ: 0.00, SIRQ: 0.00, IOwait: 0.00
CPU7: CPU Utilization (percentage of time spent)
User: 10.41, System: 33.63, Nice: 0.00, Idle: 55.85
IRQ: 0.00, SIRQ: 0.10, IOwait: 0.00
```

show diag slot R0 eeprom detail：例

```
Router# show diag slot R0 eeprom detail
Slot R0 EEPROM data:

EEPROM version : 4
Compatible Type : 0xFF
PCB Serial Number : FHH153900AU
Controller Type : 1902
Hardware Revision : 0.0
PCB Part Number : 73-13854-01
Top Assy. Part Number : 800-36894-01
Board Revision : 01
Deviation Number : 122081
Fab Version : 01
Product Identifier (PID) : CISCO------<0A>
Version Identifier (VID) : V01<0A>
```

```
Chassis Serial Number : FHH1539P00Q
Chassis MAC Address : 0000.0000.0000
MAC Address block size : 96
Asset ID : REV1B<0A>
Asset ID :
```

show version：例

```
Router# show version
Cisco IOS XE Software, Version 03.13.00.S - Standard Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.4(3)S,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 27-May-14 05:36 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2014 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 2 hours, 19 minutes
Uptime for this control processor is 2 hours, 22 minutes
System returned to ROM by reload
System image file is "tftp: isr4400-universalk9.03.13.00.S.154-3.S-std.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    Technology-package           Technology-package
                   Current        Type                Next reboot
------------------------------------------------------------------
appx               None            None                None
uc                 None            None                None
security           None            None                None
ipbase             ipbasek9       Permanent            ipbasek9
```

```
cisco 4451 ISR processor with 1213154K/6147K bytes of memory.
Processor board ID FHH1539P00Q
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3391455K bytes of Compact flash at bootflash:.

Configuration register is 0x0”
```

電源モードの設定

ルータおよび接続している Power over Ethernet（PoE）モジュールの両方の電源を設定できます。

ルータの電源モードの設定

power main redundant コマンドを使用して、ルータの主電源を設定します。

- **power main redundant**：主電源を Redundant モードに設定します。
- **no power main redundant**：主電源を Boost モードに設定します。

（注） ルータの電源のデフォルト モードは redundant（冗長）モードです。

外部 PoE サービス モジュールの電源モードの設定

power inline redundant コマンドを使用して、外部 PoE サービスモジュールの電源を次のように設定します。

- **power inline redundant**：外部 PoE サービスモジュール電源を redundant モードに設定します。
- **no power inline redundant**：外部 PoE サービスモジュール電源を boost モードに設定します。

（注） 外部 PoE サービス モジュールの電源のデフォルト モードは redundant （冗長）モードです。

show power コマンドは、boost と redundant のどちらのモードが設定されているか、およびそのモードがシステムで現在実行中かどうかを示します。

電源モードの設定例

例：主電源装置および PoE モジュールの設定モード：Boost

この例では、**show power** コマンドにより、設定済みのモードとして `Boost` が表示されます。これは現在のランタイム状態でもあります。`Main PSU` には、主電源の情報が表示されます。`PoE Module` には、インライン/PoE 電源の情報が表示されます。この例では、主電源の現在のランタイム状態が、設定された状態（`Boost` モード）と同じになっています。

```
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 2000 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1000 Watts
Router#
```

例：主電源装置および PoE モジュールの設定モード：Boost

この例では、**show power** コマンドにより、デバイスに存在する電源が表示されます。主電源装置と PoE モジュールは `Boost` モードに設定されており、これは現在のランタイム状態と異なります。現在のランタイム状態は `Redundant` モードです。この理由として、ルータに存在する主電源が 1 つのみであることが考えられます。使用可能な PoE 電力 （236 ページ）の「動作モード」表のモード例 4 を参照してください。

show platform コマンドを入力すると、デバイスに存在する電源を表示できます。

```
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : No
Total power available : 1000 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : No
Total power available : 500 Watts
Router#
```

例：主電源装置および PoE モジュールの設定モード：Redundant

この例では、**show power** コマンドにより、主電源とインラインパワーの両方に設定されたモードとして Redundant が表示されます。システムには 450 W の電源と 100 W の電源がそれぞれ 1 台ずつあります。

```
Router# show power
Main PSU :
Configured Mode : Redundant
Current runtime state same : Yes
Total power available : 450 Watts
POE Module :
Configured Mode : Redundant
Current runtime state same : No
Total power available : 0 Watts
Router#
```

例：主電源の設定モード：Boost

この例では、**power main redundant** コマンドの **no** 形式を使用して、主電源が Boost モードになるように設定されます。これにより、主電源は 1450 W の Boost モード、インラインパワーは 500 W の Redundant モードに設定されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power main redundant
Router(config)#
*Jan 31 03:35:22.284: %PLATFORM_POWER-6-MODEMATCH: Inline power is in Redundant mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Redundant
Current runtime state same : Yes
Total power available : 500 Watts
Router#
```

例：PoE 電源の設定モード：Boost

この例では、**power inline redundant** コマンドの **no** 形式を使用して、インラインパワーを Boost モードに設定しようとしています。インラインパワーのモードは、Boost モードには変更されません。Boost モードに変更するには、Redundant モードで使用可能な総電力として 1000 W が必要となるためです。インラインパワーのモードは Redundant です。これは、PoE モジュールの次の値によって示されます。

- Configured Mode : Boost
- Current runtime state same : No

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power inline redundant
Router(config)#
*Jan 31 03:42:40.947: %PLATFORM_POWER-6-MODEMISMATCH: Inline power not in Boost mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : No
Total power available : 500 Watts
Router#
```

使用可能な PoE 電力

外部 PoE モジュールで PoE 機能を使用可能にするには、電源から供給される総電力が 500 W 以上である必要があります。

（注） 外部 PoE モジュールで PoE 機能が動作することを確認するには **show platform** コマンドおよび **show power** コマンドを使用して、ルータの PoE 電力の可用性を検証します。

外部 PoE サービスモジュール用に十分な PoE 電力があることを判別するには、**show platform** コマンドと **show power** コマンドを使用し、主電源および PoE インバータのワット値に基づいて、使用可能な PoE 電力量を計算します。

P0 および P1 主電源の値を使用して、総電力量（主電源用）を求めます。次に、PoE1 および PoE2 の電源インバータの値を使用して、PoE 総電力量を計算します。

実際の設定に類似していると思われる操作モードの例を、次の表に示します。

接続している PoE サービス モジュールで PoE 機能が動作するためには、表の最終列の「PoE 総電力」の値が 500 W 以上である必要があります。

（注） 外部 PoE モジュールを挿入する前に、ルータに電源インバーターを追加します。このようにしないと、PoE 総電力量が十分であったとしても、外部 PoE モジュールにより PoE 電力が使用されず、PoE 機能が適切に機能させるためにモジュールをリブートする必要が生じます。

主電源で電力モードとして Boost または Redundant を設定すると、PoE 総電力量の値に影響が生じることがあります。

次の表に、総電力量をワット単位で示します。主電源のワット数は、「主電源P0」および「主電源 P1」列に示されます。PoE インバーターのワット数は、「PoE0」および「PoE1」列に示されます。

表 *25 :* 動作モード

モードの例	主電源 P0	主電源 P1	設定モード	総電力量（主電源）	PoE0	PoE1	設定モード	PoE 総電力量
1	450	なし	Redundant または Boost	450	なし	500	Redundant または Boost	0（なし）
2	450	450	BOOST	900	なし	500	Redundant または Boost	0（なし）
3	450	450	冗長	450	500	なし	Redundant または Boost	0（なし）
4	1000	なし	Redundant または Boost	1000	500	なし	Redundant または Boost	500
5	1000	450	冗長	450	500	500	Redundant または Boost	0（なし）
6	1000	450	BOOST	1450	500	500	BOOST	500
7	1000	1000	冗長	1000	500	500	BOOST	500
8	1000	1000	BOOST	2000	500	500	BOOST	1000

（注） 上記の表では、500 W 以上の PoE 総電力量が使用可能になるには、（主電源の）「総電力量」が 1000 W 以上でなければなりません。

PoE 総電力量が 1000 W（上記のモード例 8 を参照）の場合、1000 W の主電源（`Boost` モード）が 2 台と、PoE インバータ（`Boost` モード）が 2 台必要です。

⚠

注意 電源と電源インバータを取り外す際には（特に `Boost` モードで動作している場合は）注意が必要です。総消費電力が、1 台の電源だけで供給可能な電力を超えている場合、この状態で電源を取り外すとハードウェアが損傷する可能性があります。その結果、システムが不安定になったり使用できない状態になることがあります。

同様に、サービス モジュールに PoE 電力を供給する PoE インバーターが 1 台だけの場合、この状態で PoE インバーターを取り外すと、ハードウェアが損傷し、システムが不安定または使用不能になることがあります。

PoE の管理

Power Over Ethernet（PoE）機能により、FPGE ポートで電力を管理できます。PoE を使用すると、接続先の PoE 対応装置に壁面コンセントから電力を供給する必要がなくなります。これにより、接続先の装置に必要であった追加の電気配線にかかる費用が削減されます。ルータは PoE（802.3af）および PoE+（802.3at）をサポートします。PoE の最大供給電力は 15.4 W、PoE+ の最大供給電力は 30 W です。

- FPGE ポートでの PoE サポート （238 ページ）
- 電源の監視 （238 ページ）
- Cisco Discovery Protocol の有効化 （39 ページ）
- FPGE ポートでの PoE の設定 （241 ページ）

FPGE ポートでの PoE サポート

PoE モジュールは、gig0/0/0 や gig0/0/1 などの Front Panel Gigabit Ethernet（FPGE）ポートで PoE をサポートします。**power inline** コマンドを使用して、FPGE 向けに PoE サービスモジュールを設定できます。これにより、IEEE 電話やデバイスなどの接続済みデバイスの電源をオンまたはオフにできます。詳細については、FPGE ポートでの PoE の設定 （241 ページ）を参照してください。

電源の監視

ルータで使用可能な総電力バジェットをモニターするには、特権 EXEC モードで **show power inline [GigabitEthernet detail]** コマンドを使用できます。

このコマンドを使用すると、受電デバイスをルータに接続する前に、受電デバイス タイプに対して十分な電力が使用可能であるかどうかを確認できます。

例：PoE モジュールがない場合のインライン パワー

この例では、PoE をサポートするモジュールがありません。電力は IP フォンとスイッチに供給されます。

```
Router# show power inline
Available:31.0(w)  Used:30.3(w)  Remaining:0.7(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Gi0/0/0   auto   on         14.9    IP Phone 7971       3     30.0
Gi0/0/1   auto   on         15.4    WS-C2960CPD-8PT-L   4     30.0
Router#
```

この例では、コマンドに次の情報が含まれています。

Available:31.0(w)：使用可能な PoE 電力

Used:30.3(w)：ルータのすべてのポートにより使用される PoE 電力

Oper：接続されている各受電デバイスの PoE 電力状態（on/off）

Power：接続されている各受電デバイスで使用される PoE 電力

Class：PoE 電力分類

例：1 つの PoE モジュールのインライン パワー

この例では、PoE をサポートするモジュールが 1 つあります。Cisco IOS XE 3.10 以降では、外部 PoE モジュールがサポートされています。

```
Router# show power inline
Available:31.0(w)  Used:30.3(w)  Remaining:0.7(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Gi0/0/0   auto   on         14.9    IP Phone 7971       3     30.0
Gi0/0/1   auto   on         15.4    WS-C2960CPD-8PT-L   4     30.0

Available:500.0(w)  Used:11.7(w)  Remaining:488.3(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
Et2/0/0   auto   off        11.7    n/a                 n/a   750.0
Router#
```

例：接続された IP フォンへのインライン パワー

```
Router# show power inline
Available:31.0(w)  Used:30.8(w)  Remaining:0.2(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------ ----- ----
```

```
Gi0/0/0   auto   on         15.4    Ieee PD             4     30.0
Gi0/0/1   auto   on         15.4    Ieee PD             4     30.0
```

例：1 つのギガビット イーサネット ポートへのインライン パワー

```
Router# show power inline gigabitEthernet 0/0/0
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/0/0   auto   on         15.4    Ieee PD             4     30.0
```

例：1 つのギガビット イーサネット ポートへのインライン パワー（詳細）

```
Router# show power inline gigabitEthernet 0/0/0 detail
Interface: Gi0/0/0
 Inline Power Mode: auto
 Operational status: on
 Device Detected: yes
 Device Type: Ieee PD
 IEEE Class: 4
 Discovery mechanism used/configured: Ieee
 Police: off

 Power Allocated
 Admin Value: 30.0
 Power drawn from the source: 15.4
 Power available to the device: 15.4

 Absent Counter: 0
 Over Current Counter: 0
 Short Current Counter: 0
 Invalid Signature Counter: 0
 Power Denied Counter: 0
```

例：外部 PoE サービスモジュールへのインライン パワー

この例では、Gi0/0/0 および Gi0/0/1 に関する出力行の後に、外部 PoE サービス モジュールの出力行があります。Cisco IOS XE 3.10 以降では、外部 PoE モジュールがサポートされています。Et1/0/0 は、1 番目の PoE サービス モジュールの内部ポート（スロット 1/0）を示します。Et2/0/0 は、2 番目の PoE サービス モジュールの内部ポート（スロット 2/0）を示します。

両方のスロットが 750 W の PoE 電力を消費可能ですが、このデバイスで使用可能な PoE 電力は 500 W だけです。スロット 2/0（Et2/0/0）には PoE 電力 369.6 W が割り当てられています。

```
Router# show power inline
Available:31.0(w)  Used:15.4(w)  Remaining:15.6(w)
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------  ----   --------   -----   ------------------  ---   ---
Gi0/0/0   auto   on         15.4    Ieee PD             4     30.0
Gi0/0/1   auto   off        0.0     n/a                 n/a   30.0

Available:500.0(w)  Used:369.6(w)  Remaining:500.0(w)
Interface Admin  Oper       Power   Device              Class Max
```

```
                                  (Watts)
--------  ----   --------   -----   ------------------   ---   ---
Et1/0/0   auto   off        0.0     n/a                  n/a   750.
Et2/0/0   auto   off        369.6   n/a                  n/a   750.
```

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。

（注） Cisco アグリゲーション サービス ルータまたは Cisco CSR 1000v では、CDP はデフォルトでイネーブルに設定されていません。

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。

FPGE ポートでの PoE の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cdp run**
4. **interface gigabitethernet** *slot/subslot/port*
5. **cdp enable**
6. **power inline** {**auto** { **auto** [**max** *milli-watts*] | **never**}
7. **exit**

手順の詳細

	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： `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 3	**cdp run** 例： `Router(config)# cdp run`	ルータ上で Cisco Discovery Protocol（CDP）をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**interface gigabitethernet** *slot/subslot/port* 例： `Router(config)# interface gigabitEthernet 0/0/0`	ポート 0 および 1 の PoE を設定できるようにします。 • ポート 0 および 1 で PoE を設定できます。
ステップ 5	**cdp enable** 例： `Router(config-if)# cdp enable`	インターフェイス コンフィギュレーション モードで CDP をイネーブルにします。
ステップ 6	**power inline** {**auto** { **auto** [**max** *milli-watts*] | **never**} 例： `Router(config-if)# power inline auto`	FPGE ポートの電源インライン オプションを設定できるようにします。 • **auto**：**auto** キーワードを指定すると、電源インラインデバイスが自動的に検出され、これらのデバイスに電力が供給されます。 • **max** *milli-watts*：**max** キーワードにより、インターフェイスの許容最大電力が設定されます。 • **never**：**never** キーワードを指定すると、検出が無効になり、インライン電力の供給が中止されます。
ステップ 7	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

FPGE ポートで PoE がイネーブルになっているかどうかの確認

show platform：例

show diag chassis eeprom：例

FPGE ポートで PoE がイネーブル状態であるかどうかを確認するには、このポートの外部 LED を確認します。FPGE ポートの外部 LED には、GE POE というラベルが付いています。内部 PoE モジュールが接続されて適切に動作している場合は、GE POE LED が緑色に点灯します。内部 PoE が接続されているが、適切に動作していない場合は、GE POE LED が黄色に点灯します。PoE モジュールが接続されていない場合、GE PoE LED は消灯します。LED の詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』を参照してください。

また、**show platform** コマンドと **show diag** コマンドを使用して PoE を検出することもできます。

詳細については、次の例を参照してください。

```
Router# show platform
Chassis type: ISR4451/K9

Chassis type: ISR4451/K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4451/K9          ok                    3d11h
 0/0      ISR4451-X-4x1GE     ok                    3d11h
 0/2       NIM-4MFT-T1/E1    ok                    3d11h
 0/3      NIM-SSD             ok                    3d11h
1         ISR4451/K9          ok                    3d11h
 1/0      SM-X-1T3/E3         ok                    3d11h
2         ISR4451/K9          ok                    3d11h
 2/0      SM-ES3X-24-P        ok                    3d11h
R0        ISR4451/K9          ok, active            3d11h
F0        ISR4451/K9          ok, active            3d11h
P0        XXX-XXXX-XX         ok                    3d11h
P1        XXX-XXXX-XX         ok                    3d11h
P2        ACS-4451-FANTRAY    ok                    3d11h
POE0      PWR-POE-4451-X      ok                    3d11h
POE1      PWR-POE-4451-X      ok                    3d11h
GE-POE    800G2-POE-2         ok                    3d11h

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         12090323            15.3(01r)S            [ciscouser-ISRRO...
1         12090323            15.3(01r)S            [ciscouser-ISRRO...
2         12090323            15.3(01r)S            [ciscouser-ISRRO...
R0        12090323            15.3(01r)S            [ciscouser-ISRRO...
F0        12090323            15.3(01r)S            [ciscouser-ISRRO...

Router# show diag chassis eeprom
MIDPLANE EEPROM data:

        Product Identifier (PID) : ISR-4451/K9
        Version Identifier (VID) : V01
        PCB Serial Number        : FOC16145VL8
        Hardware Revision        : 1.0
        Asset ID                 : P1C-R03-CP1.0-UMT-RVC
        CLEI Code                : TBD
Power/Fan Module P0 EEPROM data:

        Product Identifier (PID) : PWR-4450-AC
        Version Identifier (VID) : V01
        PCB Serial Number        : DCA1547X02U
        CLEI Code                : 0000000000
Power/Fan Module P1 EEPROM data is not initialized

Power/Fan Module P2 EEPROM data is not initialized

Internal PoE EEPROM data:

        Product Identifier (PID) : PWR-GE-POE-4400
        Version Identifier (VID) : V01
        PCB Serial Number        : FOC151849VD
        Hardware Revision        : 1.0
        CLEI Code                : 0000000000
```

その他の参考資料

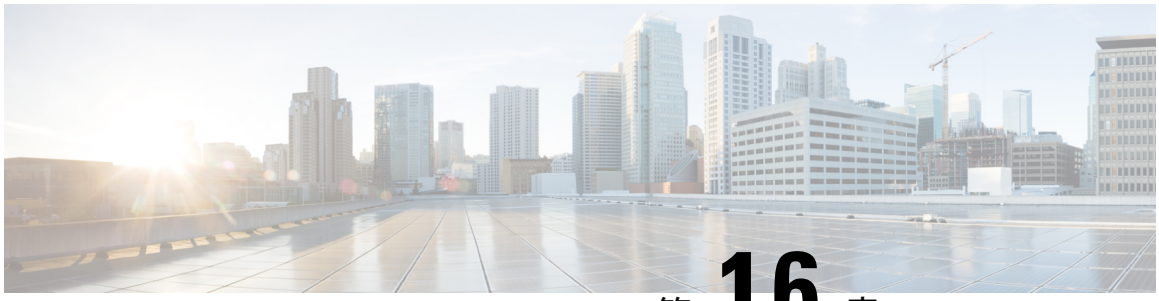
以降のセクションで、電力効率管理機能に関連した参考資料について説明します。

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。 また、『MIB Specifications Guide for the Cisco 4451-X Integrated Services Router』も参照してください。

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 16 章

初期設定へのリセット

この章では、初期設定へのリセット機能と、この機能を使用してルータを保護状態、または以前の完全に機能する状態に復元する方法について説明します。

初期設定へのリセットに関する機能情報

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

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

表 *26* : 初期設定へのリセットに関する機能情報

機能名	リリース	機能情報
工場出荷時の状態へのリセット（Factory Reset）	Cisco IOS XE Everest 16.6.1	この機能が導入されました。
セキュアな初期設定へのリセット	Cisco IOS XE Amsterdam 17.2.1	**factory-reset all secure** コマンドが追加されました。

機能名	リリース	機能情報
factory-reset keep-licensing-info コマンドを使用して RUM レポート、SLR、および HSEC キーを保持するオプション	Cisco IOS XE Bengaluru 17.5.1	この機能が導入されました。

初期設定へのリセットに関する情報

初期設定へのリセットは、ルータの現在の実行コンフィギュレーション情報およびスタートアップ コンフィギュレーション情報をクリアし、ルータを以前の完全に機能する状態にリセットするプロセスです。Cisco IOS XE Amsterdam XE 17.2 以降では、**factory-reset all secure** コマンドを使用してルータをリセットし、ブートフラッシュメモリに保存されているファイルを安全にクリアできます。

表 *27 :* 初期設定へのリセット時に消去および保持されるデータ

コマンド名	消去されるデータ	保持されるデータ
factory-reset all secure	不揮発性ランダムアクセスメモリ（NVRAM）データ	リモート Field-Replaceable Unit（FRU）からのデータ。
	OBFL（オンボード障害ロギング）ログ	コンフィギュレーション レジスタの値
	ライセンス	USB の内容
	ユーザーデータ、スタートアップ コンフィギュレーション、および実行コンフィギュレーション	ログイン情報（セキュアな固有デバイス識別子（SUDI）証明書、公開キーインフラストラクチャ（PKI）キー、および FIPS 関連キー）
	ROMMON 変数	
	すべての書き込み可能ファイルシステムおよび個人データ。 （注） 現在のブートイメージがリモートイメージであるか USB、NIM-SSD などに保存されている場合は、初期設定へのリセットを実行する前に、必ずイメージのバックアップを作成してください。	

コマンド名	消去されるデータ	保持されるデータ
factory-reset keep-licensing-info	• ライセンスブートレベルの設定 • スループットレベルの設定 • スマートライセンス転送タイプ • スマートライセンス URL データ	• リアルユーザーモニタリング（RUM）レポート（オープン/未承認ライセンス使用状況レポート） • 使用状況レポートの詳細情報（受信した最後の ACK、スケジュールされた次の ACK、最後/次のレポートプッシュ） • 固有デバイス ID（UDI）信頼コード • CSSM から受け取った顧客ポリシー • SLAC、SLR 承認コードのリターンコード • 工場出荷時にインストールされた購入情報

初期設定へのリセットプロセスが完了すると、ルータが再起動して ROMMON モードになります。ゼロタッチプロビジョニング（ZTP）機能がセットアップされている場合、ルータが初期設定へのリセット手順を完了すると、ルータは ZTP 設定で再起動します。

初期設定へのリセット実行の前提条件

- 初期設定へのリセットを実行する前に、すべてのソフトウェアイメージ、設定、および個人データがバックアップされていることを確認してください。
- 初期設定へのリセットが進行中の場合は、電源の中断がないことを確認します。
- システムが、ローカル（ブートフラッシュまたはハードディスク）に保存されているイメージから起動されている場合、初期設定へのリセットプロセスでは、ブートイメージのバックアップが作成されます。現在のブートイメージがリモートイメージであるかUSB、NIM-SSD などに保存されている場合は、初期設定へのリセットを実行する前に、必ずイメージのバックアップを作成してください。
- イメージがローカルに保存されている場合でも、**factory-reset all secure** コマンドにより、ブートイメージを含むすべてのファイルを消去します。現在のブートイメージがリモートイメージであるか USB、NIM-SSD などに保存されている場合は、初期設定へのセキュアなリセットを実行する前に、必ずイメージのバックアップを作成してください。

- 初期設定へのリセットを実行する前に、ISSU/ISSD（In-Service Software Upgrade または In-Service Software Downgrade）が進行中でないことを確認してください。

初期設定へのリセット実行の制限事項

- ルータにインストールされているソフトウェアパッチは、初期設定へのリセット操作後に復元されません。
- 仮想テレタイプ（VTY）セッションを介して factory reset コマンドが発行された場合、初期設定へのリセットプロセスの完了後にセッションは復元されません。

初期設定にリセットする場合

- 返品許可（RMA）：RMA のためにルータをシスコに返送する場合、すべての機密情報を削除することが重要です。
- ルータの侵害：悪意のある攻撃によってルータのデータが侵害された場合、ルータを初期設定にリセットしてから、今後の使用のためにもう一度設定しなおす必要があります。
- 再利用：ルータを新しいトポロジまたは市場に移動させる必要がある場合、現在のサイトから別のサイトに移動するときにリセットします。

初期設定へのリセットの実行方法

始める前に

表 2 を参照して、削除および保持する情報を判断します。必要な情報に基づいて、以下に示す適切なコマンドを実行してください。

ステップ 1 Cisco 4000 ISR にログインします。

重要 現在のブートイメージがリモートイメージであるか USB または NIM-SSD に保存されている場合は、初期設定へのリセットプロセスを開始する前に、必ずイメージのバックアップを作成してください。

ステップ 2 この手順は 2 つの部分（a と b）に分かれています。**factory-reset** コマンドの実行中にライセンス情報を保持する必要がある場合は、手順 2 の a に従います。ライセンス情報を保持する必要がなく、すべてのデータを消去する場合は、手順 2 の b を実行します。

a) **factory-reset keep-licensing-info** コマンドを実行してライセンスデータを保持します。

factory-reset keep-licensing-info コマンドを使用すると、次のメッセージが表示されます。

```
Router# factory-reset keep-licensing-info

The factory reset operation is irreversible for Keeping license usage. Are you sure? [confirm]
This operation may take 20 minutes or more. Please do not power cycle.

Dec 1 20:58:38.205: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: process exit with
reload chassis code
/bootflash failed to mount
Dec 01 20:59:44.264: Factory reset operation completed.
Initializing Hardware ...

Current image running: Boot ROM1

Last reset cause: LocalSoft

ISR4331/K9 platform with 4194304 Kbytes of main memory
rommon 1
```

b) **factory-reset all secure 3-pass** コマンドまたは **factory-reset all secure 7-pass** コマンドのいずれかを実行します。

factory-reset all secure 3-pass コマンドを使用すると、次のメッセージが表示されます。

```
Router# factory-reset all secure 3-pass

The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]
This operation may take hours. Please do not power cycle.

*Jun 19 00:53:33.385: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.Jun
 19 00:53:42.856: %PMAN-5-EXITACTION:

Enabling factory reset for this reload cycle
  Jun 19 00:54:06.914: Factory reset secure operation. Write 0s. Please do not power cycle.
  Jun 19 01:18:36.040: Factory reset secure operation. Write 1s. Please do not power cycle.
  Jun 19 01:43:49.263: Factory reset secure operation. Write random. Please do not power cycle.
  Jun 19 02:40:29.770: Factory reset secure operation completed.
Initializing Hardware ....
```

factory-reset all secure 7-pass コマンドを使用すると、次のメッセージが表示されます。

```
Router# factory-reset all secure 7-pass

The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]
This operation may take hours. Please do not power cycle.

*Apr 25 12:36:29.281: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.Apr
 25 12:36:59.275: Factory reset secure operation. Write 0s.   Apr 25 12:40:48.143: Factory reset
 secure operation. Write 1s.
  Apr 25 12:44:54.977: Factory reset secure operation. Write random. Please do not power cycle.
  Apr 25 13:02:00.424: Factory reset secure operation. Write random. Please do not power cycle.
  Apr 25 13:19:02.930: Factory reset secure operation. Write 0s. Please do not power cycle.
  Apr 25 13:22:56.965: Factory reset secure operation. Write 1s. Please do not power cycle.
  Apr 25 13:27:05.775: Factory reset secure operation. Write random. Please do not power cycle.
  Apr 25 13:44:11.174: Factory reset secure operation completed.
Both copies of Nvram are corrupted.
```

ステップ 3 **confirm** と入力して初期設定へのリセットを続行します。

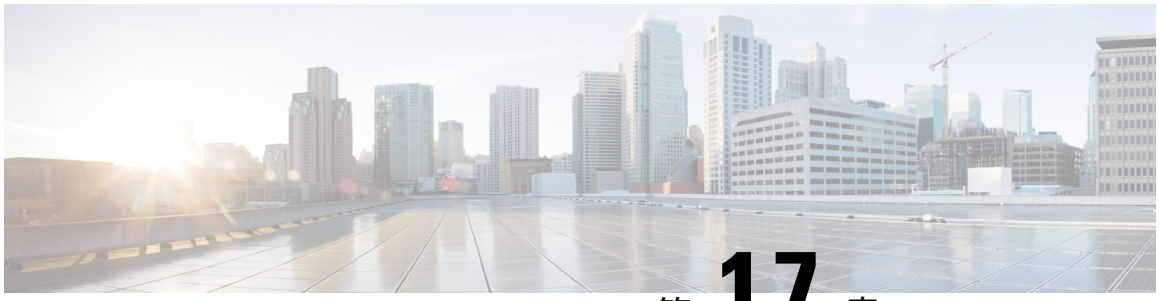
（注） 初期設定へのリセットプロセスの所要時間は、ルータのストレージのサイズによって異なります。これは、高可用性セットアップでは、30 分～ 3 時間延長できます。初期設定へのリセットプロセスを終了する場合は、**Escape** キーを押します。

初期設定へのリセット後の動作

初期設定へのリセットが正常に完了すると、ルータが起動します。ただし、初期設定へのリセットプロセスが開始される前に、コンフィギュレーション レジスタが ROMMON から手動で起動するように設定されていた場合、ルータは ROMMON で停止します。

スマートライセンスを設定したら、**#show license status** コマンドを実行して、インスタンスでスマートライセンスが有効になっているかどうかをチェックします。

（注） 初期設定へのリセットを実行する前に特定ライセンス予約を有効にしていた場合は、同じライセンスを使用し、スマートエージェントから受け取ったライセンスキーを入力します。



第 17 章

ハイ アベイラビリティの設定

Cisco ハイ アベイラビリティ（HA）テクノロジーにより、ネットワークのどの部分でも発生し得る中断から迅速にリカバリでき、ネットワーク全体の保護が実現します。ネットワークのハードウェアとソフトウェアは、Cisco ハイ アベイラビリティ テクノロジーと連携して、中断から迅速にリカバリすることに加えて、ユーザとネットワーク アプリケーションに対して障害の透過性を提供します。

ここでは、ルータで Cisco ハイ アベイラビリティ機能を設定する方法について説明します。

Cisco ハイ アベイラビリティについて

ルータ独自のハードウェアおよびソフトウェア アーキテクチャは、あらゆるネットワーク イベントの発生時にルータのアップタイムを最大化するように設計されているため、すべてのネットワーク シナリオで最大アップタイムと復元力が実現します。

ここでは、Cisco 4000 シリーズ ルータで使用される Cisco ハイ アベイラビリティのいくつかの側面について説明します。

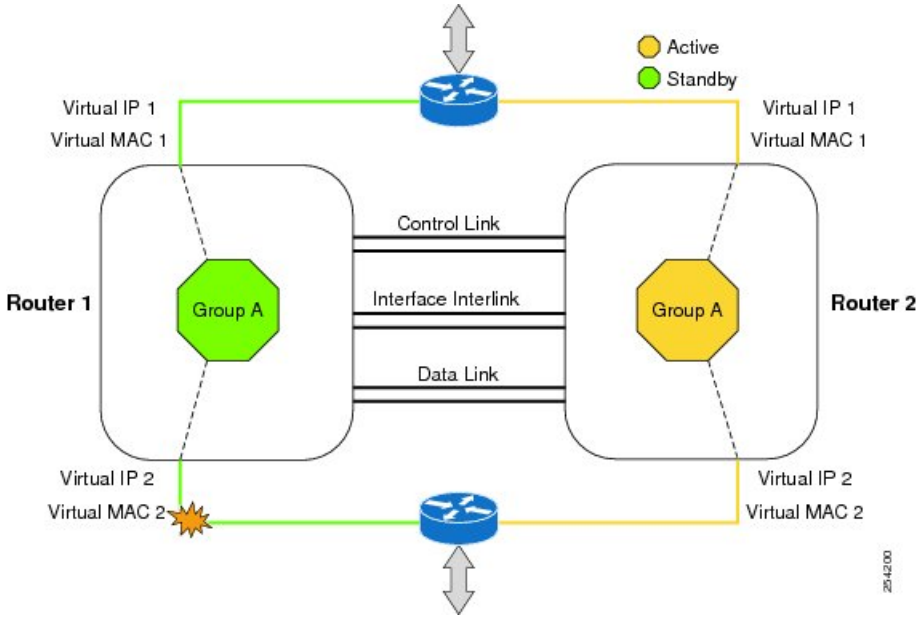
シャーシ間ハイ アベイラビリティ

シャーシ間ハイ アベイラビリティ（HA）機能は、ボックスツーボックス冗長性機能とも呼ばれます。シャーシ間ハイ アベイラビリティを使用すると、相互にバックアップとして動作するルータのペアを設定できます。いくつかのフェールオーバー条件に基づいてアクティブ ルータ

を決定するよう、この機能を設定できます。フェールオーバーが発生すると、中断なくスタンバイ ルータが引き継ぎ、コール シグナリングの処理と、メディア転送タスクの実行を開始します。

冗長インターフェイスのグループは、冗長グループと呼ばれます。次の図は、アクティブ/スタンバイ デバイスのシナリオを示しています。また、1つの発信インターフェイスを持つルータのペアについて、冗長グループを設定する方法を示します。

図 *2:* 冗長グループの設定



設定可能なコントロール リンクおよびデータ同期リンクによってルータが結合されます。コントロール リンクは、ルータのステータスを通信するために使用されます。データ同期リンクを使ってステートフル情報を転送し、コールとメディア フローに関してステートフル データベースを同期します。冗長インターフェイスの各ペアは同じ一意の ID 番号（RII とも呼びます）で設定されます。ルータでのシャーシ間 HA 設定の詳細については、シャーシ間ハイ アベイラビリティの設定 （255 ページ）を参照してください。

IPsec フェールオーバー

IPsec フェールオーバー機能により、IPsec ネットワークの総稼働時間（または可用性）が向上します。従来の方法として、元の（アクティブ）ルータの他に冗長（スタンバイ）ルータを導入することで、IPsec ネットワークの可用性が向上します。アクティブ ルータが何らかの理由で使用不可になると、スタンバイ ルータが IKE および IPsec の処理を引き継ぎます。IPsec フェールオーバーは、ステートレス フェールオーバーおよびステートフル フェールオーバーの 2 種類に分類されます。

ルータでは、ステートレス IPSec フェールオーバーだけがサポートされています。このステートレス フェールオーバーは、ホット スタンバイ ルータ プロトコル（HSRP）などのプロトコルを使用して、プライマリからセカンダリへのカットオーバーを行います。また、アクティブ

およびスタンバイの VPN ゲートウェイを許可して、共通の仮想 IP アドレスを共有することができます。

双方向フォワーディング検出

双方向フォワーディング検出（BFD）は、すべてのメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルのために短時間での転送パス障害検出を提供するよう設計された検出プロトコルです。BFD は、転送パス障害を高速で検出するだけでなく、ネットワーク管理者のために一貫した障害検出方式を提供します。ネットワーク管理者は BFD を使用することで、さまざまなルーティング プロトコルの HELLO メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

BFD の詳細については、『IP Routing BFD Configuration Guide, Cisco IOS XE Release 3S』の「Bidirectional Forwarding Detection」を参照してください。

双方向フォワーディング検出オフロード

双方向フォワーディング検出オフロード機能は、障害検出にかかる時間を短縮するために、BDF セッション管理をフォワーディング エンジンにオフロードできるようにします。BFD オフロードにより、ルーティング テーブル再計算のために迅速な障害検出パケット（メッセージ）をルーティング プロトコルに送信することで、全体的なネットワーク コンバージェンス時間が短縮されます。BFD オフロードの設定 （257 ページ）を参照してください。

Cisco ハイ アベイラビリティの設定

シャーシ間ハイ アベイラビリティの設定

前提条件

- アクティブ デバイスとスタンバイ デバイスは、同じバージョンの Cisco IOS XE ソフトウェアを実行する必要があります。
- アクティブ デバイスとスタンバイは、制御パス用の L2 接続を介して接続する必要があります。

- 組み込みサービス プロセッサ（ESP）は、アクティブ デバイスとスタンバイ デバイスで同じである必要があります。また、ルートプロセッサが互いに一致し、類似の物理構成でなければなりません。
- タイムスタンプとコール タイマーが一致するように、両方のデバイスでネットワーク タイム プロトコル（NTP）を設定するか、クロックを同じに設定する必要があります。
- データの正確な同期のために、アクティブ ルータとスタンバイ ルータで仮想ルータ転送（VRF）を同じ順序で定義する必要があります。
- 遅延時間は、タイム アウトを防止するため、すべての制御リンクおよびデータ リンクで最小にする必要があります。
- Gigabit EtherChannel などの物理的に冗長なリンクを、制御パスおよびデータ パスに使用する必要があります。

制約事項

- ボックスツーボックスアプリケーションのフェールオーバー時間は、非ボックスツーボックス アプリケーションではより高くなります。
- LAN および MESH シナリオはサポートされません。
- VRF はサポートされておらず、ZBFW 高可用性データおよび制御インターフェイスでは設定できません。
- Front Panel Gigabit Ethernet（FPGE）インターフェイスでサポートされる仮想 MAC（および VRF）の最大数は、プラットフォームによって異なります。サポートされているインターフェイスとモジュールは、「Interfaces and Modules」ページに示されています。Cisco 4451 ISR および Cisco 4431 ISR FPGE は、4 つの FPGE インターフェイスすべてで共有できる 2 つの予約済み MAC と 24 のフィルタをサポートしています。Cisco 4351 ISR、Cisco 4331 ISR、および Cisco 4321 ISR FPGE は、1 つの予約済みフィルタ（BIA）と 15 のフィルタによって最大 16 の MAC をサポートしています。NIM-1GE-CU-SFP、NIM-2GE-CU-SFP、SM-X-6X1G、および SM-X-4X1G-1X10G モジュールでは、各ポートが 1023 の MAC フィルタをサポートしています。リストに示されていないモジュールでサポートされている MAC フィルタについては、シスコの担当者にお問い合わせください。
- スタンバイ ルータに複製された設定は、スタートアップ コンフィギュレーションにコミットされず、実行コンフィギュレーション内に設定されます。アクティブルータから同期された変更を適用するには、スタンバイルータで **write memory** コマンドを実行する必要があります。

シャーシ間ハイ アベイラビリティの設定方法

ルータでのシャーシ間ハイアベイラビリティの設定の詳細については、『IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S』を参照してください。

双方向フォワーディングの設定

ご使用のルータでの BFD の設定については、『IP Routing BFD Configuration Guide』を参照してください。

BFD コマンドについては、『Cisco IOS IP Routing: Protocol-Independent Command Reference』を参照してください。

BFD オフロードの設定

制約事項

- BFD バージョン 1 のみサポートされます。
- これを設定すると、オフロードされる BFD セッションだけがサポートされ、RP の BFD セッションはサポートされません。
- BFD の非同期モードまたはエコーなしモードだけがサポートされます。
- 511 非同期 BFD セッションがサポートされます。
- BFD ハードウェア オフロードは、エコーなしモードの IPv4 セションでのみサポートされます。
- BFD オフロードは、ポート チャネル インターフェイスでのみサポートされます。
- BFD オフロードは、イーサネット インターフェース用にのみサポートされます。
- BFD オフロードは、IPv6 BFD セッションではサポートされません。
- BFD オフロードは、TE/FRR を使用する BFD セッションではサポートされません。

BFD オフロードの設定方法

BFDオフロード機能はデフォルトでイネーブルに設定されています。ルートプロセッサでBFDハードウェア オフロードを設定できます。詳細については、『Configuring BFD』と『IP Routing BFD Configuration Guide』を参照してください。

シャーシ間ハイ アベイラビリティの検証

シャーシ間高可用性を検証するには、次の **show** コマンドを使用します。

（注） シャーシ間ハイ アベイラビリティの設定に関する前提条件とマニュアルへのリンクが、シャーシ間ハイ アベイラビリティの設定 （255 ページ）にリストされています。

- **show redundancy application group [group-id | all]**
- **show redundancy application transport {client | group [group-id]}**

- **show redundancy application control-interface group [group-id]**
- **show redundancy application faults group [group-id]**
- **show redundancy application protocol {protocol-id | group [group-id]}**
- **show redundancy application if-mgr group [group-id]**
- **show redundancy application data-interface group [group-id]**

次の例は、ルータで設定された冗長アプリケーション グループを示します。

```
Router# show redundancy application group
Group ID    Group Name                      State
--------    ----------                      -----
1           Generic-Redundancy-1            STANDBY
2           Generic-Redundancy2             ACTIVE
```

次の例は、冗長アプリケーション グループ 1 の詳細を示します。

```
Router# show redundancy application group 1
Group ID:1
Group Name:Generic-Redundancy-1

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: STANDBY HOT
Peer RF state: ACTIVE
```

次の例は、冗長アプリケーション グループ 2 の詳細を示します。

```
Router# show redundancy application group 2
Group ID:2
Group Name:Generic-Redundancy2

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-two
RF state: ACTIVE
Peer RF state: STANDBY HOT
```

次の例は、冗長アプリケーション トランスポート クライアントの詳細を示します。

```
Router# show redundancy application transport client
Client          Conn#  Priority   Interface   L3        L4
( 0)RF            0      1         CTRL       IPV4      SCTP

( 1)MCP_HA        1      1         DATA       IPV4      UDP_REL

( 4)AR            0      1         ASYM       IPV4      UDP
```

```
( 5)CF           0      1          DATA       IPV4       SCTP
```

次の例は、冗長アプリケーション トランスポート グループの設定の詳細を示します。

```
Router# show redundancy application transport group
Transport Information for RG (1)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
0    0       10.1.1.1        59000    10.2.2.2        59000    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
1    1       10.9.9.2        53000    10.9.9.1        53000    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
2    0       10.0.0.0        0        10.0.0.0        0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
3    0       10.9.9.2        59001    10.9.9.1        59001    DATA    IPV4    SCTP
Transport Information for RG (2)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
8    0       10.1.1.1        59004    10.1.1.2       59004    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
9    1       10.9.9.2        53002    10.9.9.1        53002    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
10   0       10.0.0.0        0        10.0.0.0        0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
11   0       10.9.9.2        59005    10.9.9.1        59005    DATA    IPV4    SCTP
```

次の例は、冗長アプリケーション トランスポート グループ 1 の設定の詳細を示します。

```
Router# show redundancy application transport group 1
Transport Information for RG (1)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
0    0       10.1.1.1        59000    10.1.1.2       59000    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
1    1       10.9.9.2        53000    10.9.9.1        53000    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
2    0       10.0.0.0        0        10.0.0.0        0        NONE_IN NONE_L3 NONE_L4
Client = CF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
3    0       10.9.9.2        59001    10.9.9.1        59001    DATA    IPV4    SCTP
```

次の例は、冗長アプリケーション トランスポート グループ 2 の設定の詳細を示します。

```
Router# show redundancy application transport group 2
Transport Information for RG (2)
Client = RF
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
8    0       10.1.1.1        59004    10.1.1.2        59004    CTRL    IPV4    SCTP
Client = MCP_HA
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
9    1       10.9.9.2        53002    10.9.9.1        53002    DATA    IPV4    UDP_REL
Client = AR
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
10   0       10.0.0.0        0        10.0.0.0        0        NONE_IN NONE_L3 NONE_L4
Client = CF
```

```
TI   conn_id my_ip           my_port  peer_ip         peer_por intf    L3      L4
11   0       10.9.9.2        59005    10.9.9.1        59005    DATA    IPV4    SCTP
```

次の例は、冗長アプリケーション コントロール インターフェイス グループの設定の詳細を示します。

```
Router# show redundancy application control-interface group
The control interface for rg[1] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.1.2 Active RGs: 1 Standby RGs: 2 BFD handle: 0

The control interface for rg[2] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.1.2 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

次の例は、冗長アプリケーション コントロール インターフェイス グループ 1 の設定の詳細を示します。

```
Router# show redundancy application control-interface group 1
The control interface for rg[1] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.1.2 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

次の例は、冗長アプリケーション コントロール インターフェイス グループ 2 の設定の詳細を示します。

```
Router# show redundancy application control-interface group 2
The control interface for rg[2] is GigabitEthernet0/0/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.1.2 Active RGs: 1 Standby RGs: 2 BFD handle: 0
```

次の例は、冗長アプリケーション フォールト グループの設定の詳細を示します。

```
Router# show redundancy application faults group
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

次の例は、冗長アプリケーション フォールト グループ 1 に固有の設定の詳細を示します。

```
Router# show redundancy application faults group 1
Faults states Group 1 info:
Runtime priority: [50]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

次の例は、冗長アプリケーション フォールト グループ 2 に固有の設定の詳細を示します。

```
Router# show redundancy application faults group 2
Faults states Group 2 info:
Runtime priority: [135]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 2
```

次の例は、冗長アプリケーション プロトコル グループの設定の詳細を示します。

```
Router# show redundancy application protocol group
RG Protocol RG 1
------------------
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 10.1.1.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 117, Bytes 7254, HA Seq 0, Seq Number 117, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 115, Bytes 3910, HA Seq 0, Seq Number 1453975, Pkt Loss 0



RG Protocol RG 2
------------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 10.1.1.2, priority 130, intf Gi0/0/0
Log counters:
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
Ctx State: Active
```

```
Protocol ID: 2
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 118, Bytes 7316, HA Seq 0, Seq Number 118, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 102, Bytes 3468, HA Seq 0, Seq Number 1453977, Pkt Loss 0
```

次の例は、冗長アプリケーション プロトコル グループ 1 の設定の詳細を示します。

```
Router# show redundancy application protocol group 1
RG Protocol RG 1
------------------
Role: Standby
Negotiation: Enabled
Priority: 50
Protocol state: Standby-hot
Ctrl Intf(s) state: Up
Active Peer: address 10.1.1.2, priority 150, intf Gi0/0/0
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 120, Bytes 7440, HA Seq 0, Seq Number 120, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 118, Bytes 4012, HA Seq 0, Seq Number 1453978, Pkt Loss 0
```

次の例は、冗長アプリケーション プロトコル グループ 2 の設定の詳細を示します。

```
Router# show redundancy application protocol group 2
RG Protocol RG 2
------------------
Role: Active
Negotiation: Enabled
Priority: 135
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 10.1.1.2, priority 130, intf Gi0/0/0
Log counters:
```

```
role change to active: 1
role change to standby: 1
disable events: rg down state 1, rg shut 0
ctrl intf events: up 2, down 1, admin_down 1
reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
Ctx State: Active
Protocol ID: 2
Media type: Default
Control Interface: GigabitEthernet0/0/0
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 123, Bytes 7626, HA Seq 0, Seq Number 123, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 1
Standby Peer: Present. Hold Timer: 10000
Pkts 107, Bytes 3638, HA Seq 0, Seq Number 1453982, Pkt Loss 0
```

次の例は、冗長アプリケーション プロトコル 1 の設定の詳細を示します。

```
Router# show redundancy application protocol 1
Protocol id: 1, name: rg-protocol-1
BFD: ENABLE
Hello timer in msecs: 3000
Hold timer in msecs: 10000
OVLD-1#show redundancy application protocol 2
Protocol id: 2, name: rg-protocol-2
BFD: ENABLE
Hello timer in msecs: 3000
Hold timer in msecs: 10000
```

次の例は、冗長アプリケーション インターフェイス マネージャ グループの設定の詳細を示します。

```
Router# show redundancy application if-mgr group
 RG ID: 1
 ==========

 interface      GigabitEthernet0/0/3.152
 ---------------------------------------
 VMAC           0007.b421.4e21
 VIP            10.1.1.255
 Shut           shut
 Decrement      10

 interface      GigabitEthernet0/0/2.152
 ---------------------------------------
 VMAC           0007.b421.5209
 VIP            10.1.2.255
 Shut           shut
 Decrement      10


 RG ID: 2
 ==========

 interface      GigabitEthernet0/0/3.166
 ---------------------------------------
```

```
 VMAC            0007.b422.14d6
 VIP             10.1.255.254
 Shut            no shut
 Decrement       10

 interface       GigabitEthernet0/0/2.166
 --------------------------------------
 VMAC            0007.b422.0d06
 VIP             10.2.255.254
 Shut            no shut
 Decrement       10
```

次の例は、冗長アプリケーション インターフェイス マネージャ グループ 1 およびグループ 2 の設定の詳細を示します。

```
Router# show redundancy application if-mgr group 1

 RG ID: 1
 ==========

 interface       GigabitEthernet0/0/3.152
 --------------------------------------
 VMAC            0007.b421.4e21
 VIP             10.1.1.255
 Shut            shut
 Decrement       10

 interface       GigabitEthernet0/0/2.152
 --------------------------------------
 VMAC            0007.b421.5209
 VIP             10.2.1.255
 Shut            shut
 Decrement       10

Router# show redundancy application if-mgr group 2
 RG ID: 2
 ==========

 interface       GigabitEthernet0/0/3.166
 --------------------------------------
 VMAC            0007.b422.14d6
 VIP             10.1.255.254
 Shut            no shut
 Decrement       10

 interface       GigabitEthernet0/0/2.166
 --------------------------------------
 VMAC            0007.b422.0d06
 VIP             10.2.255.254
 Shut            no shut
 Decrement       10
```

次の例は、冗長アプリケーションデータ インターフェイス グループの設定の詳細を示します。

```
Router# show redundancy application data-interface group
The data interface for rg[1] is GigabitEthernet0/0/1
The data interface for rg[2] is GigabitEthernet0/0/1
```

次の例は、冗長アプリケーション データ インターフェイス グループ 1 およびグループ 2 に固有の設定の詳細を示します。

```
Router# show redundancy application data-interface group 1
The data interface for rg[1] is GigabitEthernet0/0/1
```

```
Router # show redundancy application data-interface group 2
The data interface for rg[2] is GigabitEthernet0/0/1
```

BFD オフロードの検証

ルータの BFD オフロード機能を検証および監視するには、次のコマンドを使用します。

（注） BFDオフロードの設定については、双方向フォワーディングの設定（257ページ）に説明があります。

- **show bfd neighbors [details]**
- **debug bfd [packet | event]**
- **debug bfd event**

show bfd neighbors コマンドは、BFD 隣接関係データベースを表示します。

```
Router# show bfd neighbor

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.10                            362/1277       Up        Up        Gi0/0/1.2
192.0.2.11                            445/1278       Up        Up        Gi0/0/1.3
192.0.2.12                           1093/961        Up        Up        Gi0/0/1.4
192.0.2.13                           1244/946        Up        Up        Gi0/0/1.5
192.0.2.14                           1094/937        Up        Up        Gi0/0/1.6
192.0.2.15                           1097/1260       Up        Up        Gi0/0/1.7
192.0.2.16                           1098/929        Up        Up        Gi0/0/1.8
192.0.2.17                           1111/928        Up        Up        Gi0/0/1.9
192.0.2.18                           1100/1254       Up        Up        Gi0/0/1.10
```

debug bfd neighbor detail コマンドは、BFD パケットに関連するデバッグ情報を表示します。

```
Router# show bfd neighbor detail

IPv4 Sessions
NeighAddr                              LD/RD         RH/RS     State     Int
192.0.2.10                            362/1277       Up        Up        Gi0/0/1.2
Session state is UP and not using echo function.
Session Host: Hardware
OurAddr: 192.0.2.11
Handle: 33
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holddown (hits): 0(0), Hello (hits): 50(0)
Rx Count: 3465, Rx Interval (ms) min/max/avg: 42/51/46
Tx Count: 3466, Tx Interval (ms) min/max/avg: 39/52/46
Elapsed time watermarks: 0 0 (last: 0)
Registered protocols: CEF EIGRP
Uptime: 00:02:50
Last packet: Version: 1                  - Diagnostic: 0
             State bit: Up               - Demand bit: 0
             Poll bit: 0                 - Final bit: 0
             C bit: 1
             Multiplier: 3               - Length: 24
             My Discr.: 1277             - Your Discr.: 362
```

```
            Min tx interval: 50000      - Min rx interval: 50000
            Min Echo interval: 0
```

show bfd summary コマンドは、BFD の概要情報を表示します。

```
Router# show bfd summary

                   Session          Up          Down

Total                  400         400             0
```

show bfd drops コマンドは、BFD でドロップされたパケットの数を表示します。

```
Router# show bfd drops
BFD Drop Statistics
                      IPV4     IPV6    IPV4-M    IPV6-M    MPLS_PW   MPLS_TP_LSP
Invalid TTL             0        0         0         0         0         0
BFD Not Configured      0        0         0         0         0         0
No BFD Adjacency        33       0         0         0         0         0
Invalid Header Bits     0        0         0         0         0         0
Invalid Discriminator   1        0         0         0         0         0
Session AdminDown       94       0         0         0         0         0
Authen invalid BFD ver  0        0         0         0         0         0
Authen invalid len      0        0         0         0         0         0
Authen invalid seq      0        0         0         0         0         0
Authen failed           0        0         0         0         0         0
```

debug bfd packet コマンドは、BFD 制御パケットに関するデバッグ情報を表示します。

```
Router# debug bfd packet
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1941/0 diag:0(No Diagnostic)
 Down C cnt:4 ttl:254 (0)
*Nov 12 23:08:27.982: BFD-DEBUG Packet: Tx IP:192.0.2.22 ld/rd:983/1941 diag:3(Neighbor
 Signaled Session Down) Init  C cnt:44 (0)
*Nov 12 23:08:28.007: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1941/983 diag:0(No
Diagnostic) Up PC cnt:4 ttl:254 (0)
*Nov 12 23:08:28.007: BFD-DEBUG Packet: Tx IP:192.0.2.22 ld/rd:983/1941 diag:0(No
Diagnostic) Up F C cnt:0 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1941/983 diag:0(No
Diagnostic) Up FC cnt:0 ttl:254 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Tx IP:192.0.2.22 ld/rd:983/1941 diag:0(No
Diagnostic) Up  C cnt:0 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1907/0 diag:0(No Diagnostic)
 Down C cnt:3 ttl:254 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Tx IP:192.0.2.22 ld/rd:993/1907 diag:3(Neighbor
 Signaled Session Down) Init  C cnt:43 (0)
*Nov 12 23:08:28.311: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1941/983 diag:0(No
Diagnostic) Up C cnt:0 ttl:254 (0)
*Nov 12 23:08:28.626: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1907/993 diag:0(No
Diagnostic) Up PC cnt:3 ttl:254 (0)
*Nov 12 23:08:28.626: BFD-DEBUG Packet: Tx IP:192.0.2.22 ld/rd:993/1907 diag:0(No
Diagnostic) Up F C cnt:0 (0)
*Nov 12 23:08:28.645: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1907/993 diag:0(No
Diagnostic) Up C cnt:0 ttl:254 (0)
*Nov 12 23:08:28.700: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1907/993 diag:0(No
Diagnostic) Up FC cnt:0 ttl:254 (0)
*Nov 12 23:08:28.700: BFD-DEBUG Packet: Tx IP:192.0.2.22 ld/rd:993/1907 diag:0(No
Diagnostic) Up  C cnt:0 (0)
*Nov 12 23:08:28.993: BFD-DEBUG Packet: Rx IP:192.0.2.22 ld/rd:1907/993 diag:0(No
Diagnostic) Up C cnt:0 ttl:254 (0)
```

debug bfd event コマンドは、BFD 状態遷移に関するデバッグ情報を表示します。

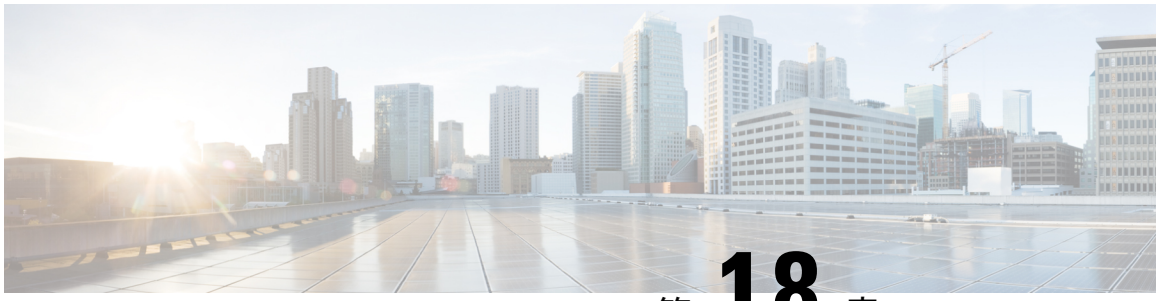
```
Router# deb bfd event
```

