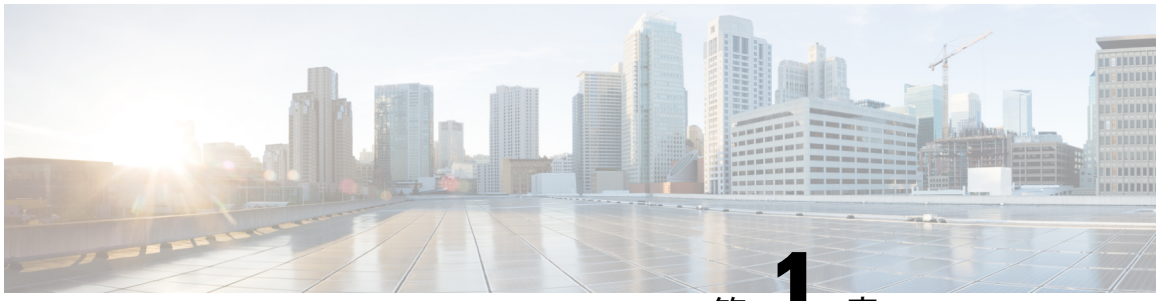
Cisco 8500 シリーズ セキュア ルータ ソフトウェア設定ガイド

最終更新：2026 年 2 月 25 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/

目 次



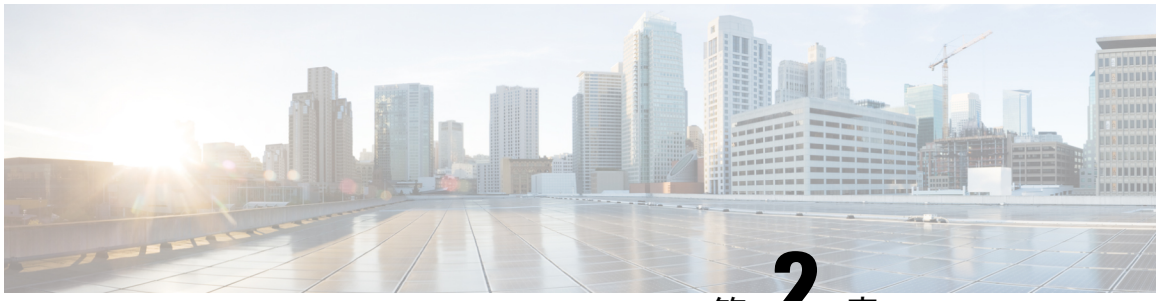
第 1 章

概要

Cisco 8500 シリーズセキュアルータは、データセンターおよびコロケーション展開に適したコンパクトな 1RU プラットフォームです。これらのルータの主なユースケースは、企業 WAN アグリゲーションです。

このドキュメントでは、次のモデルの設定の詳細について説明します。

- C8550-G2
- C8570-G2



第 2 章

ソフトウェアの実装およびアーキテクチャ

Cisco 8500 シリーズ セキュアルータには、新しいソフトウェア パッケージ モデルとアーキテクチャが導入されています。

この章では、この新しい実装とアーキテクチャについて説明します。内容は、次のとおりです。

Cisco 8500 シリーズ セキュアルータでのソフトウェアパッケージ

この項では、次のトピックについて取り上げます。

Cisco 8500 シリーズ セキュアルータ ソフトウェア概要

Cisco 8500 シリーズ セキュアルータは、パフォーマンスの高い WAN アグリゲーション プラットフォームです。

統合パッケージ

統合パッケージは、いくつかの個別のソフトウェア サブパッケージ ファイルで構成される単一のイメージです。単一の統合パッケージファイルはブート可能なファイルで、Cisco 8500 シリーズ セキュアルータは統合パッケージを使用して実行できます。

各統合パッケージには、プロビジョニング ファイルも含まれています。プロビジョニング ファイルは、統合パッケージから抽出された個別のサブパッケージ、またはオプションのサブパッケージを使用してルータを実行する場合にブート処理に使用されます。統合パッケージ全体を実行する場合のメリットとデメリットについての詳細情報は、「*Cisco 8500* シリーズ セキュアルータの実行：概要」を参照してください。

統合パッケージに関する重要事項

統合パッケージに関する重要な情報は次のとおりです。

- 統合パッケージファイルは、ブート可能なファイルです。ルータが統合パッケージ全体を使用して稼働するように設定されている場合は、統合パッケージファイルを使用してルータをブートします。ルータが個別のサブパッケージを使用して稼働するように設定されている場合は、プロビジョニングファイルを使用してルータをブートします。統合パッケージ全体を実行する場合のメリットとデメリットについての詳細情報は、「*Cisco 8500* シリーズ セキュアルータの実行：概要」のセクションを参照してください。
- オプションのサブパッケージをインストールする場合は、個別のサブパッケージと同様に、プロビジョニング ファイルを使用してルータをブートする必要があります。

個別のサブパッケージに関する重要事項

個別のサブパッケージに関する重要な情報は次のとおりです。

- 個別のサブパッケージを Cisco.com から別々にダウンロードできません。ユーザがこれらの個別のサブパッケージを入手するには、最初に統合パッケージをダウンロードしてから、コマンドラインインターフェイスを使用して、統合パッケージからサブパッケージを抽出する必要があります。
- ルータが統合パッケージではなく、個別のサブパッケージを使用して稼働している場合は、プロビジョニング ファイルを使用してルータをブートする必要があります。プロビジョニングファイルはすべての統合パッケージの中に含まれており、個別のサブパッケージが抽出されるたびに、それぞれのサブパッケージに含まれるイメージから抽出されます。

プロビジョニング ファイル

（注） オプションのサブパッケージをインストールする場合は、プロビジョニングファイルを使用してブート プロセスを管理する必要があります。

Cisco 8500 シリーズ セキュアルータが個別のサブパッケージまたはオプションのサブパッケージ（Cisco Webex ノードの Cisco 8500 シリーズ セキュアルータ シリーズ用のパッケージなど）を使用して稼働するように設定されている場合は、プロビジョニングファイルがブートプロセスを管理します。個別のサブパッケージを使用して Cisco 8500 シリーズ セキュアルータを実行する場合は、プロビジョニングファイルをブートするようにルータを設定する必要があります。プロビジョニングファイルによって、個別のサブパッケージのブートアップが管理され、Cisco 8500 シリーズ セキュアルータは通常どおりに動作します。

個別のサブパッケージが統合パッケージから抽出されると、プロビジョニングファイルも自動的に抽出されます。

統合パッケージ全体を使用してルータを実行する場合、プロビジョニングファイルは必要ありません。この場合は、統合パッケージ ファイルを使用してルータをブートします。

プロビジョニング ファイルについての重要事項

プロビジョニング ファイルに関する重要な情報は次のとおりです。

- 各統合パッケージには、2つのプロビジョニング ファイルが格納されています。1つのファイルは「packages.conf」という決められた名前が付いたプロビジョニングファイルで、もう1つのファイルは統合パッケージの命名規則に基づく名前のプロビジョニングファイルです。2つのプロビジョニング ファイルの機能は、すべての統合パッケージで完全に同一です。
- ほとんどの場合、ルータのブートには、「packages.conf」プロビジョニングファイルを使用する必要があります。通常は、「packages.conf」ファイルを使用してブートするようにルータを設定する方が簡単です。このファイルでブートするように設定すると、Cisco IOS XE をアップグレードする際に、ブートステートメントを変更する必要がなくなるためです（**boot system** *file-system*:**packages.conf** コンフィギュレーション コマンドをアップグレードの前後で変更する必要がなくなります）。
- プロビジョニング ファイルと個別のサブパッケージ ファイルは、同じディレクトリに保管する必要があります。プロビジョニング ファイルが、個別のサブパッケージとは異なるディレクトリ内にあると、適切に動作しません。
- プロビジョニング ファイルの名前は変更できますが、個別のサブパッケージのファイルの名前は変更できません。
- プロビジョニング ファイルと個別のサブパッケージ ファイルを同じディレクトリに格納して、ルータをブートしたあとは、これらのファイルの名前変更、削除、または変更を行わないことを強く推奨します。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。

Field-Programmable ハードウェア デバイスをアップグレードするファイル

Field-Programmable ハードウェアデバイスのアップグレードに使用される Field-Programmable パッケージが必要に応じてリリースされています。パッケージファイルは、フィールドのアップグレードが必要な場合に、カスタマーの Field Programmable デバイスに提供されます。Cisco 8500 シリーズセキュアルータに互換性のないバージョンのハードウェア プログラマブル ファームウェアが含まれている場合、そのファームウェアのアップグレードが必要になる場合があります。

通常アップグレードは、システムメッセージが Cisco 8500 シリーズ セキュアルータの Field-Programmable デバイスの 1 つにアップグレードが必要であることを示す、または Cisco のテクニカルサポートの担当者がアップグレードを提案する場合にのみ必要です。

プロセスの概要

Cisco IOS XE には、Cisco 8500 シリーズ セキュアルータ上で完全に別々のプロセスとして稼働する数多くのコンポーネントがあります。このモジュラ アーキテクチャにより、それぞれの動

作を担当するプロセスが分散されるため、すべての動作が Cisco IOS ソフトウェアに依存する場合よりも、ネットワークの復元力が向上します。

プロセスとしての IOS

従来、ほとんどすべてのシスコ ルータ プラットフォームでは、ほとんどすべての内部ソフトウェア プロセスが Cisco IOS メモリを使用して実行されてきました。

Cisco 8500 シリーズ セキュアルータには、分散ソフトウェアアーキテクチャが導入されています。これにより、オペレーティングシステムで実行する数多くの処理に IOS プロセスが関与しなくても済むようになります。このアーキテクチャでは、以前はほとんどすべての内部ソフトウェア プロセスを処理していた IOS が、多数の Linux プロセスの 1 つとして稼働するようになり、ルータを実行する役割を他の Linux プロセスと共有できるようになりました。このアーキテクチャを使用すると、メモリをさらに有効に割り当てることができるため、ルータを効率よく稼働できます。

デュアル IOS プロセス

Cisco 8500 シリーズ セキュアルータでは、デュアル IOS プロセスを導入しているため、高可用性を常に向上させることができます。

SSO を使用すると、2 番目の IOS プロセスを Cisco 8500 シリーズ セキュアルータで有効にすることができます。

これらのデュアル IOS プロセスの状態は、 **show platform** コマンドを入力して確認できます。

2 つめの IOS プロセスの使用によって、次の利点を得られます。

- 耐障害性の向上：アクティブ IOS 障害のイベントが発生しても、サービスをほとんど中断させることなく、即座に 2 番めの IOS プロセスがアクティブ IOS プロセスになります。

Cisco 8500 シリーズ セキュアルータのファイルシステム

次の表に、Cisco 8500 シリーズ セキュア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 *1:* ファイル システム

ファイルシステム	説明
bootflash:	アクティブ RP 上のブートフラッシュ メモリのファイル システム
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:	Onboard Failure Logging 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
usb:	アクティブ RP 上の USB フラッシュ ドライブのファイル システム

上記の表にリストされていないファイルシステムを発見した場合は、**?** ヘルプオプションを入力するか、そのファイルシステムの追加情報について **copy** コマンドリファレンスを参照してください。

自動生成されるファイル ディレクトリおよびファイル

このセクションでは、Cisco 8500 シリーズ セキュアルータ上で表示される可能性のある、自動生成されるファイルとディレクトリ、およびこれらのディレクトリ内のファイルの管理方法について説明します。

次の表に、Cisco 8500 シリーズ セキュアルータで自動生成されるファイルのリストと説明を示します。

表 *2:* 自動生成されるファイル

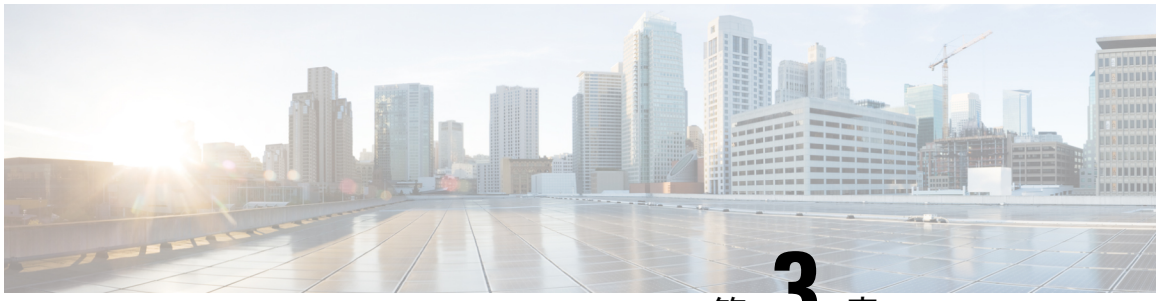
ファイルまたはディレクトリ	説明
crashinfo ファイル	crashinfo ファイルが bootflash: ファイルシステムに保存されることがあります。 これらのファイルでは、クラッシュに関する情報が提供されており、調整またはトラブルシューティングを行う場合に役立ちます。ただし、ファイルはルータ動作に含まれていないため、ルータの機能に影響を及ぼさずに消去することができます。
core ディレクトリ	.core ファイルのストレージ領域 このディレクトリは消去されると、ブートアップ時に自動的に再生成されます。このディレクトリ内の .core ファイルは、ルータ機能に影響を及ぼさずに消去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。

- bootflash: ディレクトリに自動生成されたファイルは、カスタマー サポートから指示されない限り、削除、名前変更、移動、またはその他の変更は行わないでください。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、core、およびtraceファイルは削除できますが、bootflash: ファイルシステムに自動的に含まれている core および tracelog ディレクトリは削除しないでください。



第 3 章

IOS-XE と SDWAN の展開

概要

Cisco 8500 シリーズ セキュアルータの universalk9 イメージは、ルーティングと SD-WAN の両方をサポートしています。

機能制限

自律モードまたはコントローラモード

Cisco IOS XE と Cisco IOS XE の SD-WAN 機能には、それぞれ自律モードとコントローラ実行モードでアクセスします。自律モードはルータのデフォルトモードで、Cisco IOS XE 機能が含まれています。Cisco IOS XE SD-WAN 機能にアクセスするには、コントローラモードに切り替えます。

詳細については、https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/sdwan-xe-gs-book/install-upgrade-17-2-later.html#Cisco_Concept.dita_42020dbf-1563-484f-8824-a0b3f468e787を参照してください。

コントローラモードと自律モードの切り替え

デバイスのデフォルトモードは自律モードです。コントローラモードと自律モードを切り替えるには、特権 EXEC モードで **controller-mode** コマンドを使用します。

controller-mode enable コマンドは、デバイスをコントローラモードに切り替えます。

controller-mode disable コマンドは、デバイスを自律モードに切り替えます。

詳細については、『Cisco SD-WAN Getting Started Guide』を参照してください。

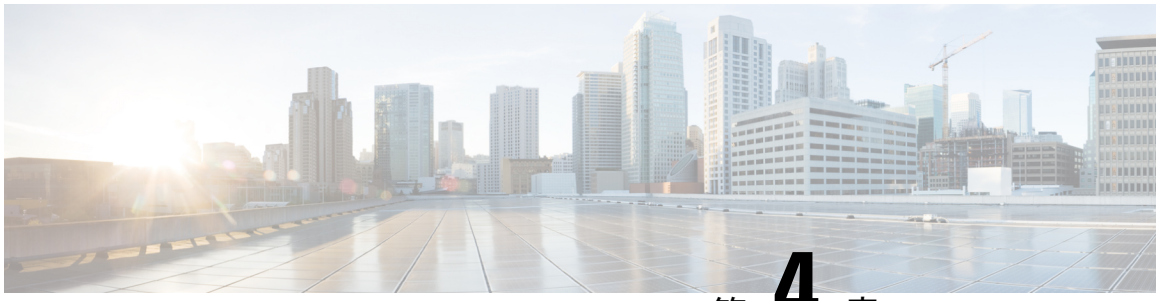
PnP 検出プロセス

既存のプラグアンドプレイ ワークフローを使用してデバイスのモードを決定できます。

PnP ベースの検出プロセスは、コントローラの検出に基づいてデバイスが動作するモードを決定し、必要に応じてモード変更を開始します。この検出は、スマートアカウント/バーチャルアカウントのデバイス UID に関連付けられたコントローラプロファイルに基づいています。モードを変更すると、デバイスが再起動します。再起動が完了すると、デバイスは適切な検出プロセスを実行します。

プラグアンドプレイ（PnP）導入には、次の検出プロセスシナリオが含まれます。

ブートアップモード	ディスカバリ プロセス	モード変更
自律	プラグアンドプレイ接続の検出またはオンプレミスのプラグアンドプレイサーバーの検出	モード変更なし
コントローラ	プラグアンドプレイ接続の検出またはオンプレミスのプラグアンドプレイサーバーの検出	自律モードへのモード変更



第 4 章

Cisco IOS XE ソフトウェアの使用

この章では、Cisco 8500 シリーズ セキュアルータを設定するための準備について説明します。

ルータ コンソールを使用して CLI にアクセスする方法

ここでは、直接接続されたコンソールを使用してコマンドライン インターフェイス（CLI）にアクセスする方法や、Telnet またはモデムを使用してリモート コンソールを設定し、CLI にアクセスする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

ここでは、ルータのコンソール ポートに接続し、コンソール インターフェイスを使用して CLI にアクセスする方法について説明します。

Cisco 8500 シリーズ セキュアルータのコンソール 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、RJ-45 コネクタを使用します。コンソール ポートは、各ルート プロセッサ（RP）の前面パネルに位置しています。

コンソール ポートとの接続

コンソール ポートに接続する手順は次のとおりです。

手順の概要

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。
2. RJ-45/RJ-45 ケーブルと RJ-45/DB-25 DTE（データ端末装置）アダプタ、または RJ-45/DB-9 DTE アダプタ（「Terminal」のラベル）を使用して、ポートに接続します。

手順の詳細

手順

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
- 1 ストップ ビット
- 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（データ端末装置）アダプタ、または RJ-45/DB-9 DTE アダプタ（「Terminal」のラベル）を使用して、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

コンソール インターフェイスを使用して CLI にアクセスする手順は、次のとおりです。

手順の概要

1. ルータのコンソール ポートに端末ハードウェアを接続し、端末エミュレーション ソフトウェアを適切に設定すると、次のプロンプトが表示されます。
2. **Return** を押して、ユーザー EXEC モードを開始します。次のプロンプトが表示されます。
3. ユーザー EXEC モードで、次のように **enable** コマンドを入力します。
4. パスワードプロンプトに、システムパスワードを入力します。システムで有効なパスワードが設定されていない場合、この手順は省略します。次に、「enablepass」というパスワードを入力する例を示します。
5. 有効な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。
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。
7. コンソールセッションを終了するには、次のように **quit** コマンドを入力します。

手順の詳細

手順

ステップ 1 ルータのコンソール ポートに端末ハードウェアを接続し、端末エミュレーション ソフトウェアを適切に設定すると、次のプロンプトが表示されます。

例：

```
Press RETURN to get started.
```

ステップ 2 **Return** を押して、ユーザー EXEC モードを開始します。次のプロンプトが表示されます。

例：

```
Router>
```

ステップ 3 ユーザー EXEC モードで、次のように **enable** コマンドを入力します。

例：

```
Router>enable
```

ステップ 4 パスワードプロンプトに、システム パスワードを入力します。システムで有効なパスワードが設定されていない場合、この手順は省略します。次に、「enablepass」というパスワードを入力する例を示します。

例：

```
Password:enablepass
```

ステップ 5 有効な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。

例：

```
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 コンソールセッションを終了するには、次のように **quit** コマンドを入力します。

例：

```
Router#quit
```

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 を使用してルータのコンソール インターフェイスに接続し、CLI にアクセスする方法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

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前に、**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（vty）をサポートするようにルータを設定する必要があります。また、ログインを要求するように vty を設定し、パスワードを指定する必要もあります。

（注） 回線上でログインがディセーブル化されないようにするには、**login** ライン コンフィギュレーション コマンドを設定するときに、**password** コマンドでパスワードを指定する必要があります。認証、許可、アカウンティング（AAA）を使用している場合は、**login authentication** ライン コンフィギュレーション コマンドを設定する必要があります。**login authentication** コマンドを使用してリストを設定する場合に、回線上で AAA 認証に関するログインがディセーブル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』および『Cisco IOS Security Command Reference Guide』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

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手順は、次のとおりです。

手順の概要

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。
2. パスワード プロンプトで、ログイン パスワードを入力します。次に、mypass というパスワードを入力する例を示します。
3. ユーザー EXEC モードで、次のように **enable** コマンドを入力します。
4. パスワード プロンプトに、システム パスワードを入力します。次に、enablepass というパスワードを入力する例を示します。
5. 有効な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。
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。
7. Telnet セッションを終了するには、次の例のように **exit** または **logout** コマンドを使用します。

手順の詳細

手順

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*]

この構文では、*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。詳細については、『Cisco IOS Configuration Fundamentals Command Reference Guide』を参照してください。

（注）
アクセスサーバーを使用している場合は、ホスト名や IP アドレスのほかに、 **telnet 172.20.52.40 2004** などの有効なポート番号を指定する必要があります。

次の例では、**telnet** コマンドで、router という名称のルータに接続しています。

例：

```
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 パスワード プロンプトで、ログイン パスワードを入力します。次に、mypass というパスワードを入力する例を示します。

