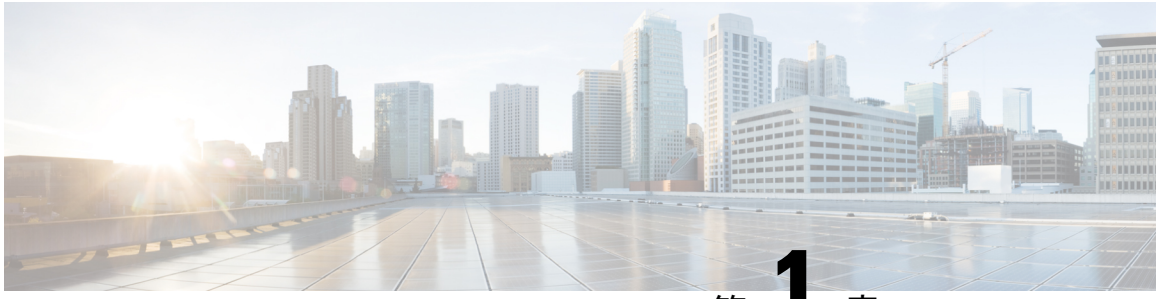
Cisco Catalyst 8500 および 8500L シリーズ エッジ プラットフォーム ソフトウェア コンフィギュレーション ガイド

最終更新：2024 年 10 月 15 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

はじめに

ここでは、このマニュアルの目的、構成、および関連製品やサービスに関する詳細の入手方法について説明します。

目標

このドキュメントでは、Cisco Catalyst 8500 シリーズエッジ（Cisco Catalyst 8500 プラットフォームおよび Cisco Catalyst 8500L シリーズ プラットフォームを含む）に固有のソフトウェア機能の概要について説明します。このマニュアルは、Cisco Catalyst 8500 シリーズ エッジ プラットフォームを使用して実行できるソフトウェア機能のすべてを説明する完全ガイドではなく、このプラットフォームに特化したソフトウェア機能だけを説明します。

Cisco Catalyst 8500 シリーズ エッジ プラットフォームでも使用できる一般的なソフトウェア機能については、その特定のソフトウェア機能の Cisco IOS XE テクノロジーガイドを参照してください。

マニュアルの変更履歴

次の変更履歴表は、このマニュアルにおける技術的な変更内容を記録したものです。この表には、変更に対応する Cisco IOS XE ソフトウェアのリリース番号とマニュアルのリビジョン番号、変更した日付、および変更点を示します。

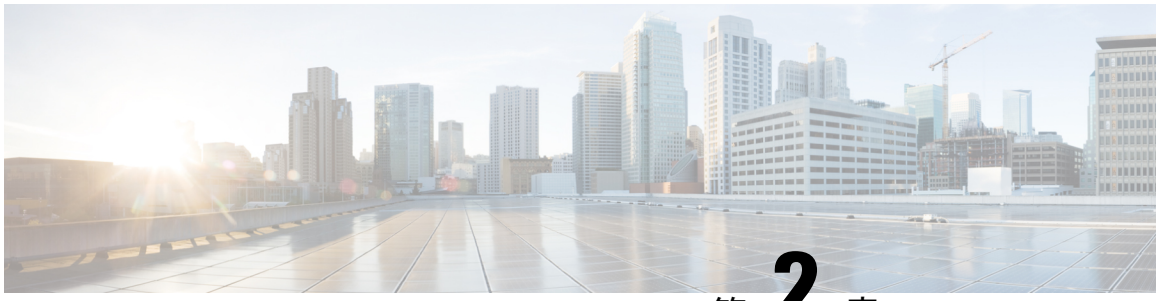
リリース番号	日付	変更点
IOS XE 17.4	2021 年 3 月 17 日	Cisco Catalyst 8500L シリーズ プラットフォームに関する情報が含まれています。
IOS XE 17.3.2	2020 年 10 月 22 日	マニュアルの初回リリース。

通信、サービス、およびその他の情報

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

シスコバグ検索ツール

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



第 2 章

最初にお読みください

機能情報

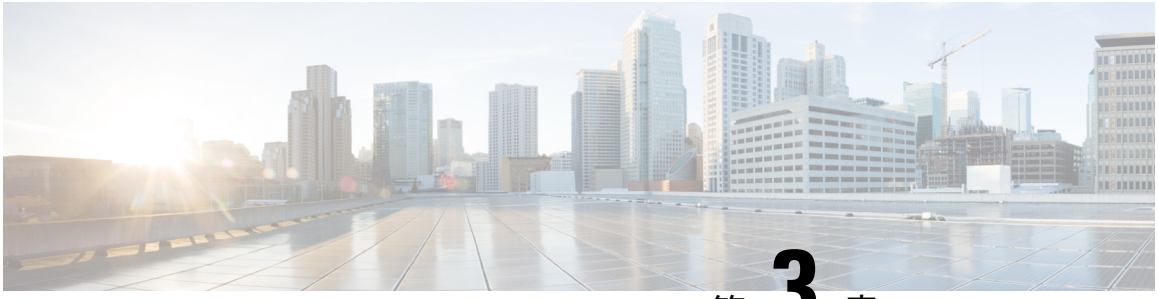
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- Cisco IOS コマンド リファレンス、全リリース

マニュアルの入手方法およびテクニカル サポート

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



第 3 章

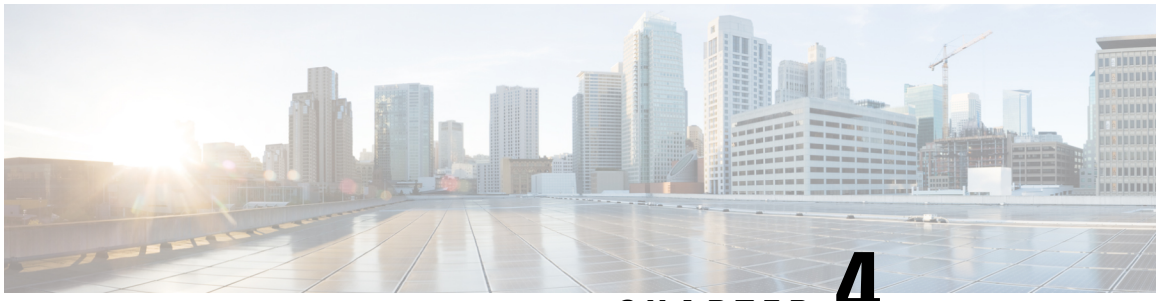
概要

Cisco 8500 シリーズ Catalyst エッジプラットフォームは、サービスパフォーマンス、ルータスループット、ルータスケールを低コストで大幅に向上させます。

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。

- Catalyst 8500 プラットフォーム（C8500-12X4QC、C8500-12X、および C8500-20X6C）
- Catalyst 8500L プラットフォーム（C8500L-8S4X）

機能	C8500-12X4QC	C8500-12X	C8500L-8S4X	C8500-20X6C
In-Service Software Upgrade（ISSU）のサポート	サポート対象外	サポート対象外	サポート対象外	サポート対象外
データプレーン処理	QFP 3.0	QFP 3.0	ソフトウェアベース	QFP 3.0
統合脅威防御（UTD）のサポート	サポート対象外	サポート対象外	サポートあり	サポート対象外
Fast Reroute（FRR）のサポート	サポート対象外	サポート対象外	サポート対象外	サポートあり



CHAPTER 4

ソフトウェアの実装およびアーキテクチャ

Cisco Catalyst 8500 シリーズ エッジ プラットフォーム（Cisco Catalyst 8500 プラットフォームおよび Cisco Catalyst 8500L シリーズ プラットフォームを含む）では、新しいソフトウェア実装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 Catalyst 8500 シリーズ エッジ プラットフォームでのソフトウェアの実装

この項では、次のトピックについて取り上げます。

Cisco Catalyst 8500 シリーズ エッジ プラットフォーム ソフトウェアの概要

Cisco Catalyst 8500 シリーズ エッジ プラットフォームは、サービスの高速化、マルチレイヤセキュリティ、クラウドネイティブの俊敏性、エッジでのインテリジェンスを実現し、クラウドへの移行を促進するために設計された、高性能のクラウド エッジ 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 Catalyst 8500 シリーズ エッジ プラットフォーム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

実行する場合の利点および欠点についての詳細情報は、「*Cisco Catalyst 8500* シリーズ エッジ プラットフォームの実行：概要」を参照してください。

統合パッケージについての重要事項

統合パッケージに関する重要な情報は次のとおりです。

- 各統合パッケージのバージョンが異なる場合でも、RPBase、RPControl、および ESPBase サブパッケージは統合パッケージ間では同一となります。
- RPIOS サブパッケージは、各統合パッケージのバージョンごとに内容がすべて異なります。
- 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利点および欠点についての詳細情報は、「*Cisco Catalyst 8500* シリーズ エッジ プラットフォームの実行：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。

統合パッケージに含まれる個別のソフトウェア サブパッケージ

このセクションでは、Cisco Catalyst 8500 シリーズ エッジ プラットフォームのサブパッケージと、各個別サブパッケージの目的について説明します。どの統合パッケージにも、これらの個別サブパッケージがすべて含まれます。特定の Cisco IOS XE Release に含まれる各個別サブパッケージの詳細については、そのリリースの『Cisco IOS XE Software Release Notes』を参照してください。

Table 1: 個別のサブパッケージ

サブパッケージ	目的
RPBase	ルート プロセッサ（RP）のオペレーティング システム ソフトウェアを提供します。
RPControl	IOS プロセスとプラットフォームの他の部分との間のインターフェイスとなるコントロール プレーンのプロセスを制御します。
RPAccess	セキュアソケットレイヤ（SSL）、セキュアシェル（SSH）、その他のセキュリティ機能など、制限付きコンポーネントの処理をエクスポートします。
RPIOS	Cisco IOS 機能が保存および実行される Cisco IOS カーネルを提供します。 各統合パッケージには、異なる RPIOS が含まれています。
ESPBase	ESP オペレーティング システム、制御プロセス、および ESP ソフトウェアを提供します。

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

Note 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 Catalyst 8500 シリーズ エッジ プラットフォーム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 Catalyst 8500 シリーズエッジプラットフォーム 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 Catalyst 8500 シリーズ エッジ プラットフォームを実行する場合は、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 Catalyst 8500 シリーズ エッジ プラットフォーム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

Cisco IOS XE Release 17.3.2 以降、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 Catalyst 8500 シリーズ エッジ プラットフォーム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 Catalyst 8500 シリーズ エッジ プラットフォームの 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 Catalyst 8500 シリーズ エッジ プラットフォーム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 Catalyst 8500 シリーズ エッジ プラットフォームでは、オペレーティングシステムの多数の役割を IOS プロセスから移行させる分散型ソフトウェアアーキテクチャを導入しています。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 Catalyst 8500 シリーズ エッジ プラットフォームでは、デュアル IOS プロセスを導入しているため、ハイアベイラビリティ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 Catalyst 8500 シリーズ エッジルータで有効にすることができます。Cisco Catalyst 8500 シリーズ エッジ プラットフォームでデュアルルートプロセッサを設定すると、2 番目の IOS プロセスがスタンバイルートプロセッサ上で稼働します。

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 Catalyst 8500 シリーズ エッジ プラットフォームのファイルシステム

次の表に、Cisco Catalyst 8500 シリーズ エッジ プラットフォーム上で確認できるファイルシステムのリストを示します。

Table 2: 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
harddisk:	アクティブ RP 上のハード ディスクのファイル システム
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
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[0-1]:	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

ここでは、Cisco Catalyst 8500 シリーズ エッジ プラットフォーム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 Catalyst 8500 シリーズ エッジ プラットフォームで自動生成されるファイルのリストと説明を示します。

Table 3: 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 ファイルは、bootflash: または harddisk: ファイル システムに作成される場合があります。 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。
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。

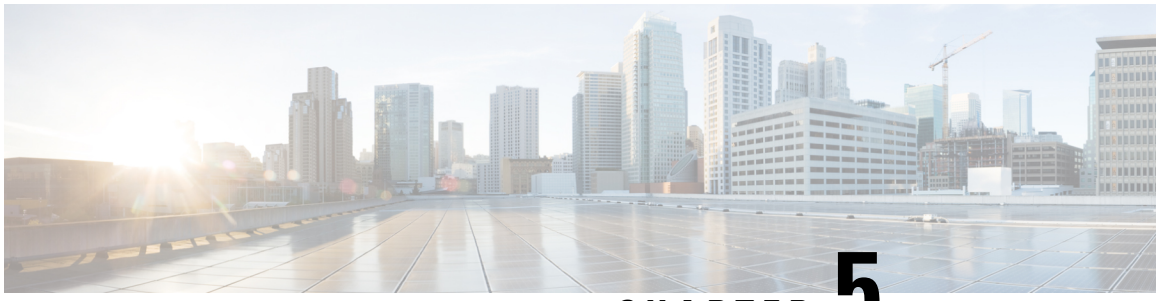
自動生成されるディレクトリに関する重要事項

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、harddisk: 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。



CHAPTER 5

IOS-XE と SDWAN の展開

概要

universalk9 イメージを使用して、Cisco IOS XE SD-WAN と Cisco IOS XE の両方を Cisco IOS XE デバイスに展開できます。これは SD-WAN と非 SD-WAN の両方の機能と展開のシームレスなアップグレードに役立ちます。

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。

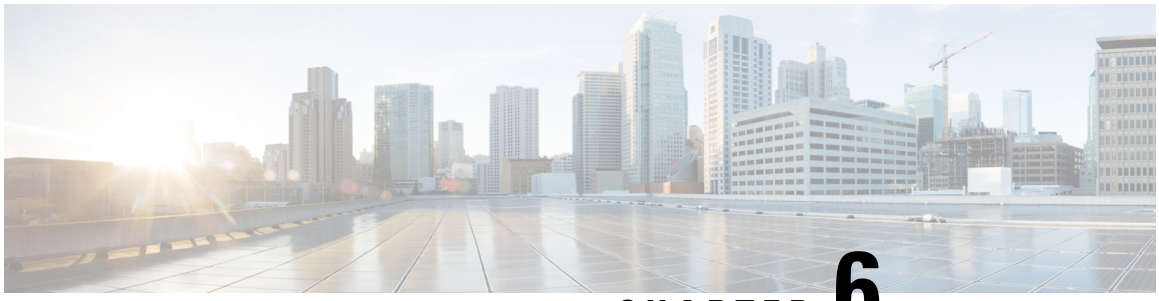
PnP 検出プロセス

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



CHAPTER 6

Cisco IOS XE ソフトウェアの使用

この章では、Cisco Catalyst 8500 シリーズ エッジ プラットフォーム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 にアクセスする方法

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 Catalyst 8500 シリーズ エッジ プラットフォーム上のコンソール ポートは、EIA/TIA-232 非同期、フロー制御なしのシリアル接続で、コネクタは RJ-45 コネクタを使用します。コンソール ポートは、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。

SUMMARY STEPS

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。

DETAILED STEPS

Procedure

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方法

Cisco Catalyst 8500 シリーズエッジプラットフォームのすべての RP には、コンソールインターフェイスがあります。デュアル RP 構成のアクティブ RP だけではなく、スタンバイ RP にもコンソール ポートを使用してアクセスできます。

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。

SUMMARY STEPS

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。

DETAILED STEPS

Procedure

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。

Example:

```
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。

Example:

```
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。

Example:

```
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。

Example:

```
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。

Example:

```
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。

Example:

```
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。

Note 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。

SUMMARY STEPS

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。

DETAILED STEPS

Procedure

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。

Note 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。

Example:

```
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。

Example:

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

Note 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。

Example:

```
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。

Example:

```
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。

Example:

```
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。

Example:

```
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。

Table 4: 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。

Table 5: 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。

Table 6: 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。

Table 7: 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。

Table 8: コマンド オプションの検索

コマンド	コメント

`Router> enable`
`Password: <password>`
`Router#`
	enable コマンドとパスワードを入力して、特権 EXEC コマンドにアクセスします。プロンプトが「>」から「#」に変わったら（例：Router> から Router#）、特権 EXEC モードに切り替わっています。

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

コマンド	コメント
Router(config)# **interface serial ?** <0-6> Serial interface number Router(config)# **interface serial 4 ?** / Router(config)# **interface serial 4/ ?** <0-3> Serial interface number Router(config)# **interface serial 4/0 ?** <cr> Router(config)# **interface serial 4/0** Router(config-if)#	**interface serial** 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、設定するシリアルインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 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、シリアル 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。

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)#
	シリアル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 Catalyst 8500 シリーズ エッジ プラットフォームでは、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 Catalyst 8500 シリーズ エッジ プラットフォームに固有ではなく、いくつかの Cisco 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。

コアの動的割り当て

Cisco Catalyst 8500L シリーズ プラットフォームでの動的コア割り当てにより、ユーザーはさまざまなサービスや CEF/IPSec のパフォーマンスに CPU コアを柔軟に活用できます。Cisco Catalyst 8500L シリーズ プラットフォームには、12 個の CPU コアが搭載されており、データプレーンからサービスプレーンにコアを柔軟に割り当てることができます。このコア割り当ては、これらのプラットフォームで使用可能なさまざまなサービスのお客様による設定に基づいています。

Cisco IOS XE リリース 17.4 以降は、**platform resource { service-plane-heavy | data-plane-heavy }**コマンドを使用して、サービスプレーンとデータプレーンの間でコアを調整します。ただし、設定したプロファイルを有効にするには、デバイスを再起動する必要があります。

```
Router(config)# platform resource { service-plane-heavy | data-plane-heavy }
```

（注） デフォルトでは、デバイス起動時のモードは service-plane-heavy です。

次の show コマンド出力は、データプレーンへの CPU コア割り当てを示しています。

```
Router# show platform software cpu allocation
CPU alloc information:

  Control plane cpu alloc: 0-1,12-13

  Data plane cpu alloc: 2-11

  Service plane cpu alloc: 0

  Template used: CLI-data_plane_heavy
```

（注） 上記の例で、データプレーンコア割り当ての最大数は 12 です。

次の show コマンド出力は、サービスプレーンへの CPU コア割り当てを示しています。

```
Router# show platform software cpu allocation

CPU alloc information:
  Control plane cpu alloc: 0-1,12-13

  Data plane cpu alloc: 6-11

  Service plane cpu alloc: 2-5,14-17

  Template used: CLI-service_plane_heavy
```

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。

```
13RU#sh run | inc usb
platform usb disable
13RU#
```

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...
Calculating the ROMMON CRC...CRC is correct.
```

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

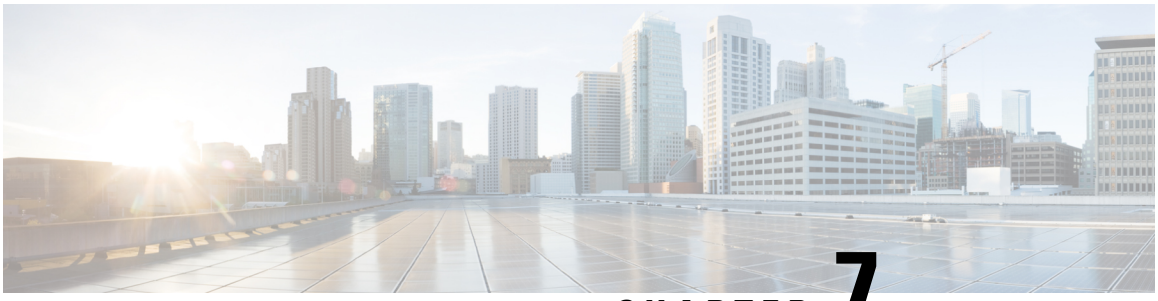
このツールにアクセスするには、Cisco.com の登録ユーザである必要があります。

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。



CHAPTER 7

ベイ構成

ベイ構成 C8500-12X4QC

C8500-12X4QC 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 0/0/8

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 0/1/2 0/1/3
ベイ 2 3xQSFP	40/100G EPA	3 つの 40G インターフェイス （0/1/0 ～ 0/1/2） 1 つの 100G インターフェイス（0/0/0） （0/0/0）	0/0/0 0/1/0 0/1/1 0/1/2

Note 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、C8500-12X4QC 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: C8500-12X4QC

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C8500-12X4QC        ok                    1w3d
 0/0      BUILTIN-8x1/10G     ok                    1w3d
 0/1      BUILTIN-100/40/4x10Gok                    00:04:53
 0/2      BUILTIN-100G/3X40G  ok                    00:08:16
R0        C8500-12X4QC        ok                    1w3d
 R0/0                         ok, active            1w3d
 R0/1                         ok, standby           1w3d
F0        C8500-12X4QC        ok, active            1w3d
P0        AIR-AC-750W-R       ok                    1w3d
P1        AIR-AC-750W-R       ps, fail              1w3d
P2        C8500-FAN-1R        ok                    1w3d