```
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.153, ld:1401,
handle:77, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.153, ld:1401,
handle:77, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.153, ld:1400,
handle:39, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.153, ld:1400,
handle:39, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.153, ld:1399,
handle:25, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.153, ld:1399,
handle:25, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.153, ld:1403,
handle:173, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.153, ld:1403,
handle:173, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.153, ld:1402,
handle:95, event:DOWN adminDown, (0)
*Nov 12 23:11:29.503: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.153, ld:1402,
handle:95, event:DOWN adminDown, (0)
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Timers: Tx timer 1000000 Detect timer 0
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Flags: Poll 0 Final 0
*Nov 12 23:11:30.639: BFD-HW-API: Handle 1404: Buffer: 0x23480318 0x0000057C 0x00000000
 0x000F4240 0x000F4240 0x00000000 size 24
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Timers: Tx timer 1000000 Detect timer 0
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Flags: Poll 0 Final 0
*Nov 12 23:11:30.641: BFD-HW-API: Handle 1405: Buffer: 0x23480318 0x0000057D 0x00000000
 0x000F4240 0x000F4240 0x00000000 size 24
*Nov 12 23:11:30.649: BFD-DEBUG Packet: Rx IP:192.0.2.33 ld/rd:1601/1404
diag:7(Administratively Down) AdminDown C cnt:0 ttl:254 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: V1 FSM ld:1404 handle:207 event:RX ADMINDOWN
state:UP (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: resetting timestamps ld:1404 handle:207 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.33, ld:1404,
handle:207, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Tx IP:192.0.2.33 ld/rd:1404/0 diag:3(Neighbor
Signaled Session Down) Down C cnt:0 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Rx IP:192.0.2.85 ld/rd:1620/1405
diag:7(Administratively Down) AdminDown C cnt:0 ttl:254 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: V1 FSM ld:1405 handle:209 event:RX ADMINDOWN
state:UP (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: resetting timestamps ld:1405 handle:209 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.85, ld:1405,
handle:209, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Packet: Tx IP:192.10.85.1 ld/rd:1405/0 diag:3(Neighbor
Signaled Session Down) Down C cnt:0 (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.33, ld:1404,
handle:207, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.33, ld:1404,
handle:207, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(EIGRP) IP:192.0.2.85, ld:1405,
handle:209, event:DOWN adminDown, (0)
*Nov 12 23:11:30.650: BFD-DEBUG Event: notify client(CEF) IP:192.0.2.85, ld:1405,
handle:209, event:DOWN adminDown, (0)
*Nov 12 23:11:31.035: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 192.0.2.191
```

その他の参考資料

BFD 機能に関連する情報を収録したマニュアルを以下に示します。

関連項目	マニュアル タイトル
ステートフル シャーシ間設定。	『*Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS XE Release 3S*』（http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-data-zbf-xe-book.html）。
IP ルーティング プロトコル独立型コマンド。	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』（http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/command/iri-cr-book.html）。



第 18 章

Secure Sockets Layer Virtual Private Network（SSL VPN）

Secure Sockets Layer Virtual Private Network（SSL VPN）機能は Cisco IOS ソフトウェアでサポートされています。この機能を使用することにより、リモートユーザーはインターネット上のどこからでも企業ネットワークにアクセスできるようになります。リモートアクセスは、Secure Socket Layer 対応（SSL 対応）の SSL VPN ゲートウェイを介して提供されます。SSL VPN ゲートウェイによりリモート ユーザはセキュアな VPN トンネルを確立できます。SSL VPN 機能は、フルトンネルクライアントが初めから備えている HTTP over SSL（HTTPS）ブラウザサポートを使用して、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできる包括的なソリューションを実現します。

SSL VPN の前提条件

SSL VPN サービスのリモート ユーザが、SSL VPN ゲートウェイ背後にあるプライベート ネットワーク上のリソースに安全にアクセスするには、次が必要です。

- アカウント（ログイン名とパスワード）
- Cisco AnyConnect Client を使用したフルトンネルモードのサポート
- Cisco AnyConnect Client をインストールするための管理者権限

SSL VPN の制約事項

- ACL は DENY ステートメントをサポートしていません。
- Cisco AnyConnect VPN を使用して、高い起動レートでトンネルを作成すると、障害が発生する可能性があります。多数の VPN SSL セッション（1000 など）を作成する場合は、15 TPS 以下の起動レートを使用してください。より高い TPS レートを使用すると、障害が発生する可能性があります。
- SSL VPN ピア検出（PD）は、AnyConnect クライアントバージョン 3.x 以降でのみサポートされています。

SSL VPN に関する情報

SSL VPN の概要

Cisco IOS XE SSL VPN は、データ、音声、およびワイヤレス向け統合型プラットフォームに備わる業界最先端のセキュリティ機能およびルーティング機能に SSL VPN リモートアクセス接続機能を統合して提供するルータベースのソリューションです。セキュリティはエンドユーザーの介入を必要とせず、簡単に管理できます。エンドユーザーは Cisco IOS XE SSL VPN を使用して、自宅やワイヤレスホットスポットなど、インターネットに接続されている任意の場所から安全にアクセスすることができます。また、Cisco IOS XE SSL VPN は、機密データを保護したまま、企業ネットワークへのアクセスを海外のパートナーやコンサルタントに拡張する場合にも使用できます。Cisco IOS XE SSL VPN と動的にダウンロードされる Cisco AnyConnect VPN Client を組み合わせて使用することにより、ほぼすべての企業アプリケーションへの完全なネットワークアクセスをリモートユーザーに提供することができます。

SSL VPN には次の 3 つのアクセス モードがありますが、Cisco IOS XE ソフトウェアでサポートされているのはトンネル モードのみです。

- クライアントレス：クライアントレスモードでは、プライベート Web リソースおよび Web コンテンツへのセキュアなアクセスが可能です。このモードは、インターネットアクセス、データベース、Web インターフェイスを使用するオンラインツールなど、Web ブラウザでアクセスするようなほとんどのコンテンツにアクセスする場合に便利です。
- シンクライアント（ポートフォワーディング Java アプレット）：シンクライアントモードでは、Web ブラウザの暗号化機能が拡張され、Post Office Protocol バージョン 3（POP3）、Simple Mail Transfer Protocol（SMTP）、Internet Message Access Protocol（IMAP）、Telnet、セキュアシェル（SSH）などの TCP ベースアプリケーションにリモートアクセスできます。
- フルトンネルモード：フルトンネル クライアント モードでは、動的にダウンロードされる SSL VPN 用 Cisco AnyConnect VPN Client（次世代の SSL VPN Client）を介して幅広いアプリケーションがサポートされます。フルトンネル クライアント モードでは、どのアプ

リケーションにも仮想的にネットワーク層アクセスできる、軽量で中央集約的な設定の、サポートが簡単な SSL VPN トンネリングクライアントが提供されます。

（注） **ip http secure-server** が有効になっている場合、SSL VPN は機能しません。

この機能は、次のプラットフォームでサポートされます。

プラットフォーム	サポートされている **Cisco IOS XE** リリース
Cisco Cloud Services Router 1000V シリーズ	Cisco IOS XE リリース 16.9
Cisco Catalyst 8000V	Cisco IOS XE Bengaluru 17.4.1
Cisco 4461 サービス統合型ルータ Cisco 4451 サービス統合型ルータ Cisco 4431 サービス統合型ルータ	Cisco IOS XE Cupertino 17.7.1a

リモートアクセスのモード

通常のクライアントレス リモート アクセス シナリオでは、リモートユーザーは SSL トンネルを確立してアプリケーション層（Web および E メールなど）の内部ネットワーク間のデータを移動します。トンネル モードでは、リモート ユーザは SSL トンネルを使用してネットワーク（IP）レイヤでデータを移動します。したがって、トンネル モードではほとんどの IP ベースアプリケーションがサポートされます。トンネルモードでは多くの一般的な企業アプリケーション（Microsoft Outlook、Microsoft Exchange、Lotus Notes E-mail、Telnet など）がサポートされています。

フルトンネルモードでサポートされる SSL VPN の機能と利点は次のとおりです。

- クライアントレス IPsec VPN に似た動作
- Java または ActiveX を使用して読み込まれるトンネル クライアント
- アプリケーションにとらわれない：すべての IP ベースアプリケーションのサポート
- スケーラブル
- インストールに必要なローカル管理許可

フルトンネル クライアント モードでは、動的にダウンロードされる SSL VPN 用 Cisco AnyConnect VPN Client（次世代の SSL VPN Client）を介して幅広いアプリケーションがサポートされます。フルトンネル クライアント モードでは、どのアプリケーションにも仮想的にネットワーク層アクセスできる、軽量で中央集約的な設定の、サポートが簡単な SSL VPN トンネリングクライアントが提供されます。SSL VPN の利点は、追加デスクトップソフトウェアをインストール

することなく、ほとんどどのインターネット接続されたシステムからもアクセスできる点です。Cisco SSL AnyConnect VPN を使用すると、リモートユーザーが SSL VPN ゲートウェイ経由でインターネットから企業ネットワークにアクセスできるようになります。ゲートウェイとの間で SSL VPN 接続を確立する際に、リモートユーザーの機器（ラップトップ、モバイル端末、PDA など）に Cisco AnyConnect VPN Client がダウンロードされてインストールされます。リモートユーザーが SSL VPN ゲートウェイにログインすると、トンネル接続が確立されます。トンネル接続は、グループポリシー設定によって指定されます。デフォルトでは、接続が閉じると Cisco AnyConnect VPN Client はクライアント PC から削除されます。ただし、Cisco AnyConnect VPN Client をクライアント機器にインストールしたままにしておくこともできます。

Cisco SSL AnyConnect VPN を使用すると会社のネットワーク内のサービスに簡単にアクセスすることができます。また、SSL VPN ゲートウェイでの VPN 設定も簡素化されます。それにより、システム管理者の負荷が軽減されます。

SSL VPN CLI の構成要素

SSL プロポーザル

SSL プロポーザルでは、サポートする暗号スイートが指定されています。各暗号スイートでは、キー交換アルゴリズム、一括暗号化アルゴリズム、および MAC アルゴリズムが定義されています。SSL ネゴシエーション時に、設定されている暗号スイートのいずれかがクライアントのプロポーザルから選択されます。クライアントのプロポーザルに含まれるスイートと設定されているスイートがまったく一致しない場合は、ネゴシエーションが終了します。現在のところ、暗号方式はクライアントの優先順位に基づいて選択されます。

SSL プロポーザルは、SSL ハンドシェイクプロトコルによる暗号化と復号のネゴシエーションで使用されます。ユーザが定義したプロポーザルが存在しない場合は、デフォルトの SSL プロポーザルが SSL ポリシーで使用されます。デフォルトのプロポーザルでは、次の順序で暗号方式が指定されています。

```
protection rsa-aes256-sha1 rsa-aes128-sha1 rsa-3des-ede-sha1 rsa-3des-ede-sha1
```

SSL ポリシー

SSL ポリシーでは、サポートする暗号スイートと、SSL ネゴシエーションで使用するトラストポイントが定義されています。SSL ポリシーは SSL ネゴシエーションで使用されるすべてのパラメータのコンテナです。ポリシーの選択は、ポリシーで設定されているパラメータに対してセッションのパラメータを照合することによって行われます。デフォルトのポリシーはありません。各ポリシーには、プロポーザルとトラストポイントが関連付けられています。

SSL プロファイル

SSL VPN プロファイルでは、認証およびアカウンティングのリストが定義されています。プロファイルの選択は、ポリシーと URL 値によって決定されます。プロファイルには、デフォルトの認可ポリシーを関連付けることもできます。

次のルールが適用されます。

- ポリシーおよび URL は SSL VPN プロファイルごとに一意である必要があります。
- セッションを起動するためには、1 つ以上の認可方式が指定されている必要があります。
- 3 つの認可タイプ（ユーザー、グループ、およびキャッシュ）を同時に使用することもできます。
- デフォルトの認可タイプはありません。
- 認可の優先順位は、ユーザ認可、キャッシュ認可、グループ認可の順になります。グループ認可を優先するように設定されている場合の優先順位は、グループ許可、ユーザー認可、キャッシュ認可の順になります。

SSL 認可ポリシー

SSL認可ポリシーはリモートクライアントにプッシュされる認可パラメータのコンテナです。プッシュされた認可パラメータは仮想アクセスインターフェイスでローカルに、またはデバイス上でグローバルに適用されます。認可ポリシーはSSL VPNプロファイルから参照されます。

SSL VPN MIB

SSL VPN MIB は、SSL VPN を実装するシスコのエンティティに関し、シスコの実装に固有の属性を表します。この MIB は、SSL VPN、トラップ制御、および通知グループを管理することにより、シスコの SSL VPN 実装における運用情報を提供します。たとえば、SSL VPN MIB は、デバイス上でアクティブな SSL トンネルの数などの情報を提供します。

SSL VPN の設定方法

ここでは、SSL VPN の設定に関連するさまざまなタスクについて説明します。

SSL プロポーザルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ssl proposal** *proposal-name*
4. **protection**
5. **end**
6. **show crypto ssl proposal** [*proposal name*]

手順の詳細

	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	**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	**crypto ssl proposal** *proposal-name* 例： `Device(config)# crypto ssl proposal proposal1`	SSL プロポーザル名を定義し、SSL プロポーザル コンフィギュレーション モードを開始します。
ステップ 4	**protection** 例： `Device(config-crypto-ssl-proposal)# protection rsa-3des-ede-sha1 rsa-aes128-sha1`	次の暗号スイートの中から 1 つまたは複数を指定します。 • rsa-3des-ede-sha1 • rsa-aes128-sha1 • rsa-aes256-sha1 • rsa-rc4128-md5
ステップ 5	**end** 例： `Device(config-crypto-ssl-proposal)# end`	SSL プロポーザル 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 6	**show crypto ssl proposal** [*proposal name*] 例： `Device# show crypto ssl proposal`	（任意）SSL プロポーザルを表示します。

SSL ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ssl policy** *policy-name*
4. **ip address local** *ip-address* [**vrf** *vrf-name*] [**port** *port-number*] [**standby** *redundancy-name*]
5. **ip interface local** *interface-name* [**vrf** *vrf-name*] [**port** *port-number*] [**standby** *redundancy-name*]
6. **pki trustpoint** *trustpoint-name* **sign**
7. **ssl proposal** *proposal-name*
8. **no shut**

9. **end**
10. **show crypto ssl policy** [*policy-name*]

手順の詳細

	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	**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	**crypto ssl policy** *policy-name* 例： `Device(config)# crypto ssl policy policy1`	SSL ポリシー名を定義し、SSL ポリシー 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	**ip address local** *ip-address* [**vrf** *vrf-name*] [**port** *port-number*] [**standby** *redundancy-name*] 例： `Device(config-crypto-ssl-policy)# ip address local 10.0.0.1 port 446`	TCP リスナーを開始するためのローカル IP アドレスを指定します。 （注） このコマンドまたは **ip interface local** コマンドの実行は必須です。
ステップ 5	**ip interface local** *interface-name* [**vrf** *vrf-name*] [**port** *port-number*] [**standby** *redundancy-name*] 例： `Device(config-crypto-ssl-policy)# ip interface local FastEthernet redundancy1`	TCP リスナーを開始するためのローカル インターフェイスを指定します。 （注） このコマンドまたは **ip address local** コマンドの実行は必須です。
ステップ 6	**pki trustpoint** *trustpoint-name* **sign** 例： `Device(config-crypto-ssl-policy)# pki trustpoint tp1 sign`	（任意）SSL ハンドシェイク中にサーバー証明書を送信するトラストポイントを指定します。 （注） このコマンドが指定されていない場合は、デフォルトの自己署名トラストポイントが使用されます。デフォルトの自己署名トラストポイントが存在しない場合は、システムによりデフォルトの自己署名証明書が作成されます。
ステップ 7	**ssl proposal** *proposal-name* 例： `Device(config-crypto-ssl-policy)# ssl proposal pr1`	（任意）SSL ハンドシェイク中に選択する暗号スイートを指定します。 （注） プロポーザルが指定されていない場合は、デフォルトのプロポーザルが使用されます。

	コマンドまたはアクション	目的
ステップ 8	**no shut** 例： `Device(config-crypto-ssl-policy)# no shut`	設定に基づいて TCP リスナーを開始します。
ステップ 9	**end** 例： `Device(config-crypto-ssl-policy)# end`	SSL ポリシー 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 10	**show crypto ssl policy** [*policy-name*] 例： `Device# show crypto ssl policy`	（任意）SSL ポリシーを表示します。

SSL プロファイルの設定

始める前に

AAA 設定の詳細については、『*Authentication Authorization and Accounting Configuration Guide*』を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ssl profile** *profile-name*
4. **aaa accounting user-pass list** *list-name*
5. **aaa authentication user-pass list** *list-name*
6. **aaa authorization group** [**override**] **user-pass list** *aaa-listname aaa-username*
7. **aaa authorization user user-pass** {**cached** | **list** *aaa-listname aaa-username*}
8. **match policy** *policy-name*
9. **match url** *url-name*
10. **no shut**
11. **end**
12. **show crypto ssl profile** [*profile-name*]

手順の詳細

	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。

	コマンドまたはアクション	目的
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	**crypto ssl profile** *profile-name* 例： `Device(config)# crypto ssl profile profile1`	SSL プロファイルを定義し、SSL プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**aaa accounting user-pass list** *list-name* 例： `Device(config-crypto-ssl-profile)# aaa accounting user-pass list list1`	認証、認可、およびアカウンティング（AAA）方式リストを指定します。
ステップ 5	**aaa authentication user-pass list** *list-name* 例： `Device(config-crypto-ssl-profile)# aaa authentication user-pass list list2`	AAA 方式リストを指定します。
ステップ 6	**aaa authorization group** [**override**] **user-pass list** *aaa-listname aaa-username* 例： `Device(config-crypto-ssl-profile)# aaa authorization group override user-pass list list1 user1`	グループ認可用の AAA 方式リストとユーザー名を指定します。 • **group**：グループ認可を指定します。 • **override**：（任意）属性のマージ中はグループ認可からの属性を優先する必要があることを指定します。デフォルトでは、ユーザー属性が優先されます。 • **user-pass**：ユーザーパスワードに基づく認可を指定します。 • *aaa-listname*：AAA 方式リスト名。 • *aaa-username*：AAA 要求で使用する必要があるユーザー名。デバイスで定義されている SSL 認可ポリシー名を参照します。
ステップ 7	**aaa authorization user user-pass** {**cached** | **list** *aaa-listname aaa-username*} 例： `Device(config-crypto-ssl-profile)# aaa authorization user user-pass list list1 user1`	ユーザー認可用の AAA 方式リストとユーザー名を指定します。 • **user**：ユーザー認可を指定します。 • **user-pass**：ユーザーパスワードに基づく認可を指定します。 • **cached**：EAP 認証中に受信した属性または AAA 事前共有キーから取得した属性をキャッシュする必要があることを指定します。

	コマンドまたはアクション	目的
		• *aaa-listname*：AAA 方式リスト名。 • *aaa-username*：AAA 認可要求で使用する必要があるユーザー名。
ステップ 8	**match policy** *policy-name* 例： `Device(config-crypto-ssl-profile)# match policy policy1`	match 文を使用し、SSL ポリシー名に基づいてピアの SSL プロファイルを選択します。
ステップ 9	**match url** *url-name* 例： `Device(config-crypto-ssl-profile)# match url www.abc.com`	match 文を使用し、URL に基づいてピアの SSL プロファイルを選択します。
ステップ 10	**no shut** 例： `Device(config-crypto-ssl-profile)# no shut`	**match policy** コマンドで指定されているポリシーが使用されるまでそのプロファイルを閉じないよう指定します。
ステップ 11	**end** 例： `Device(config-crypto-ssl-profile)# end`	SSL プロファイル 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 12	**show crypto ssl profile** [*profile-name*] 例： `Device# show crypto ssl profile`	（任意）SSL プロファイルを表示します。

SSL 認可ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ssl authorization policy** *policy-name*
4. **banner** *banner-text*
5. **client profile** *profile-name*
6. **def-domain** *domain-name*
7. 次のコマンドの 1 つを実行します。
   - **dns** *primary-server* [*secondary-server*]
   - または
   - **ipv6 dns** *primary-server* [*secondary-server*]
8. **dpd-interval** {**client** | **server**} *interval*

9. **homepage** *homepage-text*
10. **include-local-lan**
11. **ipv6 prefix** *prefix*
12. **keepalive** *seconds*
13. **module** *module-name*
14. **msie-proxy exception** *exception-name*
15. **msie-proxy option** {**auto** | **bypass** | **none**}
16. **msie-proxy server** {*ip-address* | *dns-name*}
17. **mtu** *bytes*
18. **netmask** *mask*
19. 次のコマンドの 1 つを実行します。
    - **pool** *name*
    - または
    - **ipv6 pool** *name*
20. **rekey time** *seconds*
21. 次のコマンドの 1 つを実行します。
    - **route set access-list** *acl-name*
    - または
    - **ipv6 route set access-list** *access-list-name*
22. **smartcard-removal-disconnect**
23. **split-dns** *string*
24. **timeout** {**disconnect** *seconds* | **idle** *seconds* | **session** *seconds*}
25. **wins** *primary-server* [*secondary-server*]
26. **end**
27. **show crypto ssl authorization policy** [*policy-name*]

手順の詳細

	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	**crypto ssl authorization policy** *policy-name* 例： `Device(config)# crypto ssl authorization policy policy1`	SSL 認可ポリシーを指定し、SSL 認可ポリシー 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 4	**banner** *banner-text* 例： `Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel. NOTE: DO NOT dial emergency response numbers (e.g. 911,112) from software telephony clients. Your exact location and the appropriate emergency response agency may not be easily identified.`	バナーを指定します。バナーはトンネルが正常に確立されると表示されます。
ステップ 5	**client profile** *profile-name* 例： `Device(config-crypto-ssl-auth-policy)# client profile Employee`	AnyConnect クライアントプロファイルを指定します。**crypto vpn anyconnect profile** コマンドを使用してすでに指定されているプロファイルを使用する必要があります。AnyConnect イメージおよびプロファイルの設定例については、例：AnyConnect イメージおよびプロファイルの指定（288 ページ）のセクションを参照してください。 AnyConnect の設定の詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』を参照してください。
ステップ 6	**def-domain** *domain-name* 例： `Device(config-crypto-ssl-auth-policy)# def-domain example.com`	デフォルト ドメインを指定します。このパラメータでは、クライアントが使用できるデフォルト ドメインを指定します。

ステップ 7	次のコマンドの 1 つを実行します。
	• **dns** *primary-server* [*secondary-server*]
	• または
	• **ipv6 dns** *primary-server* [*secondary-server*]
	例：
	`Device(config-crypto-ssl-auth-policy)# dns 198.51.100.1 198.51.100.100`
	例：
	`Device(config-crypto-ssl-auth-policy)# ipv6 dns 2001:DB8:1::1 2001:DB8:2::2`
		プライマリおよびセカンダリ Domain Name Service（DNS）サーバーの IPv4 アドレスまたは IPv6 アドレスを指定します。
		• *primary-server*：プライマリ DNS サーバーの IP アドレス。
		• *secondary-server*：（任意）セカンダリ DNS サーバーの IP アドレス。

ステップ 8	**dpd-interval** {**client** | **server**} *interval* 例： `Device(config-crypto-ssl-auth-policy)# dpd-interval client 1000`	クライアントまたはサーバーの Dead Peer Detection（DPD; デッドピア検出）をグローバルに設定します。 • **client**：クライアントモードの DPD。デフォルト値は 300（5 分）です。 • **server**：サーバーモードの DPD。デフォルト値は 300（5 分）です。

	コマンドまたはアクション	目的
		• *interval*：間隔（秒単位）。範囲は 5 ～ 3600 です。
ステップ 9	**homepage** *homepage-text* 例： `Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com`	SSL VPN ホーム ページの URL を指定します。
ステップ 10	**include-local-lan** 例： `Device(config-crypto-ssl-auth-policy)# include-local-lan`	このキーワードを指定すると、ローカル LAN のリソース（ネットワーク プリンタなど）にリモート ユーザがアクセスできるようになります。
ステップ 11	**ipv6 prefix** *prefix* 例： `Device(config-crypto-ssl-auth-policy)# ipv6 prefix 64`	IPv6 アドレスの IPv6 プレフィックスを定義します。 • *prefix*：プレフィックス長。有効な範囲は 1 ～ 128 です。
ステップ 12	**keepalive** *seconds* 例： `Device(config-crypto-ssl-auth-policy)# keepalive 500`	キープアライブの最小値、最大値、およびデフォルト値を秒単位で設定します。
ステップ 13	**module** *module-name* 例： `Device(config-crypto-ssl-auth-policy)# module gina`	VPN を特定のグループに接続するために必要なモジュールをサーバ ゲートウェイにダウンロードします。 • **dart**：AnyConnect Diagnostics and Reporting Tool（DART）モジュールをダウンロードします。 • **gina**：Start Before Logon（SBL）モジュールをダウンロードします。
ステップ 14	**msie-proxy exception** *exception-name* 例： `Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2`	*exception-name* 引数で指定された DNS 名または IP アドレスにはプロキシ経由で送信が行われないようになります。
ステップ 15	**msie-proxy option** {**auto** | **bypass** | **none**} 例： `Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass`	Microsoft Internet Explorer ブラウザのプロキシ設定を指定します。内部のプロキシサーバを指定して、企業ネットワークへの接続時にブラウザのトラフィックがプロキシ サーバを経由するように設定する場合は、プロキシ設定が必要です。

	コマンドまたはアクション	目的
		• **auto**：プロキシサーバー設定を自動検出するようにブラウザを設定します。 • **bypass**：ローカルアドレスの場合はプロキシサーバーを経由しません。 • **none**：プロキシサーバーを使用しないようにブラウザを設定します。
ステップ 16	**msie-proxy server** {*ip-address* | *dns-name*} 例： `Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2`	プロキシサーバーの IP アドレスまたは DNS 名（後にポート番号を付けることもできます）。 （注） **msie-proxy option bypass** コマンドが指定されている場合、このコマンドは必須です。
ステップ 17	**mtu** *bytes* 例： `Device(config-crypto-ssl-auth-policy)# mtu 1000`	（任意）MTU の最小値、最大値、およびデフォルト値を設定します。 （注） このコマンドで指定された値は、Cisco AnyConnect Secure クライアントの設定で指定されているデフォルトの MTU 値よりも優先されます。このコマンドを指定しない場合は、Cisco AnyConnect Secure クライアントの設定で指定されている値が MTU 値として使用されます。計算された MTU がこのコマンドで指定されている MTU を下回っている場合、このコマンドは無視されます。
ステップ 18	**netmask** *mask* 例： `Device(config-crypto-ssl-auth-policy)# netmask 255.255.255.0`	クライアントに IP アドレスを割り当てるサブネットのネットマスクを指定します。 • *mask*：サブネット マスク アドレス。

ステップ 19	次のコマンドの 1 つを実行します。
	• **pool** *name*
	• または
	• **ipv6 pool** *name*
	例：
	`Device(config-crypto-ssl-auth-policy)# pool abc`
	例：
	`Device(config-crypto-ssl-auth-policy)# ipv6 pool ipv6pool`
		リモートアクセス クライアントに IP アドレスを割り当てるためのローカル IPv4 アドレス プールまたはローカル IPv6 アドレス プールを定義します。
		• *name*：ローカル IP アドレス プールの名前。
		（注） **ip local pool** コマンドを使用してすでに定義されているローカル IP アドレス プールを使用する必要があります。

	コマンドまたはアクション	目的
ステップ 20	**rekey time** *seconds* 例： `Device(config-crypto-ssl-auth-policy)# rekey time 1110`	キー再生成の間隔を秒単位で指定します。デフォルト値は 3600 です。

ステップ 21	次のコマンドの 1 つを実行します。
	• **route set access-list** *acl-name*
	• または
	• **ipv6 route set access-list** *access-list-name*
	例：
	`Device(config-crypto-ssl-auth-policy)# route set access-list acl1`
	例：
	`Device(config-crypto-ssl-auth-policy)# ipv6 route set access-list acl1`
		アクセスリストを使用して、トンネルを介してセキュリティで保護する必要がある IPv4 または IPv6 ルートを確立します。
		• *acl-name*：アクセス リスト名。

ステップ 22	**smartcard-removal-disconnect** 例： `Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect`	スマートカードの削除による接続解除を有効にし、スマート カードが削除されたときにクライアント側でセッションを終了するよう指定します。
ステップ 23	**split-dns** *string* 例： `Device(config-crypto-ssl-auth-policy)# split-dns example.com example.net`	クライアント側でプライベート ネットワーク用に使用するドメイン名を 10 個まで指定できます。
ステップ 24	**timeout** {**disconnect** *seconds* | **idle** *seconds* | **session** *seconds*} 例： `Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000`	タイムアウトを秒単位で指定します。 • **disconnect** *seconds*：Cisco AnyConnect クライアントからゲートウェイサーバーへの接続を再試行する期間を秒単位で指定します。デフォルト値は 0 です • **idle** *seconds*：アイドルタイムアウトを秒単位で指定します。デフォルト値は 1800（30 分）です。 • **session** *seconds*：セッションタイムアウトを秒単位で指定します。デフォルト値は 43200（12 時間）です。
ステップ 25	**wins** *primary-server* [*secondary-server*] 例： `Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115`	内部の Windows Internet Naming Service（WINS）サーバのアドレスを指定します。 • *primary-server*：プライマリ WINS サーバーの IP アドレス。

	コマンドまたはアクション	目的
		• *secondary-server*：（任意）セカンダリ WINS サーバーの IP アドレス。
ステップ 26	**end** 例： `Device(config-crypto-ssl-auth-policy)# end`	SSL 認可ポリシー 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 27	**show crypto ssl authorization policy** [*policy-name*] 例： `Device(config-crypto-ssl-auth-policy)# show crypto ssl authorization policy`	（任意）SSL 認可ポリシーを表示します。

SSL VPN 設定の確認

このセクションでは、**show** コマンドを使用して SSL VPN の設定を確認する方法について説明します。

手順の概要

1. **enable**
2. **show crypto ssl proposal** [*name*]
3. **show crypto ssl policy** [*name*]
4. **show crypto ssl profile** [*name*]
5. **show crypto ssl authorization policy** [*name*]
6. **show crypto ssl session** {**user** *user-name* | **profile** *profile-name*}
7. **show crypto ssl stats** [**profile** *profile-name*] [**tunnel**] [**detail**]
8. **clear crypto ssl session** {**profile** *profile-name*| **user** *user-name*}

手順の詳細

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 **show crypto ssl proposal** [*name*]

例：

```
Device# show crypto ssl proposal

SSL Proposal: sslprop
    Protection: 3DES-SHA1
```

SSL プロポーザルを表示します。

ステップ 3 **show crypto ssl policy** [*name*]

例：

```
Device# show crypto ssl policy

 SSL Policy: sslpolicy
  Status     : ACTIVE
  Proposal   : sslprop
  IP Address : 10.78.106.23
  Port       : 443
  fvrf       : 0
  Trust Point: TP-self-signed-1183786860
  Redundancy : none
```

SSL ポリシーを表示します。

ステップ 4 **show crypto ssl profile** [*name*]

例：

```
Device# show crypto ssl profile

SSL Profile: sslprofile
 Status: ACTIVE
 Match Criteria:
   URL: none
   Policy:
    sslpolicy
 AAA accounting List      : local
 AAA authentication List  :none
 AAA authorization cached  :true
 AAA authorization user List   :default
 AAA authorization user name: sslauth
 AAA authorization group List   :none
 AAA authorization group name: none
 Authentication Mode      : user credentials
 Interface                : SSLVPN-VIF1
   Status: ENABLE
```

SSL プロファイルを表示します。

ステップ 5 **show crypto ssl authorization policy** [*name*]

例：

```
Device# show crypto ssl authorization policy

SSL Auth Policy: sslauth
 V4 Parameter:
   Address Pool: SVC_POOL
   Netmask: 255.255.255.0
   Route ACL : split-include
 Banner                   : none
 Home Page                : none
 Idle timeout             : 300
 Disconnect Timeout       : 0
 Session Timeout          : 43200
 Keepalive Interval       : 0
 DPD Interval             : 300
 Rekey
   Interval: 0
```

```
  Method  : none
Split DNS               : none
Default domain          : none
Proxy Settings
    Server: none
    Option: NULL
    Exception(s): none
Anyconnect Profile Name :
SBL Enabled             : NO
MAX MTU                 : 1406
Smart Card
Removal Disconnect      : NO
```

SSL 認可ポリシーを表示します。

ステップ 6 **show crypto ssl session** {**user** *user-name* | **profile** *profile-name*}

例：

```
Device# show crypto ssl session user LAB

Session Type      : Full Tunnel
Client User-Agent : AnyConnect Windows 3.0.08057

Username          : LAB                  Num Connection : 1
Public IP         : 10.163.209.245
Profile           : sslprofile              Policy Group   : sslauth
Last-Used         : 00:00:02           Created        : *00:58:44.219 PDT Thu Jul 25 2013
Session Timeout   : 43200           Idle Timeout   : 300
DPD GW Timeout    : 300           DPD CL Timeout : 300
Address Pool      : sslvpn-pool     MTU Size       : 1406
Rekey Time        : 0                    Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 10.1.1.2             Netmask        : 255.255.255.0
Rx IP Packets     : 0                    Tx IP Packets  : 125
CSTP Started      : 00:01:12          Last-Received  : 00:00:02
CSTP DPD-Req sent : 0             Virtual Access : 0
Msie-ProxyServer  : None          Msie-PxyPolicy : Disabled
Msie-Exception    :
Client Ports      : 34552

Device# show crypto ssl session profile sslprofile

SSL profile name: sslprofile
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
LAB                10.163.209.245             1         00:00:33  00:00:00
Error receiving show session info from remote cores
```

SSL VPN セッション情報を表示します。

ステップ 7 **show crypto ssl stats** [**profile** *profile-name*] [**tunnel**] [**detail**]

例：

```
Device# show crypto ssl stats

SSLVPN Global statistics:
    Active connections       : 0          AAA pending reqs         : 0
    Peak connections         : 1          Peak time                : 1w6d
    Authentication failures  : 21
    VPN session timeout      : 1          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Login Denied             : 0
    Connect succeed          : 1          Connect failed           : 0
    Reconnect succeed        : 0          Reconnect failed         : 0
```

```
    IP Addr Alloc Failed     : 0          VA creation failed       : 0
    Route Insertion Failed   : 0
    IPV6 Addr Alloc Failed   : 0
    IPV6 Route Insert Failed : 0
    IPV6 Hash Insert Failed  : 0
    IPV6 STC Alloc Failed    : 0
    in  CSTP control         : 5          out CSTP control         : 3
    in  CSTP data            : 21         out CSTP data            : 8

Device# show crypto ssl stats tunnel profile prf1
SSLVPN Profile name : prf1
Tunnel Statistics:
    Active connections       : 0
    Peak connections         : 0          Peak time                : never
    Connect succeed          : 0          Connect failed           : 0
    Reconnect succeed        : 0          Reconnect failed         : 0
    DPD timeout              : 0
  Client
    in  CSTP frames          : 0          in  CSTP control         : 0
    in  CSTP data            : 0          in  CSTP bytes           : 0
    out CSTP frames          : 0          out CSTP control         : 0
    out CSTP data            : 0          out CSTP bytes           : 0
    cef in  CSTP data frames : 0          cef in  CSTP data bytes  : 0
    cef out CSTP data frames : 0          cef out CSTP data bytes  : 0
  Server
    In  IP pkts              : 0          In  IP bytes             : 0
    Out IP pkts              : 0          Out IP bytes             : 0
```

SSL VPN の統計情報を表示します。

ステップ 8 **clear crypto ssl session** {**profile** *profile-name*| **user** *user-name*}

例：

```
Device# clear crypto ssl session sslprofile
```

SSL VPN セッションをクリアします。

SSL VPN の設定例

例：SSL VPN の仮想テンプレートの作成

次の例では、SSL VPN のテンプレートを作成する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface virtual-template 1 type vpn
Device(config-if)# ip unnumbered Te0/0/4
Device(config-if)# ip tcp adjust-mss 1300
Device(config-if)# end
```

例：AnyConnect イメージおよびプロファイルの指定

次の例は、Cisco AnyConnect イメージおよびプロファイルの指定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto vpn anyconnect bootflash:/webvpn/anyconnect-win-3.1.04072-k9.pkg
 sequence 1
Device(config)# crypto vpn anyconnect profile Employee bootflash:/Employee.xml
Device(config)# end
```

例：SSL プロポーザルの設定

次の例は、SSL プロポーザルの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl proposal proposal1
Device(config-crypto-ssl-proposal)# protection rsa-3des-ede-sha1 rsa-aes128-sha1
Device(config-crypto-ssl-proposal)# end
```

例：SSL ポリシーの設定

次の例は、SSL ポリシーの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl policy policy1
Device(config-crypto-ssl-policy)# ip address local 10.0.0.1 port 443
Device(config-crypto-ssl-policy)# pki trustpoint tp1 sign
Device(config-crypto-ssl-policy)# ssl proposal proposal1
Device(config-crypto-ssl-policy)# no shut
Device(config-crypto-ssl-policy)# end
```

例：SSL プロファイルの設定

次の例は、SSL プロファイルの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl profile profile1
Device(config-crypto-ssl-profile)# aaa accounting user-pass list list1
Device(config-crypto-ssl-profile)# aaa authentication user-pass list list2
Device(config-crypto-ssl-profile)# aaa authorization group override user-pass list list1
 user1
Device(config-crypto-ssl-profile)# aaa authorization user user-pass list list1 user1
Device(config-crypto-ssl-profile)# match policy policy1
Device(config-crypto-ssl-profile)# match url www.abc.com
Device(config-crypto-ssl-profile)# virtual-template 1
Device(config-crypto-ssl-profile)# no shut
Device(config-crypto-ssl-profile)# end
```

例：SSL 認可ポリシーの設定

次の例は、SSL 認可ポリシーの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl authorization policy policy1
Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel.
Device(config-crypto-ssl-auth-policy)# client profile Employee
Device(config-crypto-ssl-auth-policy)# def-domain cisco
Device(config-crypto-ssl-auth-policy)# dns 198.51.100.1 198.51.100.100
Device(config-crypto-ssl-auth-policy)# dpd client 1000
Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com
Device(config-crypto-ssl-auth-policy)# include-local-lan
Device(config-crypto-ssl-auth-policy)# keepalive 500
Device(config-crypto-ssl-auth-policy)# module gina
Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2
Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass
Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2
Device(config-crypto-ssl-auth-policy)# mtu 1000
Device(config-crypto-ssl-auth-policy)# netmask 255.255.255.0
Device(config-crypto-ssl-auth-policy)# pool abc
Device(config-crypto-ssl-auth-policy)# rekey interval 1110
Device(config-crypto-ssl-auth-policy)# route set access-list acl1
Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect
Device(config-crypto-ssl-auth-policy)# split-dns abc1
Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000
Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115
Device(config-crypto-ssl-auth-policy)# end
```

次の例は、SSL VPN の IPv6 サポート機能をイネーブルにする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ssl authorization policy policy1
Device(config-crypto-ssl-auth-policy)# banner This is SSL VPN tunnel.
Device(config-crypto-ssl-auth-policy)# client profile profile1
Device(config-crypto-ssl-auth-policy)# def-domain cisco
Device(config-crypto-ssl-auth-policy)# ipv6 dns 2001:DB8:1::1 2001:DB8:2::2
Device(config-crypto-ssl-auth-policy)# dpd client 1000
Device(config-crypto-ssl-auth-policy)# homepage http://www.abc.com
Device(config-crypto-ssl-auth-policy)# include-local-lan
Device(config-crypto-ssl-auth-policy)# ipv6 prefix 64
Device(config-crypto-ssl-auth-policy)# ipv6 route set access-list acl1
Device(config-crypto-ssl-auth-policy)# keepalive 500
Device(config-crypto-ssl-auth-policy)# module gina
Device(config-crypto-ssl-auth-policy)# msie-proxy exception 198.51.100.2
Device(config-crypto-ssl-auth-policy)# msie-proxy option bypass
Device(config-crypto-ssl-auth-policy)# msie-proxy server 198.51.100.2
Device(config-crypto-ssl-auth-policy)# mtu 1000
Device(config-crypto-ssl-auth-policy)# ipv6 pool ipv6pool
Device(config-crypto-ssl-auth-policy)# rekey interval 1110
Device(config-crypto-ssl-auth-policy)# route set access-list acl1
Device(config-crypto-ssl-auth-policy)# smartcard-removal-disconnect
Device(config-crypto-ssl-auth-policy)# split-dns abc1
Device(config-crypto-ssl-auth-policy)# timeout disconnect 10000
Device(config-crypto-ssl-auth-policy)# wins 203.0.113.1 203.0.113.115
Device(config-crypto-ssl-auth-policy)# end
```

SSL VPN のその他の関連資料

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』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

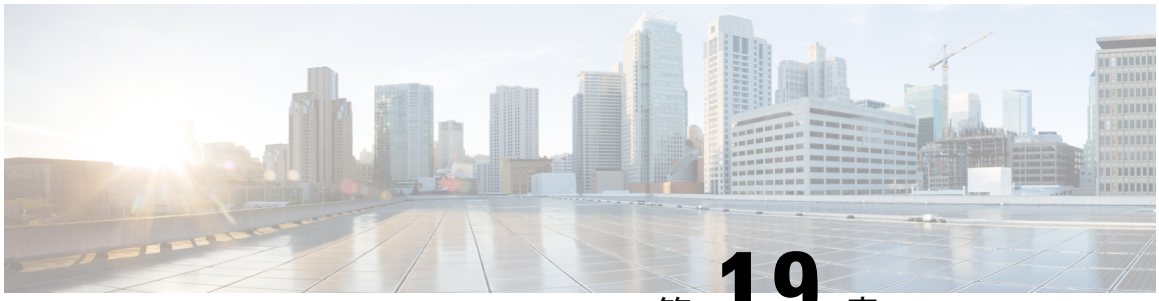
SSL VPN の機能情報

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

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

表 *28 : SSL VPN* の機能情報

機能名	リリース	機能情報
SSL VPN	Cisco IOS XE リリース 17.7.1a	SSL VPN 機能が導入されました。この機能は Cisco IOS XE ソフトウェアでサポートされています。この機能を使用することにより、リモートユーザーはインターネット上のどこからでも企業ネットワークにアクセスできるようになります。



第 19 章

Call Home の設定

Call Home 機能は、クリティカルなシステム イベントを E メールおよび Web 上で通知します。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの適切な互換性のために、さまざまなメッセージの形式が使用できます。この機能の一般的な使用方法としては、ネットワーク サポート技術者の直接ページング、ネットワーク オペレーション センターへの E メール通知、サポート Web サイトへの XML 送信、シスコのテクニカル サポート（TAC）で事例を直接生成するための Cisco Smart Call Home サービスの使用などがあります。

この章では、Cisco ISR 4400 シリーズ ルータ用および Cisco ISR 4300 シリーズ ルータ用の Cisco IOS Release 15.4(3) S 以降のリリースで Call Home 機能を設定する方法について説明します。

この章は、次の項で構成されています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポート、および Cisco IOS、Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator

にアクセスするには、http://tools.cisco.com/ITDIT/CFN/を参照してください。Cisco Feature Navigator にアクセスするために、シスコのアカウントは必要ありません。

Call Home の前提条件

Call Home を設定するための前提条件を次に示します。

- 受信者が受け取ったメッセージの送信元を判別できるように、連絡先の電子メールアドレス（Smart Call Home のフル登録では必須、Call Mode が匿名モードでイネーブルになっている場合は任意）、電話番号（任意）、住所情報（任意）を設定する必要があります。
- 少なくとも 1 つの宛先プロファイル（定義済みまたはユーザ定義）を設定する必要があります。使用する宛先プロファイルは、受信エンティティがポケットベル、電子メールアドレス、または Cisco Smart Call Home などの自動サービスのいずれであるかによって異なります。

  宛先プロファイルが E メール メッセージ送信を使用している場合、シンプル メール転送プロトコル（SMTP）サーバを指定する必要があります。
- ルータは E メール サーバまたは宛先 HTTP サーバに IP 接続されている必要があります。
- Cisco Smart Call Home を使用する場合は、完全な Cisco Smart Call Home サービスを提供するために、デバイスを対象とした有効なサービス契約が必要です。

Call Home の概要

Call Home 機能を使用すると、設定、環境条件、インベントリ、syslog、スナップショット、およびクラッシュ イベントについての情報を含むアラート メッセージを送信できます。これらのアラート メッセージは、電子メール ベースまたは Web ベースのメッセージとして提供されます。複数のメッセージ フォーマットから選択できるので、ポケットベル サービス、標準的な電子メール、または XML ベースの自動解析アプリケーションとの互換性が得られます。この機能では、複数の受信者（Call Home 宛先プロファイルという）にアラートを送信できます。宛先プロファイルごとに、メッセージ形式とコンテンツのカテゴリを設定できます。Cisco TAC（callhome@cisco.com）にアラートを送信するための事前定義された宛先プロファイルが用意されています。また、独自の宛先プロファイルを定義することもできます。

柔軟なメッセージの配信オプションとフォーマット オプションにより、個別のサポート要件を簡単に統合できます。

ここでは、次の内容について説明します。

- Call Home を使用するメリット
- Smart Call Home サービスの取得

Call Home を使用するメリット

Call Home 機能には次のようなメリットがあります。

- 次のような複数のメッセージ形式オプション：
  - ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。
  - プレーン テキスト：人間が読むのに適した形式に完全整形されたメッセージ情報。
  - XML：XML および Adaptive Markup Language（AML）Document Type Definitions（DTD）を使用するマシンが判読可能な形式です。XML 形式では、シスコ TAC と通信できます。
- 複数のメッセージ宛先への同時配信が可能。
- 複数のメッセージ カテゴリ（設定、環境条件、インベントリ、syslog、スナップショット、クラッシュ イベントなど）。
- シビラティ（重大度）とパターンマッチによるメッセージのフィルタリング
- 定期的なメッセージ送信のスケジューリング

Smart Call Home サービスの取得

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービスに登録できます。Smart Call Home は、Smart Call Home メッセージを分析し、背景説明と推奨措置を提供します。既知の問題、特にオンライン診断障害については、TAC に Automatic Service Request が作成されます。

Smart Call Home には、次の機能があります。

- 継続的なデバイス ヘルス モニタリングとリアルタイムの診断アラート。
- Smart Call Home メッセージの分析。必要に応じて、自動サービス要求（詳細な診断情報が含まれる）が作成され、該当する TAC チームにルーティングされるため、問題解決を高速化できます。
- セキュアなメッセージ転送が、ご使用のデバイスから直接、または HTTP プロキシ サーバやダウンロード可能な転送ゲートウェイ（TG）を経由して行われます。TG 集約ポイントは、複数のデバイスをサポートする場合またはセキュリティ要件によって、デバイスをインターネットに直接接続できない場合に使用できます。
- すべての Smart Call Home デバイスの Smart Call Home メッセージと推奨事項、インベントリ情報、および設定情報に Web アクセスすることにより、関連するフィールド通知、セキュリティ勧告、およびサポート終了日情報にアクセスできます。

Smart Call Home で次の項目を登録する必要があります。

- ルータの SMARTnet 契約番号

- 電子メール アドレス
- Cisco.com のユーザ名

Smart Call Home の詳細については、https://supportforums.cisco.com/community/4816/smart-call-home を参照してください。

Anonymous Reporting

Smart Call Home は、多くのシスコ サービス契約に含まれるサービス機能で、顧客が問題をより迅速に解決できるように支援することを目的としています。また、クラッシュ メッセージから取得した情報は、シスコが現場の機器や発生している問題を理解しやすくします。Smart Call Home を使用しない場合でも、Anonymous Reporting をイネーブルにすると、シスコはデバイスから最小限のエラーおよびヘルス情報をセキュアに受信できます。Anonymous Reporting をイネーブルにした場合、顧客が誰であるかは匿名のままで、識別情報は送信されません。

（注） Anonymous Reporting をイネーブルにすると、シスコまたはシスコに代わって業務を行うベンダーに指定データを転送することに同意することになります（米国以外の国を含む）。シスコでは、すべてのお客様のプライバシーを保護しています。シスコでの個人情報の取り扱いについては、シスコのプライバシー ステートメント（http://www.cisco.com/web/siteassets/legal/privacy.html）参照してください。

Call Home が匿名で設定されていると、クラッシュ、インベントリ、およびテスト メッセージだけがシスコに送信されます。顧客の識別情報は送信されません。

これらのメッセージの送信内容の詳細については、アラート グループの起動イベントとコマンド （337 ページ）を参照してください。

Call Home の設定方法

以下の項では、1 つのコマンドを使用して Call Home を設定する方法について説明します。

- Smart Call Home の設定（単一コマンド） （297 ページ）
- Smart Call Home の設定と有効化 （298 ページ）

以下の項では、詳細な設定およびオプションの設定について説明します。

- Call Home のイネーブル化とディセーブル化 （298 ページ）
- 連絡先情報の設定 （299 ページ）
- 宛先プロファイルの設定 （301 ページ）
- アラート グループへの登録 （305 ページ）
- 一般的な電子メール オプションの設定 （310 ページ）

Smart Call Home の設定（単一コマンド）

1 つのコマンドですべての Call Home の基本設定をイネーブルにするには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home reporting** {**anonymous**	**contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address*	*ipv6-address*	*name*} **port** *port-number*] 例： `Router(config)# call-home reporting contact-email-addr email@company.com`	1 つのコマンドを使用して Call Home の基本設定をイネーブルにします。 • **anonymous**：Call-Home TAC プロファイルがクラッシュメッセージ、インベントリメッセージ、およびテストメッセージのみを送信し、これらのメッセージを匿名で送信するようにします。 • **contact-email-addr**：Smart Call Home サービスのフル レポート機能をイネーブルにし、フル インベントリ メッセージを Call Home TAC プロファイルから Smart Call Home サーバに送信してフル登録プロセスを開始します。 • **http-proxy** {*ipv4-address*	*ipv6-address*	*name*}：IPv4 または IPv6 アドレス、あるいはサーバー名を設定します。最大長は 64 文字です。

	コマンドまたはアクション	目的
		• **port** *port-number*：ポート番号。 有効値の範囲は 1 ～ 65535 です。 （注） HTTP プロキシ オプションでは、バッファリングするための独自のプロキシ サーバおよびデバイスからのセキュア接続を利用できます。 （注） **call-home reporting** コマンドを使用して匿名またはフル登録モードで Call Home を正常にイネーブルにした後、インベントリ メッセージが送信されます。Call Home がフル登録モードでイネーブルになっている場合、フル登録モードのフル インベントリ メッセージが送信されます。Call Home が匿名モードでイネーブルになっている場合、匿名のインベントリ メッセージが送信されます。これらのメッセージの送信内容の詳細については、アラート グループの起動イベントとコマンド（337 ページ）を参照してください。

Smart Call Home の設定と有効化

Cisco Smart Call Home サービスのアプリケーションおよび設定に関する情報については、https://supportforums.cisco.com/community/4816/smart-call-home にある『Smart Call Home User Guide』の「Getting Started」の項を参照してください。このマニュアルには、デバイスから直接、または転送ゲートウェイ（TG）集約ポイントを介して Smart Call Home メッセージを送信するための設定例が含まれています。

（注） HTTPS には追加的なペイロード暗号化が含まれているため、セキュリティ上の理由から、HTTPS 転送オプションを使用することをお勧めします。インターネットへの接続に集約ポイントまたはプロキシが必要な場合は、Cisco.com からダウンロード可能な転送ゲートウェイ ソフトウェアを使用できます。

Call Home のイネーブル化とディセーブル化

Call Home 機能をイネーブルまたはディセーブルにするには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **service call-home**
3. **no service call-home**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**service call-home** 例： `Router(config)# service call-home`	Call Home 機能をイネーブルにします。
ステップ 3	**no service call-home** 例： `Router(config)# no service call-home`	Call Home 機能をディセーブルにします。

連絡先情報の設定

各ルータには、連絡先電子メール アドレスが含まれる必要があります（ただしCall Homeが匿名モードでイネーブルに設定されている場合を除く）。任意で、電話番号、住所、契約 ID、カスタマー ID、サイト ID を割り当てることができます。

連絡先情報を割り当てるには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **call-home**
3. **contact-email-addr** *email-address*
4. **phone-number** *+phone-number*
5. **street-address** *street-address*
6. **customer-id** *text*
7. **site-id** *text*
8. **contract-id** *text*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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
	`Router# configure terminal`	
ステップ 2	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**contact-email-addr** *email-address* 例： `Router(cfg-call-home)# contact-email-addr username@example.com`	自分の電子メール アドレスを指定します。E メール アドレス フォーマットにはスペースなしで最大 200 文字まで入力できます。
ステップ 4	**phone-number** *+phone-number* 例： `Router(cfg-call-home)# phone-number +1-800-555-4567`	（任意）自分の電話番号を割り当てます。 （注） 番号は必ずプラス（+）記号で始まり、ダッシュ（-）と数字だけが含まれるようにしてください。17 文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。
ステップ 5	**street-address** *street-address* 例： `Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345“`	（任意）RMA 機器の配送先である自分の住所を割り当てます。最大 200 文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。
ステップ 6	**customer-id** *text* 例： `Router(cfg-call-home)# customer-id Customer1234`	（任意）カスタマー ID を指定します。最大 64 文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。
ステップ 7	**site-id** *text* 例： `Router(cfg-call-home)# site-id Site1ManhattanNY`	（任意）カスタマー サイト ID を指定します。最大 200 文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。
ステップ 8	**contract-id** *text* 例： `Router(cfg-call-home)# contract-id Company1234`	（任意）ルータの契約 ID を指定します。最大 64 文字まで入力できます。スペースを含める場合は、エントリを引用符（“”）で囲む必要があります。

例

次に、連絡先情報を設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr username@example.com
Router(cfg-call-home)# phone-number +1-800-555-4567
```