例：

```
User Access Verification
Password: mypass
```

（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 ユーザー EXEC モードで、次のように **enable** コマンドを入力します。

例：

```
Router> enable
```

ステップ 4 パスワード プロンプトに、システム パスワードを入力します。次に、enablepass というパスワードを入力する例を示します。

例：

```
Password: enablepass
```

ステップ 5 有効な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。

例：

```
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、次の例のように **exit** または **logout** コマンドを使用します。

例：

```
Router# logout
```

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 *3:* キーボードのショートカット

キーストローク	目的
Ctrl-B または **Left Arrow** キー [1]	カーソルを 1 文字分だけ後退させます。
Ctrl-F または **Right Arrow** キー 1	カーソルを 1 文字分だけ進めます。
Ctrl-A	コマンドラインの先頭にカーソルを移動します。
Ctrl-E	コマンドラインの末尾にカーソルを移動します。
Esc B	カーソルをワード 1 つ分だけ後退させます。
Esc F	カーソルをワード 1 つ分だけ進めます。

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

履歴バッファによるコマンドの呼び出し

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

次の表に、ヒストリ置換コマンドの一覧を示します。

表 *4:* ヒストリ置換コマンド

コマンド	目的
Ctrl-P または **Up Arrow** キー [2]	履歴バッファに保存されているコマンドを、最新のコマンドから順に呼び出します。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 **Down Arrow** キー 1	**Ctrl-P** または **Up Arrow** キーを使用してコマンドを呼び出した後、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を表示します。

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

コマンド モードの概要

Cisco IOS XE で使用可能なコマンド モードは、従来の Cisco IOS CLI で使用可能なコマンド モードとまったく同じです。

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 プロンプトで疑問符（**?**）を入力すると、それぞれのコマンドモードで使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** コマンドは重要なステータス情報を表示し、**clear** コマンドはカウンタまたはインターフェイスをクリアします。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 *5:* 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	ユーザー EXEC モードで、**enable** EXEC コマンドを使用します。	`Router#`	ユーザー 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 モードから、**configure terminal** 特権 EXEC 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** または **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、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、ルータが行います。 ユーザーが **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。アクセスポリシーの設定については、このマニュアルの4章「Console Port, Telnet, and SSH Handling」を参照してください。 ルータには、RP の補助ポートからアクセスされることがあります。 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)#`	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、IOS 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 に接続するように設定された方法を使用します。 RP の補助ポートを介してルータにアクセスしている場合は、別のポートを介してルータにアクセスします。ただし、補助ポートでルータにアクセスしても、カスタマーの要求を処理できません。
ROM モニタ	特権 EXEC モードから、**reload** 特権 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。	>	ROM モニターモードを終了する場合は、**continue** コマンドを使用します。

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参照するには、次の表に記載されているコマンドのいずれかを使用します。

表 *6 :* ヘルプ コマンドおよび説明

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。

コマンド	目的
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（コマンドと疑問符の間にはスペースを入れないでください）。
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可能なすべてのコマンドをリストします。
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（コマンドと疑問符の間にスペースを入れてください）。

コマンドオプションの検索

ここでは、コマンドの構文を表示する方法の例を示します。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、疑問符（**?**）をコンフィギュレーション プロンプトで入力するか、またはコマンドの一部を入力した後に 1 スペース空けて入力します。Cisco IOS XE ソフトウェアでは、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 モードから **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場合は、**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** 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> 記号自体は、使用できる引数とキーワードがないため、**Enter** を押してコマンドを終了する必要があることを示します。

次の表に、 疑問符（**?**） を使ったコマンド入力のアシスト方法を示します。

表 *7:* 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。

コマンド	コメント
Router# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	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** 特権 EXEC コマンドを入力します。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 Ethernet ?** <0-6> Ethernet interface number Router(config)#**interface Ethernet 4 ?** / Router(config)#**interface Ethernet 4/ ?** <0-3> Ethernet interface number Router(config)#**interface Ethernet 4/0 ?** <cr> Router(config)#**interface Ethernet 4/0** Router(config-if)#	**interface Ethernet** 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。 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、イーサネットインターフェイスのスロット番号とポート番号を、スラッシュで区切って入力する必要があります。 <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)#	イーサネット 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。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、**ipaddress** 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。 CR（<cr>）が表示されないため、コマンドを完了するには、キーワードまたは引数をさらに入力する必要があります。
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> が表示されないため、コマンドを完了するには、キーワードまたは引数をさらに入力する必要があります。

コマンド	コメント
Router(config-if)#**ip address 172.16.0.1 255.255.255.0 ?** 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** を押してコマンドを終了するか、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)#	この例では、**Enter** を押してコマンドを完了しています。

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。**default** *command-name* コマンドを実行することで、コマンドをデフォルトの設定にすることができます。コマンドの **default** 形式が、そのプレーン形式や **no** 形式とは実行する機能が異なる場合、Cisco IOS ソフトウェアのコマンドリファレンスにコマンドの **default** 形式の機能が記載されています。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、コマンドラインインターフェイスの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...
```

設定の保存には 1 ～ 2 分かかります。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、コンフィギュレーションが 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

Cisco 8500 シリーズ セキュアルータでは、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 ファイルの保存に関する設定は、Cisco 8500 シリーズ セキュアルータに固有のものではなく、いくつかのシスコ ルータ プラットフォームで使用されています。

Cisco 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ーにもコピーして）、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。次の例では、バック アップされる NVRAM のスタートアップ コンフィギュレーション ファイルを示します。

例 1：bootflash へのスタートアップ コンフィギュレーション ファイルのコピー

```
Router# dir bootflash:
Directory of bootflash:/
  11 drwx 16384 Sep 18 2020 15:16:35 +00:00 lost+found
1648321 drwx 4096 Oct 22 2020 12:08:47 +00:00 .installer
97921 drwx 4096 Sep 18 2020 15:18:00 +00:00 .rollback_timer
12 -rw- 1910 Oct 22 2020 12:09:09 +00:00 mode_event_log
1566721 drwx 4096 Sep 18 2020 15:33:23 +00:00 core
1215841 drwx 4096 Oct 22 2020 12:09:48 +00:00 .prst_sync
1289281 drwx 4096 Sep 18 2020 15:18:18 +00:00 bootlog_history
13 -rw- 133219 Oct 22 2020 12:09:34 +00:00 memleak.tcl
14 -rw- 20109 Sep 18 2020 15:18:39 +00:00 ios_core.p7b
15 -rwx 1314 Sep 18 2020 15:18:39 +00:00 trustidrootx3_ca.ca
391681 drwx 4096 Oct 6 2020 15:08:54 +00:00 .dbpersist
522241 drwx 4096 Sep 18 2020 15:32:59 +00:00 .inv
783361 drwx 49152 Oct 27 2020 08:36:44 +00:00 tracelogs
832321 drwx 4096 Sep 18 2020 15:19:17 +00:00 pnp-info
1207681 drwx 4096 Sep 18 2020 15:19:20 +00:00 onep
750721 drwx 4096 Oct 22 2020 12:09:57 +00:00 license_evlog
946561 drwx 4096 Sep 18 2020 15:19:24 +00:00 guest-share
383521 drwx 4096 Sep 18 2020 15:34:13 +00:00 pnp-tech
1583041 drwx 4096 Oct 22 2020 11:27:38 +00:00 EFI
16 -rw- 34 Oct 6 2020 13:56:03 +00:00 pnp-tech-time
17 -rw- 82790 Oct 6 2020 13:56:14 +00:00 pnp-tech-discovery-summary
18 -rw- 8425 Oct 6 2020 15:09:18 +00:00 1g_snake
19 -rw- 6858 Oct 7 2020 10:53:21 +00:00 100g_snake
20 -rw- 4705 Oct 22 2020 13:01:54 +00:00 startup-config

26975526912 bytes total (25538875392 bytes free)
```

```
Router# copy nvram:startup-config bootflash:
Destination filename [startup-config]?
3517 bytes copied in 0.647 secs (5436 bytes/sec)
```

例2：**USB**フラッシュディスクへのスタートアップコンフィギュレーションファイルのコピー

```
Router# dir usb0:
Directory of usb0:/
43261 -rwx 208904396 Oct 27 2020 14:10:20 -07:00
c8000aep-universalk9.17.02.01.SPA.bin
255497216 bytes total (40190464 bytes free)
Router# copy nvram:startup-config usb0:
Destination filename [startup-config]?
3172 bytes copied in 0.214 secs (14822 bytes/sec)
Router# dir usb0:
Directory of usb0:/
43261 -rwx 208904396 Oct 27 2020 14:10:20 -07:00
c8000aep-universalk9.17.02.01.SPA.bin
15:40:45 -07:00 startup-config255497216 bytes total (40186880 bytes free)
```

例 3：**TFTP** サーバへのスタートアップ コンフィギュレーション ファイルのコピー

```
Router# copy bootflash:startup-config tftp:
Address or name of remote host []? 172.17.16.81
Destination filename [pe24_asr-1002-confg]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)
```

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」のセクションを参照してください。

show および more コマンド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および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 *command* | {**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。次に、**show interface** コマンドに出力修飾子を使用して、「protocol」という表現が現れる行のみを出力する例を示します。

```
Router# show interface | include protocol
FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

前面パネルの USB ポートの無効化

手順の概要

1. enable
2. configure terminal
3. platform usb disable
4. end
5. write memory

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	platform usb disable 例： `Device # platform usb disable`	USB ポートを無効化します。 （注） 前面パネルの USB ポートを再度有効にするには、コマンドの no 形式を使用します（**no platform usb disable**）。
ステップ 4	end 例： `Device(config-router-af)# end`	アドレス ファミリ 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。
ステップ 5	write memory	設定を保存します。

前面パネルの USB ポートの無効化の設定例

例：自律、コントローラ、および vManage モードで前面パネルの USB ポートを無効にする

次の例は、自律、コントローラ、および vManage モードで前面パネルの USB ポートを無効にする設定を示しています。

```
Router# sh run | inc usb
platform usb disable
Router#
```

前面パネルの USB ポートの無効化の確認

デバイスの USB ポートが無効になっていることを確認するには、次の show コマンドを使用します。

show platform usb status

```
Router#show platform usb status
USB enabled
Router#
```

ルータの電源切断

電源モジュールをオフにする前に、シャーシがアース接続されていること、および電源モジュールでソフト シャットダウンが実行されることを確認してください。通常、ソフト シャットダウンを実行しなくても、ルータには悪影響は及びませんが、問題が発生する場合もあります。

ルータの電源を切断する前にソフトシャットダウンを実行するには、**reload** コマンドを入力して、システムを停止させてから、ROM モニターが実行されるのを待機し、次の手順に進みます。

次の出力では、このプロセスの例を示します。

```
Router# reload
Proceed with reload? [confirm]
...(Some messages are omitted here)
Initializing Hardware...
```

このメッセージを確認してから、電源モジュールのスイッチを OFF の位置にします。

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

シスコのソフトウェアには、特定のプラットフォームに対応したソフトウェアイメージで構成されるフィーチャセットが含まれています。特定のプラットフォームで使用できるフィーチャセットは、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する場合、またはある機能が特定の 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するには、Cisco Feature Navigator を使用するか、ソフトウェア リリース ノート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 を使用すると、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。

Software Advisor の使用

機能が Cisco IOS XE のリリースでサポートされているかどうかを確認するか、その機能のソフトウェアマニュアルを検索する場合、またはルータに取り付けられたハードウェアとの Cisco IOS XE ソフトウェアの最低要件を確認するために、シスコでは、次の URL の Cisco.com で Software Advisor ツールを保守しています。http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl

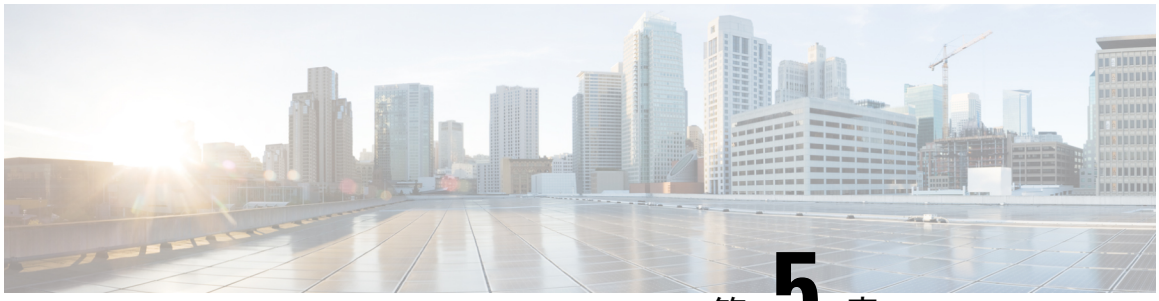
このツールにアクセスするには、Cisco.com の登録ユーザである必要があります。

ソフトウェア リリース ノートの使用

Cisco IOS XE ソフトウェア リリースには、次の情報が記載されたリリース ノートが含まれています。

- プラットフォームのサポート情報
- メモリに関する推奨事項
- 新機能の情報
- 全プラットフォームの未解決および解決済みの重大度 1 および 2 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。以前の機能の情報については、Cisco Feature Navigator を参照してください。



第 5 章

改ざん検出

改ざん検出は、潜在的な改ざんイベントを特定するために Cisco 8000 シリーズ セキュアルータに実装されたセキュリティ機能です。各ルータは、シャーシカバーが安全に取り付けられた状態で製造元から出荷されます。出荷後にシャーシカバーが開かれた場合、ハードウェアは、デバイスの電源がオンになっているかオフになっているかに関係なく、すべてのシャーシカバーが開閉されたイベントを改ざん防止メモリに記録します。

起動時に、ソフトウェアは最新のイベントインデックスを読み取り、以前の既知のインデックスと比較します。不一致がある場合、ソフトウェアは起動時にSyslogメッセージを生成して、改ざんイベントを報告します。デバイスの電源が完全にオンになると、ソフトウェアはSyslogメッセージと SNMP トラップをただちに生成します。

利点

改ざん検出通知は、不正な物理アクセスやデバイスを侵害する試みを検出して、機密データとネットワークの完全性を保護します。

制限事項

改ざん検出機能は現在、SDWAN/SD ルーティングモードではサポートされていません。

改ざん検出の設定

改ざん検出はルータでデフォルトで有効になっています。シャーシカバーの開くまたは閉じるイベントが自動的に記録されます。

改ざんイベント通知は、config モードで以下のコマンドを使用して有効または無効にできます。

- 設定モードで次のコマンドを使用して、改ざん検出通知を有効にします（デフォルトで有効）。

```
Router(config)#platform tamper detection
```

- config モードで次のコマンドを使用して、改ざん検出通知を無効化します。

```
Router(config)#no platform tamper detection
```

改ざん検出イベントのマーク

改ざんイベントのマーキングは、

- 承認されたユーザーに対して特定のアクティビティが改ざんイベントとして表示されないようにし、
- システムが許可されたアクセスと不正なアクセスを区別できるようにすることで
- 改ざんイベントログの精度を維持する機能です。

改ざん検出イベントの設定

承認されたアクティビティがログで改ざんイベントとして表示されないようにする方法です。次の手順を実行します。

手順

ステップ 1 次のコマンドを使用して、同意トークンを取得するためのチャレンジを生成します。

例：

```
request consent-token generate-challenge tamper-auth auth-timeout <mins>
```

この手順により、承認ユーザーによってのみ同意トークンが生成されるようにできます。

ステップ 2 チャレンジが検証され、同意トークンが生成されたら、次のコマンドを使用して同意トークンを受け入れます。

例：

```
request consent-token accept-response tamper-auth <consent token>
```

ステップ 3 次のコマンドを使用して、改ざん検出イベントをマークします

例：

```
request platform hardware tamper-detection event-mark
```

request platform hardware tamper-detection event-mark コマンドは、Cisco IOS XE 17.17.1a からサポートされています。

最後の既知のイベントインデックスとタイムスタンプがマークされ、承認されたアクティビティがログに改ざんイベントとして表示されないようにします。

改ざん検出イベントの確認

```
Router# show platform tamper-detection event [power-off | power-on] [all | lastx | new]
```

オプション	説明
電源オフ	**電源オフ** オプションは、ルータに電源ケーブルが接続されていない場合に改ざんイベントを指定します。
電源の投入	**電源オン** オプションは、ルータの電源がオンになったときの改ざんイベントを指定します。
all	[**all**]オプションでは、記録されたすべての改ざんイベントが指定されます。システムは最大 500 エントリを表示できます。 500 エントリごとにロールオーバーカウンタが 1 つ増加します。
lastx	**lastx** オプションでは、表示するイベントの数を指定します。たとえば、「lastx 10」と入力すると、直近の 10 件のイベントが表示されます。
new	**new** オプションでは、最後の既知のイベントインデックス以降の新しい改ざんイベントを指定します。

show コマンドでは、以下の詳細を含むイベントログが提供されます。

- 現在のイベントインデックス
- 現在の時刻
- ロールオーバーステータスとロールオーバー回数：
  - 改ざんイベント数が 500 以下の場合、ロールオーバー数は 0、ロールオーバーステータス：No
  - 500 ログごとに、ロールオーバー数は 1 ずつ増加します：
  - 501 ～ 1000 が 1 ～ 500 を上書きする場合、ロールオーバー数は 1、ロールオーバーステータス：Yes
  - 1001 ～ 1500が 501～ 1000 を上書きする場合、ロールオーバー数は 2、ロールオーバーステータス：Yes
- イベントタイプとタイムスタンプを示すイベント

システムの電源がオフになっているときのイベントの確認

システムの電源がオフになっている場合、ルータはバッテリ電源を使用して改ざんイベントを記録します。ルータは、最後の電源オフから次の電源オンまでの最初のシャーシカバーが開いたイベントを記録します。電源オフ中にシャーシカバーが何度も開いたり閉じたりした場合、最初の開いたイベントだけが記録されます。次に、システムの電源がオフになったときのイベントログを示します。

```
Router#show platform tamper-detection event power-off all
Current Time: 2025/04/25 19:55:03       Rollover Status: No     Rollover Count: 0
-------------------------------------------------------------------------------------------------
Tamper event index      |       Tamper event timestamp  |       Tamper events description
-------------------------------------------------------------------------------------------------

    #2                           2024/08/08 02:36:41             Chassis is opened
    #1                           2000/00/00 00:00:00             Battery not present or
used up
```

システムの電源が部分的にまたは完全にオンになっている場合のイベントの確認

システムの電源が使用できる場合、ルータはすべてのシャーシカバーの開閉イベントを記録します。次の例は、システムの電源が部分的にまたは完全にオンになっているときのイベントログを示しています。

```
Router show platform tamper-detection event power-on lastx 10
Current Time: 2025/04/25 19:54:46      Rollover Status: No     Rollover Count: 0
-------------------------------------------------------------------------------------------------
Tamper event index      |       Tamper event timestamp  |       Tamper events description
-------------------------------------------------------------------------------------------------

    #2                  025/04/24 22:10:14             Chassis is opened
    #1                   025/04/24 22:02:33             Chassis is closed
```

改ざん検出 SYSlog

ルータが起動すると、イベントログから現在のイベントインデックスが読み取られ、以前に保存されていた最後の既知のインデックスと比較されます。インデックス間に不一致がある場合、またはタイムスタンプが異なる場合、IOS は警告レベルの SYSlog メッセージを生成し、コントローラモードでコントローラに通知を送信します。

このセクションでは、SYSlog イベントの例を示します。

- 電源投入イベントの SYSlog

  改ざん検出が有効で、システムの電源がオンになっている場合、電源オンの SYSlog メッセージが起動中に表示されます。

  ```
  Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
  was opened 0 times and closed 0 times during power up since last known event index
  7 at 2025/04/24 22:11:51
  ```

- 電源オフイベントの SYSlog

改ざん検出が有効になっていてシステムの電源がオフになっている場合、電源オフの SYSlog メッセージが起動中に表示されます。

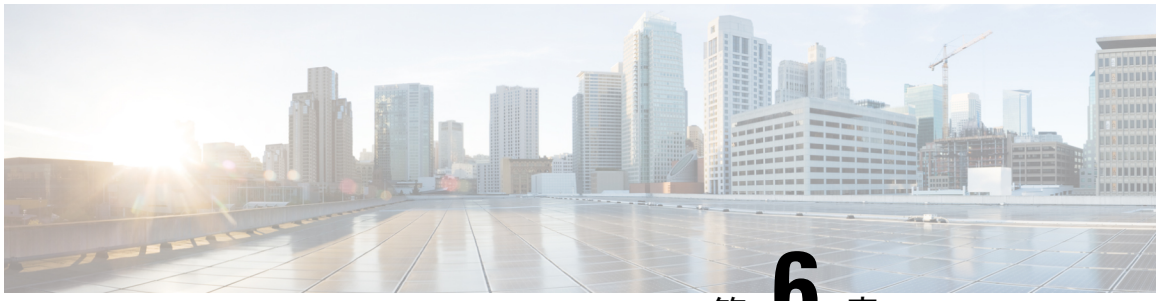
```
Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
was opened 0 times and closed 0 times during power down since last known event index
 5 at 2025/04/24 22:11:51
```

- ランタイムイベントの SYSlog

```
*Aug 29 06:56:34.560: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has
been opened !!
*Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 2 times and closed 0 times during power down since last known event index
 50 at 2025/06/04 08:03:06
*Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 20 times and closed 20 times during power up since last known event index
 1638 at 2025/06/05 07:08:12