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         19020715            12.2(20181120:104547) [user-gd_secur...
R0        19020715            12.2(20181120:104547) [user-gd_secur...
F0        19020715            12.2(20181120:104547) [user-gd_secur...
```

```
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、C8500-12X4QC 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、C8500-12X4QC 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]

The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
```

```
The "[no] negotiation auto" command will have no effect with this interface
*Oct 29 17:58:10.020 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be
lost
*Oct 29 17:58:10.028 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 17:58:10.028 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 17:58:10.028 IST: BUILTIN-100/40/4x10G[0/1] : TenGigabitEthernet0/1/0 moved to
default config
*Oct 29 17:58:10.028 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 1 would be
lost
*Oct 29 17:58:10.035 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 17:58:10.036 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 17:58:10.036 IST: BUILTIN-100/40/4x10G[0/1] : TenGigabitEthernet0/1/1 moved to
default config
*Oct 29 17:58:10.036 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 2 would be
lost
*Oct 29 17:58:10.043 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 17:58:10.043 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 17:58:10.043 IST: BUILTIN-100/40/4x10G[0/1] : TenGigabitEthernet0/1/2 moved to
default config
*Oct 29 17:58:10.043 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 3 would be
lost
*Oct 29 17:58:10.050 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 17:58:10.050 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 17:58:10.050 IST: BUILTIN-100/40/4x10G[0/1] : TenGigabitEthernet0/1/3 moved to
default config
*Oct 29 17:58:11.050 IST: BUILTIN-100/40/4x10G[0/1] : Received mode change request from
 10G to 40G! system_configured TRUE
*Oct 29 17:58:11.057 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(BUILTIN-100/40/4x10G) reloaded
 on subslot 0/1
*Oct 29 17:58:11.057 IST: BUILTIN-100/40/4x10G[0/1] : EPA moving from 10G mode to 40G
mode
*Oct 29 17:58:11.057 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be
lost
*Oct 29 17:58:11.058 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 1 would be
lost
*Oct 29 17:58:11.059 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 2 would be
lost
*Oct 29 17:58:11.059 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 3 would be
lost
*Oct 29 17:58:11.060 IST: BUILTIN-100/40/4x10G[0/1] : Old mode cleanup done!
*Oct 29 17:58:11.061 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-100/40/4x10G) offline in
 subslot 0/1
*Oct 29 17:58:16.297 IST: BUILTIN-100/40/4x10G[0/1] : Number of ports 1
*Oct 29 17:58:16.298 IST: BUILTIN-100/40/4x10G[0/1] : XCVR namestring create: Maximum
number of XCVR = 1
```

次の例は、C8500-12X4QC 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
Changing mode of subslot 0/1 to 100G will cause EPA in subslot 0/0 to go offline
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]

*Oct 29 18:09:01.360 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be
lost
```

```
*Oct 29 18:09:01.368 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:01.368 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
The "[no] negotiation auto" command will have no effect with this interface
*Oct 29 18:09:01.368 IST: BUILTIN-100/40/4x10G[0/1] : FortyGigabitEthernet0/1/0 moved
to default config
*Oct 29 18:09:02.368 IST: BUILTIN-8x1/10G[0/0] : config for spa port 0 would be lost
*Oct 29 18:09:02.375 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.376 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.376 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/0 moved to default
 config
*Oct 29 18:09:02.376 IST: BUILTIN-8x1/10G[0/0] : config for spa port 1 would be lost
*Oct 29 18:09:02.382 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.382 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.382 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/1 moved to default
 config
*Oct 29 18:09:02.382 IST: BUILTIN-8x1/10G[0/0] : config for spa port 2 would be lost
*Oct 29 18:09:02.389 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.389 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.389 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/2 moved to default
 config
*Oct 29 18:09:02.389 IST: BUILTIN-8x1/10G[0/0] : config for spa port 3 would be lost
*Oct 29 18:09:02.395 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.395 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.395 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/3 moved to default
 config
*Oct 29 18:09:02.395 IST: BUILTIN-8x1/10G[0/0] : config for spa port 4 would be lost
*Oct 29 18:09:02.402 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.402 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.402 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/4 moved to default
 config
*Oct 29 18:09:02.402 IST: BUILTIN-8x1/10G[0/0] : config for spa port 5 would be lost
*Oct 29 18:09:02.409 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.409 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.409 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/5 moved to default
 config
*Oct 29 18:09:02.409 IST: BUILTIN-8x1/10G[0/0] : config for spa port 6 would be lost
*Oct 29 18:09:02.415 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.415 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.415 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/6 moved to default
 config
*Oct 29 18:09:02.415 IST: BUILTIN-8x1/10G[0/0] : config for spa port 7 would be lost
```

```
*Oct 29 18:09:02.422 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.422 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:09:02.422 IST: BUILTIN-8x1/10G[0/0] : TenGigabitEthernet0/0/7 moved to default
 config
*Oct 29 18:09:03.423 IST: BUILTIN-100/40/4x10G[0/1] : Received mode change request from
 40G to 100G! system_configured TRUE
*Oct 29 18:09:03.433 IST: BUILTIN-8x1/10G[0/0] : config for spa port 0 would be lost
*Oct 29 18:09:03.434 IST: BUILTIN-8x1/10G[0/0] : config for spa port 1 would be lost
*Oct 29 18:09:03.435 IST: BUILTIN-8x1/10G[0/0] : config for spa port 2 would be lost
*Oct 29 18:09:03.435 IST: BUILTIN-8x1/10G[0/0] : config for spa port 3 would be lost
*Oct 29 18:09:03.436 IST: BUILTIN-8x1/10G[0/0] : config for spa port 4 would be lost
*Oct 29 18:09:03.437 IST: BUILTIN-8x1/10G[0/0] : config for spa port 5 would be lost
*Oct 29 18:09:03.437 IST: BUILTIN-8x1/10G[0/0] : config for spa port 6 would be lost
*Oct 29 18:09:03.438 IST: BUILTIN-8x1/10G[0/0] : config for spa port 7 would be lost
*Oct 29 18:09:03.439 IST: BUILTIN-8x1/10G[0/0] : Old mode cleanup done!
*Oct 29 18:09:03.440 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-8x1/10G) offline in subslot
 0/0
*Oct 29 18:09:03.445 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(BUILTIN-100/40/4x10G) reloaded
 on subslot 0/1
*Oct 29 18:09:03.445 IST: BUILTIN-100/40/4x10G[0/1] : EPA moving from 40G mode to 100G
mode
*Oct 29 18:09:03.445 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be
lost
*Oct 29 18:09:03.446 IST: BUILTIN-100/40/4x10G[0/1] : Old mode cleanup done!
*Oct 29 18:09:03.446 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-100/40/4x10G) offline in
 subslot 0/1
*Oct 29 18:09:08.790 IST: BUILTIN-100/40/4x10G[0/1] : Number of ports 1
*Oct 29 18:09:08.792 IST: BUILTIN-100/40/4x10G[0/1] : XCVR namestring create: Maximum
number of XCVR = 1
Router(config)#
*Oct 29 18:09:15.552 IST: %SPA_OIR-6-ONLINECARD: SPA (BUILTIN-100/40/4x10G) online in
subslot 0/1
```

次の例は、C8500-12X4QC 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]
*Oct 29 18:14:36.484 IST: %PLATFORM_SCC-1-AUTHENTICATION_FAIL: Chassis authentication
failed

*Oct 29 18:14:38.219 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be
lost
*Oct 29 18:14:38.227 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:14:38.227 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:14:38.227 IST: BUILTIN-100/40/4x10G[0/1] : HundredGigE0/1/0 moved to default
 config
*Oct 29 18:14:39.228 IST: BUILTIN-100/40/4x10G[0/1] : Received mode change request from
 100G to 10G! system_configured TRUE
*Oct 29 18:14:39.230 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(BUILTIN-100/40/4x10G) reloaded
 on subslot 0/1
*Oct 29 18:14:39.230 IST: BUILTIN-100/40/4x10G[0/1] : EPA moving from 100G mode to 10G
mode
*Oct 29 18:14:39.230 IST: BUILTIN-100/40/4x10G[0/1] : config for spa port 0 would be
lost
*Oct 29 18:14:39.231 IST: BUILTIN-100/40/4x10G[0/1] : Old mode cleanup done!
*Oct 29 18:14:39.232 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-100/40/4x10G) offline in
 subslot 0/1
*Oct 29 18:14:44.472 IST: BUILTIN-100/40/4x10G[0/1] : Number of ports 4
```

```
*Oct 29 18:14:44.475 IST: BUILTIN-100/40/4x10G[0/1] : XCVR namestring create: Maximum
number of XCVR = 4
*Oct 29 18:15:03.336 IST: %SPA_OIR-6-ONLINECARD: SPA (BUILTIN-100/40/4x10G) online in
subslot 0/1
```

次の例は、C8500-12X4QC 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]

*Oct 29 18:17:03.394 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 0 would be lost
*Oct 29 18:17:03.401 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:17:03.401 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:17:03.401 IST: BUILTIN-100G/3X40G[0/2] : FortyGigabitEthernet0/2/0 moved to
default config
*Oct 29 18:17:03.401 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 1 would be lost
*Oct 29 18:17:03.406 IST: BUILTIN-100G/3X40G[0/2] : Breakout XCVR type QSFP 4X10G AC7M
(546) is not allowed as XCVR port Fortyrnet0/2/0 is not configured in breakout
*Oct 29 18:17:03.406 IST: %IOSXE_EPA-3-XCVR_PROHIBIT: Transceiver is prohibited to come
 online for interface FortyGigabitEther
*Oct 29 18:17:03.407 IST: BUILTIN-100G/3X40G[0/2] : XCVR prohibited on port
FortyGigabitEthernet0/2/0, epa_name=BUILTIN-100G/3=FortyGigabitEthernet0/2/0,
xcvr_speed=40000000, admin_state=UNSHUT xcvr_type=546

*Oct 29 18:17:03.409 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:17:03.409 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:17:03.409 IST: BUILTIN-100G/3X40G[0/2] : FortyGigabitEthernet0/2/4 moved to
default config
*Oct 29 18:17:03.409 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 2 would be lost
*Oct 29 18:17:03.417 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:17:03.417 IST: %SYS-5-CONFIG_P: Configured programmatically by process Exec
from console as console
*Oct 29 18:17:03.417 IST: BUILTIN-100G/3X40G[0/2] : FortyGigabitEthernet0/2/8 moved to
default config
*Oct 29 18:17:03.423 IST: BUILTIN-100G/3X40G[0/2] : Breakout XCVR type QSFP 4SFP10G CU4M
 (541) is not allowed as XCVR port Forhernet0/2/4 is not configured in breakout
*Oct 29 18:17:03.423 IST: %IOSXE_EPA-3-XCVR_PROHIBIT: Transceiver is prohibited to come
 online for interface FortyGigabitEther
*Oct 29 18:17:03.423 IST: BUILTIN-100G/3X40G[0/2] : XCVR prohibited on port
FortyGigabitEthernet0/2/4, epa_name=BUILTIN-100G/3=FortyGigabitEthernet0/2/4,
xcvr_speed=40000000, admin_state=UNSHUT xcvr_type=541

*Oct 29 18:17:04.418 IST: BUILTIN-100G/3X40G[0/2] : Received mode change request from
40G to 100G! system_configured TRUE
*Oct 29 18:17:04.423 IST: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(BUILTIN-100G/3X40G) reloaded
 on subslot 0/2
*Oct 29 18:17:04.423 IST: BUILTIN-100G/3X40G[0/2] : EPA moving from 40G mode to 100G
mode
*Oct 29 18:17:04.423 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 0 would be lost
*Oct 29 18:17:04.424 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 1 would be lost
*Oct 29 18:17:04.425 IST: BUILTIN-100G/3X40G[0/2] : config for spa port 2 would be lost
*Oct 29 18:17:04.425 IST: BUILTIN-100G/3X40G[0/2] : Old mode cleanup done!
*Oct 29 18:17:04.426 IST: %SPA_OIR-6-OFFLINECARD: SPA (BUILTIN-100G/3X40G) offline in
subslot 0/2
*Oct 29 18:17:09.685 IST: BUILTIN-100G/3X40G[0/2] : Number of ports 1
*Oct 29 18:17:09.686 IST: BUILTIN-100G/3X40G[0/2] : XCVR namestring create: Maximum
number of XCVR = 1
```

```
Router(config)#
Router(config)#
*Oct 29 18:17:16.017 IST: %SPA_OIR-6-ONLINECARD: SPA (BUILTIN-100G/3X40G) 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。Cisco IOS XE 17.4 以降、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 C8500-12X4QC 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。

Note ブレークアウトサポートは、C8500-12X4QC でのみサポートされます（C8500-20X6C ではサポートされません）。

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。

Table 9: 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
	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	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

Note 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
```

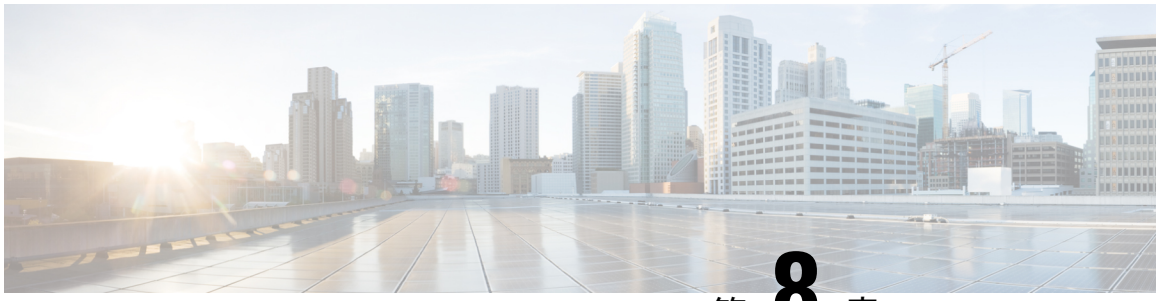
ベイ構成 C8500-12X

C8500-12X4 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。

ベイ構成 C8500-20X6C

C8500-20X6C には、設定可能な 2 つの組み込み EPA があります。

ベイ番号	EPA	ポート設定	インターフェイス番号
ベイ 0 20xSFP+	1/10G EPA	20 個の 1G インターフェイス 20 個の 10G インターフェイス 20 個の 1/10G インターフェイス	0/0/0 0/0/1 0/0/2 0/0/3 0/0/4 0/0/5 0/0/6 0/0/7 0/0/8 0/0/9 0/0/10 0/0/11 0/0/12 0/0/13 0/0/14 0/0/15 0/0/16 0/0/17 0/0/18 0/0/19
ベイ 1 6xQSFP+	40/100G EPA	6 個の 40/100G インターフェイスがアクティブ ベイは次のモードで使用できます。 • 6 個の 40G インターフェイス 6 個の 100G インターフェイス • 6 個の 40/100G インターフェイス	0/1/0 0/1/1 0/1/2 0/1/3 0/1/4 0/1/5



第 8 章

ライセンスとライセンスモデル

この章では、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで使用可能なライセンス、サポートされているスループットのオプション、および使用可能なライセンスとスループットを設定する方法について説明します。また、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで使用可能なライセンスモデルについても説明します。

（注） この章の情報は、主に自律モードで動作するデバイスに適用されます。比較と完全性を期すために、特定のセクションにはコントローラモードへの参照が含まれています。情報がコントローラモードに適用される場合、その旨が明確に示されています。

シスコのライセンスの詳細については、https://cisco.com/go/licensingguide を参照してください。

この章の主な内容は、次のとおりです。

使用可能なライセンスとライセンスモデルの機能情報

次の表に、Cisco Catalyst 8000 エッジ プラットフォーム ファミリに適用されるライセンス関連の変更の概要を示します。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。

Table 10: 使用可能なライセンスとライセンスモデルの機能情報

機能名	リリース	機能情報
自律モードでの Tier 1 および 250 Mbps スループット設定の 500 Mbps 集約	Cisco IOS XE 17.14.1a	仮想プラットフォームでは、250 Mbps または T1 のスループットを設定すると、HSECK9 ライセンスがデバイスで使用可能な場合、スループットは 500 Mbps の送信（Tx）データのみに制限されます。以前のリリースでは、スループットは 200 Mbps Tx に制限されていました。 物理プラットフォームでは、250 Mbps または T1 のスループットを設定すると、HSECK9 ライセンスがデバイスで使用可能な場合、総スループットのスロットリングが有効になります。スループットは 500 Mbps に制限され、アップストリームおよびダウンストリーム方向のトラフィックの分散が許可されます。以前のリリースでは、双方向スループットスロットリングは T1 および 250 Mbps に適用され、スループットは各方向で 250 Mbps に制限されていました。 スロットリング動作のリリースごとの変更, on page 62を参照してください。
総スループットのスロットリング - 仮想プラットフォーム	Cisco IOS XE Cupertino 17.9.1a	Cisco Catalyst 8000 エッジ プラットフォーム ファミリの仮想プラットフォームでは、すべてのスループットレベルで、デバイスに双方向スループット値を設定すると、総スループットのスロットリングが有効になります。 この機能拡張は、仮想プラットフォームに常に適用されていたスロットリング動作を変更しません。スロットリングは、送信されるデータ（Tx）にのみ適用されます。受信したデータ（Rx）はスロットリングされません。 スループット , on page 59および数値および階層ベースのスループット, on page 59を参照してください。

機能名	リリース	機能情報
総スループットのスロットリング - 物理プラットフォーム	Cisco IOS XE Cupertino 17.8.1a	Cisco Catalyst 8000 エッジ プラットフォーム ファミリの物理プラットフォームでは、スループットレベルが 250 Mbps を超え、階層 2 以上の階層で、デバイスに双方向スループット値を設定すると、総スループットのスロットリングが有効になります。これは、アップストリームおよびダウンストリーム方向のトラフィックの分布に関係なく、トラフィックが集約的にスロットルされることを意味します。 双方向スループットは、ライセンス PID で表されます（たとえば、Cisco DNA-C-**500M**-E-3Y および Cisco DNA-C-**T2**-E-3Y）。総スループットは双方向スループットの 2 倍です。 スロットリング動作のリリースごとの変更, on page 62を参照してください。
階層ベース ライセンス	Cisco IOS XE Cupertino 17.7.1a	既存の帯域幅ベースの（数値）スループットの設定に加えて、階層ベースのスループット設定のサポートが導入されました。 最も低いスループットレベルから始めて、使用可能な階層は階層 0（T0）、階層 1（T1）、階層 2（T2）、階層 3（T3）です。それぞれの階層はスループットレベルを表します。 製品のライセンス PID が階層ベースの場合、ライセンスは CSSM Web UI の階層値とともに表示されます。 階層ベースのライセンスを持つ製品の場合、階層ベースのスループット値を設定でき、階層ベースのスループット値に変換することもできます。 スループット , on page 59および数値および階層ベースのスループット, on page 59を参照してください。

機能名	リリース	機能情報
Cisco Digital Network Architecture（Cisco DNA）ライセンス	Cisco IOS XE Amsterdam 17.3.2	Cisco DNA ライセンスのサポートは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで導入されました。 Cisco DNA ライセンスは、ネットワーク スタック ライセンスと DNA スタックアドオンライセンスに分類されます。 Cisco DNA ライセンス, on page 53を参照してください。
高セキュリティライセンス（HSECK9）	Cisco IOS XE Amsterdam 17.3.2	HSECK9 ライセンスのサポートは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで導入されました。 高セキュリティライセンス , on page 55を参照してください。
Cisco Unified Border Element ライセンス（Cisco UBE ライセンス） Cisco Unified Communications Manager Express ライセンス（Cisco Unified CME ライセンス） Cisco Unified Survivable Remote Site Telephony ライセンス（Cisco Unified SRST ライセンス）	Cisco IOS XE Amsterdam 17.3.2	Cisco UBE、Cisco Unified CME、Cisco Unified SRST ライセンスのサポートは Cisco Catalyst 8000 エッジプラットフォーム ファミリで導入されました Cisco CUBE ライセンス, on page 58、Cisco Unified CME ライセンス, on page 58、および Cisco Unified SRST ライセンス, on page 58を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、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。

入手可能なライセンス

このセクションでは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで使用可能なすべてのライセンス、使用ガイドライン、および注文に関する考慮事項について説明します。

Cisco DNA ライセンス

Cisco Digital Network Architecture（Cisco DNA）ソフトウェアライセンスは、いくつかの機能固有のライセンスを組み合わせたものです。

（注） Cisco DNA ライセンスには、次を除くすべての機能ライセンスが含まれています。高セキュリティ（HSECK9）、Cisco Unified Border Element（Cisco UBE）、Cisco Unified Communications Manager Express（Cisco Unified CME）、および Cisco Unified Survivable Remote Site Telephony（Cisco Unified SRST）。『Cisco DNA ライセンスの発注時の考慮事項 （54 ページ）』を参照してください。