```
Router(cfg-call-home)# street-address “1234 Picaboo Street, Any city, Any state, 12345”
Router(cfg-call-home)# customer-id Customer1234
Router(cfg-call-home)# site-id Site1ManhattanNY
Router(cfg-call-home)# contract-id Company1234
Router(cfg-call-home)# exit
```

宛先プロファイルの設定

宛先プロファイルには、アラート通知に必要な配信情報が入っています。少なくとも1つの宛先プロファイルが必要です。1 つまたは複数のタイプの複数の宛先プロファイルを設定できます。

新しい宛先プロファイルを作成して定義することも、定義済みの宛先プロファイルをコピーして使用することもできます。新しい宛先プロファイルを定義する場合は、プロファイル名を割り当てる必要があります。

（注） Cisco Smart Call Home サービスを使用する場合、宛先プロファイルは XML メッセージ フォーマットでなければなりません。

次の属性を宛先プロファイルに設定できます。

- プロファイル名：ユーザ定義の宛先プロファイルを一意に識別する文字列。プロファイル名は 31 文字までで大文字と小文字は区別されません。

（注） プロファイル名として **all** は使用できません。

- 転送方法：アラートを送信するための転送メカニズム（電子メールまたは HTTP（HTTPS を含む））。
  - ユーザ定義の宛先プロファイルの場合、E メールがデフォルトで、どちらかまたは両方の転送メカニズムをイネーブルにできます。両方の方法をディセーブルにすると、E メールがイネーブルになります。
  - あらかじめ定義された Cisco TAC プロファイルの場合、いずれかの転送メカニズムをイネーブルにできますが、同時にはイネーブルにできません。
- 宛先アドレス：アラートを送信する転送方法に関連した実際のアドレス。
- メッセージ形式：アラートの送信に使用するメッセージ形式。ユーザ定義宛先プロファイルの形式オプションは、ロングテキスト、ショートテキスト、または XML です。デフォルトは XML です。定義済みのシスコ TAC プロファイルの場合、XML しか使用できません。
- メッセージ サイズ：宛先メッセージの最大サイズ。有効範囲は 50 ～ 3,145,728 バイトです。デフォルト値は 3,145,728 バイトです。

Anonymous Reporting：顧客 ID を匿名のままにするよう選択できます。これにより、識別情報が送信されません。

- 関心のあるアラート グループへの登録：各自の関心事項を示すアラート グループに登録することができます。

ここでは、次の内容について説明します。

新しい宛先プロファイルの作成

新しい宛先プロファイルを作成し、設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. [**no**] **destination transport-method** {**email** | **http**}
5. **destination address** {**email** *email-address* | **http** *url*}
6. **destination preferred-msg-format** {**long-text** | **short-text** | **xml**}
7. **destination message-size-limit** *bytes*
8. **active**
9. **end**
10. **show call-home profile** {*name* | **all**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**profile** *name* 例： `Router(config-call-home)# profile profile1`	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。指定された宛先プロファイルが存在しない場合、作成されます。

	コマンドまたはアクション	目的
ステップ 4	[**no**] **destination transport-method** {**email** | **http**} 例： `Router(cfg-call-home-profile)# destination transport-method email`	（任意）メッセージ転送方法をイネーブルにします。**no** オプションを選択すると、方法がディセーブルになります。
ステップ 5	**destination address** {**email** *email-address* | **http** *url*} 例： `Router(cfg-call-home-profile)# destination address email myaddress@example.com`	Call Home メッセージを送信する宛先 E メール アドレスまたは URL を設定します。 （注） 宛先 URL を入力する場合は、サーバがセキュア サーバであるかどうかに応じて **http://** または **https://** を指定します。
ステップ 6	**destination preferred-msg-format** {**long-text** | **short-text** | **xml**} 例： `Router(cfg-call-home-profile)# destination preferred-msg-format xml`	（任意）使用するメッセージ形式を設定します。デフォルトは XML です。
ステップ 7	**destination message-size-limit** *bytes* 例： `Router(cfg-call-home-profile)# destination message-size-limit 3145728`	（任意）宛先プロファイルの宛先メッセージの最大サイズを設定します。
ステップ 8	**active** 例： `Router(cfg-call-home-profile)# active`	宛先プロファイルをイネーブルにします。デフォルトでは、プロファイルは作成時にイネーブルになります。
ステップ 9	**end** 例： `Router(cfg-call-home-profile)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show call-home profile** {*name* | **all**} 例： `Router# show call-home profile profile1`	指定されたプロファイル、または設定済みのすべてのプロファイルに関する宛先プロファイル設定を表示します。

宛先プロファイルのコピー

既存のプロファイルをコピーして新しい宛先プロファイルを作成するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **call-home**
3. **copy profile** *source-profile target-profile*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**copy profile** *source-profile target-profile* 例： `Router(cfg-call-home)# copy profile profile1 profile2`	既存の宛先プロファイルと同じ設定で新しい宛先プロファイルを作成します。

プロファイルの匿名モードの設定

匿名プロファイルを設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **call-home**
3. **profile** *name*
4. **anonymous-reporting-only**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**profile** *name* 例： `Router(cfg-call-home) profile Profile-1`	プロファイル コンフィギュレーション モードをイネーブルにします。
ステップ 4	**anonymous-reporting-only** 例：	プロファイルを匿名モードに設定します。

	コマンドまたはアクション	目的
	`Router(cfg-call-home-profile)# anonymous-reporting-only`	（注） デフォルトで、Call Home は、プロファイルに登録されているすべてのイベントタイプに関する完全なレポートを送信します。**anonymous-reporting-only** が設定されている場合は、クラッシュ、インベントリ、およびテストメッセージだけが送信されます。

アラート グループへの登録

アラート グループは、すべてのルータでサポートされている Call Home アラートをあらかじめ定義したサブセットです。Call Home アラートはタイプごとに別のアラート グループにグループ化されます。次のアラート グループが使用可能です。

- Crash
- 設定
- Environment
- Inventory
- Snapshot
- Syslog

ここでは、次の内容について説明します。

- 定期通知 （308 ページ）
- メッセージシビラティ（重大度）しきい値 （309 ページ）
- スナップショット コマンド リストの設定 （309 ページ）

各アラート グループの起動イベントを アラート グループの起動イベントとコマンド （337 ページ）に示します。アラート グループ メッセージの内容を メッセージの内容 （344 ページ）に示します。

宛先プロファイルごとに受信するアラート グループを 1 つまたは複数選択できます。

（注） Call Home アラートは、その Call Home アラートが含まれているアラート グループに登録されている宛先プロファイルにしか送信されません。さらに、アラート グループをイネーブルにする必要があります。

宛先プロファイルを 1 つまたは複数のアラート グループに加入させる場合、次の手順に従います。

手順の概要

1. **configure terminal**
2. **call-home**
3. **alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog** | **crash** | **snapshot**}
4. **profile** *name*
5. **subscribe-to-alert-group all**
6. **subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]
7. **subscribe-to-alert-group environment** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]
8. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]
9. **subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}]
10. **subscribe-to-alert-group crash**
11. **subscribe-to-alert-group snapshot periodic** {**daily** *hh:mm* | **hourly** *mm* | **interval** *mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}
12. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**alert-group** {**all** | **configuration** | **environment** | **inventory** | **syslog** | **crash** | **snapshot**} 例： `Router(cfg-call-home)# alert-group all`	指定されたアラート グループをイネーブルにします。すべてのアラート グループをイネーブル（有効）にするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。
ステップ 4	**profile** *name* 例： `Router(cfg-call-home)# profile profile1`	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定サブモードに入ります。
ステップ 5	**subscribe-to-alert-group all** 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group all`	最も低いシビラティ（重大度）を使用しているすべての使用可能なアラート グループに登録します。 ステップ 6 からステップ 11 で説明しているように、特定のタイプごとに個別にアラート グループに登録することもできます。

	コマンドまたはアクション	目的
		（注） このコマンドは、syslog のデバッグのデフォルトのシビラティ（重大度）に登録されます。これにより、大量の syslog メッセージが生成されます。可能な場合は、適切なシビラティ（重大度）およびパターンを使用してアラート グループに個別に登録してください。
ステップ 6	**subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic daily 12:00`	この宛先プロファイルを Configuration アラート グループに登録します。定期通知 （308 ページ） で説明しているように、定期的な通知用に Configuration アラート グループを設定できます。
ステップ 7	**subscribe-to-alert-group environment** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major`	この宛先プロファイルを Environment アラート グループに登録します。メッセージシビラティ（重大度）しきい値 （309 ページ） で説明しているように、シビラティ（重大度）に応じてメッセージをフィルタリングするために Environment アラート グループを設定できます。
ステップ 8	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic monthly 1 12:00`	この宛先プロファイルを Inventory アラート グループに登録します。定期通知 （308 ページ） で説明しているように、定期的な通知用に Inventory アラート グループを設定できます。
ステップ 9	**subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major`	この宛先プロファイルを Syslog アラート グループに登録します。メッセージシビラティ（重大度）しきい値 （309 ページ） で説明しているように、シビラティ（重大度）に応じてメッセージをフィルタリングするよう Syslog アラート グループを設定できます。 各 syslog メッセージ内で照合するテキスト パターンを指定できます。パターンを設定すると、指定されたパターンが含まれ、シビラティ（重大度）しきい値に一致する場合にだけ Syslog アラート グループ メッセージが送信されます。パターンにスペー

	コマンドまたはアクション	目的
		スが含まれる場合は、引用符（“”）でスペースを囲む必要があります。宛先プロファイルごとにパターンを 5 つまで指定できます。
ステップ 10	**subscribe-to-alert-group crash** 例： `Router(cfg-call-home-profile)# [no | default] subscribe-to-alert-group crash`	ユーザ プロファイルの Crash アラート グループに登録します。デフォルトで TAC プロファイルは Crash アラート グループに登録され、登録を解除できません。
ステップ 11	**subscribe-to-alert-group snapshot periodic** {**daily** *hh:mm* | **hourly** *mm* | **interval** *mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*} 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00`	この宛先プロファイルを Snapshot アラート グループに登録します。定期通知 （308 ページ）で説明しているように、定期的な通知用に Snapshot アラート グループを設定できます。 デフォルトでは、Snapshot アラート グループに実行するコマンドはありません。コマンドをアラート グループの中に追加できます（スナップショット コマンド リストの設定 （309 ページ）を参照）。こうすることで、Snapshot アラート グループに追加されたコマンドの出力がスナップショット メッセージに組み込まれます。
ステップ 12	**exit** 例： `Router(cfg-call-home-profile)# exit`	Call Home 宛先プロファイル設定サブモードを終了します。

定期通知

Configuration、Inventory、または Snapshot アラート グループに宛先プロファイルを登録するとき、アラート グループ メッセージを非同期的に受信するか、または指定の時間に定期的に受信するかを選択できます。送信期間は、次のいずれかにできます。

- 日次：24 時間表記の時間:分形式（*hh:mm*）で送信する時刻を指定します（例：14:30）。
- 週次：*day hh:mm* の形式で曜日と時刻を指定します。day は曜日を省略せずスペルアウトします（例：Monday）。
- 月次：*date hh:mm* の形式で 1 ～ 31 の日と時刻を指定します。
- 間隔：定期的なメッセージが送信される間隔を 1 ～ 60 分で指定します。
- 毎時：定期的なメッセージが送信される時刻（分）を 0 ～ 59 分で指定します。

（注） 毎時および間隔による定期通知は、Snapshot アラート グループでのみ使用可能です。

メッセージシビラティ（重大度）しきい値

宛先プロファイルを Environment、または Syslog アラート グループに登録するとき、メッセージシビラティ（重大度）に基づいてアラート グループ メッセージを送信するためのしきい値を設定できます。宛先プロファイルに指定したしきい値より低い値のメッセージは、宛先に送信されません。

シビラティ（重大度）しきい値の設定に使用されるキーワードを、次の表に示します。シビラティ（重大度）しきい値の範囲は、catastrophic（レベル 9、最高緊急度）から debugging（レベル 0、最低緊急度）です。Syslog または Environment アラート グループのシビラティ（重大度）しきい値が設定されていない場合、デフォルトは debugging （レベル 0）です。Configuration アラート グループおよび Inventory アラート グループではシビラティ（重大度）は設定できません。シビラティ（重大度）は常に normal に固定されます。

（注） Call Home のシビラティ（重大度）は、システム メッセージ ロギングのシビラティ（重大度）とは異なります。

表 *29* : シビラティ（重大度）と *syslog* レベルのマッピング

レベル	キーワード	Syslog レベル	説明
9	catastrophic	—	ネットワーク全体に壊滅的な障害が発生しています。
8	disaster	—	ネットワークに重大な影響が及びます。
7	fatal	緊急（0）	システムが使用不可能な状態。
6	critical	アラート（1）	クリティカルな状態、ただちに注意が必要。
5	major	重要（2）	重大な状態。
4	minor	エラー（3）	軽微な状態。
3	warning	警告（4）	警告状態。
2	notification	通知（5）	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	normal	情報（6）	標準状態に戻ることを示す標準イベントです。
0	debugging	デバッグ（7）	デバッグ メッセージ。

スナップショット コマンド リストの設定

スナップショット コマンド リストを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**

2. **call-home**
3. [**no** | **default**] **alert-group-config snapshot**
4. [**no** | **default**] **add-command** *command string*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	[**no** | **default**] **alert-group-config snapshot** 例： `Router(cfg-call-home)# alert-group-config snapshot`	スナップショット コンフィギュレーション モードを開始します。 **no** または **default** コマンドは、すべてのスナップショット コマンドを削除します。
ステップ 4	[**no** | **default**] **add-command** *command string* 例： `Router(cfg-call-home-snapshot)# add-command "show version"`	Snapshot アラート グループにコマンドを追加します。**no** または **default** コマンドは、対応するコマンドを削除します。 • *command string*：IOS コマンド。最大長は 128 文字です。
ステップ 5	**exit** 例： `Router(cfg-call-home-snapshot)# exit`	終了し、設定を保存します。

一般的な電子メール オプションの設定

E メール メッセージ転送を使用するには、少なくとも 1 つの Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）E メール サーバ アドレスを設定する必要があります。発信元と返信先 E メール アドレスを設定し、バックアップ E メール サーバを 4 つまで指定できます。

一般的な電子メール オプションの設定時には、次の点に注意してください。

- バックアップ E メール サーバは、異なるプライオリティ番号を使用して、**mail-server** コマンドを繰り返すと定義できます。
- **mail-server priority** number パラメータは 1 ～ 100 に設定可能です。プライオリティが最も高い（プライオリティ番号が最も低い）サーバを最初に試します。

一般的な E メール オプションを設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **call-home**
3. **mail-server** [{*ipv4-address* | *ipv6-address*} | *name*] **priority** *number*
4. **sender from** *email-address*
5. **sender reply-to** *email-address*
6. **source-interface** *interface-name*
7. **vrf** *vrf-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**mail-server** [{*ipv4-address* | *ipv6-address*} | *name*] **priority** *number* 例： `Router(cfg-call-home)# mail-server stmp.example.com priority 1`	E メール サーバ アドレスを割り当て、設定済みの E メール サーバ内の相対的なプライオリティを割り当てます。 次のいずれかの方法で指定します。 • 電子メール サーバの IP アドレス • 電子メール サーバの完全修飾ドメイン名（FQDN）（64 文字まで）。 1（最高のプライオリティ）から 100（最低のプライオリティ）のプライオリティ番号を割り当てます。
ステップ 4	**sender from** *email-address* 例： `Router(cfg-call-home)# sender from username@example.com`	（任意）Call Home 電子メール メッセージの [from] フィールドに表示される電子メール アドレスを割り当てます。アドレスが指定されていない場合は、連絡用の E メール アドレスが使用されます。
ステップ 5	**sender reply-to** *email-address* 例： `Router(cfg-call-home)# sender reply-to username@example.com`	（任意）Call Home 電子メール メッセージの [reply-to] フィールドに表示される電子メール アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 6	**source-interface** *interface-name* 例： `Router(cfg-call-home)# source-interface loopback1`	Call-Home メッセージを送信するための発信元インターフェイス名を割り当てます。 • *interface-name*：発信元インターフェイス名。最大長は 64 文字です。 （注） HTTP メッセージの場合、発信元インターフェイス名を設定するには、グローバル コンフィギュレーション モードで **ip http client source-interface** *interface-name* コマンドを使用します。これにより、デバイスのすべての HTTP クライアントが同じ発信元インターフェイスを使用できるようになります。
ステップ 7	**vrf** *vrf-name* 例： `Router(cfg-call-home)# vrf vpn1`	（任意）Call-Home 電子メール メッセージを送信するため VRF インスタンスを指定します。VRF を指定しないと、グローバル ルーティング テーブルが使用されます。 （注） HTTP メッセージでは、発信元インターフェイスが VRF に関連付けられている場合、グローバルコンフィギュレーション モードで **ip http client source-interface** *interface-name* コマンドを使用して、デバイスのすべての HTTP クライアントで使われる VRF インスタンスを指定します。

例

次に、プライマリ E メール サーバおよびセカンダリ E メール サーバなど、一般的な E メール パラメータの設定例を示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# call-home
Router(cfg-call-home)# mail-server smtp.example.com priority 1
Router(cfg-call-home)# mail-server 192.168.0.1 priority 2
Router(cfg-call-home)# sender from username@example.com
Router(cfg-call-home)# sender reply-to username@example.com
Router(cfg-call-home)# source-interface loopback1
Router(cfg-call-home)# vrf vpn1
Router(cfg-call-home)# exit
Router(config)#
```

Call Home メッセージ送信のレート制限の指定

Call Home メッセージ送信のレート制限を指定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **call-home**
3. **rate-limit** *number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**rate-limit** *number* 例： `Router(cfg-call-home)# rate-limit 40`	1 分間に送信するメッセージ数の制限を指定します。 • *number*：範囲は 1 ～ 60 です。デフォルトは 20 です。

HTTP プロキシ サーバの指定

宛先に Call Home HTTP（S）メッセージを送信するために HTTP プロキシ サーバを指定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **call-home**
3. **http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**http-proxy** {*ipv4-address* | *ipv6-address* | *name*} **port** *port-number* 例： `Router(cfg-call-home)# http-proxy 192.0.2.1 port 1`	HTTP 要求のプロキシ サーバを指定します。

Call Home メッセージの IOS コマンドを実行するための AAA 認証の有効化

宛先に Call Home HTTP（S）メッセージを送信するために HTTP プロキシ サーバを指定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **call-home**
3. **aaa-authorization**
4. **aaa-authorization** [**username** *username*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**aaa-authorization** 例： `Router(cfg-call-home)# aaa-authorization`	AAA 認証をイネーブルにします。 （注） デフォルトでは、AAA 認証は Call Home でディセーブルです。
ステップ 4	**aaa-authorization** [**username** *username*] 例： `Router(cfg-call-home)# aaa-authorization username user`	許可のためのユーザ名を指定します。 • **username** ユーザー名：デフォルトのユーザー名は callhome です。最大長は 64 文字です。

syslog スロットリングの設定

宛先に Call Home HTTP（S）メッセージを送信するために HTTP プロキシ サーバを指定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **call-home**
3. [**no**] **syslog-throttling**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	[**no**] **syslog-throttling** 例： `Router(cfg-call-home)# syslog-throttling`	Call Home syslog メッセージのスロットリングをイネーブルまたはディセーブルにし、Call Home syslog メッセージが繰り返し送信されないようにします。 （注） デフォルトでは、syslog メッセージ スロットリングはイネーブルです。

Call Home データ プライバシーの設定

data-privacy コマンドは、顧客のプライバシーを保護するために、IP アドレスなどのデータのスクラビング処理を行います。data-privacy コマンドをイネーブルにすると、大量のデータのスクラビング処理を行ったときに CPU 使用率に影響を及ぼすことがあります。現在、**show running-config all** および **show startup-config data** コマンド出力の中の設定メッセージを除いて、**show** コマンドの出力はスクラビング処理されません。

手順の概要

1. **configure terminal**
2. **call-home**
3. **data-privacy** {**level** {**normal** | **high**} | **hostname**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# 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	**call-home** 例： `Router(config)# call-home`	Call Home 設定サブモードに入ります。
ステップ 3	**data-privacy** {**level** {**normal** | **high**} | **hostname**} 例： `Router(cfg-call-home)# data-privacy level high`	ユーザのプライバシーを保護するために、実行コンフィギュレーション ファイルのデータをスクラビング処理します。デフォルトの data-privacy レベルは normal です。 （注） data-privacy コマンドをイネーブルにすると、大量のデータのスクラビング処理を行ったときに CPU 使用率に影響を及ぼすことがあります。 • **normal**：すべての標準レベル コマンドをスクラビング処理します。 • **high**：標準レベル コマンドに加えて、IP ドメイン名と IP アドレスのコマンドのスクラビング処理を行います。 • **hostname**：高レベル コマンドに加えて hostname コマンドのスクラビング処理を行います。 （注） 一部のプラットフォームでは、設定メッセージのホスト名をスクラビング処理すると、Smart Call Home 処理が失敗することがあります。

Call Home 通信の手動送信

数種類の Call Home 通信を手動で送信できます。Call Home 通信を送信するには、この項の作業を実行します。ここでは、次の内容について説明します。

• 1 つのコマンドまたはコマンド リスト用のコマンド出力メッセージの手動送信 （320 ページ）

Call Home テスト メッセージの手動送信

call-home test コマンドを使用して、ユーザー定義の Call Home テストメッセージを送信できます。

Call Home テスト メッセージを手動で送信するには、次の手順に従います。

手順の概要

1. **call-home test** [*“test-message”*] **profile** *name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**call-home test** [*“test-message”*] **profile** *name* 例： `Router# call-home test profile profile1`	指定された宛先プロファイルにテストメッセージを送信します。ユーザ定義のテストメッセージのテキストは任意指定ですが、スペースが含まれる場合には、引用符（“”）で囲む必要があります。ユーザ定義のメッセージが設定されていない場合、デフォルト メッセージが送信されます。

Call Home アラート グループ メッセージの手動送信

call-home send コマンドを使用して、特定のアラートグループメッセージを手動で送信できます。

Call Home アラート グループメッセージを手動で送信する場合は、次の注意事項に従ってください。

- 手動で送信できるのは、Crash、Snapshot、Configuration、および Inventory アラート グループだけです。
- Crash、Snapshot、Configuration、または Inventory アラート グループ メッセージを手動でトリガーする場合、宛先プロファイル名を指定すると、プロファイルのアクティブ ステータス、加入ステータス、またはシビラティ（重大度）設定に関係なく、宛先プロファイルにメッセージが送信されます。
- Crash、Snapshot、Configuration、または Inventory アラート グループ メッセージを手動でトリガーするとき、宛先プロファイル名を指定しないと、normal または指定されたアラート グループへの定期的な登録に指定されたアクティブなプロファイルすべてにメッセージが送信されます。

Call Home アラート グループ メッセージを手動でトリガーするには、次の手順に従います。

手順の概要

1. **call-home send alert-group snapshot** [**profile** *name*]
2. **call-home send alert-group crash** [**profile** *name*]
3. **call-home send alert-group configuration** [**profile** *name*]
4. **call-home send alert-group inventory** [**profile** *name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**call-home send alert-group snapshot** [**profile** *name*] 例： `Router# call-home send alert-group snapshot profile profile1`	1 つの宛先プロファイル（指定されている場合）または登録されているすべての宛先プロファイルに Snapshot アラート グループ メッセージを送信します。
ステップ 2	**call-home send alert-group crash** [**profile** *name*] 例： `Router# call-home send alert-group crash profile profile1`	1 つの宛先プロファイル（指定されている場合）または登録されているすべての宛先プロファイルに Crash アラート グループ メッセージを送信します。
ステップ 3	**call-home send alert-group configuration** [**profile** *name*] 例： `Router# call-home send alert-group configuration profile profile1`	宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Configuration アラート グループ メッセージを送信します。
ステップ 4	**call-home send alert-group inventory** [**profile** *name*] 例： `Router# call-home send alert-group inventory profile profile1`	宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Inventory アラート グループ メッセージを送信します。

Call Home 分析およびレポート要求の送信

call-home request コマンドを使用すると、システムに関する情報を Cisco に送信して、システム固有の便利な分析/およびレポート情報を受け取ることができます。セキュリティの警告、既知のバグ、ベスト プラクティス、コマンド リファレンスなど、さまざまなレポートを要求できます。

Call Home 分析およびレポート要求を手動で送信する場合、次の注意事項に従ってください。

- **profile** *name* を指定すると、要求はプロファイルに送信されます。プロファイルが指定されていない場合、要求は Cisco TAC プロファイルに送信されます。Call Home 要求の受信者プロファイルをイネーブルにする必要はありません。要求メッセージを Cisco TAC に転送し、Smart Call Home サービスから返信を受信できるように、Transport Gateway が設定された電子メール アドレスをプロファイルに指定します。

- **ccoid** *user-id* は、Smart Call Home ユーザの登録済み ID です。*user-id* を指定すると、応答は登録ユーザの E メール アドレスに送信されます。*user-id* を指定しなければ、応答はデバイスの連絡先電子メール アドレスに送信されます。
- 要求するレポートのタイプを指定するキーワードに基づいて、次の情報が返されます。
  - **config-sanity**：現在の実行コンフィギュレーションに関連するベスト プラクティス情報。
  - **bugs-list**：実行バージョンおよび現在適用されている機能に関する既知のバグ。
  - **command-reference**：実行コンフィギュレーションのすべてのコマンドに対する参照リンク。
  - **product-advisory**：ネットワーク内のデバイスに影響する可能性のある Product Security Incident Response Team（PSIRT）通知、サポート終了（EOL）または販売終了（EOS）通知、あるいは Field Notice（FN）。

Cisco Output Interpreter ツールから分析およびレポート情報の要求を送信するには、次の手順に従います。

手順の概要

1. **call-home request output-analysis** *"show-command"* [**profile** *name*] [**ccoid** *user-id*]
2. **call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**call-home request output-analysis** *"show-command"* [**profile** *name*] [**ccoid** *user-id*] 例： `Router# call-home request output-analysis "show diag" profile TG`	指定した show コマンドの出力を分析用に送信します。show コマンドは、引用符（""）で囲む必要があります。
ステップ 2	**call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*] 例： `Router# call-home request config-sanity profile TG`	分析のために、**show running-config all**、**show version** または **show module** コマンドなどの所定のコマンドセットの出力を送信します。また、**call home request product-advisory** サブコマンドには、すべてのインベントリ アラート グループ コマンドが含まれます。**request** の後に指定されたキーワードにより、必要なレポートのタイプが指定されます。

例

次に、ユーザ指定の **show** コマンドの分析要求の例を示します。

```
Router# call-home request output-analysis "show diag" profile TG
```

1 つのコマンドまたはコマンド リスト用のコマンド出力メッセージの手動送信

call-home send コマンドを使用して、1 つの IOS コマンドまたは IOS コマンドのリストを実行し、コマンド出力を HTTP または電子メールプロトコルを介して送信できます。

コマンド出力を送信する場合は、次の注意事項に従ってください。

- IOS コマンドまたは IOS コマンド リストとして、すべてのモジュール用のコマンドを含めて、任意の実行コマンドを指定できます。コマンドは、引用符（“”）で囲む必要があります。
- 「email」キーワードを使って電子メール オプションを選択し、電子メール アドレスを指定すると、コマンド出力はそのアドレスに送信されます。電子メール オプションも HTTP オプションも指定しない場合、出力は指定のサービス要求番号と共にロング テキスト形式で Sisco TAC （attach@cisco.com）に送信されます。
- 「email」キーワードも「http」キーワードも指定しない場合、ロング テキスト形式と XML メッセージ形式の両方でサービス要求番号が必要とされ、電子メールの件名行にサービス要求番号が示されます。
- HTTP オプションを指定している場合、CiscoTac-1 プロファイルの宛先 HTTP または HTTPS URL が宛先として使用されます。Smart Call Home から電子メール アドレスにメッセージを転送するよう、宛先の電子メールアドレスを指定できます。ユーザは、宛先の電子メール アドレスまたは SR 番号のいずれかを指定する必要があります（両方を指定することもできます）。

コマンドを実行し、コマンド出力を送信するには、次の手順を実行します。

手順の概要

1. **call-home send** {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**call-home send** {*cli command* | *cli list*} [**email** *email* **msg-format** {**long-text** | **xml**} | **http** {**destination-email-address** *email*}] [**tac-service-request** *SR#*] 例： `Router# call-home send “show version;show running-config;show inventory” email support@example.com msg-format xml`	CLI または CLI リストを実行し、電子メールまたは HTTP 経由で出力を送信します。 • {*cli command* | *cli list*}：1 つの IOS コマンドまたは（「,」で区切った）IOS コマンドリストを指定します。すべてのモジュールに対するコマンドを含む、あらゆる run コマンドを指定できます。これらのコマンドは引用符（“”）で囲む必要があります。

	コマンドまたはアクション	目的
		• **email** *email* **msg-format {long-text | xml}**：この **email** オプションが選択されている場合、指定の電子メールアドレスに向けてロングテキスト形式または XML 形式でコマンド出力が送信され、サービス要求番号がその件名に含められます。電子メールアドレス、サービス要求番号、またはその両方を指定する必要があります。電子メールアドレスが指定されない場合は、サービス リクエスト番号が必要です（デフォルトでは、ロング テキスト形式の場合は attach@cisco.com、XML 形式の場合は callhome@cisco.com）。 • **http** {**destination-email-address** *email*}：この **http** オプションが選択されている場合、コマンド出力は XML 形式で Smart Call Home バックエンド サーバー（TAC プロファイルで指定された URL）に送信されます。 **destination-email-address** *email* を指定して、バックエンドサーバーから電子メールアドレスにメッセージを転送できるようにすることが可能です。電子メール アドレス、サービス要求番号、またはその両方を指定する必要があります。 • **tac-service-request** *SR#*：サービス要求番号を指定します。電子メールアドレスが指定されない場合は、サービス リクエスト番号が必要です。

例

次に、コマンドの出力をユーザ指定の電子メール アドレスに送信する例を示します。

```
Router# call-home send "show diag" email support@example.com
```

次に、SR 番号が指定され、ロング テキスト形式で attach@cisco.com に送信されるコマンド出力の例を示します。

```
Router# call-home send "show version; show run" tac-service-request 123456
```

次に、XML メッセージ形式で callhome@cisco.com に送信されるコマンド出力の例を示します。

```
Router# call-home send "show version; show run" email callhome@cisco.com msg-format xml
```

次に、SR 番号が指定され、XML メッセージ形式で Cisco TAC バックエンド サーバへ送信されたコマンド出力の例を示します。

```
Router# call-home send “show version; show run” http tac-service-request 123456
```

次に、Cisco TAC バックエンド サーバに HTTP プロトコルを使用して送信され、ユーザが指定した電子メール アドレスに転送されたコマンド出力の例を示します。

```
Router# call-home send “show version; show run” http destination-email-address
user@company.com
```

診断シグニチャの設定

診断シグニチャ機能は、デジタル署名されたシグニチャをデバイスにダウンロードします。診断シグニチャ（DS）ファイルは、診断イベントの情報を含んでいるフォーマット済みファイルです。これにより、シスコ ソフトウェアをアップグレードすることなくトラブルシューティングを実行できます。DS の目的は、お客様のネットワークで発生している既知の問題を解決するために使用可能なトラブルシューティング情報を検出/収集できる、柔軟性の高いインテリジェンスを提供することです。

診断シグニチャについて

診断シグニチャの概要

Call Home システムの診断シグニチャ（DS）に備わっている柔軟なフレームワークにより、新しいイベントおよび対応する CLI を定義できます。これらの CLI を使用すると、シスコ ソフトウェアをアップグレードせずにこれらのイベントを分析できます。

DS により、標準の Call Home 機能でサポートされていないイベント タイプとトリガー タイプを追加的に定義できます。DS サブシステムは、ファイルをデバイスにダウンロードして処理し、診断シグニチャ イベントのコールバックを処理します。

診断シグニチャ機能は、ファイルの形式のデジタル署名シグニチャをデバイスにダウンロードします。DS ファイルは、診断イベントの情報を照合し、これらのイベントのトラブルシューティング手段を提供する、フォーマット済みファイルです。

DS ファイルには、イベントの説明を指定する XML データと、必要なアクションを実行する CLI コマンドまたはスクリプトが含まれています。これらのファイルは、整合性、信頼性、セキュリティを証明するために、シスコまたはサード パーティによりデジタル署名されています。

DS ファイルの構造は、次のいずれかです。

- イベント タイプを指定する、メタデータに基づく単純な署名。また、イベントの照合やアクションの実行（たとえばCLIを使用した情報の収集）に使用できるその他の情報もこれに含まれます。さらに、この署名は、特定のバグに対する回避策としてデバイスの設定を変更することもできます。
- 組み込みイベント マネージャ（EEM）Tool Command Language（Tcl）スクリプトに基づく署名。これはイベント レジスタ行で新しいイベントを指定し、Tcl スクリプトで追加のアクションを指定します。
- 上記の両方の形式の組み合わせ。

DS ファイルには次の基本情報が含まれています。

- **ID（一意の番号）**：DS の検索に使用できる DS ファイルを表す一意のキー。
- **名前（ShortDescription）**：選択用リストで使用できる、DS ファイルに関する一意の記述。
- **説明**：署名に関する詳細な記述。
- **リビジョン**：バージョン番号。DS の内容が更新されると大きくなります。
- **イベントおよびアクション**：検出対象のイベントと、イベントの発生後に実行すべきアクションを定義します。

診断シグニチャの前提条件

デバイスに診断シグニチャ（DS）をダウンロードして設定する前に、次の条件を満たしていることを確認します。

- デバイスに 1 つ以上の DS を割り当てる必要があります。デバイスへの DS の割り当ての詳細については、診断シグニチャのダウンロード （324 ページ）を参照してください。
- DS ファイルをダウンロードするためにはHTTP/Secure HTTP（HTTPS）トランスポートが必要です。宛先 HTTPS サーバの認証をイネーブルにするには、認証局（CA）証明書をインストールする必要があります。

（注） トラストプール機能を設定する場合は、CA 証明書は不要です。

診断シグニチャのダウンロード

診断シグニチャ（DS）ファイルをダウンロードするには、セキュアHTTP（HTTPS）プロトコルが必要です。デバイスにファイルをダウンロードする方式として電子メール転送方式をすでに設定している場合、DS をダウンロードして使用するには、割り当て済みプロファイル転送方式を HTTPS に変更する必要があります。

Cisco ソフトウェアは既知の証明機関（CA）からの証明書プールをプロビジョニング、保存、および管理する方式を作成するためにPKIトラストプール管理機能を使用します。デバイスではこの機能がデフォルトでイネーブルに設定されています。トラストプール機能により、CA 証明書が自動的にインストールされます。CA 証明書は、宛先 HTTPS サーバの認証に必要です。

DS ファイルをダウンロードするための DS 更新要求には、標準ダウンロードと強制ダウンロードの 2 種類があります。標準ダウンロードは、最近更新された DS ファイルを要求します。標準ダウンロード要求をトリガーするには、定期的な設定を使用するか、またはオンデマンドで CLI を開始します。標準ダウンロード更新は、要求された DS バージョンがデバイス上の DS バージョンと異なる場合にのみ実行されます。定期的なダウンロードは、DS Web ポータルからデバイスにすでに割り当てられた DS が存在する場合にのみ開始されます。割り当てが行われた後、同じデバイスからの定期インベントリ メッセージへの応答の中に、定期的な DS のダウンロードおよび更新を開始するようデバイスに通知するフィールドが含まれます。DS 更新要求メッセージには、DS のステータスとリビジョン番号が含まれます。これにより、最新リビジョン番号の DS だけがダウンロードされます。

強制ダウンロードでは、特定の 1 つの DS または一連の DS がダウンロードされます。強制ダウンロード更新要求をトリガーする唯一の方法は、オンデマンドで CLI を開始することです。強制ダウンロード更新要求では、デバイス上の現在の DS ファイルのバージョンに関係なく、最新バージョンの DS ファイルがダウンロードされます。

DS ファイルにはデジタル署名が付いています。ダウンロードされるすべての DS ファイルに対して署名の検証が実行され、ファイルが信頼できるソースからのものであることが確認されます。

診断シグニチャのワークフロー

Cisco ソフトウェアでは診断シグニチャ（DS）機能がデフォルトでイネーブルに設定されています。診断シグニチャを使用する際のワークフローを次に示します。

- ダウンロードする DS を見つけて、それらをデバイスに割り当てます。このステップは、標準の定期ダウンロードでは必須ですが、強制ダウンロードでは必要ではありません。
- デバイスは、標準の定期ダウンロードまたはオンデマンドの強制ダウンロードで、割り当てられているすべての DS または特定の 1 つの DS をダウンロードします。
- デバイスはすべての DS のデジタル署名を検証します。検証に合格すると、デバイスはブートフラッシュやハードディスクなどの固定型ディスクに DS ファイルを保存します。これにより、デバイスのリロード後に DS ファイルを読み取ることができます。ルータでは、DS ファイルが bootflash:/call home ディレクトリに保存されます。

- デバイスは DS の最新リビジョンを取得してデバイス内の古いリビジョンを置き換えるために、標準の定期 DS ダウンロード要求を送信し続けます。
- デバイスはイベントを監視し、イベントが発生すると、DS ファイルに定義されているアクションを実行します。

診断シグニチャのイベントとアクション

イベントセクションとアクションセクションは、診断シグニチャで使用される主な領域です。イベントセクションでは、イベント検出に使用されるすべてのイベントの属性を定義します。アクションセクションでは、イベント発生後に実行する必要があるすべてのアクション（たとえば show コマンド出力を収集して解析のために Smart Call Home に送信）がリストされます。

診断シグニチャのイベント検出

診断シグニチャ（DS）のイベント検出の方法として、単一イベント検出と複数イベント検出の 2 つが定義されています。

単一イベント検出

単一イベント検出では、DS 内で 1 つのイベント ディテクタだけが定義されます。イベントの指定形式は、次の 2 種類のいずれかです。

- DS イベント指定タイプ：サポートされているイベント タイプは、syslog、定期、設定、即時活性挿抜（OIR）、および Call Home です。「即時」とは、このタイプの DS はイベントを検出せず、ダウンロードされると直ちにそのアクションが実行されることを示しています。Call-Home タイプは、既存のアラート グループに関して定義されている現在の CLI コマンドを変更します。
- 組み込みイベント マネージャ（EEM）指定タイプ：Cisco ソフトウェアを変更することなく、すべての新しい EEM イベント ディテクタをサポートします。

  EEM を使用したイベント検出以外では、Tool Command Language（Tcl）スクリプトを使ってイベント検出タイプが指定されると、DS がトリガーされます。

複数イベント検出

複数イベント検出では、複数のイベントディテクタ、対応する複数の追跡対象オブジェクト状態、およびイベント発生期間を定義します。複数イベント検出の指定形式には、追跡対象イベントディテクタに関する複合イベント相関を含めることができます。たとえば、3 つのイベント ディテクタ（syslog、OIR、IPSLA）が、DS ファイルの作成時に定義されます。これらのイベント ディテクタに関して指定される相関は、syslog イベントおよび OIR イベントが同時にトリガーされるか、または IPSLA が単独でトリガーされる場合に、DS がアクションを実行することを示します。

診断シグニチャのアクション

診断シグニチャ（DS）ファイルは、イベントの発生時に開始すべきさまざまなアクションで構成されます。アクションタイプは、特定のイベントに対応して開始されるアクションの種類を示します。

変数は、ファイルをカスタマイズするために使用される DS 内の要素です。

DS アクションは、次の 4 つのタイプに分類されます。

- call-home
- command
- emailto
- script

DS アクション タイプ call-home および emailto はイベント データを収集し、Call-Home サーバまたは定義済み電子メール アドレスにメッセージを送信します。このメッセージでは、メッセージ タイプとして「diagnostic-signature」、メッセージ サブタイプとして DS ID が使用されます。

DS アクション タイプに関して定義されているコマンドは、デバイスの設定の変更、show コマンド出力の収集、またはデバイスでの任意の EXEC コマンドの実行を行う CLI コマンドを開始します。DS アクション タイプ script は、Tcl スクリプトを実行します。

診断シグニチャの変数

変数は診断シグニチャ（DS）内で参照され、DS ファイルをカスタマイズするために使用されます。DS 変数を他の変数と区別するために、すべての DS 変数名にはプレフィックス ds_ が付いています。サポートされる DS 変数のタイプを以下に示します。

- システム変数：設定を変更することなく、デバイスにより自動的に割り当てられる変数。診断シグニチャ機能では、ds_hostname および ds_signature_id の 2 つのシステム変数がサポートされています。
- 環境変数：call-home diagnostic-signature コンフィギュレーション モードで **environment** *variable-name variable-value* コマンドを使って手動で割り当てられる値。すべての DS 環境変数の名前と値を表示するには、**show call-home diagnostic-signature** コマンドを使用します。未解決の環境変数が DS ファイルに含まれている場合、変数が解決されるまで、この DS は保留状態のままになります。
- プロンプト変数：特権 EXEC モードで **call-home diagnostic-signature install** *ds-id* コマンドを使って手動で割り当てられる値。この値を設定しない場合、DS のステータスは保留中になります。
- 正規表現変数：事前定義された CLI コマンド出力との、正規表現を使用したパターンマッチによって割り当てられる値。この値は DS の実行中に割り当てられます。
- syslog イベント変数：DS ファイルでの syslog イベント検出中に割り当てられる値。この変数は、syslog イベント検出に関してのみ有効です。

診断シグニチャの設定方法

診断シグニチャの Call Home サービスの設定

診断シグニチャ（DS）に関連する通知の送信先である連絡先の電子メール アドレスや、DS ファイルのダウンロード元である HTTP/secure HTTP（HTTPS） URL などの属性を設定するために、Call Home サービス機能を設定します。

また、新しいユーザ プロファイルを作成し、正しい属性を設定し、そのプロファイルを DS プロファイルとして割り当てることもできます。定期的なダウンロードの場合、フルインベントリ メッセージの直後に要求が送信されます。インベントリの定期設定を変更すると、DS の定期ダウンロードも再スケジュールされます。

（注） デフォルトでは、事前定義された Cisco TAC-1 プロファイルが DS プロファイルとしてイネーブルに設定されます。これを使用することをお勧めします。これを使用する場合、必要となる設定は、宛先転送方式の設定を **http** に変更することだけです。

手順の概要

1. **configure terminal**
2. **service call-home**
3. **call-home**
4. **contact-email-addr** *email-address*
5. **mail-server** {*ipv4-addr* | *name*} **priority** *number*
6. **profile** *profile-name*
7. **destination transport-method** {**email** | **http**}
8. **destination address** {**email** *address* | **http** *url*}
9. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**service call-home** 例：	デバイスで Call Home サービスをイネーブルにします。

	コマンドまたはアクション	目的
	`Router(config)# service call-home`	
ステップ 3	**call-home** 例： `Router(config)# call-home`	Call Home を設定するために、Call-Home 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	**contact-email-addr** *email-address* 例： `Router(cfg-call-home)# contact-email-addr userid@example.com`	（任意）Call Home の顧客連絡先に使用する電子メール アドレスを割り当てます。
ステップ 5	**mail-server** {*ipv4-addr* | *name*} **priority** *number* 例： `Router(cfg-call-home)# mail-server 10.1.1.1 priority 4`	（任意）Call Home の Simple Mail Transfer Protocol（SMTP）の電子メール サーバ アドレスを設定します。このコマンドは、いずれかの DS で定義されているアクションに電子メール送信が含まれる場合にのみ使用されます。
ステップ 6	**profile** *profile-name* 例： `Router(cfg-call-home)# profile user1`	Call Home の宛先プロファイルを設定し、Call Home プロファイル コンフィギュレーション モードを開始します。
ステップ 7	**destination transport-method** {**email** | **http**} 例： `Router(cfg-call-home-profile)# destination transport-method http`	Call Home の宛先プロファイルの転送方式を指定します。 （注） 診断シグニチャを設定するには、**http** オプションを使用する必要があります。
ステップ 8	**destination address** {**email** *address* | **http** *url*} 例： `Router(cfg-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`	Call Home メッセージ送信先のアドレス タイプとロケーションを設定します。 （注） 診断シグニチャを設定するには、**http** オプションを使用する必要があります。
ステップ 9	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30`	Call Home の Inventory アラート グループに関するメッセージを送信するよう、宛先プロファイルを設定します。 • このコマンドは、DS ファイルの定期的ダウンロード用にのみ使用されます。
ステップ 10	**exit** 例： `Router(cfg-call-home-profile)# exit`	Call Home プロファイル コンフィギュレーション モードを終了して、Call Home コンフィギュレーション モードに戻ります。

次のタスク

前述の手順で設定したプロファイルを DS プロファイルとして設定し、その他の DS パラメータを設定します。

診断シグニチャの設定

始める前に

Call Home 機能を設定して、Call Home プロファイルの属性を設定します。デフォルトの Cisco TAC-1 プロファイルを使用するか、新しく作成したユーザ プロファイルを使用できます。

手順の概要

1. **call-home**
2. **diagnostic-signature**
3. **profile** *ds-profile-name*
4. **environment** *ds_env-var-name ds-env-var-value*
5. **end**
6. **call-home diagnostic-signature** [{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*]
7. **show call-home diagnostic-signature** [*ds-id* {**actions** | **events** | **prerequisite** | **prompt** | **variables** | **failure** | **statistics** | **download**}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**call-home** 例： `Router(config)# call-home`	Call Home を設定するために、Call-Home 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	**diagnostic-signature** 例： `Router(cfg-call-home)# diagnostic-signature`	Call Home 診断シグニチャ モードを開始します。
ステップ 3	**profile** *ds-profile-name* 例： `Router(cfg-call-home-diag-sign)# profile user1`	デバイス上で診断シグニチャ（DS）が使用する宛先プロファイルを指定します。
ステップ 4	**environment** *ds_env-var-name ds-env-var-value* 例： `Router(cfg-call-home-diag-sign)# environment ds_env1 envarval`	デバイスの DS の環境変数値を設定します。
ステップ 5	**end** 例： `Router(cfg-call-home-diag-sign)# end`	Call-Home 診断シグニチャ モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**call-home diagnostic-signature** [{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*] 例： `Router# call-home diagnostic-signature download 6030`	デバイスで診断シグニチャ ファイルをダウンロード、インストール、またはアンインストールします。
ステップ 7	**show call-home diagnostic-signature** [*ds-id* {**actions** | **events** | **prerequisite** | **prompt** | **variables** | **failure** | **statistics** | **download**}] 例： `Router# show call-home diagnostic-signature actions`	Call-Home 診断シグニチャ情報を表示します。

診断シグニチャの設定例

次に、診断シグニチャ（DS）ファイルの定期的なダウンロード要求をイネーブルにする例を示します。この設定では、毎日午後 2:30 にサービス Call-Home サーバに向けてダウンロード要求が送信され、DS ファイルのチェックをします。転送方法は HTTP に設定されます。

```
Router> enable
Router# configure terminal
Router(config)# service call-home
Router(config)# call-home
Router(cfg-call-home)# contact-email-addr userid@example.com
Router(cfg-call-home)# mail-server 10.1.1.1 priority 4
Router(cfg-call-home)# profile user-1
Router(cfg-call-home-profile)# destination transport-method http
Router(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
Router(cfg-call-home-profile)# exit
Router(cfg-call-home)# diagnostic-signature
Router(cfg-call-home-diag-sign)# profile user1
Router(cfg-call-home-diag-sign)# environment ds_env1 envarval
Router(cfg-call-home-diag-sign)# end
```

次に、前述の構成での **show call-home diagnostic-signature** コマンドの出力例を示します。

```
outer# show call-home diagnostic-signature

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: user1 (status: ACTIVE)
Environment variable:
ds_env1: abc
Downloaded DSes:
DS ID    DS Name                          Revision Status     Last Update (GMT+00:00)
-------- -------------------------------- -------- ---------- -------------------
6015     CronInterval                     1.0      registered 2013-01-16 04:49:52
6030     ActCH                            1.0      registered 2013-01-16 06:10:22
```

```
6032     MultiEvents                    1.0      registered 2013-01-16 06:10:37
6033     PureTCL                        1.0      registered 2013-01-16 06:11:48
```

Call Home 設定情報の表示

show call-home コマンドをさまざまな形式で使用して、Call Home 設定情報を表示できます。

設定済み Call Home 情報を表示するには、次の手順に従います。

手順の概要

1. **show call-home**
2. **show call-home detail**
3. **show call-home alert-group**
4. **show call-home mail-server status**
5. **show call-home profile** {**all** | *name*}
6. **show call-home statistics** [**detail** | **profile** *profile_name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show call-home** 例： `Router# show call-home`	Call Home 設定の概要を表示します。
ステップ 2	**show call-home detail** 例： `Router# show call-home detail`	Call Home 設定の詳細を表示します。
ステップ 3	**show call-home alert-group** 例： `Router# show call-home alert-group`	使用可能なアラート グループとそれらのステータスを表示します。
ステップ 4	**show call-home mail-server status** 例： `Router# show call-home mail-server status`	設定済みのE メール サーバのアベイラビリティをチェックして表示します。
ステップ 5	**show call-home profile** {**all** | *name*} 例： `Router# show call-home profile all`	指定された宛先プロファイルの設定を表示します。**all** キーワードを使用してすべての宛先プロファイルの設定を表示します。
ステップ 6	**show call-home statistics** [**detail** | **profile** *profile_name*] 例：	Call Home イベントの統計情報を表示します。

	コマンドまたはアクション	目的
	Router# show call-home statistics	

例

Call Home 情報の要約

Call Home 情報の詳細

使用可能な **Call Home** アラート グループ

E メール サーバのステータス情報

すべての宛先プロファイルの情報

ユーザ定義宛先プロファイルの情報

Call Home の統計情報

次に、**show call-home** コマンドの異なるオプションを使用した場合の出力例を示します。

```
Router# show call-home
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.0.2.2 Priority: 1
    Mail-server[2]: Address: 203.0.113.1 Priority: 2
    http proxy: 192.0.2.1:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show clock
```

```
Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: campus-noc
    Profile Name: CiscoTAC-1
Router#
```

```
Router# show call-home detail
Current call home settings:
    call home feature : enable
    call home message's from address: router@example.com
    call home message's reply-to address: support@example.com

    vrf for call-home messages: Not yet set up

    contact person's email address: technical@example.com

    contact person's phone number: +1-408-555-1234
    street address: 1234 Picaboo Street, Any city, Any state, 12345
    customer ID: ExampleCorp
    contract ID: X123456789
    site ID: SantaClara

    source ip address: Not yet set up
    source interface: GigabitEthernet0/0
    Mail-server[1]: Address: 192.0.2.2 Priority: 1
    Mail-server[2]: Address: 203.0.113.1 Priority: 2
    http proxy: 192.0.2.1:80

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show version
    Snapshot command[1]: show clock

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
```

```
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#
```

```
Router# show call-home alert-group
Available alert groups:
    Keyword                   State   Description
    ------------------------ ------- --------------------------------
    configuration             Enable  configuration info
    crash                     Enable  crash and traceback info
    environment               Enable  environmental info
    inventory                 Enable  inventory info
    snapshot                  Enable  snapshot info
    syslog                    Enable  syslog info
Router#
```

```
Router# show call-home mail-server status
Please wait. Checking for mail server status ...

    Mail-server[1]: Address: 192.0.2.2 Priority: 1 [Not Available]
    Mail-server[2]: Address: 203.0.113.1 Priority: 2 [Available]
Router#
```

```
Router# show call-home profile all

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up
```

```
    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Profile Name: CiscoTAC-1
    Profile status: INACTIVE
    Profile mode: Full Reporting
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 14 day of the month at 11:12

    Periodic inventory info message is scheduled every 14 day of the month at 10:57

    Alert-group               Severity
    ------------------------  ------------
    crash                     normal
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug
Router#
```

```
Router# show call-home profile campus-noc
Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     normal
    environment               debug
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
 .*CALL_LOOP.*             debug

Router#
```

```
Router# show call-home statistics
Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   3                    3                    0
    Config      3                    3                    0
    Crash       0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
```

```
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Total In-Queue  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Total Failed    0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Total Ratelimit
      -dropped  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0

Last call-home message sent time: 2011-09-26 23:26:50 GMT-08:00
Router#
```

Call Home のデフォルト設定

次の表に、Call Home のデフォルト設定を示します。

表 *30 : Call Home* のデフォルト設定

パラメータ	デフォルト
Call Home 機能のステータス	ディセーブル
ユーザ定義プロファイルのステータス	Active
定義済みのシスコ TAC プロファイルのステータス	Inactive

パラメータ	デフォルト
転送方法	電子メール
メッセージのフォーマット タイプ	XML
ロングテキスト、ショートテキスト、または XML 形式で送信されるメッセージの宛先メッセージのサイズ	3,145,728
アラート グループのステータス	イネーブル
Call Home メッセージのシビラティ（重大度）しきい値	Debug
1 分間に送信するメッセージのレート制限	20
AAA Authorization	ディセーブル
Call Home の syslog メッセージ スロットリング	イネーブル
データ プライバシー レベル	標準

アラート グループの起動イベントとコマンド

Call Home 起動イベントはアラート グループに分類され、各アラート グループには、イベント発生時に実行されるコマンドが割り当てられます。転送されるメッセージにはコマンド出力が含まれます。次の表では、各アラート グループに含まれる起動イベントを示します。アラート グループの各イベントのシビラティ（重大度）と、実行されるコマンドも示します。

表 *31 : Call Home* アラート グループ、イベント、および動作

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
Crash	SYSTEM_CRASH	–	–	ソフトウェア クラッシュに関連するイベント。 The following commands are executed: **show version** **show logging** **show region** **show inventory** **show stack** **crashinfo file**（このコマンドは crashinfo ファイルの内容を表示します）
–	TRACEBACK	–	–	ソフトウェアのトレース バック イベントを検出します。 The following commands are executed: **show version** **show logging** **show region** **show stack**

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
設定	–	–	–	設定または設定変更イベントに関するユーザ生成された要求。 The following commands are executed: **show platform** **show inventory** **show running-config all** **show startup-config** **show version**
環境	–	–	–	電源、ファン、温度アラームなどの環境センシング要素に関連するイベント。 The following commands are executed: **show environment** **show inventory** **show platform** **show logging**
–	–	SHUT	0	環境モニタがシャットダウンを開始しました。
–	–	ENVCRIT	2	温度または電圧測定値がクリティカルなしきい値を超えました。
–	–	BLOWER	3	必要な数のファントレイがない。

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
–	–	ENVWARN	4	温度または電圧測定値が警告しきい値を超えました。
–	–	RPSFAIL	4	電源に故障したチャネルがあります。
–	ENVM	PSCHANGE	6	電源名の変更
–	–	PSLEV	6	電源状態の変更
–	–	PSOK	6	電源が正常に動作しているようです。

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
Inventory	–	–	–	

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
				Inventory ステータスは、ユニットがコールド ブートされた場合や、FRU が挿入または取り外された場合に指定される。これは、重大ではないイベントと見なされ、情報はステータスと資格設定に使用される 匿名モードで送信されるすべてのインベントリ メッセージとフル登録モードで送信されるデルタ インベントリ メッセージに対して実行されるコマンド： **show diag all eeprom detail** **show version** **show inventory oid** **show platform** フル登録モードで送信されるフル インベントリ メッセージに対して実行されるコマンド： **show platform** **show diag all eeprom detail** **show version** **show inventory oid** **show bootflash: all** **show**

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
				data-corruption **show interfaces** **show file systems** **show memory statistics** **show process memory** **show process cpu** **show process cpu history** **show license udi** **show license detail** **show buffers**
–	HARDWARE_ REMOVAL	REMCARD	6	カードがスロット %d から取り外され、インターフェイスがディセーブルになった。
–	HARDWARE_ INSERTION	INSCARD	6	カードがスロット %d に挿入されました。管理上インターフェイスはシャットダウンします。
Syslog	–	–	–	syslog にログ記録されるイベント The following commands are executed: **show inventory** **show logging**
–	SYSLOG	LOG_EMERG	0	システムが使用不可能な状態。
–	SYSLOG	LOG_ALERT	1	即時対処が必要。
–	SYSLOG	LOG_CRIT	2	深刻な状況です。