*Aug 29 06:57:04.563: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has
been closed !!
*Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 2 times and closed 0 times during power down since last known event index
 50 at 2025/06/04 08:03:06
*Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover
 was opened 20 times and closed 21 times during power up since last known event index
 1638 at 2025/06/05 07:08:12
```

（注） 改ざん検出機能が無効になっている場合、SYSlog メッセージは起動時に表示されません。



第 6 章

ベイ構成

ベイ構成 C8570-G2

C8570-G2 には、設定可能な 3 つの組み込み EPA があります。

次の表でポートの詳細について説明します。

ベイ番号	EPA	ポート設定	インターフェイス番号
ベイ 0 8xSFP+	1/10G EPA	8 つの 1/10G インターフェイス - TE0 - TE7 ベイ 1 で 100G ポートが使用されている場合は無効	0/0/0 0/0/1 0/0/2 0/0/3 0/0/4 0/0/5 0/0/6 0/0/7

ベイ番号	EPA	ポート設定	インターフェイス番号
ベイ 1 4xSFP+/1xQSFP	1/10/40/100G EPA	4 つの 1/10G インターフェイスがアクティブ - TE0 - TE3（インターフェイス 0/1/0 … 0/1/3） ベイは次のモードで使用できます。 • 4 つの 1/10G インターフェイス • 1 つの 40G インターフェイスがアクティブ • 1 つの 100G インターフェイス。ベイ 0 の 8 つの 1/10G ポートを使用	0/1/0 0/1/1 0/1/1 0/1/3
ベイ 2 3xQSFP	40/100G EPA	3 つの 40G インターフェイス (0/2/0、0/2/4、0/2/8) 1 つの 100G インターフェイス （0/2/0）	0/2/0 0/2/4 0/2/8

（注） 10G インターフェイスの速度は、ポートに接続されている SFP トランシーバによって 1G または 10G にすることができます。速度が変更されても、インターフェイス名は TenGigabitEthernet として表示されます。

デフォルトでは、C8570-G2 はベイ 1 を 10G モードで、ベイ 2 を 40G モードで動作させます。ベイ 1 モードは、10G から 40G、100G へ、またはその逆に変更できます。ただし、ベイ 1 が 100G に設定されている場合、ベイ 0 のすべてのポートは管理上ダウン状態になり、ポートは機能しなくなります。

ベイ 2 モードは、40G から 100G に、またはその逆に変更できます。ベイ 2 のモード変更は、ベイ 1 のトラフィックには影響しません。

show platform および **show ip interface** コマンドを使用して、ベイとインターフェイスの詳細を表示します。

```
Router#show platform
Chassis type: C8570-G2

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C8570-G2            ok                    2w6d
 0/0      8xSFP+              ok                    2w6d
 0/1      4xSFP+/1xQSFP       ok                    2w6d
 0/2      3xQSFP              ok                    2w6d
R0        C8570-G2            ok, active            2w6d
F0        C8570-G2            ok, active            2w6d
P0        PWR-CH1-750WACR     ok                    2w6d
P1        Unknown             empty                 never
P2        C8500-FAN-1R        ok                    2w6d

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         23122108            17.15(5r)
R0        23122108            17.15(5r)
F0        23122108            17.15(5r)
```

```
Router#show ip interface
Te0/0/0                unassigned      YES NVRAM  down                    down
Te0/0/1                unassigned      YES NVRAM  down                    down
Te0/0/2                unassigned      YES NVRAM  down                    down
Te0/0/3                unassigned      YES NVRAM  down                    down
Te0/0/4                unassigned      YES NVRAM  down                    down
Te0/0/5                unassigned      YES NVRAM  down                    down
Te0/0/6                unassigned      YES NVRAM  down                    down
Te0/0/7                unassigned      YES NVRAM  down                    down
Te0/1/0                unassigned      YES NVRAM  down                    down
Te0/1/1                unassigned      YES NVRAM  down                    down
Te0/1/2                unassigned      YES NVRAM  down                    down
Te0/1/3                unassigned      YES NVRAM  down                    down
Fo0/2/0                unassigned      YES unset  down                    down
Fo0/2/4                unassigned      YES unset  down                    down
Fo0/2/8                unassigned      YES unset  down                    down
GigabitEthernet0       10.104.33.213   YES NVRAM  up                      up
Router#
```

ベイ構成の例

次の例は、C8570-G2 でモードを変更してさまざまなトラフィック速度を実現する方法を示しています。

例

次の例は、C8570-G2 のベイ 1 で 40G モードに変更する方法を示しています。

```
Router(config)# hw-module subslot 0/1 mode 40G
Present configuration of this subslot will be erased and will not be restored.
CLI will not be available until mode change is complete and EPA returns to OK state.
Do you want to proceed? [confirm]

*Jul  7 08:46:56.550: 4xSFP+/1xQSFP[0/1] : config for spa port 0 would be lost
*Jul  7 08:46:56.556: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:46:56.556: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
```

```
 console as console
*Jul  7 08:46:56.557: 4xSFP+/1xQSFP[0/1] : TenGigabitEthernet0/1/0 moved to default
config
*Jul  7 08:46:56.557: 4xSFP+/1xQSFP[0/1] : config for spa port 1 would be lost
*Jul  7 08:46:56.561: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:46:56.562: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:46:56.562: 4xSFP+/1xQSFP[0/1] : TenGigabitEthernet0/1/1 moved to default
config
*Jul  7 08:46:56.562: 4xSFP+/1xQSFP[0/1] : config for spa port 2 would be lost
*Jul  7 08:46:56.566: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:46:56.567: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:46:56.567: 4xSFP+/1xQSFP[0/1] : TenGigabitEthernet0/1/2 moved to default
config
*Jul  7 08:46:56.567: 4xSFP+/1xQSFP[0/1] : config for spa port 3 would be lost
*Jul  7 08:46:56.571: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:46:56.572: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:46:56.572: 4xSFP+/1xQSFP[0/1] : TenGigabitEthernet0/1/3 moved to default
config
*Jul  7 08:46:57.572: 4xSFP+/1xQSFP[0/1] : Received mode change request from 10G to 40G!
 system_configured TRUE
*Jul  7 08:46:57.586: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(4xSFP+/1xQSFP) reloaded on subslot
 0/1
*Jul  7 08:46:57.588: 4xSFP+/1xQSFP[0/1] : EPA moving from 10G mode to 40G mode
*Jul  7 08:46:57.588: 4xSFP+/1xQSFP[0/1] : config for spa port 0 would be lost
*Jul  7 08:46:57.589: 4xSFP+/1xQSFP[0/1] : config for spa port 1 would be lost
*Jul  7 08:46:57.589: 4xSFP+/1xQSFP[0/1] : config for spa port 2 would be lost
*Jul  7 08:46:57.590: 4xSFP+/1xQSFP[0/1] : config for spa port 3 would be lost
*Jul  7 08:46:57.590: 4xSFP+/1xQSFP[0/1] : Old mode cleanup done!
*Jul  7 08:46:57.593: %SPA_OIR-6-OFFLINECARD: SPA (4xSFP+/1xQSFP) offline in subslot 0/1
*Jul  7 08:47:02.828: 4xSFP+/1xQSFP[0/1] : Number of ports 1
Encore(config)#
*Jul  7 08:47:10.402: %SPA_OIR-6-ONLINECARD: SPA (4xSFP+/1xQSFP) online in subslot 0/1
```

次の例は、C8570-G2 のベイ 1 で 40G モードを 100G に変更する方法を示しています。

```
Router(config)# hw-module subslot 0/1 mode 100G
Present configuration of this subslot will be erased and will not be restored.
CLI will not be available until mode change is complete and EPA returns to OK state.
Do you want to proceed? [confirm]

*Jul  7 08:39:21.152: 4xSFP+/1xQSFP[0/1] : config for spa port 0 would be lost
*Jul  7 08:39:21.165: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:21.165: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:21.166: 4xSFP+/1xQSFP[0/1] : FortyGigabitEthernet0/1/0 moved to default
config
*Jul  7 08:39:22.165: 8xSFP+[0/0] : config for spa port 0 would be lost
*Jul  7 08:39:22.171: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.172: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.172: 8xSFP+[0/0] : TenGigabitEthernet0/0/0 moved to default config
*Jul  7 08:39:22.172: 8xSFP+[0/0] : config for spa port 1 would be lost
*Jul  7 08:39:22.176: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.177: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
```

```
*Jul  7 08:39:22.177: 8xSFP+[0/0] : TenGigabitEthernet0/0/1 moved to default config
*Jul  7 08:39:22.177: 8xSFP+[0/0] : config for spa port 2 would be lost
*Jul  7 08:39:22.181: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.182: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.182: 8xSFP+[0/0] : TenGigabitEthernet0/0/2 moved to default config
*Jul  7 08:39:22.182: 8xSFP+[0/0] : config for spa port 3 would be lost
*Jul  7 08:39:22.186: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.186: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.187: 8xSFP+[0/0] : TenGigabitEthernet0/0/3 moved to default config
*Jul  7 08:39:22.187: 8xSFP+[0/0] : config for spa port 4 would be lost
*Jul  7 08:39:22.193: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.194: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.194: 8xSFP+[0/0] : TenGigabitEthernet0/0/4 moved to default config
*Jul  7 08:39:22.194: 8xSFP+[0/0] : config for spa port 5 would be lost
*Jul  7 08:39:22.199: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.199: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.200: 8xSFP+[0/0] : TenGigabitEthernet0/0/5 moved to default config
*Jul  7 08:39:22.200: 8xSFP+[0/0] : config for spa port 6 would be lost
*Jul  7 08:39:22.204: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.204: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.205: 8xSFP+[0/0] : TenGigabitEthernet0/0/6 moved to default config
*Jul  7 08:39:22.205: 8xSFP+[0/0] : config for spa port 7 would be lost
*Jul  7 08:39:22.209: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.209: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:39:22.210: 8xSFP+[0/0] : TenGigabitEthernet0/0/7 moved to default config
*Jul  7 08:39:23.210: 4xSFP+/1xQSFP[0/1] : Received mode change request from 40G to 100G!
 system_configured TRUE
*Jul  7 08:39:23.210: %SPA_OIR-6-SHUTDOWN: subslot 0/0 is administratively shutdown; Use
 'no hw-module  shutdown' to enable
*Jul  7 08:39:23.244: %SPA_OIR-6-OFFLINECARD: SPA (8xSFP+) offline in subslot 0/0
*Jul  7 08:39:23.250: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(4xSFP+/1xQSFP) reloaded on subslot
 0/1
*Jul  7 08:39:23.251: 4xSFP+/1xQSFP[0/1] : EPA moving from 40G mode to 100G mode
*Jul  7 08:39:23.251: 4xSFP+/1xQSFP[0/1] : config for spa port 0 would be lost
*Jul  7 08:39:23.252: 4xSFP+/1xQSFP[0/1] : Old mode cleanup done!
*Jul  7 08:39:23.252: %SPA_OIR-6-OFFLINECARD: SPA (4xSFP+/1xQSFP) offline in subslot 0/1
*Jul  7 08:39:28.599: 4xSFP+/1xQSFP[0/1] : Number of ports 1
*Jul  7 08:39:38.023: %SPA_OIR-6-ONLINECARD: SPA (4xSFP+/1xQSFP) online in subslot 0/1
```

次の例は、C8570-G2 のベイ 1 で 100G から 10G モードに変更する方法を示しています。

```
Router(config)# hw-module subslot 0/1 mode 10G
Present configuration of this subslot will be erased and will not be restored.
CLI will not be available until mode change is complete and EPA returns to OK state.
Do you want to proceed? [confirm]

*Jul  7 08:45:59.779: 4xSFP+/1xQSFP[0/1] : config for spa port 0 would be lost
*Jul  7 08:45:59.785: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:45:59.785: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:45:59.786: 4xSFP+/1xQSFP[0/1] : FortyGigabitEthernet0/1/0 moved to default
```

```
config
*Jul  7 08:46:00.785: 4xSFP+/1xQSFP[0/1] : Received mode change request from 40G to 10G!
 system_configured TRUE
*Jul  7 08:46:00.790: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(4xSFP+/1xQSFP) reloaded on subslot
 0/1
*Jul  7 08:46:00.791: 4xSFP+/1xQSFP[0/1] : EPA moving from 40G mode to 10G mode
*Jul  7 08:46:00.791: 4xSFP+/1xQSFP[0/1] : config for spa port 0 would be lost
*Jul  7 08:46:00.791: 4xSFP+/1xQSFP[0/1] : Old mode cleanup done!
*Jul  7 08:46:00.792: %SPA_OIR-6-OFFLINECARD: SPA (4xSFP+/1xQSFP) offline in subslot 0/1
*Jul  7 08:46:06.025: 4xSFP+/1xQSFP[0/1] : Number of ports 4
Encore(config)#
*Jul  7 08:46:13.676:  Dot3 Stats : 0/3 not valid intf
*Jul  7 08:46:13.684: %SPA_OIR-6-ONLINECARD: SPA (4xSFP+/1xQSFP) online in subslot 0/1
*Jul  7 08:46:15.675: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/1/0, changed state
to down
*Jul  7 08:46:15.676: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/1/1, changed state
to down
*Jul  7 08:46:15.677: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/1/2, changed state
to down
*Jul  7 08:46:15.678: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/1/3, changed state
to down
*Jul  7 08:46:15.687: %LINK-3-UPDOWN: SIP0/1: Interface TenGigabitEthernet0/1/0, changed
 state to down
*Jul  7 08:46:19.254: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/1/0, changed state
to up
*Jul  7 08:46:20.254: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet0/1/0, changed state to up
*Jul  7 08:46:19.254: %LINK-3-UPDOWN: SIP0/1: Interface TenGigabitEthernet0/1/0, changed
 state to up
```

次の例は、C8570-G2 のベイ 2 で 100G から 100G モードに変更する方法を示しています。

```
Router(config)# hw-module subslot 0/2 mode 100G
Present configuration of this subslot will be erased and will not be restored.
CLI will not be available until mode change is complete and EPA returns to OK state.
Do you want to proceed? [confirm]

*Jul  7 08:48:15.432: 3xQSFP[0/2] : config for spa port 0 would be lost
*Jul  7 08:48:15.462: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:48:15.463: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:48:15.463: 3xQSFP[0/2] : FortyGigabitEthernet0/2/0 moved to default config
*Jul  7 08:48:15.463: 3xQSFP[0/2] : config for spa port 1 would be lost
*Jul  7 08:48:15.469: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:48:15.470: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:48:15.470: 3xQSFP[0/2] : FortyGigabitEthernet0/2/4 moved to default config
*Jul  7 08:48:15.470: 3xQSFP[0/2] : config for spa port 2 would be lost
*Jul  7 08:48:15.475: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:48:15.476: %SYS-5-CONFIG_P: Configured programmatically by process Exec from
 console as console
*Jul  7 08:48:15.476: 3xQSFP[0/2] : FortyGigabitEthernet0/2/8 moved to default config
*Jul  7 08:48:16.476: 3xQSFP[0/2] : Received mode change request from 40G to 100G!
system_configured TRUE
*Jul  7 08:48:16.487: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(3xQSFP) reloaded on subslot 0/2
*Jul  7 08:48:16.489: 3xQSFP[0/2] : EPA moving from 40G mode to 100G mode
*Jul  7 08:48:16.489: 3xQSFP[0/2] : config for spa port 0 would be lost
*Jul  7 08:48:16.490: 3xQSFP[0/2] : config for spa port 1 would be lost
*Jul  7 08:48:16.490: 3xQSFP[0/2] : config for spa port 2 would be lost
*Jul  7 08:48:16.491: 3xQSFP[0/2] : Old mode cleanup done!
*Jul  7 08:48:16.493: %SPA_OIR-6-OFFLINECARD: SPA (3xQSFP) offline in subslot 0/2
```

```
*Jul  7 08:48:21.731: 3xQSFP[0/2] : Number of ports 1
*Jul  7 08:48:21.733: 3xQSFP[0/2] : XCVR namestring create: Maximum number of XCVR = 1
Encore(config)#
Encore(config)#
*Jul  7 08:48:35.865: %SPA_OIR-6-ONLINECARD: SPA (3xQSFP) online in subslot 0/2
```

ブレークアウトサポート

ブレークアウトサポートの理解

ポートのブレークアウトサポートは、高密度ポートを複数の独立した論理ポートに分割するのに役立ちます。ブレークアウトサポートは、ブレークアウト対応の40Gネイティブポートをサポートする C8570-G2 のベイ 2 に導入されています。ブレークアウトサポートは 4X10G で、3 タプルアプローチを使用します。

次の表は、ブレークアウトが設定されている場合のインターフェイス名について説明しています。

表 *8:* ブレークアウトが設定されているときのインターフェイス名

シリアル番号	インターフェイス名	説明
	Te0/2/0、Te0/2/1、Te0/2/2、Te0/2/3、Te0/2/4、Te0/2/5、Te0/2/6、Te0/2/7、Te0/2/8、Te0/2/9、Te0/2/10、Te0/2/11	10G ブレークアウトモードで動作する 3 つの 40 G ネイティブポートすべて
	Fo0/2/0、Fo0/2/4、 Te0/2/8、Te0/2/9、Te0/2/10、Te0/2/11	40G モードの最初のネイティブポート 40G モードの 2 番目のネイティブポート 10G ブレークアウトモードの 3 番目のネイティブポート
	Fo0/2/0、 Te0/2/4、Te0/2/5、Te0/2/6、Te0/2/7 Fo0/2/8	40G モードの最初のネイティブポート 10G ブレークアウトモードの 2 番目のネイティブポート 40G モードの 3 番目のネイティブポート

シリアル番号	インターフェイス名	説明
	Te0/2/0、Te0/2/1、Te0/2/2、Te0/2/3、 Fo0/2/4、 Fo0/2/8	10G ブレークアウトモードの最初のネイティブポート 40G モードの 2 番目のネイティブポート 40G モードの 3 番目のネイティブポート
	Fo0/2/0、 Te0/2/4、Te0/2/5、Te0/2/6、Te0/2/7、 Te0/2/8、Te0/2/9、Te0/2/10、Te0/2/11	40G モードの最初のネイティブポート 10G ブレークアウトモードの 2 番目のネイティブポート 10G ブレークアウトモードの 3 番目のネイティブポート
	Te0/2/0、Te0/2/1、Te0/2/2、Te0/2/3、 Te0/2/4、Te0/2/5、Te0/2/6、Te0/2/7、 Fo0/2/8	10G ブレークアウトモードの最初のネイティブポート 10G ブレークアウトモードの 2 番目のネイティブポート 40G モードの 3 番目のネイティブポート
	Te0/2/0、Te0/2/1、Te0/2/2、Te0/2/3、 Fo0/2/4、 Te0/2/8、Te0/2/9、Te0/2/10、Te0/2/11	10G ブレークアウトモードの最初のネイティブポート 40G モードの 2 番目のネイティブポート 10G ブレークアウトモードの 3 番目のネイティブポート

ブレークアウトサポート

（注） ブレークアウト機能を使用する前に、ベイ 2 が 40G モードで設定されていることを確認してください

```
Router(config)#hw-module subslot 0/2 breakout 10G port ?

all                configure all native ports in breakout mode
native_port_0      configure native port 0 in breakout mode
native_port_4      configure native port 4 in breakout mode
native_port_8      configure native port 8 in breakout mode
```

ブレークアウトサポートを設定するためのコマンド例

native_port 0 と 8 が 10G ブレークアウトにあり、native_port 4 が 40G モードで実行されている場合

```
hw-module subslot 0/2 breakout 10g port native_port_0
hw-module subslot 0/2 breakout 10g port native_port_8
```

3 つのネイティブ 40G ポートすべてに同じブレークアウト設定がある場合

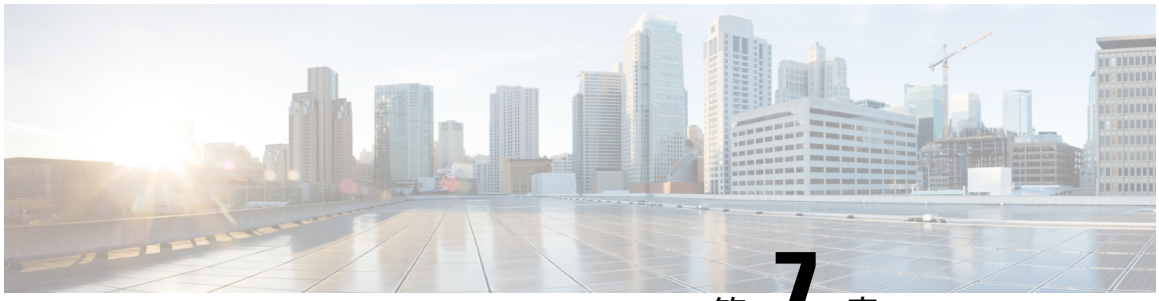
```
hw-module subslot 0/2 breakout 10g port all
hw-module subslot 0/2 breakout none port all
```

すべてのポートからブレークアウト設定を削除したい場合