Cisco DNA ライセンスは、ネットワーク スタック ライセンスと DNA スタックアドオンライセンスに分類されます。

Catalyst 8000V エッジソフトウェア、Catalyst 8200、および 8300 シリーズ エッジ プラットフォームで使用可能な Cisco DNA ライセンス：

ネットワークスタック ライセンス：

- Network Essentials
- Network Advantage：Network Essentials で使用可能な機能などが含まれます。
- Network Premier：Network Essentials、Network Advantage で使用可能な機能などが含まれます。

Cisco DNA スタックアドオンライセンス：

- Cisco DNA Essentials：Network Essentials でのみ使用可能なアドオンライセンス。
- Cisco DNA Advantage：Network Advantage でのみ使用可能なアドオンライセンス。Cisco DNA Essentials で使用可能な機能などが含まれます。
- Cisco DNA Premier：Network Premier でのみ使用可能なアドオンライセンス。Cisco DNA Essentials、Cisco DNA Advantage で使用可能な機能などが含まれます。

Catalyst 8500 シリーズ エッジ プラットフォームで使用可能な Cisco DNA ライセンス：

ネットワークスタック ライセンス：

- Network Advantage
- Network Premier：Network Advantage で使用可能な機能などが含まれます。

Cisco DNA スタックアドオンライセンス：

- Cisco DNA Advantage
- Cisco DNA Premier：Network Premier でのみ使用可能なアドオンライセンス。Cisco DNA Advantage で使用可能な機能などが含まれます。

Cisco DNA ライセンスの使用に関するガイドライン

- Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべてのプラットフォームに適用されるガイドライン：
  - ネットワークスタック ライセンスは恒久的つまり永久ライセンスであり、有効期限はありません。
  - Cisco DNA スタックアドオンライセンスは、サブスクリプションつまり期限付きライセンスであり、特定の日付までのみ有効です。3 年間および 5 年間のオプションは、すべての Cisco DNA スタックアドオンライセンスで使用できます。特定の Cisco DNA スタックアドオンライセンスでは、7 年間のサブスクリプションのオプションを使用できます。
  - Tier 3（T3）以上の階層は、Network Essentials および Cisco DNA Essentials ライセンスではサポートされていません。

    これは、T3 以上の階層をスループットとして設定している場合、ブートレベルライセンスを Network Essentials および Cisco DNA Essentials に変更できないことも意味します。

    Cisco DNA ライセンスで使用可能なさまざまな階層の詳細については、階層および数値のスループットのマッピング （63 ページ）を参照してください。

- Catalyst 8000V エッジソフトウェアにのみ適用されるガイドライン：

  Catalyst 8000V エッジソフトウェアでは、ネットワークスタック ライセンスを設定するときに、対応する Cisco DNA スタックアドオンライセンスも設定する必要があります。

- Catalyst 8200、8300、8500 シリーズ エッジプラットフォームにのみ適用されるガイドライン：
  - 各 ネットワークスタック ライセンスで使用できる Cisco DNA スタックアドオンライセンスはオプションです。Cisco DNA スタックアドオンライセンスなしでネットワークスタック ライセンスを設定できますが、対応するネットワークスタック ライセンスなしで Cisco DNA スタックアドオンライセンスを設定することはできません。
  - Cisco DNA スタックアドオンライセンスを使用する場合は、有効期限が切れる前にライセンスを更新して引き続き使用するか、Cisco DNA スタックアドオンライセンスを非アクティブ化してからデバイスをリロードしてネットワークスタック ライセンス機能での運用を継続します。

Cisco DNA ライセンスの発注時の考慮事項

Cisco DNA ライセンスには、すべてのパフォーマンス、ブースト、およびテクノロジー パッケージ ライセンス（securityk9、uck9、および appxk9）が含まれます。つまり、Cisco DNA ネットワーク スタック ライセンスまたは Cisco DNA スタックアドオンライセンスを注文する際に、パフォーマンス、ブースト、およびテクノロジーパッケージのライセンスが必要であるか適用される場合、注文に自動的に追加されます。

購入するライセンス製品 ID（PID）は、Cisco DNA スタックアドオンライセンス PID のみです。

新しいハードウェアと一緒にCisco DNAライセンスを注文した場合でも、ライセンスはデバイスに事前設定されていません。デバイスでブートレベルライセンスを設定してからスループットを設定する必要があります。

Cisco DNA ライセンスを注文する場合は、スループット値も指定します。注文するスループットが 250 Mbps を超える場合は、Catalyst 8500 および 8500L シリーズ エッジ プラットフォームを除く、Cisco Catalyst 8000 エッジプラットフォーム ファミリのすべてのバリアントでHSECK9ライセンスが必要です。詳細については、「高セキュリティライセンス （55 ページ）」を参照してください。

階層ベースのスループット値が T1 のライセンス PID を注文すると、HSECK9 ライセンスが自動的に注文に追加されます。

高セキュリティライセンス

高セキュリティライセンス（HSECK9ライセンス）は輸出規制ライセンスであり、米国の輸出管理法によって制限されています。このライセンスは、完全な暗号化機能、つまり 250 Mbps を超えるスループット、および一定数以上のトンネル数を使用するために必要です（次の表を参照）。この要件は、Catalyst 8500 および 8500L シリーズ エッジ プラットフォームを除く Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべてのデバイスに適用されます。

Catalyst 8500 および 8500L シリーズ エッジ プラットフォームでのみ、スループットとトンネルの規模は、HSECK9 ライセンスが利用できないことによる影響を受けません。これらのプラットフォームでは、HSECK9 ライセンスはコンプライアンスの目的でのみ必要です。Cisco Catalyst 8000 エッジ プラットフォーム ファミリの残りのすべてのモデルでは、HSECK9 ライセンスがない場合、サポートされるトンネル数とスループットが制限されます。次の表に、HSECK9 ライセンスなしでサポートされるトンネル数とサポートされるスループットを示します。

PID	HSECK9 ライセンスなしのトンネルの数	HSECK9 ライセンスなしでサポートされるスループット
C8000V	150	T0、T1
C8200-1N-4T	1000	T0、T1
C8200L-1N-4T	1000	T0、T1
C8300-1N1S-4T2X	1000	T0、T1
C8300-1N1S-6T	1000	T0、T1
C8300-2N2S-4T2X	1000	T0、T1

PID	HSECK9 ライセンスなしのトンネルの数	HSECK9 ライセンスなしでサポートされるスループット
C8300-2N2S-6T	1000	T0、T1
C8500-12X4QC	該当なし	該当なし
C8500-12X	該当なし	該当なし
C8500-20X6C	該当なし	該当なし
C8500L-8S4X	該当なし	該当なし

（注） 「スループット」という用語は、物理プラットフォームで暗号化されたスループットを指します。仮想プラットフォームでは、暗号化されたスループットと非暗号化スループットを組み合わせたものを指します。

HSECK9 ライセンスを使用すると、トンネル数の制限が解除され、250 Mbps を超えるスループットを設定することもできます。使用可能なスループットオプションの詳細については階層および数値のスループットのマッピング （63 ページ）を参照してください。

HSECK9 ライセンスがデバイスで使用されているかどうかを確認するには、特権 EXEC モードで **show license summary** コマンドを入力します。Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべてのデバイスで、HSECK9 ライセンスは次のように表示されます。Router US Export Lic. for DNA (DNA_HSEC)。次に例を示します。

```
Device# show license summary

Account Information:
  Smart Account: Eg-SA As of Dec 03 15:26:02 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-advantage_T2    (NWSTACK_T2_A)                    1 IN USE
  dna-advantage_T2        (DSTACK_T2_A)                     1 IN USE
  Router US Export Lic... (DNA_HSEC)                        1 IN USE
```

HSECK9 ライセンスの使用に関するガイドライン

HSECK9 ライセンスはシャーシに関連付けられています。そのため、暗号化機能を使用するシャーシ UDI ごとに 1 つの HSECK9 ライセンスが必要です。

HSECK9 ライセンスは、使用前に承認が必要です。この承認は、Smart Licensing Authorization Code（SLAC）によって提供されます。使用する HSECK9 ライセンスごとに SLAC をインストールする必要があります。SLAC は CSSM で生成され、CSSM から取得されます。CSSM か

らSLACを取得する方法は、実装したトポロジによって異なります。詳細については、「HSECK9 ライセンス用の SLAC のインストール （77 ページ）」を参照してください。