アラート グループ	Call Home 起動イベント	Syslog イベント	シビラティ（重大度）	説明および実行されるコマンド
–	SYSLOG	LOG_ERR	3	エラー状態です。
–	SYSLOG	LOG_WARNING	4	警告状態。
–	SYSLOG	LOG_NOTICE	5	正常だが重大な状態。
–	SYSLOG	LOG_INFO	6	通知
–	SYSLOG	LOG_DEBUG	7	デバッグレベル メッセージ。
Test	–	TEST	–	ユーザが作成したテスト メッセージ The following commands are executed: **show platform** **show inventory** **show version**

（注） Cisco ISR 4321 は、**show inventory** コマンドにより、電源およびファントレイのシリアル番号が表示されません。

メッセージの内容

ここでは、アラート グループ メッセージの内容の形式を示すいくつかの表を示します。

このセクションには、サンプル メッセージを記載した次のサブセクションも含まれています。

- ロング テキスト形式での Syslog アラート通知の例 （350 ページ）
- XML 形式での syslog アラート通知の例 （351 ページ）

次の表に、ショート テキスト メッセージの内容フィールドを示します。

表 *32:* ショート テキスト メッセージの形式

データ項目	説明
デバイス ID	設定されたデバイス名

データ項目	説明
日時スタンプ	起動イベントのタイム スタンプ
エラー判別メッセージ	起動イベントの簡単な説明（英語）
アラームの緊急度	システム メッセージに適用されるようなエラー レベル

次の表に、すべてのロングテキストメッセージとXMLメッセージに共通する内容フィールドを示します。特定のアラート グループ メッセージに固有のフィールドは、共通フィールドの間に挿入されます。挿入ポイントは表に示しています。

表 *33 :* ロング テキスト メッセージと *XML* メッセージすべてに共通のフィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
Time stamp	ISO 時刻表記（*YYYY-MM-DD HH:MM:SS GMT+HH:MM*）によるイベントの日付とタイム スタンプ。	CallHome/EventTime
メッセージ名	メッセージの名前。具体的なイベント名のリストはアラート グループの起動イベントとコマンド（337ページ）に示されています。	ショート テキスト メッセージの場合のみ
メッセージ タイプ	「Call Home」を指定。	CallHome/Event/Type
Message subtype	特定のメッセージ タイプ：full、delta、test	CallHome/Event/SubType
メッセージ グループ	「reactive」を指定。デフォルトは「reactive」であるため、任意。	Long-text メッセージ専用
シビラティ（重大度）	メッセージのシビラティ（重大度）（メッセージシビラティ（重大度）しきい値（309ページ）を参照）。	Body/Block/Severity
送信元 ID	ワークフロー エンジンから経路指定する製品タイプ。一般に製品ファミリ名です。	Long-text メッセージ専用

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
デバイス ID	メッセージを生成するエンドデバイスの Unique Device Identifier（UDI）。メッセージがファブリック スイッチに固有でない場合、このフィールドは空白。形式は、*type@Sid@serial*。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：CISCO3845@C@12345678 （注） 次のプラットフォームの場合、UDI はプリント基板番号（PCB）であり、シャーシのシリアル番号（SN）ではありません。 • ISR 4221 • ISR 4321 • ISR 4331 • ISR 4351 • ISR 4431 • ISR 4451	CallHome/CustomerData/ContractData/DeviceId

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
カスタマー ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド	CallHome/CustomerData/ContractData/CustomerId
連絡先 ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド	CallHome/CustomerData/ContractData/CustomerId
サイト ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド	CallHome/CustomerData/ContractData/CustomerId
Server ID	メッセージがファブリック スイッチから生成されている場合、これはスイッチの固有のデバイス ID（UDI）。 • *type* は、バックプレーン IDPROM からの製品の型番。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：CISCO3845@C@12345678	ロング テキスト メッセージの場合のみ。
メッセージの説明	エラーを説明する短い文章。	CallHome/MessageDescription
デバイス名	イベントが発生するノード。これは、デバイスのホスト名です。	CallHome/CustomerData/SystemInfo/NameName
担当者名	イベント発生中のノードに関する問題の問い合わせ先の担当者名。	CallHome/CustomerData/SystemInfo/Contact

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
連絡先 E メール	このユニットの連絡先である人物の電子メール アドレス。	CallHome/CustomerData/SystemInfo/ContactEmail
連絡先電話番号	このユニットの連絡先である人物の電話番号	CallHome/CustomerData/SystemInfo/ContactPhoneNumber
住所	このユニットに関連したRMA部品の送付先住所を格納しているオプションのフィールド。	CallHome/CustomerData/SystemInfo/StreetAddress
モデル名	ルータのモデル名。これは製品ファミリ名の一部である固有モデルです。	CallHome/Device/Cisco_Chassis/Model
シリアル番号	ユニットのシャーシのシリアル番号	CallHome/Device/Cisco_Chassis/SerialNumber
シャーシの部品番号	シャーシの最上アセンブリ番号	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“PartNumber”
System object ID	システムを一意に識別するシステム オブジェクト ID。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“sysObjectID”
システム記述	管理対象デバイスのシステム説明。	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“sysDescr”

次の表に、特定のアラート グループ メッセージに固有の挿入フィールドを示します。

（注） このアラート グループに対して複数のコマンドが実行されると、次のフィールドが繰り返される場合があります。

表 *34*：特定のアラート グループ メッセージに固有の挿入フィールド

コマンド出力名	実行されたコマンドの正確な名前。	/aml/Attachments/Attachment/Name
添付タイプ	アタッチメントのタイプ。通常は “inline”。	/aml/Attachments/Attachment@type
MIME タイプ	通常は、"text"、"plain"、または符号化タイプのいずれか。	/aml/Attachments/Attachment/Data@encoding

コマンド出力テキスト	自動的に実行されたコマンドの出力（アラート グループの起動イベントとコマンド（337 ページ） を参照）。	/mml/attachments/attachment/atdata

次の表に、対処的メッセージ（TAC ケースを必要とするシステム障害）と予防的メッセージ（システム パフォーマンスの低下を引き起こす可能性のある問題）に挿入される内容フィールドを示します。

表 *35*：対処的または予防的イベント メッセージに挿入されるフィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン	CallHome/Device/Cisco_Chassis/HardwareVersion
スーパーバイザ モジュールのソフトウェア バージョン	最上位ソフトウェア バージョン	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“SoftwareVersion”
影響のある FRU の名前	イベント メッセージを生成している問題の FRU の名前	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
影響のある FRU のシリアル番号	問題を起こした FRU のシリアル番号	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
影響のある FRU の製品番号	問題を起こした FRU の部品番号	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU スロット	イベント メッセージを生成している FRU のスロット番号	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU ハードウェア バージョン	問題を起こした FRU のハードウェア バージョン	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU ソフトウェア バージョン	問題を起こした FRU で動作するソフトウェア バージョン	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString

次の表に、インベントリ メッセージに挿入される内容フィールドを示します。

表 *36*：コンポーネント イベント メッセージの挿入フィールド

データ項目（プレーン テキストおよび XML）	説明（プレーンテキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン	CallHome/Device/Cisco_Chassis/HardwareVersion
スーパーバイザ モジュールのソフトウェア バージョン	最上位ソフトウェアバージョン	CallHome/Device/Cisco_Chassis/AdditionalInformation/AD@name=“SoftwareVersion”

データ項目（プレーン テキストおよび XML）	説明（プレーンテキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
FRU name	イベントメッセージを生成している問題の FRU の名前	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
FRU s/n	FRU のシリアル番号	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
FRU 製品番号	FRU の製品番号	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU スロット	FRU のスロット番号	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU ハードウェア バージョン	FRU のハードウェア バージョン	CallHome/Device/Cisco_Chassis/CiscoCard/HardwareVersion
FRU ソフトウェア バージョン	FRU 上で動作しているソフトウェア バージョン	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString

ロング テキスト形式での Syslog アラート通知の例

次に、long-text 形式での Syslog アラート通知の例を示します。

```
TimeStamp : 2014-08-13 21:41 GMT+00:00
Message Name : syslog
Message Type : Call Home
Message Group : reactive
Severity Level : 2
Source ID : ISR 4400
Device ID : ISR4451-X/K9@C@FTX1830AKF9
Customer ID :
Contract ID :
Site ID :
Server ID : ISR4451-X/K9@C@FTX1830AKF9
Event Description : *Aug 13 21:41:35.835: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console
System Name : Router
Contact Email : admin@yourdomain.com
Contact Phone :
Street Address :
Affected Chassis : ISR4451-X/K9
Affected Chassis Serial Number : FTX1830AKF9
Affected Chassis Part No : 800-36894-03
Affected Chassis Hardware Version : 1.0
Supervisor Software Version : 15.4(20140812:034256)
Command Output Name : show logging
Attachment Type : command output
MIME Type : text/plain
Command Output Text : show logging
Syslog logging: enabled (0 messages dropped, 4 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.
```

```
No Inactive Message Discriminator.


    Console logging: level debugging, 71 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 73 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 70 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (4096 bytes):

*Aug 13 21:38:04.994: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
*Aug 13 21:40:55.706: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
*Aug 13 21:41:27.042: %SYS-5-CONFIG_I: Configured from console by console
Router#
Command Output Name : show inventory
Attachment Type : command output
MIME Type : text/plain
Command Output Text : show inventory
NAME: "Chassis", DESCR: "Cisco ISR4451 Chassis"
PID: ISR4451-X/K9      , VID: V03, SN: FTX1830AKF9

NAME: "Power Supply Module 0", DESCR: "450W AC Power Supply for Cisco ISR4450, ISR4350"
PID: PWR-4450-AC       , VID: V01, SN: DCA1822X0G4

NAME: "Fan Tray", DESCR: "Cisco ISR4450, ISR4350 Fan Assembly"
PID: ACS-4450-FANASSY  , VID:    , SN:

NAME: "module 0", DESCR: "Cisco ISR4451 Built-In NIM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
PID: ISR4451-X-4x1GE   , VID: V01, SN: JAB092709EL

NAME: "module 1", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "module 2", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "module R0", DESCR: "Cisco ISR4451 Route Processor"
PID: ISR4451-X/K9      , VID: V03, SN: FOC18271QLX

NAME: "module F0", DESCR: "Cisco ISR4451 Forwarding Processor"
PID: ISR4451-X/K9      , VID:    , SN:


Router#
```

XML 形式での syslog アラート通知の例

次に、XML 形式での Syslog アラート通知の例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M4:FTX1830AKF9:53EBDBDA</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block:Type>
<aml-block:CreationDate>2014-08-13 21:42:50 GMT+00:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>ISR 4400</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G5:FTX1830AKF9:53EBDBDA</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome" version="1.0">
<ch:EventTime>2014-08-13 21:42:49 GMT+00:00</ch:EventTime>
<ch:MessageDescription>*Aug 13 21:42:49.406: %CLEAR-5-COUNTERS: Clear counter on all
interfaces by console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>ISR XE Series Routers</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>admin@yourdomain.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>ISR4451-X/K9@C@FTX1830AKF9</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Router</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>admin@yourdomain.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
```

```
<rme:Model>ISR4451-X/K9</rme:Model>
<rme:HardwareVersion>1.0</rme:HardwareVersion>
<rme:SerialNumber>FTX1830AKF9</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="800-36894-03" />
<rme:AD name="SoftwareVersion" value="15.4(20140812:034256)" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.1707" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, ISR Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version 15.4(20140812:034256)
[v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140812_020034-ios 150]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 12-Aug-14 00:13 by mcpre" />
<rme:AD name="ServiceNumber" value="" />
<rme:AD name="ForwardAddress" value="" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[show logging
Syslog logging: enabled (0 messages dropped, 4 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: level debugging, 75 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 77 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 74 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (4096 bytes):

*Aug 13 21:42:20.187: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
*Aug 13 21:42:23.364: %SYS-5-CONFIG_I: Configured from console by console
Router#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show inventory</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[show inventory
NAME: "Chassis", DESCR: "Cisco ISR4451 Chassis"
PID: ISR4451-X/K9      , VID: V03, SN: FTX1830AKF9

NAME: "Power Supply Module 0", DESCR: "450W AC Power Supply for Cisco ISR4450, ISR4350"
PID: PWR-4450-AC       , VID: V01, SN: DCA1822X0G4

NAME: "Fan Tray", DESCR: "Cisco ISR4450, ISR4350 Fan Assembly"
PID: ACS-4450-FANASSY  , VID:    , SN:
```

```
NAME: "module 0", DESCR: "Cisco ISR4451 Built-In NIM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
PID: ISR4451-X-4x1GE   , VID: V01, SN: JAB092709EL

NAME: "module 1", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "module 2", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451-X/K9      , VID:    , SN:

NAME: "module R0", DESCR: "Cisco ISR4451 Route Processor"
PID: ISR4451-X/K9      , VID: V03, SN: FOC18271QLX

NAME: "module F0", DESCR: "Cisco ISR4451 Forwarding Processor"
PID: ISR4451-X/K9      , VID:    , SN:

Router#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```

その他の参考資料

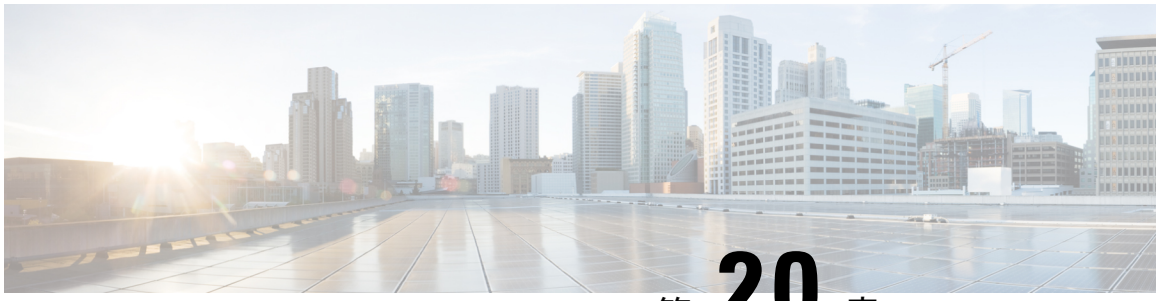
この章では、Call Home 機能に関連する参考資料を説明します。

関連資料

マニュアル タイトル	説明
『Smart Call Home User Guide』	Smart Call Home サービスが選択したシスコ デバイスに Web アクセスする方法、また予防的診断を行い、リアルタイム アラートを提供することでネットワークのアベイラビリティと運用効率を向上させる方法を説明します。

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/techsupport



第 20 章

ブリッジ ドメイン インターフェイスの設定

Cisco 4000 シリーズ ISR デバイスは、レイヤ 3 IP アドレスにレイヤ 2 イーサネットセグメントをパッケージングするためのブリッジドメインのインターフェイス（BDI）機能をサポートします。

ブリッジ ドメイン インターフェイスの制約事項

ブリッジ ドメイン インターフェイスに関連する制約事項は次のとおりです。

- システムごとにサポートされるブリッジ ドメイン インターフェイスは 4096 のみです。
- ブリッジドメインインターフェイスの場合、最大伝送単位（MTU）サイズは 1500 および 9216 バイトの間で設定できます。
- ブリッジ ドメイン インターフェイスは次の機能のみをサポートします。
  - IPv4 マルチキャスト
  - QoS マーキングとポリシング。シェーピングとキューイングはサポートされません。
  - IPv4 VRF
  - IPv6 ユニキャスト転送
  - BGP、OSPF、EIGRP、RIP、IS-IS、STATIC などのダイナミックルーティング
  - IOS XE 3.8.0 以降の Hot Standby Router Protocol（HSRP）
  - IOS XE 3.8.0 以降の Virtual Router Redundancy Protocol（VRRP）

- Flexible NetFlow

（注） Flexible NetFlow は、Cisco IOS XE 17.7.1a 以降のリリースでサポートされています。

- ブリッジ ドメイン インターフェイスは次の機能をサポートしません。
  - PPP over Ethernet（PPPoE）
  - 双方向フォワーディング検出（BFD）プロトコル
  - QoS
  - Network-Based Application Recognition（NBAR）または Advanced Video Coding（AVC）

ブリッジ ドメイン インターフェイスに関する情報

ブリッジ ドメイン インターフェイスは、レイヤ 2 ブリッジ型ネットワークとレイヤ 3 のルーテッド ネットワーク トラフィック間のトラフィックの双方向フローを許可する論理インターフェイスです。ブリッジ ドメイン インターフェイスは、ブリッジ ドメインと同じインデックスによって識別されます。各ブリッジ ドメインは、レイヤ 2 ブロードキャスト ドメインを表します。ブリッジドメインに関連付けることができるブリッジドメインインターフェイスは、1 つだけです。

ブリッジ ドメイン インターフェイスは次の機能をサポートします。

- IP 終了
- レイヤ 3 VPN の終了
- アドレス解決プロトコル（ARP）、G-ARP および P-ARP の処理
- MAC アドレスの割り当て

ブリッジ ドメイン インターフェイスを設定する前に、次の概念を理解しておく必要があります:

- イーサネット仮想回線の概要
- ブリッジ ドメイン インターフェイスのカプセル化
- MAC アドレスの割り当て
- IP プロトコルのサポート
- IP 転送のサポート
- パケット転送

- ブリッジ ドメイン インターフェイスの統計情報

イーサネット仮想回線の概要

イーサネット仮想回線（EVC）は、プロバイダーが提供しているレイヤ2サービスの単一インスタンスのエンドツーエンド表現です。さまざまなパラメータが統合されて、サービスが提供されます。シスコ EVC フレームワークでは、ブリッジ ドメインは、サービス インスタンスと呼ばれているレイヤ2インターフェイス（1つまたは複数）で構成されます。サービス インスタンスは、あるルータ上のあるポート上で EVC をインスタンス化したものです。サービス インスタンスは、設定に基づいてブリッジ ドメインに関連付けられます。

着信フレームは、次の基準に基づいてサービス インスタンスとして分類できます。

- シングル 802.1Q VLAN タグ、優先度タグ付き、または 802.1ad VLAN タグ
- 両 QinQ（内部および外部）VLAN タグ、または 802.1ad S-VLAN と C-VLAN タグの両方
- 外部 802.1p CoS ビット、内部 802.1p CoS ビット、またはその両方
- ペイロード イーサネット タイプ（5 つの選択肢をサポート：IPv4、IPv6、PPPoE-all、PPoE-discovery、PPPoE-session）

サービス インスタンスは、他のマッピング基準もサポートします。

- [Untagged]：802.1Q または 802.1ad ヘッダがないすべてのフレームにマッピングします。
- [Default]：すべてのフレームにマッピングします。

EVC アーキテクチャの詳細については、『Carrier Ethernet Configuration Guide』の「*Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Router*」のセクションを参照してください。

ブリッジ ドメイン インターフェイスのカプセル化

セキュリティ グループの分類には、送信先グループや宛先グループが含まれます。これは送信元の SGT と DGT で指定します。SGT ベースの PBR 機能では、SGT/DGT ベースのパケット分類のために PBR ルートマップの match 句を使用できます。SGT ベースの PBR 機能では設定できるタグの数に制限はありませんが、プラットフォームで使用できるメモリに基づいてタグを設定することをお勧めします。

EVC はブリッジ ドメインに存在する各イーサネット フロー ポイント（EFP）で様々なカプセル化を使用する機能を提供します。パケットは異なるカプセル化を設定した1つまたは複数の EFP から出力されている可能性があるため、BDI 出力ポイントは出力パケットのカプセル化を認識しないことがあります。

ブリッジ ドメインでは、すべての EFP で異なるカプセル化がある場合、BDI のタグ付けを解除する必要があります（802.1Q タグなしを使用）。EFP でブリッジ ドメインのすべてのトラフィック（ポップまたはプッシュ）をカプセル化します。ブリッジ ドメインのトラフィックのカプセル化を可能にするためには、各 EFP で rewrite を設定します。

ブリッジドメインでは、すべてのEFPで同じカプセル化がある場合は、encapsulationコマンドを使用してBDI上にカプセル化を設定します。BDIでのカプセル化をイネーブルにすると、タグのプッシングまたはポッピングが有効になり、それにより EFP で rewrite コマンドを設定する必要がなくなります。BDI でのカプセル化の設定の詳細については、「ブリッジ ドメイン インターフェイスの設定方法」を参照してください。

MAC アドレスの割り当て

Cisco 4000 シリーズ ISR シャーシ上のすべてのブリッジドメインは、同じ MAC アドレスを共有します。最初のブリッジドメインインターフェイスにMACアドレスが割り当てられます。その後、同じ MAC アドレスが、そのブリッジ ドメインで作成されたすべてのブリッジ ドメイン インターフェイスに割り当てられます。

（注） **mac-address** コマンドを使用して、ブリッジ ドメイン インターフェイスにスタティック MAC アドレスを設定できます。

IP プロトコルのサポート

ブリッジ ドメイン インターフェイスは、Cisco 4000 シリーズ ISR デバイスを有効にし、次の IP 関連プロトコルのレイヤ 2 ブリッジドメインのレイヤ 3 のエンドポイントとして機能します。

- ARP
- DHCP
- HTTP
- ICMP
- NTP
- RARP
- SNMP
- TCP
- Telnet
- TFTP
- UDP

IP 転送のサポート

ブリッジ ドメイン インターフェイスは次の IP 転送機能をサポートします。

- IPv4 の入力および出力アクセス コントロール リスト（ACL）

- IPv4 の入力および出力 QoS ポリシー。ブリッジ ドメイン インターフェイスの入力および出力サービス ポリシーでサポートされる動作は次のとおりです。
  - 分類
  - マーキング
  - ポリシング
- IPv4 L3 VRF

パケット転送

ブリッジ ドメイン インターフェイスはレイヤ 2 およびレイヤ 3 ネットワーク インフラ間のブリッジングおよび転送サービスを提供します。

レイヤ 2 から 3

レイヤ2ネットワークからレイヤ3ネットワークへのパケット フローの間に、着信パケットの宛先 MAC アドレスがブリッジ ドメイン インターフェイスの MAC アドレスと一致するか、宛先 MAC アドレスがマルチキャスト アドレスの場合、パケットまたはパケットのコピーがブリッジ ドメイン インターフェイスに転送されます。

（注） MAC アドレス ラーニングは、ブリッジ ドメイン上のインターフェイスで実行できません。

レイヤ 3 からレイヤ 2

パケットがルータの物理インターフェイスのレイヤ3に到達すると、ルート検索アクションが実行されます。ルート検索がブリッジ ドメイン インターフェイスに向かうと、ブリッジ ドメイン インターフェイスはレイヤ 2 カプセル化を追加し、対応するブリッジ ドメインにフレームを転送します。バイト カウンタが更新されます。

ブリッジドメインインターフェイスが属するブリッジドメインでのレイヤ2検索中に、ブリッジ ドメインは、宛先 MAC アドレスに基づいて適切なサービス インスタンスにパケットを転送します。

ブリッジ ドメインとブリッジ ドメイン インターフェイスのステートをリンクする

ブリッジ ドメイン インターフェイスはレイヤ 3 のルーティング可能な IOS インターフェイスおよびブリッジ ドメインのポートとして機能します。ブリッジ ドメイン インターフェイスとブリッジ ドメインのいずれも、個々の管理状態で動作します。

ブリッジ ドメイン インターフェイスをシャットダウンすると、レイヤ 3 データ サービスは停止しますが、関連するブリッジ ドメインの状態は上書きされず、影響を受けません。

ブリッジ ドメインをシャットダウンすると、サービス インスタンスやブリッジ ドメイン インターフェイスを含むすべての関連メンバへのレイヤ2転送が停止します。関連するサービスインスタンスはブリッジドメインの動作状態に影響を与えます。ブリッジ ドメインインターフェイスは、関連するサービスインスタンスの 1 つが起動しない限り、動作することはできません。

（注） ブリッジ ドメイン インターフェイスは内部インターフェイスであるため、ブリッジ ドメイン インターフェイスの動作状態はブリッジ ドメインの動作状態には影響しません。

BDI の初期状態

BDI 最初の管理ステートは、BDI の作成方法によって異なります。スタートアップ コンフィギュレーションで起動時にBDIを作成すると、BDIのデフォルトの管理状態がアップになります。スタートアップ コンフィギュレーションに shutdown コマンドが含まれていない限り、この状態のままになります。この動作は、他のすべてのインターフェイスと一致します。コマンドプロンプトで BDI を動的に作成すると、デフォルトの管理状態はダウンになります。

BDI のリンク状態

BDI は、管理上のダウン状態、動作上のダウン状態、アップ状態の 3 種類のステートからなるリンク状態を維持します。BDIのリンク状態は、対応するユーザーによって設定されたBDI管理状態セットおよびインターフェイスステートの下位レベルの障害表示の状態の2つの独立する入力から得られます。BDI のリンク状態は、2 つの入力の状態に基づいて定義されます。

障害表示の状態	BDI 管理	
{emdash を開始}{emdash を終了}	**Shutdown**	**No Shutdown**
No faults asserted	Admin-down	Up
At least one fault asserted	Admin-down	Operationally-Down

ブリッジ ドメイン インターフェイスの統計情報

ブリッジ ドメイン インターフェイスなどの仮想インターフェイスの場合は、プロトコル カウンタは QFP から定期的に検索されます。

パケットがレイヤ 2 ブリッジ ドメイン ネットワークからドメインのインターフェイスを介してレイヤ 3 のルーティング ネットワークに流れると、パケットはブリッジ ドメイン インターフェイスの入力パケットおよびバイトとして処理されます。パケットがレイヤ3インターフェイスに到達し、ブリッジ ドメイン インターフェイスを介してレイヤ 2 ブリッジ ドメインに転送されると、パケットは出力パケットおよびバイトとして処理され、カウンタが適宜更新されます。

BDI はすべての Cisco IOS インターフェイスで、ケースとしてレイヤ 3 パケット カウンタの標準セットを維持します。レイヤ 3 のパケット カウンタを表示するには、show interface コマンドを使用します。

カウンタの表記法は、レイヤ 3 クラウドに関連しています。たとえば、input はレイヤ 2 BD からレイヤ 3 クラウドに入るトラフィックを示し、output はレイヤ 3 クラウドからレイヤ 2 BD に向かうトラフィックを示します。

BDI ステータスの統計情報を表示するには、**show interfaces accounting** コマンドを使用します。送受信されるパケットおよびバイト全体のカウントを表示するには、**show interface** <*if-name*> コマンドを使用します。

ブリッジ ドメイン インターフェイスの作成または削除

Cisco IOS ルータのインターフェイスまたはサブインターフェイスを定義する場合は、名前を付け、どのように IP アドレスに割り当てられるかを指定します。システムにブリッジドメインを追加する前にブリッジ ドメイン インターフェイスを作成できます。この新しいブリッジドメインインターフェイスは、関連するブリッジドメインの設定後にアクティブになります。

（注） ブリッジ ドメイン インターフェイスが作成されると、ブリッジ ドメインが自動的に作成されます。

ブリッジ ドメイン インターフェイスとブリッジドメインを作成すると、システムは、ブリッジドメインとブリッジ ドメイン インターフェイスのペアをマッピングするために必要なアソシエーションを保持します。

ブリッジ ドメインとブリッジ ドメイン インターフェイスのマッピングはシステムに保持されます。ブリッジドメインインターフェイスは、アソシエーションを示すために関連するブリッジ ドメインのインデックスを使用されます。

ブリッジ ドメイン インターフェイスのスケーラビリティ

次の表に、Cisco 4000 シリーズ ISR デバイスのフォワーディングプロセッサ（FP）のタイプに基づいた、ブリッジ ドメイン インターフェイスのスケーラビリティの数値を示します。

表 *37 : Cisco 4000* シリーズ *ISR* デバイスのフォワーディングプロセッサのタイプに基づいた、ブリッジ ドメイン インターフェイスのスケーラビリティの数値

説明	0
ルータごとのブリッジ ドメイン インターフェイスの最大数	

ブリッジドメイン仮想 IP インターフェイス

仮想 IP インターフェイス（VIF）機能は、複数の BDI インターフェイスを BD インスタンスに関連付けるのに役立ちます。BD-VIF インターフェイスは、IOS 論理 IP インターフェイスの既存のすべての L3 機能を継承します。

（注） すべての BD-VIF インターフェイスに一意の MAC アドレスを設定する必要があり、異なる VRF に属している必要があります。

仮想 IP インターフェイス（VIF）機能には、次の制限事項があります。

- BD-VIF インターフェイスは IP マルチキャストをサポートしていません。
- 自動生成された MAC アドレスを持つ BD-VIF インターフェイスの数は、プラットフォームによって異なります。
- BD-VIF インターフェイスは MPLS をサポートしていません。
- ブリッジドメインごとの BD-VIF インターフェイスの最大数と、システムごとの BD-VIF インターフェイスの総数は、プラットフォームのタイプによって異なります。

サポートされる BD-VIF の最大数は、プラットフォームによって異なります。

- ASR 1000 は、ブリッジドメインに対して最大 100 の BD-VIF をサポートします。
- CSR 1000v は、ブリッジドメインに対して最大 16 の BD-VIF をサポートします。
- ISR 4000 は、ブリッジドメインに対して最大 16 の BD-VIF をサポートします。

Cisco IOS XE 17.7.1a リリースから、BD-VIF は Flexible Netflow（FnF）をサポートします。

ブリッジ ドメイン インターフェイスの設定方法

ブリッジ ドメイン 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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface BDI** *{interface number}*
4. **encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]*
5. 次のいずれかを実行します。
6. **match security-group destination tag** *sgt-number*
7. **mac address** *{mac-address}*
8. **no shut**
9. **shut**

手順の詳細

	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。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	**configure terminal** 例： `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 3	**interface BDI** *{interface number}* 例： `Router(config-if)# interface BDI3`	ブリッジドメインインターフェイスを指定します。
ステップ 4	**encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]* 例： `Router(config-if)# encapsulation dot1Q 1 second-dot1q 2`	カプセル化タイプを定義します。 例では、カプセル化タイプとして dot1q を定義しています。

ステップ 5	次のいずれかを実行します。
	例：
	ip address *ip-address mask*
	例：
	
	例：
	ipv6 address *{X:X:X:X::X* **link-local**| *X:X:X:X::X/prefix [***anycast** | **eui-64***]* | **autoconfig** *[***default***]}*
	例：
	`Router(config-if)# ip address 10.2.2.1 255.255.255.0`
	例：
	
	例：
	`Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64`
		ブリッジ ドメイン インターフェイスの IPv4 または IPv6 アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 6	**match security-group destination tag** *sgt-number* 例： `Router(config-route-map)# match security-group destination tag 150`	security-group destination security tag の値を設定します。
ステップ 7	**mac address** *{mac-address}* 例： `Router(config-if)# mac-address 1.1.3`	ブリッジ ドメイン インターフェイスの MAC アドレスを指定します。
ステップ 8	**no shut** 例： `Router(config-if)# no shut`	ブリッジ ドメイン インターフェイスを有効にします。
ステップ 9	**shut** 例： `Router(config-if)# shut`	ブリッジ ドメイン インターフェイスを無効にします。

例

次に、IP アドレス 10.2.2.1 255.255.255.0 でブリッジ ドメイン インターフェイスを設定する例を示します。

```
Router# configure terminal
Router(config)# interface BDI3
Router(config-if)# encapsulation dot1Q 1 second-dot1q 2
Router(config-if)# ip address 10.2.2.1 255.255.255.0
Router(config-if)# mac-address 1.1.3
Router(config-if)# no shut
Router(config-if)# exit
```

ブリッジ ドメイン インターフェイス設定の表示と確認

手順の概要

1. **enable**
2. **show interfaces bdi**
3. **show platform software interface fp active name**
4. **show platform hardware qfp active interface if-name**
5. **debug platform hardware qfp feature**
6. **platform trace runtime process forwarding-manager module**
7. **platform trace boottime process forwarding-manager module interfaces**

手順の詳細

	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。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	**show interfaces bdi** 例： `Router# show interfaces BDI3`	対応する BDI の設定の概要を表示します。
ステップ 3	**show platform software interface fp active name** 例： `Router# show platform software interface fp active name BDI4`	フォワーディングプロセッサのブリッジ ドメイン インターフェイス設定を表示します。
ステップ 4	**show platform hardware qfp active interface if-name** 例： `Router# show platform hardware qfp active interface if-name BDI4`	データパスのブリッジ ドメイン インターフェイス設定を表示します。
ステップ 5	**debug platform hardware qfp feature** 例： `Router# debug platform hardware qfp active feature l2bd client all`	選択した CPP L2BD Client のデバッグがオンになります。
ステップ 6	**platform trace runtime process forwarding-manager module** 例： `Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module interfaces level info`	Forwarding Manager プロセスの Forwarding Manager Route Processor および Embedded Service Processor のトレースメッセージを有効にします。
ステップ 7	**platform trace boottime process forwarding-manager module interfaces** 例： `Router(config)# platform trace boottime slot R0 bay 1 process forwarding-manager forwarding-manager level max`	ブートアップ中の、Route Processor Forwarding Manager プロセスの Forwarding Manager Route Processor および Embedded Service Processor のトレースメッセージを有効にします。

次のタスク

各コマンドに使用できるコマンドおよびオプションの詳細については、『Cisco IOS Configuration Fundamentals Command Reference Guide』を参照してください。

ブリッジドメイン仮想 IP インターフェイスの設定

```
enable
configure terminal
[no] interface BD-VIF interface-number
  [ [no] vrf forwarding vrf-name]
  [ [no] mac address mac-address]
  [ [no] ip address ip-address mask]
  [ [no] ipv6 address {X:X:X:X::X link-local| X:X:X:X::X/prefix [anycast | eui-64] |
autoconfig [default]}]

exit
```

BD-VIF インターフェイスを削除するには、このコマンドの 'no' 形式を使用します。

VIF インターフェイスのブリッジ ドメインへの関連付け

```
enable
configure terminal
bridge-domain bridge-domain number
[no] member BD-VIF interface-number
exit
```

VIF インターフェイスの関連付けを解除するには、このコマンドの「no」形式を使用します。

ブリッジドメイン仮想 IP インターフェイスの確認

インターフェイスおよび IP インターフェイスの既存のすべての show コマンドは、BD-VIF インターフェイスに使用できます。

show interface bd-vif *bd-vif-id*

show ip interface bd-vif *bd-vif-id*

show bd-vif interfaces in fman-fp

show pla sof inter fp ac brief | i BD_VIF

ブリッジドメイン仮想 IP インターフェイスの設定例

```
Detail sample:

interface Port-channel1
mtu 9000
no ip address
 !Ethernet service endpoint one per neutron network
service instance 1756 ethernet
  description 4e8e5957-649f-477b-9e5b-f1f75b21c03c
  encapsulation dot1q 1756
```

```
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1756
!
interface BD-VIF5001
no shutdown
vrf forwarding vrf5001
ip address 10.0.0.1 255.255.255.0
interface BD-VIF5002
no shutdown
vrf forwarding vrf5002
ip address 10.0.0.2 255.255.255.0

bridge-domain 1756
member Port-channel1 service-instance 1756
member bd-vif5001
member bd-vif5002
```

ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. {**ip | ipv6**}**flow monitor** *monitor-name* [**sampler** *sampler-name*] {**input | output**}
5. **exit**

手順の詳細

	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	**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	**interface** *type number* 例： `Device (config)# interface BD-VIF 100`	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 モードを開始します。BD-VIF 番号を入力します。
ステップ 4	{**ip	ipv6**}**flow monitor** *monitor-name* [**sampler** *sampler-name*] {**input	output**} 例：	ルータがインターフェイスで送受信する IP トラフィックの Flexible NetFlow フローモニターを有効にします。

	コマンドまたはアクション	目的
	`Device(config-if)# ip flow monitor FLOW-MONITOR-1 input`	
ステップ 5	**exit** 例： `Device(config-if)# exit`	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。

例：ブリッジドメイン仮想 IP インターフェイスを介した Flexible NetFlow

次に、フローモニターの QFP 情報およびフロー方向を表示する **show platform hardware qfp active interface if-name** コマンドの出力例を示します。次の表に、CLI 出力のキーを示します。

設定	出力
ip flow monitor <monitor-name> input	IPV4_INPUT_FNF_FIRST IPV4_INPUT_FNF_FINAL
ip flow monitor <monitor-name> output	IPV4_BDI_OUTPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> input	IPV6_INPUT_FNF_FIRST IPV6_INPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> output	IPV6_BDI_OUTPUT_FNF_FINAL

```
Device# show run interface bd-vif2
Building configuration...

Current configuration: 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
ipv6 flow monitor test2 output
ipv6 address 2001:DB8::1/32
end

Device# show platform hardware qfp active interface if-name BD-VIF 2
General interface information
  Interface Name: BD-VIF2
  Interface state: VALID
  Platform interface handle: 20
  QFP interface handle: 17
  Rx uidb: 262138
  Tx uidb: 262127
  Channel: 0
Interface Relationships

BGPPA/QPPB interface configuration information
  Ingress: BGPPA/QPPB not configured. flags: 0000
```

```
  Egress: BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
ipv6_input enabled.
ipv6_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:
2 GIC FIA state
66 PUNT INJECT DB
70 cpp_l2bd_svr
43 icmp_svr
45 ipfrag_svr
46 ipreass_svr
47 ipv6reass_svr
44 icmp6_svr
58 stile
Protocol 0 - ipv4_input
FIA handle - CP:0x55a7f59df038 DP:0x3fff1000
  IPV4_INPUT_DST_LOOKUP_ISSUE (M)
  IPV4_INPUT_ARL_SANITY (M)
  IPV4_INPUT_SRC_LOOKUP_ISSUE
  IPV4_INPUT_DST_LOOKUP_CONSUME (M)
  IPV4_INPUT_SRC_LOOKUP_CONSUME
  IPV4_INPUT_FOR_US_MARTIAN (M)
  IPV4_INPUT_STILE_LEGACY
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_LOOKUP_PROCESS (M)
  IPV4_INPUT_FNF_FINAL
  IPV4_INPUT_IPOPTIONS_PROCESS (M)
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x55a7f59df0d8 DP:0x3ffeff00
  IPV4_VFR_REFRAG (M)
  IPV4_OUTPUT_SRC_LOOKUP_ISSUE
  IPV4_OUTPUT_L2_REWRITE (M)
  IPV4_OUTPUT_SRC_LOOKUP_CONSUME
  IPV4_OUTPUT_STILE_LEGACY
  IPV4_OUTPUT_FRAG (M)
  IPV4_BDI_OUTPUT_FNF_FINAL.
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
Protocol 6 - ipv6_input
FIA handle - CP:0x55a7f59dee58 DP:0x3fff4300
  IPV6_INPUT_SANITY_CHECK (M)
  IPV6_INPUT_DST_LOOKUP_ISSUE (M)
  IPV6_INPUT_SRC_LOOKUP_ISSUE
  IPV6_INPUT_ARL (M)
  IPV6_INPUT_DST_LOOKUP_CONT (M)
  IPV6_INPUT_SRC_LOOKUP_CONT
  IPV6_INPUT_DST_LOOKUP_CONSUME (M)
  IPV6_INPUT_SRC_LOOKUP_CONSUME
  IPV6_INPUT_STILE_LEGACY
  IPV6_INPUT_FNF_FIRST
  IPV6_INPUT_FOR_US (M)
  IPV6_INPUT_LOOKUP_PROCESS (M)
  IPV6_INPUT_FNF_FINAL
  IPV6_INPUT_LINK_LOCAL_CHECK (M)
```

```
  IPV6_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 7 - ipv6_output
FIA handle - CP:0x55a7f59dee08 DP:0x3fff4b80
  IPV6_VFR_REFRAG (M)
  IPV6_OUTPUT_SRC_LOOKUP_ISSUE
  IPV6_OUTPUT_SRC_LOOKUP_CONT
  IPV6_OUTPUT_SRC_LOOKUP_CONSUME
  IPV6_OUTPUT_L2_REWRITE (M)
  IPV6_OUTPUT_STILE_LEGACY
  IPV6_OUTPUT_FRAG (M)
  IPV6_BDI_OUTPUT_FNF_FINAL
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV6_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
```

次に、キャッシュ出力をレコード形式で表示する **show flow monitor** [[**name**] [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] コマンドの出力例を示します。

```
Device# show flow monitor name FLOW-MONITOR-1 cache format record

Cache type:  Normal
Cache size:  1000
Current entries:  4
High Watermark:  4
Flows added:  101
Flows aged:  97
- Active timeout (1800 secs) 3
- Inactive timeout  (15 secs) 94
- Event aged  0
- Watermark aged  0
- Emergency aged
IPV4 DESTINATION ADDRESS:
198.51.100.1 0
ipv4 source address: 10.10.11.1
trns source port: 25
trns destination port: 25
counter bytes: 72840
counter packets: 1821
IPV4 DESTINATION ADDRESS: 198.51.100.2
ipv4 source address: 10.10.10.2
trns source port: 20
trns destination port: 20
counter bytes: 3913860
counter packets: 7326
IPV4 DESTINATION ADDRESS: 198.51.100.200
ipv4 source address: 192.168.67.6
trns source port: 0
trns destination port: 3073
counter bytes: 51072
counter packets: 1824


Device# show flow monitor name FLOW-MONITOR-2 cache format record

Cache type:  Normal
Cache size: 1000
Current entries: 2
High Watermark: 3
Flows added: 95
Flows aged: 93
- Active timeout (1800 secs) 0
```

```
- Inactive timeout (15 secs) 93
- Event aged 0
- Watermark aged 0
- Emergency aged 0
IPV6 DESTINATION ADDRESS: 2001:DB8:0:ABCD::1
ipv6 source address: 2001:DB8:0:ABCD::2
trns source port: 33572
trns destination port: 23
counter bytes: 19140
counter packets: 349
IPV6 DESTINATION ADDRESS: FF02::9
ipv6 source address: 2001:DB8::A8AA:BBFF:FEBB

trns source port: 521
trns destination port: 521
counter bytes: 92
counter packets: 1
```

次に、インターフェイスのフローステータスを表示する **show flow interface** コマンドの出力例を示します。

```
Device# show flow interface BD-VIF2001

Interface GigabitEthernet0/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Input
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction:    Input traffic(ipv6): on

Device# show flow interface BD-VIF2002

Interface GigabitEthernet1/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Output
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction:    Input traffic(ipv6): on
```

次に、Flexible NetFlow 設定のフローモニターの QFP 情報およびフロー方向を表示する **show platform hardware qfp active interface if-name** | **in FNF** コマンドの出力例を示します。次の表に、CLI 出力のキーを示します。

設定	出力
ip flow monitor <monitor-name> input	IPV4_INPUT_FNF_FIRST IPV4_INPUT_FNF_FINAL
ip flow monitor <monitor-name> output	IPV4_BDI_OUTPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> input	IPV6_INPUT_FNF_FIRST IPV6_INPUT_FNF_FINAL
ipv6 flow monitor <monitor-name> output	IPV6_BDI_OUTPUT_FNF_FINAL

```
Device# show run interface bd-vif2
Building configuration...

Current configuration : 227 bytes
!
interface BD-VIF2
```

```
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
ipv6 flow monitor test2 output
ipv6 address 2001::8/64
end
 Device# show platform hardware qfp active interface if-name BD-VIF 2  | in FNF
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_FNF_FINAL
  IPV4_BDI_OUTPUT_FNF_FINAL.
  IPV6_INPUT_FNF_FIRST
  IPV6_INPUT_FNF_FINAL
  IPV6_BDI_OUTPUT_FNF_FINAL
```

clear flow monitor name *monitor-name* [**cache** [**force-export**] | **force-export** | **statistics**] コマンドを使用すると、Flexible NetFlow フローモニター、フローモニターキャッシュ、またはフローモニター統計情報がクリアされ、フローモニターキャッシュ内のデータを強制的にエクスポートできます。

Flexible NetFlow の設定の詳細については、『Flexible NetFlow Configuration Guide, Cisco IOS XE 17』を参照してください。

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 ASR 1000 シリーズ アグリゲーション サービス ルータでのイーサネット仮想接続の設定	『Carrier Ethernet Configuration Guide』
EVC Quality of Service	http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/qos_evc_xe.html

MIB

MIB	MIB のリンク
なし	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

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	https://www.cisco.com/c/en_in/support/index.html

ブリッジ ドメイン インターフェイスの機能情報

次の表に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

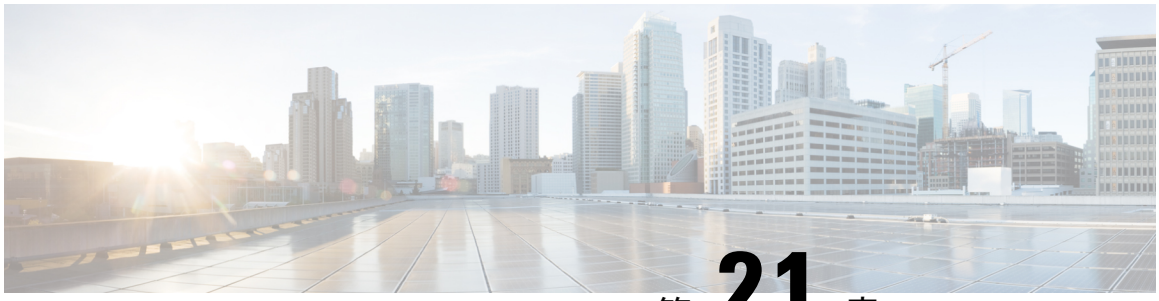
プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *38* : ブリッジ ドメイン インターフェイスの機能情報

機能名	リリース	機能情報
ブリッジ ドメイン インターフェイスの設定	Cisco IOS XE Cupertino 17.7.1a	この機能が Cisco 4000 シリーズ ISR デバイスに導入されました。
ブリッジドメイン仮想 IP インターフェイス	Cisco IOS XE Cupertino 17.7.1a	この機能が Cisco 4000 シリーズ ISR デバイスに導入されました。 ブリッジドメイン仮想 IP インターフェイス（VIF）は、複数のブリッジ ドメイン インターフェイス（BDI）を単一の BD インスタンスに接続し、L2 ネットワーク内の各 IP サブネットを単一の VRF に関連付けることができるようになりました。

機能名	リリース	機能情報
ブリッジドメイン仮想 IP インターフェイス（BD-VIF）上の Flexible NetFlow（FNF）	Cisco IOS XE Cupertino 17.7.1a	この機能が Cisco 4000 シリーズ ISR デバイスに導入されました。次のコマンドが導入されました。 **{ip | ipv6} flow monitor** *monitor-name* **[sampler** *sampler-name***] {input | output}**



第 21 章

Cisco 拡張サービス モジュールおよびネットワーク インターフェイス モジュールの管理

ルータは Cisco 拡張サービス モジュールおよび Cisco ネットワーク インターフェイス モジュール（NIM）をサポートしています。これらのモジュールは、アダプタ（キャリア カード）を使用して、ルータのさまざまなスロットに装着されます。詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』を参照してください。

この章で説明する内容は、次のとおりです。

Cisco 拡張サービス モジュールおよびネットワーク インターフェイス モジュールについて

ルータは、アーキテクチャに組み込まれているモジュール管理機能を使用して、サポートされている Cisco 拡張サービス モジュール（SM）とネットワーク インターフェイス モジュール（NIM）を設定、管理、制御します。この新しい一元化されたモジュール管理機能により、システムのすべてのモジュールを、そのタイプや用途とは無関係に共通の方法で制御および監視できます。ルータでサポートされるすべての Cisco 拡張サービス モジュールとネットワーク インターフェイス モジュールは、標準 IP プロトコルを使用してホスト ルータと通信します。Cisco IOS ソフトウェアは、モジュール間の切り替えに異種データ パス統合を使用します。

サポートされるモジュール

Cisco ISR 4400 シリーズおよびCisco ISR 4300 シリーズのルータでサポートされるインターフェイスとモジュールについては、http://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/relevant-interfaces-and-modules.htmlを参照してください。

ネットワーク インターフェイス モジュール

サポートされるネットワーク インターフェイス プロトコルは、次のとおりです。

Cisco 第 4 世代 LTE ネットワーク インターフェイス モジュール

Cisco 4G LTE NIM は、Cisco 4000 シリーズ ISR でのモジュラ 4G LTE セルラー接続に対応します。これは、ISR 製品ラインの最初のワイヤレスモジュールではありませんが、最初のワイヤレス NIM です。Cisco 4G LTE NIM に最も近いモジュラカードは、単一の LTE モデムを搭載できる Cisco EHWIC 4G LTE です。Cisco 4G LTE NIM は、Cisco EHWIC 4G LTE と機能互換性があります。詳細については、『Cisco Fourth-Generation LTE Network Interface Module Software Configuration Guide』を参照してください。

Cisco 4 ポートおよび 8 ポート レイヤ 2 ギガビット EtherSwitch ネットワーク インターフェイス モジュール

Cisco 4 ポートおよび 8 ポート レイヤ 2 ギガビット EtherSwitch ネットワーク インターフェイス モジュール（NIM）は、レイヤ2機能を統合し、モジュール間通信用にマルチギガビットファ

ブリック（MGF）への 1 Gbps の接続を提供します。Cisco 4 ポートおよび 8 ポートレイヤ 2 ギガビット EtherSwitch NIM の設定の詳細については、http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4_8PortGENIM.html.を参照してください。

Cisco 第 4 世代 T1/E1 音声および WAN ネットワーク インターフェイス モジュール

Cisco 第 4 世代 T1/E1 音声および WAN ネットワーク インターフェイス モジュール（NIM）は、ルータのスロットに装着され、T1/E1 トランクのデータおよび音声をサポートします。音声関連およびその他の DSP 機能をサポートするには、Cisco PVDM4（Cisco パケット音声デジタル信号プロセッサ モジュール）もまた必要です。詳細については、次のマニュアルを参照してください。

- Installing the Cisco Fourth-Generation T1/E1 Voice and WAN Network Interface Module
- 『Configuring the Cisco Fourth-Generation T1/E1 Voice and WAN Network Interface Module』
- 『Installing the Cisco PVDM4』

Cisco SSD/HDD キャリア カード NIM

ルータでは、単一の Cisco HDD および SSD キャリア カード NIM がサポートされます。スロット 0 およびサブスロット 1、2、または 3 にこれを装着する必要があります。

Cisco SSD/HDD キャリア カード NIM は次のいずれかです。

- Cisco SSD キャリア カード NIM：1 ～ 2 台のソリッド ステート ドライブ（SSD）をサポート。
- Cisco HDD キャリア カード NIM：1 台のハード ディスク ドライブ（HDD）をサポート。

（注） ISR-WAAS が動作している場合は、NIM-SSD および NIM-HDD の活性挿抜（OIR）を実行しないでください。

SSD/HDD キャリアカード NIM のハードウェア特性の詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』を参照してください。

SSD/HDD キャリア カード NIM の非アクティブ化または再アクティブ化のの詳細については、SSD/HDD キャリア カード NIM の非アクティブ化および再アクティブ化 （386 ページ）を参照してください。

Cisco 1 ポート、2 ポート、および 4 ポート シリアル NIM

Cisco 1 ポート、2 ポート、および 4 ポート シリアル NIM は、Cisco 4400 シリーズ ISR でサポートされているマルチプロトコル同期シリアル ネットワーク インターフェイス モジュール（NIM）

です。Cisco 1 ポート、2 ポート、および 4 ポート シリアル NIM はルータ機能を拡張し、高速ハイレベル データ リンク制御用の 8 Mbps までのデータ レートを含む、さまざまなアプリケーションでの同期インターフェイスの接続性を提供します。これらの機能は、ポイントツーポイント Cisco HDLC WAN インターフェイスまたはフレーム リレー インターフェイスとして使用できます。Cisco 1 ポート、2 ポート、および 4 ポート シリアル NIM は、独自のシリアル通信コントローラ（SCC）を持ち、ホスト ルータの SCC には依存しません。この NIM の設定の詳細については、「Configuring the Cisco 1-, 2-, and 4-port Serial Network Interface Modules for the Cisco 4400 Series ISRs」を参照してください。

HDD または SSD のファームウェアのアップグレード

SSD または HDD のファームウェアをアップグレードするには、**upgrade hw-programmable module filename bootflash:***filename slot/sub-slot* コマンドを使用できます。

filename の標準形式は *nim_ssd_manufacturer_firmware-version-number.bin* です。

ファームウェアは、**bootflash:** 以外の場所でも使用できます。

たとえば、**bootflash:***filename* の代わりに以下のいずれかの場所を指定できます。

- **flash:***filename*
- **harddisk:***filename*
- **usb1:***filename*

（注） Cisco SSD キャリア カード NIM または Cisco HDD キャリア カード NIM の場合、スロット 0 と、サブスロット 1、2、3 のいずれか 1 つだけを使用する必要があります。

次に、**upgrade hw-programmable module filename bootflash:***filename slot/sub-slot* コマンドを使用して Micron P400m ディスクをファームウェアリビジョン 200 にアップグレードする例を示します。

```
Router# upgrade hw-programmable module filename bootflash:nim_ssd_Micr nP400m_E200.bin
Info: Trying to upgrade Module in 0/3 with nim_ssd_MicronP400m_E200.bin
Info: Current NIM-SSD disk config.
Info: Disk1: rev: 0200 model: MicronP400m-MTFDDAK200MAN
Info: Disk2: rev: 0200 model: MicronP400m-MTFDDAK200MAN
/dev/sde:
fwdownload: xfer_mode=3 min=1 max=255 size=512
.....................................................................................................
 Done.
/dev/sdf:
fwdownload: xfer_mode=3 min=1 max=255 size=512
.....................................................................................................
 Done.
Info: Performing post upgrade check ......
Info: Upgrade to Firmware version E200 on disk1 successful.
Info: Upgrade to Firmware version E200 on disk2 successful.
Info: Current NIM-SSD disk config.
Info: Disk1: rev: E200 model: MicronP400m
```

エラー モニタリング

シスコ SDD/HDD キャリア カード NIM のドライブでは、SMART エラーが発生しているかどうかが監視されます。SMART エラーが発生すると、次の例に示すように Cisco IOS エラー メッセージが表示されます。

```
%IOSXE-5-PLATFORM:logger: INFO:/dev/sde:SMART error present:please do
'more bootflash:/tracelogs/smart_errors.log'.
```

エラー ログ（bootflash: /tracelogs/smart_errors.log）で追加情報を確認できます。

拡張サービス モジュール

次のサービス モジュールがルータでサポートされています。

- Cisco SM-1 T3/E3 サービス モジュール （381 ページ）
- Cisco UCS E シリーズ サーバ （381 ページ）
- Cisco SM-X レイヤ 2/3 EtherSwitch サービス モジュール （381 ページ）
- Cisco 6 ポート GE SFP サービス モジュール （382 ページ）

Cisco SM-1 T3/E3 サービス モジュール

詳細については、『Cisco SM-1T3/E3 Enhanced Service Module Configuration Guide』を参照してください。

Cisco UCS E シリーズ サーバ

詳細については、「Cisco UCS E-Series Server Roadmap」に記載されているマニュアルを参照してください。

Cisco SM-X レイヤ 2/3 EtherSwitch サービス モジュール

このモジュールには次の機能があります。

- レイヤ 2 スイッチ機能とレイヤ 3 スイッチ機能の統合、およびルータが Cisco SM-X レイヤ 2/3 ESM（16 ポートおよび 24 ポート）を独立レイヤ 3 スイッチとして使用できる機能。
- ルータの CPU に大きな負荷をかけずにモジュール間通信を可能にする、マルチギガビット ファブリック（MGF）への 1 Gbps 接続。
- 堅牢な Power over Ethernet Plus（PoE+）機能と、IEEE 802.3AE Media Access Control Security（MACSec）ポート ベースの hop-to-hop 暗号化および Cisco TrustSec による、ポートあたり最大 30 W の供給電力。