```
hw-module subslot 0/2 breakout none port all
```

ベイ構成 C8550-G2

C8550-G2 には、SFP/SFP+ トランシーバ用のポート TE0 ～ TE11 をサポートする 1 つの組み込み EPA があります。



第 7 章

統合パッケージの管理

この章では、統合パッケージがどのように管理され、Cisco 8500 シリーズ セキュアルータを実行するために使用されるか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 8500 シリーズ セキュアルータの実行：概要

Cisco 8500 シリーズ セキュアルータは、完全な統合パッケージを使用して実行できます。

この項では、次のトピックについて取り上げます。

統合パッケージを使用した Cisco 8500 シリーズ セキュアルータの実行：概要

Cisco 8500 シリーズ セキュアルータは、統合パッケージを使用して動作するように設定することもできます。

ルータで統合パッケージでの実行が設定されている場合は、統合パッケージ ファイル全体がルータにコピーされるか、または TFTP またはその他のネットワーク転送方式でルータからアクセスされます。ルータは、統合パッケージ ファイルを使用して稼働します。

Cisco 8500 シリーズ セキュアルータが統合パッケージファイルを使用して動作するように設定されている場合、ルータ要求の処理に多くのメモリが消費されます。要求のたびにルータによるサイズの大きなファイルの検索が必要になるためです。ネットワーク トラフィックの転送に使用できるメモリの最大量は、統合パッケージによる実行が設定されている方が少なくて済みます。

統合パッケージを使用して稼働するように設定された Cisco 8500 シリーズ セキュアルータは、統合パッケージファイルをブートすることで起動します。

統合パッケージは TFTP またはその他のネットワーク転送方式でブートして使用することができます。特定のネットワーク環境でルータを実行する場合、統合パッケージを使用してルータを実行するのが適切な方法です。

この方式を使用してルータを実行する場合は、統合パッケージを bootflash:、usb[0]:、またはリモートファイルシステムに保存する必要があります。

Cisco 8500 シリーズ セキュアルータ：概要

このセクションでは、Cisco 8500 シリーズ セキュアルータの各実行メソッドの長所と短所について簡単に説明します。

統合パッケージを使用してルータを実行する場合は、次の利点があります。

- インストールを簡素化：複数の個別のイメージではなく、1 つのソフトウェア ファイルだけが管理されます。
- ストレージ：統合パッケージは、bootflash:、USB フラッシュディスク、ネットワークサーバーのいずれかに保存した状態でルータを実行できます。統合パッケージは TFTP またはその他のネットワーク転送方式を使用してブートおよび利用できます。

コマンドセットを使用したソフトウェア ファイルの管理

ソフトウェアファイルは、3 つの異なるコマンドセットを使用して Cisco 8500 シリーズ セキュアルータで管理できます。ここでは、次のコマンド セットの概要について説明します。

request platform コマンド セット

request platform software package コマンドは、Cisco 8500 シリーズ セキュアルータで導入されたより大きな **request platform** コマンドセットの一部です。各 **request platform** コマンドと、それぞれのコマンドで使用可能なオプションの詳細については、『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

request platform software package コマンドは、個別のサブパッケージおよび統合パッケージ全体をアップグレードする場合に使用でき、Cisco 8500 シリーズ セキュアルータ上のソフトウェアのアップグレードに使用されます。**request platform software package** コマンドは、特に個別のサブパッケージをアップグレードする場合に推奨されます。また、ルータが個別のサブパッケージを実行している場合、ルータ上の個別のサブパッケージをダウンタイムなしでアップグレードできる唯一の方法でもあります。

request platform software package コマンドを使用する場合は、コマンドラインで宛先デバイスまたはプロセスを指定する必要があるため、このコマンドを使用すると、アクティブまたはスタンバイプロセッサの両方でソフトウェアをアップグレードできます。**request platform software package** コマンドは、ほとんどのシナリオにおいて、ダウンタイムなしのソフトウェアのアップグレードを実現します。

このコマンドの基本シンタックスは、**request platform software package install rp** *rp-slot-number* **file** *file-URL* です。ここで、*rp-slot-number* には RP スロットの番号を、*file-URL* には Cisco 8500 シリーズセキュアルータのアップグレードに使用するファイルへのパスを指定します。このコマンドには、その他にもオプションがあります。このコマンドセットで使用できるすべてのオプションについては、**request platform software package** コマンドリファレンスを参照してください。

copy コマンド

Cisco 8500 シリーズセキュアルータ上の統合パッケージをアップグレードするには、他のほとんどのシスコルータの場合と同じように、 **copy** コマンドを使用して統合パッケージをルータ上のファイルシステム（通常は bootflash: または usb[0-1]:）にコピーします。このコピーを行ってから、統合パッケージ ファイルを使用してブートするようにルータを設定します。

copy コマンドで使用可能なオプションの一覧については、**copy** コマンドリファレンスを参照してください。

統合パッケージを使用して実行されるルータの管理および設定

ここでは、次の内容について説明します。

クイック スタート ソフトウェア アップグレード

次の手順では、Cisco 8500 シリーズセキュアルータを実行するソフトウェアを簡単にアップグレードするための方法について説明します。この手順は、ユーザーが統合パッケージにアクセスできること、統合パッケージファイルを bootflash: ファイルシステムに保存すること、およびファイルを格納するための領域が十分にあることを前提とします。

インストールの詳細な例については、この章の他のセクションを参照してください。

クイック スタート バージョンを使用してソフト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。

手順の概要

1. **copy** *URL-to-image* **bootflash:** コマンドを使用して、統合パッケージを bootflash: にコピーします。
2. **dir bootflash:** コマンドを入力して、bootflash: ディレクトリ内の統合パッケージを確認します。
3. ブート用のブート パラメータを設定します。**config-register 0x2102** グローバル コンフィギュレーション コマンドを入力して、コンフィギュレーション レジスタを 0x2 に設定し、**boot system flash bootflash:***image-name* を入力します。
4. **copy running-config startup-config** を入力して設定を保存します。

5. **reload** コマンドを入力して、ルータをリロードし、ブートを終了します。リロード完了時には、アップグレードされたソフトウェアが実行されています。

手順の詳細

手順

ステップ 1 **copy** *URL-to-image* **bootflash:** コマンドを使用して、統合パッケージを bootflash: にコピーします。

ステップ 2 **dir bootflash:** コマンドを入力して、bootflash: ディレクトリ内の統合パッケージを確認します。

ステップ 3 ブート用のブート パラメータを設定します。**config-register 0x2102** グローバル コンフィギュレーション コマンドを入力して、コンフィギュレーション レジスタを 0x2 に設定し、**boot system flash bootflash:***image-name* を入力します。

ステップ 4 **copy running-config startup-config** を入力して設定を保存します。

ステップ 5 **reload** コマンドを入力して、ルータをリロードし、ブートを終了します。リロード完了時には、アップグレードされたソフトウェアが実行されています。

統合パッケージで実行するルータの管理および設定

ここでは、次の手順について説明します。

copy コマンドを使用した統合パッケージの管理および設定

copy コマンドを使用して Cisco 8500 シリーズ セキュアルータ上の統合パッケージをアップグレードするには、他のほとんどのシスコルータの場合と同じように、 **copy** コマンドを使用して統合パッケージをルータ上の bootflash: ディレクトリにコピーします。このコピーを行ってから、統合パッケージ ファイルを使用してブートするようにルータを設定します。

次の例では、統合パッケージ ファイルを TFTP から bootflash: ファイル システムにコピーしています。さらに、**boot system** コマンドを使用して起動するようにコンフィギュレーション レジスタを設定し、この **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:/

2203649  drwx            40960   Jul 7 2025 14:06:44 +05:30  tracelogs
1630209  drwx             4096   Jul 7 2025 13:28:19 +05:30  memaudit_log
90113    drwx             8192   Jul 7 2025 10:29:48 +05:30  license_evlog
17506305  drwx              4096   Jul 7 2025 10:28:06 +05:30  sdavc
13       -rw-           144302   Jul 7 2025 10:27:43 +05:30  memleak.tcl
7946241  drwx             4096   Jul 7 2025 10:27:29 +05:30  .inv
12       -rwx            32397   Jul 7 2025 10:27:27 +05:30  mode_event_log
12558337  drwx             4096   Jul 6 2025 19:49:31 +05:30  sysboot
```

```
9609217  drwx             4096   Jul 4 2025 10:12:42 +05:30  .sdp_install
11886593  drwx             4096   Jul 3 2025 13:41:56 +05:30  core
4890625  drwx             4096   Jul 2 2025 11:48:30 +05:30  system_report_stage
11206657  drwx             4096   Jul 2 2025 11:48:26 +05:30  .prst_sync
13099009  drwx             4096   Jul 2 2025 08:35:30 +05:30  .rollback_timer
28      -rw-            1376   Jul 2 2025 08:35:28 +05:30  packages.conf
30      -rw-            1376   Jul 2 2025 08:35:23 +05:30
c8500x_COMPUTE_ASR1K.image.BLD_LUX_DEV_S2C_20250629_135017-2-g6d472f6332eb.SSA.conf
15990792  -rw-         66959470   Jul 2 2025 08:35:22 +05:30
c8500x_COMPUTE_ASR1K.rpboot.BLD_LUX_DEV_S2C_20250629_135017-2-g6d472f6332eb.SSA.pkg
15990785  drwx             4096   Jul 2 2025 08:35:21 +05:30  .images
29      -rw-        947406255   Jul 2 2025 08:34:33 +05:30  c8000aep.bin
21      -rw-       1232501326   Jul 2 2025 08:33:11 +05:30
c8500x_COMPUTE_ASR1K.image.BLD_LUX_DEV_S2C_20250629_135017-2-g6d472f6332eb.SSA.bin
15990805  -rw-             5284   Jul 1 2025 23:09:02 +05:30
c8500x_COMPUTE_ASR1K.empty.BLD_LUX_DEV_S2C_20250629_135017-2-g6d472f6332eb.SSA.pkg
32      -rw-        945615620   Jul 1 2025 11:22:38 +05:30
c8000aep-universalk9.BLD_POLARIS_DEV_LATEST_20250628_033228_V17_19_0_21.SSA.bin
15589377  drwx             4096  Jun 26 2025 19:40:17 +05:30  core_temp
17      -rw-           583287  Jun 26 2025 15:58:31 +05:30
CRFT__uut__000001__C8570-G2_2025-06-26_10-28-31.tar.gz
73750   -rwx            64520  Jun 20 2025 16:19:02 +05:30  tam_util_tool
4923393  drwx             4096  Jun 16 2025 20:38:50 +05:30  EFI
26656769  drwx             4096  May 21 2025 23:08:19 +05:30  orch_test_logs
73744   -rw-        145309462  May 20 2025 21:22:55 +05:30  IOSD_start.undo
73743   -rw-             6526  May 20 2025 19:56:45 +05:30  undo-engine.json
73742   -rwx         21387416  May 20 2025 14:15:44 +05:30  live-record_x64
73741   -rwx            10645  May 20 2025 14:14:54 +05:30  live-record_polaris
73733   -rw-            98614   May 6 2025 09:49:32 +05:30  collated_log_20250506-041923
73736   -rw-          1207993   May 5 2025 15:18:45 +05:30  mcp_diag.image
24      -rw-            16319  Apr 29 2025 09:58:52 +05:30  test_rumack.txt
31      -rw-             3566  Apr 23 2025 10:44:06 +05:30  Rum-Report-v0010.txt
73731   -rw-             4785   Apr 2 2025 13:53:10 +05:30  backup_config.cfg
73730   -rw-             2689  Mar 17 2025 14:06:29 +05:30  ipconfig.config
28147713  drwx             4096   Mar 8 2025 14:58:59 +05:30  pnp-tech
18      -rw-              257   Mar 8 2025 14:58:16 +05:30  .iox_dir_list
14516225  drwx             4096  Jan 30 2025 15:04:49 +05:30  pcap
27074561  drwx             4096  Jan 30 2025 15:04:49 +05:30  SHARED-IOX
11      drwx             4096  Jan 30 2025 15:04:32 +05:30  lost+found
1998849  drwx             4096   Dec 4 2024 13:55:50 +05:30  .geo

468237697024 bytes total (434919051264 bytes free)

Router#copy tftp: bootflash:
Address or name of remote host []? 172.18.5.151
Source filename []? $cpprtp/efg/c8000aep-universalk9.2025-11-06_15.11_abc.SSA.bin
Destination filename [c8000aep-universalk9.2025-11-06_15.11_abc.SSA.bin]?
Accessing
tftp://172.18.5.151//auto/tftp-cpprtp/efg/c8000aep-universalk9.2025-11-06_15.11_abc.SSA.bin...
Loading /auto/tftp-cpprtp/efg/c8000aep-universalk9.2025-11-06_15.11_abc.SSA.bin from
172.18.5.151 (via GigabitEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!$
!!!!!!!!!!!!!!O!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!
!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
O!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!O!!!!!
O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 947877424 bytes]

947877424 bytes copied in 576.308 secs (1644741 bytes/sec)
Router#
Router#
Router#dir bootflash:
Directory of bootflash:/

29      -rw-        947877424   Nov 7 2025 07:44:40 +00:00
c8000aep-universalk9.2025-11-06_15.11_abc.SSA.bin
873121  drwx             4096   Nov 7 2025 03:40:36 +00:00  .installer
28      -rw-           379569   Nov 7 2025 03:32:10 +00:00
threshold_lowmem_info_20251107-033207-UTC
1109761  drwx             8192   Nov 7 2025 03:32:07 +00:00  license_evlog
22      -rw-           144588   Nov 7 2025 03:32:02 +00:00  memleak.tcl
1591201  drwx             4096   Nov 7 2025 03:31:54 +00:00  .prst_sync
16      -rwx            30662   Nov 7 2025 03:31:46 +00:00  mode_event_log
25      -rw-              219   Nov 7 2025 03:31:14 +00:00  harddisk_info_history
122401  drwx             8192   Nov 7 2025 03:27:20 +00:00  tracelogs
24      -rw-           376820   Nov 7 2025 03:26:49 +00:00
threshold_lowmem_info_20251107-032647-UTC
987361  drwx             4096   Nov 7 2025 03:25:18 +00:00  sysboot
1052653  -r--              706   Nov 7 2025 03:25:15 +00:00  debug.conf
17      -rw-       213923558   Nov 7 2025 03:22:00 +00:00  mcpcc00_recording.19592.undo
15      -rw-       172239006   Nov 7 2025 03:21:54 +00:00  mcpcc01_recording.19592.undo
14      -rw-         71206936   Nov 9 2021 12:02:46 +00:00  castor_top_SMAP.bin
12      -rw-        730948780   Nov 9 2021 12:02:15 +00:00  10g_p2a.bin
11      drwx            16384   Nov 9 2021 12:01:39 +00:00  lost+found

26975526912 bytes total (7310331904 bytes free)
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no boot system
Router(config)#
Warning: Booting with bundle mode will be deprecated in the near future. Migration to
install mode is required.
Router(config)#confi
Router(config)#config-reg
Router(config)#config-register 0x1822
Router(config)#exit
Router#
Router#
Router#sho
Router#show run
Router#show running-config | inc boot
boot-start-marker
boot system flash bootflash:c8000aep-universalk9.2025-11-06_15.11_abc.SSA.bin
boot-end-marker
diagnostic bootup level minimal
exception crashinfo file bootflash:threshold_lowmem_info
Router#
Router#
Router#wr
Building configuration...
[OK]
Router#
Router#
Router#reload
Proceed with reload? [confirm]
Nov  7 07:47:09.14
```

インストールコマンドを使用したソフトウェアのインストール

Cisco 8500 シリーズセキュアルータは、デフォルトではインストールモードで出荷されます。ユーザーは、一連の **install** コマンドを使用して、プラットフォームを起動し、Cisco IOS XE ソフトウェアバージョンにアップグレードまたはダウングレードできます。

インストールコマンドを使用したソフトウェアのインストールに関する制約事項

- ISSU はこの機能ではカバーされません。
- インストールモードでは、システムの再起動が必要です。

インストールコマンドを使用したソフトウェアのインストールに関する情報

次の表に、バンドルモードとインストールモードの違いを示します。

表 *9:* バンドルモードとインストールモード

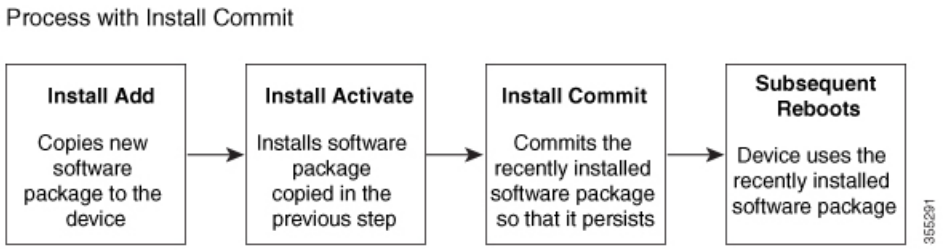
バンドルモード	インストールモード
このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。 （注） USB および TFTP ブートからのバンドルブートはサポートされていません。	このモードでは、ブートプロセスにローカル（ブートフラッシュ）の packages.conf ファイルを使用します。
このモードでは、1 つの .bin ファイルを使用します。	このモードでは、.bin ファイルは拡張された .pkg ファイルに置き換えられます。
CLI： `#boot system file <filename>`	CLI： `#install add file bootflash: [activate commit]`
このモードでアップグレードするには、boot system が新しいソフトウェアイメージをポイントするようにします。	このモードでアップグレードするには、**install** コマンドを使用します。

バンドルモード	インストールモード
イメージの自動アップグレード：新しい Field Replaceable Unit（FRU）がモジュラ型シャーシに挿入された場合、アクティブな FRU と同じバージョンで新しい FRU を実行するには、手動による作業が必要です。	イメージの自動アップグレード：新しい FRU がモジュラ型シャーシに挿入された場合、結合する FRU は、アクティブな FRU と同期してイメージバージョンに自動アップグレードされます。
ロールバック：複数のソフトウェアメンテナンスの更新（SMU）を使用して以前のイメージにロールバックするには、複数回のリロードが必要になる場合があります。	ロールバック：1 回のリロードで、複数のパッチを含む、Cisco IOS XE ソフトウェアの以前のバージョンへのロールバックを有効にします。

インストールモードのプロセスフロー

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

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



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

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

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

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

次の一連のインストールコマンドが使用できます。

表 *10* : インストールコマンド一覧

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

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

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

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

次の show コマンドも使用できます。

表 *11 : show* コマンドの一覧

コマンド	構文	目的
show install log	**show install log**	プラットフォームがブートされた後に実行されたすべてのインストール操作の履歴と詳細を提供します。
show install package	**show install package** <*filename*>	指定された .pkg/.bin ファイルに関する詳細を提供します。
show install summary	**show install summary**	すべての FRU のイメージバージョンとそれに対応するインストール状態の概要を提供します。 • 表示される表には、この情報が適用される FRU が示されます。 • 存在するイメージとその状態に関してすべての FRU が同期している場合、1つの表のみが表示されます。 • ただし、FRU 間でイメージまたは状態の情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表にリストされます。
show install active	**show install active**	すべての FRU のアクティブなパッケージに関する情報を提供します。 FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。

コマンド	構文	目的
show install inactive	**show install inactive**	すべての FRU に非アクティブなパッケージがあれば、そのパッケージに関する情報を提供します。 FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
show install committed	**show install committed**	すべての FRU のコミットされたパッケージに関する情報を提供します。 FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
show install uncommitted	**show install uncommitted**	すべての FRU について、コミットされていないパッケージがある場合はそのパッケージに関する情報を提供します。 FRU 間で情報に違いがある場合は、スタックの残りの部分と異なる各 FRU が個別の表に示されます。
show install rollback	**show install rollback {point-id | label}**	保存されているインストールポイントに関連付けられたパッケージを表示します。
show version	**show version [rp-slot] [installed [user-interface] | provisioned | running]**	ハードウェアとプラットフォームの情報とともに、現在のパッケージに関する情報を表示します。

プラットフォームをインストールモードで起動

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

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

1 ステップインストールまたはバンドルモードからインストールモードへの変換

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

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

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

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

手順の概要

1. **enable**
2. **install add file location:** *filename* [**activate commit**]
3. **exit**

手順の詳細

手順

	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。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
	`Device>enable`	
ステップ 2	**install add file location:** *filename* [**activate commit**] 例： `Device#install add file bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_15_4o_117.SSA.bin activate commit`	ソフトウェア インストール パッケージをローカルまたはリモートの場所（FTP、HTTP、HTTPs、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよびpackages.confファイルに展開します。プラットフォームおよびイメージバージョンの検証および互換性チェックを実行し、パッケージをアクティブ化し、そのパッケージをコミットして複数回リロードしても維持されるようにします。 このコマンドを実行すると、プラットフォームがリロードされます。
ステップ 3	**exit** 例： `Device#exit`	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

3 ステップインストール

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

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

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

手順の概要

1. **enable**
2. **install add file location:** *filename*
3. **show install summary**
4. **install activate** [**auto-abort-timer** <*time*>]
5. **install abort**