SLAC がインストールされているかどうかを確認するには、特権 EXEC モードで **show license authorization** コマンドを入力します。SLACがインストールされている場合、ステータスフィールドに「SMART AUTHORIZATION INSTALLED on <timestamp>」と表示されます。次に例を示します。

```
Device# show license authorization
Overall status:
  Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
       Status: SMART AUTHORIZATION INSTALLED on Dec 03 08:24:35 2021 UTC
       Last Confirmation code: 418b11b3

Authorizations:
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for DNA based Routers
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

HSECK9 ライセンスの発注時の考慮事項

Catalyst 8000 ハードウェア プラットフォームと同じ注文で Cisco DNA ライセンスを注文した場合、HSECK9 ライセンスを注文するオプションが使用可能であるか、該当する場合は選択されています。たとえば、Catalyst 8500 シリーズ エッジ プラットフォームの場合、ハードウェアを注文すると、HSECK9 ライセンスが自動的に注文に追加されます。これは、これらのプラットフォームでは 250 Mbps を超えるスループットのサポートが開始されるためです。さらに、HSECK9 ライセンスに必要な SLAC もデバイスに工場出荷時にインストールされています。

Catalyst 8000 ハードウェア プラットフォームとは別の注文で Cisco DNA ライセンスを注文する場合、必要に応じて、Catalyst 8000 ハードウェア プラットフォームの注文で HSECK9 ライセンスを別に注文する必要があります。

注文する新しいハードウェアで HSECK9 ライセンスを使用する予定の場合は、スマートアカウントとバーチャルアカウントの情報を注文時に提供します。これにより、シスコは工場出荷時に HSECK9 ライセンスの SLAC をハードウェアにインストールできます。デバイスの使用を開始する前に、デバイスのスループットを設定する必要があります。

（注） HSECK9 ライセンスを（ハードウェアの注文ではなく）個別に注文した場合、SLAC を工場でインストールすることはできません。

Cisco CUBE ライセンス

Cisco Unified Border Element ライセンス（Cisco UBE ライセンス）では、有効にする前にブートレベルを設定する必要はありません。購入後、設定ガイドを参照して、使用可能な Cisco UBE 機能を設定できます。

Cisco UBE ライセンスで使用できる機能については、次の場所にある必要なリリースの『Cisco Unified Border Element Configuration Guide』を参照してください。https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html

サポートされているプラットフォームおよび Cisco UBE ライセンスの購入については、https://www.cisco.com/c/ja_jp/products/collateral/unified-communications/unified-border-element/data-sheet-c78-729692.html のデータシートを参照してください。必要に応じて、Cisco UBE ライセンスを個別に注文する必要があります。他のライセンスには自動的には含まれません。

Cisco UBE ライセンスの使用状況をレポートする方法については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』を参照してください。このライセンスモデルのコンテキストでは、Cisco UBE ライセンスは非強制ライセンスです。

Cisco Unified CME ライセンス

Cisco Unified Communications Manager Express ライセンス（Cisco Unified CME ライセンス）では、有効にする前にブートレベルを設定する必要はありません。購入後、設定ガイドを参照して、使用可能な機能を設定できます。

Cisco Unified CME ライセンスで使用可能な機能については、『Cisco Unified Communications Manager Express System Administrator Guide』を参照してください。

サポートされているプラットフォームおよび Cisco Unified CME ライセンスの購入については、https://www.cisco.com/c/ja_jp/products/collateral/unified-communications/unified-communications-manager-express/datasheet-c78-744069.html のデータシートを参照してください。必要に応じて、Cisco Unified CME ライセンスを個別に注文する必要があります。他のライセンスには自動的には含まれません。

Cisco Unified CME ライセンスの使用状況をレポートする方法については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』を参照してください。このライセンスモデルのコンテキストでは、Cisco Unified CME ライセンスは非強制ライセンスです。

Cisco Unified SRST ライセンス

Cisco Unified Survivable Remote Site Telephony ライセンス（Cisco Unified SRST ライセンス）では、有効にする前にブートレベルを設定する必要はありません。購入後、設定ガイドを参照して、使用可能な Unified SRST 機能を設定できます。

Cisco Unified SRST ライセンスで使用可能な機能については、『Cisco Unified SCCP and SIP SRST System Administrator Guide (All Versions)』を参照してください。

サポートされているプラットフォームおよび Cisco Unified SRST ライセンスの購入については、https://www.cisco.com/c/ja_jp/products/collateral/unified-communications/unified-communications-manager-express/datasheet-c78-744069.html

のデータシートを参照してください。必要に応じて、Cisco Unified SRST ライセンスを個別に注文する必要があります。他のライセンスには自動的には含まれません。

Unified SRST ライセンスの使用状況をレポートする方法については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』を参照してください。このライセンスモデルのコンテキストでは、Unified SRST ライセンスは非強制ライセンスです。

スループット

スループットは、デバイスを介して転送できるデータの量を示します。この値は、自律モードで設定します。その後、設定されたレートでデータが送信（Tx）および受信（Rx）されます。

スループットを明示的に設定しない場合、デフォルトのスループットが有効になります。

デバイスの設定されたスループットを確認するには、該当するコマンドを入力します。

- 物理プラットフォームの場合、**show platform hardware throughput crypto** コマンドを特権 EXEC モードで入力します。
- 仮想プラットフォームの場合、**show platform hardware throughput level** コマンドを特権 EXEC モードで入力します。

次のセクションでは、スループット値の表示方法、デバイスのスループットが暗号化されたスループットと暗号化されていないスループットのどちらを指しているかとその意味、デバイスのスループットに制限を適用するかどうかとその方法について説明します。

数値および階層ベースのスループット

使用できるスループットは、デバイスの Cisco DNA ライセンス製品 ID（PID）で指定されます。これは、数値または階層で表すことができる値です。デバイスにも設定されているのと同じ値です。

数値スループット値

スループットが数値で表される場合、数値スループット値と呼ばれます。たとえば、Cisco DNA-C-**10M**-E-3Y は、10M（= 10 Mbps）の数値スループット値を持つライセンス PID です。

デバイスに応じて、他の使用可能な数値スループット値の例は、15M、25M、50M、100M、250M、500M、1G、2.5G、5G、10G などです。250 Mbps を超えるスループットには、HSECK9 ライセンスが必要です。

階層ベースのスループット値

スループットが階層によって表される場合、階層ベースのスループット値と呼ばれます。階層はスループットレベルを表し、数値スループット値にマッピングされます。たとえば、DNA-C-**T0**-E-3Y は、階層ベースのスループット値 T0 を持つライセンス PID です。これに相当するマッピングされる数値は、最大 25 Mbps のスループットです。

（注） 階層ベースのスループットの設定は、Cisco IOS XE Cupertino 17.7.1a 以降でサポートされます。このリリース以降、階層ベースのスループット設定は、デバイスでスループットを設定する方法としても推奨されます。

最も低いスループットレベルから始めて、使用可能な階層は階層 0（T0）、階層 1（T1）、階層 2（T2）、階層 3（T3）、階層 4（T4）、階層 5（T5）です。T2 以上の階層は、HSECK9 ライセンスが必要です。

階層については、次の点に注意してください。

- すべての階層が、すべての Cisco DNA ライセンスで利用できるわけではありません。

  たとえば、T3 以上の階層は Network Essentials および Cisco DNA-Essentials ライセンスでは使用できません。これは、設定されたスループットとして T3 がある場合、ブートレベルライセンスを Network Essentials および Cisco DNA Essentials に変更できないことも意味します。

- 各階層は、プラットフォームごとに異なる数値にマッピングされるか、異なる数値を意味します。

  Cisco Catalyst 8000 エッジ プラットフォーム ファミリの異なるプラットフォームは、異なる最大スループットレベルをサポートします。たとえば、T2 は、C8300-2N2S-4T2X の場合は 1G スループット、C8200-1N-4T の場合は 500M、C8200L-1N-4T の場合は 250M になります。

特定の Cisco DNA ライセンスで使用可能な階層を確認し、特定のプラットフォームの各階層に相当する数値を調べるには、この章の階層および数値のスループットのマッピング （63 ページ）のセクションを参照してください。

デバイス上で数値スループット値を設定するタイミングと、階層ベースのスループットを設定するタイミングについては、この章の数値と階層ベースのスループットの設定 （71 ページ）セクションを参照してください。

暗号化および非暗号化スループット

暗号化スループットは、暗号スループットとも呼ばれ、暗号化アルゴリズムによって保護されるスループットです。

一方、非暗号化スループットはプレーンテキストです。非暗号化スループットは、Cisco Express Forwarding（CEF）トラフィックとも呼ばれます。

重要 物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズエッジプラットフォーム）の場合、このドキュメントでの「スループット」とはすべて、暗号スループットを指します。

仮想プラットフォーム（Catalyst 8000V エッジソフトウェア）の場合、このドキュメントでの「スループット」とはすべて、暗号スループットと非暗号化スループットを組み合わせたものを指します。

スロットルされたスループットとスロットルされていないスループット

スロットルされたスループットは、制限が適用されているスループットです（スループット値を設定すると、設定された範囲までデバイスのスループットがスロットルされます）。

スロットルされていないスループットは、制限が適用されないことを意味し、デバイスのスループットはデバイスの最大能力になります。

（注） 仮想プラットフォームでは、スループットがスロットルされている場合、スロットルは送信データにのみ適用されます。受信データは常にスロットルされません。物理プラットフォームでは、スループットがスロットルされている場合、スロットルは送信および受信データに適用されます。

物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズエッジプラットフォーム）では、暗号化されていないスループット（送信および受信）はデフォルトでスロットルされません。

スロットリング動作のタイプ：集約および双方向

システムは、双方向の方法または集約的な方法でスロットリングを適用できます。

双方向スループットスロットリング

ここで、システムは各方向のデータをスロットルします。双方向スロットリングが有効な場合、送信データは双方向スループット値で制限され、受信データは双方向スループット値で個別に制限されます（仮想プラットフォームに常に適用される例外に注意してください。受信データはスロットリングされません）。

たとえば、双方向スループット値が 25 Mbps または T0 で、双方向スループット スロットリングが有効である場合は、次のようになります。

- 仮想プラットフォームでは、送信データの上限は 25 Mbps です。受信データはスロットリングされません。
- 物理プラットフォームでは、Tx データの上限は 25 Mbps、Rx データの上限は 25 Mbps です。

（注） ライセンスPIDに表示される値（数値または階層ベース）は、双方向スループット値を表します。

総スループットのスロットリング

ここで、システムは設定された値を2倍にし、この集約制限でスループットをスロットリングします。総スループットのスロットリングが有効な場合、トラフィックは各方向で個別にスロットリングされません。

たとえば、設定されている双方向スループット値が 500 Mbps で、総スループットのスロットリングが有効である場合は、次のようになります。

- 仮想プラットフォームでは、送信データの上限は 1 Gbps です。受信データはスロットリングされません。
- 物理プラットフォームでは、アップストリームおよびダウンストリーム方向のトラフィックは、1 Gbps の集約制限内の任意の比率にすることができます。たとえば、800 Mbps 送信と 200 Mbps 受信、または 300 Mbps 送信と 700 Mbps 受信）

スロットリング動作のリリースごとの変更

デバイスのスループットが双方向の方法でスロットリングされるか、集約的な方法でスロットリングされるかを確認するには、デバイスで実行されているソフトウェアバージョンを確認し、以下で説明するスロットリング動作のリリースごとの変更点を参照してください。

- **Cisco IOS XE Cupertino 17.7.x 以前**：双方向のスループットスロットリングのみが有効です。これは、物理プラットフォームと仮想プラットフォームに適用されます。
- **Cisco IOS XE Cupertino 17.8.1a 以降**：
  - 物理プラットフォームでのみ、250 Mbps を超えるスループット値または T2 以上の階層を設定すると、総スループットのトスロットリングが有効になります。

    C8200L-1N-4T では、250 Mbps の数値を設定すると、双方向のスループットスロットリングが有効になり、各方向で最大 250 Mbps を使用できます。ただし、階層 T2 を設定すると、集約スロットリングが有効になり、任意の送信および受信データ比率で 500 Mbps を使用できます。
  - 仮想プラットフォームでは、送信データのスロットリングは引き続き適用され、受信データは引き続きスロットリングされません。
- **Cisco IOS XE Cupertino 17.9.1a 以降**：仮想プラットフォームでは、すべてのスループットレベルとすべての階層で、集約スループットスロットリングが有効です。

（注） 仮想プラットフォームで設定したスループットレベルの集約が 250 Mbps を超える場合、HSECK9 ライセンスがデバイスで使用可能でない限り（つまり、SLAC がインストールされている場合）、総スループットスロットリングは有効になりません。

- **Cisco IOS XE 17.14.1a 以降**：物理および仮想プラットフォームでは、250 Mbps または T1 のスループットを設定すると、HSECK9 ライセンスがデバイスで使用可能である限り、総スループットスロットリングが有効になります。仮想プラットフォームでは、これは送信データのスループットが 500 Mbps に制限されることを意味します。物理プラットフォームでは、これは 500 Mbps の集約制限が任意の送信および受信データの比率で使用できることを意味します。

  HSECK9 ライセンスがデバイスで使用できず、250 Mbps または T1 のスループット値を設定すると、双方向スループットスロットリングが有効になります。仮想プラットフォームでは、これは送信データのスループットが 250 Mbps でスロットリングされることを意味します。物理プラットフォームでは、スループットは各方向で 250 Mbps でスロットリングされます。

階層および数値のスループットのマッピング

次の表に、各階層に相当する数値と、各階層で使用可能な Cisco DNA ライセンスに関する情報を示します。

ヒント マッピング表では、階層に相当する数値のみを明示します。このマッピングは、ユーザーが利用できる最終的なスループットを反映するものではありません。利用できるスループットは、デバイスの機能、デバイスで実行されているソフトウェアバージョン、およびそのバージョンのスロットリング動作によって異なります。

（注） 階層ベースのスループット値が T1 のライセンス PID を購入すると、HSECK9 ライセンスが自動的に提供されます。

Y：Network Premium および Cisco DNA Premium

Y：Network Advantage および Cisco DNA Advantage

Y：Network Essentials および Cisco DNA Essentials

* は HSECK9 ライセンスが必要です。C8500 および C8500L では、HSECK9 ライセンスはコンプライアンス目的でのみ必要です。

表 *11* : 仮想プラットフォームの階層および数値スループットマッピング（*C8000v*）

17.9.1a 以降の階層：	**T0**		**T1**		**T2***			**T3***			**T4***
17.7.x、17.8.x の階層：	**T0**	**T1**			**T2***			**T3***			**T4***
数値マッピング：	**15 M**	**25M**	**50M**	**100M**	**250M**	**500M**	**1G**	**2.5G**	**5G**	**10G**	スロットルなし
使用可能な Cisco DNA ライセンス：	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y	Y Y	Y Y	Y Y

表 *12* : 物理プラットフォームの階層および数値スループットマッピング（*C8200*、*C8300*、*C8500*）

17.8.1a 以降の階層：	T0		T1			T2*			T3*			T4*	T5*
17.7.x の階層：	T0		T1			T2*			T3*			該当なし	該当なし
設定された数値：	**10M**	**15 M**	**25M**	**50M**	**100M**	**250M**	**500M**	**1G**	**2.5G**	**5G**	**10G**	**50G**	スロットルなし
C8200-1N-4T	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y						
C8200L-1N-4T	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y							
C8300-1N1S-4T2X	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y				
C8300-1N1S-6T	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y					
C8300-2N2S-4T2X	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y				
C8300-2N2S-6T	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y	Y Y Y					
C8500-12X									Y Y	Y Y	Y Y		
C8500-12X4QC									Y Y	Y Y	Y Y		
C8500-20X6C												Y Y	Y Y
C8500L-8S4X								Y Y	Y Y	Y Y	Y Y		

自律モードで使用可能なスループットとスロットリングの仕様

これらの表は、利用資格があるスループットを示します。これは、デバイス、スループット値（集約または数値）、およびスロットリングが集約または双方向のどちらで適用されるかを決定するリリースに基づいています。

表 *13 : C8000v*

スループット＝暗号化および非暗号化スループット 受信データはスロットリングされません * HSECK9 ライセンスが必要です。				
サポートされるスループット値（デフォルトは 10M）	**17.4.1a 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.9.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M Tx のみ	10M Tx のみ	20M Tx のみ	20M Tx のみ
15 M	15M Tx のみ	15M Tx のみ	30M Tx のみ	30M Tx のみ
25M	25M Tx のみ	25M Tx のみ	50M Tx のみ	50M Tx のみ
50M	50M Tx のみ	50M Tx のみ	100M Tx のみ	100M Tx のみ
100M	100M Tx のみ	100M Tx のみ	200M Tx のみ	200M Tx のみ
250M	250M Tx のみ	250M Tx のみ	250M Tx のみ	HSECK9 あり：500M Tx HSECK9 なし：250M Tx
500M*	500M Tx のみ	500M Tx のみ	1G Tx のみ	1G Tx のみ
1G*	1G Tx のみ	1G Tx のみ	2G Tx のみ	2G Tx のみ
2.5G*	2.5G Tx のみ	2.5G Tx のみ	5G Tx のみ	5G Tx のみ
5G*	5G Tx のみ	5G Tx のみ	10G Tx のみ	10G Tx のみ
10G*	10G Tx のみ	10G Tx のみ	20G Tx のみ	20G Tx のみ
T0	-	15M Tx のみ	50M Tx のみ	50M Tx のみ
T1	-	100M Tx のみ	200M Tx のみ	HSECK9 あり：500M Tx HSECK9 なし：250M Tx
T2*	-	1G Tx のみ	2G Tx のみ	2G Tx のみ
T3*	-	10 Tx のみ	20G Tx のみ	20G Tx のみ

T4*	-	スロットルなし	スロットルなし	スロットルなし

表 *14 : C8200-1N-4T*

スループット = 暗号化されたスループット * HSECK9 ライセンスが必要です。				
サポートされるスループット値（デフォルトは 10M）	**17.4.1a 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M 双方向	10M 双方向	10M 双方向	10M 双方向
15 M	15M 双方向	15M 双方向	15M 双方向	15M 双方向
25M	25M 双方向	25M 双方向	25M 双方向	25M 双方向
50M	50M 双方向	50M 双方向	50M 双方向	50M 双方向
100M	100M 双方向	100M 双方向	100M 双方向	100M 双方向
250M	250M 双方向	250M 双方向	250M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
500M*	500M 双方向	500M 双方向	1G 集約	1G 集約
T0	-	15M 双方向	25M 双方向	25M 双方向
T1	-	100M 双方向	100M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T2	-	500M 双方向	1G 集約	1G 集約

表 *15 : C8200L-1N-4T*

スループット = 暗号化されたスループット * HSECK9 ライセンスが必要です。				
サポートされるスループット値（デフォルトは 10M）	**17.5.1a 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M 双方向	10M 双方向	10M 双方向	10M 双方向

15 M	15M 双方向	15M 双方向	15M 双方向	15M 双方向
25M	25M 双方向	25M 双方向	25M 双方向	25M 双方向
50M	50M 双方向	50M 双方向	50M 双方向	50M 双方向
100M	100M 双方向	100M 双方向	100M 双方向	100M 双方向
250M	250M 双方向	250M 双方向	250M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T0	-	15M 双方向	25M 双方向	25M 双方向
T1	-	100M 双方向	100M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T2*	-	250M 双方向	500M 集約	500M 集約
-			（注） 17.8.1a 以降、C8200-1N-4T-L では、250 Mbps の数値を設定すると、各方向で最大 250 Mbps を使用できます。ただし、階層ベースの値 T2 を設定する場合（HSECK9 ライセンスが必要）、500 Mbps を任意の送信および受信データ比率で使用できます。	

表 *16 : C8300-1N1S-4T2X、C8300-2N2S-4T2X*

スループット = 暗号化されたスループット * HSECK9 ライセンスが必要です。				
サポートされるスループット値 **（デフォルトは 10M）**	**17.3.2 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M 双方向	10M 双方向	10M 双方向	10M 双方向
15 M	15M 双方向	15M 双方向	15M 双方向	15M 双方向
25M	25M 双方向	25M 双方向	25M 双方向	25M 双方向
50M	50M 双方向	50M 双方向	50M 双方向	50M 双方向
100M	100M 双方向	100M 双方向	100M 双方向	100M 双方向

250M	250M 双方向	250M 双方向	250M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
500M*	500M 双方向	500M 双方向	1G 集約	1G 集約
1G*	1G 双方向	1G 双方向	2G 集約	2G 集約
2.5G*	2.5G 双方向	2.5G 双方向	5G 集約	5G 集約
T0	-	15M 双方向	25M 双方向	25M 双方向
T1	-	100M 双方向	100M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T2*	-	1G 双方向	2G 集約	2G 集約
T3*	-	10G 双方向	20G 集約	20G 集約

表 *17 : C8300-1N1S-6T、C8300-2N2S-6T*

				スループット = 暗号化されたスループット * HSECK9 ライセンスが必要です。
サポートされるスループット値 **（デフォルトは 10M）**	**17.3.2 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**	**17.14.1a 以上で使用可能なスループットとスロットリング**
10M	10M 双方向	10M 双方向	10M 双方向	10M 双方向
15 M	15M 双方向	15M 双方向	15M 双方向	15M 双方向
25M	25M 双方向	25M 双方向	25M 双方向	25M 双方向
50M	50M 双方向	50M 双方向	50M 双方向	50M 双方向
100M	100M 双方向	100M 双方向	100M 双方向	100M 双方向
250M	250M 双方向	250M 双方向	250M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
500M*	500M 双方向	500M 双方向	1G 集約	1G 集約
1G*	1G 双方向	1G 双方向	2G 集約	2G 集約
T0	-	15M 双方向	25M 双方向	25M 双方向

T1	-	100M 双方向	100M 双方向	HSECK9 あり：500M 集約 HSECK9 なし：250M 双方向
T2*	-	1G 双方向	2G 集約	2G 集約

表 *18 : C8500-12X、C8500-12X4QC*

スループット = 暗号化されたスループット *HSECK9 ライセンスは、コンプライアンス目的でのみ必要です。			
サポートされるスループット値 **（デフォルトは 10M）**	**17.3.2 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**
2.5G*	2.5G 双方向	2.5G 双方向	5G 集約
5G*	5G 双方向	5G 双方向	10G 集約
10G*	10G 双方向	10G 双方向	20G 集約
T3*	-	10G 双方向	20G 集約

表 *19 : C8500L-8S4X*

スループット = 暗号化されたスループット *HSECK9 ライセンスは、コンプライアンス目的でのみ必要です。			
サポートされるスループット値 **（デフォルトは 10M）**	**17.4.1a 以上で使用可能なスループットとスロットリング**	**17.7.1a 以上で使用可能なスループットとスロットリング**	**17.8.1a 以上で使用可能なスループットとスロットリング**
1G*	1G 双方向	1G 双方向	2G 集約
2.5G*	2G 双方向	2G 双方向	5G 集約
5G*	5G 双方向	5G 双方向	10G 集約
10G*	10G 双方向	10G 双方向	20G 集約
T2*	-	1G 双方向	2G 集約
T3*	-	10G 双方向	20G 集約

表 *20 : C8500-20X6C*

スループット = 暗号化されたスループット *HSECK9 ライセンスは、コンプライアンス目的でのみ必要です。	
サポートされるスループット値 （デフォルトは T4）	**17.10.1a 以上で使用可能なスループットとスロットリング**
T4*	50G 集約
T5*	スロットルなし

SD-WAN コントローラモードで使用可能なスループットとスロットリングの仕様

PID	**PID** の導入リリース	**HSECK9** なしのスループット（双方向）	**HSECK9** ありのスループット（**17.3.2** 以上 **17.8.1a** 未満、双方向）	**HSECK9** ありのスループット（**17.8.1a** より後、集約）
C8300-1N1S-4T2X（デフォルトは 250M）	17.3.2	250M	スロットルなし	スロットルなし
C8300-2N2S-6T（デフォルトは 250M）	17.3.2	250M	1G	2G
C8300-1N1S-6T（デフォルトは 250M）	17.3.2	250M	1G	2G
C8300-2N2S-4T2X（デフォルトは 250M）	17.3.2	250M	スロットルなし	スロットルなし
C8200-1N-4T（デフォルトは 250M）	17.4.1a	250M	500M	1G
C8200L-1N-4T（デフォルトは 250M）	17.5.1a	250M	250M	500M
C8500-12X4QC（デフォルトはスロットルなし）	17.3.2	スロットルなし	スロットルなし	スロットルなし

PID	PID の導入リリース	HSECK9 なしのスループット（双方向）	HSECK9 ありのスループット（17.3.2 以上 17.8.1a 未満、双方向）	HSECK9 ありのスループット（17.8.1a より後、集約）
C8500-12X（デフォルトはスロットルなし）	17.3.2	スロットルなし	スロットルなし	スロットルなし
C8500L-8S4X（デフォルトはスロットルなし）	17.4.1a	スロットルなし led	スロットルなし	スロットルなし
C8500-20X6C（デフォルトは T4）	17.10.1a	スロットルなし	-	スロットルなし
C8000v（デフォルトは 250M）	17.4.1a	250M	スロットルなし	スロットルなし

数値と階層ベースのスループットの設定

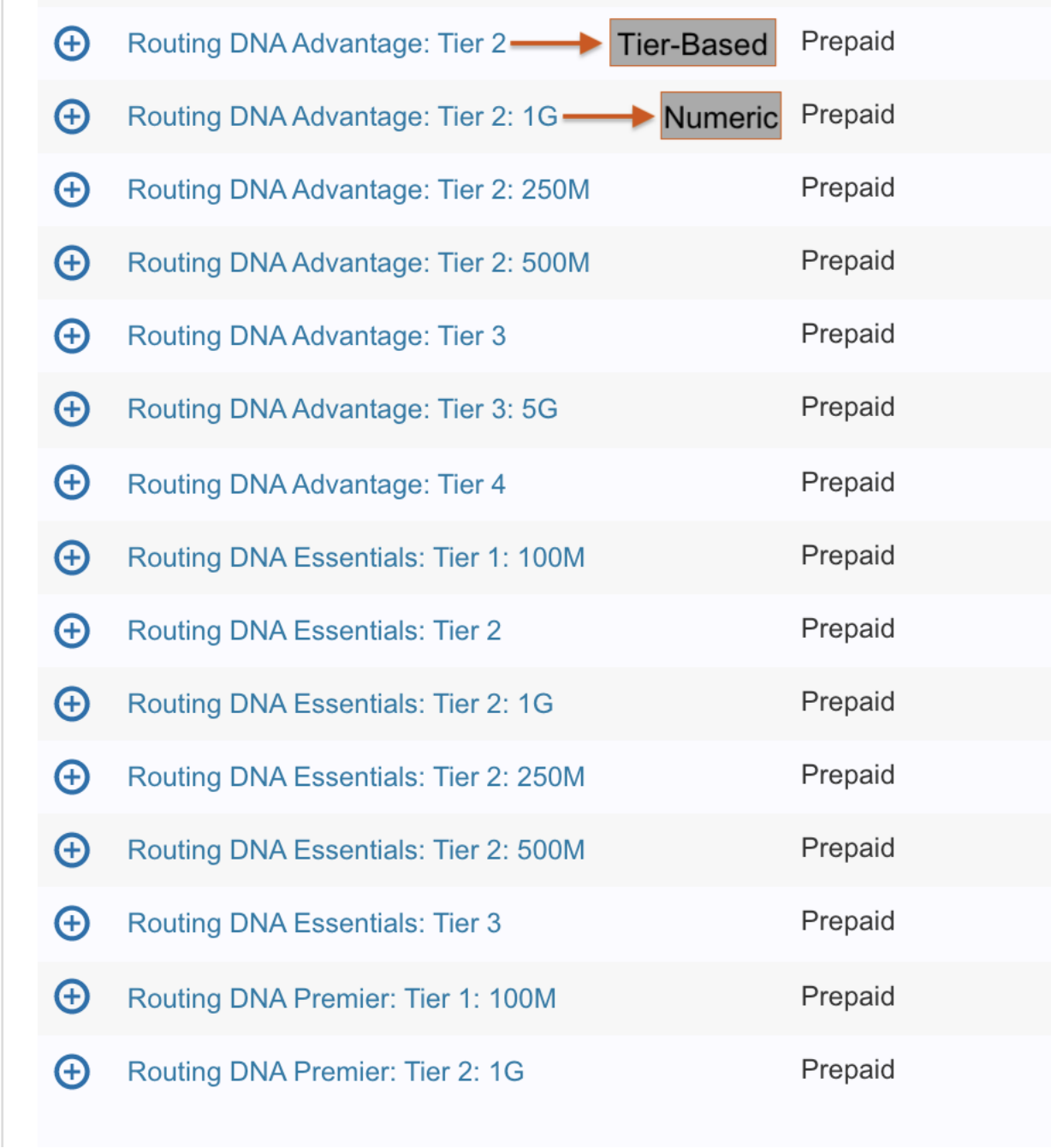
Cisco IOS XE Cupertino 17.7.1a での階層ベースのスループットの設定の導入により、デバイスでスループットを設定する際に、数値と階層ベースの両方のオプションを使用できます。このセクションでは、数値のスループット値を設定するタイミングと、階層ベースのスループットを設定するタイミングについて説明します。

階層ベースまたは数値ライセンスのいずれがあるかの識別

Cisco Smart Software Manager（CSSM）は、すべてのシスコ ソフトウェア ライセンスを管理できるポータルです。購入したすべてのライセンス PID は、CSSM Web UI の https://software.cisco.com → [Manage licenses] に一覧表示されます。階層ベースのライセンスと数値ライセンスのどちらがあるかを識別する方法の 1 つは、CSSM でライセンスがどのように表示されるかを確認することです。

これを行うには、ポータルにログインし、対応するスマートアカウントとバーチャルアカウントで、[Inventory] > [Licences] に移動して、アカウントのライセンスを表示します。次のスクリーンショットは、両方がどのように表示されるかを示しています。

図 *1 : CSSM Web UI* に表示される数値と階層の値



数値または階層ベースのスループット値を設定するかどうかに関する推奨事項

- 数値のライセンス PID を購入した場合、ライセンスは CSSM Web UI に数値のスループット値と階層ベースの値とともに表示されます。このようなライセンスでは、数値のスループット値のみを設定することをお勧めします。

  『数値のスループットの設定 （77 ページ）』を参照してください。

- 階層ベースのライセンス PID を購入した場合、ライセンスは CSSM Web UI に階層の値のみで表示されます。このようなライセンスの場合、CSSM Web UI の表示と一致するように階層ベースのスループット値を設定するか、数値のスループット値を設定できます。

  階層ベースのスループットの設定 （81 ページ）または数値のスループットの設定 （77 ページ）を参照してください。

（注） CSSM に階層ベースのライセンス PID があり、デバイスで数値のスループット値を設定する場合、機能への影響はありません。

設定された値を数値または階層ベースの値に変換するタイミング

次のシナリオでは、数値から階層ベースのスループットの設定に、または階層ベースのスループットの設定から数値に変換できるタイミング、変換が必要なタイミング、および変換がオプションであるタイミングをさらに明確にします。

- デバイスに数値のスループット値を設定し、ライセンス PID が数値のライセンスの場合：階層ベースのスループット値に変換してはなりません。
- デバイスに数値のスループット値を設定し、ライセンス PID が階層ベースのライセンスの場合：スループットの設定を階層ベースの値に変換できますが、これはオプションです。階層ベースのスループット値に変換しない場合、機能への影響はありません。

  階層ベースの値に変換する場合は、数値のスループット値から階層への変換 （86 ページ）を参照してください。

- 階層ベースのスループット値がサポートされているリリースにアップグレードし、ライセンス PID が階層ベースの場合：アップグレード後にスループットを階層ベースの値に変換できますが、これはオプションです。階層ベースのスループット値に変換しない場合、機能への影響はありません。

  『数値のスループットをサポートするリリースから階層をサポートするリリースへのアップグレード （88 ページ）』を参照してください。

- 階層ベースのスループット値がサポートされているリリースにアップグレードし、ライセンス PID が数値である場合：階層ベースのスループット値に変換してはなりません。
- 数値のスループット値のみがサポートされているリリースにダウングレードし、ライセンス PID とスループットの設定が階層ベースである場合：ダウングレードする前に、設定を数値のスループット値に変更する必要があります。

  階層をサポートするリリースから数値のスループットのみをサポートするリリースへのダウングレード （89 ページ）を参照してください。

使用可能なライセンスとスループットの設定方法

このセクションでは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリで使用可能なさまざまなライセンスについて、使用を開始する前にタスクを完了する必要のあるシーケンスについて説明します。

Cisco DNA ライセンスの場合：[Configure a Boot Level License] → [Configure Numeric or Tier-Based Throughput] → [Implement a Smart Licensing Using Policy Topology] → [Report License Usage (If Applicable)]。

HSECK9 ライセンスの場合：[Configure a Boot Level License] → [Implement a Smart Licensing Using Policy Topology] → [Install SLAC] [3]→ [Enable HSECK9 on applicable platforms] [4]→ [Configure Numeric or Tier-Based Throughput] → [Report License Usage (If Applicable)]。

Cisco UBE、Cisco Unified CME、または Cisco Unified SRST ライセンスの場合：[Implement a Smart Licensing Using Policy Topology] → [Report License Usage (If Applicable)]。

ブートレベルライセンスの設定

新しいデバイス用にCisco DNAライセンスを購入した場合、または既存のデバイスがあり、デバイスに現在設定されているライセンスを変更（アップグレードまたはダウングレード、追加または削除）する場合は、次のタスクを実行します。

これによりライセンスレベルが設定されます。設定された変更を有効にする前にリロードが必要です。

手順

ステップ 1 **show version**

現在設定されているブートレベルライセンスを表示します。

添付の例では、Network Advantage と Cisco DNA Advantage のライセンスがデバイスに設定されています。

例：