詳細については、次のマニュアルを参照してください。

- Cisco SM-X Layer 2/3 EtherSwitch Service Module Configuration Guide for Cisco 4451-X ISR
- Connecting Cisco SM-X Layer 2/3 EtherSwitch Service Module to the Network

Cisco 6 ポート GE SFP サービス モジュール

Cisco 6 ポート GE SFP モジュールは、ルータの SM スロットに装着可能なギガビット イーサネット モジュールであり、ルーティング可能な外部インターフェイスでのギガビット イーサネット機能を提供します。このサービスモジュールの設定の詳細については、『Software Configuration Guide for the Cisco 6-port GE SFP Service Module』を参照してください。

Cisco 4 ポート GE SFP および 1 ポート 10 GE SFP サービス モジュール

Cisco 4 ポート GE SFP および 1 ポート 10 GE SFP サービス モジュール（SM X 4x1GE-1x10GE）は、Cisco ISR 4400 シリーズ ルータ用の、ソフトウェアによる設定が可能な高速接続ルーティング ポート サービス モジュールです。このサービス モジュールにより、Cisco ISR 4400 シリーズ ルータのイーサネット インターフェイスの密度が向上します。このサービスモジュールの設定の詳細については、『Software Configuration Guide for the Cisco 6-port GE SFP Service Module and Cisco 4-port GE SFP and 1-port 10 GE SFP Service Module』を参照してください。

Cisco 1GE-CU-SFP および 2GE-CU-SFP ネットワーク インターフェイス モジュール

Cisco 1GE-CU-SFP および 2GE-CU-SFP ネットワーク インターフェイス モジュール（NIM）は、Cisco 4000 および Cisco ISR 4300 シリーズ サービス統合型ルータ（ISR）用のソフトウェア設定可能な高速接続ルーティング ポート ネットワーク インターフェイス モジュールです。これらのネットワーク インターフェイス モジュールは、Cisco 4000 ISR のイーサネット インターフェイスの密度を高めます。この NIM の設定の詳細については、『Configuring the Cisco 1GE-CU-SFP and 2GE-CU-SFP Network Interface Modules in Cisco 4000 Series Integrated Services Routers』を参照してください。

（注） Cisco 4221 ISR は、2GE-CU-SFP ネットワーク インターフェイス モジュールをサポートしていません。

ルータでの SM および NIM の実装

- モジュール ファームウェアのダウンロード （383 ページ）
- SM と NIM のインストール （383 ページ）

• コンソール接続または Telnet 経由でのモジュールへのアクセス （383 ページ）
• 活性挿抜（OIR） （384 ページ）

モジュール ファームウェアのダウンロード

サービス モジュールを使用できるようにするには、ルータにモジュール ファームウェアをロードする必要があります。詳細については、ファームウェア サブパッケージのインストール（138 ページ）を参照してください。

ファームウェアをダウンロードするために、モジュールは内部 eth0 インターフェイスを介して RP に接続します。最初に、モジュールは BOOTP を介して自身の IP アドレスを取得します。また、BOOTP はイメージのダウンロードに使われる TFTP サーバのアドレスも提供します。イメージがロードされ、モジュールが起動された後、モジュールは DHCP を介して実行中のイメージの IP アドレスを提供します。

SM と NIM のインストール

詳細については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』の「Installing and Removing NIMs and SMs」を参照してください。

コンソール接続または Telnet 経由でのモジュールへのアクセス

モジュールにアクセスするには、その前にルータ コンソールまたは Telnet 経由でホスト ルータに接続する必要があります。ルータに接続したら、モジュールに接続されているギガビット イーサネット インターフェイスで IP アドレスを設定する必要があります。ルータ上で特権 EXEC モードで **hw-module session** コマンドを使用して、モジュールへのセッションを開始します。

モジュールへの接続を確立するには、Telnet またはセキュアシェル（SSH）を使用してルータ コンソールに接続し、ルータ上で特権 EXEC モードで **hw-module session** *slot/subslot* コマンドを使用して、スイッチへのセッションを開始します。

次の設定例を使用して、接続を確立します。

- 次に、**hw-module session** コマンドを使用してルータからセッションを開始する例を示します。

```
Router# hw-module session slot/card
Router# hw-module session 0/1 endpoint 0

Establishing session connect to subslot 0/1
```

- 次に、キーボードで **Ctrl-A** を押した後に **Ctrl-Q** を押して、ルータからセッションを終了する例を示します。

```
type ^a^q
picocom v1.4

port is         : /dev/ttyDASH2
```

```
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : ascii_xfr -s -v -l10
receive_cmd is : rz -vv
```

活性挿抜（OIR）

ルータはCisco拡張サービス モジュールおよびCiscoネットワーク インターフェイス モジュールの活性挿抜（OIR）をサポートしています。OIR機能を使用して、次の作業を実行できます。

（注） ISR-WAAS が動作している場合は、活性挿抜（OIR）を実行しないでください。

モジュールの活性挿抜の準備

ルータでは、装着されている別のモジュールの取り外しに関係なく、モジュールの活性挿抜（OIR）がサポートされています。つまり、アクティブなモジュールをルータに装着したままで、別のモジュールをいずれかのサブスロットから取り外すことができます。モジュールを直ちに交換する予定がない場合は、サブスロットにブランク フィラー プレートを必ず取り付けてください。

モジュールの非アクティブ化

先にモジュールを非アクティブ化することなく、ルータからモジュールを取り外すことができます。ただし、モジュールを取り外す前に、モジュールを正しく非アクティブにすること（またはグレースフルに電源をオフにすること）を推奨します。正常に非アクティブにするには、EXEC モードで **hw-module subslot** *slot/subslot* **stop** コマンドを実行します。

（注） モジュールのOIRを準備しているときには、モジュールを非アクティブ化する前に各インターフェイスを個別にシャット ダウンする必要はありません。EXEC モードで **hw-module subslot** *slot/subslot* **stop** コマンドを実行すると、インターフェイスのトラフィックが自動的に停止し、OIR に備えてモジュールと共にこれらのインターフェイスが非アクティブ化されます。同様に、OIR の後にモジュールのインターフェイスを個別に再起動する必要はありません。

次の例では、**show facility-alarm status** コマンドを使用して、モジュールがシステムから取り外された時点でクリティカルアラームが生成されるかどうかを確認します。

```
Router# show facility-alarm status
System Totals  Critical: 5  Major: 1  Minor: 0

Source                  Severity      Description [Index]
------                  --------      -------------------
Power Supply Bay 1      CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/1    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/2    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3    CRITICAL      Physical Port Link Down [1]
xcvr container 0/0/0    INFO          Transceiver Missing [0]
xcvr container 0/0/1    INFO          Transceiver Missing [0]
xcvr container 0/0/2    INFO          Transceiver Missing [0]
xcvr container 0/0/3    INFO          Transceiver Missing [0]
V: 1.0v PCH R0/18       MAJOR         Volt Above Normal [3]
```

（注） 正しい非アクティブ化の後にモジュールを取り外した場合でも、クリティカルアラーム（Active Card Removed OIR Alarm）が生成されます。

いくつかのコマンド モードでのモジュールおよびインターフェイスの非アクティブ化

次のいずれかのモードで **hw-module subslot** コマンドを使用して、モジュールとそのインターフェイスを非アクティブにすることができます。

- グローバル コンフィギュレーション モードで **hw-module subslot** *slot/subslot* **shutdown unpowered** コマンドを実行してモジュールとそのインターフェイスを非アクティブにする場合は、ルータを何度リブートしてもモジュールがブートしないように設定を変更することができます。リモート場所に設置されているモジュールをシャットダウンする必要がある場合、ルータのリブート時にモジュールが自動的にブートしないようにするには、このコマンドが役立ちます。
- EXEC モードで **hw-module subslot** *slot/subslot* **stop** コマンドを使用すると、モジュールが正常にシャットダウンされます。**hw-module subslot** *slot/subslot* **start** コマンドを実行すると、モジュールがリブートされます。

モジュールを取り外す前に、モジュールとそのインターフェイスをすべて非アクティブにするには、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。

手順

	コマンドまたはアクション	目的
ステップ 1	**hw-module subslot** *slot*/*subslot* **shutdown unpowered** 例： `Router# hw-module subslot 0/2 shutdown unpowered`	ルータの指定のスロットおよびサブスロットに装着されているモジュールを非アクティブにします。ここで、 • *slot*：モジュールが装着されているシャーシスロット番号を指定します。 • *subslot*：モジュールが装着されているシャーシのサブスロット番号を指定します。 • **shutdown**：指定したモジュールをシャットダウンします。 • **unpowered**：実行コンフィギュレーションからモジュールのすべてのインターフェイスを削除し、モジュールの電源をオフにします。
ステップ 2	**hw-module subslot** *slot*/*subslot* [**reload** | **stop** | **start**] 例： `Router# hw-module subslot 0/2 stop`	指定のスロットおよびサブスロットに装着されたモジュールを非アクティブにします。ここで、 • *slot*：モジュールが装着されているシャーシスロット番号を指定します。 • *subslot*：モジュールが装着されているシャーシのサブスロット番号を指定します。 • **reload**：指定したモジュールを停止してから再起動します。 • **stop**：モジュールからすべてのインターフェイスを削除し、モジュールの電源をオフにします。 • **start**：指定のスロットに物理的に装着されたモジュールの場合と同様に、モジュールの電源をオンにします。モジュール ファームウェアがリブートし、モジュール初期化シーケンス全体がIOMd および Input/Output Module daemon（IOSd）プロセスで実行されます。

SSD/HDD キャリア カード NIM の非アクティブ化および再アクティブ化

次の制約事項が適用されます。

- HDD または SSD ディスクのない状態で SSD/HDD キャリア カード NIM を非アクティブ化または再アクティブ化する操作はサポートされていません。

- 1 つの（SSD または HDD）キャリア カード NIM だけをベイに装着できます。追加の（SSD または HDD）キャリア カード NIM を別のベイに接続すると、モジュールの電源がオフになり、カーネル メッセージ、ログ メッセージ、またはエラー メッセージが Cisco IOS コンソールに表示されます。追加のドライブでファイル システムが破損することが稀にあります。

⚠

注意 SSD/HDD キャリア カード NIM を非アクティブ化すると、データが失われることがあります。

SSD/HDD キャリア カード NIM を非アクティブ化するには、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	**virtual-service** *name* **例**： `Router(config)# virtual-service my-kwaas-instance`	**no activate** コマンドでルータをシャットダウンするための準備として、ルータでサポートされている kWAAS サービスを（名前で）指定します。SSD または HDD を装着し直したり交換したりする前に、このコマンドを使用することをお勧めします。
ステップ 2	**no activate** **例**： `Router(config-virt-serv)# no activate`	ルータの kWAAS インスタンスをシャットダウンします。kWAAS サービスはインストールされたままになります。HDD/SSD NIM（モジュール）の再起動後に、このサービスを再アクティブ化する必要があります。

ステップ 3	**hw-module subslot** *slot*/*subslot* [**reload** | **stop** | **start**]
	例：
	`Router# hw-module subslot 0/2 stop`
	`Proceed with stop of module? [confirm]`
	`Router#`
	`*Mar 6 15:13:23.997: %SPA_OIR-6-OFFLINECARD: SPA (NIM-SSD) offline in subslot 0/2`
	`...`
		指定のスロットおよびサブスロットのモジュールを非アクティブまたはアクティブにします。
		• *slot*：モジュールが装着されているシャーシのスロット番号。
		• *subslot*：モジュールが装着されているシャーシのサブスロット番号。
		• **reload**：指定のモジュールを非アクティブにしてから再アクティブ化（停止してから再起動）します。
		• **stop**：モジュールからすべてのインターフェイスを削除し、モジュールの電源をオフにします。
		• **start**：指定のスロットに物理的に装着されたモジュールの場合と同様に、モジュールの電源をオンにします。モジュール ファームウェアがリ

	コマンドまたはアクション	目的
		ブートし、モジュール初期化シーケンス全体が IOSd および IOMd プロセスで実行されます。
ステップ 4	EN（Enable） LED が消灯するまで待ち、その後 SSD/HDD キャリア カード NIM を取り外してください。	

モジュールの再アクティブ化

hw-module subslot *slot/subslot* **stop** コマンドを使用してモジュールを非アクティブにした後に、OIR を実行せずにモジュールを再アクティブ化するには、次のいずれかのコマンドを（特権 EXEC モードで）使用します。

- **hw-module subslot** *slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

モジュールの非アクティブ化およびアクティブ化の確認

モジュールを非アクティブにすると、対応するインターフェイスも非アクティブになります。そのため、これらのインターフェイスは **show interface** コマンドの出力に表示されなくなります。

1. モジュールが非アクティブになったかどうかを確認するには、特権 EXEC コンフィギュレーション モードで **show hw-module subslot all oir** コマンドを入力します。

   確認するモジュールに対応した [Operational Status] フィールドを調べます。次の例では、ルータのサブスロット 1 に装着されているモジュールが管理上、ダウン状態になっています。

```
Router# show hw-module subslot all oir

Module         Model              Operational Status

-------------- ------------------ -------------------------

subslot 0/0    ISR4451-4X1GE      ok
subslot 1/0    SM-X-T1/E1         ok
```

2. モジュールがアクティブ化されて適切に動作していることを確認するには、**show hw-module subslot all oir** コマンドを入力して、次の例のように [Operational Status] フィールドに「ok」と表示されるかどうかを調べます。

```
Router# show hw-module subslot all oir

Module         Model               Operational Status

-------------- ------------------  -------------------------

subslot 0/1    NIM-8MFT-T1/E1      ok
subslot 1/0    SM-X T1/E1          ok

Router# show platform hardware backplaneswitch-manager R0 status
```

```
slot  bay   port   enable   link status   speed(Mbps)   duplex   autoneg   pause_tx
   pause_rx   mtu
------------------------------------------------------------------------------------------
0      0     CP     True       Up           1000          Full    ENABLED    ENABLED
    ENABLED   10240
1      0     GE1    True       Up           1000          Full    DISABLED   ENABLED
    ENABLED   10240
1      0     GE0    True       Up           1000          Full    DISABLED   ENABLED
    ENABLED   10240
2      0     GE1    True       Up           1000          Full    DISABLED   ENABLED
    ENABLED   10240
2      0     GE0    True       Up           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      1     GE1    True     Down           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      1     GE0    True     Down           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      2     GE1    True     Down           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      2     GE0    True     Down           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      3     GE1    True     Down           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      3     GE0    True     Down           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      4     GE1    True     Down           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      4     GE0    True     Down           1000          Full    DISABLED   ENABLED
    ENABLED   10240
0      0     FFP    True       Up          10000          Full    ENABLED    DISABLED
   DISABLED  10240
slot  bay   port            mac    vid   modid     flags - Layer 2
-------------------------------------------------------------------------------
0      0    FFP  2c54.2dd2.661b   2351       1              0x20
0      0    FFP  2c54.2dd2.661b   2352       1              0x20
0      0     CP  2c54.2dd2.661e   2351       0              0xC60
0      0     CP  2c54.2dd2.661e   2352       0              0x20
1      0    GE0  58bf.ea3a.00f6   2350       0              0x460
0      0    FFP  2c54.2dd2.661b   2350       1              0x20
1      0    GE0  58bf.ea3a.00f6   2352       0              0x20
0      0     CP  2c54.2dd2.661e   2350       0              0x20
1      0    GE0  58bf.ea3a.00f6   2351       0              0xC60
Port block masks: rows=from port, columns=to port, u=unknown unicast, m=unknown
multicast, b=broadcast, A=all

           CP    FFP  1/0/1  1/0/0  2/0/1  2/0/0  0/1/1  0/1/0  0/2/1  0/2/0  0/3/1
  0/3/0  0/4/1 0/4/0 drops
-------------------------------------------------------------------------------------------
CP          -     A     um     um     um     um     um     um     um     um     um
    um     um     um      1
FFP         A     -      -      -      -      -      -      -      -      -      -
     -      -      -      0
1/0/1      um    umb      -    umb    umb    umb    umb    umb    umb    umb    umb
   umb    umb    umb      0
1/0/0      um    umb    umb      -    umb    umb    umb    umb    umb    umb    umb
   umb    umb    umb      6
2/0/1      um    umb    umb    umb      -    umb    umb    umb    umb    umb    umb
   umb    umb    umb      0
2/0/0      um    umb    umb    umb    umb      -    umb    umb    umb    umb    umb
   umb    umb    umb      6
0/1/1      um    umb    umb    umb    umb    umb      -    umb    umb    umb    umb
   umb    umb    umb      0
0/1/0      um    umb    umb    umb    umb    umb    umb      -    umb    umb    umb
   umb    umb    umb      0
```

```
  0/2/1       um     umb    umb     umb     umb     umb     umb     umb      -      umb     umb
     umb     umb     umb      0
  0/2/0       um     umb    umb     umb     umb     umb     umb     umb     umb     -       umb
     umb     umb     umb      0
  0/3/1       um     umb    umb     umb     umb     umb     umb     umb     umb     umb      -
     umb     umb     umb      0
  0/3/0       um     umb    umb     umb     umb     umb     umb     umb     umb     umb     umb
      -      umb     umb      0
  0/4/1       um     umb    umb     umb     umb     umb     umb     umb     umb     umb     umb
     umb      -      umb      0
  0/4/0       um     umb    umb     umb     umb     umb     umb     umb     umb     umb     umb
     umb     umb      -       0

  Port VLAN membership: [untagged vlan] U=untagged T=tagged <VLAN range begin>-<VLAN
  range end>

      CP [2352] U:0001-0001 T:0002-2351 U:2352-2352 T:2353-4095
     FFP [2352] T:0001-4095
   1/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   1/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   2/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   2/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   0/1/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   0/1/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   0/2/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   0/2/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   0/3/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   0/3/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   0/4/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
   0/4/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
```

show platform hardware backplaneswitch-manager rp active ffp statistics：例

```
Router# show platform hardware backplaneswitch-manager rp active ffp statistics
Broadcom 10G port(e.g: FFP) status:
                          Rx pkts          Rx Bytes          Tx Pkts          Tx Bytes
-------------------------------------------------------------------------------------
All                             0                 0                0                 0
  =64                           0                                  0
  65~127                        0                                  0
  128~255                       0                                  0
  256~511                       0                                  0
  512~1023                      0                                  0
  1024~1518                     0                                  0
  1519~2047                     0                                  0
  2048~4095                     0                                  0
  4096~9216                     0                                  0
  9217~16383                    0                                  0
  Max                           0                                  0
Good                            0                                  0
  CoS 0                                                            0                 0
  CoS 1                                                            0                 0
  CoS 2                                                            0                 0
  CoS 3                                                            0                 0
  CoS 4                                                            0                 0
  CoS 5                                                            0                 0
  CoS 6                                                            0                 0
  CoS 7                                                            0                 0
  Unicast                       0                                  0
  Multicast                     0                                  0
  Broadcast                     0                                  0
  Control                       0
```

```
Errored
  FCS                        0                                   0
  Undersize                  0
  Ether len                  0
  Fragment                   0                                   0
  Jabber                     0
  MTU ck, good               0
  MTU ck, bad                0
  Tx underflow                                                                  0
  err symbol                 0
  frame err                  0
  junk                       0
Drops
  CoS 0                                                          0              0
  CoS 1                                                          0              0
  CoS 2                                                          0              0
  CoS 3                                                          0              0
  CoS 4                                                          0              0
  CoS 5                                                          0              0
  CoS 6                                                          0              0
  CoS 7                                                          0              0
  STP                        0
  backpress                  0
  congest                    0                  0
  purge/cell                 0
  no destination             0
Pause PFC                    0                                   0
  CoS 0                      0
  CoS 1                      0
  CoS 2                      0
  CoS 3                      0
  CoS 4                      0
  CoS 5                      0
  CoS 6                      0
  CoS 7                      0
```

モジュールおよびインターフェイスの管理

ルータはさまざまなモジュールをサポートしています。サポートされるモジュールの一覧については、サポートされるモジュール（378 ページ）を参照してください。モジュール管理プロセスでは、モジュールのリソースを利用できるよう、モジュールを起動する操作が行われます。このプロセスは、モジュールの検出、認証、クライアントによる設定、ステータス の報告、リカバリなどのタスクから成ります。モジュール設定の詳細については、『Documentation Roadmap for the Cisco 4000 Series Integrated Services Routers』に記載されているモジュールのマニュアルを参照してください。

ルータでサポートされる Small Form-Factor Pluggable（SFP） モジュールの一覧については、『Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers』の「Installing and Upgrading Internal Modules and FRUs」の項を参照してください。

ここでは、モジュールとインターフェイスの管理に関する追加情報を示します。

- モジュール インターフェイスの管理 （392 ページ）
- バックプレーン スイッチを使用したモジュールとインターフェイスの管理 （392 ページ）

モジュール インターフェイスの管理

モジュールの稼動後に、そのモジュール インターフェイスを制御および監視できます。インターフェイス管理には、**shut** または **no shut** コマンドを使用したクライアントの設定や、インターフェイスの状態およびインターフェイスレベルの統計情報のレポートが含まれます。

モジュールおよびインターフェイスの監視とトラブルシューティング（396ページ）にリストされている **show** コマンドを使用して、モジュールの状態や他の統計情報を監視します。

バックプレーンスイッチを使用したモジュールとインターフェイスの管理

バックプレーン イーサネット スイッチ

ルータのバックプレーンイーサネットスイッチにより、拡張サービスモジュールとネットワーク インターフェイス モジュール（NIM）を接続できます。バックプレーン イーサネット スイッチは、ホスト ルータとその着脱可能モジュールの間のすべてのパケット転送を促進します。

バックプレーン イーサネット スイッチはホスト ルータの管理機能として動作し、モジュールを制御し、モジュールとの間で論理フロー制御情報を交換します。これにより、ルータ機能に正確なフィードバックが提供されます。詳細については、「モジュールおよびインターフェイスの管理 （391ページ）」を参照してください。また、バックプレーン イーサネット スイッチは、ホスト ルータからモジュールへの制御プレーン トラフィック フローも促進します。バックプレーン スイッチはモジュールおよびインターフェイス カードを管理し、モジュールとの通信に使用されます。パケット フローと制御トラフィック バッファリングを設定するため、モジュール ドライバがバックプレーン スイッチと統合されます。

バックプレーン スイッチに対して設定タスクを実行する必要はありません。モジュールから、すべての設定を行います。この設定によりバックプレーン スイッチが変更されることも、変更されないこともあります。アダプタの装着の詳細については、『Hardware Installation Guide for the Cisco ISR 4000 Series Integrated Services Routers』を参照してください。

（注） IEEE 802.1D Spanning Tree Protocol（STP）などのレイヤ 2 プロトコルは、バックプレーン イーサネット スイッチではサポートされません。

ルータ上のモジュールおよびインターフェイス カード ステータスの表示

特権 EXEC モードで **show platform** コマンドを使用して、モジュールおよびインターフェイス カードの詳細を表示できます。

次の例は、**show platform** コマンドの出力例です。

```
Router# show platform
Chassis type: ISR4451/K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4451/K9          ok                    15:57:33
 0/0      ISR4451-4X1GE       ok                    15:55:24
 0/3      NIM-SSD             ok                    15:55:24
1         ISR4451/K9          ok                    15:57:33
 1/0      SM-1T3/E3           ok                    15:55:24
2         ISR4451/K9          ok                    15:57:33
 2/0      SM-1T3/E3           ok                    15:55:24
R0        ISR4451/K9          ok, active            15:57:33
F0        ISR4451-FP          ok, active            15:57:33
P0        Unknown             ps, fail              never
P1        XXX-XXXX-XX         ok                    15:56:58
P2        ACS-4450-ASSY       ok                    15:56:58

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         12090323            15.3(01r)S            [ciscouser-ISRRO...
1         12090323            15.3(01r)S            [ciscouser-ISRRO...
2         12090323            15.3(01r)S            [ciscouser-ISRRO...
R0        12090323            15.3(01r)S            [ciscouser-ISRRO...
F0        12090323            15.3(01r)S            [ciscouser-ISRRO...
```

バックプレーン スイッチ統計情報の表示

各スロットの統計情報レポートには、着信および発信されたパケット数またはバイト数が示されます。この情報を使用して、バックプレーン スイッチのさまざまなポートでのトラフィック フローを調べることができます。次に、**show platform hardware backplaneswitch-manager rp active summary** コマンドの出力例を示します。

```
Router# show platform hardware backplaneswitch-manager rp active summary
slot     bay       port         InBytes          InPkts         OutBytes         OutPkts

-------------------------------------------------------------------------------------

   0       0         CP            6242         9361008             6241          403209

   1       0        GE1               0               0                0
0
   1       0        GE0            6306          407477             6241         9360934

   2       0        GE1               0               0                0
0
   2       0        GE0               0               0                0
0
   0       1        GE1               0               0                0
0
   0       1        GE0               0               0                0
0
   0       2        GE1               0               0                0
0
```

```
   0       2        GE0              0              0              0
0
   0       3        GE1              0              0              0
0
   0       3        GE0              0              0              0
0
   0       4        GE1              0              0              0
0
   0       4        GE0              0              0              0
0
   0       0        FFP              0              0              0
0
   0       0        FFP              0              0              0
0
```

バックプレーン スイッチ ポート統計情報の表示

バックプレーンスイッチに接続しているポートに関連する統計情報を表示するには、**show platform hardware backplaneswitch-manager rp active subslot GEO statistics** コマンドを使用できます。次の例は、バックプレーン スイッチと、このスイッチに接続しているポートに関連する統計情報を表示します。

```
Router# show platform hardware backplaneswitch-manager rp active subslot 1/0 GE0 statistics
Broadcom 1G port(e.g: NIM, ESM, CP) status:
                          Rx pkts         Rx Bytes          Tx Pkts         Tx Bytes
-------------------------------------------------------------------------------------
All                          6306           407477             6241          9360934
  =64                        6237                               72
  65~127                       66                                3
  128~255                       0                                0
  256~511                       1                                3
  512~1023                      2                                0
  1024~1518                     0                             6163
  1519~2047                     0                                0
  2048~4095                     0                                0
  4096~9216                     0                                0
Good                         6306                             6241
  CoS 0                                                       6171          9356426
  CoS 1                                                          0                0
  CoS 2                                                          0                0
  CoS 3                                                          0                0
  CoS 4                                                          0                0
  CoS 5                                                          0                0
  CoS 6                                                         70             4508
  CoS 7                                                          0                0
  Unicast                    6294                             6241
  Multicast                     6                                0
  Broadcast                     6                                0
  Control                       0                                0
  VLAN                          0                                0
Errored
  FCS                           0                                0
  Runts                         0               0
  Undersize                     0
  Ether len                     0
  Fragment                      0                                0
  Jabber                        0                                0
  MTU                           0
Drops
  CoS 0                                                          0                0
  CoS 1                                                          0                0
```

```
  CoS 2                                                          0              0
  CoS 3                                                          0              0
  CoS 4                                                          0              0
  CoS 5                                                          0              0
  CoS 6                                                          0              0
  CoS 7                                                          0              0
  STP                          0
  backpress                    0
  congest                      0               0
  purge/cell                   0
  no destination              65
Pause                          0                               0
```

スロット割り当ての表示

スロット割り当てを表示するには、次の例に示すように特権 EXEC モードで **show inventory** コマンドを使用します。

```
Router# show inventory
NAME: "Chassis", DESCR: "Cisco ISR4451 Chassis"
PID: ISR4451/K9         , VID: V01, SN: FGL163910CM

NAME: "Power Supply Module 1", DESCR: "Cisco 4451-X ISR 450W AC Power Supply"
PID: XXX-XXXX-XX        , VID: XXX, SN: DCA1623X05N

NAME: "Fan Tray", DESCR: "Cisco 4451-X ISR Fan tray"
PID: ACS-4450-FANASSY   , VID:    , SN:

NAME: "module 0", DESCR: "Cisco ISR4451 Built-In NIM controller"
PID: ISR4451/K9         , VID:    , SN:

NAME: "NIM subslot 0/1", DESCR: " NIM-1MFT-T1/E1 - T1/E1 Serial Module"
PID:  NIM-1MFT-T1/E1    , VID: V01, SN: FOC16254E71

NAME: "subslot 0/1 db module 0", DESCR: "PVDM4-TDM-280 Voice DSP Module"
PID: PVDM4-TDM-280      , VID: V01, SN: FOC16290GRT

NAME: "NIM subslot 0/0", DESCR: "Front Panel 4 ports Gigabitethernet Module"
PID: ISR4451-X-4x1GE    , VID: V01, SN: JAB092709EL

NAME: "module 1", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451/K9         , VID:    , SN:

NAME: "module 2", DESCR: "Cisco ISR4451 Built-In SM controller"
PID: ISR4451/K9         , VID:    , SN:

NAME: "SM subslot 2/0", DESCR: "SM-X-1T3/E3 - Clear T3/E3 Serial Module"
PID: SM-1T3/E3          , VID: V01, SN: FOC15495HSE

NAME: "module R0", DESCR: "Cisco ISR 4451-X Route Processor"
PID: ISR4451/K9         , VID: V01, SN: FOC163679GH

NAME: "module F0", DESCR: "Cisco ISR4451-X Forwarding Processor"
PID: ISR4451/K9         , VID:    , SN:
```

（注） Cisco ISR 4321 は、**show inventory** コマンドにより、電源およびファントレイのシリアル番号が表示されません。

モジュールおよびインターフェイスの監視とトラブルシューティング

モジュールおよびインターフェイスの監視とトラブルシューティングを行うには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

- **show platform**
- **show platform software backplaneswitch-manager RP [active [detail]]**
- **show platform hardware backplaneswitch-manager RPactive CP statistics**
- **show platform hardware backplaneswitch-manager RP active summary**
- **show platform hardware backplaneswitch-manager [R0 [status] | RP]**
- **show diag all eeprom details**

show platform

```
Router# show platform
Chassis type: ISR4451/K9

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ISR4451/K9          ok                    15:57:33
 0/0      ISR4451-4X1GE       ok                    15:55:24
1         ISR4451/K9          ok                    15:57:33
 1/0      SM-1T3/E3           ok                    15:55:24
2         ISR4451/K9          ok                    15:57:33
 2/0      SM-1T3/E3           ok                    15:55:24
R0        ISR4451/K9          ok, active            15:57:33
F0        ISR4451-FP          ok, active            15:57:33
P0        Unknown             ps, fail              never
P1        XXX-XXXX-XX         ok                    15:56:58
P2        ACS-4450-FANASSY    ok                    15:56:58

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         12090323            15.3(01r)S            [ciscouser-ISRRO...
1         12090323            15.3(01r)S            [ciscouser-ISRRO...
2         12090323            15.3(01r)S            [ciscouser-ISRRO...
R0        12090323            15.3(01r)S            [ciscouser-ISRRO...
F0        12090323            15.3(01r)S            [ciscouser-ISRRO...
```

表 *39 : show platform* のフィールドの説明

フィールド	説明
スロット	スロット番号
タイプ	モジュールのタイプ
状態	モジュールのステータス

フィールド	説明
Insert Time	モジュールの起動後の経過時間

show platform software backplaneswitch-manager RP [active [detail]]

```
Router# show platform software backplaneswitch-manager RP active detail
BSM Software Display

 module port   port type  alien type    traf type
-------------------------------------------------
       0/1/0        NGIO       TRUNK         NGIO
       0/1/1        NGIO       TRUNK         NGIO
       0/2/0        NGIO       TRUNK         NGIO
       0/2/1        NGIO       TRUNK         NGIO
       0/3/0        NGIO       TRUNK         NGIO
       0/3/1       ALIEN       TRUNK         NGIO
       0/4/0        NGIO       TRUNK         NGIO
       0/4/1        NGIO       TRUNK         NGIO
       1/0/0        NGIO       TRUNK         NGIO
       1/0/1        NGIO       TRUNK         NGIO
       2/0/0        NGIO       TRUNK         NGIO
       2/0/1        NGIO       TRUNK         NGIO
```

show platform hardware backplaneswitch-manager RPactive CP statistics

```
Router# show platform hardware backplaneswitch-manager RP active CP statistics
Broadcom 1G port(e.g:  NIM, NGSM, CP) status:
                          Rx pkts         Rx Bytes          Tx Pkts         Tx Bytes
-------------------------------------------------------------------------------------
All                          6242          9361008             6241           403209
  =64                          72                              6178
  65~127                        4                                60
  128~255                       0                                 0
  256~511                       3                                 1
  512~1023                      0                                 2
  1024~1518                  6163                                 0
  1519~2047                     0                                 0
  2048~4095                     0                                 0
  4096~9216                     0                                 0
Good                         6242                              6241
  CoS 0                                                           0               0
  CoS 1                                                           0               0
  CoS 2                                                           0               0
  CoS 3                                                        6241          403209
  CoS 4                                                           0               0
  CoS 5                                                           0               0
  CoS 6                                                           0               0
  CoS 7                                                           0               0
  Unicast                    6241                              6235
  Multicast                     1                                 0
  Broadcast                     0                                 6
  Control                       0                                 0
  VLAN                          0                                 0
Errored
  FCS                           0                                 0
  Runts                         0               0
  Undersize                     0
  Ether len                     0
  Fragment                      0                                 0
  Jabber                        0                                 0
  MTU                           0
```

```
Drops
  CoS 0                                                    0                0
  CoS 1                                                    0                0
  CoS 2                                                    0                0
  CoS 3                                                    0                0
  CoS 4                                                    0                0
  CoS 5                                                    0                0
  CoS 6                                                    0                0
  CoS 7                                                    0                0
  STP                          0
  backpress                    0
  congest                      0               0
  purge/cell                   0
  no destination               1
Pause                          0                          0
```

show platform hardware backplaneswitch-manager RP active summary

```
Router# show platform hardware backplaneswitch-manager RP active summary
  slot     bay          port           InBytes            InPkts         OutBytes  OutPkts

-------------------------------------------------------------------------------------------

     0       0            CP               242                 0                0   0

     1       0           GE1                 0                 0                0   0

     1       0           GE0                 0                 0                0   0

     2       0           GE1                 0                 0                0   0

     2       0           GE0                 0                 0                0   0

     0       1           GE1                 0                 0                0   0

     0       1           GE0                 0                 0                0   0

     0       2           GE1                 0                 0                0   0

     0       2           GE0                 0                 0                0   0

     0       3           GE1                 0                 0                0   0

     0       3           GE0                 0                 0                0   0

     0       4           GE1                 0                 0                0   0

     0       4           GE0                 0                 0                0   0

     0       0           FFP                 0                 0                0   0
```

show platform hardware backplaneswitch-manager [R0 [status] | RP]

```
Router# show platform hardware backplaneswitch-manager R0 status
slot  bay   port   enable   link status   speed(Mbps)   duplex   autoneg   pause_tx
pause_rx   mtu
-------------------------------------------------------------------------------------------------
0      0     CP     True      Up           1000          Full    ENABLED    ENABLED
ENABLED   10240
1      0     GE1    True      Up           1000          Full    DISABLED   ENABLED
ENABLED   10240
1      0     GE0    True      Up           1000          Full    DISABLED   ENABLED
```

```
ENABLED   10240
2       0      GE1     True       Up            1000           Full     DISABLED   ENABLED
ENABLED   10240
2       0      GE0     True       Up            1000           Full     DISABLED   ENABLED
ENABLED   10240
0       1      GE1     True      Down           1000           Full     DISABLED   ENABLED
ENABLED   10240
0       1      GE0     True      Down           1000           Full     DISABLED   ENABLED
ENABLED   10240
0       2      GE1     True      Down           1000           Full     DISABLED   ENABLED
ENABLED   10240
0       2      GE0     True      Down           1000           Full     DISABLED   ENABLED
ENABLED   10240
0       3      GE1     True      Down           1000           Full     DISABLED   ENABLED
ENABLED   10240
0       3      GE0     True      Down           1000           Full     DISABLED   ENABLED
ENABLED   10240
0       4      GE1     True      Down           1000           Full     DISABLED   ENABLED
ENABLED   10240
0       4      GE0     True      Down           1000           Full     DISABLED   ENABLED
ENABLED   10240
0       0      FFP     True        Up          10000           Full     ENABLED    DISABLED
DISABLED  10240
slot  bay   port             mac     vid   modid     flags - Layer 2
--------------------------------------------------------------------------------
0       0     FFP  2c54.2dd2.661b   2351       1              0x20
0       0     FFP  2c54.2dd2.661b   2352       1              0x20
0       0      CP  2c54.2dd2.661e   2351       0              0xC60
0       0      CP  2c54.2dd2.661e   2352       0              0x20
1       0     GE0  58bf.ea3a.00f6   2350       0              0x460
0       0     FFP  2c54.2dd2.661b   2350       1              0x20
1       0     GE0  58bf.ea3a.00f6   2352       0              0x20
0       0      CP  2c54.2dd2.661e   2350       0              0x20
1       0     GE0  58bf.ea3a.00f6   2351       0              0xC60
Port block masks: rows=from port, columns=to port, u=unknown unicast, m=unknown multicast,
 b=broadcast, A=all

            CP    FFP  1/0/1  1/0/0  2/0/1  2/0/0  0/1/1  0/1/0  0/2/1  0/2/0  0/3/1
0/3/0  0/4/1 0/4/0 drops
--------------------------------------------------------------------------------------------------------------
CP           -     A     um     um     um     um     um     um     um     um     um
um     um     um     1
FFP          A     -      -      -      -      -      -      -      -      -      -
 -      -      -     0
1/0/1        um    umb     -     umb    umb    umb    umb    umb    umb    umb    umb
umb    umb    umb     0
1/0/0        um    umb    umb     -     umb    umb    umb    umb    umb    umb    umb
umb    umb    umb     6
2/0/1        um    umb    umb    umb     -     umb    umb    umb    umb    umb    umb
umb    umb    umb     0
2/0/0        um    umb    umb    umb    umb     -     umb    umb    umb    umb    umb
umb    umb    umb     6
0/1/1        um    umb    umb    umb    umb    umb     -     umb    umb    umb    umb
umb    umb    umb     0
0/1/0        um    umb    umb    umb    umb    umb    umb     -     umb    umb    umb
umb    umb    umb     0
0/2/1        um    umb    umb    umb    umb    umb    umb    umb     -     umb    umb
umb    umb    umb     0
0/2/0        um    umb    umb    umb    umb    umb    umb    umb    umb     -     umb
umb    umb    umb     0
0/3/1        um    umb    umb    umb    umb    umb    umb    umb    umb    umb     -
umb    umb    umb     0
0/3/0        um    umb    umb    umb    umb    umb    umb    umb    umb    umb    umb
-     umb    umb     0
```

```
0/4/1       um     umb    umb     umb     umb     umb     umb     umb     umb     umb     umb
umb      -      umb      0
0/4/0       um     umb    umb     umb     umb     umb     umb     umb     umb     umb     umb
umb     umb      -       0

Port VLAN membership: [untagged vlan] U=untagged T=tagged <VLAN range begin>-<VLAN range
 end>

    CP [2352] U:0001-0001 T:0002-2351 U:2352-2352 T:2353-4095
   FFP [2352] T:0001-4095
 1/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 1/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 2/0/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 2/0/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/1/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/1/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/2/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/2/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/3/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/3/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/4/1 [2352] T:0002-2351 U:2352-2352 T:2353-4095
 0/4/0 [2352] T:0002-2351 U:2352-2352 T:2353-4095
```

show diag all eeprom details

```
Router# show diag all eeprom details
MIDPLANE EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        PCB Serial Number        : FOC15520B7L
        Controller Type          : 1902
        Hardware Revision        : 1.0
        PCB Part Number          : 73-13854-02
        Top Assy. Part Number    : 800-36894-01
        Board Revision           : 05
        Deviation Number         : 123968
        Fab Version              : 02
        Product Identifier (PID) : ISR4451/K9
        Version Identifier (VID) : V01
        CLEI Code                : TDBTDBTDBT
        Processor type           : D0
        Chassis Serial Number    : FGL1601129D
        Chassis MAC Address      : 30f7.0d53.c7e0
        MAC Address block size   : 144
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Asset ID                 : P1B-R2C
Power/Fan Module P0 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1509
        Unknown Field (type 00DF): 1.85.1.236.1
        Deviation Number         : 0
        PCB Serial Number        : DCA1547X037
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Version Identifier (VID) : XXX
        Product Identifier (PID) : XXX-XXXX-XX
        CLEI Code                : 0000000000
        Environment Monitor Data : 41 01 C2 42 00 05 F8 00
                                   50 01 F4 1B 58 03 E8 1F
                                   4A 05 DC 21 34 07 D0 21
```

```
                                    FC 09 C4 22 60 0B B8 22
                                    92 0D AC 22 D8 0F A0 22
                                    F8 11 94 22 F6 13 88 23
                                    3C 15 7C 23 28 17 70 23
                                    00 19 64 22 D8 1B 58 22
                                    C4 1D 4C 22 BA 1F 40 22
                                    A6 21 34 22 9C 23 28 22
                                    92 25 1C 22 88 27 10 22
                                    60
        Board Revision            : P0
Power/Fan Module P1 EEPROM data is not initialized

Power/Fan Module P2 EEPROM data is not initialized

Slot R0 EEPROM data:

        EEPROM version            : 4
        Compatible Type           : 0xFF
        PCB Serial Number         : FOC15520B7L
        Controller Type           : 1902
        Hardware Revision         : 1.0
        PCB Part Number           : 73-13854-02
        Top Assy. Part Number     : 800-36894-01
        Board Revision            : 05
        Deviation Number          : 123968
        Fab Version               : 02
        Product Identifier (PID)  : ISR4451/K9
        Version Identifier (VID)  : V01
        CLEI Code                 : TDBTDBTDBT
        Processor type            : D0
        Chassis Serial Number     : FGL1601129D
        Chassis MAC Address       : 30f7.0d53.c7e0
        MAC Address block size    : 144
        Manufacturing Test Data   : 00 00 00 00 00 00 00 00
        Asset ID                  : P1B-R2C
        Asset ID                  :
Slot F0 EEPROM data:

        EEPROM version            : 4
        Compatible Type           : 0xFF
        Controller Type           : 3567
        Hardware Revision         : 4.1
        PCB Part Number           : 73-12387-01
        MAC Address block size    : 15
        Chassis MAC Address       : aabb.ccdd.eeff
        Product Identifier (PID)  : ISR4451-FP
        Version Identifier (VID)  : V00
        PCB Serial Number         : FP123456789
        Asset ID                  :
Slot 0 EEPROM data:

        EEPROM version            : 4
        Compatible Type           : 0xFF
        Controller Type           : 1612
        Hardware Revision         : 4.1
        PCB Part Number           : 73-12387-01
        MAC Address block size    : 15
        Chassis MAC Address       : aabb.ccdd.eeff
        Product Identifier (PID)  : ISR4451-NGSM
        Version Identifier (VID)  : V00
        PCB Serial Number         : NGSM1234567
        Asset ID                  :
Slot 1 EEPROM data:
```

```
        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1612
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-NGSM
        Version Identifier (VID) : V00
        PCB Serial Number        : NGSM1234567
        Asset ID                 :
Slot 2 EEPROM data:

        EEPROM version           : 4
        Compatible Type          : 0xFF
        Controller Type          : 1612
        Hardware Revision        : 4.1
        PCB Part Number          : 73-12387-01
        MAC Address block size   : 15
        Chassis MAC Address      : aabb.ccdd.eeff
        Product Identifier (PID) : ISR4451-NGSM
        Version Identifier (VID) : V00
        PCB Serial Number        : NGSM1234567
        Asset ID                 :
SPA EEPROM data for subslot 0/0:

        EEPROM version           : 5
        Compatible Type          : 0xFF
        Controller Type          : 1902
        Hardware Revision        : 2.2
        Boot Timeout             : 400 msecs
        PCB Serial Number        : JAB092709EL
        PCB Part Number          : 73-8700-01
        PCB Revision             : A0
        Fab Version              : 01
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Deviation Number         : 78409
        Product Identifier (PID) : ISR4451-4X1GE
        Version Identifier (VID) : V01
        Top Assy. Part Number    : 68-2236-01
        Top Assy. Revision       : A0
        IDPROM Format Revision   : 36
        System Clock Frequency   : 00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00
        CLEI Code                : CNUIAHSAAA
        Base MAC Address         : 00 00 00 00 00 00
        MAC Address block size   : 0
        Manufacturing Test Data  : 00 00 00 00 00 00 00 00
        Field Diagnostics Data   : 00 00 00 00 00 00 00 00
        Calibration Data         : Minimum: 0 dBmV, Maximum: 0 dBmV
              Calibration values :
        Power Consumption        : 13100 mWatts (Maximum)
        Environment Monitor Data : 03 30 0C E4 46 32 09 C4
                                   46 32 05 DC 46 32 05 DC
                                   46 32 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 FE 02 F9 6E
        Processor Label          : 00 00 00 00 00 00 00 00
        Platform features        : 00 00 00 00 00 00 00 00
```

```
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
                                   00 00 00 00 00 00 00 00
        Asset ID                 :
        Asset Alias              :
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 1/0 is not available

SPA EEPROM data for subslot 1/1 is not available

SPA EEPROM data for subslot 1/2 is not available

SPA EEPROM data for subslot 1/3 is not available

SPA EEPROM data for subslot 1/4 is not available

SPA EEPROM data for subslot 2/0 is not available

SPA EEPROM data for subslot 2/1 is not available

SPA EEPROM data for subslot 2/2 is not available

SPA EEPROM data for subslot 2/3 is not available

SPA EEPROM data for subslot 2/4 is not available
```

設定例

ここでは、モジュールを非アクティブおよびアクティブにする例を示します。

モジュール設定の非アクティブ化：例

モジュールを非アクティブにして、そのモジュールのOIRを実行できます。次に、モジュール（およびそのインターフェイス）を非アクティブにしてモジュールの電源を切断する例を示します。この例では、モジュールはルータのサブスロット0に装着されています。

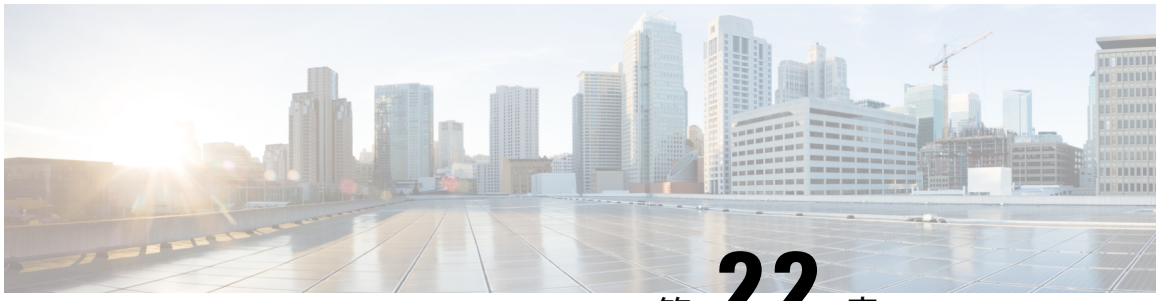
```
Router(config)# hw-module slot 1 subslot 1/0 shutdown unpowered
```

モジュール設定のアクティブ化：例

以前にモジュールを非アクティブにした場合は、そのモジュールをアクティブ化できます。OIR実行中にモジュールとそのインターフェイスを非アクティブにしなかった場合は、ルータを再アクティブ化するとモジュールが自動的に再アクティブ化されます。

次に、モジュールをアクティブにする例を示します。この例では、ルータのスロット1にあるサブスロット0にモジュールが装着されています。

```
Router(config)# hw-module slot 1 subslot 1/0 start
```



第 22 章

SFP Auto-Detect および Auto-Failover

Cisco 4000 シリーズ サービス統合型ルータ（ISR）には、銅線ケーブルとファイバ ケーブルの同時接続をサポートする Front Panel Gigabit Ethernet（FPGE）ポートがあります。ネットワークがダウンした場合に、フェールオーバー冗長性を保つようメディアを設定できます。この機能は、Cisco ISR プラットフォームでのみサポートされます。

この章は、次の項で構成されています。

Auto-Detect のイネーブル化

メディア タイプが設定されていない場合、デフォルトで Auto-Detect 機能がイネーブルになります。Auto-Detect機能は、接続されているメディアを自動的に検出してリンクアップします。両方のメディアが接続されている場合、最初に起動したメディアがリンクされます。デフォルトでは、FPGE ポートのメディア タイプは auto-select に設定されます。ユーザーは FPGE インターフェイスで **media-type rj45/sfp** コマンドを使用して、メディアタイプ設定を RJ-45 または SFP に上書きできます。また、**no media-type** コマンドが設定されると、メディアタイプ設定が「Auto-select」モードに戻ります。Auto-Detect 機能をイネーブルにするには、インターフェイス コンフィギュレーション モードで **no media-type** コマンドを使用できます。

Auto-Detect の設定

Auto-Detect機能は、前面パネルの Gige ポートでデフォルトでイネーブルに設定されています。「media-type auto-select」または「no media-type」を設定することで、これがイネーブルになります。Auto-Detect を設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface gigabitethernet** {**slot** | **bay** | **port**}
3. **media-type auto-select**
4. **End**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface gigabitethernet** {**slot** | **bay**| **port**} 例： `Router(config)# interface gigabitethernet slot/port`	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。
ステップ 3	**media-type auto-select** 例： `Router(config-if)# media-type auto-select`	auto-select モードでは、接続されている任意のコネクタが使用されます。次のオプションがあります。 • **rj45**：RJ45 コネクタを使用します。 • **sfp**：SFP コネクタを使用します。
ステップ 4	**End** 例： `Router(config-if)#end`	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

次に、デフォルトの設定の例を示します。「no media-type」が選択されている場合は show running configuration によりメディア タイプが表示されません。

```
Router(config)# show running interface gigabitethernet 0/0/0
Building configuration...

Current configuration : 71 bytes
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
end
```

プライマリおよびセカンダリ メディアの設定

プライマリ メディアがダウンしていることを示す通知をルータが受け取ると、セカンダリ フェールオーバー メディアがイネーブルになります。スイッチオーバー後にプライマリ メディアが復旧しても、それはプライマリ メディアに切り替わりません。**shut** コマンドまたは **no shut** コマンドを使用するか、またはモジュールをリロードして、メディアタイプをプライマリ（優先）メディアに戻す必要があります。

GE-SFP ポートでプライマリまたはセカンダリ フェールオーバー メディアを割り当てるには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface gigabitethernet** {**slot** | **port**}
3. **media-type rj45 autofailover**
4. **End**

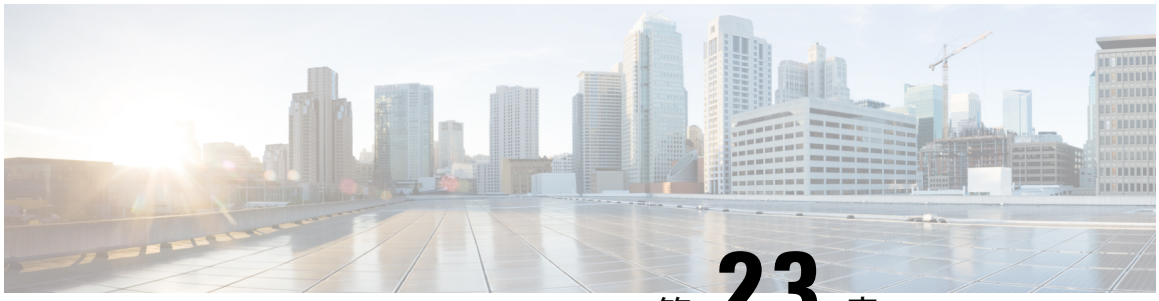
手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface gigabitethernet** {**slot** | **port**} 例： `Router(config)# interface gigabitethernet slot/port`	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。
ステップ 3	**media-type rj45 autofailover** 例： `Router(config-if)# media-type rj45 autofailover`	自動フェールオーバーのプライマリ メディアとして rj45 を指定してポートを設定します。
ステップ 4	**End** 例： `Router(config-if)#end`	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

次に、プライマリ設定の例を示します。

```
Router(config)# show running interface gigabitethernet 0/0/0
Building configuration...

Current configuration : 102 bytes
!
interface GigabitEthernet0/0/0
 no ip address
 media-type rj45 auto-failover
 negotiation auto
end
```



第 23 章

セルラー IPv6 アドレス

この章では、IPv6 アドレスの概要と、Cisco 4000 シリーズ ISR でセルラー IPv6 アドレスを設定する方法について説明します。

この章は、次の項で構成されています。

セルラー IPv6 アドレス

IPv6 アドレスは、x:x:x:x:x:x:x:x のようにコロン（:）で区切られた一連の 16 ビットの 16 進フィールドで表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:CDBA:0000:0000:0000:0000:3257:9652
- 2001:CDBA::3257:9652（ゼロは省略可能）

IPv6 アドレスには通常、連続する 16 進数のゼロのフィールドが含まれています。IPv6 アドレスの先頭、中間、または末尾にある連続した 16 進数のゼロのフィールドを圧縮するために、2 つのコロン（::）が使用されることがあります（このコロンは連続した 16 進数のゼロのフィールドを表します）。次の表に、圧縮された IPv6 アドレスの形式を示します。

IPv6 アドレス プレフィックスは、ipv6-prefix/prefix-length の形式で、アドレス空間全体のビット連続ブロックを表すために使用できます。ipv6-prefix は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:cdba::3257:9652 /64 は有効な IPv6 プレフィックスです。

IPv6 ユニキャスト ルーティング

IPv6 ユニキャスト アドレスは、単一ノード上の単一インターフェイスの識別子です。ユニキャスト アドレスに送信されたパケットは、そのアドレスが示すインターフェイスに配信されます。

Cisco 4000 シリーズ ISR は、次のアドレスタイプをサポートしています。

リンクロックアドレス

リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10（1111 1110 10）と変更された EUI-64 形式のインターフェイス識別子を使用するすべてのインターフェイスを自動的に設定できる IPv6 ユニキャスト アドレスです。IPv6 アドレスが有効になっている場合、リンクローカル アドレスはセルラーイ ンターフェイスで自動的に設定されます。

データ コールが確立されると、セルラー インターフェイスのリンクローカル アドレスは、ホストによって生成されたリンクローカル アドレス（リンクローカル プレフィックス FF80::/10 (1111 1110 10) と USB ハードウェア アドレスから自動生成されたインターフェイス識別子で構成）で更新されます。次の図は、以下のリンク ローカル アドレスの構造を示しています。

グローバル アドレス

グローバル IPv6 ユニキャスト アドレスは、グローバル ルーティング プレフィックス、サブネット ID、およびインターフェイス ID で定義されます。ルーティング プレフィックスは PGW から取得されます。インターフェイス識別子は、修正された EUI-64 形式のインターフェイス識別子を使用して、USB ハードウェア アドレスから自動的に生成されます。ルータのリロード後に、USB ハードウェア アドレスが変更されます。