6. **install commit**
7. **install rollback to committed**
8. **install remove** {**file** *filesystem: filename* | **inactive**}
9. **show install summary**
10. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device>enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**install add file location:** *filename* 例： `Device#install add file bootflash:c8000aep-universalk9.17.15.04a.SPA.bin`	ソフトウェア インストール パッケージをリモートの場所（FTP、HTTP、HTTPs、またはTFTP経由）からプラットフォームにコピーし、.packageファイルの個々のコンポーネントをサブパッケージおよびpackages.confファイルに展開します。
ステップ 3	**show install summary** 例： `Device#show install summary`	（オプション）すべての FRU のイメージバージョンとそれに対応するインストール状態の概要を提供します。
ステップ 4	**install activate** [**auto-abort-timer** <*time*>] 例： `Device# install activate auto-abort-timer 120`	以前に追加されたパッケージをアクティブ化し、プラットフォームをリロードします。 • ソフトウェアの完全インストールを実行する場合は、パッケージ ファイル名を指定しないでください。 • 3 ステップインストールのバリアントでは、**install activate** コマンドで **auto-abort-timer** が自動的に開始されます。タイマーのデフォルトは 120 分です。タイマーの期限が切れる前に **install commit** コマンドが実行されない場合、インストールプロセスは自動的に終了します。プラットフォームがリロードされ、最後にコミットされたバージョンで起動します。
ステップ 5	**install abort** 例： `Device#install abort`	（オプション）ソフトウェアインストールのアクティブ化を中止し、プラットフォームを最後にコミットされたバージョンに戻します。

	コマンドまたはアクション	目的
		• このコマンドは、イメージがアクティブ化されている状態でのみ使用できます。イメージがコミットされた状態の場合は使用できません。
ステップ 6	**install commit** 例： `Device#install commit`	新しいパッケージのインストールをコミットし、リロード後も変更が持続されるようにします。
ステップ 7	**install rollback to committed** 例： `Device#install rollback to committed`	（オプション）最後にコミットした状態にプラットフォームをロールバックします。
ステップ 8	**install remove** {**file** *filesystem: filename* | **inactive**} 例： `Device#install remove inactive`	（オプション）ソフトウェア インストール ファイルを削除します。 • **file**：特定のファイルを削除します • **inactive**：未使用および非アクティブ状態のインストールファイルを削除します。
ステップ 9	**show install summary** 例： `Device#show install summary`	（オプション）現在のシステムの状態に関する情報を表示します。このコマンドの出力は、このコマンドよりも先に実行された **install** コマンドに応じて変化します。
ステップ 10	**exit** 例： `Device#exit`	特権 EXEC モードを終了し、ユーザー EXEC モードに戻ります。

インストール モードでのアップグレード

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

インストールモードでのダウングレード

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

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

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

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

ソフトウェアインストールの中止

ソフトウェアパッケージのアクティブ化は次の方法で中止できます。

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

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

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

インストールコマンドを使用したソフトウェアインストールの設定例

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

```
Router #install add file
bootflash:c8000aep-universalk9.BLD_POLARIS_DEV_LATEST_20250628_033228_V17_19_0_21.SSA.bin
 activate commit
install_add_activate_commit: START Mon Jul 07 14:22:07 IST 2025
install_add: START Mon Jul 07 14:22:07 IST 2025
install_add: Adding IMG
--- Starting initial file syncing ---
Copying
bootflash:c8000aep-universalk9.BLD_POLARIS_DEV_LATEST_20250628_033228_V17_19_0_21.SSA.bin
 from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members

*Jul  7 08:52:07.326: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
 add_activate_commit
bootflash:c8000aep-universalk9.BLD_POLARIS_DEV_LATEST_20250628_033228_V17_19_0_21.SSA.binChecking
 status of Add on [R0]
Add: Passed on [R0]
```

```
Image added. Version: 17.19.01.0.224220

Finished Add

install_activate: START Mon Jul 07 14:22:16 IST 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c8000aep-firmware_ngwic_t1e1.BLD_POLARIS_DEV_LATEST_20250628_033228_V17_19_0_21.SSA.pkg
/bootflash/c8000aep-firmware_nim_ssd.BLD_POLARIS_DEV_LATEST_20250628_033228_V17_19_0_21.SSA.pkg
/bootflash/c8000aep-mono-universalk9.BLD_POLARIS_DEV_LATEST_20250628_033228_V17_19_0_21.SSA.pkg
/bootflash/c8000aep-rpboot.BLD_POLARIS_DEV_LATEST_20250628_033228_V17_19_0_21.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]
*Jul  7 08:52:16.603: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
 activate NONEy

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

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

SUCCESS: install_add_activate_commit Mon Jul 07 14:22:41 IST 2025
Encore#
*Jul  7 08:52:41.750: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed
install add_activate_commitJul  7 14:22:48.332: %PMAN-5-E




Initializing Hardware ...


System integrity status: 90170200  21030106
Procyon RSM done


System Bootstrap, Version Private [sajjha-blue_pqc 109], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2025 by cisco Systems, Inc.
Compiled Fri Jun 13 14:17:01 2025 by sajjha

Current image running: Boot ROM0
Last reset cause: LocalSoft

Disk ID:#0,MSA281400HY-Micron_7450_MTFDKBA480TFR    - Disk already unlocked
C8570-G2 platform with 33554432 Kbytes of main memory

Enc_5_P2B 1 >
```

以下は、3 ステップインストールの例です。

```
Router #install add file boo
Encore#$rsalk9.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.bin
```

```
install_add: START Mon Jul 07 14:53:11 IST 2025
install_add: Adding IMG
--- Starting initial file syncing ---
Copying
bootflash:c8000aep-universalk9.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.bin
 from  R0 to  R0
Info: Finished copying to the selected
Finished initial file syncing

--- Starting Add ---
Performing Add on all members

*Jul  7 09:23:11.416: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
 add
bootflash:c8000aep-universalk9.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.binChecking
 status of Add on [R0]
Add: Passed on [R0]
Image added. Version: 17.19.01.0.223976

Finished Add

SUCCESS: install_add
/bootflash/c8000aep-universalk9.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.bin
 Mon Jul 07 14:53:19 IST 2025

Encore#
*Jul  7 09:23:19.987: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed
install add
bootflash:/c8000aep-universalk9.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.bin
Encore#
Encore#install activate
install_activate: START Mon Jul 07 14:54:14 IST 2025
install_activate: Activating IMG
Following packages shall be activated:
/bootflash/c8000aep-firmware_ngwic_t1e1.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.pkg
/bootflash/c8000aep-firmware_nim_ssd.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.pkg
/bootflash/c8000aep-mono-universalk9.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.pkg
/bootflash/c8000aep-rpboot.BLD_POLARIS_DEV_LATEST_20250625_033136_V17_19_0_20.SSA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]
                                                                                *Jul  7
 09:24:14.874: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install activate
 NONEy

--- Starting Activate ---
Performing Activate on all members
 [1] Activate package(s) on  R0

*Jul  7 09:25:18.674: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds [1] Finished Activate on  R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

SUCCESS: install_activate Mon Jul 07 14:55:25 IST 2025

Encore#
*Jul  7 09:25:25.208: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed
install activateJul  7 14:55:31.791: %PMAN-5-EXITAC
Encore#install commit
install_commit: START Mon Jul 07 14:59:12 IST 2025
--- Starting Commit ---
Performing Commit on all members
 [1] Commit packages(s) on  R0
```

```
*Jul  7 09:29:12.013: %INSTALL-5-INSTALL_START_INFO: R0/0: install_mgr: Started install
 commit [1] Finished Commit packages(s) on  R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit operation

SUCCESS: install_commit Mon Jul 07 14:59:13 IST 2025

Encore#
*Jul  7 09:29:13.749: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_mgr: Completed
install commit
```

以下は、インストールモードでのダウングレードの例です。

```
Router# install activate file bootflash:c8000be-universalk9.17.06.01a.SPA.bin activate
commit

install_add_activate_commit: START Fri Dec 10 18:07:17 GMT 2021

*Dec 10 18:07:18.405 GMT: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started
install one-shot
bootflash:c8000be-universalk9.17.06.01a.SPA.bininstall_add_activate_commit: Adding PACKAGE
install_add_activate_commit: Checking whether new add is allowed ....

--- Starting Add ---
Performing Add on Active/Standby
  [1] Add package(s) on R0
  [1] Finished Add on R0
Checking status of Add on [R0]
Add: Passed on [R0]
Finished Add

Image added. Version: 17.06.01a.0.298
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/c8000be-rpboot.17.06.01a.SPA.pkg
/bootflash/c8000be-mono-universalk9.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_async.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_1t3e3.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_sm_10g.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_prince.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_xdsl.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_ssd.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_shdsl.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_ge.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_cwan.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_bri_st_fw.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_nim_async.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_ngwic_t1e1.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.17.06.01a.SPA.pkg
/bootflash/c8000be-firmware_dreamliner.17.06.01a.SPA.pkg

This operation may require a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on Active/Standby
  [1] Activate package(s) on R0
  [1] Finished Activate on R0
Checking status of Activate on [R0]
```

```
Activate: Passed on [R0]
Finished Activate

--- Starting Commit ---
Performing Commit on Active/Standby
  [1] Commit package(s) on R0
Building configuration...

  [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit

[OK]
*Dec 10 18:14:57.782 GMT: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
 config fileSend model notification for install_add_activate_commit before reload
/usr/binos/conf/install_util.sh: line 164: /bootflash/.prst_sync/reload_info: No such
file or directory
/usr/binos/conf/install_util.sh: line 168: /bootflash/.prst_sync/reload_info: No such
file or directory
cat: /bootflash/.prst_sync/reload_info: No such file or directory
Install will reload the system now!
SUCCESS: install_add_activate_commit  Fri Dec 10 18:15:23 GMT 2021

ROUTER#
*Dec 10 18:15:23.955 GMT: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine:
Completed install one-shot PACKAGE bootflash:c8000be-universalk9.17.06.01a.SPA.binDec
10 18:15:27.708: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload action
 requested

Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610
Rom image verified correctly

System Bootstrap, Version 17.3(5r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoft
ROUTER platform with 8388608 Kbytes of main memory

□

Press RETURN to get started!

□

ROUTER#
ROUTER# show version
Cisco IOS XE Software, Version 17.06.01a
Cisco IOS Software [Bengaluru], c8000be Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Version 17.6.1a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Sat 21-Aug-21 03:27 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2021 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: 17.3(5r)

ROUTER uptime is 0 minutes
Uptime for this control processor is 2 minutes
System returned to ROM by LocalSoft
System image file is "bootflash:packages.conf"
Last reload reason: LocalSoft

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     Type         Technology-package Technology-package
                            Current            Next Reboot
------------------------------------------------------------------
Smart License  Perpetual    None               None
Smart License  Subscription None               None

The current crypto throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

cisco ROUTER (1RU) processor with 3747220K/6147K bytes of memory.
Processor board ID FDO2521M27S
Router operating mode: Autonomous
5 Gigabit Ethernet interfaces
2 2.5 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
7573503K bytes of flash memory at bootflash:.
1875361792K bytes of NVMe SSD at harddisk:.
16789568K bytes of USB flash at usb0:.

Configuration register is 0x2102
```

以下は、ソフトウェアのインストールを終了する例です。

```
Router# install abort
install_abort: START Fri Oct 29 02:42:51 UTC 2021

This install abort would require a reload. Do you want to proceed? [y/n]
                                                                    *Oct 29
```

```
02:42:52.789: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install aborty
--- Starting Abort ---
Performing Abort on Active/Standby

  [1] Abort package(s) on R0
  [1] Finished Abort on R0
Checking status of Abort on [R0]
Abort: Passed on [R0]
Finished Abort

Send model notification for install_abort before reload
Install will reload the system now!
SUCCESS: install_abort  Fri Oct 29 02:44:47 UTC 2021

Router#
*Oct 29 02:44:47.866: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install abort PACKAGEOct 29 02:44:51.577: %PMAN-5-EXITACTION: R0/0: pvp: Process manager
 is exiting: reload action requested

Initializing Hardware ...

Checking for PCIe device presence...done
System integrity status: 0x610

System Bootstrap, Version 17.3(4.1r), RELEASE SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.

Current image running   : Boot ROM1
Last reset cause        : LocalSoft
C8300-2N2S-6T platform with 8388608 Kbytes of main memory

□

Press RETURN to get started!

□
```

以下は、show コマンドの出力例です。

show install log

```
Device# show install log
[0|install_op_boot]: START Thu Oct 28 22:09:29 Universal 2021
[0|install_op_boot(INFO, )]: Mount IMG INI state base image
[0|install_op_boot]: END SUCCESS  Thu Oct 28 22:09:30 Universal 2021
```

show install summary

```
Device# show install summary
[ R0 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------
IMG   C    17.07.01.0.1515

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

show install package *filesystem: filename*

```
Device# show install package
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
Package: c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin

  Size: 831447859
  Timestamp: 2021-10-23 17:08:14 UTC
  Canonical path:
/bootflash/c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin


  Raw disk-file SHA1sum:
    5c4e7617a6c71ffbcc73dcd034ab58bf76605e3f
  Header size:     1192 bytes
  Package type:    30000
  Package flags:   0
  Header version:  3

  Internal package information:
    Name: rp_super
    BuildTime: 2021-10-21_13.00
    ReleaseDate: 2021-10-21_03.11
    BootArchitecture: i686
    RouteProcessor: radium
    Platform: C8000BE
    User: mcpre
    PackageName: universalk9
    Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
    CardTypes:

  Package is bootable from media and tftp.
  Package contents:

  Package:
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
    Size: 2966620
    Timestamp: 2021-10-21 20:10:44 UTC

    Raw disk-file SHA1sum:
      501d59d5f152ca00084a0da8217bf6f6b95dddb1
    Header size:     1116 bytes
    Package type:    40000
    Package flags:   0
    Header version:  3

    Internal package information:
      Name: firmware_nim_ge
      BuildTime: 2021-10-21_13.00
      ReleaseDate: 2021-10-21_03.11
      BootArchitecture: none
      RouteProcessor: radium
      Platform: C8000BE
      User: mcpre
      PackageName: firmware_nim_ge
      Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
      CardTypes:

    Package is not bootable.
  Package:
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
    Size: 10204252
    Timestamp: 2021-10-21 20:10:43 UTC

    Raw disk-file SHA1sum:
      a57bed4ddecfd08af3b456f69d11aaeb962865ea
```

```
    Header size:     1116 bytes
    Package type:    40000
    Package flags:   0
    Header version:  3

    Internal package information:
      Name: firmware_prince
      BuildTime: 2021-10-21_13.00
      ReleaseDate: 2021-10-21_03.11
      BootArchitecture: none
      RouteProcessor: radium
      Platform: C8000BE
      User: mcpre
      PackageName: firmware_prince
      Build: BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117
      CardTypes:

    Package is not bootable.
```

show install active

```
Device# show install active
[ R0 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------
IMG   C    17.07.01.0.1515

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

show install inactive

```
Device# show install inactive
[ R0 ] Inactive Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------
No Inactive Packages
```

show install committed

```
Device# show install committed
[ R0 ] Committed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------
IMG   C    17.07.01.0.1515

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

show install uncommitted

```
Device# show install uncommitted
[ R0 ] Uncommitted Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
```

```
--------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------
No Uncommitted Packages
```

インストールコマンドを使用したソフトウェアインストールのトラブルシューティング

問題 ソフトウェアインストールのトラブルシューティング

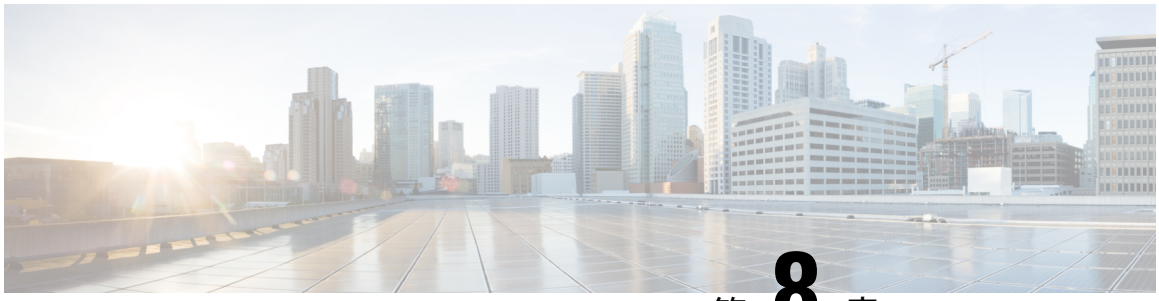
解決法 インストールの概要、ログ、およびソフトウェアバージョンを表示するには、次のshowコマンドを使用します。

- **show install summary**
- **show install log**
- **show version**
- **show version running**

問題 インストールに関するその他の問題

解決法 インストールに関する問題を解決するには、次のコマンドを使用します。

- **dir** <*install directory*>
- **more location:***packages.conf*
- **show tech-support install**：このコマンドはインストール情報に固有の情報を表示する**show**コマンドを自動的に実行します。
- **request platform software trace archive target bootflash** <*location*>：このコマンドは、最後のリロード以降にシステム上で実行されているすべてのプロセスに関連するすべてのトレースログをアーカイブし、この情報を指定された場所に保存します。

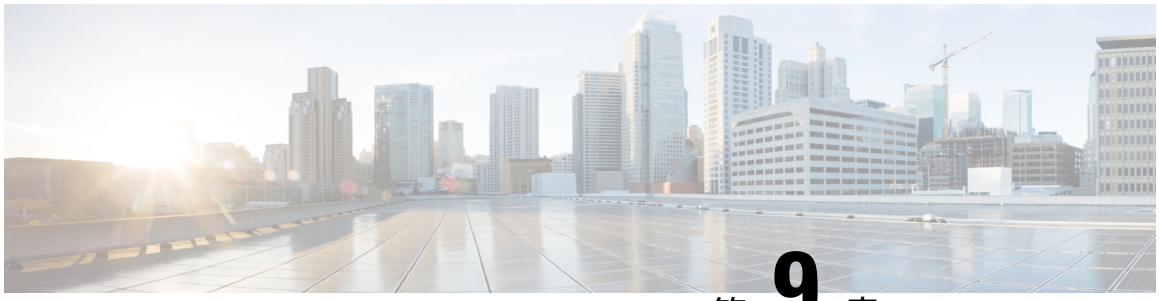


第 8 章

ソフトウェア アップグレード プロセス

ROMMON と IOS を同時にアップグレードする場合は、次の手順を実行します。

- XE イメージをルータにコピーし、新しいイメージをポイントするようにブートシステムを設定します。
- ROMMON パッケージをルータにコピーし、ROMMON アップグレードを実行します。
- ルータをリロードし、新しい XE イメージの IOS プロンプトで起動することを確認します。
- show platform を使用して、新しい ROMMON イメージが正常にインストールされたことを確認します。



第 9 章

工場出荷時の状態へのリセット

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。

工場出荷時の状態へのリセットに関する機能情報

表 *12 :* 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	Cisco IOS XE 17.15.4a	Cisco IOS XE 17.15.4a 以降、Cisco 8500 シリーズ セキュア ルータでは、次のコマンドがサポートされています。 **factory-reset all** **factory-reset all secure** **factory-reset keep-licensing-info** **factory-reset sed**

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、デバイス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、以前のフル機能を備えた状態にデバイスをリセットするプロセスです。

初期設定へのリセットプロセスでは、**factory-reset all** コマンドを使用して既存のコンフィギュレーション情報のバックアップを取ってから、以前のフル機能を備えた状態にルータをリセットします。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サイズによって異なります。統合プラットフォームでは 30 分で、高可用性設定では最大 3 時間かかる場合があります。

NIST PURGE/CLEAR の標準に従って、**factory-reset all secure** コマンドを使用してルータをリセットし、ルータの永続ストレージを消去できます。また、ルータを起動したイメージは保持されず、ルータは ROMmon プロンプトにフォールバックします。このプロセスには 5 分 ～ 2 時間かかります。

表 *13 :* 初期設定へのリセット時に消去または保持されるデータ

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	USB の内容
	ライセンス	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）
	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	
	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） 工場出荷時設定へのリセットが完了した後、不揮発性ストレージからすべて消去されるため、ルータはリモートストレージまたはUSBに保存されているイメージから起動する必要があります。	
	コンフィギュレーション レジスタの値 **重要** 設定レジスタの値は、Cisco 8500 シリーズ セキュアルータで **factory-reset all secure** コマンドを使用して消去できます。	

コマンド名	消去されるデータ	保持されるデータ
factory-reset all	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	USB の内容
	ライセンス	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）
	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	コンフィギュレーション レジスタの値
	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。	
factory-reset keep-licensing-info	ライセンスブートレベルの設定	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）
	スループットレベルの設定	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）
	スマートライセンス転送タイプ	固有デバイス ID（UDI）信頼コード
	スマートライセンス URL データ	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

コマンド名	消去されるデータ	保持されるデータ
factory-reset sed	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	USB の内容
	ライセンス	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）
	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	ROMMON 変数
	SED 対応ディスク上のすべてのデータ。	コンフィギュレーション レジスタの値

次の表に **factory-reset sed** コマンドでサポートされるプラットフォームの概要を示します。

プラットフォーム	ブートフラッシュ	ハードディスク
C8550-G2	SED 有効	該当なし
C8570-G2	SED 有効	該当なし

factory-reset all secure コマンドでは、常に ROMMON が起動します。他のコマンドの場合、config-register 値に基づきます。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のソフトウェアおよびハードウェアサポート

- 初期設定へのリセットプロセスは、スタンドアロンルータに加えて、高可用性向けに設定されたルータでもサポートされています。

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、**factory-reset all** コマンドでは、ブートイメージのバックアップが作成されます。
- 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。この場合、TFTP または USB に保存されているイメージを使用してルータを起動する必要があります。
- 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。
- **factory-reset all secure** コマンドは、仮想テレタイプ（VTY）セッションではサポートされていません。

初期設定へのリセットを実行する場合

- 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。

手順

ステップ1 Cisco 8500 シリーズ セキュア ルータへのログイン

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4つの部分（a、b、c、d）に分かれています。起動イメージを保持せずに、NISTの標準に従ってすべてのデータを消去する場合は、手順2.aに従います。構成登録値およびローカルブートイメージを保持した状態でデータを消去する場合は、手順2.bに従います。sedドライブを消去するだけの場合は、手順2.cに従います。factory-resetコマンドを実行している間、ライセンス情報を保持する必要がある場合は、手順2.dに従います。

a) NISTの標準に従って、**factory-reset all secure** コマンドを実行して消去します。

factory-reset all secure 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
The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]
 This is a NIST CLEAR/PURGE.
 The following will be deleted as a part of factory reset:
 1: All writable file systems and personal data
 2: OBFL logs
 3: Licenses
 4: Userdata and Startup config
 5: Rommon variables
 6: User Credentials
 The system will reload to perform factory reset.
 This operation can take anywhere between 30 minutes to 3 hours
 DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
 Are you sure you want to continue? [confirm]
 The image saved on the router would be lost. The router will fall to the rommon prompt
 Are you sure you want to continue? [confirm]
Mar

Enabling factory reset for this reload cycle


Enabling factory reset for this reloa
*Mar 24 08:19:02.634: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : Starting ACT2/AIKIDO
 CLEANUP

*Mar 24 08:19:17.289: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : ACT2/AIKIDO Cleanup
 done
```

```
*Mar 24 08:19:17.413: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : Erasing Rommon
Variables and Config Register

*Mar 24 08:19:18.400: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : Successfully erased
 the rommon variables and config register

*Mar 24 08:19:18.568: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : Starting Datawipe

*Mar 24 08:19:18.685: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : Erasing the storage
 devices as per NIST-SP-800-88-r standard:
Executing Data Sanitization...
bootflash
NVMe Data Sanitization started ...
!!! Please, wait - NVMe sanitizing /dev/nvme0n1 !!!
NVME Sanitize Status: Successful
NVMe Data Sanitization completed ...
Data Sanitization Success! Exiting...

*Mar 24 08:19:48.948: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Purge non-volatile storage done.
========================
#CISCO C8500-G2 DATA SANITIZATION REPORT#
START : 24-03-2025, 08:19:21
  END : 24-03-2025, 08:19:44
-NVMe-
PNM : MSA281400FR
PRV : E2MU200
SN : /dev/ng0n1
Status : SUCCESS
NIST : PURGE
========================

*Mar 24 08:19:49.357: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : Datawipe Completed

*Mar 24 08:20:02.980: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : Report save done.

*Mar 24 08:20:03.097: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Factory reset successfull. Continuing
 with reboot...
```