```
Device# show version
<output truncated>
Technology Package License Information:

------------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
------------------------------------------------------------------
Smart License  Perpetual    network-advantage  network-advantage
Smart License  Subscription dna-advantage      dna-advantage
```

[3] SLAC がシスコ出荷時にインストールされている場合（新しいハードウェアの場合）、このステップはスキップします
[4] Catalyst 8200 および 8300 シリーズ エッジ プラットフォームだけのグローバル コンフィギュレーション モードで **license feature hseck9** コマンドを入力します。

```
<output truncated>
```

ステップ 2 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。

例：

```
Device# configure terminal
```

ステップ 3 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを設定します。

- 物理プラットフォームの場合：[**no**] **license boot level** {**network-advantage** [**addon dna-advantage**] | **network-essentials** [**addon dna-essentials**] | **network-premier** [**addon dna-premier**] }
- 仮想プラットフォームの場合：[**no**] **license boot level** {**network-advantage** {**addon dna-advantage**} | **network-essentials** {**addon dna-essentials**} | **network-premier** {**addon dna-premier**} }

ブートレベルライセンスを設定します。

すべてのプラットフォームで、最初にネットワーク スタック ライセンスを設定します。この後にのみ、対応するアドオンライセンスを設定できます。

コマンド構文では、Cisco DNA スタックアドオンライセンスの設定が物理プラットフォームではオプションであり、仮想プラットフォームでは必須であることに注意してください。

添付の例は、物理プラットフォームである C8300-1N1S-4T2X ルータの設定を示しています。ネットワーク スタック ライセンスである Network Premier と、対応するアドオンライセンスである Cisco DNA-Premier が設定されています。

例：

```
Device(config)# license boot level network-premier addon dna-premier
% use 'write' command to make license boot config take effect on next boot
```

ステップ 4 exit

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

```
Device# exit
```

ステップ 5 copy running-config startup-config

コンフィギュレーション ファイルに設定を保存します。

例：

```
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
<output truncated>
```

ステップ 6 reload

デバイスがリロードされます。ステップ 3 で設定されたライセンスレベルは、このリロード後にのみ有効になり、表示されます。

例：

```
Device# reload
Proceed with reload? [confirm]

*Dec  8 01:04:12.287: %SYS-5-RELOAD: Reload requested by console.
Reload Reason: Reload Command.
<output truncated>
```

ステップ 7 **show version**

現在設定されているブートレベルライセンスを表示します。

添付の例では、出力により、Network Premier および Cisco DNA-Premier ライセンスが設定されていることが確認されます。

例：

```
Device# show version
<output truncated>
Technology Package License Information:

------------------------------------------------------------------
Technology     Type         Technology-package Technology-package
                            Current            Next Reboot
------------------------------------------------------------------
Smart License  Perpetual    network-premier    network-premier
Smart License  Subscription dna-premier        dna-premier
<output truncated>
```

ステップ 8 **show license summary**

使用されているライセンス、カウント、およびステータスに関する情報を含む、ライセンス使用状況の概要を表示します。

例：

```
Device# show license summary

Account Information:
  Smart Account: Eg-SA As of Dec 08 08:10:33 2021 UTC
  Virtual Account: Eg-VA

License Usage:
  License                 Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  network-premier_T2      (NWSTACK_T2_P)                    1 IN USE
  dna-premier_T2          (DSTACK_T2_P)                     1 IN USE
```

ステップ 9 完全な使用状況レポート（必要な場合）

ライセンスレベルを設定した後、ライセンス使用情報を報告するために、RUM レポート（リソース使用率測定レポート）を CSSM に送信する必要がある場合があります。レポートが必要かどうかを確認するには、システムメッセージを待つか、show コマンドを使用してポリシーを参照します。

- レポートが必要であることを示すシステムメッセージ：%SMART_LIC-6-REPORTING_REQUIRED: A Usage report acknowledgement will be required in [dec] days. [dec] は、レポート要件を満たすために残された時間（日数）です。
- show コマンドを使用する場合は、**show license status** 特権 EXEC コマンドの出力を参照し、[Next ACK deadline] フィールドを確認します。これは、この日付までに RUM レポートを送信して CSSM から acknowledgement（ACK）をインストールする必要があることを意味します。

RUM レポートの送信方法は、ポリシーを使用したスマートライセンシング環境で実装したトポロジによって異なります。詳細については、『How to Configure Smart Licensing Using Policy: Workflows by Topology』を参照してください。

HSECK9 ライセンス用の SLAC のインストール

Smart Licensing Authorization Code（SLAC）は、Cisco Smart Software Manager（CSSM）ポータルで生成、取得されます。

製品を CSSM に接続して SLAC を取得する方法はいくつかあります。CSSM に接続する各方法がトポロジと呼ばれます。サポートされているトポロジの 1 つを実装して、対応するメソッドで SLAC をインストールできるようにする必要があります。

すべてのメソッドの詳細については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』ドキュメントの「Supported Topologies」を参照してください。

（注） デバイスにブートレベルライセンスがすでに設定されていることを確認します。ブートレベルライセンスの設定 （74 ページ）を参照してください。show version 特権 EXEC コマンドの出力で、ライセンスが [License Level] フィールドに指定されていることを確認します。

SLAC のインストール後に必要なタスク

SLAC をインストールした後、プラットフォームに該当する場合のみ、次の必要なタスクを完了します。

プラットフォーム	SLAC のインストール後に必要なタスク
Catalyst 8200 および 8300 シリーズエッジプラットフォームの場合	グローバル コンフィギュレーション モードで **license feature hseck9** コマンドを入力します。これにより、これらのプラットフォームで HSECK9 ライセンスが有効になります。
Catalyst 8500 シリーズ エッジ プラットフォームの C8500L モデルの場合	SLAC のインストール後にデバイスをリロードします。

数値のスループットの設定

このタスクでは、物理プラットフォームおよび仮想プラットフォームで数値のスループットレベルを変更する方法を示します。スループットレベルを設定しない場合、プラットフォームのデフォルトのスループットレベルが有効になります。

スループットレベルを設定するには、物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズ エッジ プラットフォーム）でリロードが必要です。仮想プラットフォーム（Catalyst 8000V エッジソフトウェア）の場合、リロードは必要ありません。

始める前に

- 数値および階層ベースのスループット （59ページ）および数値と階層ベースのスループットの設定 （71 ページ）のセクションを参照してください。
- デバイスにブートレベルライセンスがすでに設定されていることを確認します。ライセンスが設定されていないと、スループット値を設定できなくなります。ブートレベルライセンスの設定 （74 ページ）を参照してください。**show version** 特権 EXEC コマンドの出力で、ライセンスが [License Level] フィールドに指定されていることを確認します。
- 250 Mbps を超えるスループットを設定する場合は、このタスクを開始する前に Smart Licensing Authorization Code（SLAC）をインストールする必要があります。HSECK9 ライセンス用の SLAC のインストール （77 ページ）を参照してください。
- `250M`の値は、HSECK9 ライセンスの有無にかかわらず設定できます。システムでは両方が許可されます。違いは、HSECK9 がデバイスで使用可能な場合には集約スロットリングが有効になることです。スロットリング動作のリリースごとの変更 （62 ページ）を参照してください。
- 使用できるスループットに注意してください。これは、購入した Cisco DNA ライセンス PID に示されています。

手順

ステップ 1 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**show platform hardware throughput crypto**
- 仮想プラットフォームの場合：**show platform hardware throughput level**

デバイスの現在のスループットレベルを表示します。

添付の例：

- **show platform hardware throughput crypto** の出力例は、物理プラットフォーム（C8300-2N2S-4T2X）のものです。ここでは、スループットレベルが 250M にスロットルされています。
- **show platform hardware throughput level** の出力例は、仮想プラットフォーム（C8000V）のものです。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: 250M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 250M
Crypto Throughput is throttled at 250M
Default Crypto throughput level: 10M
Current boot level is network-advantage
```

```
OR

Device# show platform hardware throughput level
The current throughput level is 1000000 kb/s
```

ステップ 2 **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。

例：

```
Device# configure terminal
```

ステップ 3 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを設定します。

- 物理プラットフォームの場合：**platform hardware throughput crypto** {**100M** | **10M** | **15M** | **1G** | **2.5G** | **250M** | **25M** | **500M** | **50M**}
- 仮想プラットフォームの場合：**platform hardware throughput level MB** {**100** | **1000** | **10000** | **15** | **25** | **250** | **2500** | **50** | **500** | **5000**}

スループットレベルを設定します。表示されるスループットオプションは、デバイスによって異なります。

（注） 物理プラットフォームおよび仮想プラットフォームでは、ブートレベルライセンスが設定されていることを確認します。そうしないと、コマンドがコマンド ライン インターフェイスで有効なものとして認識されません。

添付の例：

- 物理プラットフォームで 1 Gbps が設定されています。デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは集約スループットスロットリングが適用されることを意味します。リロード後は、アップストリームとダウンストリームのスループットの合計が 2 Gbps の制限を超えることはありません。
- 仮想プラットフォームで 5000 Mbps が設定されています。デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは送信データが 5000 Mbps でスロットリングされることを意味します。受信データはスロットリングされません。

例：

```
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
Device(config)# platform hardware throughput crypto 1G
% These values don't take effect until the next reboot.
Please save the configuration.

OR

Device(config)# platform hardware throughput level MB 5000
%Throughput has been set to 5000 Mbps.
```

ステップ 4 **exit**

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

```
Device# exit
```

ステップ 5 **copy running-config startup-config**

コンフィギュレーション ファイルに設定を保存します。

例：

```
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

ステップ 6 **reload**

デバイスがリロードされます。

（注） スループットを設定しているデバイスが物理プラットフォーム上にある場合にのみ、この手順を実行します。

仮想プラットフォームでスループットを設定している場合は、この手順をスキップしてください。

例：

```
Device# reload
```

ステップ 7 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- **物理プラットフォームの場合**：**show platform hardware throughput crypto**
- **仮想プラットフォームの場合**：**show platform hardware throughput level**

デバイスの現在のスループットレベルを表示します。

ヒント 物理プラットフォームでは、**show platform hardware qfp active feature ipsec state** 特権 EXEC コマンドを入力して、設定されているスループットレベルを表示することもできます。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: 1G
     Level is saved, reboot is not required
Current enforced crypto throughput level: 1G
Crypto Throughput is throttled at 2G(Aggregate)
Default Crypto throughput level: 10M

OR

Device# show platform hardware throughput level
The current throughput level is 5000000 kb/s
```

階層ベースのスループットの設定

このタスクでは、物理および仮想プラットフォームで階層ベースのスループットレベルを設定する方法を示します。スループットレベルを設定しない場合、プラットフォームのデフォルトのスループットレベルが有効になります。

階層ベースのスループットレベルは、Cisco IOS XE Cupertino 17.7.1a 以降でのみサポートされます。

スループットレベルを設定するには、物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズ エッジ プラットフォーム）でリロードが必要です。仮想プラットフォーム（Catalyst 8000V エッジソフトウェア）の場合、リロードは必要ありません。

始める前に

- 数値および階層ベースのスループット （59ページ）および数値と階層ベースのスループットの設定 （71 ページ）のセクションを参照してください。
- デバイスにブートレベルライセンスがすでに設定されていることを確認します。ライセンスが設定されていないと、スループット値を設定できなくなります。ブートレベルライセンスの設定 （74 ページ）を参照してください。**show version** 特権 EXEC コマンドの出力で、ライセンスが [License Level] フィールドに指定されていることを確認します。
- Tier 2（T2）以上の階層を設定する場合は、このタスクを開始する前に Smart Licensing Authorization Code（SLAC）をインストールする必要があります。HSECK9 ライセンス用の SLAC のインストール （77 ページ）を参照してください。
  - 物理プラットフォームでは、SLAC がインストールされていない場合、T2 以上の階層は表示されません。
  - 仮想プラットフォームでは、SLAC がインストールされていない場合でも、すべての階層オプションが表示されます。ただし、T2 以上の階層を設定する場合は SLAC が必要です。
- 階層 3（T3）を設定する場合は、ブートレベルライセンスが Network Advantage/Cisco DNA Advantage、または Network Premier/Cisco DNA Premier であることを確認してください。T3 以上の階層は、Network Essentials および Cisco DNA Essentials ではサポートされていません。
- `T1` 値は、HSECK9 ライセンスの有無にかかわらず設定できます。システムでは両方が許可されます。違いは、HSECK9 がデバイスで使用可能な場合には集約スロットリングが有効になることです。スロットリング動作のリリースごとの変更 （62 ページ）を参照してください。
- 使用できるスループットに注意してください。これは、購入した Cisco DNA ライセンス PID に示されています。

手順

ステップ 1 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**show platform hardware throughput crypto**
- 仮想プラットフォームの場合：**show platform hardware throughput level**

デバイスの現在のスループットレベルを表示します。

添付の例：

- **show platform hardware throughput crypto** の出力例は、物理プラットフォーム（C8300-2N2S-4T2X）のものです。この例ではスループットは現在 250 Mbps にスロットルされています。
- **show platform hardware throughput level** の出力例は、仮想プラットフォーム（C8000V）のものです。この例では現在のスループットレベルは 10 Mbps です。

例：

```
Device# show platform hardware throughput crypto
show platform hardware throughput crypto
Current configured crypto throughput level: 250M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 250M
Crypto Throughput is throttled at 250M
Default Crypto throughput level: 10M
Current boot level is network-premier

OR

Device# show platform hardware throughput level
The current throughput level is 10000 kb/s
```

ステップ 2 **show license authorization**

（オプション）製品インスタンスの SLAC 情報を表示します。

添付の例：

- SLAC は物理プラットフォームにインストールされています。これは、T2 を設定できるようにするためです。
- SLAC は仮想プラットフォームでは使用できません。これが後続の手順でスループットの設定にどのように影響するかに注意してください。

例：

```
Device# show license authorization
Overall status:
  Active: PID:C8300-2N2S-4T2X,SN:FDO2250A0J5
      Status: SMART AUTHORIZATION INSTALLED on Mar 02 05:05:19 2022 UTC
      Last Confirmation code: 418b11b3

Authorizations:
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for
    DNA based Routers
```

```
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available

OR

Device# show license authorization
Overall status:
  Active: PID:C8000V,SN:9I8GRCH8CMN
      Status: NOT INSTALLED
```

ステップ 3 **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。

例：

```
Device# configure terminal
```

ステップ 4 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを設定します。

- 物理プラットフォームの場合：**platform hardware throughput crypto** {**T0** | **T1** | **T2** | **T3** | **T4** | **T5**}
- 仮想プラットフォームの場合：**platform hardware throughput level MB** {**T0** | **T1** | **T2** | **T3** | **T4** }

階層ベースのスループットを設定します。表示されるスループットオプションは、デバイスによって異なります。

（注） わかりやすくするために、階層のみがコマンドで指定されています。CLI でコマンドを入力すると、添付の例に示すように、数値と階層の値が表示されます。

以下は、物理プラットフォームと仮想プラットフォームの両方に適用されます。

- ブートレベルライセンスはすでに設定されていることを確認します。そうでなければ、スループットの設定のコマンドはコマンド ライン インターフェイスで有効なものとして認識されません。
- T2 以上の階層を設定している場合は、SLAC がインストールされています。

  物理プラットフォームでは、SLAC がインストールされていない場合、T2 以上の階層を設定することはできません。

  仮想プラットフォームで、SLAC なしで T2 以上の階層を設定すると、製品インスタンスは自動的に CSSM にアクセスして SLAC を要求してインストールしようとします。成功した場合、スループットは設定された階層に設定されます。成功しなかった場合、システムはスループットを 250 Mbps に設定します。SLAC がインストールされている場合、スループットは自動的に最後に設定された値に設定されます。

添付の例：

- 物理プラットフォームで 1 Gbps が設定されています。デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは集約スループットスロットリングが適用される

ことを意味します。リロード後は、アップストリームとダウンストリームのスループットの合計が 2 Gbps の制限を超えることはありません。

- 仮想プラットフォームで5000 Mbpsが設定されています。デバイスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.8.1a であり、これは送信データが 5000 Mbps でスロットリングされることを意味します。受信データはスロットリングされません。

- 物理プラットフォーム（**platform hardware throughput crypto**）では、SLAC がインストールされているため、T2 以上の階層が表示されます。SLAC が使用できない場合、表示される最上位の階層は T1 です。

  デバイスで実行されているソフトウェアバージョンはCisco IOS XE Cupertino 17.8.1a であり、これは集約スループットスロットリングが適用されることを意味します。リロード後は、アップストリームとダウンストリームのスループットの合計が 2 Gbps の制限を超えることはありません。

- 仮想プラットフォーム（**platform hardware throughput level MB**）では、すべての階層が表示されます。T2 が設定された後、SLAC がインストールされていないために設定が行われていないことを警告するシステムメッセージが表示されます。

例：

```
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
  T0    T0(up to 15 mbps) bidirectional thput
  T1    T1(up to 100 mbps) bidirectional thput
  T2    T2(up to 2 gbps) aggregate thput
  T3    T3(up to 5 gbps) aggregate thput

Device(config)# platform hardware throughput crypto T2
% These values don't take effect until the next reboot.
Please save the configuration.
*Mar 02 05:06:19.042: %CRYPTO_SL_TP_LEVELS-6-SAVE_CONFIG_AND_RELOAD:
New throughput level not applied until reload; please save config

OR
Device(config)# platform hardware throughput level MB ?
  100    Mbps
  1000   Mbps
  10000  Mbps
  15     Mbps
  25     Mbps
  250    Mbps
  2500   Mbps
  50     Mbps
  500    Mbps
  5000   Mbps
  T0     Tier0(up to 15M throughput)
  T1     Tier1(up to 100M throughput)
  T2     Tier2(up to 1G throughput)
  T3     Tier3(up to 10G throughput)
  T4     Tier4(unthrottled)
```

```
Device(config)# platform hardware throughput level MB T2
%Requested throughput will be set once HSEC authorization
code is installed
```

ステップ 5 **exit**

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例：

```
Device# exit
```

ステップ 6 **copy running-config startup-config**

コンフィギュレーション ファイルに設定を保存します。

例：

```
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

ステップ 7 **reload**

デバイスがリロードされます。

（注） スループットを設定しているデバイスが物理プラットフォーム上にある場合にのみ、この手順を実行します。

仮想プラットフォームでスループットを設定している場合は、この手順をスキップしてください。

例：

```
Device# reload
```

ステップ 8 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- **物理プラットフォームの場合**：**show platform hardware throughput crypto**
- **仮想プラットフォームの場合**：**show platform hardware throughput level**

デバイスの現在のスループットレベルを表示します。

添付の例：

- 物理プラットフォームでは、階層の値は T2 に設定されています。

  ヒント 物理プラットフォームでは、**show platform hardware qfp active feature ipsec state** 特権 EXEC コマンドを入力して、設定されているスループットレベルを表示することもできます。

- 仮想プラットフォームでは、スループットは 250 Mbps に設定されています。SLAC がインストールされている場合、スループットは自動的に最後に設定された値である T2 に設定されます。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: T2
```

```
     Level is saved, reboot is not required
Current enforced crypto throughput level: 1G
Crypto Throughput is throttled at 2G(Aggregate)
Default Crypto throughput level: 10M
Current boot level is network-premier

OR

Device# show platform hardware throughput level
The current throughput level is 250000 kb/s
```

数値のスループット値から階層への変換

このタスクでは、数値のスループット値を階層ベースのスループット値に変換する方法を示します。数値のスループット値が階層の値にどのようにマッピングされるかを知るには、階層および数値のスループットのマッピング （63 ページ）の表を参照してください。

スループットレベルを変換するには、物理プラットフォーム（Catalyst 8200、8300、および 8500 シリーズ エッジ プラットフォーム）でリロードが必要です。仮想プラットフォーム（Catalyst 8000V エッジソフトウェア）の場合、リロードは必要ありません。