セルラー IPv6 アドレスの設定

セルラー IPv6 アドレスを設定するには、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface Cellular** {**type** | **number**}
3. ip address negotiated
4. encapsulation slip
5. load-interval***seonds***
6. dialer in-band
7. dialer idle-timeout ***seonds***
8. dialer string **string**
9. dialer-group**group-number**
10. no peer default ip address
11. ipv6 address autoconfig
12. async mode interactive
13. routing dynamic
14. **dialer-listdialer-groupprotocolprotocol-name** {**permit** | deny|**list** | *access-list-number* | *access-group* }
15. **ipv6 route** *ipv6-prefix/prefix-length 128*
16. **End**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**interface Cellular** {**type** | **number**} 例： `Router(config)# interface cellular 0/1/0`	セルラー インターフェイスを指定します。
ステップ 3	ip address negotiated 例： `Router(config-if)# ipv6 address negotiated`	このインターフェイスの IP アドレスが動的に取得されるように設定します。
ステップ 4	encapsulation slip 例： `Router(config-if)# encapsulation slip`	ダイヤルオンデマンド ルーティング（DDR）に対して設定されたインターフェイスのシリアル ライン インターネット プロトコル（SLIP）カプセル化を指定します。
ステップ 5	load-interval***seonds*** 例： `Router(config-if)# load-interval 30`	（任意）負荷統計情報の計算に使用されるデータを取る時間の長さを指定します。
ステップ 6	dialer in-band 例： `Router(config-if)# dialer in-band`	DDR をイネーブルにし、インバンド ダイヤリングを使用するよう、指定したシリアル インターフェイスを設定します。
ステップ 7	dialer idle-timeout ***seonds*** 例： `Router(config-if)# dialer idle-timeout 0`	ダイヤラのアイドル タイムアウト期間を指定します。
ステップ 8	dialer string **string** 例： `Router(config-if)# dialer string lte`	ダイヤルする番号または文字列を指定します。
ステップ 9	dialer-group**group-number** 例： `Router(config-if)# dialer-group 1`	指定したインターフェイスが属するダイヤラ アクセス グループの番号を指定します。
ステップ 10	no peer default ip address 例： `Router(config-if)# no peer default ip address`	設定からデフォルトアドレスを削除します。

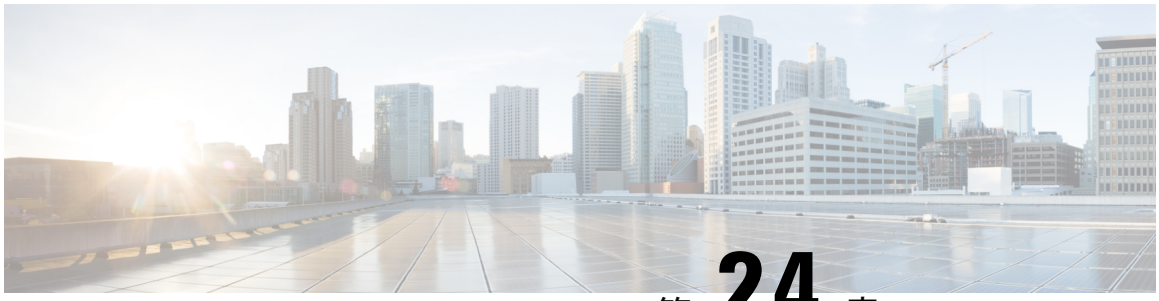
	コマンドまたはアクション	目的
ステップ 11	ipv6 address autoconfig 例： `Router(config-if)# ipv6 address autoconfig`	インターフェイスに対してステートレス自動設定を使用した IPv6 アドレスの自動設定をイネーブルにし、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 12	async mode interactive 例： `Router(config-if)# async mode interactive`	入力を提供してください。
ステップ 13	routing dynamic 例： `Router(config-if)#routing dynamic`	ルータがインターフェイスを使用して他のルータにルーティングアップデートを渡せるようにします。
ステップ 14	**dialer-listdialer-groupprotocolprotocol-name** {**permit** |deny|**list** |*access-list-number* | *access-group* } 例： `Router(config)# dialer-list 1 protocol ipv6 permit`	プロトコルによって、またはプロトコルと以前に定義したアクセス リストの組み合わせによって、ダイヤルするためのダイヤルオンデマンド ルーティング（DDR）ダイヤラ リストを定義します。
ステップ 15	**ipv6 route** *ipv6-prefix/prefix-length 128* 例： `Router(config)#ipv6 route 2001:1234:1234::3/128 Cellular0/1/0`	
ステップ 16	**End** 例： `Router(config-if)#end`	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

次の例は、セルラー IPv6 の設定を示しています。

```
Router(config)# interface Cellular0/0/0
ip address negotiated
encapsulation slip
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer-group 1
no peer default ip address
ipv6 address autoconfig
async mode interactive
routing dynamic
!
interface Cellular0/1/0
ip address negotiated
encapsulation slip
```

```
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer-group 1
no peer default ip address
ipv6 address autoconfig
async mode interactive
routing dynamic

dialer-list 1 protocol ipv6 permit
ipv6 route 2001:1234:1234::/64 Cellular0/1/0
ipv6 route 2001:4321:4321::5/128 Cellular0/1/1
```



第 24 章

無線対応ルーティング

無線対応ルーティング（RAR）は、無線がルーティングプロトコルOSPFv3と情報を交換し、1ホップルーティングネイバーのアピアランス、ディスアピアランス、およびリンク状態について信号で伝えるメカニズムです。

大規模なモバイルネットワークでは、ルーティングネイバーへの接続が距離と無線障害により中断されることがよくあります。該当する信号がルーティングプロトコルに到達しない場合、プロトコルタイマーを使用してネイバーのステータスが更新されます。ルーティングプロトコルには期間の長いタイマーがありますが、モバイルネットワークでは推奨されません。

RAR機能は、Cisco ISR G2およびG3シリーズ ルータ、Cisco ISR 4000シリーズ ルータでサポートされています。

PPPoE拡張は、Cisco 4000シリーズ ISRでサポートされるRARプロトコルです。集約によるPPPoE拡張のサポートは、Cisco IOS XE Fuji 16.7リリースから導入されています。OSPFv3およびEIGRPは、サポートされているルーティングプロトコルです。

無線対応ルーティングの利点

無線対応ルーティング機能には次のようなメリットがあります。

- 変更を即座に認識することで、ネットワーク コンバージェンスを高速化します。
- 障害の発生している、または減衰している無線リンクのルーティングを有効にします。
- ラインオブサイトパスと非ラインオブサイトパス間のルーティングを容易にします。

- 高速コンバージェンスと最適なルート選択が可能になるため、音声やビデオなど遅延の影響を受けやすいトラフィックが中断されません。
- 無線リソースと帯域幅の効率的な使用が可能になります。
- ルータで輻輳制御を実行することにより、無線リンクへの影響を軽減します。
- 無線電力の節減に基づくルート選択が可能になります。
- ルーティング機能と無線機能の分離を有効にします。
- RFC 5578、R2CP、および DLEP に準拠した無線へのシンプルなイーサネット接続を実現します。

制約事項と制限

無線対応ルーティング機能には次の制約事項と制限があります。

- DLEP および R2CP プロトコルは、Cisco 4000 シリーズ ISR ではサポートされていません。
- マルチキャストトラフィックは、集約モードではサポートされていません。
- 高可用性（HA）はサポートされていません。

ライセンス要件

この機能は、AX ライセンスで使用できます。

システム コンポーネント

無線対応ルーティング（RAR）機能は、PPPoE、仮想マルチポイント インターフェイス（VMI）、QoS、ルーティング プロトコル インターフェイス、RAR プロトコルなどのさまざまなコンポーネントで構成される MANET（モバイル アドホック ネットワーク）インフラストラクチャを使用して導入されます。

Point-to-Point Protocol over Ethernet（PPPoE）

PPPoE は、クライアントとサーバーの間の明確に定義された通信メカニズムです。RAR の導入では、無線が PPPoE クライアントの役割を果たし、ルータが PPPoE サーバーの役割を果たします。その結果、明確に定義された予測可能な通信メカニズムを提供しながら、無線とルータを疎結合することが可能になります。

PPPoE はセッションまたは接続指向プロトコルであるため、外部無線から IOS ルータへのポイントツーポイント無線周波数（RF）リンクを拡張します。

PPPoE 拡張

PPPoE 拡張は、ルータが無線と通信するときに使用されます。PPPoE の Cisco IOS 導入では、個々のセッションは仮想アクセスインターフェイス（無線ネイバーへの接続）で表され、これらの PPPoE 拡張を使用して QoS を適用できます。

RFC5578 は、信頼ベースのフロー制御とセッションベースのリアルタイム リンク メトリックをサポートするための PPPoE の拡張を実現します。この拡張は、可変帯域幅および制限付きバッファリング機能（無線リンクなど）を使用した接続に非常に役立ちます。

仮想マルチポイント インターフェイス（VMI）

PPPoE拡張によってルータと無線間で通信するためのセットアップの大部分が実現しますが、VMIは、上位レイヤ（ルーティングプロトコルなど）が消費するイベントを管理および変換する必要に対処します。また、VMI はバイパスモードで動作します。

バイパスモードでは、無線ネイバーを表すすべての仮想アクセスインターフェイス（VAI）がルーティングプロトコル OSPFv3 および EIGRP に明示されるため、ルーティングプロトコルは、ユニキャストとマルチキャスト両方のルーティング プロトコル トラフィックに関してそれぞれの VAI と直接通信します。

集約モードでは、VMI がルーティングプロトコル（OSPF）に明示されるため、ルーティングプロトコルは VMI を活用して効率を最適化できます。ネットワークネイバーが、VMI でのブロードキャストおよびマルチキャスト機能を備えたポイントツーマルチポイント リンク上のネットワークの集合と見なされる場合、VMIは、PPPoEから作成された複数の仮想アクセスインターフェイスの集約に役立ちます。VMIは、単一のマルチアクセスレイヤ2ブロードキャスト対応インターフェイスを提供します。VMI レイヤは、ユニキャスト ルーティング プロトコル トラフィックを適切な P2P リンク（仮想アクセスインターフェイス）にリダイレクトし、フローする必要があるすべてのマルチキャスト/ブロードキャストトラフィックを複製します。ルーティングプロトコルは単一のインターフェイスと通信するため、ネットワークの完全性に影響を与えることなく、トポロジデータベースのサイズが縮小されます。

PPPoE 拡張セッションでの QoS プロビジョニング

次の例では、PPPoE 拡張セッションでの QoS プロビジョニングについて説明します。

```
policy-map rar_policer
 class class-default
  police 10000 2000 1000 conform-action transmit  exceed-action drop  violate-action
drop
policy-map rar_shaper
 class class-default
  shape average percent 1

interface Virtual-Template2
 ip address 10.92.2.1 255.255.255.0
 no peer default ip address
 no keepalive
 service-policy input rar_policer
end
```

例：バイパスモードでの RAR 機能の設定

次に、バイパスモードにおける RAR のエンドツーエンド設定の例を示します。

（注） RAR を設定する前に、まず **subscriber authorization enable** コマンドを設定して RAR セッションを起動する必要があります。認証され有効になっていないと、ポイントツーポイントプロトコルはこれを RAR セッションとして認識せず、PPPoE Active Discovery Initiate（PADI）の提示の際に *manet_radio* をタグ付けしない場合があります。デフォルトでは、設定にバイパスモードが表示されません。モードがバイパスとして設定されている場合にのみ表示されます。

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

ブロードバンドの設定

```
bba-group pppoe VMI2
 virtual-template 2
service profile rar-lab
!
interface GigabitEthernet0/0/0
 description Connected to Client1
  negotiation auto
  pppoe enable group VMI2
!
```

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

バイパスモードの設定

- 仮想テンプレートで明示的に設定された IP アドレス

```
interface Virtual-Template2
ip address 192.0.2.3 255.255.255.0
no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
```

```
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

- 仮想テンプレートで設定された番号なしの VMI

```
interface Virtual-Template2
ip unnumbered vmi2
no ip redirects
peer default ip address pool PPPoEpool2
ipv6 enable
ospfv3 1 network manet
ospfv3 1 ipv4 area 0
ospfv3 1 ipv6 area 0
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

バイパスモードでの仮想マルチポイント インターフェイスの設定

```
interface vmi2 //configure the virtual multi interface
ip address 192.0.2.1 255.255.255.0
physical-interface GigabitEthernet0/0/0
mode bypass

interface vmi3//configure the virtual multi interface
 ip address 192.0.2.3 255.255.255.0
 physical-interface GigabitEthernet0/0/1
mode bypass
```

OSPF ルーティングの設定

```
router ospfv3 1
 router-id 192.0.2.1
!
 address-family ipv4 unicast
  redistribute connected metric 1 metric-type 1
  log-adjacency-changes
 exit-address-family
 !
 address-family ipv6 unicast
  redistribute connected metric-type 1
  log-adjacency-changes
 exit-address-family
!
ip local pool PPPoEpool2 198.51.100.1 198.51.100.254
```

例：集約モードでの RAR 機能の設定

次に、集約モードにおける RAR のエンドツーエンド設定の例を示します。

（注） RAR を設定する前に、まず **subscriber authorization enable** コマンドを設定して RAR セッションを起動する必要があります。許可を有効にしないと、ポイントツーポイント プロトコルはこれを RAR セッションとして認識せず、PADI で *manet_radio* がタグ付けされない場合があります。

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

ブロードバンドの設定

```
bba-group pppoe VMI2
 virtual-template 2
service profile rar-lab

!
interface GigabitEthernet0/0/0
 description Connected to Client1
  negotiation auto
  pppoe enable group VMI2

!
```

RAR のサービスの設定

```
policy-map type service rar-lab
 pppoe service manet_radio //note: Enter the pppoe service policy name as manet_radio
!
```

集約モードでの設定

```
interface Virtual-Template2
ip unnumbered vmi2
no ip redirects
no peer default ip address
ipv6 enable
no keepalive
service-policy input rar_policer Or/And
service-policy output rar_shaper
```

集約モードでの仮想マルチポイント インターフェイスの設定

```
interface vmi2 //configure the virtual multi interface
ip address 192.0.2.1 255.255.255.0
physical-interface GigabitEthernet0/0/0
mode aggregate

interface vmi3//configure the virtual multi interface
 ip address 192.0.2.3 255.255.255.0
 no ip redirects
```

```
 no ip split-horizon eigrp 1
 physical-interface GigabitEthernet0/0/1
mode aggregate
```

OSPF ルーティングの設定

```
router ospfv3 1
 router-id 192.0.2.1
!
 address-family ipv4 unicast
  redistribute connected metric 1 metric-type 1
  log-adjacency-changes
 exit-address-family
 !
 address-family ipv6 unicast
  redistribute connected metric-type 1
  log-adjacency-changes
 exit-address-family
!
ip local pool PPPoEpool2 198.51.100.1 198.51.100.254
ip local pool PPPoEpool3 203.0.113.1 203.0.113.254
```

RAR セッションの詳細の確認

RAR セッションの詳細を取得するには、次の show コマンドを使用します。

```
Router#show pppoe session packets all
Total PPPoE sessions 2

session id: 9
local MAC address: 006b.f10e.a5e0, remote MAC address: 0050.56bc.424a
virtual access interface: Vi2.1, outgoing interface: Gi0/0/0
    1646 packets sent, 2439363 received
    176216 bytes sent, 117250290 received

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 32928     PADG Timer index: 0
 PADG last rcvd Seq Num: 17313
 PADG last nonzero Seq Num: 17306
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33308  rcvd: 17313
 PADC xmit: 17313  rcvd: 19709
 In-band credit pkt xmit: 7 rcvd: 2434422
 Last credit packet snapshot
  PADG xmit: seq_num = 32928, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 32928, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17313, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17313, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0
```

```
session id: 10
local MAC address: 006b.f10e.a5e1, remote MAC address: 0050.56bc.7dcb
virtual access interface: Vi2.2, outgoing interface: Gi0/0/1
    1389302 packets sent, 1852 received
    77869522 bytes sent, 142156 received

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 18787     PADG Timer index: 0
 PADG last rcvd Seq Num: 18784
 PADG last nonzero Seq Num: 18768
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 18787  rcvd: 18784
 PADC xmit: 18784  rcvd: 18787
 In-band credit pkt xmit: 1387764 rcvd: 956
 Last credit packet snapshot
  PADG xmit: seq_num = 18787, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 18787, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18784, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 18784, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 1


Router#show pppoe session packets
Total PPPoE sessions 2

SID     Pkts-In         Pkts-Out        Bytes-In        Bytes-Out
9       2439391         1651            117252098       176714
10      1858            1389306         142580          77869914


Router#show vmi counters
Interface vmi2: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =       4280
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Interface vmi3: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0
```

```
Output Counts:
  Transmit:
       VMI Process DQ  =       2956
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Interface vmi4: - Last Clear Time =

Input Counts:
  Process Enqueue      =          0 (VMI)
  Fastswitch           =          0
  VMI Punt Drop:
       Queue Full      =          0

Output Counts:
  Transmit:
       VMI Process DQ  =          0
       Fastswitch VA   =          0
       Fastswitch VMI  =          0
  Drops:
       Total           =          0
       QOS Error       =          0
       VMI State Error =          0
       Mcast NBR Error =          0
       Ucast NBR Error =          0
Router#


Router#show vmi neighbor details
1 vmi2 Neighbors
      1 vmi3 Neighbors
      0 vmi4 Neighbors
      2 Total Neighbors

vmi2   IPV6 Address=FE80::21E:E6FF:FE43:F500
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.2, Uptime=05:15:01
       Output pkts=89, Input pkts=0
       No Session Metrics have been received for this neighbor.
       Transport PPPoE, Session ID=9
       INTERFACE STATS:
          VMI Interface=vmi2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.1,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/0,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33038     PADG Timer index: 0
 PADG last rcvd Seq Num: 17423
 PADG last nonzero Seq Num: 17420
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33418  rcvd: 17423
```

```
 PADC xmit: 17423  rcvd: 19819
 In-band credit pkt xmit: 7 rcvd: 2434446
 Last credit packet snapshot
  PADG xmit: seq_num = 33038, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33038, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17423, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17423, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


vmi3   IPV6 Address=FE80::21E:7AFF:FE68:6100
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.4, Uptime=05:14:55
       Output pkts=6, Input pkts=0
       METRIC DATA: Total rcvd=1, Avg arrival rate (ms)=0
          CURRENT: MDR=128000 bps, CDR=128000 bps
                   Lat=0 ms, Res=100, RLQ=100, load=0
          MDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
          CDR      Max=128000 bps, Min=128000 bps, Avg=128000 bps
          Latency  Max=0, Min=0, Avg=0 (ms)
          Resource Max=100%, Min=100%, Avg=100%
          RLQ      Max=100, Min=100, Avg=100
          Load     Max=0%, Min=0%, Avg=0%
       Transport PPPoE, Session ID=10
       INTERFACE STATS:
          VMI Interface=vmi3,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          V-Access intf=Virtual-Access2.2,
             Input qcount=0, drops=0, Output qcount=0, drops=0
          Physical intf=GigabitEthernet0/0/1,
             Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 18896     PADG Timer index: 0
 PADG last rcvd Seq Num: 18894
 PADG last nonzero Seq Num: 18884
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 18896  rcvd: 18894
 PADC xmit: 18894  rcvd: 18896
 In-band credit pkt xmit: 1387764 rcvd: 961
 Last credit packet snapshot
  PADG xmit: seq_num = 18896, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 18896, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 18894, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 18894, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 0, bcn = 64222
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 1


Router#show vmi neighbor details vmi 2
              1 vmi2 Neighbors

vmi2   IPV6 Address=FE80::21E:E6FF:FE43:F500
       IPV6 Global Addr=::
       IPV4 Address=192.0.2.2, Uptime=05:16:03
```

```
        Output pkts=89, Input pkts=0
        No Session Metrics have been received for this neighbor.
        Transport PPPoE, Session ID=9
        INTERFACE STATS:
           VMI Interface=vmi2,
              Input qcount=0, drops=0, Output qcount=0, drops=0
           V-Access intf=Virtual-Access2.1,
              Input qcount=0, drops=0, Output qcount=0, drops=0
           Physical intf=GigabitEthernet0/0/0,
              Input qcount=0, drops=0, Output qcount=0, drops=0

PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33100     PADG Timer index: 0
 PADG last rcvd Seq Num: 17485
 PADG last nonzero Seq Num: 17449
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33480  rcvd: 17485
 PADC xmit: 17485  rcvd: 19881
 In-band credit pkt xmit: 7 rcvd: 2434460
 Last credit packet snapshot
  PADG xmit: seq_num = 33100, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33100, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17485, fcn = 0, bcn = 65535
  PADC xmit: seq_num = 17485, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534
    ==== PADQ Statistics ====
     PADQ xmit: 0  rcvd: 0


Router#show platform hardware qfp active feature ess session
Current number sessions: 2
Current number TC flow: 0
Feature Type: A=Accounting D=Policing(DRL) F=FFR M=DSCP Marking L=L4redirect P=Portbundle
 T=TC

   Session    Type      Segment1      SegType1      Segment2      SegType2 Feature Other
-------------------------------------------------------------------------------------

        21     PPP 0x0000001500001022    PPPOE 0x0000001500002023    LTERM -------
        24     PPP 0x0000001800003026    PPPOE 0x0000001800004027    LTERM -------


Router#show platform software subscriber pppoe_fctl evsi 21
PPPoE Flow Control Stats
 Local Credits: 65535   Peer Credits: 65535   Local Scaling Value 64 bytes
 Credit Grant Threshold: 28000    Max Credits per grant: 65535
 Credit Starved Packets: 0
 PADG xmit Seq Num: 33215     PADG Timer index: 0
 PADG last rcvd Seq Num: 17600
 PADG last nonzero Seq Num: 17554
 PADG last nonzero rcvd amount: 2
 PADG Timers: (ms)   [0]-1000    [1]-2000    [2]-3000    [3]-4000    [4]-5000
 PADG xmit: 33595  rcvd: 17600
 PADC xmit: 17600  rcvd: 19996
 In-band credit pkt xmit: 7 rcvd: 2434485
 Last credit packet snapshot
  PADG xmit: seq_num = 33215, fcn = 0, bcn = 65535
  PADC rcvd: seq_num = 33215, fcn = 65535, bcn = 65535
  PADG rcvd: seq_num = 17600, fcn = 0, bcn = 65535
```

```
  PADC xmit: seq_num = 17600, fcn = 65535, bcn = 65535
  In-band credit pkt xmit: fcn = 61, bcn = 65533
  In-band credit pkt rcvd: fcn = 0, bcn = 65534

BQS buffer statistics
 Current packets in BQS buffer: 0
 Total en-queue packets: 0 de-queue packets: 0
 Total dropped packets: 0

Internal flags: 0x0
```

```
Router#show platform hardware qfp active feature ess session id 21
Session ID: 21

  EVSI type: PPP
  SIP Segment ID: 0x1500001022
  SIP Segment type: PPPOE
  FSP Segment ID: 0x1500002023
  FSP Segment type: LTERM
  QFP if handle: 16
  QFP interface name: EVSI21
  SIP TX Seq num: 0
  SIP RX Seq num: 0
  FSP TX Seq num: 0
  FSP RX Seq num: 0
  Condition Debug: 0x00000000
    session
```

```
Router#show ospfv3 neighbor

          OSPFv3 1 address-family ipv4 (router-id 10.3.3.3)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.0.2.1         0    FULL/  -        00:01:32    19              Virtual-Access2.1

          OSPFv3 1 address-family ipv6 (router-id 10.3.3.3)

Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
192.0.2.1         0    FULL/  -        00:01:52    19              Virtual-Access2.1
Router#
```

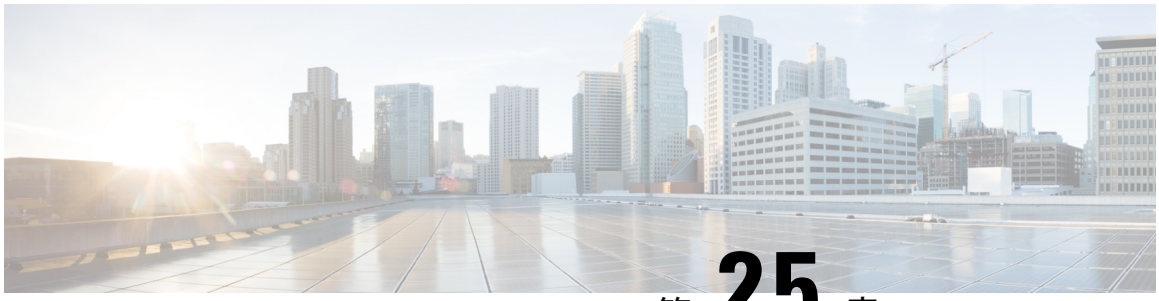
```
Router#sh ip route

Codes: L - local, 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, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.90.90.0/24 is directly connected, Virtual-Access2.1
O        10.90.90.4/32 [110/1] via 192.0.2.4, 00:00:03, Virtual-Access2.1
L        10.90.90.5/32 is directly connected, Virtual-Access2.1
```

```
      10.92.90.0/32 is subnetted, 1 subnets
C        10.92.2.21 is directly connected, Virtual-Access2.1
```

無線対応ルーティングのトラブルシューティング

RAR をトラブルシューティングするには、次の debug コマンドを使用します。

- **debug pppoe errors**
- **debug pppoe events**
- **debug ppp error**
- **debug vmi error**
- **debug vmi neighbor**
- **debug vmi packet**
- **debug vmi pppoe**
- **debug vmi registries**
- **debug vmi multicast**
- **debug vtemplate cloning**
- **debug vtemplate event**
- **debug vtemplate error**
- **debug plat hard qfp ac feature subscriber datapath pppoe detail**



第 25 章

Session Initiation Protocol トリガー VPN

Session Initiation Protocol トリガー VPN（SIP トリガー VPN または VPN SIP）は、サービス プロバイダーが提供するサービスで、Session Initiation Protocol（SIP）を使用して、オンデマンド メディアやピア間のアプリケーション共有に必要な VPN が設定されます。VPN SIP 機能は、2 つの SIP ユーザ エージェントが相互の IP アドレスを解決し、自己署名証明書、サードパーティ証明書、または事前共有キーのフィンガープリントを安全に交換して、IPsec ベース VPN の確立に同意するプロセスを定義します（訳注：NTT東日本及び西日本の提供する「ひかり電話データコネクト」サービスに接続するための機能です）。

サービス プロバイダーは、銀行の ATM や支店など、SIP ベースのサービスを必要とする顧客に VPN SIP サービスを提供します。この VPN SIP サービスは、バックアップ ネットワーク機能の ISDN 接続に代わるものです。プライマリのブロードバンド サービス リンクがダウンした場合、これらの銀行の ATM や支店は VPN SIP サービスを介して中央ヘッドエンドまたはデータ センターに接続します。

サービス プロバイダーの SIP サーバは、VPN SIP サービスの調整に加えて、サービスの使用時間を基にしたサービス料金の請求にも使用されます。

VPN SIP の情報

VPN SIP ソリューションのコンポーネント

VPN SIP は、IPSec 静的仮想トンネル インターフェイス（SVTI）を使用します。IPSec SVTI は、IPSec セキュリティ アソシエーション（SA）がトンネル インターフェイスと SVTI ピア間でまったく確立されていない場合でも、アクティブ（UP）な状態のままになります。

VPN SIP ソリューションの 3 つのコンポーネントを次に示します。

- SIP
- VPN SIP
- 暗号（IP Security（IPsec）、インターネットキーエクスチェンジ（IKE）、トンネル保護（TP）、暗号内の Public Key Infrastructure（PKI）モジュール）

Session Initiation Protocol

SIP は、IKE セッションを開始するための名前解決メカニズムとして使用されます。VPN SIP は、SIP サービスを使用して、固定 IP アドレスを持たないホーム ルータまたはスモール ビジネス ルータに VPN 接続を確立します。この接続は、自己署名証明書か事前共有キーを使用して実現されます。SIP は、Session Description Protocol（SDP）オファー/アンサー モデルでのメディア セッションに必要な IKE の使用をネゴシエートします。

SIP は静的に設定されています。リモート SIP 番号それぞれに対して、1 つのトンネル インターフェイスを設定する必要があります。

SIP は、VPN SIP サービスの使用料を SIP 番号に基づいて顧客に請求する課金機能もサービス プロバイダーに提供します。SIP 番号に基づく請求は、サービス プロバイダー ネットワーク内で発生するものであり、Cisco VPN SIP ルータのようなエンド デバイスとは無関係です。

VPN SIP のソリューション

VPN SIP は、SIP モジュールと暗号モジュールを連携し、両者の間を抽象化する中央ブロックです。

SIP 番号の背後にあるリモート ネットワークへ向けられたトラフィックがトンネル インターフェイスにルーティングされると、そのピアには IPSEC SA が設定されていないため、IPSec コントロール プレーンはパケット スイッチング パスからのトリガーを受け取ります。このトンネルは VPN SIP 用に設定されているため、IPsec コントロール プレーンは VPN SIP にトリガーを渡します。

（注） その SIP 番号のリモート ネットワークの静的ルートは、このトンネル インターフェイスを指すように設定される必要があります。

VPN SIP サービスがトリガーされると、SIP は SIP 電話番号のペアを使用してコールを設定します。SIP は VPN SIP に着信コールの詳細も渡し、ローカルの自己署名証明書または事前共有キーのローカル アドレスとフィンガープリント情報を使用して、IKE メディア セッションをネゴシエートします。SIP は VPN SIP にリモート アドレスとフィンガープリント情報も渡します。

VPN SIP サービスはトンネル ステータスの更新をリッスンし、SIP を呼び出して、SIP セッションを切断します。VPN SIP サービスは、現在のアクティブなセッションを表示する手段も提供します。

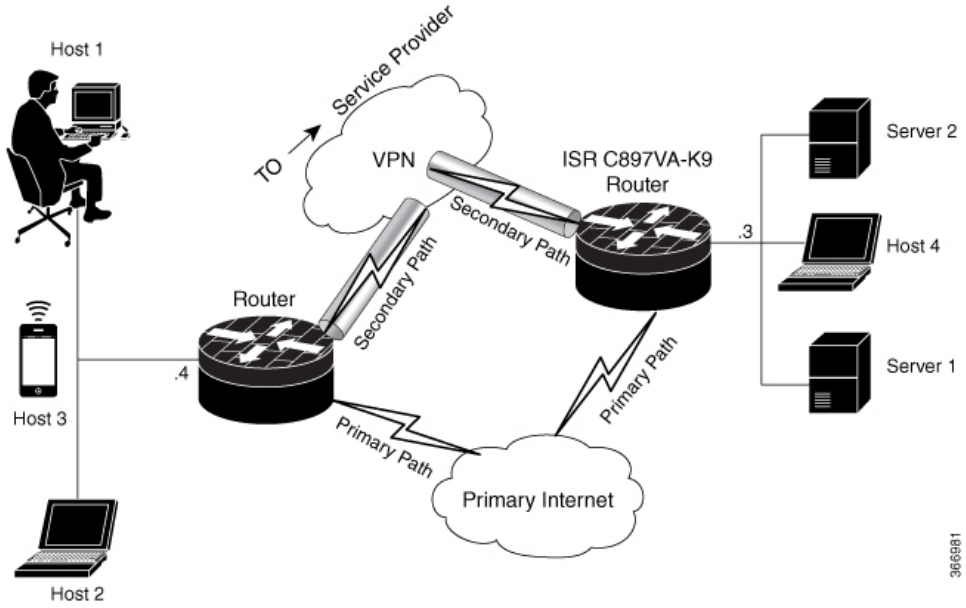
機能一覧

次に、VPN SIP 機能の概略を示します。

- IP SLA は、ルート トラッキングを使用してプライマリ リンクをモニタリングします。プライマリ リンクが失敗すると、IP SLA はこの障害を検出します。
- プライマリ パスが失敗すると、IP SLA はルーターに設定されているメトリックがさらに高いルートにデフォルト ルートを切り替えます。
- 関連するトラフィックがセカンダリ リンクを使用してフローを試みると、SIP は SIP サーバに招待メッセージを送信し、VPN ピア情報を取得します。
- ルータは VPN ピア情報（IP アドレス、ローカル SIP 番号とリモート SIP 番号、IKE ポート、およびフィンガープリント）を受け取って、VPN SIP トンネルを確立します。
- プライマリ パスが復帰すると、IP SLA はプライマリ パスを検出し、ルートが元のパスに戻ります。アイドル タイマーの有効期限が切れると、IPSec は破棄され、SIP コールは切断されます。

次に、VPN SIP ソリューションのトポロジを示します。

図 *3 : VPN SIP* のトポロジ



SIP コール フロー

SIP コールフローは、ローカル ピアでの開始とリモート ピアでのコールの受信に分かれます。

SIP コールの開始

データ プレーン内の SVTI インターフェイスにパケットがルーティングされると、そのアドレスを解決するためにピア SIP 番号に対して SIP コールを発呼する必要があります。これにより、VPN トンネルがアクティブになります。

- ローカル認証タイプが PSK の場合、IKEv2 はピア SIP 番号と一致するキーを検索します。IKEv2 キーリングは、各 SIP ピアの SIP 番号として id_key_id 型（文字列）で設定する必要があります。IKEv2 は検索されたキーのフィンガープリントを計算し、VPN SIP に渡します。
- ローカル認証タイプが自己署名証明書やサード パーティ証明書の場合、IKEv2 は IKEv2 プロファイルに設定されているローカルの証明書のフィンガープリントを計算し、VPN SIP に渡します。

VPN SIP モジュールは、ピアに SIP コールを設定するために SIP と対話します。コールが成功すると、VPN SIP は解決された IP アドレスを SVTI のトンネル接続先として設定し、SVTI に対して VPN トンネルを開始するように要求します。

（注） ワイルドカード キーが必要な場合は、IKEv2 プロファイルで、authentication local pre-share key コマンドと authentication remote pre-share key コマンドを使用します。

リモート ピアでの SIP コールの受信

ピアから SIP コールを受信すると、さまざまな暗号モジュールが以下のように相関して動作します。

- トンネル保護は、VPN SIP モジュールによるトンネルの宛先アドレスの設定に協力します。
- IKEv2 は、ローカル認証タイプ（PSK または PKI）とローカル フィンガープリントを VPN SIP モジュールに返します。ローカル認証タイプが PSK の場合、IKEv2 は対応する SIP 番号と一致するキーを検索します。

（注） IKEv2 は SIP 番号によってのみピアを識別できます。

ピア間で SIP コール ネゴシエーションが行われている間に、各ピアは SDP 上で交換される一意のローカル IKEv2 ポート番号を選択する必要があります。セッションごとに異なるポート番号をサポートするため、VPN SIP モジュールは IP ポート アドレス変換（PAT）をプログラムにより自動的に設定します。PAT は、IKEv2 ポート（4500）と、SDP 上で交換されるポート番号との変換を担います。変換には、セカンダリ リンク上に IP NAT が設定され、ループバック インターフェイスが VPN SIP トンネルの送信元として設定される必要があります。変換の有効期間は、VPN SIP セッションの有効期間で決まります。

SDP オファーとアンサー

RFC 6193 で定義されている、SIP コールでネゴシエートされる SDP オファーとアンサーの例を次に示します。

```
offer SDP
      ...
      m=application 50001 udp ike-esp-udpencap
      c=IN IP4 10.6.6.49
      a=ike-setup:active
      a=fingerprint:SHA-1 \
      b=AS:512
      4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
      ...

   answer SDP
      ...
      m=application 50002 udp ike-esp-udpencap
      c=IN IP4 10.6.6.50
      a=ike-setup:passive
      a=fingerprint:SHA-1 \
      b=AS:512
      D2:9F:6F:1E:CD:D3:09:E8:70:65:1A:51:7C:9D:30:4F:21:E4:4A:8E
```

SDP ネゴシエーションの一環として、両方のピアが「b=AS :number」という SDP 属性を使用し、VPN SIP セッションの最大帯域幅のレートをネゴシエートします。SDP に表示されるピア双方の帯域幅が異なる場合、小さい方の値が最大帯域幅として使用される必要があります。「b=AS :number」SDP 属性がオファーかアンサーに含まれていない場合、SIP コールは正常に設定されていません。

ネゴシエートされた最大帯域幅は、プログラムによって設定される出力方向の QoS ポリシーを介して SVTI トンネル インターフェイスに適用されます。静的に設定されたポリシーが既に存在する場合は、プログラムによって設定される QoS ポリシーは適用されず、セッションは失敗します。

SIP コールが完了し、ピアのアドレスが解決されると、VPN SIP は SVTI のトンネル接続先を設定し、トンネルを開始する要求を送信します。

IKEv2 ネゴシエーション

次に、IKEv2 セキュリティ セッション（SA）ネゴシエーションのプロセスを示します。

- セッションの開始前に、IKEv2 は VPN SIP を使用して、そのセッションが VPN SIP セッションであるかどうかを確認します。
- セッションが VPN SIP セッションで、ローカル認証タイプが PSK の場合、IKEv2 はピアの IP アドレスの代わりにピアの SIP 番号を使用して、PSK キー ペアを検索します。
- 自己署名証明書を検証する場合、IKEv2 はその証明書が自己署名されたものかを確認して、証明書を検証します。
  - IKEv2 プロトコルの一部である既存の AUTH ペイロード検証に加えて、IKEv2 は受信した証明書または検索された PSK のハッシュを計算して、IKEv2 が VPN SIP モジュールからクエリする SIP ネゴシエーションのフィンガープリントと比較します。フィンガープリントが一致する場合のみ、IKEv2 はピアの認証が有効であると見なします。一致しない場合、IKEv2 はそのピアが認証に失敗したことを宣言し、VPN セッションを終了します。

VPN SIP ソリューションは、バックアップ VPN でトラフィックをルーティングする必要がなくなったことを、IPSEC アイドル タイマーに基づいて検出します。トラフィックがない時にセッションが切断されるようにするには、IPSec プロファイルにアイドル時間を設定する必要があります。推奨設定は 120 秒です。

VPN SIP と SIP は、連係して SIP コールを切断します。

IPsec アイドル時間の有効期限が切れると、VPN SIP モジュールは IPsec トンネルをダウンするように IKEv2 に通知します。VPN SIP は、SIP モジュールに対して、IKEv2 からの確認を待機せずに SIP コールを切断するように要求します。

SIP コールの切断をピアから受信すると、VPN SIP モジュールは IPsec トンネルをダウンするように IKEv2 に通知し、SIP に対して SIP コールの切断を許可します。

サポートされるプラットフォーム

VPN SIP 機能は次のプラットフォームでサポートされています。

VPN SIP の前提条件

- セキュリティ K9 ライセンスをルータで有効にする必要があります。
- ルータには最低 1 GB のメモリが必要です。
- SIP ユーザ エージェントの SIP 登録要求が成功するには、VPN SIP ルータが SIP レジストラを使用できる必要があります。
- DHCP サーバは、SIP サーバ アドレスを取得するためにオプション 120 と 125 をサポートする必要があります。SIP サーバ アドレスは、SIP セッションの登録と確立に必要になります。
- プライマリ パスがダウンしたときにバックアップ WAN パスが使用される ようにするには、ルーティングを適切に設定しておく必要があります。
- トンネル インターフェイスの最大伝送ユニット（MTU）は、セカンダリ WAN インターフェイスの MTU よりも小さくなければなりません。
- IKEv2 認証に自己署名証明書やサード パーティ証明書を使用する場合は、IP 層のフラグメンテーションを避けるために、VPN SIP ルータに IKEv2 フラグメンテーションを設定します。
- NAT SIP ALG は無効にする必要があります。
- 発信者ID通知サービス（訳注：「ナンバー・ディスプレイ」）が該当の加入者契約において、ネットワーク側で設定されている必要があります。

VPN SIP の制約事項

- VPN SIP と CUBE/SIP ゲートウェイを同一デバイス上で設定することはできません。CUBE ライセンスがデバイス上でアクティブな場合、CUBE のみが有効になります。
- トランスポートとメディア（SIP 登録、SIP シグナリング、および IPv4 トランスポートを介して暗号化された IPv4 パケットの IPv4 トランスポート）では、IPv4 のみがサポートされています。
- NAT の背後にあるピア デバイスを使用した SIP シグナリングはサポートされていません（ICE および STUN はサポートされていません）。
- SIP ネゴシエーションは、グローバル VRF でのみサポートされています。
- プライベート アドレスの割り当て、設定モード交換（CP ペイロード）、ルート交換などのリモート アクセス VPN 機能はサポートされていません。
- VPN SIP セッションでのルーティング プロトコルはサポートされていません。
- Rivest-Shamir-Addleman（RSA）サーバ自己署名証明書のみがサポートされています。

- 認証、認可、およびアカウンティング（AAA）を使用した事前共有キーの検索機能は、サポートされていません。
- IPSec アイドル タイマーは、ipsec-profile コマンドを使用して IPSec プロファイルごとに設定します。アイドル時間は、特定の IPSec プロファイルを使用するすべての VPN SIP セッションで同じです。
- IPSLA のモニタリングに使用されるトラック オブジェクトは、Cisco IOS ソフトウェアで最大 1000 オブジェクトまでに制限されています。1 つのトラック オブジェクトを使用して 1 台のピア ルーターを追跡する場合、1 台の IOS デバイスが処理できる VPN SIP セッションの最大数は、トラック オブジェクトの最大数で決まります。
- Cisco IOS ソフトウェアでは、ローカル SIP 番号は 1 つのみサポートされています。
- 静的に設定されたポリシーが既に存在する場合は、プログラムによって設定される QoS ポリシーは適用されず、セッションは失敗します。SVTI インターフェイス上に静的に設定された QoS ポリシーは、すべて削除してください。
- すべての Cisco ISR 1100 シリーズルータでは、VPN-SIP 機能がサポートされる対象は 300 セッションまでです。
- シスコ以外のベンダーによって実装された VPN SIP との相互運用性は、サポートされていません。
- VPN-SIP トンネルに付加されたポリシーマップに含まれるクラスポリシーについては、プライオリティキューイングとクラスベース重み付け均等化キューイング（CBWFQ）のみがサポートされます。
- CBWFQ の設定でサポートされているのは、`bandwidth percent` *`percent`* コマンドのみです。VPN-SIP セッションの帯域幅はピアルータとのネゴシエーションによって変わるため、`bandwidth` *`bandwidth`* コマンドはサポートされていません。

VPN SIP の設定方法

VPN SIP の設定

VPN SIP を設定する手順は次のとおりです。

1. サードパーティ証明書、自己署名証明書、または事前共有キーを使用してトンネル認証を設定します。
    1. 証明書を使用するトンネル認証

       顧客のネットワーク内にある証明機関（CA）サーバから証明書を取得するためのトラストポイントを設定します。これはトンネル認証で必要です。次の設定を使用します。

       ```
       peer1(config)# crypto pki trustpoint CA
        enrollment url http://10.45.18.132/
       ```

```
 serial-number none
 subject-name CN=peer2
 revocation-check crl
 rsakeypair peer2

peer2(config)# crypto pki authenticate CA
Certificate has the following attributes:
       Fingerprint MD5: F38A9B4C 2D80490C F8E7581B BABE7CBD
      Fingerprint SHA1: 4907CC36 B1957258 5DFE23B2 649E7DDA 99BDB7C3
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

peer2(config)#crypto pki enroll CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: CN=peer2
% The subject name in the certificate will include: peer2
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA' command will show the fingerprint.
Certificate map for Trustpoint
crypto pki certificate map data 1
issuer-name co cn = orange
```

2. 自己署名証明書を使用するトンネル認証

自己署名証明書を使用して認証を行う場合、そのデバイス上に自己署名証明書を生成する PKI トラストポイントを設定します。次の設定を使用します。

```
peer4(config)#crypto pki trustpoint Self
    enrollment selfsigned
    revocation-check none
    rsakeypair myRSA
    exit
crypto pki enroll Self

Do you want to continue generating a new Self Signed Certificate? [yes/no]: yes
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

3. 事前共有キーを使用してトンネル認証を設定します。

```
crypto ikev2 keyring keys
peer peer1
identity key-id 1234
pre-shared-key key123
```

2. • 証明書の IKEv2 プロファイルを設定します。

```
crypto ikev2 profile IPROF
match certificate data
identity local key-id 5678
authentication remote rsa-sig
authentication local rsa-sig
```

```
keyring local keys
pki trustpoint self
nat force-encap
```

- 事前共有キーの IKEv2 プロファイルを設定します。

```
crypto ikev2 profile IPROF
match identity remote any
identity local key-id 5678
authentication remote pre-share
authentication local pre-share
keyring local keys
nat force-encap
```

（注） IKEv2 SA を設定するには、両方のピアで **nat force-encap** コマンドを設定する必要があります。UDP のカプセル化が SDP でネゴシエートされるので、IKEv2 はポート 4500 で開始し続行される必要があります。

3. IPsec プロファイルを設定します。

```
crypto ipsec profile IPROF
set security-association idle-time 2000
```

4. LAN 側インタ フェースを設定します。

```
interface Vlan101
         ip address 192.0.2.3 255.255.255.0
         no shutdown
!
     interface GigabitEthernet2
         switchport access vlan 101
         no ip address
```

5. ループバック インターフェイスを設定します。

ループバック インターフェイスは、セカンダリ VPN トンネルの送信元インターフェイスとして使用されます。

```
interface loopback 1
    ip address 192.0.2.1 255.0.0.0
    ip nat inside
```

6. セカンダリ インターフェイスを設定します。

（注） セカンダリ インターフェイスは、IP アドレス、SIP サーバ アドレス、およびベンダー固有の情報を DHCP 経由で受信するように設定する必要があります。

```
interface GigabitEthernet8
     ip dhcp client request sip-server-address
     ip dhcp client request vendor-identifying-specific
     ip address dhcp
    ip nat outside
```

7. トンネル インターフェイスを設定します。

```
interface Tunnel1
     ip address 192.0.2.1 255.255.255.255
     load-interval 30
     tunnel source Loopback1
     tunnel mode ipsec ipv4
     tunnel destination dynamic
     tunnel protection ipsec profile IPROF ikev2-profile IPROF
     vpn-sip local-number 5678 remote-number 1234 bandwidth 1000
```

vpn-sip local-number *local-number* **remote-number** *remote-number* **bandwidth** *bw-number* コマンドを使用して、SVTI インターフェイスに VPN-SIP を設定します。帯域幅とは、このピアとネゴシエートされる必要のある最大データ伝送速度のことで、ネゴシエートされた値がトンネル インターフェイスに設定されます。使用できる値は 64 Kbps、128 Kbps、256 Kbps、512 Kbps、および 1000 Kbps です。（訳注：128および256 Kbpsが設定可能なのは IOS XE 17.10以降です。）

VPN SIP 用に SVTI を設定した後で、トンネル モード、トンネルの接続先、トンネルの送信元、およびトンネル保護を変更することはできません。モード、送信元、接続先、またはトンネル保護を変更するには、その SVTI インターフェイスから VPN SIP 設定を削除する必要があります。

8. 接続先ネットワークにスタティックルートを追加します。

メトリックが高いセカンダリ ルートを追加します。

```
ip route 192.0.2.168 255.255.255.0 Tunnel0 track 1
ip route 192.0.2.168 255.255.255.0 Tunnel1 254
```

9. IP SLA を設定します。

```
ip sla 1
         icmp-echo 192.0.2.11
         threshold 500
         timeout 500
         frequency 2
        ip sla schedule 1 life forever start-time now
```

10. ルート トラッキングを設定します。

```
track 1 ip sla 1 reachability
```

11. VPN SIP を有効化します。

```
vpn-sip enable
vpn-sip local-number 5678 address ipv4 GigabitEthernet8
vpn-sip tunnel source Loopback1
vpn-sip logging
```

VPN SIP を設定するには、ローカルの SIP 番号とローカル アドレスを設定する必要があります。**vpn-sip local-number** *SIP-number* **address ipv4** *WAN-interface-name* コマンドを使用して、SIP コールに使用するローカル SIP 番号と、関連づけられた IPv4 アドレスを設定します。

（注） IPv4 アドレスのみ設定できます。暗号モジュールはデュアル スタックをサポートしていません。

- バックアップ WAN インターフェイスのアドレスは、DHCP 割り当てに基づいて変わることがあります。

プライマリ WAN インタ フェースが機能している場合、VPN SIP トンネルの接続先はバックアップ WAN インターフェイスに設定され、トンネル インターフェイスが有効になります。トラフィックがトンネルインターフェイスにルーティングされる場合、接続先は SIP ネゴシエーションの SDP から学習されるピアの IP アドレスに設定されます。プライマリ WAN インターフェイスが失敗した場合、バック ルートがアクティブ化されていれば、パケットはバックアップを介して sVTI にルーティングされます。

（注） ループバック インターフェイスのアドレスにはルーティング不可能な未使用のアドレスを使用し、そのループバック インターフェイスは他のいかなる目的にも使用しないようにお勧めします。ループバック インターフェイスを設定すると、VPN SIP はこのインターフェイスに対するすべての更新プログラムをリッスンし、それらをブロックします。**vpn-sip logging** コマンドにより、セッションの開始、終了、障害発生などのイベントに関する VPN-SIP モジュールのシステムロギングが有効になります。

ローカル ルータの VPN SIP の確認

登録スターテスの確認

```
Peer1# show vpn-sip registration-status
 SIP registration of local number 0388881001 : registered 10.6.6.50
```

SIP レジストラの確認

```
Peer1#show vpn-sip sip registrar

Line          destination      expires(sec)  contact   transport     call-id
=============================================================================================
0388881001    example.com         2359        10.6.6.50  UDP
3176F988-9EAA11E7-8002AFA0-8EF41435
```

VPN SIP ステータスの確認

```
Peer1#show vpn-sip session detail
VPN-SIP session current status

Interface: Tunnel1
   Session status: SESSION_UP (I)
   Uptime        : 00:00:42
   Remote number : 0388881001 =====> This is the Remote Router's SIP number
   Local number  : 0388882001 =====> Local router's SIP number
```

```
   Remote address:port: 10.6.6.49:50002
   Local address:port : 10.6.6.50:50001
   Crypto conn handle: 0x8000017D
   SIP Handle         : 0x800000C7
   SIP callID         : 1554
   Configured/Negotiated bandwidth: 64/64 kbps
```

暗号化セッションの確認

```
Peer1# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP Vpn-sip

Interface: Tunnel1
Profile: IPROF
Uptime: 00:03:53
Session status: UP-ACTIVE
Peer: 10.6.6.49 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.6.6.49
      Desc: (none)
  Session ID: 43
  IKEv2 SA: local 10.11.1.1/4500 remote 10.6.6.49/50002 Active
          Capabilities:S connid:1 lifetime:23:56:07 ====> Capabilities:S indicates this
 is a  SIP VPN_SIP Session
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 6 drop 0 life (KB/Sec) 4222536/3366
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4222537/3366
```

IP NAT 変換の確認

```
Peer1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 2.2.2.2:4500       10.6.6.50:50001    10.6.6.49:50002    10.6.6.49:50002
```

DHCP SIP 設定の確認

```
Peer9#show vpn-sip sip dhcp
SIP DHCP Info

SIP-DHCP interface:  GigabitEthernet8

SIP server address:
Domain name:         dns:example.com
```

リモート ルータの VPN SIP の確認

リモート ルータの VPN SIP 登録ステータスの確認

```
Peer2# show vpn-sip registration-status
 SIP registration of local number 0388882001 : registered 10.6.6.49
```

リモート ルータの VPN SIP レジストラの確認

```
Peer2# show vpn-sip sip registrar
Line          destination      expires(sec)  contact    transport    call-id
=============================================================================================
0388882001    example.com    2478         10.6.6.49   UDP
E6F23809-9EAB11E7-80029279-40B97F59
```

リモート ルータの VPN SIP セッションに関する詳細の確認

```
Peer2# show vpn-sip session detail
VPN-SIP session current status
Interface: Tunnel1
   Session status: SESSION_UP (R)
   Uptime        : 00:00:21
   Remote number : 0388882001 =====> This is the Peer1 Router's SIP number
   Local number  : 0388881001 =====> Local router's SIP number
   Remote address:port: 10.6.6.50:50001
   Local address:port : 10.6.6.49:50002
   Crypto conn handle: 0x8000017E
   SIP Handle        : 0x800000BE
   SIP callID        : 1556
   Configured/Negotiated bandwidth: 1000/64 kbps
```

リモート ルータの暗号化セッションに関する詳細の確認

```
Peer2 #show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN-SIP

Interface: Tunnel1
Profile: IPROF
Uptime: 00:02:32
Session status: UP-ACTIVE
Peer: 10.6.6.50 port 50001 fvrf: (none) ivrf: (none)
      Phase1_id: 10.6.6.50
      Desc: (none)
  Session ID: 147
  IKEv2 SA: local 10.17.1.1/4500 remote 10.6.6.50/50001 Active
          Capabilities:S connid:1 lifetime:23:57:28 ====> Capabilities:S indicates this
 is a  SIP VPN-SIP Session
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 4 drop 0 life (KB/Sec) 4293728/3448
        Outbound: #pkts enc'ed 6 drop 0 life (KB/Sec) 4293728/3448
```

リモート ルータの IP NAT 変換の確認

```
Peer2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 3.3.3.3:4500       10.6.6.49:50002    10.6.6.50:50001    10.6.6.50:50001
```

VPN-SIP 用 QoS の設定

必要に応じて、Quality of Service（QoS）ポリシーを VPN-SIP に適用できます。QoS ポリシーを設定することで、特定のタイプのトラフィックに対して安全で予測/測定が可能なサービス、場合によっては保証されたサービスを提供することができます。

1. 適切なポリシーマップを設定します。

```
Device(config)#class-map match-all UDP
 match protocol ip
!
policy-map CBWFQ
 class UDP
  bandwidth percent 60
  queue-limit 12 packets
```

2. ポリシーマップを VPN-SIP に付加します。

```
Device(config)#interface Tunnel1
.
.
.
vpn-sip local-number 5678 remote-number 1234 bandwidth 1000 service-policy CBWFQ
```

（注） VPN-SIPセッションが正常にネゴシエートされて開かれると、暗黙的なサービスポリシーがトンネルインターフェイスに自動的に適用されます。このインターフェイスに対して `show running-config` コマンドを実行しても、暗黙的なサービス ポリシーは表示されません。デバイスで作成したポリシーマップは、この暗黙的サービスポリシーの子ポリシーとなります。

VPN-SIP の QoS の確認

ポリシーマップ適用の確認

```
Peer1#sh policy-map int tun1
 Tunnel1

  Service-policy output: VPN-SIP-Tunnel1-Bandwidth

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      QoS Set
        dscp cs4
          Packets marked 0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000

      Service-policy : CBWFQ
```

```
        Class-map: UDP (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: protocol ip
          Queueing
          queue limit 12 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 60% (600 kbps)


        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: any

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
Peer1#sh vpn-sip session detail
VPN-SIP session current status

Interface: Tunnel1
   Session status: SESSION_UP (R)
   Uptime        : 00:00:15
   Remote number : 5678
   Local number  : 1234
   Remote address:port: 6.6.6.40:51878
   Local address:port : 6.6.6.89:50010
   Crypto conn handle: 0x40000017
   SIP Handle        : 0x4000000B
   SIP callID        : 2288
   Configured/Negotiated bandwidth: 1000/1000 kbps
   Applied service policy: CBWFQ
```

トラフィックフローの確認

ポリシーを適用する方向に UDP トラフィックを送信した後、次のようにトラフィックフローを確認します。

```
Peer1#sh policy-map int tun1
 Tunnel1

  Service-policy output: VPN-SIP-Tunnel1-Bandwidth

    Class-map: class-default (match-any)
      105782 packets, 4865972 bytes
      5 minute offered rate 130000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/98707/0
      (pkts output/bytes output) 7068/890568
      QoS Set
        dscp cs4
          Packets marked 105782
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000

      Service-policy : CBWFQ

        Class-map: UDP (match-all)
          105775 packets, 4865650 bytes
```

```
  5 minute offered rate 130000 bps, drop rate 331000 bps
  Match: protocol ip
  Queueing
  queue limit 12 packets
  (queue depth/total drops/no-buffer drops) 11/98707/0
  (pkts output/bytes output) 7068/890568
  bandwidth 60% (600 kbps)


Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: any

  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 0/0
```

VPN SIP の設定例

認証用自己署名証明書の使用

認証用の自己署名証明書を使用して VPN SIP を設定する例を次に示します。VPN SIP では、イニシエータとレスポンダのロールに違いはありません。ピア ノード上の設定は、変更されたローカルの SIP 番号と同一になります。

```
// Self-signed certificate
crypto pki trustpoint selfCert
  rsakeypair myRSA
  enrollment selfsigned
  revocation-check none
!
crypto ikev2 profile vpn-sip-profile
 match identity remote any
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint selfCert // Use same self-signed trustpoint for sign and verify
 nat force-encap
!
crypto ipsec profile vpn-sip-ipsec
 set security-association idle-time 120
!
vpn-sip enable
vpn-sip local-number 0388883001 address ipv4 GigabitEthernet1
vpn-sip tunnel source Loopback11
vpn-sip logging
!
// one tunnel per peer - configuration is for peer with a SIP-number of 0388884001
int tunnel0
 ip unnumbered loopback 0
 tunnel source loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile vpn-sip-ipsec ikev2-profile vpn-sip-profile
 vpn-sip local-number 0388883001 remote-number 0388884001 bandwidth 1000
!
// ip unnumbered of tunnel interfaces
int loopback 0
  ip address 10.21.1.1 255.255.255.255
```

```
!
int loopback11
ip address 10.9.9.9 255.255.255.255
ip nat inside
!
// one tunnel per peer - this is for peer with SIP-number 0388885001
int tunnel1
 ip unnumbered loopback 0
 tunnel source loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile vpn-sip-ipsec ikev2-profile iprof
 vpn-sip sip-local 0388883001 sip-remote 0388885001 bandwidth 1000
!
interface GigabitEthernet8
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 ip address dhcp
ip nat outside


// backup routes configured with higher AD so that these routes will be activated only
when primary path goes down. AD need to be chosen to be greater than that of primary
route.
ip route 10.0.0.0 255.0.0.0 tunnel 0 250
ip route 10.1.0.0 255.0.0.0 tunnel 0 250
ip route 10.2.0.0 255.0.0.0 tunnel 0 250
ip route 10.3.0.0 255.0.0.0 tunnel 0 250
```

VPN SIP のトラブルシューティング

show コマンドの出力にトンネル インターフェイスを表示する

症状

Show VPN-SIP セッションにトンネルインタ フェースの情報が表示されません。次の例では、トンネル インターフェイスである tunnel1 の情報が表示されていません。

```
Peer5-F#show vpn-sip session
VPN-SIP session current status

Interface: Tunnel2
   Session status: READY_TO_CONNECT
   Remote number : 0334563333
   Local number  : 0623458888
   Remote address:port: 10.10.0.0:0
   Local address:port : 192.0.2.22:0

Interface: Tunnel3
   Session status: READY_TO_CONNECT
   Remote number : 0323452222
   Local number  : 0623458888
   Remote address:port: 10.10.0.0:0
   Local address:port : 192.0.2.22:0

Interface: Tunnel4
   Session status: READY_TO_CONNECT
   Remote number : 0612349999
   Local number  : 0623458888
```

```
   Remote address:port: 10.10.0.0:0
   Local address:port : 192.0.2.22:0

Interface: Tunnel6
   Session status: READY_TO_CONNECT
   Remote number : 0634567777
   Local number  : 0623458888
   Remote address:port: 10.10.0.0:0
   Local address:port : 172.30.18.22:0
```

考えられる原因

そのトンネル インターフェイスに VPN SIP が設定されていません。

```
Peer5-F#sh run int tun1
Building configuration...