b) **factory-reset all** コマンドを実行して、データを消去します。

factory-reset all 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
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
 The following will be deleted as a part of factory reset:
 1: All writable file systems and personal data
 2: OBFL logs
 3: Licenses
 4: Userdata and Startup config
 5: Rommon variables
 6: User Credentials
 The system will reload to perform factory reset.
 This operation can take anywhere between 30 minutes to 3 hours
 DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
 Are you sure you want to continue? [confirm]
 Factory reset will take a backup of the boot image if the system is currently booted from an
image stored locally. If the current boot image is a remote image or stored on a usb/nim-ssd,
please take a backup of the image before executing this command.
 Are you sure you want to continue? [confirm]
Mar

Enabling factory reset for this reload cycle
```

```
Enabling factory reset for this reload cycle

*Mar 24 10:36:43.858: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Taking a backup of
bootflash:packages.conf. It will be restored to bootflash: after factory reset is complete

*Mar 24 10:36:45.571: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : Starting ACT2/AIKIDO
 CLEANUP

*Mar 24 10:37:00.098: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): % FACTORYRESET : ACT2/AIKIDO Cleanup
 done

*Mar 24 10:37:00.596: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Erasing file system

*Mar 24 10:37:01.458: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Erasing file system

*Mar 24 10:37:01.796: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Erasing file system
 . . . . . .
 . . . . . .
 . . . . . .
 . . . . . .
. . . . . .
. . . . . .
.
 . . . . . .
 . . . . . .
. . . . . .
. . . . . .
.
 . . . . . .
 . . . . . .
. . . . . .

*Mar 24 11:32:04.869: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Erasing file system
 .

*Mar 24 11:32:07.004: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Erasing file system
 .

*Mar 24 11:32:09.133: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Erasing file system
 .

*Mar 24 11:32:11.262: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Erasing file system
 .

*Mar 24 11:32:15.568: %IOSXEBOOT-4-FACTORY_RESET: (rp/0): Factory reset successfull. Continuing
 with reboot...


Initializing Hardware ...
```

c) **factory-reset sed** コマンドを実行して、sed ドライブを消去します。

factory-reset sed 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 sed
% Warning: factory reset on SED drive reloads router
Do you want to continue? (yes/[no]): yes
SUCCESS

Router#
Router#


***
```

```
*** --- SHUTDOWN NOW ---
***

*Jan 14 00:48:41.482: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload due to
 factory reset on SED.Jan 14 00:48:48.499: %PMAN-5-EXITACTION: R



Initializing Hardware ...
```

d) **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
```

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。

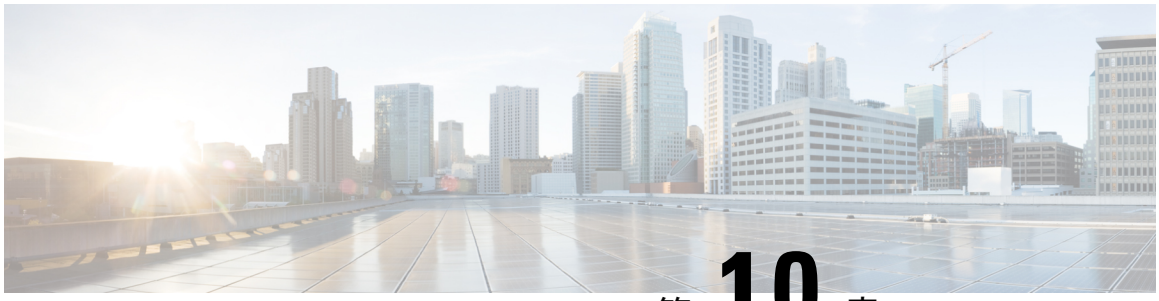
（注）
初期設定へのリセットプロセスの所要時間は、ルータのストレージのサイズによって異なります。これは、高可用性セットアップでは、5 分から 3 時間延長できます。初期設定へのリセットプロセスを終了する場合は、**Escape** キーを押します。

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 10 章

Security-Enhanced Linux のサポート

この章では SELinux の機能について説明します。具体的な内容は次のとおりです。

概要

Security-Enhanced Linux（SELinux）は、Linux カーネル セキュリティ モジュールとシステム ユーティリティで構成されるソリューションで、強力で柔軟な Mandatory Access Control（MAC）アーキテクチャを Cisco IOS-XE プラットフォームに組み込みます。

SELinux には機密性と整合性の要件に基づいて情報を分離するための拡張メカニズムが備わっています。これにより、アプリケーションのセキュリティメカニズムの改ざんやバイパスの脅威に対処し、悪意のあるアプリケーションや欠陥のあるアプリケーションによって引き起こされる可能性のある障害を封じ込めることができます。

SELinux の前提条件

この機能に関する固有の要件はありません。

SELinux の制限事項

この機能に関する特定の制限はありません。

SELinux に関する情報

SELinux はユーザープログラムやシステムサービスを、割り当てられた機能を実行するために必要になる最小限の権限に制限する強制アクセス制御ポリシーを適用します。これにより、（バッファのオーバーフローや設定ミスなどによって）侵害された場合、害を生じさせるこれらのプログラムやデーモンの能力が削減または排除されます。これは、Cisco IOS-XE プラットフォームで MAC を適用することによる最小権限の原則の実用的な実装です。この制限メカニズムは、従来の Linux アクセス制御メカニズムとは独立して機能します。SELinux は、アプリケーションプロセスからリソースオブジェクトへのアクセスを制御するポリシーを定義する機能を提供します。これにより、プロセス動作の明確な定義と制限を明確にできます。

SELinux は、システムで有効になっている場合、**Permissive モード**または **Enforcing モード**のいずれかで動作します。

- Permissive モードでは、SELinux はポリシーを適用せず、リソースアクセスポリシーの違反によって発生した拒否のシステムログのみを生成します。操作は拒否されず、リソースアクセスポリシー違反についてのみログに記録されます。
- Enforcing モードでは、SELinux ポリシーが有効になり、適用されます。アクセスポリシールールに基づいてリソースアクセスを拒否し、システムログを生成します。

サポートされている Cisco IOS XE プラットフォームでは、SELinux はデフォルトで Enforcing モードで有効になっています。Enforcing モードでは、必要な許可ポリシーを持たないシステムリソースアクセスは違反として扱われ、操作は拒否されます。拒否が発生すると、違反操作は失敗し、システムログが生成されます。Enforcing モードでは、ソリューションはアクセス違反防止モードで機能します。

SELinux の設定

Enforcing モードで SELinux 機能を有効化または操作するために必要な追加の要件や設定手順はありません。

SELinux の機能の一部として、次のコマンドが導入されています。

```
platform security selinux {enforcing | permissive}
show platform software selinux
```

SELinux の設定（EXEC モード）

set platform software selinux コマンドを使用して、EXEC モードで SELinux を設定します。

次に、EXEC モードでの SELinux 設定の例を示します。

```
Device# set platform software selinux ?

default  Set SELinux mode to default
enforcing  Set SELinux mode to enforcing
permissive  Set SELinux mode to permissive
```

SELinux の設定（CONFIG モード）

platform security selinux コマンドを使用して、コンフィギュレーション モードで SELinux を設定します。

次の例は、CONFIG モードでの SELinux 設定を示しています。

```
Device(config)# platform security selinux

enforcing  Set SELinux policy to Enforcing mode
permissive  Set SELinux policy to Permissive mode

Device(config)# platform security selinux permissive

Device(config)#
*Oct 20 21:52:45.155: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!

Device(config)#
```

SELinux の例

次に、モードを Enforcing から Permissive に変更した場合の出力例を示します。

```
"*Oct 20 21:44:03.609: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode downgraded to permissive!"
```

次に、モードを Permissive から Enforcing に変更した場合の出力例を示します。

```
"*Oct 20 21:44:34.160: %IOSXE-1-PLATFORM: R0/0:
SELINUX_MODE_PROG: Platform Selinux confinement mode upgraded to enforcing!"
```

（注） SELinux モードが変更されると、この変更はシステム セキュリティ イベントと見なされ、システムログメッセージが生成されます。

Syslog メッセージリファレンス

機能重大度ニーモニック	%SELINUX-1-VIOLATION
重大度の意味	アラートレベルログ
メッセージ	該当なし
メッセージの説明	リソースのアクセスポリシーが存在しないプロセスによって、リソースアクセスが実行されました。操作にフラグが設定され、リソースアクセスが拒否されました。プロセスリソースアクセスが拒否されたという情報を含むシステムログが生成されました。
コンポーネント	SELINUX

機能重大度ニーモニック	%SELINUX-1-VIOLATION
推奨処置	次の関連情報を添付ファイルとしてCisco TACにご連絡ください。 • コンソールまたはシステムに出力されるとおりのメッセージ • **show tech-support** コマンドの出力（テキストファイル） • ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）： **request platform software trace archive target <URL>** • **show platform software selinux** コマンドの出力

次に、syslog メッセージの例を示します。

例 1：

```
*Nov 14 00:09:04.943: %SELINUX-1-VIOLATION: R0/0: audispd: type=AVC
msg=audit(1699927057.934:129): avc: denied { getattr } for pid=5899 comm="ls"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive=0
```

例 2：

```
*Nov 14 00:09:04.947: %SELINUX-1-VIOLATION: R0/0: audispd: t type=AVC
msg=audit(1699927198.486:130): avc: denied { write } for pid=6012 comm="echo"
path="/root/test" dev="rootfs" ino=25839
scontext=system_u:system_r:polaris_iosd_t:s0
tcontext=system_u:object_r:admin_home_t:s0 tclass=file permissive= 0
```

SELinux の有効化の確認

show platform software selinux コマンドを使用して、SELinux 設定モードを表示します。

```
Device# show platform software selinux
========================================
IOS-XE SELINUX STATUS
========================================
SElinux Status :    Enabled
Current Mode :      Enforcing
Config file Mode :  Enforcing
```

SELinux のトラブルシューティング

デバイスまたはネットワークで SELinux 違反のインスタンスがある場合は、次の詳細を Cisco TAC に連絡してください。

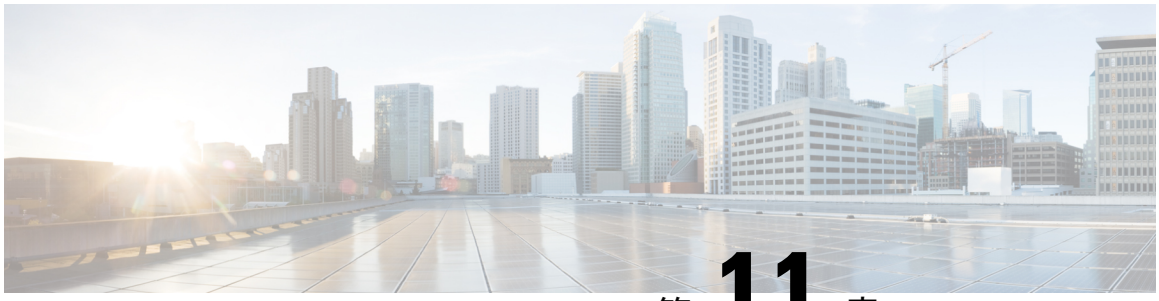
- コンソールまたはシステムログに出力されるとおりのメッセージ。次に例を示します。

```
device#request platform software trace archive target
    flash:selinux_btrace_logs
```

- **show tech-support** コマンドの出力（テキストファイル）
- ボックスからの Btrace ファイルのアーカイブ（次のコマンドを使用）：

  request platform software trace archive target <URL>

- **show platform software selinux** コマンドの出力



第 11 章

高可用性の概要

Cisco HA（ハイ アベイラビリティ）により、ネットワークのどの場所でも発生する障害からの高速回復が可能になり、ネットワーク規模での保護が実現されます。Cisco HA を使用すると、ネットワークのハードウェアおよびソフトウェアが連携し、中断からの高速回復が可能となるため、ユーザおよびネットワーク アプリケーションへの障害の透過性が保証されます。

Cisco 8500 シリーズ セキュア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限のアップタイムと復元力が実現します。

このガイドでは、Cisco 8500 シリーズ セキュアルータ独自の高可用性の特徴について説明します。このマニュアルには、高可用性に関する総合的な説明は記載されていません。また、Cisco 8500 シリーズ セキュアルータ上と同様に設定され、導入されている他のシスコルータで使用できる高可用性機能の説明も掲載されていません。この章と併せて、Cisco IOS 機能に関する資料およびマニュアルを参照して、複数のシスコのプラットフォームで使用でき、Cisco 8500 シリーズ セキュアルータ上でも同様に動作する高可用性機能に関する情報を入手してください。

この章で紹介する機能情報の入手方法

ご使用のソフトウェア リリースで、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。

目次

このセクションでは、Cisco 8500 シリーズ セキュアルータのさまざまな高可用性の特徴について説明します。内容は、次のとおりです。

Cisco 8500 シリーズ セキュアルータのソフトウェア冗長性

この項では、次のトピックについて取り上げます。

ソフトウェア冗長性の概要

Cisco 8500 シリーズ セキュアルータでは、IOS はオペレーティングシステム内の多くのプロセスの 1 つとして実行されます。この点は、Cisco IOS 内ですべてのプロセスが実行されている従来の Cisco IOS とは異なります。Cisco 8500 シリーズセキュアルータのプロセスとしての IOS の詳細については、「IOS as a Process」セクション（2 ～ 7 ページ）を参照してください。

このアーキテクチャにより、Cisco IOS ソフトウェアを稼働するその他のプラットフォームでは使用できないソフトウェアの冗長性が実現します。スタンバイ IOS プロセスを、アクティブ IOS プロセスと同じ RP 上で使用することができます。このスタンバイ IOS プロセスは、IOS に障害が発生した場合に切り替えることができます。

2 つの Cisco IOS プロセスの設定

Cisco 8500 シリーズ セキュアルータでは、Cisco IOS が多くのプロセスの 1 つとして実行されます。このアーキテクチャは、ソフトウェアの冗長性の機会をサポートします。具体的には、スタンバイ Cisco IOS プロセスをアクティブ Cisco IOS プロセスと同じルートプロセッサで使用することができます。Cisco IOS で障害が発生した場合、システムはスタンバイ Cisco IOS プロセスに切り替わります。

手順の概要

1. enable
2. **configure terminal**
3. redundancy
4. mode SSO
5. **exit**
6. reload

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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	redundancy 例： `Router(config)# redundancy`	冗長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	mode SSO 例： `Router(config)# mode SSO`	SSO を設定します。このコマンドが入力されると、冗長スーパーバイザエンジンがリロードされ、SSO モードで動作を開始します。

ステップ 5	**exit**
	例：
	`Router(config)# exit`
	例：
	`Router #`
		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 モードに戻ります。

ステップ 6	reload 例： `Router # reload`	IOS をリロードします。

ステートフル スイッチオーバー

Cisco 8500 シリーズ セキュアルータでは、Stateful Switchover（SSO）を使用して、2 番目の IOS プロセスを有効にすることができます。

SSO は、NSF と連携すると、さらに威力を発揮します。SSO により、デュアル IOS プロセスは常にステートを維持できます。また、スイッチオーバーが発生すると、ノンストップ フォワーディングによってスイッチオーバーがシームレスに実行されます。

NSF/SSO の詳細については、『Cisco Nonstop Forwarding』マニュアルを参照してください。

SSO 認識プロトコルおよびアプリケーション

SSO によってサポートされるライン プロトコルとアプリケーションは、SSO 認識である必要があります。機能やプロトコルが、RP スイッチオーバーを経ても、一部または全体が問題なく動作し続ける場合、その機能やプロトコルは SSO 認識です。SSO 認識プロトコルおよびアプリケーションのステート情報をアクティブからスタンバイに同期することにより、これらのプロトコルおよびアプリケーションでの SSO が実現されます。

SSO 非認識のプロトコルおよびアプリケーションの場合、ステートをダイナミックに作成しても、スイッチオーバー時に失われるため、スイッチオーバーの際に再初期化と再起動が必要になります。

ルータ上のどのプロトコルが SSO 対応であるかを確認するには、次のコマンドを使用します。**show redundancy client** または **show redundancy history**

IPsec フェールオーバー

IPSec フェールオーバーは、カスタマーの IPsec ネットワークの合計稼働時間（または可用性）を増やす機能です。従来、これは元の（アクティブな）ルータに加えて冗長（スタンバイ）ルータを使用することで実現されています。アクティブ ルータが何らかの理由で使用できなくなると、スタンバイ ルータは、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 種類のカテゴリに分類されます。

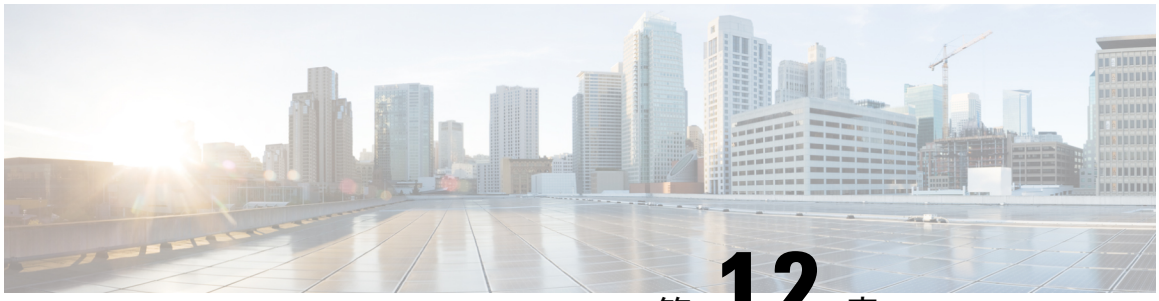
Cisco 8500 シリーズ セキュア ルータの IPSec は、ステートレス フェイルオーバーのみをサポートします。ステートレス フェールオーバーは、ホット スタンバイ ルータ プロトコル（HSRP）のようなプロトコルを使用して、プライマリからセカンダリへのカットオーバーを行い、さらにアクティブおよびスタンバイの VPN ゲートウェイを許可して、共通の仮想 IP アドレスを共有することができます。

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ために設計された検出プロトコルです。高速転送パス障害検出に加えて、BFD はネットワーク管理者に整合性のある障害検出方法を提供します。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。

Cisco 8500 シリーズ セキュアルータでは、IPv4 スタティックルート用の BFD と BGP 用の BFD が完全にサポートされます。

BFD の詳細については、『Bidirectional Forwarding Detection』マニュアルを参照してください。



第 12 章

管理イーサネット インターフェイスの使用

Cisco 8500 シリーズ セキュアルータには、1 つのギガビットイーサネットの管理イーサネットインターフェイスがあります。

この章で紹介する機能情報の入手方法

ご使用のソフトウェア リリースで、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。

目次

このマニュアルは、次の内容で構成されています。

ギガビット イーサネット管理インターフェイスの概要

このインターフェイスの目的は、ユーザがルータ上で管理タスクを実行できるようにすることです。基本的には、インターフェイスが原因で不要にネットワーク トラフィックが転送されたり、また、ほとんどの場合は転送できなかったりしますが、Telnet およびセキュア シェル（SSH）を経由すれば、ルータへのアクセスが可能となり、ルータ上のほとんどの管理タスクを実行することができます。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 SPA 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。

- 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。
- イーサネット管理インターフェイスは、合法的傍受の MD ソース インターフェイスとしては使用できません。
- 管理イーサネット インターフェイスは、自身の VPN ルーティングおよび転送（VRF）の一部です。詳細については、ギガビット イーサネット管理インターフェイスの VRF（101 ページ）を参照してください。

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。

このポートには、Cisco ASR 8500 シリーズ セキュアルータ上の他のポートと同様に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)#
```