始める前に

- 数値と階層ベースのスループットの設定 （71 ページ）のセクションを参照してください。
- 250 Mbps 以上の数値のスループットを変換する場合は、デバイスに SLAC がインストールされていることを確認してください。HSECK9 ライセンス用の SLAC のインストール （77 ページ）を参照してください。
- このデバイスで実行されているソフトウェアバージョンは、Cisco IOS XE Cupertino 17.7.1 以降のリリースです。

手順

ステップ 1 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**show platform hardware throughput crypto**
- 仮想プラットフォームの場合：**show platform hardware throughput level**

デバイスで現在実行されているスループットを表示します。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: 500M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 500M
Crypto Throughput is throttled at 500M
Default Crypto throughput level: 10M
Current boot level is network-premier
```

```
OR

Device# show platform hardware throughput level
The current throughput level is 100000 kb/s
```

ステップ 2 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**license throughput crypto auto-convert**
- 仮想プラットフォームの場合：**license throughput level auto-convert**

数値のスループットを階層ベースのスループット値に変換します。変換された階層の値は CLI に表示されます。

例：

```
Device# license throughput crypto auto-convert
Crypto throughput auto-convert from level 500M to T2

% These values don't take effect until the next reboot.
Please save the configuration.
*Dec  8 03:21:01.401: %CRYPTO_SL_TP_LEVELS-6-SAVE_CONFIG_AND_RELOAD:
New throughput level
not applied until reload; please save config

OR

Device# license throughput level auto-convert
%Throughput tier set to T1 (100 Mbps)
% Tier conversion is successful.
Please write memory to save the tier config
```

ステップ 3 **copy running-config startup-config**

コンフィギュレーション ファイルに設定を保存します。

（注） 数値から階層ベースのスループットへの変換に使用するコマンドは特権 EXEC コマンドですが、このコマンドは実行コンフィギュレーションを数値から階層ベースの値に変更します。したがって、次のリロードが階層の値とともに表示されるように設定を保存する必要があります。

例：

```
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

ステップ 4 **reload**

デバイスがリロードされます。

（注） リロードは、物理プラットフォームでのみ必要です。

例：

```
Device# reload
Proceed with reload? [confirm]
*Dec  8 03:24:09.534: %SYS-5-RELOAD: Reload requested by console.
Reload Reason:
Reload Command
```

ステップ 5 デバイスが物理デバイスか仮想デバイスかに応じて、該当するコマンドを入力します。

- 物理プラットフォームの場合：**show platform hardware throughput crypto**
- 仮想プラットフォームの場合：**show platform hardware throughput level**

デバイスで現在実行されているスループットを表示します。

例：

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: T2
     Level is saved, reboot is not required
Current enforced crypto throughput level: 1G
Crypto Throughput is throttled at 1G
Default Crypto throughput level: 10M
Current boot level is network-premier


OR

Device# show platform hardware throughput level
The current throughput level is 100000 kb/s
```

ステップ 6 変換が完了したことを確認します。

- 物理プラットフォームの場合：**license throughput crypto auto-convert**
- 仮想プラットフォームの場合：**license throughput level auto-convert**

ヒント　変換が完了したことをクロスチェックするために、変換コマンドを再度入力することもできます。数値のスループット値がすでに変換されている場合は、変換されていることを確認するメッセージが表示されます。

例：

```
Device# license throughput crypto auto-convert
Crypto throughput is already tier based, no need to convert.

OR

Device# license throughput level auto-convert
% Tier conversion not possible since the device is already
in tier licensing
```

数値のスループットをサポートするリリースから階層をサポートするリリースへのアップグレード

Cisco IOS XE Cupertino 17.7.1 以降のリリースにアップグレードし、さらにライセンス PID が階層ベースの場合、スループットの設定を階層ベースの値に変換するか、数値のスループットの設定を保持できます。

（注） CSSM に階層ベースのライセンス PID があり、デバイスで数値のスループット値が設定されている場合、機能への影響はありません。

階層ベースの値に変換する場合は、設定されているスループットレベルに応じて必要なアクションに注意してください。

アップグレード前のスループットの設定	アップグレード前のアクション	17.7.1 以降へのアップグレード後のアクション
250 Mbps 未満	処置は不要です。	数値のスループット値から階層への変換 （86 ページ）
250 Mbps と等しい	T2 に変換する場合は、HSECK9 ライセンスを取得して SLAC をインストールします。	数値のスループット値から階層への変換 （86 ページ）
250 Mbps より大きい	処置は不要です。	数値のスループット値から階層への変換 （86 ページ）

階層をサポートするリリースから数値のスループットのみをサポートするリリースへのダウングレード

数値のスループットの設定のみがサポートされているリリースにダウングレードする場合は、ダウングレードする前に、階層ベースのスループットの設定を数値のスループット値に変換する必要があります。これは、ライセンス PID が階層ベースのライセンス PID である場合でも適用されます。

注意 階層ベースのスループット値がダウングレード前に設定されていて、数値に変更せずにダウングレードした場合、階層の設定は 17.7.1 より前のイメージでは認識されず、設定は失敗します。さらに、スループットがダウングレード前のレベルに復元されない場合があり、ダウングレード後に数値のスループットレベルを設定する必要があります。

ダウングレード前のスループットの設定	ダウングレード前のアクション	17.7.1 より前のバージョンにダウングレードした後のアクション
数値	処置は不要です。	処置は不要です。
階層	数値のスループットの設定 （77 ページ）	処置は不要です。

使用可能なライセンスモデル

ライセンスモデルは、使用するライセンスをシスコへどのように説明するか、または報告するかを定義します。Cisco Catalyst 8000 エッジ プラットフォーム ファミリでは、次のライセンスモデルを使用できます。

ポリシーを使用したスマートライセンス

このライセンスモデルでは、使用するライセンスを購入し、デバイスで設定してから、必要に応じてライセンスの使用状況を報告します。輸出規制ライセンスおよび適用ライセンスを使用している場合を除き、ソフトウェアとそれに関連付けられているライセンスの使用を開始する前に、キーの登録や生成などのライセンス固有の操作を完了する必要はありません。

このライセンスモデルは、Cisco Catalyst 8000 エッジ プラットフォーム ファミリのすべての製品でサポートされています。

詳細については、『Smart Licensing Using Policy for Cisco Enterprise Routing Platforms』を参照してください。

ペイアズユーゴー（PAYG）ライセンス

（注） このライセンスモデルは、Catalyst 8000V エッジソフトウェアでのみ使用できます。

Cisco Catalyst 8000V は、自律モードとコントローラモードの両方で、Amazon Web Services（AWS）および Microsoft Azure Marketplace での PAYG ライセンスモデルをサポートします。Cisco Catalyst 8000V 時間課金 Amazon マシンイメージ（AMI）またはペイアズユーゴー ライセンスモデルでは、指定された期間インスタンスを使用できます。

- 自律モードでは、AWS または Azure Marketplace から直接インスタンスを起動して使用を開始できます。ライセンスはイメージに埋め込まれ、インスタンスを起動すると、選択したライセンスパッケージと設定されたスループットレベルが有効になります。
- Cisco IOS-XE Bengaluru 17.5.1 からサポートされるコントローラモードでは、『Onboard Cisco Catalyst 8000V Edge Software Hosted by a Cloud Service, Using PAYG Licensing』に従って、最初にデバイスを Cisco SD-WAN にオンボードする必要があります。この後、AWS からインスタンスを起動すると、無制限のスループットのためにライセンスがすでにインストールされたデバイスが表示されます。

マネージド サービス ライセンス契約

マネージド サービス ライセンス契約（MSLA）は、サービスプロバイダー向けの購入プログラム契約です。

- **Cisco SD-WAN コントローラモードの MSLA**

Cisco SD-WAN コントローラモードでは、MSLA は Cisco Catalyst 8000 エッジ プラットフォームファミリのすべての製品でサポートされます。詳細については、以下を参照してください。

『Managed Service Licensing Agreement (MSLA) for Cisco SD-WAN At-a-Glance』

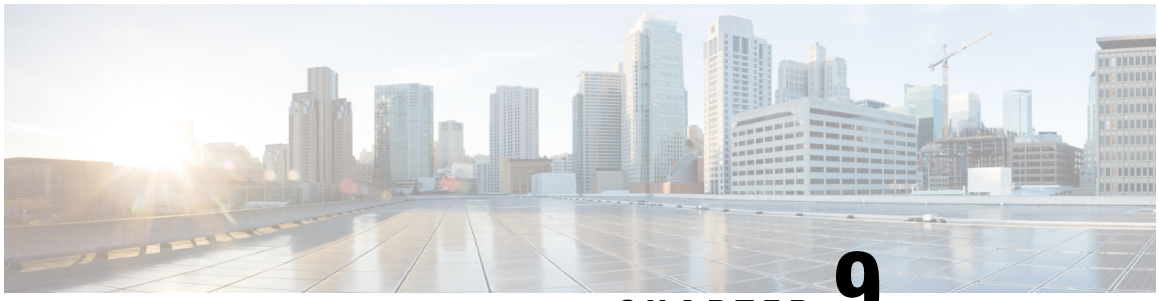
『Cisco SD-WAN Getting Started Guide』→「Manage Licenses for Smart Licensing Using Policy」

『Cisco vManage How-Tos for Cisco IOS XE SD-WAN Devices』→「Manage Licenses for Smart Licensing Using Policy」

- **自律のモードの MSLA**

  自律モードでは、MSLA は Cisco IOS XE Cupertino 17.9.1a 以降の Catalyst 8000V エッジソフトウェアでのみ使用できます。

  詳細については、「MSLA」を参照してください。



CHAPTER 9

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 Catalyst 8500 シリーズ エッジ プラットフォームを実行するために使用されるかについて説明します。

Note このプロセスは、C8500L-8S4X には適用されません。

ここで説明する内容は、次のとおりです。

Cisco Catalyst 8500 シリーズ エッジ プラットフォームの実行：概要

Cisco Catalyst 8500 シリーズ エッジ プラットフォームは、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 Catalyst 8500 シリーズ エッジ プラットフォームの実行：概要

Cisco Catalyst 8500 シリーズ エッジ プラットフォームは、統合パッケージを使用して実行するように設定できます。

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 Catalyst 8500 シリーズ エッジ プラットフォームが統合パッケージファイルを使用して実行するように設定されている場合、ルータ要求の処理に、より多くのメモリが消費されます。これは、要求のたびにルータにより、さらに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実行するように設定された Cisco Catalyst 8500 シリーズ エッジ プラットフォームは、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[0-1]:、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 Catalyst 8500 シリーズ エッジ プラットフォームの実行：概要

ここでは、Cisco Catalyst 8500 シリーズ エッジ プラットフォームの各実行方法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 Catalyst 8500 シリーズ エッジ プラットフォームで管理できます。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 Catalyst 8500 シリーズ エッジ プラットフォームに導入されているより大きな **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 Catalyst 8500 シリーズ エッジ プラットフォーム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構文は、**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 Catalyst 8500 シリーズ エッジ プラットフォーム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 Catalyst 8500 シリーズ エッジ プラットフォーム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Cisco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 Catalyst 8500 シリーズ エッジ プラットフォーム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。

SUMMARY STEPS

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。

DETAILED STEPS

Procedure

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 Catalyst 8500 シリーズ エッジ プラットフォーム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 Cisco 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:/
   11  drwx       16384   Dec 4 2007 04:32:46 -08:00  lost+found
86401  drwx        4096   Dec 4 2007 06:06:24 -08:00  .ssh
14401  drwx        4096   Dec 4 2007 06:06:36 -08:00  .rollback_timer
28801  drwx        4096  Mar 18 2008 17:31:17 -07:00  .prst_sync
43201  drwx        4096   Dec 4 2007 04:34:45 -08:00  .installer
   13  -rw-       45977   Apr 9 2008 16:48:46 -07:00  target_support_output.tgz.tgz
928862208 bytes total (712273920 bytes free)
Router# copy tftp bootflash:



Router# dir bootflash:


Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.

Router# reload
```

request platform software package install コマンドを使用した統合パッケージの管理および設定

次の例では、 **request platform software package install** コマンドを使用して RP 0 上で実行されている統合パッケージをアップグレードしています。また、すべてのプロンプトを無視して（すでに同じ統合パッケージがインストールされている場合など）強制的にアップグレードを実行する **force** オプションを使用しています。

```
Router# request platform software package install rp 0 file bootflash: force

--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Verifying image file locations
Locating image files and validating name syntax
Inspecting image file types
Processing image file constraints
Extracting super package content
Verifying parameters
Validating package type
Copying package files
Checking and verifying packages contained in super package
Creating candidate provisioning file

  WARNING:
  WARNING: Candidate software will be installed upon reboot
  WARNING:

Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
```

```
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
Determining whether installation is valid ... skipped
Checking IPC compatibility with running software
Checking IPC compatibility with running software ... skipped
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Finished compatibility testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned.  New software will load on reboot.
```

Router# **reload**

Note この手順を終了するには、リロードを行う必要があります。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, on page 96 には、統合パッケージを使用してルータをブートするように設定する例と、インストールを終了するためにリロードが実行された結果の例を示します。

インストールコマンドを使用したソフトウェアのインストール

Cisco IOS XE Cupertino 17.7.1a 以降、Cisco Catalyst 8000 エッジプラットフォームはデフォルトでインストールモードで出荷されます。ユーザーは、一連の **install** コマンドを使用して、プラットフォームを起動し、Cisco IOS XE ソフトウェアバージョンにアップグレードまたはダウングレードできます。

インストールコマンドを使用したソフトウェアのインストールに関する制約事項

- 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

Cisco IOS XE Cupertino 17.7.1a リリース以降、インストールモードで出荷されるルータの場合、一連の **install** コマンドを使用して、インストールモードでプラットフォームを起動、アップグレード、およびダウングレードできます。この更新は、Cisco Catalyst 8000 エッジプラットフォームに適用されます。

次の表に、バンドルモードとインストールモードの違いを示します。

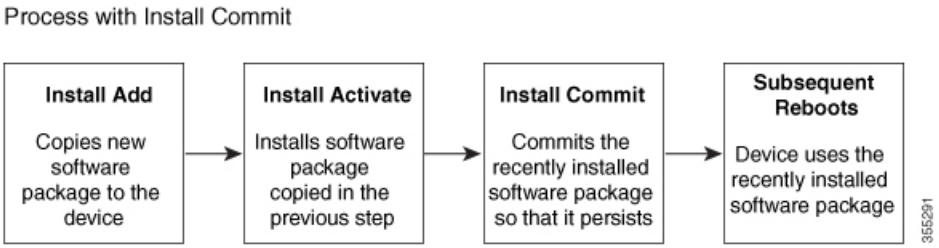
表 *21* : バンドルモードとインストールモード

バンドルモード	インストールモード
このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。	このモードでは、ブートプロセスにローカル（ブートフラッシュ）の packages.conf ファイルを使用します。
このモードでは、1 つの .bin ファイルを使用します。	このモードでは、.bin ファイルは拡張された .pkg ファイルに置き換えられます。
CLI： `#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。
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 *22* : 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 *23 : 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_7_0_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:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin`	ソフトウェア インストール パッケージをリモートの場所（FTP、HTTP、HTTPs、またはTFTP経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよび packages.conf ファイルに展開します。
ステップ 3	**show install summary** 例： `Device#show install summary`	（オプション）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:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin
 activate commit
install_add_activate_commit: START Thu Oct 28 21:57:21 UTC 2021

System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]y
Building configuration...

[OK]Modified configuration has been saved

*Oct 28 21:57:39.818: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
config file
*Oct 28 21:57:39.925: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 one-shot
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.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: 17.07.01.0.1515
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
/bootflash/c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.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

*Oct 28 22:05:49.484: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [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]
*Oct 28 22:06:55.375: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private
config fileSend model notification for install_add_activate_commit before reload
Install will reload the system now!
SUCCESS: install_add_activate_commit  Thu Oct 28 22:07:22 UTC 2021

Router#
*Oct 28 22:07:22.661: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install one-shot PACKAGE
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.binOct
 28 22:07:26.864: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: reload
```

```
action requested

□

Press RETURN to get started!
```

以下は、3 ステップインストールの例です。

```
Router# install add file
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin

install_add: START Thu Oct 28 22:36:43 UTC 2021

*Oct 28 22:36:44.526: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 add
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bininstall_add:
 Adding PACKAGE
install_add: 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: 17.07.01.0.1601
SUCCESS: install_add  Thu Oct 28 22:40:25 UTC 2021

Router#
*Oct 28 22:40:25.971: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install add PACKAGE
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin

Router# 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
[0|install_op_boot(INFO, )]: cleanup_trap  remote_invocation 0 operation install_op_boot
 .. 0 .. 0
[1|display_install_log]: START Thu Oct 28 22:12:11 UTC 2021
[2|install_add]: START Thu Oct 28 22:36:43 UTC 2021
[2|install_add(INFO, )]: Set INSTALL_TYPE to PACKAGE
[2|install_add(CONSOLE, )]: Adding PACKAGE
[2|install_add(CONSOLE, )]: Checking whether new add is allowed ....
[2|install_add(INFO, )]: check_add_op_allowed: Install type PACKAGE
[remote|install_add]: START Thu Oct 28 22:37:12 UTC 2021
[remote|install_add]: END SUCCESS  Thu Oct 28 22:40:10 UTC 2021
[remote|install_add(INFO, )]: cleanup_trap  remote_invocation 1 operation install_add
.. 0 .. 0
[2|install_add(INFO, )]: Remote output from R0
[2|install_add(INFO, )]: install_add: START Thu Oct 28 22:37:12 UTC 2021
Expanding image file:
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
Verifying parameters
Expanding superpackage
bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.bin
... parameters verified
Validating package type
... package type validated
Copying package files
```

```
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
   c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

    c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
  WARNING: A different version of provisioning file packages.conf already exists in
bootflash:
  WARNING: The provisioning file from the expanded bundle will be saved as
  WARNING: bootflash:c8000be-universalk9.BLD_V177_THROTTLE_LATEST_20211027_0.conf
... package files copied
SUCCESS: Finished expanding all-in-one software package.
Image file expanded
SUCCESS: install_add  Thu Oct 28 22:40:10 UTC 2021
[2|install_add]: END SUCCESS  Thu Oct 28 22:40:25 UTC 2021
[2|install_add(INFO, )]: cleanup_trap  remote_invocation 0 operation install_add .. 0
.. 0
[3|COMP_CHECK]: START Thu Oct 28 22:40:26 UTC 2021
[3|COMP_CHECK]: END FAILED exit(1)  Thu Oct 28 22:40:27 UTC 2021
[3|COMP_CHECK(INFO, )]: cleanup_trap  remote_invocation 0 operation COMP_CHECK .. 1 ..
1
[4|install_activate]: START Thu Oct 28 22:42:53 UTC 2021
[4|install_activate(INFO, require user prompt)]: install_cli
[4|install_activate(CONSOLE, )]: Activating PACKAGE
```

```
[4|install_activate(INFO, )]: Acquiring transaction lock...
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: tmp_global_trans_lock: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: tmp lock does not exist: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: tmp_global_trans_lock: /tmp/tmp_install_global_trans_lock
[4|install_activate(INFO, )]: local_trans_lock:
/bootflash/.installer/install_local_trans_lock
[4|install_activate(INFO, )]: global_trans_lock:
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, )]: validate_lock: lock_duration is 7200
[4|install_activate(INFO, )]: install type stored in lock PACKAGE, install type PACKAGE,
 install operation install_activate
[4|install_activate(INFO, )]: lock duration: 7200
[4|install_activate(INFO, )]: extend trans lock done.
/bootflash/.installer/install_global_trans_lock
[4|install_activate(INFO, require user prompt)]: install_cli
[4|install_activate( FATAL)]: Cannot proceed activate because of user input
[4|install_activate(INFO, )]: cleanup_trap  remote_invocation 0 operation install_activate
 .. 6 .. 0
[5|install_add]: START Thu Oct 28 22:45:48 UTC 2021
[5|install_add(INFO, )]: Set INSTALL_TYPE to PACKAGE
[5|install_add(CONSOLE, )]: Adding PACKAGE
[5|install_add(CONSOLE, )]: Checking whether new add is allowed ....
[5|install_add(INFO, )]: check_add_op_allowed: Install type PACKAGE
[5|install_add( FATAL)]: Super package already added. Add operation not allowed. install
 remove inactive can be used to discard added packages

Router# install activate
install_activate: START Thu Oct 28 23:57:57 UTC 2021
install_activate: Activating PACKAGE

*Oct 28 23:57:57.823: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activateFollowing packages shall be activated:
/bootflash/c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
/bootflash/c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.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