Current configuration : 201 bytes
!
interface Tunnel1
 ip address 10.5.5.5 255.255.255.0
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
end
```

推奨処置

そのトンネル インターフェイスに VPN SIP を設定します。

```
:

Peer5-F#show running interface tunnel 1
Building configuration...

Current configuration : 278 bytes
!
interface Tunnel1
 ip address 10.5.5.5 255.255.255.255
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
 vpn-sip local-number 0623458888 remote-number 0312341111 bandwidth 1000
end
```

次に、上記のシナリオを実行した出力を示します。

```
Peer5-F#show vpn-sip session detail
VPN-SIP session current status

Interface: Tunnel1
   Session status: READY_TO_CONNECT
   Remote number : 0312341111
   Local number  : 0623458888
   Remote address:port: 10.0.0.0:0
   Local address:port : 172.30.18.22:0

   Crypto conn handle: 0x8000002C
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 1000/0 kbps
```

```
Interface: Tunnel2
   Session status: READY_TO_CONNECT
   Remote number : 0334563333
   Local number  : 0623458888
   Remote address:port: 10.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000012
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 512/0 kbps

Interface: Tunnel3
   Session status: READY_TO_CONNECT
   Remote number : 0323452222
   Local number  : 0623458888
   Remote address:port: 10.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000031
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 512/0 kbps

Interface: Tunnel4
   Session status: READY_TO_CONNECT
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 10.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x8000002F
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 1000/0 kbps

Interface: Tunnel6
   Session status: READY_TO_CONNECT
   Remote number : 0634567777
   Local number  : 0623458888
   Remote address:port: 10.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000026
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 1000/0 kbps
```

SIP 登録ステータスのトラブルシューティング

症状

SIP 登録ステータスが登録されていません。

```
Peer5#show vpn-sip sip registrar
Line          destination      expires(sec)  contact
transport     call-id
============================================================

Peer5-F#show vpn-sip registration-status

 SIP registration of local number 0623458888 : not registered
```

考えられる原因

その WAN インターフェイスに IP アドレスが設定されていません。

```
Peer5#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  down                  down
GigabitEthernet0/1         unassigned      YES unset  up                    up
GigabitEthernet0/2         unassigned      YES unset  down                  down
GigabitEthernet0/3         unassigned      YES unset  down                  down
GigabitEthernet0/4         unassigned      YES unset  up                    up
GigabitEthernet0/5         10.5.5.5        YES manual up                    up
Vlan1                      10.45.1.5       YES NVRAM  up                    up
NVI0                       10.1.1.1        YES unset  up                    up
Loopback1                  10.1.1.1        YES NVRAM  up                    up
Loopback5                  10.5.5.5        YES NVRAM  administratively down down
Loopback11                 10.11.11.11     YES NVRAM  up                    up
Tunnel1                    10.5.5.5        YES NVRAM  up                    down
Tunnel2                    10.2.2.2        YES NVRAM  up                    down
Tunnel3                    10.3.3.3        YES NVRAM  up                    down
Tunnel4                    10.4.4.4        YES NVRAM  up                    down
Tunnel6                    10.8.8.8        YES NVRAM  up                    down

Peer5-F#show run interface gigabitEthernet 0/4
Building configuration...

Current configuration : 213 bytes
!
interface GigabitEthernet0/4
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 no ip address           ====> no IP address
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
end
```

推奨処置

ip address dhcp コマンドを使用してインターフェイスの IP アドレスを設定する。

```
Peer5-F#show running-config interface gigabitEthernet 0/4
Building configuration...

Current configuration : 215 bytes
!
interface GigabitEthernet0/4
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 ip address dhcp         ====> configure IP address DHCP
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
end


Peer5-F#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  down                  down
GigabitEthernet0/1         unassigned      YES unset  up                    up
GigabitEthernet0/2         unassigned      YES unset  down                  down
GigabitEthernet0/3         unassigned      YES unset  down                  down
GigabitEthernet0/4         172.30.18.22    YES DHCP   up                    up
GigabitEthernet0/5         10.5.5.5        YES manual up                    up
Vlan1                      10.45.1.5       YES NVRAM  up                    up
NVI0                       10.1.1.1        YES unset  up                    up
```

```
Loopback1                  10.1.1.1        YES NVRAM  up                    up
Loopback5                  10.5.5.5        YES NVRAM  administratively down down
Loopback11                 10.11.11.11     YES NVRAM  up                    up
Tunnel1                    10.6.5.5        YES NVRAM  up                    down
Tunnel2                    10.2.2.2        YES NVRAM  up                    down
Tunnel3                    10.3.3.3        YES NVRAM  up                    down
Tunnel4                    10.4.4.4        YES NVRAM  up                    down
Tunnel6                    10.8.8.8        YES NVRAM  up                    down

Peer5-F#show vpn-sip sip registrar
Line          destination      expires(sec)  contact
transport     call-id
============================================================
0623458888    example.com   2863          172.30.18.22
UDP           1E83ECF0-AF0611E7-802B8FCF-594EB9E7@10.50.18.22

Peer5-F#show vpn-sip registration-status

 SIP registration of local number 0623458888 : registered 172.30.18.22
```

Negotiating IKE 状態でのセッション停止

症状

Negotiating IKE 状態で VPN SIP セッションが停止します。

```
Peer5#show vpn-sip session remote-number 0612349999 detail
VPN-SIP session current status

Interface: Tunnel4
   Session status: NEGOTIATING_IKE (R)
   Uptime        : 00:00:58
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 72.30.168.3:24825
   Local address:port : 72.30.168.22:50012
   Crypto conn handle: 0x8000002E
   SIP Handle        : 0x8000000C
   SIP callID        : 16
   Configured/Negotiated bandwidth: 1000/1000 kbps
```

考えられる原因

IKEv2 関連の設定が不適切です。

次の例では、キーリングで設定されているキー ID が、リモート ピアの SIP 番号と一致していません。

```
Peer5-F#show running-config interface tunnel 4
Building configuration...

Current configuration : 276 bytes
!
interface Tunnel4
 ip address 10.4.4.4 255.255.255.0
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
 VPN-SIP local-number 0623458888 remote-number 0612349999 bandwidth 1000  ====> Remote
number mentioned here doesn’t match the remote number in the keyring
end
```

```
IKEv2 Keyring configs:
!
crypto ikev2 keyring keys
 peer peer1
  identity key-id 0312341111
  pre-shared-key psk1
 !
 peer abc
  identity key-id 0345674444
  pre-shared-key psk1
 !
 peer peer2
  identity key-id 0334563333
  pre-shared-key psk10337101690
 !
 peer peer6
  identity key-id 0634567777
  pre-shared-key cisco123
 !
 peer peer3
  identity key-id 0323452222
  pre-shared-key cisco123
 !
 peer peer4
  identity key-id 0645676666
  pre-shared-key psk1
 !
 peer NONID
  identity fqdn example.com
  pre-shared-key psk1
 !
!
!
crypto ikev2 profile test
 match identity remote any
 identity local key-id 0623458888
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
 dpd 10 6 periodic
 nat force-encap
```

推奨処置

キーリングの設定を修正します。

```
rypto ikev2 keyring keys
 peer peer1
  identity key-id 0312341111
  pre-shared-key psk1
 !
 peer abc
  identity key-id 0345674444
  pre-shared-key psk1
 !
 peer peer2
  identity key-id 0334563333
  pre-shared-key psk1
 !
 peer peer6
  identity key-id 0634567777
  pre-shared-key psk1
 !
 peer peer3
```

```
  identity key-id 0323452222
  pre-shared-key psk1
 !
 peer peer4
  identity key-id 0612349999
  pre-shared-key psk1
 !
 peer NONID
  identity fqdn example.com
  pre-shared-key psk1
 !
!
!
crypto ikev2 profile test
 match identity remote any
 identity local key-id 0623458888
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
 dpd 10 6 periodic
 nat force-encap
!

Peer5-F#show vpn-sip session remote-number  0612349999 detail
VPN-SIP session current status

Interface: Tunnel4
   Session status: SESSION_UP (R)
   Uptime         : 00:02:04
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 198.51.100.3:24845
   Local address:port : 198.51.100.22:50020
   Crypto conn handle: 0x8000004E
   SIP Handle         : 0x80000014
   SIP callID         : 24
   Configured/Negotiated bandwidth: 1000/1000 kbps
```

セッション開始のトラブルシューティング

症状

セッションが開始せず、Negotiating IKE 状態で停止します。

考えられる原因

大きな PKI 証明書が IKE 認証メッセージに含まれている状況で、IKE パケットがフラグメンテーションを起こしています。

推奨処置

ルータに IKEv2 フラグメンテーションを設定します。

debug コマンド

次のデバッグ コマンドを VPN SIP 設定のデバッグに使用できます。

表 *40* : デバッグ コマンド

コマンド名	説明
debug vpn-sip event	VPN SIP を使用した SVTI 登録、SIP 登録、コールセットアップなどのデバッグ メッセージを出力します。
debug vpn-sip errors	初期化、登録、コール セットアップなどの最中にエラーが発生した場合にのみ、エラーメッセージを出力します。
debug vpn-sip sip all	すべての SIP デバッグ トレースを有効化します。
debug vpn-sip sip calls	SIP SPI コールのデバッグ トレースを有効化します。
debug vpn-sip sip dhcp	SIP DHCP デバッグ トレースを有効化します。
debug vpn-sip sip error	SIP エラーのデバッグ トレースを有効化します。
debug vpn-sip sip events	SIP イベントのデバッグ トレースを有効化します。
debug vpn-sip sip feature	機能レベルでのデバッグを有効化します。
debug vpn-sip sip function	SIP 機能のデバッグ トレースを有効化します。
debug vpn-sip sip info	SIP 情報のデバッグ トレースを有効化します。
debug vpn-sip sip level	情報レベルでのデバッグを有効化します。
debug vpn-sip sip media	SIP メディアのデバッグ トレースを有効化します。
debug vpn-sip sip messages	SIP SPI メッセージのデバッグ トレースを有効化します。
debug vpn-sip sip non-call	コール コンテキスト以外のトレース（OPTIONS、SUBSCRIBE など）を有効化します。
debug vpn-sip sip preauth	SIP 事前認証のデバッグ トレースを有効化します。
debug vpn-sip sip states	SIP SPI 状態のデバッグ トレースを有効化します。

コマンド名	説明
debug vpn-sip sip translate	SIP変換のデバッグ トレースを有効化します。
debug vpn-sip sip transport	SIP トランスポートのデバッグ トレースを有効化します。
debug vpn-sip sip verbose	デバッグ モードを有効化します。

VPN SIP に関する追加情報

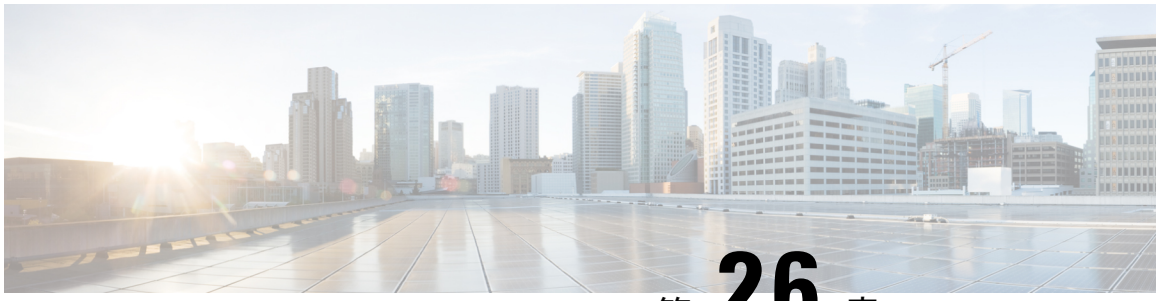
標準および RFC

標準/RFC	タイトル
RFC 6193（制約事項付き）	セッション記述プロトコル（SDP）におけるIKEのメディア記述

VPN SIP の機能情報

表 *41 : VPN SIP* の機能情報

機能名	リリース	機能情報
Session Initiation Protocol トリガー VPN		VPN SIP は、サービス プロバイダーが提供するサービスで、Session Initiation Protocol（SIP）を使用して、オンデマンド メディアやピア間のアプリケーション共有に必要な VPN が設定されます。 次のコマンドが導入されました：**nat force-encap, show vpn-sip session, show vpn-sip sip, show vpn-sip registration-status, vpn-sip local-number, vpn-sip logging, vpn-sip tunnel source**



第 26 章

音声機能の設定

この章では、Cisco 4000 シリーズ サービス統合型ルータ（ISR）での音声機能の設定について説明します。

この章の内容は、次のとおりです。

コール ウェイティング

コール待機機能を使用すると、別のコールでの通話中に、別のコールを受信できます。別のコールが着信すると、コール ウェイティング トーン（300 ms 間のトーン）が聞こえます。発信者 ID がサポートされる電話機には、発信者 ID が表示されます。フックフラッシュを使用して、待ち状態のコールに応答し、アクティブだったコールを保留状態にできます。フックフラッシュを使用すると、アクティブ コールと保留中のコールとの間を入れ替えることができます。コール ウェイティング機能がディセーブルの場合に、現在のコールを終了した場合、2 つ目のコールではビジー トーンが聞こえます。コールウェイティングの詳細については、http://www.cisco.com/c/en/us/td/docs/ios/voice/sip/configuration/guide/15_0/sip_15_0_book/sip_cg-hookflash.html#wp999028を参照してください。

着信転送

コール転送は、2 つ目のコールが 2 人のユーザ間で確立される間に、アクティブ コールが保留状態にされることです。2 つ目のコールを確立して、アクティブ コールを終了した後に、保留中のコールでは、リングバックが聞こえます。コール転送機能によって、ブラインド、準在席、在席の、コール転送の 3 つのタイプすべてがサポートされます。コール転送の詳細については、http://www.cisco.com/c/en/us/td/docs/ios/voice/sip/configuration/guide/15_0/sip_15_0_book/sip_cg-hookflash.html#wp999084を参照してください。

E1 R2 シグナリングの設定

E1 R2 を設定するには、次の手順に従います。

始める前に

この設定を開始する前に、次の前提条件が満たされていることを確認してください。

- R2 シグナリングは、E1 コントローラにのみ適用されます。
- R2 シグナリングを Cisco 4000 シリーズ ISR 上で実行するには、次のハードウェアが必要です。
- NIM-MFT-1T1/E1 または NIM-2MFT-T1/E1 または NIM-4MFT-T1/E1 または NIM-8MFT-T1/E1 または NIM-1CE1T1-PRI または NIM-2CE1T1-PRI または NIM-8CE1T1-PRI
- Cisco 4000 シリーズ ISR の E1 コントローラで ds0-group コマンドを定義します。
- Cisco IOS XE ソフトウェアリリース 15.5 (2)

手順の概要

1. コントローラ E1 を、自動構内交換式（PBX）またはスイッチに接続するように設定します。
2. E1 フレーミングの場合は、**CRC** または **non-CRC** のいずれかを選択します。
3. E1 ラインコーディングの場合は、**HDB3** または **AMI** のいずれかを選択します。
4. E1 クロックソースの場合は、internal または line のいずれかを選択します。クロックソースではさまざまな PBX にそれぞれの要件があることに注意してください。
5. 回線シグナリングを設定します。
6. レジスタ間シグナリングを設定します。
7. cas-custom を使用して、設定をカスタマイズします。

手順の詳細

ステップ 1 コントローラ E1 を、自動構内交換式（PBX）またはスイッチに接続するように設定します。

E1 のフレーミングとラインコーディングが正しく設定されていることを確認します。

ステップ 2 E1 フレーミングの場合は、**CRC** または **non-CRC** のいずれかを選択します。

ステップ 3 E1 ラインコーディングの場合は、**HDB3** または **AMI** のいずれかを選択します。

ステップ 4 E1 クロックソースの場合は、internal または line のいずれかを選択します。クロックソースではさまざまな PBX にそれぞれの要件があることに注意してください。

ステップ 5 回線シグナリングを設定します。

```
(config)# controller E1 0/2/0
```

```
 (config-controller)#ds0-group 1 timeslots 1 type ?
...
r2-analog        R2 ITU Q411
r2-digital       R2 ITU Q421
r2-pulse         R2 ITU Supplement 7
...
```

ステップ 6 レジスタ間シグナリングを設定します。

```
(config)# controller E1 0/2/0
```

```
 eefje(config)# controller E1 0/2/0
 eefje(config-controller)#ds0-group 1 timeslots 1 type r2-digital ?
dtmf               DTMF tone signaling
r2-compelled       R2 Compelled Register Signaling
r2-non-compelled   R2 Non Compelled Register Signaling
r2-semi-compelled  R2 Semi Compelled Register Signaling

...
```

シスコ実装のR2シグナリングには、デフォルトで有効になっている着信番号識別サービス（DNIS）サポートがあります。自動番号識別（ANI）オプションを有効にしても、DNIS情報の収集は引き続き実行されます。ANIオプションを指定しても、DNIS収集は無効になりません。DNISは着信側の番号、ANIは発信側の番号です。たとえば、Aというルータで Bというルータを呼び出すように設定する場合、DNIS番号はルータ Bに割り当てられ、ANI番号はルータ Aに割り当てられます。ANIは発信者 IDと似ています。

ステップ 7 cas-customを使用して、設定をカスタマイズします。

```
(config)# controller E1 0/2/0
```

```
(config-controller)#ds0-group 1 timeslots 1 type r2-digital r2-compelled ani
cas-custom 1
  country brazil
  metering
  answer-signal group-b 1

voice-port 0/2/0:1
!
dial-peer voice 200 pots
destination-pattern 43200
direct-inward-dial
port 0/2/0:1

dial-peer voice 3925 voip
destination-pattern 39...
session target ipv4:10.5.25.41
...
```

R2の設定

このドキュメントの論点となっている情報のみが表示されるように、設定は変更されています。

```
Configured for R2 Digital Non-Compelled

hostname eefje
!
```

```
controller E1 0
 clock source line primary
 dso-group 1 timeslots 1-15 type r2-digital r2-non-compelled
 cas-custom 1

!--- For more information on these commands
!--- refer to
ds0-group
 and
cas-custom.

!
voice-port 0:1
 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
cptone
.

!
dial-peer voice 123 pots
 destination-pattern 123
 direct-inward-dial
 port 0:1
 prefix 123
!
dial-peer voice 567 voip
 destination-pattern 567
 session target ipv4:10.0.0.2
```

Configured for R2 Digital Semi-Compelled

```
hostname eefje
!
controller E1 0
 clock source line primary
 ds0-group 1 timeslots 1-15 type r2-digital r2-semi-compelled
 cas-custom 1

!--- For more information on these commands
!---  refer to
ds0-group
 and
cas-custom
.

!
voice-port 0:1
 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
cptone
.

dial-peer voice 123 pots
 destination-pattern 123
 direct-inward-dial
 port 0:1
 prefix 123
!
dial-peer voice 567 voip
 destination-pattern 567
 session target ipv4:10.0.0.2
```

Configured for R2 Digital Compelled ANI

```
hostname eefje
! controller E1 0 clock source line primary ds0-group
1 timeslots 1-15 type r2-digital r2-compelled ani cas-custom 1

!--- For more information on these commands
!---  refer to
ds0-group
 and
cas-custom
.

voice-port 0:1 cptone BE

!--- The cptone command is country specific. For more
!--- information on this command,  refer to
cptone
.

dial-peer voice 123 pots destination-pattern 123 direct-inward-dial port
0:1 prefix 123
!
dial-peer voice 567 voip destination-pattern 567 session
target ipv4:10.0.0.2
```

Sample Debug Command Output

This example shows the output for the **debug vpm sig** command.

```
(config-controller)#debug vpm sig
Syslog logging: enabled
(0 messages dropped, 9 messages rate-limited, 1 flushes, 0 overruns,
 xml disabled, filtering disabled)No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled

Buffer logging:  level debugging, 163274 messages logged, xml disabled,filtering disabled

Exception Logging: size (4096 bytes)    Count and timestamp logging messages: disabled

Persistent logging: disabledNo active filter modules.
Trap logging: level informational, 172 message lines logged
Logging Source-Interface:
VRF Name:Log Buffer (4096 bytes):0): DSX (E1 0/2/0:0): STATE: R2_IN_COLLECT_DNIS R2 Got
 Event 1
*Jan 29 21:32:22.258:r2_reg_generate_digits(0/2/0:1(1)): Tx digit '1'
*Jan 29 21:32:22.369: htsp_digit_ready(0/2/0:1(1)): Rx digit='#'
*Jan 29 21:32:22.369: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0):STATE: R2_IN_COLLECT_DNIS
 R2 Got Event R2_TONE_OFF
*Jan 29 21:32:22.369: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '#'
*Jan 29 21:32:22.569: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:25.258: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0):STATE: R2_IN_COLLECT_DNIS
 R2 Got Event R2_TONE_TIMER
*Jan 29 21:32:25.258: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '3#'
*Jan 29 21:32:25.520: htsp_digit_ready_up(0/2/0:1(1)): Rx digit='1'
*Jan 29 21:32:25.520: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_CATEGORY
R2 Got Event 1
*Jan 29 21:32:25.520: Enter r2_comp_category
*Jan 29 21:32:25.520: R2 Event : 1
*Jan 29 21:32:25.520:  ####### collect_call_enable = 0
*Jan 29 21:32:25.520: ######## Not Sending B7 ##################
*Jan 29 21:32:25.520: r2_reg_event_proc(0/2/0:1(1)) ADDR_INFO_COLLECTED (DNIS=39001,
```

```
ANI=39700)
*Jan 29 21:32:25.520: r2_reg_process_event: [0/2/0:1(1), R2_REG_COLLECTING,
E_R2_REG_ADDR_COLLECTED(89)]
*Jan 29 21:32:25.520: r2_reg_ic_addr_collected(0/2/0:1(1))htsp_switch_ind
*Jan 29 21:32:25.521: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_SETUP_ACK]
*Jan 29 21:32:25.521: r2_q421_ic_setup_ack(0/2/0:1(1)) E_HTSP_SETUP_ACK
*Jan 29 21:32:25.521: r2_reg_switch(0/2/0:1(1))
*Jan 29 21:32:25.521: r2_reg_process_event: [0/2/0:1(1), R2_REG_WAIT_FOR_SWITCH,
E_R2_REG_SWITCH(96)]
*Jan 29 21:32:25.521: r2_reg_ic_switched(0/2/0:1(1))
*Jan 29 21:32:25.522: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_PROCEEDING]
*Jan 29 21:32:25.530:htsp_call_bridged invoked
*Jan 29 21:32:25.530: r2_reg_event_proc(0/2/0:1(1)) ALERTING RECEIVED
*Jan 29 21:32:25.530: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE:
R2_IN_WAIT_REMOTE_ALERT R2 Got Event R2_ALERTING
*Jan 29 21:32:25.530:rx R2_ALERTING in r2_comp_wait_remote_alert
*Jan 29 21:32:25.530: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '1'htsp_alert_notify
*Jan 29 21:32:25.531:r2_reg_event_proc(0/2/0:1(1)) ALERTING RECEIVED
*Jan 29 21:32:25.531: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_COMPLETE
R2 Got Event R2_ALERTING
*Jan 29 21:32:25.540: htsp_dsp_message: RESP_SIG_STATUS: state=0x0 timestamp=0
systime=80352360
*Jan 29 21:32:25.540:htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_DSP_SIG_0000]
*Jan 29 21:32:25.651: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:25.751: htsp_digit_ready(0/2/0:1(1)): Rx digit='#'
*Jan 29 21:32:25.751: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_COMPLETE
R2 Got Event R2_TONE_OFF
*Jan 29 21:32:25.751: r2_reg_generate_digits(0/2/0:1(1)): Tx digit '#'
*Jan 29 21:32:25.961: htsp_dialing_done(0/2/0:1(1))
*Jan 29 21:32:26.752: R2 Incoming Voice(0/0): DSX (E1 0/2/0:0): STATE: R2_IN_WAIT_GUARD
 R2 Got Event R2_TONE_TIMER
*Jan 29 21:32:26.752: R2_IN_CONNECT: call end dial
*Jan 29 21:32:26.752: r2_reg_end_dial(0/2/0:1(1))htsp_call_service_msghtsp_call_service_msg
 not EFXS (11)htsp_call_service_msghtsp_call_service_msg not EFXS (11)
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:26.754: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_VOICE_CUT_THROUGH]
*Jan 29 21:32:51.909: htsp_process_event: [0/2/0:1(1), R2_Q421_IC_WAIT_ANSWER,
E_HTSP_CONNECT]
*Jan 29 21:32:51.909: r2_q421_ic_answer(0/2/0:1(1)) E_HTSP_CONNECT
*Jan 29 21:32:51.909: r2_q421_ic_answer(0/2/0:1(1)) Tx ANSWER seizure: delay 0 ms,elapsed
 32419 msvnm_dsp_set_sig_state:[R2 Q.421 0/2/0:1(1)] set signal state = 0x4
*Jan 29 21:32:51.910: r2_reg_channel_connected(0/2/0:1(1))
*Jan 29 21:32:51.910: r2_reg_process_event: [0/2/0:1(1), R2_REG_WAIT_FOR_CONNECT,
E_R2_REG_CONNECT(90)]
*Jan 29 21:32:51.910: r2_reg_connect(0/2/0:1(1))htsp_call_service_msghtsp_call_service_msg
 not EFXS (11)
```

This example shows the output for the **debug vtsp all** command.

```
(config-controller)#debug vtsp all
Log Buffer (4096 bytes)::S_R2_DIALING_COMP, event:E_VTSP_DIGIT_END]
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_digit:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_TSP_R2_DIAL]
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_dial:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dial_nopush:
*Jan 29 21:56:33.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/ds_do_dial:     Digits To
```

```
 Dial=#
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_dial_done_cb:
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_VTSP_DSM_DIALING_COMPLETE]
*Jan 29 21:56:33.901: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/dc_dialing_done:
*Jan 29 21:56:34.690: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_R2_DIALING_COMP, event:E_TSP_R2_END_DIAL]
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/ds_end_dial:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_digit_pop:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_digit_pop:     Digit
 Reporting=FALSE
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_alert_dial_complete:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
 Stop Time=80497275
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
   Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
 Stop Time=80497275
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
   Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.691: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_peer_event_cb:
   Event=E_DSM_CC_CAPS_ACK
*Jan 29 21:56:34.692: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
     Feature ID=0, Feature Status=1
*Jan 29 21:56:34.692: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.692:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
     Feature ID=0, Feature Status=1
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.693:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_feature_notify_cb:
     Feature ID=0, Feature Status=1
*Jan 29 21:56:34.693: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:

*Jan 29 21:56:34.693:
//213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_reactivate_ringback:exit@1299
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
 Name
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
 Number 39701
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_call_connect: Connected
 oct3a  30
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_ALERTING, event:E_CC_CONNECT]
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_alert_connect:
Progress Indication=2
*Jan 29 21:56:58.140: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_ring_noan_timer_stop:
     Timer Stop Time=80499620
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_process_event:
[state:S_CONNECT, event:E_CC_SERVICE_MSG]
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/act_service_msg_down:
*Jan 29 21:56:58.142: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_timer_stop:     Timer
 Stop Time=80499620
*Jan 29 21:56:58.144: //213/85E8EDFC81D1/VTSP:(0/2/0:1):0:1:1/vtsp_dsm_fpi_event_cb:
  Event=E_DSMP_FPI_ENABLE_TDM_RTCP
```

機能グループ D の設定

機能グループ D シグナリングを設定するには、次の手順を実行します。

始める前に

機能グループ D シグナリングは、IOS XE リリース 15.5 (2) 以降、Cisco 4000 シリーズ サービス統合型ルータでサポートされています。機能グループ D サービスは、電話の顧客が長距離ネットワークを選択し、使用するキャリアに関係なく同じ桁数の番号を使用できるトランク側接続です。ルータは、キャリア環境内の音声トラフィックをサポートするために、機能グループ D を使用して長距離通信事業者とインターフェイス接続します。

この設定を開始する前に、次の前提条件が満たされていることを確認してください。

- プラットフォームでは、デジタル T1/E1 パケット音声トランク ネットワーク モジュールが使用されている必要があります。
- デジタル T1/E1 パケット音声トランク ネットワーク モジュールには、音声/WAN インターフェイス ネットワーク モジュール（NIM）用のスロットを 1 つまたは 2 つ搭載できます。NIM は 1 ー 8 個のポートをサポートします。デジタル E1 パケット音声トランク ネットワーク モジュールでは、デュアルモード（音声/WAN）マルチトランクカードのみがサポートされ、古い VIC はサポートされません。
- ドロップアンドインサート機能は、複数の同じカード上の 2 つのポート間でのみサポートされます。

手順の概要

1. **configure terminal** {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. **voice-card slot/subslot**
3. **controller T1/E1 slot/subslot/port**
4. **framing** {*sf* | *esf* }
5. **linecode** {*b8zs* | *ami*}
6. **ds0-group** *ds0-group-no***timeslots** `timeslot-list type`{*e&m-fgd* | *fgd-eana*}
7. **no shutdown**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** {*ip-address* | *interface-type interface-number* [*ip-address*]} 例： `Router(config)# 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	**voice-card slot/subslot** 例： `Router(config)# voice-card slot/subslot`	音声カードインターフェイス コンフィギュレーション モードを開始し、使用中のルータに応じて 0 ー 5 の値を使用してスロットの場所を指定します。
ステップ 3	**controller T1/E1 slot/subslot/port** 例： `Router(config)# controller T1 slot/subslot/port`	指定されたスロット/ポートの場所で、T1 コントローラのコントローラ コンフィギュレーション モードを開始します。スロットとポートの有効な値は 0 と 1 です。
ステップ 4	**framing** {*sf* | *esf* } 例： `Router(config)# framing {sf | esf}`	サービスプロバイダーの指示に従って、フレーミングを設定します。Extended Superframe（ESF）形式または Superframe（SF）形式を選択します。
ステップ 5	**linecode** {*b8zs* | *ami*}	サービスプロバイダーの指示に従って、回線エンコーディングを設定します。Bipolar-8 Zero Substitution（B8ZS）では、回線コーディング違反を検出するために、連続した 8 つの 0 を一意のバイナリシーケンスにエンコードします。Alternate Mark Inversion（AMI）では、各ビットセルで 01 を使用してゼロを表し、各ビットセルで 11 または 00 を交互に使用して 1 を表します。AMI では、送信側デバイスが ones density を維持する必要があります。ones density がデータストリームと無関係に維持されることはありません。
ステップ 6	**ds0-group** *ds0-group-no* **timeslots** *timeslot-list type*{*e&m-fgd* | *fgd-eana*}	圧縮音声コールで使用される T1 チャネルと、ルータが PBX または CO に接続するために使用するシグナリング方法を定義します。ds0-group-no は、DS0 グループを特定する 0 ～ 23 の値です。（注）ds0-group コマンドは、slot/port:ds0-group-no の形式で番号が付けられた論理音声ポートを自動的に作成します。作成される音声ポートは 1 つだけですが、該当するコールはグループ内の任意のチャネルにルーティングされます。timeslot-list は、単一の数字、カンマで区切られた複数の数字、またはタイムスロットの範囲を示すハイフンで区切られた数字のペアです。T1 に指定できる値は 1 ー 24 です。個々の DS0 タイムスロットをマッピングするには、追加のグループを定義します。システムは、定義された各グループに追加の音声ポートをマッピングします。タイプに応じたシグナリング方式の選択は、構築する接続によって異なります。e&m-fgd 設定では、

	コマンドまたはアクション	目的
		PBX トランク回線（タイ回線）および電話機器の E&M インターフェイス接続で、機能グループ D のスイッチアクセスサービスを使用できます。fgd-eana 設定では、Exchange Access North American（EANA）シグナリングがサポートされます。
ステップ 7	**no shutdown**	コントローラをアクティブにします。
ステップ 8	**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。ドロップアンドインサートを設定しない場合は、次の手順をスキップします。

メディア認証およびシグナリング認証と暗号化

Cisco IOS MGCP ゲートウェイのメディアおよびシグナリング認証および暗号化機能により、MGCP ゲートウェイでのメディアおよびシグナリング暗号化に加えて、シグナリング認証を含む音声セキュリティ機能が導入されます。メディアおよびシグナリング認証および暗号化機能の詳細については、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/mgcp/configuration/15-mt/vm-15-mt-book/vm-gw-med-sig.html を参照してください。

マルチキャスト保留音

保留音（MOH）機能を使用すると、Cisco IOS MGCP 音声ゲートウェイを使用しているときに、音楽ストリーミングサービスに登録できます。MOH サーバーから、保留になっているオンネットおよびオフネットの発信者の音声インターフェイスに音楽がストリーミングされます。Cisco Communications Manager は、ストリーミング マルチキャスト MOH サーバーから提供される音楽を保留中のコールの発信者に再生する機能をサポートしています。

Cisco Unified Communications Manager またはゲートウェイに事前設定されたマルチキャストアドレスを使用することで、ゲートウェイは、ネットワークのデフォルトルータからブロードキャストされる Real-Time Transport Protocol（RTP）パケットを「リッスン」し、ネットワーク内の指定された音声インターフェイスにパケットをリレーできます。保留中のコールを開始できます。ただし、MGCP 制御アナログ電話機で保留音を開始することはできません。着信側が発信側を保留にするたびに、Cisco Communications Manager は、事前設定されたマルチキャストアドレスを介して RTP パケットを「保留」になっているインターフェイスにストリーミングするように MOHサーバーに要求します。このようにして、RTP パケットは、適切に設定された保留状態の音声インターフェイスにリレーされます。ゲートウェイでマルチキャストアドレスを設定すると、ゲートウェイは、デフォルトルータにインターネットゲートウェイ管理プロトコル（IGMP）「join」メッセージを送信し、RTP マルチキャストパケットを受信する準備ができたことを示します。

複数の MOH サーバーが同じネットワークに存在する可能性がありますが、各サーバーには異なるクラス D IPアドレスが必要であり、そのアドレスは Cisco Communications Manager と MGCP

音声ゲートウェイで設定する必要があります。MOH の設定の詳細については、http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/voice/cminterop/configuration/15-0m/vc-15-0m-book/vc-ucm-mgcp-gw.html#GUID-A3461142-2F05-4420-AEE6-032FCA3B7952 を参照してください。

SCCP ゲートウェイでの TLS 1.2 のサポート

「SCCP ゲートウェイでの TLS 1.2 サポート」では、ユニキャスト会議ブリッジを含むデジタルシグナルプロセッサ（DSP）ファームの SCCP プロトコルでの TLS 1.2 設定について詳しく説明します。

（CFB）、メディア ターミネーション ポイント（MTP）、および SCCP テレフォニー制御（STC）アプリケーション（STCAPP）。

ゲートウェイ上の DSP は、変換またはトランスコーディングのメディアリソースとして使用できます。各メディアリソースは、Secure Skinny Client Control Protocol（SCCP）を使用して Cisco Unified Communications Manager と通信します。現在、TLS 1.0 と同等の SSL 3.1 がセキュアな信号の送信に使用されています。この機能により、TLS 1.2 のサポートが強化されます。Cisco IOS XE Cupertino 17.7.1a 以降、TLS 1.2 が拡張され、次世代暗号化（NGE）暗号スイートをサポートするようになりました。

（注） Cisco Unified Communications Manager（CUCM）バージョン 14SU2 は、AA:22:BB:44:55 または AA22BB4455 のように、コロン付きまたはコロンなしのサブジェクト名フィールド（CN 名）を持つセキュアな SCCP ゲートウェイをサポートするように拡張されました。

CUCM は、SCCP ゲートウェイからの着信証明書の CN フィールドを確認し、このゲートウェイの CUCM に設定された DeviceName と照合して確認します。DeviceName には、ゲートウェイの MAC アドレスが含まれています。CUCM は、DeviceName の MAC アドレスをコロン付きの MAC アドレスに変換し（AA:22:BB:44:55 など）、ゲートウェイの証明書の CN 名で検証します。したがって、CUCM では、ゲートウェイが証明書内の CN フィールド、つまりサブジェクト名にコロン付きの MAC アドレスの使用が求められています。

国防情報システム局（DISA）の新しいガイドラインにより、サブジェクト名フィールド CN にはコロンを使用しないことが要件となっています。たとえば、AA22BB4455 です。

SCCP TLS 接続

CiscoSSL は OpenSSL に基づいています。SCCP は CiscoSSL を使用して通信信号を保護します。

リソースがセキュアモードで設定されている場合、SCCP アプリケーションは、Transport Layer Security（TLS）ハンドシェイクを完了するプロセスを開始します。ハンドシェイクの際、サーバーは、サポートされている TLS バージョンと暗号スイートに関する情報を CiscoSSL に送信します。以前は、SCCP セキュアシグナリングでは SSL 3.1 のみがサポートされていました。SSL 3.1 は TLS 1.0 と同等です。TLS 1.2 サポート機能は、SCCP セキュアシグナリングに TLS 1.2 サポートを導入します。

TLS ハンドシェイクが完了すると、SCCP に通知され、SCCP はプロセスを強制終了します。

ハンドシェイクが正常に完了すると、REGISTER メッセージがセキュアトンネル経由で Cisco Unified Communications Manager に送信されます。ハンドシェイクが失敗し、再試行が必要な場合は、新しいプロセスが開始されます。

（注） SCCP ベースのシグナリングでは、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートのみがサポートされます。

暗号スイート

SCCP ベースのシグナリングでは、TLS_RSA_WITH_AES_128_CBC_SHA 暗号スイートがサポートされます。

Cisco IOS XE Cupertino 17.7.1a 以降、次の NGE 暗号スイートもサポートされます。

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

これらの暗号スイートにより、STCAPP アナログ電話と SCCP DSPFarm 会議サービスの両方でセキュアな音声シグナリングが可能になります。暗号スイートの選択は、ゲートウェイと CUCM の間でネゴシエートされます。

NGE 暗号スイートを使用するには、次の前提条件が適用されます。

- TLS 1.2 を設定します。詳細については、STC アプリケーションの TLS バージョンの設定（467 ページ）を参照してください。
- CUCM リリース 14.1 SU1 以降、および TLS 1.2 をサポートする音声ゲートウェイまたはプラットフォームを使用します。
- CUCM Web UI から、[Cipher Management] に移動し、[CIPHER switch] を [NGE] として設定します。詳細については、「暗号管理」を参照してください。

暗号スイートの確認の詳細については、TLS バージョンと暗号スイートの確認 （467 ページ）を参照してください。

SRTP で暗号化されたメディアの場合、より高度な暗号スイート（AEAD-AES-128-GCM または AEAD-AES-256-GCM）を使用できます。これらの暗号スイートの選択は、セキュアなアナログ音声とハードウェア会議ブリッジ音声メディアの両方について、GW と CUCM との間で自動的にネゴシエートされます。Authenticated Encryption with Associated Data（AEAD）暗号は、メッセージの完全性を検証する組み込みの SHA アルゴリズムを使用せずに機密性、完全性、および信頼性を同時に実現します。

サポートされるプラットフォーム

SCCP ゲートウェイ機能での TLS 1.2 サポートは、次のプラットフォームで使用できます。

- Cisco 4321 サービス統合型ルータ

- Cisco 4331 サービス統合型ルータ
- Cisco 4351 サービス統合型ルータ
- Cisco 4431 サービス統合型ルータ
- Cisco 4451-X サービス統合型ルータ
- Cisco 4461 サービス統合型ルータ
- Cisco Catalyst 8200 および 8300 シリーズ エッジ プラットフォーム
- Cisco VG400、VG420、および VG450 アナログ音声ゲートウェイ

STC アプリケーションの TLS バージョンの設定

STC アプリケーションの TLS バージョンを設定するには、次のタスクを実行します。

```
enable
configure terminal
stcapp security tls-version v1.2
exit
```

（注） stcapp security tls コマンドは、TLS バージョンをv.1.0、v1.1、または v1.2 のみに設定します。明示的に設定されない場合は、デフォルトで TLS v1.0 が選択されます。

DSP ファームプロファイルに対するセキュアモードでの TLS バージョンの設定

DSP ファームプロファイルの TLS バージョンをセキュアモードで設定するには、次のタスクを実行します。

```
enable
configure terminal
dspfarm profile 7 conference security
  tls-version v1.2
  exit
```

（注） 注意： **tls** コマンドは、セキュリティモードでのみ設定できます。

TLS バージョンと暗号スイートの確認

TLS バージョンと暗号スイートを確認するには、次のタスクを実行します。

```
# show dspfarm profile 100
Dspfarm Profile Configuration

 Profile ID = 100, Service = CONFERENCING, Resource ID = 2
 Profile Service Mode : secure
 Trustpoint : Overlord_DSPFarm_GW
 TLS Version  : v1.2
 TLS Cipher   : ECDHE-RSA-AES256-GCM-SHA384
 Profile Admin State : UP
```

```
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Total Number of Resources Configured : 10
 Total Number of Resources Available : 10
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Maximum conference participants : 8
 Codec Configuration: num_of_codecs:6
 Codec : g711ulaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g711alaw, Maximum Packetization Period : 30 , Transcoder: Not Required
 Codec : g729ar8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729abr8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729r8, Maximum Packetization Period : 60 , Transcoder: Not Required
 Codec : g729br8, Maximum Packetization Period : 60 , Transcoder: Not Required
```

STCAPP アプリケーションの TLS バージョンの確認

STCAPP アプリケーションの TLS バージョンを確認するには、次のタスクを実行します。

```
Device# show call application voice stcapp
App Status: Active
CCM Status: UP
CCM Group: 120
Registration Mode: CCM
Total Devices: 0
Total Calls in Progress: 0
Total Call Legs in Use: 0
ROH Timeout: 45
TLS Version: v1.2

# show stcapp dev voice 0/1/0
Port Identifier:  0/1/0
Device Type:      ALG
Device Id:        585
Device Name:      ANB3176C85F0080
Device Security Mode : Encrypted
  TLS version        : TLS version 1.2
  TLS cipher         : ECDHE-RSA-AES256-GCM-SHA384
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 80010
Dial Peer(s):     100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Line Mode:        CALL_CONF
Hook State:       OFFHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
HG Status:        Unknown
PLAR:             DISABLE
Callback State:   DISABLED
CWT Repetition Interval: 0 second(s) (no repetition)
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6
```

```
Call State for Connection 2 (ACTIVE): TsConnected
Connected Call Info:
   Call Reference: 33535871
   Call ID (DSP):  187
   Local IP Addr:  172.19.155.8
   Local IP Port:  8234
   Remote IP Addr: 172.19.155.61
   Remote IP Port: 8154
   Calling Number: 80010
   Called Number:
   Codec:          g711ulaw
   SRTP:           on
   RX Cipher:      AEAD_AES_256_GCM
   TX Cipher:      AEAD_AES_256_GCM
```

DSPfarm 接続の sRTP 暗号スイートを確認するには、次のタスクを実行します。

```
# show sccp connection detail

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id    conn_id    call-id    codec   pkt-period dtmf_method    type
bridge-info(bid, cid)   mmbridge-info(bid, cid) srtp_cryptosuite          dscp
                     call_ref   spid       conn_id_tx

16778224   -          125        N/A     N/A        rfc2833_pthru     confmsp   All
RTPSPI Callegs      All MM-MSP Callegs      N/A                       N/A
                     -          -          -

16778224   16777232   126        g711u   20         rfc2833_pthru  s- rtpspi    (101,125)
                N/A                       AEAD_AES_256_GCM          184
                     30751576   16777219   -

16778224   16777231   124        g711u   20         rfc2833_pthru  s- rtpspi    (100,125)
                N/A                       AEAD_AES_256_GCM          184
                     30751576   16777219   -


Total number of active session(s) 1, connection(s) 2, and callegs 3
```

コール情報の確認

フォワーディング プレーン インターフェイス（FPI）に保存されている TDM コールと IVR コールのコール情報を表示するには、**showvoipfpi calls** コマンドを使用します。コール ID を選択し、**show voip fpi calls confID** *call_id_number* コマンドを使用して暗号スイートを確認できます。次の例では、暗号スイート 6 は AES_256_GCM です。

```
#show voip fpi calls
Number of Calls : 2
---------- ---------- ---------- ---------- --------------- ---------------
    confID correlator    AcallID     BcallID           state           event
---------- ---------- ---------- ---------- --------------- ---------------
         1          1         87         88       ALLOCATED DETAIL_STAT_RSP
        21         21         89         90       ALLOCATED DETAIL_STAT_RSP

#show voip fpi calls confID 1
--------------------------------------------------------------------------------
VoIP-FPI call entry details:
--------------------------------------------------------------------------------
Call Type        :           TDM_IP     confID          :                1
correlator       :                1     call_state      :        ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :       1796860810
```

```
modify_start_time:                0      delete_start_time:                0
Media Type(SideA):              SRTP     cipher suite     :                6
------------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted              :         1
.....
```

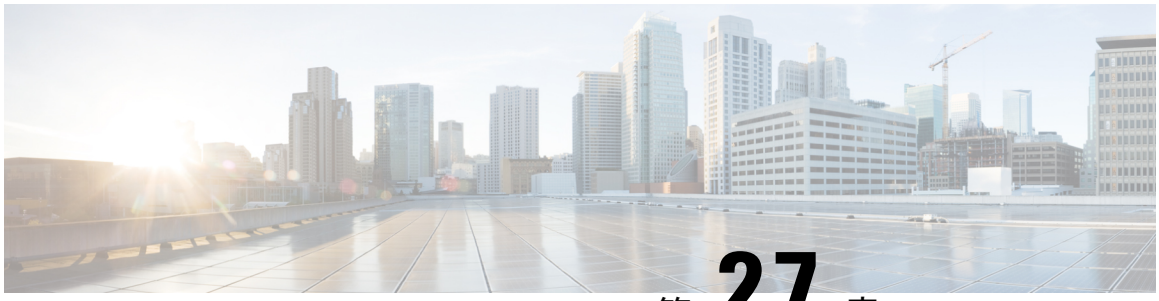
その他の参考資料

関連項目	マニュアル タイトル
Cisco IOS Voice Gateways Configuration Guide	Cisco IOS 音声ゲートウェイの FXS ポート用補足サービス機能コンフィギュレーション ガイド

SCCP ゲートウェイでの TLS 1.2 サポートの機能情報

表 *42 : SCCP* ゲートウェイでの *TLS 1.2* サポートの機能情報

機能名	リリース	機能情報
SCCP ゲートウェイでの TLS 1.2 のサポート	Cisco IOS XE Fuji 16.7.1	「SCCP ゲートウェイでの TLS 1.2 サポート」では、CFB、MTP、および STCAPP を含む DSP ファームの SCCP プロトコルでの TLS 1.2 設定について詳しく説明します。 次のコマンドが導入されました。**stcapp security tls-version**、**tls-version**
NGE 暗号スイートのサポート	Cisco IOS XE Cupertino 17.7.1a	この機能は、セキュアな音声シグナリングとセキュアなメディアでの NGE 暗号スイートをサポートします。これらの暗号スイートは、STCAPP アナログ電話と SCCP DSPFarm 会議サービスの両方に適用できます。



第 27 章

SNMP、Syslog、およびイーサネット OAM を使用した Dying Gasp

Dying Gasp：次のいずれかの回復不能な状態が発生します。

- システム リロード
- インターフェイスのシャットダウン
- 電源障害（特定のプラットフォームでサポート）

このタイプの状況はベンダー固有です。状況に関するイーサネット運用、管理、保守（OAM）通知がただちに送信される場合があります。

Dying Gasp サポートの前提条件

Dying Gasp 用の Simple Network Management Protocol（SNMP）を設定する前に、イーサネット OAM を有効にする必要があります。詳細については、『Enabling Ethernet OAM on an Interface』を参照してください。

Dying Gasp サポートの制約事項

- Cisco ISR 4000 プラットフォームのネイティブ ギガビット イーサネット インターフェイスは、次のシナリオでの Dying Gasp SNMP トラップの生成をサポートしていません。

- 電源装置（PSU）を取り外すと、ルータがダウンします。
- 電源ケーブルを取り外すと、ルーターがダウンします。

- Dying Gasp サポート機能は、CLI を使用して設定できません。SNMP を使用してホストを設定するには、以下の SNMP ホストの設定例を参照してください。
- Cisco IOS-XE Everest リリース 16.6.2 を実行している Cisco 4000 シリーズ ISR および Cisco 1100 シリーズ ISR でシステムのリロードまたはインターフェイスのシャットダウンが発生すると、Dying Gasp パケットがピアルータに送信されます。ただし、システム状態はシステムログ（syslog）または SNMP トラップでキャプチャされません。

SNMP、Syslog、およびイーサネット OAM を使用した Dying Gasp についての情報

Dying Gasp

IEEE 802.3ah で定義されている OAM 機能の 1 つにリモート障害表示があります。これは、品質の低下が原因で発生するイーサネット接続の障害の検出に役立ちます。イーサネット OAM は、OAM エンティティが、このような障害状態を OAM PDU の特定のフラグによってピアに伝達するメカニズムを提供します。障害状態について伝える方法の 1 つは、インターフェイスがシャットダウンされた場合など、回復不能な状態が発生したことを示す Dying Gasp です。このタイプの状況はベンダー固有です。障害状態に関する通知は、即座に、継続的に送信することができます。

SNMP、Syslog、およびイーサネット OAM を使用した Dying Gasp の設定方法

さまざまな SNMP サーバーのホスト/ポート設定に対する Dying Gasp トラップのサポート

（注） 最大 5 つの別個の SNMP サーバーホスト/ポートを設定できます。

ネットワーク管理サーバーでの環境設定

```
setenv SR_TRAP_TEST_PORT=UDP port
```

```
setenv SR_UTIL_COMMUNITY=public
setenv SR_UTIL_SNMP_VERSION=v2c
setenv SR_MGR_CONF_DIR=Path to the executable snmpinfo.DAT file
```

次に、ホストでの SNMP トラップ設定の例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)# snmp-server host 10.0.0.149 vrf Mgmt-intf version 2c public udp-port
6264
Router(config)#
Router(config)# ^Z
Router#
```

電源の再投入を実行すると、ルータコンソールに次の出力が表示されます。

```
Router#
System Bootstrap, Version 16.6(2r), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1994-2017  by cisco Systems, Inc.
Current image running: Boot ROM0
Last reset cause: LocalSoft
C1111-8PLTELA platform with 4194304 Kbytes of main memory
rommon 1 >

======================================
Dying Gasp Trap Received for the Power failure event:
------------------------------------------------------
  Trap on the Host
++++++++++++++

snmp-server host = 10.0.0.149 (nms1-lnx)  and SR_TRAP_TEST_PORT=6264
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 10.29.25.101
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
```

Dying Gasp 通知の受信時にピアルータに表示されるメッセージ

```
001689: *May 30 14:16:47.746 IST: %ETHERNET_OAM-6-RFI: The client on interface Gi0/0/0
has received a remote failure indication from its remote peer(failure reason = remote
client power failure action = )
```

Dying Gasp 通知の受信に関する SNMP 設定の表示

show running-config コマンドを使用して、Dying Gasp 通知を受信するための SNMP 設定を表示します。

```
Router# show running-config | i snmp
snmp-server community public RW
snmp-server host 10.0.0.149 vrf Mgmt-intf version 2c public udp-port 6264
Router#
```

SNMP、Syslog、およびイーサネット OAM を使用した Dying Gasp の設定例

例：ルータでの SNMP コミュニティストリングの設定

SNMP へのアクセスを許可するコミュニティ アクセス ストリングを設定します。

```
Router> enable
Router# configure terminal
Router(config)# snmp-server community public RW
Router(config)# exit
```

コマンドシンタックスと使用例の詳細については、『Cisco IOS Network Management Command Reference』を参照してください。