ROMmon および管理イーサネット ポートの IP アドレス処理

Cisco 8500 シリーズ セキュアルータでは、IP アドレスを ROMmon（**IP_ADDRESS=** および **IP_SUBNET_MASK=** コマンド）に、IOS コマンドライン インターフェイス（インターフェイス コンフィギュレーション モードでの **ip address** コマンド）を使用して設定できます。

Cisco ASR 8500 シリーズ セキュアルータ上で IOS プロセスが開始されない場合、ROMmom に設定された IP アドレスが管理イーサネット インターフェイスの IP アドレスとして動作します。IOS プロセスが稼働中で、管理イーサネット インターフェイスを制御している場合は、IOS CLI のインターフェイス Gigabit Ethernet 0 の設定時に指定した IP アドレスが、管理イーサ

ネット インターフェイスの IP アドレスとなります。ROMmon で定義された IP アドレスは、IOS プロセスが非アクティブな場合にだけインターフェイス アドレスとして使用されます。

このため、ROMmon と IOS CLI で指定された IP アドレスは同一になり、管理イーサネット インターフェイスはシングル RP 構成で適切に機能します。

ギガビット イーサネット管理インターフェイスの VRF

ギガビット イーサネット管理インターフェイスは、自動的に自身の VRF の一部となっています。「Mgmt-intf」という名前の VRF は Cisco 8500 シリーズ セキュアルータ上で自動的に設定され、管理イーサネットインターフェイス専用となります。他のインターフェイスはこの VRF に加入できません。したがって、この VRF はマルチプロトコル ラベル スイッチング（MPLS）VPN VRF またはその他のネットワーク規模の VRF には参加できません。Mgmt-intf VRF は、ループバック インターフェイスをサポートします。

管理イーサネット インターフェイスを自身の VRF 内に配置すると、管理イーサネット インターフェイスに次のような影響が発生します。

- VRF 内では多数の機能を設定して使用する必要があるため、特定の管理イーサネット機能に関して、CLI が Cisco 8500 シリーズ セキュアルータ上と他のルータの管理イーサネットインターフェイス上とで異なる可能性があります。
- トラフィックが、ルータを中継して通過できなくなります。すべての内蔵ポートと管理イーサネットインターフェイスはそれぞれ異なる VRF に配置されるため、中継トラフィックは管理イーサネットインターフェイスに着信できず、内蔵ポートから発信することができなくなります。また、その逆のことも発生します。
- インターフェイスのセキュリティが改善されます。Mgmt-intf VRF は自身の VRF 内に属することで、独自のルーティングテーブルがあるため、ユーザが明示的に管理イーサネットインターフェイスを開始した場合にだけ、ルートを管理イーサネットインターフェイスのルーティング テーブルに追加できます。

管理イーサネット インターフェイスの VRF では、IPv4 と IPv6 の両方のアドレス ファミリがサポートされます。

共通のイーサネット管理タスク

ユーザは管理イーサネットインターフェイスを介してルータ上のほとんどのタスクを実行できます。

このセクションでは、Cisco 8500 シリーズルータ上で共通のタスクまたは少し注意が必要なタスクについて説明します。ただし、管理イーサネットインターフェイスで実行できるすべてのタスクを包括的に説明するわけではありません。

ここでは、次のプロセスについて説明します。

VRF 設定の表示

管理イーサネット インターフェイスの VRF 設定は、**show running-config vrf** コマンドを使用して、表示できます。

次に、デフォルトの VRF 設定の例を示します。

```
Router# show running-config vrf
Building configuration...
Current configuration : 351 bytes
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
(some output removed for brevity)
```

管理イーサネット VRF の詳細な VRF 情報の表示

管理イーサネット VRF の詳細情報を表示するには、 **show vrf detail Mgmt-intf** コマンドを入力します。

```
Router# show vrf detail Mgmt-intf
```

管理イーサネット インターフェイス VRF でのデフォルト ルートの設定

管理イーサネット インターフェイス VRF でデフォルト ルートを設定するには、次のコマンドを入力します。

ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 *next-hop-IP-address*

管理イーサネット IP アドレスの設定

管理イーサネット ポートの IP アドレスは、その他のインターフェイス上の IP アドレスと同じように設定します。

次に、管理イーサネット インターフェイス上で IPv4 アドレスおよび IPv6 アドレスを設定する簡単な例を 2 つ示します。

IPv4 の例

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ip address
 A.B.C.D A.B.C.D
```

IPv6 の例

```
Router(config)# interface GigabitEthernet 0
```

Router(config-if)# **ipv6 address** *X:X:X:X::X*

管理イーサネット インターフェイス上での Telnet 接続

Telnet 接続は、管理イーサネット インターフェイスを使用して VRF 経由で行うことができます。

次の例では、ルータは管理イーサネット インターフェイスの VRF を介して 172.17.1.1 に Telnet 接続します。

```
Router# telnet 172.17.1.1 /vrf Mgmt-intf
```

管理イーサネット インターフェイス上での PING の実行

他のインターフェイスへの PING の実行は、管理イーサネット インターフェイスを使用して VRF 経由で行うことができます。

次の例では、ルータは管理イーサネットインターフェイスを介して、172.17.1.1 の IP アドレスが設定されたインターフェイスに PING を送信します。

```
Router# ping vrf Mgmt-intf 172.17.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

TFTP または FTP を使用したコピー

管理イーサネットインターフェイスにより TFTP を使用してファイルをコピーする場合、**copy tftp** コマンドには VRF 名を指定するオプションがないため、**copy tftp** コマンドを入力する前に **ip tftp source-interface GigabitEthernet 0** コマンドを入力する必要があります。

同様に、管理イーサネット インターフェイスにより FTP を使用してファイルをコピーする場合、**copy ftp** コマンドには VRF 名を指定するオプションがないため、**copy ftp** コマンドを入力する前に **ip ftp source-interface GigabitEthernet 0** コマンドを入力する必要があります。

TFTP の例

```
Router(config)# ip tftp source-interface gigabitethernet 0
```

FTP の例

```
Router(config)# ip ftp source-interface gigabitethernet 0
```

NTP サーバー

管理イーサネット インターフェイスを通じて Network Time Protocol（NTP）タイムサーバーと同期をとれるようにソフトウェアクロックを設定するには、**ntp server vrf Mgmt-intf** コマンドを入力し、アップデートを提供するデバイスの IP アドレスを指定します。

次の CLI では、このプロシージャの例を示します。

```
Router(config)# ntp server vrf Mgmt-intf 172.17.1.1
```

SYSLOG サーバー

送信元の IP または IPv6 アドレスとして管理イーサネット インターフェイスをログに記録されるように指定するには、**logging host <ip-address> vrf Mgmt-intf** コマンドを入力します。

次の CLI では、このプロシージャの例を示します。

```
Router(config)# logging host <ip-address> vrf Mgmt-intf
```

SNMP 関連サービス

管理イーサネット インターフェイスをすべての SNMP トラップメッセージのソースとして指定するには、**snmp-server source-interface traps gigabitEthernet 0** コマンドを入力します。

次の CLI では、このプロシージャの例を示します。

```
Router(config)# snmp-server source-interface traps gigabitEthernet 0
```

ドメイン名の割り当て

管理イーサネット インターフェイスへのドメイン名の割り当ては、VRF を介して実行されます。

デフォルトのドメイン名を管理イーサネット VRF インターフェイスとして定義するには、**ip domain-name vrf Mgmt-intf** *domain* コマンドを入力します。

```
Router(config)# ip domain-name vrf Mgmt-intf cisco.com
```

DNS サービス

管理イーサネット インターフェイスの VRF をネームサーバーとして指定するには、**ip name-server vrf Mgmt-intf** *IPv4-or-IPv6-address* コマンドを入力します。

```
Router(config)# ip name-server vrf Mgmt-intf
 IPv4-or-IPv6-address
```

RADIUS サーバーまたは TACACS+ サーバー

管理 VRF を AAA サーバーグループの一部としてグループ化するには、AAA サーバーグループの設定時に **ip vrf forward Mgmt-intf** コマンドを入力します。

TACACS+ サーバーグループを設定する場合も、同様にします。管理 VRF を TACACS+ サーバーグループの一部としてグループ化するには、TACACS+ サーバーグループの設定時に **ip vrf forwarding Mgmt-intf** コマンドを入力します。

RADIUS サーバーグループの設定

```
Router(config)# aaa group server radius hello
Router(config-sg-radius)# ip vrf forwarding Mgmt-intf
```

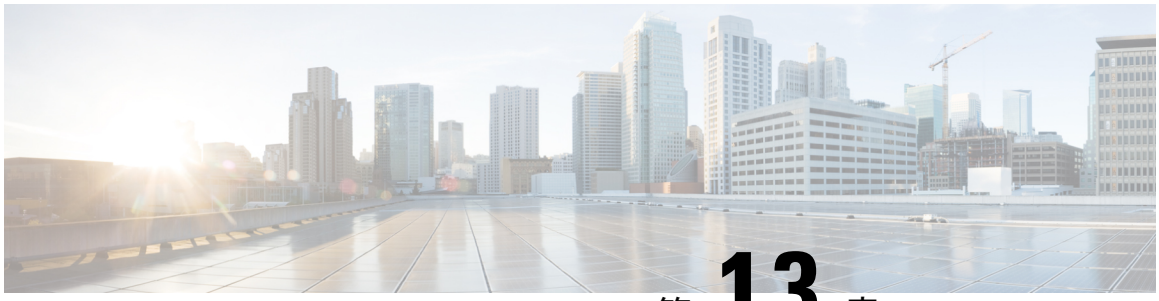
TACACS+ サーバーグループの例

```
outer(config)# aaa group server tacacs+ hello
Router(config-sg-tacacs+)# ip vrf forwarding Mgmt-intf
```

ACL を使用した VTY 回線

アクセスコントロールリスト（ACL）を、VRF を使用する（または使用しない）vty 回線に付加するには、ACL を vty 回線に付加する際に **vrf-also** オプションを使用します。

```
Router(config)# line vty 0 4
Router(config-line)# access-class 90 in vrf-also
```



第 13 章

ブリッジ ドメイン インターフェイスの設定

Cisco 8500 シリーズ セキュアルータは、レイヤ 2 イーサネットセグメントをレイヤ 3 IP にパッケージングするためのブリッジ ドメイン 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
  - ホットスタンバイ ルータ プロトコル（HSRP）
  - IOS XE 3.8.0 以降の Virtual Router Redundancy Protocol（VRRP）
- 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。

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 8500 シリーズ セキュアルータ上のすべてのブリッジ ドメイン インターフェイスは、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 8500 シリーズ セキュアルータを有効にし、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{2列にまたがって開始}{2列にまたがって終了}	
{start emdash}{end emdash}	**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。システムへ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 8500 シリーズセキュアルータ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を示します。

表 *14 : 8500* シリーズ セキュアルータ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
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。

Cisco 8500 シリーズ セキュアルータでサポートされる BD-VIF の最大数は次のとおりです。

- C8570-G2 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。
- C8550-G2 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。

BD-VIF は Flexible NetFlow（FNF）をサポートしています。

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

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 BDI** *{interface number}*

例：

```
Router(config-if)# interface BDI3
```

Cisco 8500 シリーズ セキュアルータのブリッジ 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 2.2.2.1 255.255.255.0
```

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。

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
```

Cisco 8500 シリーズ セキュアルータのブリッジ 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
```

Cisco 8500 シリーズ セキュアルータのブリッジ 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 2.2.2.1 255.255.255.0 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 2.2.2.1 255.255.255.0
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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	**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：	選択した CPP L2BD Client のデバッグがオンになります。

	コマンドまたはアクション	目的
	`Router# debug platform hardware qfp active feature l2bd client all`	
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、次の URL で『Cisco IOS Configuration Fundamentals Command Reference Guide』を参照してください。

{start hypertext}http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html{end hypertext}

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
```

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

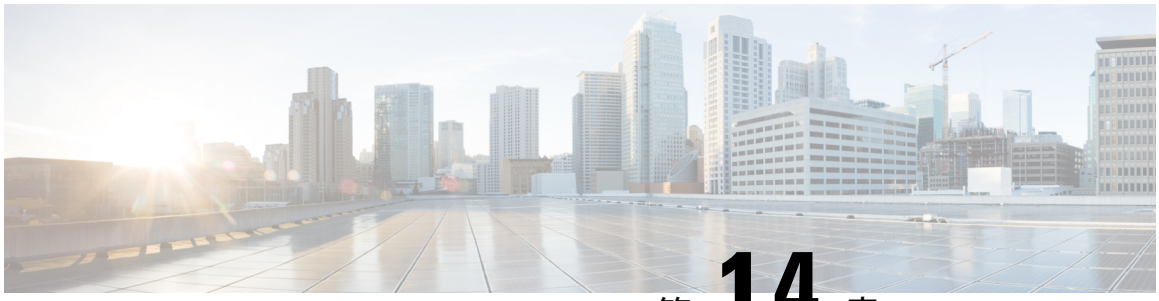
show pla sof inter fp ac brief | i BD_VIF

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
```



第 14 章

パケットトレース

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 *15*：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。

パケットトレースレベル	説明
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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを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）。
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。

	コマンドまたはアクション	目的
		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： `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 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。

	コマンドまたはアクション	目的
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

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	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	**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。
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

	コマンドまたはアクション	目的
		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。 *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。

	コマンドまたはアクション	目的
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 *16 : 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 *17 : 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      : 198.51.100.2
    Destination : 198.51.100.2
    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います。

```
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 : 224.0.0.102
    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 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
```

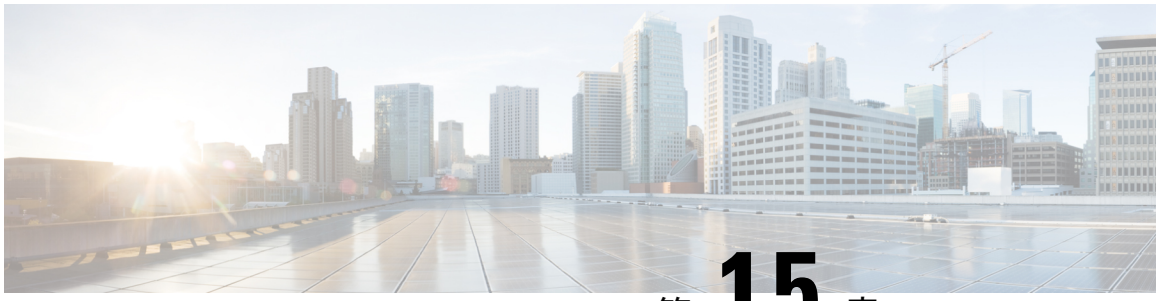
```
  FORWARDED
 TCP: Connection is in SYNRCVD state
 ACK         : 2346709419
 SEQ         : 3052140910
 Source      : 198.51.100.38(22)
 Destination : 198.51.100.55(52774)


  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#
```



第 15 章

パケット ドロップ

このドキュメントでは、Cisco 8500 シリーズ セキュアルータでのパケットドロップについて説明します。

パケットドロップについて

パケットドロップの表示

show drops コマンドを実行して、パケットドロップの根本原因をトラブルシューティングできます。

show drops コマンドを使用すると、以下を特定できます。

- 機能またはプロトコルに基づくドロップの根本原因。
- QFP ドロップの履歴。

パケットドロップ情報の表示

次の手順を実行して、インターフェイス、プロトコル、または機能に基づいて、インスタンスのパケットドロップ情報を表示およびフィルタリングできます。

手順の概要

1. **enable**
2. **show drops**
3. **show drops** { **bqs** | **crypto**| **firewall**| **interface**| **ip-all**| **nat**| **punt**| **qfp**| **qos**|**history**}

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。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 drops** 例： `Router# show drops`	ドロップ統計を表示します。
ステップ 3	**show drops** { **bqs**	**crypto**| **firewall**| **interface**| **ip-all**| **nat**| **punt**| **qfp**| **qos**|**history**} 例： `Router# show drops qfp`	選択したインターフェイスまたはプロトコルのドロップ統計と概要を表示します。 （注） Cisco IOS XE 17.13.1a から、新しいキーワードオプション history が **show drops** コマンドに追加されました。**show drop history qfp** コマンドを使用すると、QFP ドロップの履歴を表示できます。

例

パケットドロップ情報の表示例：出力例

次に、show drops コマンドの出力例を示します。この出力例には、QuantumFlow Processor（QFP）に関連した **packet drops** 情報が表示されます。

```
Router#show drops
bqs BQS related drops
crypto IPSEC related drops
firewall Firewall related drops
history History of drops
interface Interface drop statistics
ip-all IP related drops
nat NAT related drops
punt Punt path related drops
qfp QFP drop statistics
qos QoS related drops
| Output modifiers
<cr> <cr>
```

```
Router# show drops qfp
------------------ show platform hardware qfp active statistics drop detail
Last clearing of QFP drops statistics : Fri Feb 18 08:02:37 2022
(6d 23h 54m 29s ago)
-------------------------------------------------------------------------------
ID Global Drop Stats Packets
Octets
-------------------------------------------------------------------------------
319 BFDoffload 9
1350
61 Icmp 84
3780
53 IpFragErr 32136
48718168
244 IpLispHashLkupFailed 3
213
56 IpsecInput 18
4654
23 TailDrop 26713208
10952799454
216 UnconfiguredIpv6Fia 241788
26596680
------------------ show platform hardware qfp active interface all
statistics drop_summary
-----------------------------------------------------------------
Drop Stats Summary:
note: 1) these drop stats are only updated when PAL
reads the interface stats.
2) the interface stats include the subinterface
Interface Rx Pkts Tx Pkts
-------------------------------------------------------------------------------
GigabitEthernet1 60547 0
GigabitEthernet2 60782 27769658
GigabitEthernet3 60581 0
GigabitEthernet4 60502 1323990
Tunnel14095001 0 1990214
Tunnel14095002 0 3883238
Tunnel14095003 0 3879243
Tunnel14095004 0 2018866
Tunnel14095005 0 3875972
Tunnel14095006 0 3991497
Tunnel14095007 0 4107743
Tunnel14095008 0 3990601
```

パケット情報の検証

このセクションでは、パケット情報を検証するためのコマンド出力の例を示します。

パケットプロセッサエンジン（PPE）のすべてのインターフェイスでのドロップの統計を表示するには、**show drops qfp** コマンドを使用します。

（注） ラッパーコマンド **show drops qfp** は、元の **show platform hardware qfp active statistics drop** コマンドの省略表記です。

```
Router#show drops qfp
-----------------------------------------------------------------
```

```
Global Drop Stats Octets
Packets
-------------------------------------------------------------
AttnInvalidSpid 0 0
BadDistFifo 0 0
BadIpChecksum 0 0
```

パケットプロセッサエンジン（PPE）のすべてのインターフェイスでのQFPドロップの履歴を表示するには、**show drops history qfp** コマンドを使用します。このコマンドを使用すると、過去 1 分間、5 分間、および 30 分間のパケットドロップ数も追跡できます。

（注） ラッパーコマンド **show drops history qfp** は、元の **show platform hardware qfp active statistics drop history** コマンドの省略表記です。

```
Router# show drops history qfp
Last clearing of QFP drops statistics : Mon Jun 26 07:29:14
2023
(21s ago)
-------------------------------------------------------------
Global Drop Stats 1-Min
5-Min 30-Min All
-------------------------------------------------------------
Ipv4NoAdj 0
0 0 99818
Ipv4NoRoute 0
0 0 99853
```

パケットドロップ警告

ドロップ原因ごとの警告しきい値および/または合計 QFP ドロップ数を 1 秒あたりのパケット数で設定できます。設定されたしきい値を超えると、レート制限されたsyslog警告が生成されます。合計しきい値を超えると 1 つの警告が生成され、ドロップの原因ごとに 1 つの警告が生成されます。

警告は、ドロップ原因ごとに最大 1 分間に 1 回生成されます。直前の 1 分間のドロップ数がしきい値（1 秒あたりのパケット数）X 60 の値と比較され、ドロップ数がこの値を超えると、警告が生成されます。

次に、合計数およびドロップ原因ごとの数に対応するそれぞれの警告の例を示します。

```
%QFP-5-DROP_OVERALL_RATE: Exceeded the overall drop threshold 10000 pps during the last
 60-second measurement period, packets dropped in last 1 minute: 641220, last 5 minutes:
 1243420, last 30 minutes: 124342200