*Oct 29 00:04:19.400: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer:
 Install auto abort timer will expire in 7200 seconds  [1] Activate package(s) on R0
    --- Starting list of software package changes ---
```

```
    Old files list:
      Modified
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

      Modified
c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

      Modified
c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

      Modified
c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

      Modified
c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

      Modified
c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

      Modified
c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
      Modified
c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

      Modified
c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

      Modified
c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg
     Modified c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.pkg

    New files list:
      Added
c8000be-firmware_dreamliner.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

      Added
c8000be-firmware_dsp_analogbri.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

      Added
c8000be-firmware_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

      Added
c8000be-firmware_dsp_tilegx.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

      Added
c8000be-firmware_ngwic_t1e1.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
```

```
      Added
c8000be-firmware_nim_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_nim_bri_st_fw.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

      Added
c8000be-firmware_nim_cwan.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_nim_ge.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_nim_shdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_nim_ssd.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_nim_xdsl.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_prince.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_sm_10g.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_sm_1t3e3.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_sm_async.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added
c8000be-firmware_sm_dsp_sp2700.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

      Added
c8000be-firmware_sm_nim_adpt.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg

      Added
c8000be-mono-universalk9.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
      Added c8000be-rpboot.BLD_V177_THROTTLE_LATEST_20211027_030841_V17_7_0_120.SSA.pkg
    Finished list of software package changes
  [1] Finished Activate on R0
Checking status of Activate on [R0]
Activate: Passed on [R0]
Finished Activate

Send model notification for install_activate before reload
Install will reload the system now!
SUCCESS: install_activate  Fri Oct 29 00:05:09 UTC 2021

Router#
*Oct 29 00:05:09.504: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install activate PACKAGEOct 29 00:05:14.494: %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!
```

```
Router# install commit
install_commit: START Fri Oct 29 00:13:58 UTC 2021
install_commit: Committing PACKAGE

--- Starting Commit ---
Performing Commit on Active/Standby

*Oct 29 00:13:59.552: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 commit  [1] Commit package(s) on R0
  [1] Finished Commit on R0
Checking status of Commit on [R0]
Commit: Passed on [R0]
Finished Commit

SUCCESS: install_commit  Fri Oct 29 00:14:03 UTC 2021

Router#
*Oct 29 00:14:03.712: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install commit PACKAGE
```

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

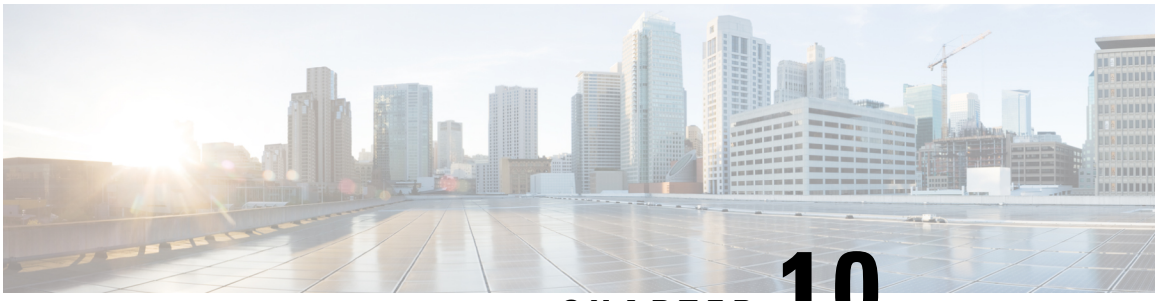
解決法 インストールの概要、ログ、およびソフトウェアバージョンを表示するには、次のshowコマンドを使用します。

- **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。

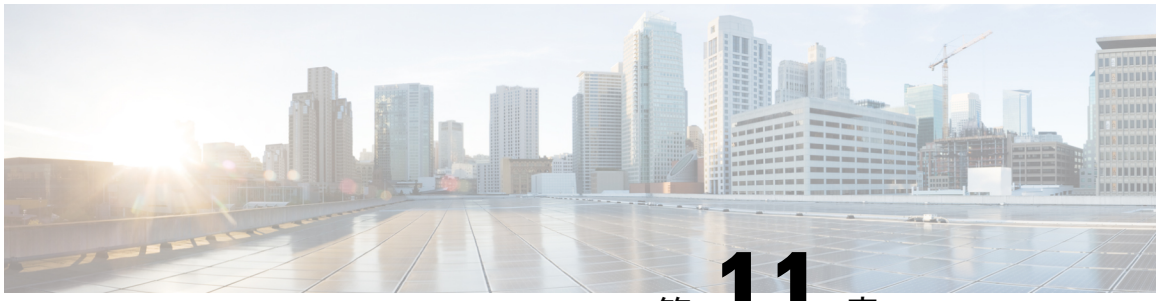


CHAPTER 10

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 11 章

工場出荷時の状態へのリセット（Factory Reset）

この章では、初期設定へのリセット機能と、この機能を使用してルータを保護状態、または以前の完全に機能する状態に復元する方法について説明します。

初期設定へのリセットに関する機能情報

表 *24 :* 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
factory-reset keep-licensing-info コマンドを使用して RUM レポート、SLR、および HSEC キーを保持するオプション	Cisco IOS XE Bengaluru 17.5.1	この機能が導入されました。
セキュアな初期設定へのリセット	Cisco IOS XE Bengaluru 17.6.1	**factory-reset all secure** コマンドが追加されました。

初期設定へのリセットに関する情報

初期設定へのリセットは、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。C8500 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。

Cisco IOS XE Bengaluru 17.6 リリース以降では、**factory-reset all secure** コマンドを使用してルータをリセットし、ブートフラッシュメモリに保存されているファイルを安全にクリアできます。

表 *25 :* 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	コンフィギュレーション レジスタの値
	ライセンス	USB の内容
	ユーザーデータ、スタートアップ コンフィギュレーション、および実行コンフィギュレーション	ログイン情報（セキュアな固有デバイス識別子（SUDI）証明書、公開キーインフラストラクチャ（PKI）キー、および FIPS 関連キー）
	ROMMON 変数	
	すべての書き込み可能ファイルシステムおよび個人データ。 （注） 現在のブートイメージがリモートイメージであるか USB、NIM-SSD などに保存されている場合は、初期設定へのリセットを実行する前に、必ずイメージのバックアップを作成してください。	

コマンド名	消去されるデータ	保持されるデータ
factory-reset keep-licensing-info	• ライセンスブートレベルの設定 • スループットレベルの設定 • スマートライセンス転送タイプ • スマートライセンス URL データ	• リアルユーザーモニタリング（RUM）レポート（オープン/未承認ライセンス使用状況レポート） • 使用状況レポートの詳細情報（受信した最後の ACK、スケジュールされた次の ACK、最後/次のレポートプッシュ） • 固有デバイス ID（UDI）信頼コード • CSSM から受け取った顧客ポリシー • SLAC、SLR 承認コードのリターンコード • 工場出荷時にインストールされた購入情報

初期設定へのリセットプロセスが完了すると、ルータが再起動して ROMMON モードになります。ゼロタッチプロビジョニング（ZTP）機能がセットアップされている場合、ルータが初期設定へのリセット手順を完了すると、ルータは ZTP 設定で再起動します。

初期設定へのリセットのソフトウェアおよびハードウェアサポート

- この機能は、すべての Cisco Catalyst 8500 および 8500L シリーズ エッジ プラットフォームでサポートされています。
- 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、初期設定へのリセットプロセスでは、ブートイメージのバックアップが作成されます。現在のブートイメージがリモートイメージであるかUSB、NIM-SSD などに保存されている場合は、初期設定へのリセットを実行する前に、必ずイメージのバックアップを作成してください。
- イメージがローカルに保存されている場合でも、**factory-reset all secure** コマンドにより、ブートイメージを含むすべてのファイルを消去します。現在のブートイメージがリモートイメージであるか USB、NIM-SSD などに保存されている場合は、初期設定へのセキュアなリセットを実行する前に、必ずイメージのバックアップを作成してください。
- 初期設定へのリセットを実行する前に、ISSU/ISSD（In-Service Software Upgrade または In-Service Software Downgrade）が進行中でないことを確認してください。

初期設定へのリセット実行の制限事項

- ルータにインストールされているソフトウェアパッチは、初期設定へのリセット操作後に復元されません。
- 仮想テレタイプ（VTY）セッションを介して factory reset コマンドが発行された場合、初期設定へのリセットプロセスの完了後にセッションは復元されません。

初期設定にリセットする場合

- 返品許可（RMA）：RMA のためにルータをシスコに返送する場合、すべての機密情報を削除することが重要です。
- ルータの侵害：悪意のある攻撃によってルータのデータが侵害された場合、ルータを初期設定にリセットしてから、今後の使用のためにもう一度設定しなおす必要があります。
- 再利用：ルータを新しいトポロジまたは市場に移動させる必要がある場合、現在のサイトから別のサイトに移動するときにリセットします。

初期設定へのリセットの実行方法

始める前に

表2を参照して、削除および保持する情報を判断します。必要な情報に基づいて、以下に示す適切なコマンドを実行してください。

手順

ステップ 1 Cisco Catalyst 8500 または 8500L デバイスにログインします。

重要 現在のブートイメージがリモートイメージであるかUSBまたはNIM-SSDに保存されている場合は、初期設定へのリセットプロセスを開始する前に、必ずイメージのバックアップを作成してください。

ステップ 2 この手順は 2 つの部分（a と b）に分かれています。**factory-reset** コマンドの実行中にライセンス情報を保持する必要がある場合は、ステップ 2 の a に従います。ライセンス情報を保持する必要がなく、すべてのデータを消去する場合は、ステップ 2 の b を実行します。

a) **factory-reset keep-licensing-info** コマンドを実行してライセンスデータを保持します。

factory-reset keep-licensing-info コマンドを使用すると、次のメッセージが表示されます。

```
Router# factory-reset keep-licensing-info

The factory reset operation is irreversible for Keeping license usage. Are you sure? [confirm]
This operation may take 20 minutes or more. Please do not power cycle.

Dec 1 20:58:38.205: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: process exit with
reload chassis code
/bootflash failed to mount
Dec 01 20:59:44.264: Factory reset operation completed.
Initializing Hardware ...

Current image running: Boot ROM1

Last reset cause: LocalSoft

ISR4331/K9 platform with 4194304 Kbytes of main memory
rommon 1
```

b) **factory-reset all secure 3-pass** コマンドを実行して、すべてのデータを安全に消去します。

factory-reset all secure 3-pass コマンドを使用すると、次のメッセージが表示されます。

```
Router# factory-reset all secure 3-pass

The factory reset operation is irreversible for securely reset all. Are you sure? [confirm]
This operation may take hours. Please do not power cycle.

*Jun 19 00:53:33.385: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.Jun
 19 00:53:42.856: %PMAN-5-EXITACTION:

Enabling factory reset for this reload cycle
  Jun 19 00:54:06.914: Factory reset secure operation. Write 0s. Please do not power cycle.
  Jun 19 01:18:36.040: Factory reset secure operation. Write 1s. Please do not power cycle.
  Jun 19 01:43:49.263: Factory reset secure operation. Write random. Please do not power cycle.
  Jun 19 02:40:29.770: Factory reset secure operation completed.
Initializing Hardware ....
```

ステップ 3 **confirm** と入力して初期設定へのリセットを続行します。

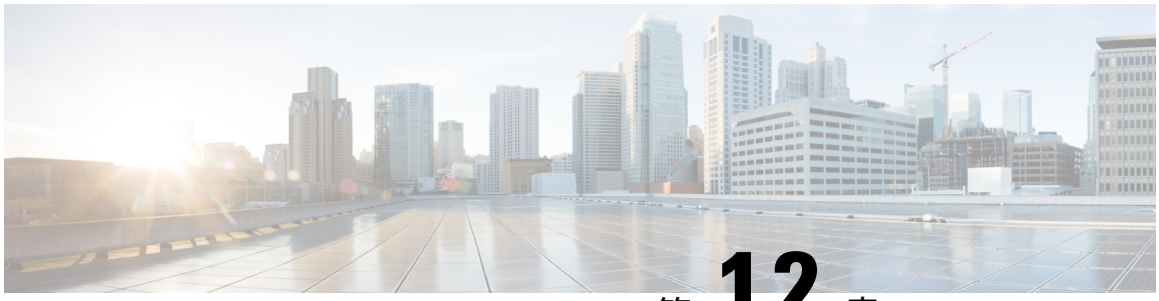
（注） 初期設定へのリセットプロセスの所要時間は、ルータのストレージのサイズによって異なります。これは、高可用性セットアップでは、30 分～ 3 時間延長できます。初期設定へのリセットプロセスを終了する場合は、**Escape** キーを押します。

初期設定へのリセット後の動作

初期設定へのリセットが正常に完了すると、ルータが起動します。ただし、初期設定へのリセットプロセスが開始される前に、コンフィギュレーション レジスタが ROMMON から手動で起動するように設定されていた場合、ルータは ROMMON で停止します。

スマートライセンスを設定したら、**#show license status** コマンドを実行して、インスタンスでスマートライセンスが有効になっているかどうかをチェックします。

（注） 初期設定へのリセットを実行する前に特定ライセンス予約を有効にしていた場合は、同じライセンスを使用し、スマートエージェントから受け取ったライセンスキーを入力します。



第 12 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不備などによって）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機能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。

Cisco IOS XE 17.13.1a 以降、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。

サポートされるプラットフォーム

Cisco IOS XE 17.13.1a 以降、SELinux は次のプラットフォームで有効になっています。

- Cisco 1000 シリーズ アグリゲーション サービス ルータ
- Cisco 1000 シリーズ サービス統合型ルータ
- Cisco 4000 シリーズ サービス統合型ルータ
- Cisco Catalyst 8000v Edge ソフトウェア
- Cisco Catalyst 8200 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8300 シリーズ エッジ プラットフォーム
- Cisco Catalyst 8500 および 8500L シリーズ エッジ プラットフォーム
- Cisco VG シリーズ ゲートウェイ：VG400、VG410、VG420、および VG450
- Cisco 1100 ターミナル サービス ゲートウェイ

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。

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

（注） これらの新しいコマンドは、**サービス内部**コマンドとして実装されます。

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
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

CHAPTER 13

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 Catalyst 8500 シリーズ エッジ プラットフォームの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時にルータのアップタイムを最大化するように設計されているため、すべてのネットワークシナリオで最大アップタイムと復元力が実現します。

このガイドでは、Cisco 8500 シリーズ Catalyst エッジプラットフォーム独自のハイアベイラビリティの特徴について説明します。このマニュアルには、ハイアベイラビリティ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 Catalyst エッジプラットフォーム上と同様に設定され、実装されている他の Cisco ルータで使用できるハイアベイラビリティ機能の説明も掲載していません。この章のほかに、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 Catalyst エッジプラットフォーム上でも同様に動作するハイアベイラビリティ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

ここでは、Cisco 8500 シリーズ Catalyst エッジプラットフォーム上のさまざまなハイアベイラビリティ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 Catalyst エッジプラットフォーム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 Catalyst エッジプラットフォームでは、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 Catalyst エッジプラットフォーム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。

Cisco 8500 シリーズ Catalyst エッジプラットフォームでは、2 番目の IOS プロセスはスタンバイルートプロセッサでのみ実行できます。

2 つの Cisco IOS プロセスの設定

Cisco 8500 シリーズ Catalyst エッジプラットフォームでは、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。

SUMMARY STEPS

1. enable
2. **configure terminal**
3. redundancy

4. mode SSO
5. **exit**
6. reload

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	enable **Example:** `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** **Example:** `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 **Example:** `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 **Example:** `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**
	Example:
	`Router(config)# exit`
	Example:
	`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 **Example:** `Router # reload`	IOS をリロードします。

例

```
Router# configure terminal
Router(config)# redundancy
Router(config)# mode SSO
```

```
Router(config)# exit
Router# reload
```

ステートフル スイッチオーバー

Cisco 8500 シリーズ Catalyst エッジプラットフォームでは、ステートフル スイッチオーバー（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。

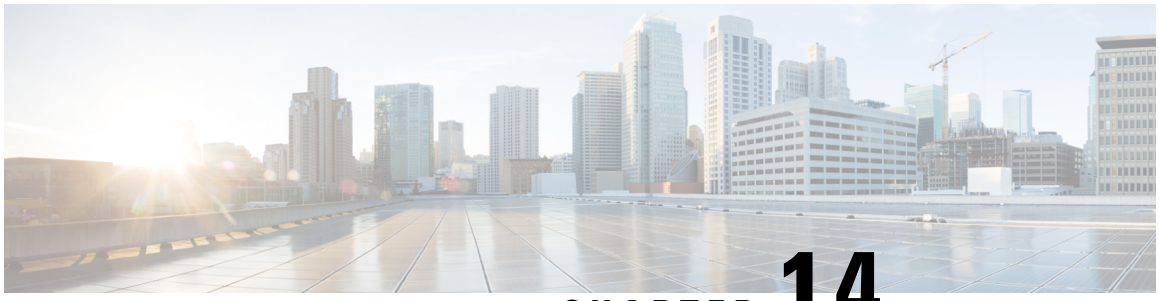
Cisco 8500 シリーズ Catalyst エッジプラットフォームの IPsec は、ステートレス フェールオーバーのみをサポートします。ステートレス フェールオーバーは、ホット スタンバイ ルータ プロトコル（HSRP）のようなプロトコルを使用して、プライマリからセカンダリへのカットオーバーを行い、さらにアクティブおよびスタンバイの VPN ゲートウェイを許可して、共通の仮想 IP アドレスを共有することができます。

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 Catalyst エッジプラットフォームでは、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。



CHAPTER 14

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 Catalyst エッジプラットフォームには、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, on page 149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。

ポートには、Cisco 8500 シリーズ Catalyst エッジプラットフォームの他のポートと同様に、設定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 Catalyst エッジプラットフォームでは、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 モードの **ip address** コマンド）を使用して設定できます。

Cisco 8500 シリーズ Catalyst エッジプラットフォーム上で IOS プロセスが開始しない場合、ROMmon 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 Catalyst エッジプラットフォーム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 Catalyst エッジプラットフォーム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。

ここでは、Cisco 8500 シリーズ Catalyst エッジプラットフォーム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
```

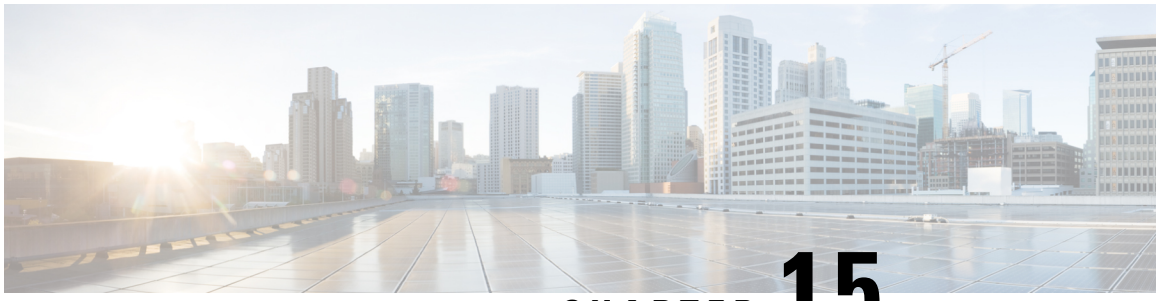
TACACS+ サーバーグループの例

```
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
```



CHAPTER 15

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 Catalyst エッジプラットフォームは、レイヤ 3 IP にレイヤ 2 イーサネットセグメントをパッケージングするためのブリッジドメインのインターフェイス（BDI）機能をサポートします。

- ブリッジ ドメイン インターフェイスの制約事項, on page 155
- ブリッジ ドメイン インターフェイスに関する情報, on page 156
- ブリッジドメイン仮想 IP インターフェイスの設定 （165 ページ）

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 Catalyst 8500 シリーズ エッジ プラットフォームのすべてのブリッジ ドメイン インターフェイスは、共通の 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。

Note **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 Catalyst エッジプラットフォームを有効にし、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。

Note 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。

Note 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}	
{emdash を開始}{emdash を終了}	**Shutdown**	**No Shutdown**
No faults asserted	Admin-down	Up
At least one fault asserted	Admin-down	Operationally-Down

ブリッジ ドメイン インターフェイスの統計情報

ブリッジ ドメイン インターフェイスなどの仮想インターフェイスの場合は、プロトコル カウンタは QFP から定期的に検索されます。

パケットがレイヤ 2 ブリッジ ドメイン ネットワークからドメインのインターフェイスを介してレイヤ 3 のルーティング ネットワークに流れると、パケットはブリッジ ドメイン インターフェイスの入力パケットおよびバイトとして処理されます。パケットがレイヤ3インターフェイスに到達し、ブリッジ ドメイン インターフェイスを介してレイヤ 2 ブリッジ ドメインに転送されると、パケットは出力パケットおよびバイトとして処理され、カウンタが適宜更新されます。