例：ルータコンソールにおける SNMP サーバーホストの詳細の設定

SNMP 通知動作の受信者を指定します。

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host X.X.X.XXX vrf mgmt-intf version 2c public udp-port 9800
Router(config)# exit
```

コマンドシンタックスと使用例の詳細については、『Cisco IOS Network Management Command Reference』を参照してください。

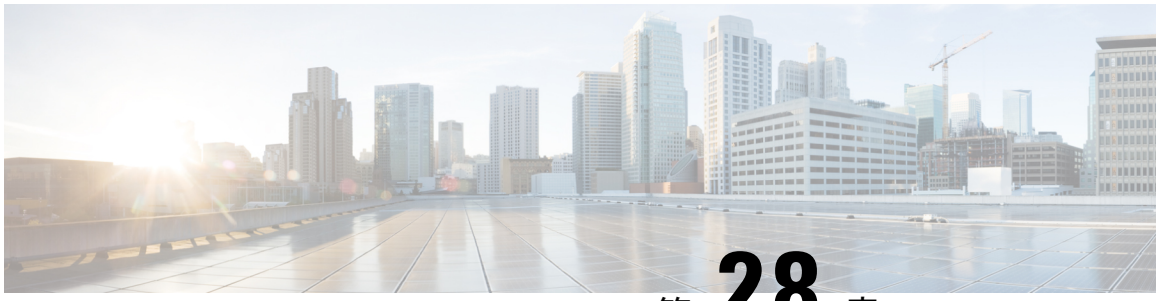
Dying Gasp サポートの機能情報

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

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

表 *43 : Dying Gasp* サポートの機能情報

機能名	リリース	機能情報
Dying Gasp	Cisco IOS XE リリース 16.6.2	イーサネットOAMは、OAMエンティティが障害状態をOAM PDU の特定のフラグによってピアに伝達するメカニズムを提供します。障害状態について伝える方法の 1 つは、インターフェイスがシャットダウンされた場合など、回復不能な状態が発生したことを示す Dying Gasp です。このタイプの状況はベンダー固有です。障害状態に関する通知は、即座に、継続的に送信することができます。



第 28 章

ソフトウェア メディア ターミネーション ポイントのサポート

ソフトウェア メディア ターミネーション ポイント（MTP）のサポート機能は、2 つの接続間のメディアストリームをブリッジして、Cisco Unified Communications Manager（CUCM）が SIP または H.323 エンドポイントを介してルーティングされたコールを Skinny Client Control Protocol（SCCP）コマンドでリレーできるようにします。これらのコマンドにより、CUCM はコール シグナリング用の MTP を確立できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

ソフトウェア メディア ターミネーション ポイントのサポートに関する情報

この機能は、ソフトウェア MTP サポートを Cisco Unified Border Element（Enterprise）に拡張します。ソフトウェア MTP は、Cisco UCM の大規模展開に不可欠なコンポーネントです。この機能により、新しい機能が有効になり、Cisco UBE が SIP トランキングに移行する大規模な展開でエンタープライズエッジのシスコ セッション ボーダー コントローラとして機能できるようになります。

ソフトウェア メディア ターミネーション ポイントの前提条件

- ソフトウェア MTP が適切に機能するには、着信コールレッグと発信コールレッグの両方に同じ方法でコーデックとパケット化を設定する必要があります。

ソフトウェア メディア ターミネーション ポイントの制約事項

- RSVP エージェントはソフトウェア MTP ではサポートされていません。
- 再パケット化のためのソフトウェア MTP はサポートされていません。
- コールしきい値は、スタンドアロンのソフトウェア MTP ではサポートされていません。
- コールごとのデバッグはサポートされていません。
- 同じ宛先 IP とポートを持つ複数の同時同期ソース（SSRC）はサポートされていません。

SRTP-DTMF インターワーキング

Cisco IOS XE 17.10.1a 以降、Secure Real-time Transport Protocol（SRTP）デュアルトーン多重周波数（DTMF）インターワーキングは、パススルーモードのソフトウェア MTP でサポートされています。SMTP は非セキュアコールの DTMF インターワーキングをサポートします。また、この機能はさらにセキュアコールの SRTP DTMF インターワーキングをサポートします。

この機能の CUCM サポートは、今後のリリースで実装される予定です。

SRTP-DTMF インターワーキングの制約事項

- SRTP-DTMF インターワーキング機能は、コーデックパススルー形式のみをサポートします。
- SRTP-DTMF インターワーキング機能は、同じ宛先 IP とポートを持つ複数の同時同期ソース（SSRC）をサポートしていません。

- SRTP-DTMF インターワーキングをサポートするコールは、非セキュア DTMF インターワーキングでサポートされるコールと比較すると、パフォーマンスにわずかな影響を与える可能性があります。

サポートされる SRTP-DTMF インターワーキングのプラットフォーム

Cisco IOS XE 17.10.1a 以降、次のプラットフォームは SMTP との SRTP DTMF インターワーキングをサポートしています。

- Cisco 4461 サービス統合型ルータ（ISR）
- Cisco Catalyst 8200 Edge シリーズ プラットフォーム
- Cisco Catalyst 8300 Edge シリーズ プラットフォーム
- Cisco Catalyst 8000V Edge ソフトウェア

ソフトウェア メディア ターミネーション ポイントのサポートの設定

ソフトウェア メディア ターミネーション ポイントのサポート機能を有効にして設定するには、次のタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-type interface-number* [**port** *port-number*]
4. **sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number*
5. **sccp**
6. **sccp ccm group** *group-number*
7. **associate ccm** *identifier-number* **priority** *number*
8. **associate profile** *profile-identifier* **register** *device-name*
9. **dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]
10. **trustpoint** *trustpoint-label*
11. **codec** *codec*
12. **maximum sessions** {**hardware** | **software**} *number*
13. **associate application sccp**
14. **no shutdown**

手順の詳細

	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。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	**configure terminal** 例： `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 3	**sccp local** *interface-type interface-number* [**port** *port-number*] 例： `Router(config)# sccp local gigabitethernet0/0/0`	Cisco UCM に登録するために SCCP アプリケーション（トランスコーディングと会議）が使用する、ローカルインターフェイスを選択します。 • *interface type*：インターフェイスアドレスまたは仮想インターフェイスアドレス（イーサネットなど）を指定できます。 • *interface number*：Cisco UCM に登録するために SCCP アプリケーションが使用するインターフェイス番号。 • （任意）**port** *port-number*：選択したインターフェイスで使用するポート番号。範囲は 1025 ～ 65535 です。デフォルトでは 2000 です。
ステップ 4	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number* 例： `Router(config)# sccp ccm 10.1.1.1 identifier 1 version 7.0+`	使用可能なサーバーのリストに Cisco UCM サーバーを追加し、次のパラメーターを設定します。 • *ipv4-address*：Cisco UCM サーバーの IP バージョン 4 アドレス。 • *ipv6-address*：Cisco UCM サーバーの IP バージョン 6 アドレス。 • *dns*：DNS 名。 • **identifier**：Cisco UCM サーバーを識別する番号を指定します。有効値の範囲は 1 ～ 65535 です。 • **port** *port-number*（任意）：TCP ポート番号を指定します。範囲は 1025 ～ 65535 です。デフォルトでは 2000 です。 • **version** *version-number*：Cisco UCM のバージョン。有効なバージョンは、3.0、3.1、3.2、3.3、

	コマンドまたはアクション	目的
		4.0、4.1、5.0.1、6.0、および7.0+ です。デフォルト値はありません。
ステップ 5	**sccp** 例： `Router(config)# sccp`	Skinny Client Control Protocol （SCCP）とそれに関連するアプリケーション（トランスコーディングと会議）を有効にします。
ステップ 6	**sccp ccm group** *group-number* 例： `Router(config)# sccp ccm group 10`	Cisco UCM グループを作成して、SCCP Cisco UCM コンフィギュレーション モードを開始します。 • *group-number*：Cisco UCM グループを識別します。範囲は 1 ～ 50 です。
ステップ 7	**associate ccm** *identifier-number* **priority** *number* 例： `Router(config-sccp-ccm)# associate ccm 10 priority 3`	Cisco UCM を Cisco UCM グループに関連付けて、グループ内の優先順位を設定します。 • *identifier-number*：Cisco UCM を識別します。有効値の範囲は1～65535 です。デフォルト値はありません。 • **priority** *number*：Cisco UCM グループ内の Cisco UCM の優先順位。範囲は 1 ～ 4 です。デフォルト値はありません。最も高い優先順位は 1 です。
ステップ 8	**associate profile** *profile-identifier* **register** *device-name* 例： `Router(config-sccp-ccm)# associate profile 1 register MTP0011`	DSP ファームプロファイルを Cisco UCM グループに関連付けます。 • *profile-identifier*：DSP ファームプロファイルを識別します。有効値の範囲は1～65535 です。デフォルト値はありません。 • **register** *device-name*：Cisco UCM 内のデバイス名。デバイス名は最大 15 文字まで入力できます。
ステップ 9	**dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**] 例： `Router(config-sccp-ccm)# dspfarm profile 1 mtp`	DSP ファーム プロファイル コンフィギュレーション モードを開始し、DSP ファームサービス用のプロファイルを定義します。 • *profile-identifier*：プロファイルを一意に識別する番号。有効値の範囲は 1 ～ 65535 です。デフォルトはありません。 • **conference**：会議用のプロファイルを有効にします。

	コマンドまたはアクション	目的
		• **mtp**：MTP用のプロファイルを有効にします。 • **transcode**：トランスコーディング用のプロファイルを有効にします。 • **security**（任意）：セキュアDSPファームサービス用のプロファイルを有効にします。設定例の詳細については、#unique_472 unique_472_Connect_42_GUID-5FB6A48E-204C-45AA-AE63-413B075A7871（483 ページ）の項を参照してください。
ステップ 10	**trustpoint** *trustpoint-label* 例： `Router(config-dspfarm-profile)# trustpoint dspfarm`	（任意）トラストポイントをDSPファーム プロファイルに関連付けます。
ステップ 11	**codec** *codec* 例： `Router(config-dspfarm-profile)# codec g711ulaw`	DSPファーム プロファイルでサポートされるコーデックを指定します。 • codec-type：優先されるコーデックを指定します。サポートされるコーデックのリストを表示するには、?を入力します。 サポートされるコーデックごとに、この手順を繰り返します。
ステップ 12	**maximum sessions** {**hardware** | **software**} *number* 例： `Router(config-dspfarm-profile)# maximum sessions software 10`	このプロファイルでサポートされる最大セッション数を指定します。 • **hardware**：MTPハードウェアリソースがサポートできるセッションの数。 • **software**：MTPソフトウェアリソースがサポートできるセッションの数。 • *number*：プロファイルでサポートされるセッションの数。範囲は0～xです。デフォルトは0です。xの値は、リソースプロバイダーで使用可能なリソースの数に応じて、実行時に決定されます。
ステップ 13	**associate application sccp** 例： `Router(config-dspfarm-profile)# associate application sccp`	SCCPをDSPファーム プロファイルに関連付けます。

	コマンドまたはアクション	目的
ステップ 14	**no shutdown** 例： `Router(config-dspfarm-profile)# no shutdown`	インターフェイスのステータスをUP状態に変更します。

例：ソフトウェア メディア ターミネーション ポイントのサポート

次に、ソフトウェアメディアターミネーションポイントのサポート機能の設定例を示します。

```
sccp local GigabitEthernet0/0/1
sccp ccm 10.13.40.148 identifier 1 version 6.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/0/1
 associate ccm 1 priority 1
 associate profile 6 register RR_RLS6
!
 dspfarm profile 6 mtp
 codec g711ulaw
 maximum sessions software 100
 associate application SCCP
!
!
gateway
media-inactivity-criteria all
timer receive-rtp 400
```

次に、セキュアな dspfarm プロファイルを使用した SRTP-DTMF インターワーキング機能の設定例を示します。

```
sccp local GigabitEthernet0/0/0
sccp ccm 172.18.151.125 identifier 1 version 7.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/0/0
 associate ccm 1 priority 1
 associate profile 1 register Router
!
dspfarm profile 1 mtp security
 trustpoint IOSCA
 codec g711ulaw
 codec pass-through
 tls-version v1.2
 maximum sessions software 5000
 associate application SCCP
```

（注） dspfarm プロファイルがコーデックパススルーでプロビジョニングされていて、TLS およびセキュリティ関連の設定がない場合、SR-TP トラフィックは SMTP リソースを通過できます。SRTP-DTMF インターワーキングのサポートを必要とするトラフィックフローの場合は、SMTP dspfarm プロファイルには **security** キーワードと TLS およびコーデックパススルー設定を含める必要があります。この dspfarm リソースプロファイルは、SRTP-DTMF インターワーキングサポートに関係なく、SRTP トラフィックを通過させることもできます。

ソフトウェア メディア ターミネーション ポイントの設定の確認

この機能を確認し、トラブルシューティングを行うには、次の **show** コマンドを使用します。

- SCCP に関する情報を確認するには、**show sccp** コマンドを使用します。

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.13.40.157, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.13.40.148, Port Number: 2000
                Priority: N/A, Version: 6.0, Identifier: 1
                Trustpoint: N/A
```

- DSPfarm プロファイルに関する情報を確認するには、**show dspfarm profile** コマンドを使用します。

```
Router# show dspfarm profile 6

Dspfarm Profile Configuration
 Profile ID = 6, Service = MTP, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Number of Resource Configured : 100
 Number of Resource Available : 100
 Hardware Configured Resources : 0
 Hardware Available Resources : 0
 Software Resources : 100
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
```

- セキュア DSPfarm プロファイルのステータスに関する情報を確認するには、**show dspfarm profile** コマンドを使用して、セキュアサービスモードが設定されていることを確認します。

```
Router# show dspfarm profile 2
Dspfarm Profile Configuration
 Profile ID = 2, Service = MTP, Resource ID = 2
 Profile Service Mode : secure
 Trustpoint : IOSCA
 TLS Version  : v1.2
 TLS Cipher   : AES128-SHA
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Total Number of Resources Configured : 8000
 Total Number of Resources Available : 8000
 Total Number of Resources Out of Service : 0
 Total Number of Resources Active : 0
 Hardware Configured Resources : 0
 Hardware Resources Out of Service: 0
 Software Configured Resources : 8000
 Number of Hardware Resources Active : 0
 Number of Software Resources Active : 0
 Codec Configuration: num_of_codecs:2
 Codec : pass-through, Maximum Packetization Period : 0
 Codec : g711ulaw, Maximum Packetization Period : 30
```

- SCCP 接続の統計を表示するには、**show sccp connections** コマンドを使用します。

```
Router# show sccp connections

sess_id   conn_id    stype  mode       codec    ripaddr         rport   sport
16808048  16789079    mtp   sendrecv   g711u    10.13.40.20     17510   7242
16808048  16789078    mtp   sendrecv   g711u    10.13.40.157    6900    18050
```

SMTP セキュア DTMF の場合、**show sccp connections** コマンドはコーデックタイプ（pass-th）、S タイプ（s-mtp）、および DTMF メソッド（rfc2833_pthru）に関する情報を表示します。

```
Router# show sccp connections

sess_id   conn_id   stype   mode      codec    sport  rport   ripaddr conn_id_tx
dtmf_method
16791234  16777308  s-mtp   sendrecv  pass_th  8006   24610   172.18.153.37
rfc2833_pthru
16791234  16777306  s-mtp   sendrecv  pass_th  8004   17576   172.18.154.2
rfc2833_report

Total number of active session(s) 1, and connection(s) 2
```

- RTP 接続に関する情報を表示するには、**show rtpspi call** コマンドを使用します。

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId  dstCallId   Mode      LocalRTP  RmtRTP  LocalIP     RemoteIP    SRTP
1    22      19         Snd-Rcv   7242      17510   0x90D080F   0x90D0814    0
2    19      22         Snd-Rcv   18050     6900    0x90D080F   0x90D080F    0
```

SRTP DTMF インターワーキングがアクティブになっている場合、SRTP フィールドにはゼロ以外の値が表示されます。

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId  dstCallId   Mode      LocalRTP  RmtRTP  LocalIP     RemoteIP    SRTP
```

```
1   13      14          Snd-Rcv   8024      18270   0xA7A5355   0xAC129A02   1
2   14      13          Snd-Rcv   8026      24768   0xA7A5355   0xAC129925   1
```

- VoIP RTP 接続に関する情報を表示するには、 **show voip rtp connections** コマンドを使用します。

```
Router# show voip rtp connections
VoIP RTP Port Usage Information
Max Ports Available: 30000, Ports Reserved: 100, Ports in Use: 102
Port range not configured, Min: 5500, Max: 65499
VoIP RTP active connections :
No. CallId    dstCallId  LocalRTP  RmtRTP    LocalIP         RemoteIP
1     114       117        19822    24556   10.13.40.157     10.13.40.157
2     115       116        24556    19822   10.13.40.157     10.13.40.157
3     116       115        19176    52625   10.13.40.157     10.13.40.20
4     117       114        16526    52624   10.13.40.157     10.13.40.20
```

- 具体的には、次のような **show** コマンドを使用できます。
  - **show sccp connection callid**
  - **show sccp connection connid**
  - **show sccp connection sessionid**
  - **show rtpspi call callid**
  - **show rtpspi stat callid**
  - **show voip rtp connection callid**
  - **show voip rtp connection type**
  - **show platform hardware qfp active feature sbc global**
- 特定の問題を切り分けるには、**debug sccp** コマンドを使用します。
  - **debug sccp** [**all** | **config** | **errors** | **events** | **keepalive** | **messages** | **packets** | **parser** | **tls**]

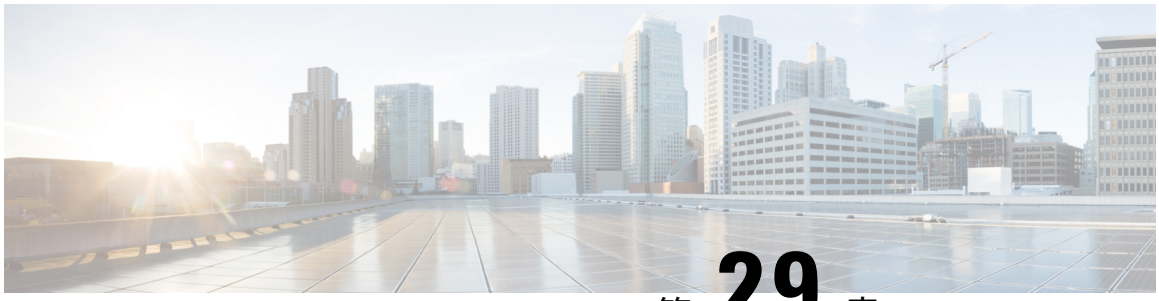
ソフトウェア メディア ターミネーション ポイントのサポートに関する機能情報

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

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

表 *44 :* ソフトウェア メディア ターミネーション ポイントのサポートに関する機能情報

機能名	リリース	機能情報
ソフトウェア メディア ターミネーション ポイントのサポート	Cisco IOS XE リリース 2.6 S	ソフトウェア メディア ターミネーション ポイント（MTP）は、Cisco Unified Communications Manager（Cisco UCM）が Skinny Client Control Protocol（SCCP）コマンドを介して音声ゲートウェイと対話する機能を提供します。これらのコマンドにより、Cisco UCM はコールシグナリング用の MTP を確立できます。
Secure Real-time Transport Protocol（SRTP）デュアルトーン多重周波数（DTMF）インターワーキングのサポート	Cisco IOS XE Dublin 17.10.1a	Secure Real-time Transport Protocol（SRTP）デュアルトーン多重周波数（DTMF）機能は、パススルーモードのみでの Secure Software MTP と CUCM との間の DTMF インターワーキングをサポートします。



第 29 章

Cisco 4000 シリーズ サービス統合型ルータでの LTE のサポート

この章では、Cisco 4000 シリーズ サービス統合型ルータ（ISR）での LTE のサポートについて説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。

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

セルラー モデム リンク リカバリの設定

セルラー モデム リンク リカバリ機能はデフォルトでは無効になっているため、リンク リカバリ機能を有効にすることを推奨します。

（注） Cisco IOS XE 17.11.1 以降では、リンクリカバリ機能により、セルラーモデムの RSRP（基準の受信信号強度）パラメータと RSRQ（基準の受信信号品質）パラメータが有効になります。

セルラー モデム リンク リカバリ機能を有効ルまたは無効にするには、次の手順に従います。

手順の概要

1. **configure terminal**
2. **controller cellular** *unit*
3. LTE モデムの場合、RSRP（基準の受信信号強度）と RSRQ（基準の受信信号品質）が信号品質の推奨指標となります。リンクリカバリのモニタリングパラメータとして RSRP または RSRQ を設定し、有効にするには、**lte modem link-recovery rsrp onset-threshold** コマンド（RSRP）および **lte modem link-recovery rsrq onset-threshold** コマンド（RSRQ）を使用します。リンクリカバリ機能を無効にするには、{**lte**} **modem link-recovery disable** | **no lte** | **modem link-recoverydisable**} コマンドを使用します。
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `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	**controller cellular** *unit* 例： `Router(config)# controller cellular 0/2/0`	セルラー コントローラ 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	LTE モデムの場合、RSRP（基準の受信信号強度）と RSRQ（基準の受信信号品質）が信号品質の推奨指標となります。リンクリカバリのモニタリングパラメータとして RSRP または RSRQ を設定し、有効にするには、**lte modem link-recovery rsrp onset-threshold** コマンド（RSRP）および **lte modem link-recovery rsrq onset-threshold** コマンド（RSRQ）を使用します。リンクリカバリ機能を無効にするには、{**lte**} **modem link-recovery disable**	**no lte**	**modem link-recoverydisable**} コマンドを使用します。
			例：
			`Router(config-controller)# lte modem link-recovery disable`
			`Router(config-controller)# no lte modem link-recovery disable`
			`Device#show run | sec controller Cellular 0/2/0`
			`controller Cellular 0/2/0`
			`lte modem link-recovery rssi onset-threshold -110`
			`lte modem link-recovery monitor-timer 20`
			`lte modem link-recovery wait-timer 10`
				セルラー モデムのリンク リカバリ機能を有効または無効にします。
				リンク リカバリを有効にすると、リンク リカバリ パラメータに対するデフォルトのシスコ推奨値が入力されます。
				例に示すように、各パラメータに CLI を使用することにより、リンクリカバリパラメータの値をデフォルトのシスコ推奨値から変更できます。
				（注） デフォルトのシスコ推奨値を変更すると、リンクリカバリ機能の理想的なパフォーマンスに影響を与えるため推奨されません。
				（注） 3 つのパラメータ（RSSI、RSRP、RSRQ）のうち、一度に設定できるのは 1 つだけです。リンクリカバリが有効になっているときにユーザーがパラメータを明示的に設定しない場合、システムは RSSI のデフォルト値にフォールバックします。

	コマンドまたはアクション	目的

	`lte modem link-recovery debounce-count 6`
	
	`Example:`
	`Device#configure terminal`
	`Device(config)#controller Cellular 0/2/0`
	`Device(config-controller)#lte modem link-recovery`
	
	`monitor-timer 30`
	`Device(config-controller)#lte modem wait-timer 15`
	`Device(config-controller)#lte modem debounce-count 8`
	`Device(config-controller)#lte modem rssi onset-threshold -100`
	
	例：
	
	RSRQ パラメータの場合：
	
	`Device#configure terminal`
	`Device(config)#controller Cellular 0/2/0`
	`Device(config-controller)#lte modem rsrq onset-threshold -19`
	
	RSRP パラメータの場合：
	
	`Device#configure terminal`
	`Device(config)#controller Cellular 0/2/0`
	`Device(config-controller)#lte modem rsrp onset-threshold -139`	

ステップ 4	**end** 例： `Router(config)# end`	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。

セルラー モデム リンク リカバリ パラメータ

セルラーリンクリカバリの動作を調整するために、設定可能なパラメータが3つあります。デフォルト値は、機能の最高のパフォーマンスのために最適化されているため、シスコが提言した場合を除き、変更は推奨されません。

次の表は、リンク リカバリ パラメータについて説明します。

表 *45:* リンク リカバリ パラメータ

パラメータ	説明
rssi onset-threshold	RSSI 値がこのパラメータの定義する値を下回った時に、リンクリカバリ機能が追加の調査をトリガーして潜在的な問題を探し、必要に応じてアクションを実行するようにします。このパラメータの範囲は -90 dBm ～ -125 dBm の範囲で設定できます。推奨のデフォルト値は -110 dBm です。
monitor-timer	このパラメータは、リンク リカバリが潜在的な問題をチェックする頻度を決定します。このパラメータのデフォルト値は20秒です。つまり、リンク リカバリ機能は20秒ごとにトリガーされ、特定のパラメータを確認して潜在的な問題があるかどうかを判断します。monitor-timer の範囲は 20 ～ 60 秒の範囲で設定できます。monitor-timer の値を 20 秒以上に増やすと、機能の応答時間が長くなります。
wait-timer と debounce-count	wait-timer パラメータは debounce-count パラメータとともに使用され、リンク リカバリ機能により、モデムの再起動により回復する必要がある潜在的な問題が特定された場合に、さらに頻繁に追加のチェックを実行します。wait-timer のデフォルト値は 10 秒で、debounce-count のデフォルト値は 6 です。この設定では、リンク リカバリが動作していないモデムの状態を特定した後、10 秒ごとに最大6回、追加のチェックを実行して、問題が解決されたかどうかを、モデムの電源再投入なしで確認します。debounce-count と wait-timer を短くすると、リンク リカバリが高速になります。これを減らすと、リカバリにかかる時間が長くなる可能性があります。wait-timer の設定可能な範囲は5～60秒です。debounce-count の設定可能な範囲は 6 ～ 20 秒です。

セルラー モデムのリンク リカバリ設定の確認

セルラーモデムのリンク リカバリが有効になっているかどうかを確認するには、**show controller cellularunit** コマンドを使用します。この例では、セルラー モデムのリンクリカバリ機能に関連する情報が強調表示されています。

```
Router# show controller cellular 0/2/0Interface Cellular0/2/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

Cellular Modem Configuration
==============================
Modem is recognized as valid
Power save mode is OFF
manufacture id =  0x00001199     product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status =  NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
---------------------------
SIM 0 is present
SIM 1 is not present
SIM 0 is active SIM

Module Reload Statistics
-------------------------
Soft OIR reloads = 0
Hard OIR reloads = 0
-------------------------

Modem Management Statistics
---------------------------
Modem resets = 1
Modem timeouts = 0
Link recovery is ON

Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6

Link recovery count is 0
```

セルラー モデムのリンク リカバリが発生し、モデムの電源が再投入されると、コンソール ログに %CELLWAN-2-MODEM_DOWN メッセージが表示されます。さらに、セルラー モデムのリンク リカバリ機能によってアクションが実行されたことを示す %CELLWAN-2-LINK_RECOVERY メッセージが表示されます。

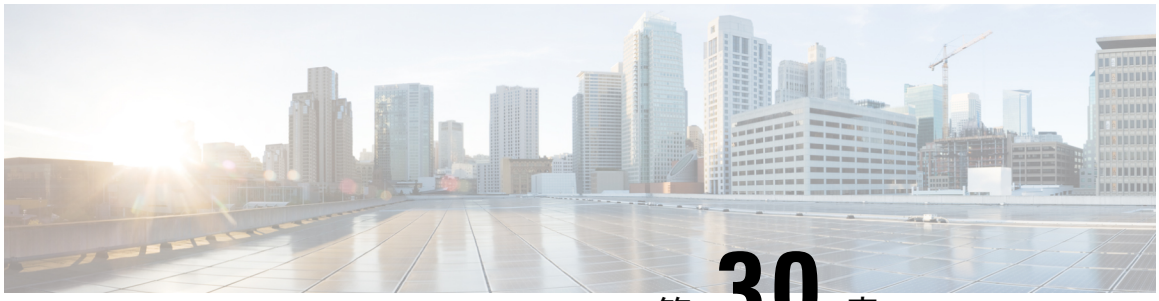
セルラー モデムのリンク リカバリが発生するたびに、show controller cellular unit コマンド出力の「モデムの管理統計情報」セクションにあるモデム タイムアウト カウンタが更新されます。最後のタイムアウト セクションのモデム パラメータには、リンクリカバリの引き金となった問題の原因を特定するのに役立つ情報が含まれています。

次のログの例では、メッセージ、モデムのタイムアウト カウンタ、および最後のタイムアウト時のモデムのパラメータが強調表示されています。

***Jul 19 17:15:18.980 PDT: %CELLWAN-2-LINK_RECOVERY: Cellular0/1/0: Cellular Modem has been power cycled**

```
Device#show controller Cellular 0/2/0
Interface Cellular0/2/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2
```

```
Cellular Modem Configuration
==============================
Modem is recognized as valid
Power save mode is OFF
manufacture id =  0x00001199     product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status =  NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
---------------------------
SIM 0 is present
SIM 1 is not present
SIM 0 is active SIM

Module Reload Statistics
-------------------------
Soft OIR reloads = 0
Hard OIR reloads = 0
-------------------------
 Modem Management Statistics
---------------------------
Modem resets = 1
Modem user initiated resets = 0
Modem user initiated power-cycles = 0
Modem timeouts = 1
Modem parameters at the last timeout:
         LTE first time attach State was No
         Radio Interface Technology Mode was AUTO
         Operating Mode was Online
         RSSI was -0 dBm
         Packet switch domain status was Not Attached
         Registration state(EMM) was Not Registered
         Downlink traffic was not present
Link recovery is ON
Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6
```



第 30 章

設定例

この章では、ルータでの一般的なネットワーキングタスクを設定する例を示します。この章に示されている例は、単なる説明用です。これらの例の背景情報はほとんど（またはまったく）提供されません。詳細については、ソフトウェアのインストール（103 ページ）を参照してください。

さらに、この項を読む際には、ネットワークに関する設定は複雑であり、何通りにも設定できることに留意してください。この項の例は、ある設定を実現する 1 つの方法を示しているだけです。

この章には、次の例が記載されています。

TFTP サーバからルータに統合パッケージをコピーする例

次に、TFTP サーバからルータに統合パッケージをコピーする例を示します。

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 17:48:41 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 17:49:14 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
```

```
7451738112 bytes total (7015186432 bytes free)
Router# copy tftp bootflash:
Address or name of remote host []? 10.81.116.4
Source filename []? rtp-isr4400-54/isr4400.bin
Destination filename [isr4400.bin]?
Accessing tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin...
Loading rtp-isr4400-54/isr4400.bin from 10.81.116.4 (via GigabitEthernet0): !!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 424317088 bytes]

424317088 bytes copied in 371.118 secs (1143348 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 17:48:41 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:05:07 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 18:01:41 +00:00  isr4400.bin

7451738112 bytes total (6590910464 bytes free)
```

ルータに保存されている統合パッケージを使用してブートするようにルータを設定する例

次に、ルータに保存されている統合パッケージを使用してブートするようルータを設定する例を示します。

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 17:48:41 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:05:07 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 18:01:41 +00:00  isr4400.bin

7451738112 bytes total (6590910464 bytes free)


Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# boot system bootflash:isr4400.bin
Router(config)# config-register 0x2102
Router(config)# exit
Router# show run | include boot
boot-start-marker
boot system bootflash:isr4400.bin
```

```
boot-end-marker
license boot level adventerprise
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 18:08:36.311 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit
with reload chassis code


Initializing Hardware ...

System integrity status: c0000600
Failures detected:
 Boot FPGA corrupt

Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2012  by cisco Systems, Inc.
Compiled Mon 06/18/2012 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory

File size is 0x194a90a0
Located isr4400.bin
Image size 424317088 inode num 13, bks cnt 103594 blk size 8*512
################################################################################################
Boot image size = 424317088 (0x194a90a0) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
 calculated 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
 expected   7294dffc:892a6c35:a7a133df:18c032fc:0670b303
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 5133 msec
Image validated
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (local/local): load_modules took: 2 seconds,
expected
max time 2 seconds

              Restricted Rights Legend
```

```
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706


Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental
Version
15.3(20120910:013018) [mcp_dev-BLD-BLD_MCP_DEV_LATEST_20120910_000023-ios 153]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 09-Sep-12 21:28 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2012 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.

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.

Warning:  the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133589K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Press RETURN to get started!
```

統合パッケージから同じファイル システムにサブパッケージを抽出する

次に、統合パッケージから同じファイルシステムにサブパッケージを抽出する例を示します。

request platform software package expand file bootflash:isr4400.bin コマンド（**to** オプションが使用されていない点に注意）を入力すると、統合パッケージのサブパッケージが **bootflash:** に解凍されます。

```
Router> enable
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:13:31 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 18:01:41 +00:00  isr4400.bin

7451738112 bytes total (6590029824 bytes free)
Router# request platform software package expand file bootflash:isr4400.bin
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:16:49 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 18:01:41 +00:00  isr4400.bin
778756  -rw-   112911096  Sep 13 2012 18:15:49 +00:00
isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778757  -rw-     2220784  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778758  -rw-      371440  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778759  -rw-     8080112  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778760  -rw-     9331440  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778761  -rw-      379632  Sep 13 2012 18:15:49 +00:00
isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
 --More--         778754  -rw-       10540  Sep 13 2012 18:15:48 +00:00
isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf
```

```
778762  -rw-    27218680  Sep 13 2012 18:15:50 +00:00
isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778763  -rw-    78938264  Sep 13 2012 18:15:50 +00:00
isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778764  -rw-    45177592  Sep 13 2012 18:15:50 +00:00
isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778765  -rw-   114662144  Sep 13 2012 18:16:01 +00:00
isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778766  -rw-    26360568  Sep 13 2012 18:16:03 +00:00
isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778767  -rw-    13091576  Sep 13 2012 18:16:06 +00:00
isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
778755  -rw-       11349  Sep 13 2012 18:16:06 +00:00  packages.conf

7451738112 bytes total (6150725632 bytes free)
```

統合パッケージから別のファイル システムにサブパッケージを抽出する

次に、統合パッケージから別のファイルシステムにサブパッケージを抽出する例を示します。

最初の **dir usb0:** コマンドは、**bootflash:** ディレクトリ内にサブパッケージがないことを示しています。

request platform software package expand file usb0:isr4400.bin to bootflash: コマンドの入力後に、**bootflash:** ディレクトリにサブパッケージが表示されます。isr4400.bin 統合パッケージファイルは **usb0:** ディレクトリの中にあります。

```
Router# dir usb0:
Directory of usb0:/

  121  -rwx   424317088  Sep 13 2012 18:27:50 +00:00  isr4400.bin

7988666368 bytes total (7564341248 bytes free)

Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:41:51 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb

7451738112 bytes total (6590418944 bytes free)
Router# request platform software package expand file usb0:isr4400.bin to bootflash:
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.
Router# dir bootflash:
Directory of bootflash:/
11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
```

```
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:46:52 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
454276  -rw-   112911096  Sep 13 2012 18:46:05 +00:00
isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454277  -rw-     2220784  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454278  -rw-      371440  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454279  -rw-     8080112  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454280  -rw-     9331440  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454281  -rw-      379632  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
 --More--         454274  -rw-       10540  Sep 13 2012 18:46:05 +00:00
isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf
454282  -rw-    27218680  Sep 13 2012 18:46:06 +00:00
isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454283  -rw-    78938264  Sep 13 2012 18:46:06 +00:00
isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454284  -rw-    45177592  Sep 13 2012 18:46:06 +00:00
isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454285  -rw-   114662144  Sep 13 2012 18:46:16 +00:00
isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454286  -rw-    26360568  Sep 13 2012 18:46:19 +00:00
isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454287  -rw-    13091576  Sep 13 2012 18:46:21 +00:00
isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454275  -rw-       11349  Sep 13 2012 18:46:21 +00:00  packages.conf

7451738112 bytes total (6575869952 bytes free)
```

サブパッケージを使用してブートするようルータを設定する

プロビジョニング ファイルとサブパッケージ ファイルをディレクトリに格納して、ルータを起動した後には、これらのファイルの名前変更、削除、変更を行わないようにしてください。ファイルの名前変更、削除、またはその他の変更を行うと、ルータで予期せぬ問題および動作が発生する可能性があります。統合パッケージの各バージョンには、たとえば次の表に示すようなサブパッケージが含まれています。ただし、統合パッケージの各バージョンには、各サブパッケージの異なるバージョンが含まれていることがあります。

表 *46 :* サブパッケージ

サブパッケージ	説明
RPBase	ルート プロセッサ（RP）のオペレーティング システム ソフトウェアを提供します。これは、唯一の起動可能なパッケージです。

サブパッケージ	説明
RPControl	Cisco IOS プロセスとプラットフォームの他の部分との間のインターフェイスとなるコントロール プレーン プロセスを制御します。
RPAccess	セキュアソケットレイヤ（SSL）、セキュア シェル（SSH）、その他のセキュリティ機能など、制限付きコンポーネントの処理をエクスポートします。
RPIOS	Cisco IOS XE 機能が保存および実行される場所となる Cisco IOS カーネルを提供します。各統合パッケージには、異なるバージョンの RPIOS が含まれています。
ESPBase	Embedded Services Processor（ESP）オペレーティング システム、制御プロセス、および ESP ソフトウェアを提供します。
SIPBase	制御プロセスを提供します。
SIPSPA	入出力（I/O）ドライバを提供します。
Firmware	ファームウェア サブパッケージ。サブパッケージ名には、ネットワーク情報モジュール（NIM）または Cisco 拡張サービス モジュールのいずれかを示すモジュール タイプが含まれています。

次の例は、サブパッケージを使って起動するようルータを設定する方法を示しています。

次の例に示すように、**dir bootflash:** コマンドにより、すべてのサブパッケージとプロビジョニングファイルが確実に同じファイルシステムに存在するようになります。

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:12:58 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:46:52 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
454276  -rw-   112911096  Sep 13 2012 18:46:05 +00:00
isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454277  -rw-     2220784  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454278  -rw-      371440  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454279  -rw-     8080112  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454280  -rw-     9331440  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454281  -rw-      379632  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
 --More--         454274  -rw-       10540  Sep 13 2012 18:46:05 +00:00
isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf
454282  -rw-    27218680  Sep 13 2012 18:46:06 +00:00
```

```
isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454283  -rw-    78938264  Sep 13 2012 18:46:06 +00:00
isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454284  -rw-    45177592  Sep 13 2012 18:46:06 +00:00
isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454285  -rw-   114662144  Sep 13 2012 18:46:16 +00:00
isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454286  -rw-    26360568  Sep 13 2012 18:46:19 +00:00
isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454287  -rw-    13091576  Sep 13 2012 18:46:21 +00:00
isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454275  -rw-       11349  Sep 13 2012 18:46:21 +00:00  packages.conf

7451738112 bytes total (6575869952 bytes free)

Router# show running | include boot
boot-start-marker
boot-end-marker
license boot level adventerprise
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# boot system bootflash:packages.conf
Router(config)# config-register 0x2102
Router(config)# exit
Router# show running | include boot
boot-start-marker
boot system bootflash:packages.conf
boot-end-marker
license boot level adventerprise
Router# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 18:49:39.720 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit
with reload chassis code


Initializing Hardware ...

System integrity status: c0000600
Failures detected:
 Boot FPGA corrupt


Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2012  by cisco Systems, Inc.
Compiled Mon 06/18/2012 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory
```

```
File size is 0x00002c55
Located packages.conf
Image size 11349 inode num 454275, bks cnt 3 blk size 8*512
#
File size is 0x04b48098
Located isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
Image size 78938264 inode num 454283, bks cnt 19273 blk size 8*512
################################################################################################################################################
Boot image size = 78938264 (0x4b48098) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
 calculated dbe960a6:d239245c:76d93622:d6c31a41:40e9e420
 expected   dbe960a6:d239245c:76d93622:d6c31a41:40e9e420
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 1159 msec
Image validated

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental
Version 15.3(20120910:013018) [mcp_dev-BLD-BLD_MCP_DEV_LATEST_20120910_000023-ios 153]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 09-Sep-12 21:28 by mcpre



Cisco IOS-XE software, Copyright (c) 2005-2012 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.



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.

Warning:  the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133589K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Press RETURN to get started!

Router>
Router> en
Router# show version
Cisco IOS XE Software, Version BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ext
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
 15.4(20140527:095327)
[v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ios 156]


IOS XE Version: BLD_V154_3_S_XE313_THROTTLE_LATEST

Cisco IOS-XE software, Copyright (c) 2005-2014 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 minute
Uptime for this control processor is 4 minutes
 --More--         System returned to ROM by reload
System image file is "bootflash:packages.conf"
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.

License Level: adventerprise
License Type: EvalRightToUse
 --More--         Next reload license Level: adventerprise

cisco ISR4451/K9 (2RU) processor with 1133589K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Configuration register is 0x2102

Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:53:29 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:54:03 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
454276  -rw-   112911096  Sep 13 2012 18:46:05 +00:00
isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454277  -rw-     2220784  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454278  -rw-      371440  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454279  -rw-     8080112  Sep 13 2012 18:46:05 +00:00
isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454280  -rw-     9331440  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454281  -rw-      379632  Sep 13 2012 18:46:06 +00:00
isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
 --More--         454274  -rw-       10540  Sep 13 2012 18:46:05 +00:00
isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf
454282  -rw-    27218680  Sep 13 2012 18:46:06 +00:00
isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454283  -rw-    78938264  Sep 13 2012 18:46:06 +00:00
isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454284  -rw-    45177592  Sep 13 2012 18:46:06 +00:00
isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454285  -rw-   114662144  Sep 13 2012 18:46:16 +00:00
isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454286  -rw-    26360568  Sep 13 2012 18:46:19 +00:00
isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454287  -rw-    13091576  Sep 13 2012 18:46:21 +00:00
isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg
454275  -rw-       11349  Sep 13 2012 18:46:21 +00:00  packages.conf

7451738112 bytes total (6574940160 bytes free)

Router# del isr4400*
Delete filename [isr4400*]?
Delete bootflash:/isr4400-espbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
```

```
Delete bootflash:/isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
 [confirm]
Delete bootflash:/isr4400-firmware_fpge.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
[confirm]
Delete bootflash:/isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
 [confirm]
Delete bootflash:/isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
 [confirm]
Delete bootflash:/isr4400-firmware_ucse.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
[confirm]
Delete bootflash:/isr4400-packages-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.conf?
 [confirm]
Delete bootflash:/isr4400-rpaccess.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-rpbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg?
 [confirm]
Delete bootflash:/isr4400-sipbase.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Delete bootflash:/isr4400-sipspa.BLD_MCP_DEV_LATEST_20120910_000023.SSA.pkg? [confirm]
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:53:29 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 18:54:03 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
454275  -rw-       11349  Sep 13 2012 18:46:21 +00:00  packages.conf

7451738112 bytes total (6574952448 bytes free)
Router# del packages.conf
Delete filename [packages.conf]?
Delete bootflash:/packages.conf? [confirm]
Router# copy tftp bootflash:
Address or name of remote host []? 10.81.116.4
Source filename []? rtp-isr4400-54/isr4400.bin
Destination filename [isr4400.bin]?
Accessing tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin...
Loading rtp-isr4400-54/isr4400.bin from 10.81.116.4 (via GigabitEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 424317088 bytes]

424317088 bytes copied in 351.758 secs (1206276 bytes/sec)
```

コンフィギュレーション ファイルのバックアップ

ここで紹介する例は、次のとおりです。

- スタートアップ コンフィギュレーション ファイルをブートフラッシュにコピーする （508 ページ）
- スタートアップ コンフィギュレーション ファイルを USB フラッシュ ドライブにコピーする （509 ページ）

• スタートアップ コンフィギュレーション ファイルを TFTP サーバにコピーする例 （509 ページ）

スタートアップコンフィギュレーションファイルをブートフラッシュにコピーする

```
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:53:29 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 19:03:19 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 19:02:50 +00:00  isr4400.bin

7451738112 bytes total (6150721536 bytes free)
Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?
1367 bytes copied in 0.116 secs (11784 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/

   11  drwx       16384   Jul 2 2012 15:25:23 +00:00  lost+found
16225  drwx        4096  Jul 31 2012 19:30:48 +00:00  core
178465  drwx        4096  Sep 13 2012 18:53:29 +00:00  .prst_sync
324481  drwx        4096   Jul 2 2012 15:26:54 +00:00  .rollback_timer
   12  -rw-           0   Jul 2 2012 15:27:06 +00:00  tracelogs.696
373153  drwx      114688  Sep 13 2012 19:03:19 +00:00  tracelogs
32449  drwx        4096   Jul 2 2012 15:27:08 +00:00  .installer
681409  drwx        4096  Jul 31 2012 19:15:39 +00:00  .ssh
697633  drwx        4096   Jul 2 2012 15:27:08 +00:00  vman_fdb
   13  -rw-   424317088  Sep 13 2012 19:02:50 +00:00  isr4400.bin
   14  -rw-        1367  Sep 13 2012 19:03:57 +00:00  startup-config

7451738112 bytes total (6150717440 bytes free)
Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.18.40.33
Destination filename [router-confg]? startup-config
!!
1367 bytes copied in 0.040 secs (34175 bytes/sec)
Router# exit

Router con0 is now available


Press RETURN to get started.
```

スタートアップ コンフィギュレーション ファイルを USB フラッシュ ドライブにコピーする

```
Router# dir usb0:
Directory of usb0:/

No files in directory

4094840832 bytes total (4094836736 bytes free)
Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?
1644 bytes copied in 0.248 secs (6629 bytes/sec)
Router# dir usb0:
Directory of usb0:/

3097__-rwx________1644__ Oct 3 2012 14:53:50 +00:00__startup-config

4094840832 bytes total (4094832640 bytes free)
Router#
```

スタートアップ コンフィギュレーション ファイルを TFTP サーバにコピーする例

```
Router# copy nvram:startup-config tftp:
Address or name of remote host []? 172.18.40.4
Destination filename [router-confg]?
!!
3274 bytes copied in 0.039 secs (83949 bytes/sec)
Router#
```

デジタル署名付き Cisco ソフトウェア署名情報の表示

次の例では、統合パッケージの真正性の詳細が画面に表示されています。

```
router# show software authenticity running
PACKAGE isr4400-rpbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
----------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48E17
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-rpcontrol.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
----------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
```

```
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48DA3
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-rpios-universalk9.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
--------------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48E98
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-rpaccess.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48DB4
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-firmware_dsp_sp2700.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
--------------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48DBE
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-firmware_sm_1t3e3.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
--------------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
```

```
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48DC7
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-firmware_nim_t1e1.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
--------------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48D74
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-espbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48D64
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-sipbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48D94
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

PACKAGE isr4400-sipspa.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
------------------------------------------------------------------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
```

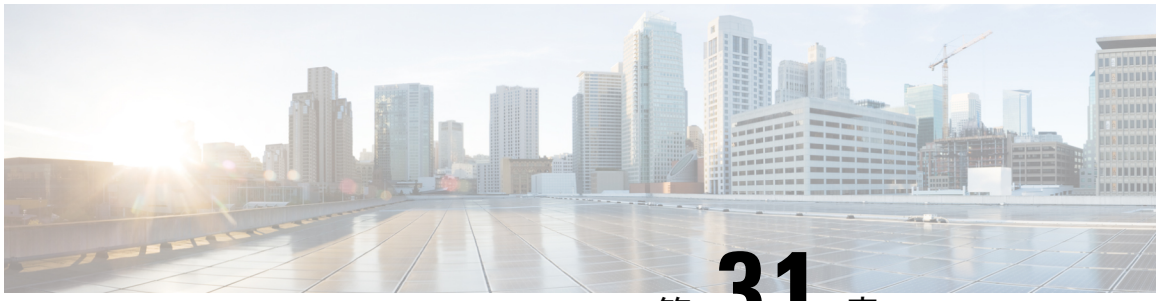
```
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48D7F
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : rp_base
        Verifier Version      : BLD_MCP_DEV_LATEST_20130114_162711

SYSTEM IMAGE
------------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50F48F33
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : System Bootstrap, Version 12.2(20121015:145923
ROMMON
------
Image type                    : Special
    Signer Information
        Common Name           : CiscoSystems
        Organization Unit     : IOS-XE
        Organization Name     : CiscoSystems
    Certificate Serial Number : 50801108
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A

    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : System Bootstrap, Version 12.2(20121015:145923
Microloader
-----------
Image type                    : Release
    Signer Information
        Common Name           : CiscoSystems
        Organization Name     : CiscoSystems
    Certificate Serial Number : bace997bdd9882f8569e5b599328a448
    Hash Algorithm            : HMAC-SHA256
    Verifier Information
        Verifier Name         : Hardware Anchor
        Verifier Version      : F01001R06.02c4c06f82012-09-17
```

モジュールまたは統合パッケージの説明を取得する

この例では、統合パッケージの内容の詳細が画面に表示されます。

```
router# request platform software package describe file
bootflash:isr4400-rpbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
Package: isr4400-rpbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg
```

```
Size: 79755832
Timestamp: 2013-01-15 15:46:59 UTC
Canonical path: /bootflash/isr4400-rpbase.BLD_MCP_DEV_LATEST_20130114_162711.SSA.pkg

Raw disk-file SHA1sum:
  5cd5916a216b147e3d9e33c0dc5afb18d86bda94

Digital Signature Verified
Computed SHA1sum:
  de80d5920819d224113b81a1d64b17449859952e
Contained SHA1sum:
  de80d5920819d224113b81a1d64b17449859952e
Hashes match. Package is valid.

Header size:     760 bytes
Package type:    30001
Package flags:   0
Header version:  1

Internal package information:
  Name: rp_base
  BuildTime: 2013-01-14_14.55
  ReleaseDate: Mon-14-Jan-13-16:27
  BootArchitecture: i686
  RouteProcessor: overlord
  Platform: ISR
  User: mcpre
  PackageName: rpbase
  Build: BLD_MCP_DEV_LATEST_20130114_162711
  CardTypes:

Package is bootable on RP when specified
by packages provisioning file.
```



第 31 章

トラブルシューティング

システム レポート

システムレポートまたはcrashinfoファイルには、シスコのテクニカルサポート担当者が、Cisco IOSイメージのクラッシュを引き起こした問題をデバッグするときに使用する情報が保存されています。重大なクラッシュに関する情報の迅速かつ確実な収集とバンドルが、特定のクラッシュ事案によって情報が識別されるような方法で行われることが必要です。システムレポートが生成され、harddisk: またはflash: ファイルシステムの「/core」ディレクトリに保存されます。リロード時はレポートは生成されません。

システムクラッシュの場合、次の詳細情報が収集されます。

1. □□□□□□□□ core
   - IOSd プロセスクラッシュが発生した場合の IOSd コアファイルおよび IOS crashinfo ファイル
2. □□□□□□□
3. □□□□□□□□□□□□
4. □□□□□□□□□
5. □□□□□□□□ /proc □□

このレポートは、ルータがROMMON/ブートローダーに対してダウン状態になる前に生成されます。この情報は、個別のファイルに格納されてから、アーカイブされて tar.gz バンドルに圧縮されます。これにより、クラッシュのスナップショットを1つの場所で取得して、分析のためにボックス外に移動できるようになります。

デバイスのホスト名、システムレポートを生成したモジュールの ID、およびその作成タイムスタンプがファイル名に組み込まれます。

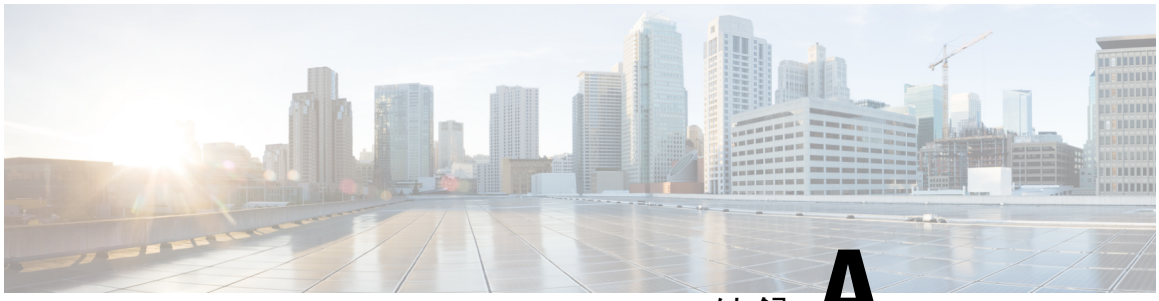
```
<hostname>_<moduleID>-system-report_<timestamp>.tar.gz
```

例：

Router1_RP_0-system-report_20210204-163559-UTC

ホスト名が Router1 のデバイスで、RP0 モジュールの予期しないリロードが発生し、2021 年 2 月 4 日午後 4 時 39 分 59 秒（UTC）にシステムレポートが生成されました。

```
├── bootflash/
│   └── pd_info/
│       ├── dmesg_output-20210204-163538-UTC.log
│       ├── filesystems-20210204-163538-UTC.log
│       ├── memaudit-20210204-163538-UTC.log
│       ├── proc_cpuinfo-20210204-163538-UTC.log
│       ├── proc_diskstats-20210204-163538-UTC.log
│       ├── proc_interrupts-20210204-163538-UTC.log
│       ├── proc_oom_stats-20210204-163538-UTC.log
│       ├── proc_softirqs-20210204-163538-UTC.log
│       ├── system_report_trigger.log
│       └── top_output-20210204-163538-UTC.log
├── harddisk/
│   ├── core/
│   │   └── Router1_RP_0_hman_17716_20210212-123836-UTC.core.gz
│   └── tracelogs/
├── tmp/
│   ├── fp/
│   │   └── trace/
│   ├── maroon_stats/
│   ├── rp/
│   │   └── trace/
│   └── Router1_RP_0-bootuplog-20210204-163559-UTC.log
└── var/
    └── log/
        └── audit/
            └── audit.log
```



付録 A

サポートされていないコマンド

Cisco 4000 シリーズ ルータには、**logging** または **platform** キーワードを指定する一連のコマンドがあり、これらを入力しても出力が生成されないか、またはお客様にとって不要な出力が表示されます。お客様にとって不要なこのようなコマンドは、サポート対象外のコマンドと見なされます。サポート対象外のコマンドに関するシスコ製品マニュアルは今後公開されない予定です。

Cisco 4000 シリーズ ルータのサポート対象外のコマンドのリストを以下に示します。

- clear logging onboard slot f0 dram
- clear logging onboard slot f0 voltage
- clear logging onboard slot f0 temperature
- show logging onboard slot f0 dram
- show logging onboard slot f0 serdes
- show logging onboard slot f0 status
- show logging onboard slot f0 temperature
- show logging onboard slot f0 uptime
- show logging onboard slot f0 uptime latest
- show logging onboard slot f0 voltage
- show logging onboard slot 0 dram
- show logging onboard slot 0 serdes
- show logging onboard slot 0 status
- show logging onboard slot 0 temperature
- show logging onboard slot 0 uptime
- show logging onboard slot 0 uptime latest
- show logging onboard slot 0 voltage
- show platform software adjacency r0 special

- show platform software adjacency rp active special
- show platform software ethernet rp active l2cp
- show platform software ethernet rp active l2cp interface GigabitEthernet0
- show platform software ethernet rp active loopback
- show platform software ethernet rp active vfi
- show platform software ethernet r0 vfi
- show platform software ethernet r0 vfi id 0
- show platform software ethernet r0 vfi name GigabitEthernet0
- show platform software ethernet r0 l2cp
- show platform software ethernet r0 l2cp interface GigabitEthernet0
- show platform software ethernet r0 bridge-domain statistics
- show platform software flow r0 exporter name GigabitEthernet0
- show platform software flow r0 exporter statistics
- show platform software flow r0 global
- show platform software flow r0 flow-def
- show platform software flow r0 interface
- show platform software flow r0 ios
- show platform software flow r0 monitor
- show platform software flow r0 sampler
- show platform hardware qfp active classification feature-manager label GigabitEthernet 0 0
- show platform software interface f0 del-track
- show platform software interface fp active del-track
- show platform software rg r0 services
- show platform software rg r0 services rg-id 0
- show platform software rg r0 services rg-id 0 verbose
- show platform software rg r0 services verbose
- show platform software rg r0 statistics
- show platform software rg rp active services
- show platform software rg rp active services rg-id 0
- show platform software rg rp active services rg-id 0 verbose
- show platform software rg rp active statistics
- show platform hardware slot 0 dram statistics

- show platform hardware slot f0 dram statistics
- show platform hardware slot 0 eobc interface primary rmon
- show platform hardware slot 0 eobc interface primary status
- show platform hardware slot 0 eobc interface standby rmon
- show platform hardware slot 0 eobc interface standby status
- show platform hardware slot f0 eobc interface primary rmon
- show platform hardware slot f0 eobc interface primary status
- show platform hardware slot f0 eobc interface standby rmon
- show platform hardware slot f0 eobc interface standby status
- show platform hardware slot f0 sensor consumer
- show platform hardware slot f0 sensor producer

サポートされていないコマンド

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。