%QFP-5-DROP_CAUSE_RATE: Exceeded the drop threshold 1000 pps for QosPolicing (drop code:
 20) during the last 60-second measurement period, packets dropped due to QosPolicing
in last 1 minute: 61220, last 5 minutes: 43420, last 30 minutes: 4611200
```

パケットドロップ警告しきい値の設定

ドロップ原因ごとの警告しきい値および/または 1 秒あたりのパケット数における合計 QFP ドロップ数を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **platform qfp drops threshold** {**per-cause** *drop_id threshold* | **total** *threshold*}

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。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	**platform qfp drops threshold** {**per-cause** *drop_id threshold*	**total** *threshold*} 例： `Router# platform qfp drops threshold per-cause 206 10`	ドロップ原因ごとのしきい値、またはドロップ合計数のしきい値を指定します。 （注） ドロップ原因 ID を表示するには、**show platform hardware qfp active statistics drop detail** コマンドを使用します。

例

次に、ドロップ原因ごとの警告しきい値と合計 QFP ドロップ数を設定する例を示します。

ドロップ原因ごとの QFP ドロップ数警告しきい値の設定例

次に、ドロップ原因 ID 24 の警告しきい値を 15 pps に設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)#platform qfp drops threshold ?
per-cause Set warning threshold for per cause QFP drops
total Set warning threshold for total QFP drops
```

```
Router(config)#platform qfp drops threshold per-cause ?
<0-1024> QFP drop cause ID
Router(config)#platform qfp drops threshold per-cause 24 ?
<0-2147483647> Drop threshold in packets per second (pps)
Router(config)#platform qfp drops threshold per-cause 24 15
```

合計 QFP ドロップ数の警告しきい値の設定例

次に、合計 QFP ドロップ数の警告しきい値を 100 pps に設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)#platform qfp drops threshold ?
per-cause Set warning threshold for per cause QFP drops
total Set warning threshold for total QFP drops
Router(config)#platform qfp drops threshold total ?
<0-2147483647> Drop threshold in packets per second (pps)
Router(config)#platform qfp drops threshold total 100
```

パケットドロップ警告しきい値の表示

設定済みのドロップ原因ごとの警告しきい値と合計 QFP ドロップ数を表示するには、次の手順を実行します。

手順の概要

1. **enable**
2. **show platform hardware qfp active statistics drop threshold**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。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 platform hardware qfp active statistics drop threshold** 例： `Router# show platform hardware qfp active statistics drop thresholds`	設定済みのドロップの原因ごとの警告しきい値と合計 QFP ドロップ数を表示します。 （注） • ラッパーコマンド **show drops thresholds** は、**show platform hardware qfp active statistics drop threshold** コマンドの省略表記です。

例

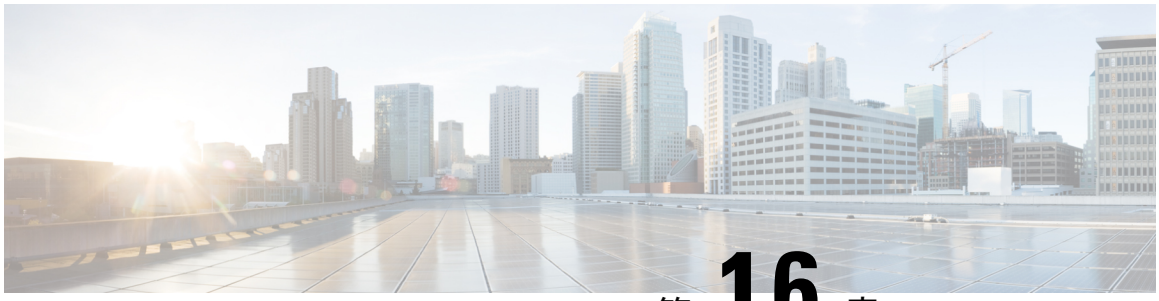
パケットドロップ警告しきい値の表示例

次に、**show platform hardware qfp active statistics drop threshold** コマンドの出力例を示します。

```
Router#show platform hardware qfp active statistics drop thresholds
------------------------------------------------------
Drop ID         Drop Cause Name             Threshold
------------------------------------------------------
10              BadIpChecksum                100
206             PuntPerCausePolicerDrops     10
20              QosPolicing                  200
                 Total                        30
```

次に、**show drops thresholds** ラッパーコマンドの出力例を示します。

```
Router#show platform hardware qfp active statistics drop thresholds
------------------------------------------------------
Drop ID         Drop Cause Name             Threshold
------------------------------------------------------
10              BadIpChecksum                100
206             PuntPerCausePolicerDrops     10
20              QosPolicing                  200
                 Total                        30
```



第 16 章

SR-TE 優先パスを介した EVPN VPWS

イーサネット VPN 仮想プライベートワイヤサービス（EVPN VPWS）の機能により、PE のペア間でEVPNインスタンスを確立するためのシグナリングおよびカプセル化技術が実装されます。この拡張により EVPN VPWS が拡張され、**preferred path** 機能を使用して SR-TE ポリシーの仕様がサポートされます。

SR-TE 優先パスを介した EVPN VPWS 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 *18 : SR-TE* 優先パスを介した *EVPN VPWS* の機能情報

機能名	リリース	機能情報
SR-TE 優先パスを介した EVPN VPWS	Cisco IOS XE Cupertino 17.15.4a	この機能が導入されました。

SR-TE 優先パスを介した EVPN VPWS の制約事項

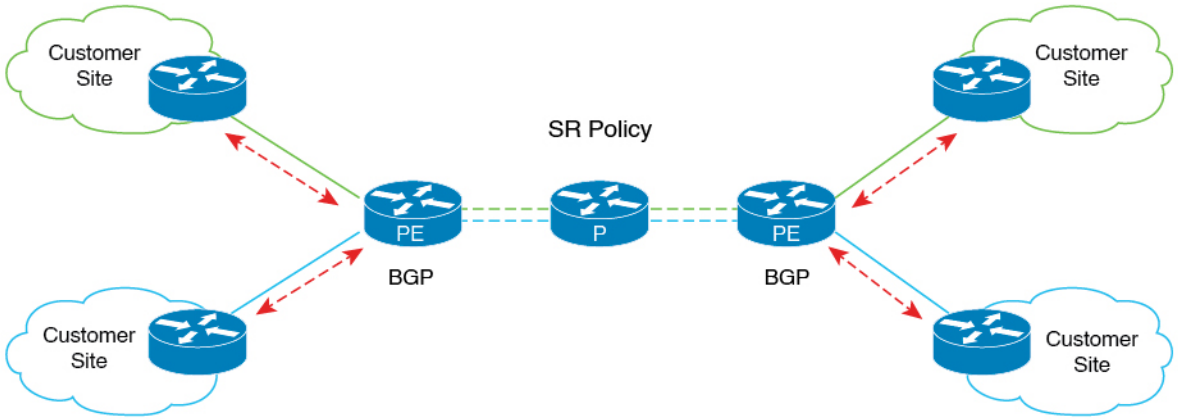
- SR オンデマンドネクストホップ（ODN）ポリシーはサポートされていません。SR 静的ポリシーのみがサポートされます。
- SR フロー単位ポリシー（PFP）はサポートされていません。SR 宛先単位ポリシー（PDP）のみがサポートされています。
- 内部ゲートウェイプロトコル（IGP）は Intermediate System-to-Intermediate system（IS-IS）です。

SR-TE 優先パスを介した EVPN VPWS に関する情報

EVPN VPWS の機能により、PE のペア間で EVPN インスタンスを確立するためのシグナリングおよびカプセル化技術が実装されます。この拡張により、EVPN VPWS は、**preferred path** 機能を使用して SR-TE ポリシーの仕様をサポートできるようになります。この機能には、優先パスがダウンした場合に代替パスにフォールバックするデフォルトの動作を無効にする **fallback disable** オプションが含まれています。

次の図にアーキテクチャを示します。

図 *1 : SR-TE* アーキテクチャを介した *EVPN VPWS*



SR-TE 優先パスを介した EVPN VPWS の設定方法

次のセクションでは、SR-TE 優先パスを介した EVPN VPWS の設定に関連するタスクについて説明します。

SR-TE 優先パスを介した EVPN VPWS の設定

次の例は、設定された SR-TE 優先パスを介した EVPN VPWS を有効にする方法を示しています。

```
l2vpn evpn instance 100 point-to-point
 rd 100:100
 route-target export 100:100
 route-target import 100:100
 !
 vpws context vc100
  preferred-path segment-routing traffic-eng policy p-100
  service target 100 source 100
interface GigabitEthernet0/0/3
service instance 100 ethernet
encapsulation dot1q 100
```

フォールバックの無効化と SR-TE 優先パスを介した EVPN VPWS の設定

fallback disable コマンドは、優先パスの SR ポリシーがダウンした場合に、デバイスがデフォルトのパスを使用しないようにします。

```
l2vpn evpn instance 100 point-to-point
rd 100:100
route-target export 100:100
route-target import 100:100
vpws context vc100
service target 100 source 100
member GigabitEthernet0/0/3 service-instance 100
preferred-path segment-routing traffic-eng policy p-100 disable-fallback
```

SR-TE 優先パスを介した EVPN VPWS からのフォールバックの無効化の削除

次の例は、SR-TE 優先パスを介した EVPN VPWS でフォールバックの無効化のオプションを削除する方法を示しています。

```
l2vpn evpn instance 100 point-to-point
 vpws context vc100
  preferred-path segment-routing traffic-eng policy p-100
```

SR-TE 優先パス設定を介した EVPN VPWS の無効化

次の例は、SR-TE 優先パス設定を介した EVPN VPWS を無効にする方法を示しています。

```
l2vpn evpn instance 100 point-to-point
 vpws context vc100
 no  preferred-path segment-routing traffic-eng policy p-100 disable-fallback
```

SR-TE 優先パスを介した EVPN VPWS の確認

次の出力例は、SR-TE 優先パスを介した EVPN VPWS とフォールバックの無効化の設定を確認する方法を示しています。

- 次に、SR-TE 優先パスを介した EVPN VPWS 設定を示す出力例を示します。

```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
  EVPN ID: 100
  VPWS Service Instance ID: Source 1, Target 2
  Labels: Local 17, Remote 17
  Next Hop Address: 6.6.6.6
  Associated member interface Gi0/0/3 up, Gi0/0/3:3000 status is up
  Output interface: Tu65536, imposed label stack {16016 17}
  Preferred path:   active
  Default path: ready

device# show l2vpn evpn vpws vc preferred-path
Tunnel         EVPN ID  Source    Target    Name      Status
-------------       ------   --------  --------  --------  ----------
Tunnel65536     100       1         2            vc100        up
```

- 次に、フォールバックが無効になっている SR-TE 優先パスを介した EVPN VPWS 設定を示す出力例を示します。

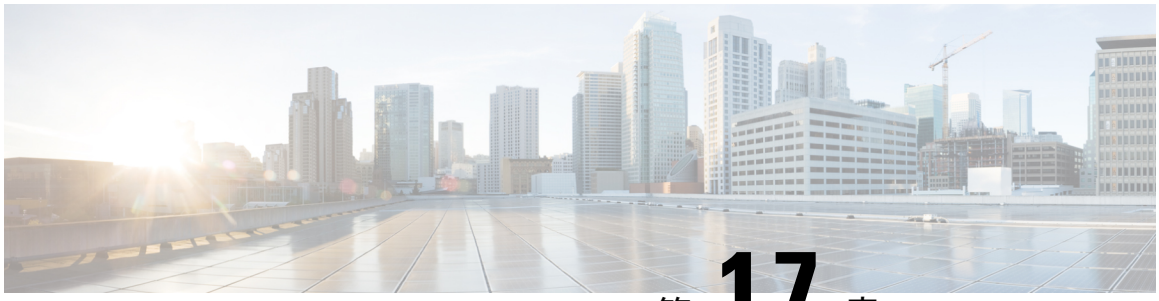
```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
  EVPN ID: 100
  VPWS Service Instance ID: Source 1, Target 2
  Labels: Local 17, Remote 17
  Next Hop Address: 6.6.6.6
  Associated member interface Gi0/0/3 up, Gi0/0/3:3000 status is up
  Output interface: Tu65536, imposed label stack {16016 17}
  Preferred path:   active
  Default path:  disabled
Dataplane:
SSM segment/switch IDs: 25037/12290 (used), PWID: 1
Rx Counters
1241 input transit packets, 463266 bytes
0 drops
Tx Counters
828 output transit packets, 402840 bytes
0 drops
24 VC FSM state transitions, Last 10 shown
DpUp: Act -> Est, Mon Sep 06 23:32:43.809 (2w2d ago)
RemDn: Est -> RemWait, Mon Sep 06 23:32:43.809 (2w2d ago)
RemUp: RemWait -> Act, Mon Sep 06 23:32:43.816 (2w2d ago)
DpUp: Act -> Est, Mon Sep 06 23:32:43.816 (2w2d ago)
DpDn: Est -> Act, Mon Sep 06 23:35:57.944 (2w2d ago)
DpUp: Act -> Est, Mon Sep 06 23:43:50.071 (2w2d ago)
DpDn: Est -> Act, Mon Sep 06 23:46:15.361 (2w2d ago)
DpUp: Act -> Est, Mon Sep 06 23:54:11.508 (2w2d ago)
DpDn: Est -> Act, Tue Sep 07 00:00:11.248 (2w2d ago)
DpUp: Act -> Est, Tue Sep 07 00:06:27.355 (2w2d ago)
```

- 次に、フォールバックの無効化のオプションが削除された、SR-TE 優先パスを介した EVPN VPWS 設定を示す出力例を示します。

```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
  EVPN ID: 100
  VPWS Service Instance ID: Source 1, Target 2
  Labels: Local 17, Remote 17
  Next Hop Address: 6.6.6.6
  Associated member interface Gi0/0/3 up, Gi0/0/3:3000 status is up
  Output interface: Tu65536, imposed label stack {16016 17}
  Preferred path:   active
  Default path:  ready
```

- 次に、SR-TE 優先パスを介した EVPN VPWS 設定が無効になっている出力例を示します。

```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
  EVPN ID: 100
  VPWS Service Instance ID: Source 1, Target 2
  Labels: Local 17, Remote 17
  Next Hop Address: 6.6.6.6
  Associated member interface Gi0/0/3 up, Gi0/0/3:3000  status is up
  Output interface: Gi0/0/0, imposed label stack {16 16}
  Preferred path: not configured
  Default path:  active
```



第 17 章

SFP の設定

SFP+ の設定

（注） いくつかのシスコプラットフォーム、NIM、および SM カードでは、同じインターフェイスでのマルチレート SFP の設定がサポートされています（10G ポートでの 1G SFP または 10G SFP+ など）。

ポートチャネルバンドルでは、すべてのメンバーインターフェイスの速度とデュプレックスが同じである必要があります。ポートチャネルを設定するには、メンバーインターフェイスと同じ速度のデュプレックス インターフェイスを使用することをお勧めします。

マルチレート SFP をサポートするインターフェイスの詳細については、対応するデータシートを参照してください。

手順の概要

1. **enable** *source-interface gigabitethernet slot/port*
2. **configure terminal**
3. **interface tengigabitethernet** *slot/port*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** *source-interface gigabitethernet slot/port* 例：	特権 EXEC モードをイネーブルにします。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
	`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	**interface tengigabitethernet** *slot/port* 例： *`Router(config)# interface tengigabitethernet 4/11`*	設定する 10 ギガビット イーサネット インターフェイスを指定します。 ここで、各変数は次のように定義されます。 slot/port：インターフェイスの場所を指定します。

FEC の設定

順方向エラー修正（FEC）は、長距離データ転送中に潜在的なエラーをチェックして回復します。Cisco 8500 シリーズ セキュアルータには SFP の範囲が長いため、FEC を設定する必要があります。

手順の概要

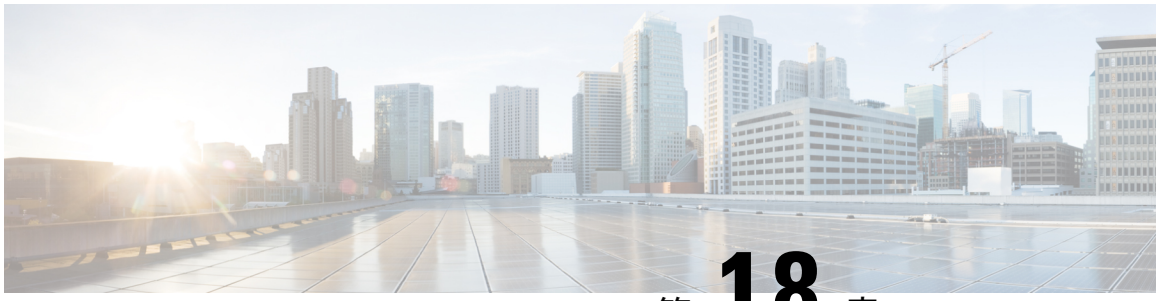
1. **enable** *source-interface gigabitethernet slot/port*
2. **configure terminal**
3. **interface twentyfivegigabitethernet** *slot/port*
4. **fec** { **auto** | **cl108** | **cl74** | **off**}

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** *source-interface gigabitethernet slot/port* 例： `Router# enable`	特権 EXEC モードをイネーブルにします。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。

	コマンドまたはアクション	目的
ステップ 3	**interface twentyfivegigabitethernet** *slot/port* 例： `Router(config)# interface twentyfivegigabitethernet 0/0/16 4/11`	設定する 10 ギガビット イーサネット インターフェイスを指定します。 ここで、各変数は次のように定義されます。 slot/port：インターフェイスの場所を指定します。
ステップ 4	**fec** { **auto** | **cl108** | **cl74** | **off**} 例： `Router(config)# interface twentyfivegigabitethernet 0/0/16 4/11`	FEC を構成します。 次に、FEC コマンドのモードを示します。 • auto— SFP タイプに基づいて FEC を有効にします • cl108— clause108 <= RS-FEC(528,514) を有効にします • cl74— clause74 <= FC-FEC を有効にします • disable—インターフェイスで FEC を無効にします （注） • FEC コマンドは 25G リンクにのみ適用されます。 • 10/25G デュアルレート SFP の場合、速度が 25G から 10G に変更された場合は、速度を変更する前に最初に FEC 設定を削除する必要があります。



第 18 章

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

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。

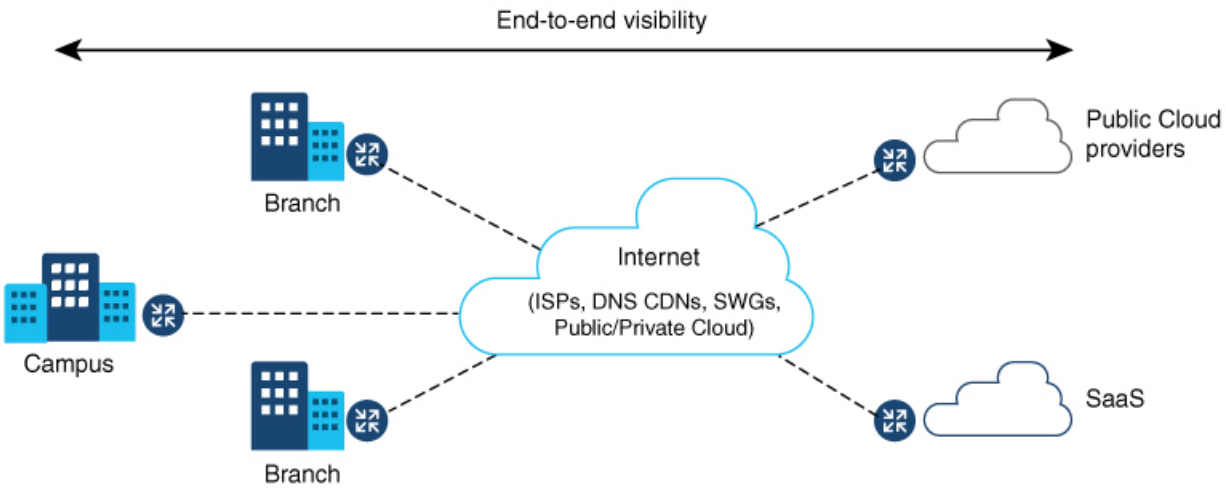
Cisco ThousandEyes エンタープライズ エージェント アプリケーションのホスティング

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。

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 8500 シリーズ セキュア ルータに展開できます。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 *2 : ThousandEyes* アプリケーションによるネットワークの表示



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 *19 : 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 17.15.4a	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。

プラットフォーム	ブートフラッシュ	DRAM
C8570-G2	480 GB NVMe SSD	32 GB デフォルト（DIMM X 2）は合計 64 GB にアップグレード可能
C8550-G2	480 GB NVMe SSD	32 GB デフォルト（DIMM X 2）は合計 64 GB にアップグレード可能

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。

手順

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 5.1 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。

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認証し、正しい Cisco ThousandEyes アカウントにチェックインします。トークンが無効であることを示すメッ

セージが表示されます。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 （160 ページ） 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。

手順

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) 1.11.0.0     : 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 75.75.75.75 □ 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 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 □ if image is locally available in bootflash:
          harddisk:   Package path □ 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。

手順

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。

手順

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。

手順

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。

手順

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. 次のパス */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. 次のパス */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。

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。

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。