BDI はすべての Cisco IOS インターフェイスで、ケースとしてレイヤ 3 パケット カウンタの標準セットを維持します。レイヤ 3 のパケット カウンタを表示するには、show interface コマンドを使用します。

カウンタの表記法は、レイヤ 3 クラウドに関連しています。たとえば、input はレイヤ 2 BD からレイヤ 3 クラウドに入るトラフィックを示し、output はレイヤ 3 クラウドからレイヤ 2 BD に向かうトラフィックを示します。

BDI ステータスの統計情報を表示するには、**show interfaces accounting** コマンドを使用します。送受信されるパケットおよびバイト全体のカウントを表示するには、**show interface** <*if-name*> コマンドを使用します。

ブリッジ ドメイン インターフェイスの作成または削除

Cisco IOS ルータのインターフェイスまたはサブインターフェイスを定義する場合は、名前を付け、どのように IP アドレスに割り当てられるかを指定します。システム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。

Note 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 Catalyst エッジプラットフォーム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。

***Table 26: Cisco 8500* シリーズ *Catalyst* エッジプラットフォーム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 Catalyst 8500 シリーズ エッジ プラットフォームでサポートされる BD-VIF の最大数は次のとおりです。

- C8500-12X4QC 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。
- C8500-12X は、ブリッジドメインに対して最大 16 の BD-VIF をサポートします。

Cisco IOS XE 17.7 リリースから、BD-VIF は Flexible Netflow（FnF）をサポートします。

ブリッジ ドメイン インターフェイスの設定方法

ブリッジ ドメイン インターフェイスを設定するには、次の手順を実行します。

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface BDI** *{interface number}*
4. **encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]*
5. 次のいずれかを実行します。
6. **match security-group destination tag** *sgt-number*
7. **mac address** *{mac-address}*
8. **no shut**
9. **shut**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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** **Example:** `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}* **Example:** `Router(config-if)# interface BDI3`	Cisco 8500 シリーズ Catalyst エッジプラットフォームのブリッジ 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>]* **Example:** `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。 **Example:** **ip address** *ip-address mask*	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。

	Command or Action	Purpose

	Example:
	
	Example:
	ipv6 address *{X:X:X:X::X* **link-local**| *X:X:X:X::X/prefix [***anycast** | **eui-64***]* | **autoconfig** *[***default***]}*
	Example:
	`Router(config-if)# ip address 2.2.2.1 255.255.255.0`
	Example:
	
	Example:
	`Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64`	

ステップ 6	**match security-group destination tag** *sgt-number* **Example:** `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}* **Example:** `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** **Example:** `Router(config-if)# no shut`	Cisco 8500 シリーズ Catalyst エッジプラットフォームのブリッジ 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** **Example:** `Router(config-if)# shut`	Cisco 8500 シリーズ Catalyst エッジプラットフォームのブリッジ 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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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** **Example:** `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** **Example:** `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** **Example:** `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** **Example:**	選択した CPP L2BD Client のデバッグがオンになります。

	Command or Action	Purpose
	`Router# debug platform hardware qfp active feature l2bd client all`	
ステップ 6	**platform trace runtime process forwarding-manager module** **Example:** `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** **Example:** `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。

What to do next

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

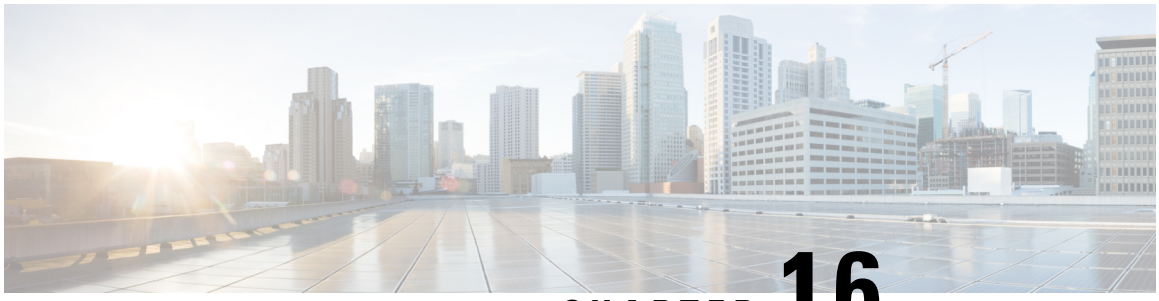
show pla sof inter fp ac brief | i BD_VIF

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
```



CHAPTER 16

パケットトレース

初版：2016 年 8 月 3 日

パケットトレース機能は、Cisco IOS XE プラットフォームによってデータパケットがどのように処理されているのかを詳細に理解できます。これは、ユーザーが問題を診断し、より効率的にトラブルシューティングするために役立ちます。このモジュールは、パケットトレース機能の使用方法に関する情報を提供します。

パケットトレースについて

パケットトレース機能は、アカウンティング、サマリー、パスデータという 3 つのレベルのパケット検査を提供します。各レベルは、一部のパケット処理機能を犠牲にして、パケット処理の詳細なビューを提供します。ただし、パケットトレースは、debug platform condition ステートメントに一致するパケットの検査を制限し、大量のトラフィックが発生する環境下でも実行可能なオプションです。

次の表で、パケットトレースによって提供される 3 つのレベルの検査について説明します。

Table 27: パケットトレースレベル

パケットトレースレベル	説明
アカウンティング	パケットトレースのアカウンティングでは、ネットワークプロセッサに出入りするパケット数が示されます。パケットトレースのアカウンティングは負荷の軽いパフォーマンス アクティビティであり、無効化されるまで継続的に実行されます。
サマリー	パケットトレースのサマリーレベルでは、限られた数のパケットデータが収集されます。パケットトレースのサマリーは、入力インターフェイスと出力インターフェイス、最終的なパケットの状態、およびパケットのパント、ドロップ、インジェクションを随時追跡します。サマリーデータの収集は、通常のパケット処理と比較してパフォーマンスが高く、問題のあるインターフェイスを分離するのに役立ちます。
パスデータ	パケットトレースのパスデータレベルでは、パケットトレースが最も詳細なレベルで実行されます。限られた数のパケットを対象にデータが収集されます。パケットトレースのパスデータでは、条件付きデバッグ ID を含むデータがキャプチャされます。このデータは、機能デバッグ、タイムスタンプ、および機能固有のパストレースデータと関連付ける際に役立ちます。 パスデータには、パケットコピーと Feature Invocation Array（FIA）トレースという 2 つのオプション機能もあります。パケットコピーオプションを使用すると、パケットの各種レイヤ（レイヤ 2、レイヤ 3、レイヤ 4）で入力パケットや出力パケットをコピーできます。FIA トレースオプションは、パケット処理中に呼び出されたすべての機能エントリを追跡します。このオプションは、パケット処理中に何が起こっているかを把握する際に役立ちます。 **Note** 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。

Note 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。

SUMMARY STEPS

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**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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）。

	Command or Action	Purpose
ステップ 2	**debug platform packet-trace packet** *pkt-num* **[fia-trace | summary-only] [circular] [data-size** *data-size***]** **Example:** `Router# debug platform packet-trace packets 2048 summary-only`	指定した数のパケットのサマリーデータを収集します。デフォルトでは機能パスデータをキャプチャし、必要に応じて FIA トレースを実行します。 *pkt-num*：所定の時間に維持されるパケットの最大数を指定します。 **fia-trace**：サマリーデータ、機能固有のデータなど、詳細なレベルのデータキャプチャを実行します。また、パケット処理中にアクセスされた各機能エントリも表示します。 **summary-only**：詳細情報を最小限にしたサマリーデータのキャプチャを有効にします。 **circular**：最近トレースされたパケットのデータを保存します。 *data-size*：各パケットの機能データと FIA トレースデータを保存するデータバッファのサイズをバイト単位で指定します。パケットで非常に重いパケット処理が実行された場合、ユーザーは必要に応じてデータバッファのサイズを増やすことができます。デフォルト値は 2048 です。
ステップ 3	**debug platform packet-trace {punt |inject|copy|drop|packet|statistics}** **Example:** `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]** **Example:** `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** **Example:** `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** **Example:** `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。

	Command or Action	Purpose
ステップ 7	**show platform packet-trace {configuration | statistics | summary | packet {all | *pkt-num*}}** **Example:** `Router# show platform packet-trace 14`	指定されたオプションに従って、パケットトレースデータを表示します。**show** コマンドのオプションの詳細については、{start cross reference} 表 21-1 {end cross reference} を参照してください。
ステップ 8	**clear platform condition all** **Example:** `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** **Example:** `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。

SUMMARY STEPS

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**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `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** **Example:** `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*
	Example:
	`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* **Example:** `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

	Command or Action	Purpose
		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*} **Example:** `Router(config)# ip access-list extended acl2`	拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。拡張 ACL は、IP パケットの送信元アドレスおよび宛先アドレスを ACL に設定されているアドレスと比較して、トラフィックを制御します。
ステップ 6	**ip access-list extended { deny | permit } udf udf-name value mask** **Example:** `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]** **Example:** `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** **Example:** `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***]** **Example:** `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。

	Command or Action	Purpose
		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10	**debug platform packet-trace {punt | inject|copy | drop |packet | statistics}** **Example:** `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** **Example:** `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** **Example:** `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。

***Table 28: 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。

コマンド	説明
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。

***Table 29: 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 Cisco ASR 1006 ルータの NAT 設定でパケットドロップのトラブルシューティングを行うシナリオの例を示します。この例には、パケットトレース機能によって提供される詳細レベルを効果的に利用して問題に関する情報を収集し、問題を切り分けて、解決策を見つける方法が示されています。

このシナリオでは、問題があることはわかりますが、どこからトラブルシューティングを開始すればよいかはわかりません。したがって、多数の着信パケットのパケットトレースのサマリーにアクセスすることを検討する必要があります。

```
Router# debug platform condition ingress
Router# debug platform packet-trace packet 2048 summary-only
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Pkt   Input             Output            State  Reason
0     Gi0/0/0           Gi0/0/0           DROP   402 (NoStatsUpdate)
1     internal0/0/rp:0  internal0/0/rp:0  PUNT   21  (RP<->QFP keepalive)
2     internal0/0/recycle:0  Gi0/0/0      FWD
```

この出力には、ギガビット イーサネット インターフェイス 0/0/0 の NAT 設定が原因でパケットがドロップされていることが示されています。これによって、問題は特定のインターフェイスで発生していることがわかります。この情報を使用して、トレースするパケットを制限し、データキャプチャのパケット数を減らし、検査レベルを上げることができます。

```
Router# debug platform packet-trace packet 256
Router# debug platform packet-trace punt
Router# debug platform condition interface Gi0/0/0
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Router# show platform packet-trace 15
Packet: 15          CBUG ID: 238
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:1
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 1166288346725 ns (06/06/2016 09:09:42.202734 UTC)
    Stop    : 1166288383210 ns (06/06/2016 09:09:42.202770 UTC)
Path Trace
  Feature: IPV4
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.64.68.3
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985
IOSd Path Flow: Packet: 15    CBUG ID: 238
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From CPP
  Feature: IP
    Pkt Direction: IN
    Source      : 10.64.68.122
    Destination : 10.64.68.255
```

```
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.64.68.122
    Destination : 10.64.68.255
    Interface   : GigabitEthernet0/0/0
  Feature: UDP
    Pkt Direction: IN
    src         : 10.64.68.122(1053)
    dst         : 10.64.68.255(1947)
    length      : 48

Router#show platform packet-trace packet 10
Packet: 10          CBUG ID: 10
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:0
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 274777907351 ns (01/10/2020 10:56:47.918494 UTC)
    Stop    : 274777922664 ns (01/10/2020 10:56:47.918509 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.78.106.2
    Destination : 224.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985

IOSd Path Flow: Packet: 10    CBUG ID: 10
  Feature: INFRA
    Pkt Direction: IN
Packet Rcvd From DATAPLANE
 Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.78.106.2
    Destination : 224.0.0.102
    Interface   : GigabitEthernet0/0/0

  Feature: UDP
    Pkt Direction: IN DROP
    Pkt : DROPPED
    UDP: Discarding silently
    src        : 881 10.78.106.2(1985)
    dst         : 224.0.0.102(1985)
    length      : 60

Router#show platform packet-trace packet  12
Packet: 12          CBUG ID: 767
Summary
  Input     : GigabitEthernet3
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 16120990774814 ns (01/20/2020 12:38:02.816435 UTC)
    Stop    : 16120990801840 ns (01/20/2020 12:38:02.816462 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 12.1.1.1
```

```
    Destination : 12.1.1.2
    Protocol    : 6 (TCP)
      SrcPort   : 46593
      DstPort   : 23
IOSd Path Flow: Packet: 12    CBUG ID: 767
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 12.1.1.1
    Destination : 12.1.1.2
    Interface   : GigabitEthernet3

  Feature: IP
    Pkt Direction: IN
    FORWARDEDTo transport layer
    Source        : 12.1.1.1
    Destination   : 12.1.1.2
    Interface     : GigabitEthernet3

  Feature: TCP
    Pkt Direction: IN
    tcp0: I NoTCB 12.1.1.1:46593 12.1.1.2:23 seq 1925377975 OPTS 4 SYN  WIN 4128
```

```
Router# show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
0     INJ.2                     Gi1                       FWD
1     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
2     INJ.2                     Gi1                       FWD
3     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
4     INJ.2                     Gi1                       FWD
5     INJ.2                     Gi1                       FWD
6     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
7     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
8     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
9     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
10    INJ.2                     Gi1                       FWD
11    INJ.2                     Gi1                       FWD
12    INJ.2                     Gi1                       FWD
13    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
14    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
15    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
16    INJ.2                     Gi1                       FWD
```

次に、パケットトレースデータの統計を表示する例を示します。

```
Router#show platform packet-trace statistics
Packets Summary
  Matched  3
  Traced   3
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     3
    Count       Code  Cause
    3           56    RP injected for-us control
  Drop     0
  Consume  0

          PKT_DIR_IN
```

```
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              0
IP               0              0              0
IPV6             0              0              0
ARP              0              0              0

         PKT_DIR_OUT
             Dropped       Consumed       Forwarded
INFRA            0              0              0
TCP              0              0              0
UDP              0              0              0
IP               0              0              0
IPV6             0              0              0
ARP              0              0              0
```

次に、コントロールプレーンからフォワーディングプロセッサに挿入およびパントされるパケットを表示する例を示します。

```
Router#debug platform condition ipv4 10.118.74.53/32 both
 Router#Router#debug platform condition start
Router#debug platform packet-trace packet 200
Packet count rounded up from 200 to 256

Router#show platform packet-tracer packet 0
show plat pack pa 0
Packet: 0           CBUG ID: 674
Summary
  Input     : GigabitEthernet1
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 17756544435656 ns (06/29/2020 18:19:17.326313 UTC)
    Stop    : 17756544469451 ns (06/29/2020 18:19:17.326346 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      : <unknown>
    Source      : 10.118.74.53
    Destination : 198.51.100.38
    Protocol    : 17 (UDP)
      SrcPort   : 2640
      DstPort   : 500

IOSd Path Flow: Packet: 0    CBUG ID: 674
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
  Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.118.74.53
    Destination : 198.51.100.38
    Interface   : GigabitEthernet1

  Feature: IP
  Pkt Direction: IN
  FORWARDED To transport layer
    Source        : 10.118.74.53
    Destination   : 198.51.100.38
    Interface     : GigabitEthernet1
```

```
  Feature: UDP
  Pkt Direction: IN
  DROPPED
 UDP: Checksum error: dropping
 Source      : 10.118.74.53(2640)
 Destination : 198.51.100.38(500)

Router#show platform packet-tracer packet 2
Packet: 2           CBUG ID: 2

IOSd Path Flow:
  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
 OPTS 4 ACK 2346709419 SYN  WIN 4128

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


  Feature: IP
  Pkt Direction: OUTRoute out the generated packet.srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

  Feature: IP
  Pkt Direction: OUTInject and forward successful srcaddr: 198.51.100.38, dstaddr:
198.51.100.55

  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 198.51.100.38:22 198.51.100.55:52774 seq 3052140910
 OPTS 4 ACK 2346709419 SYN  WIN 4128
Summary
  Input     : INJ.2
  Output    : GigabitEthernet1
  State     : FWD
  Timestamp
    Start   : 490928006866 ns (06/29/2020 13:31:30.807879 UTC)
    Stop    : 490928038567 ns (06/29/2020 13:31:30.807911 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : internal0/0/rp:0
    Output      : <unknown>
    Source      : 172.18.124.38
    Destination : 172.18.124.55
    Protocol    : 6 (TCP)
      SrcPort   : 22
      DstPort   : 52774
  Feature: IPSec
    Result    : IPSEC_RESULT_DENY
    Action    : SEND_CLEAR
    SA Handle : 0
    Peer Addr : 55.124.18.172
    Local Addr: 38.124.18.172


Router#
```

その他の参考資料

標準

標準	タイトル
なし	—

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 {start hypertext}http://www.cisco.com/go/mibs{end hypertext}

RFC

RFC	タイトル
なし	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	{start hypertext}http://www.cisco.com/cisco/web/support/index.html{end hypertext}

パケットトレースの機能情報

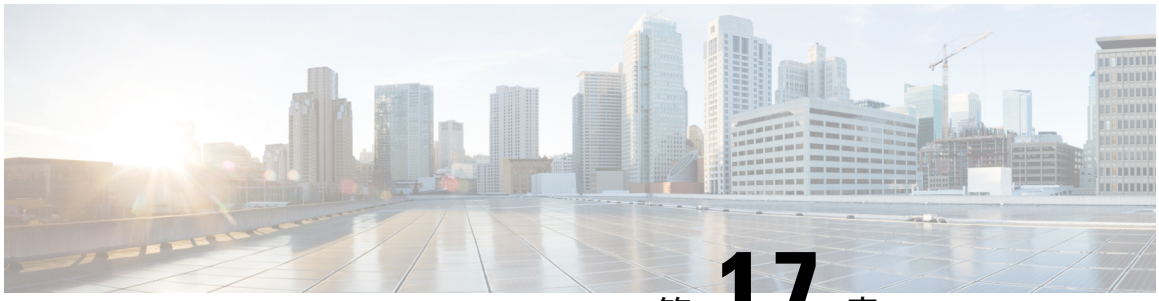
{start cross reference}表 21-4{end cross reference} に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator にアクセスするには、{start hypertext} http://www.cisco.com/go/cfn{end hypertext} に進みます。Cisco.com のアカウントは必要ありません。

Note {start cross reference}表 21-4{end cross reference} には、特定のソフトウェア リリース トレインで各機能をサポートするソフトウェアリリースだけが示されています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

Table 30: パケットトレースの機能情報

機能名	リリース	機能情報
パケットトレース	Cisco IOS XE 3.10S	パケットトレース機能は、Cisco IOS XE ソフトウェアによるデータパケットの処理方法に関する情報を提供します。 Cisco IOS XE リリース 3.10S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 次のコマンドが導入または変更されました。 • **debug platform packet-trace packet** *pkt-num* [**fia-trace** | **summary-only**] [**data-size** *data-size*] [**circular**] • **debug platform packet-trace copy packet** {**input** | **output** | **both**} [**size** *num-bytes*] [**L2** | **L3** | **L4**] • **show platform packet-trace** {**configuration** | **statistics** | **summary** | **packet** {**all** | *pkt-num*}}
	Cisco IOS XE 3.11S	Cisco IOS XE リリース 3.11S で、この機能が拡張され、次の機能が含まれるようになりました。 • 一致した統計と追跡された統計。 • トレース開始タイムスタンプに加えて、トレース停止タイムスタンプ。 次のコマンドが導入または変更されました。 • **debug platform packet-trace drop** [**code** *drop-num*] • **show platform packet-trace packet** {**all** | *pkt-num*} [*decode*]
	Cisco IOS XE Denali 16.3.1	Cisco IOS XE Denali 16.3.1 で、この機能が拡張され、IOSd とともにレイヤ 3 パケットトレースが含まれるようになりました。 次のコマンドが導入または変更されました。**debug platform packet-trace punt**.
	Cisco IOS XE Amsterdam 17.3.1	**show platform packet-trace** コマンドの出力に、IOSd から発信されたパケットか、IOSd または他の BinOS プロセス宛のパケットに関する追加のトレース情報が含まれるようになりました。



第 17 章

パケット ドロップ

このマニュアルでは、Cisco ASR 1000 シリーズ アグリゲーション サービス 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

全体的なパケットフロー

Cisco ASR 1000 シリーズ ルータは、システムの次の機能要素で構成されています。

- • Cisco ASR 1000 シリーズ ルートプロセッサ（RP）
- • Cisco ASR 1000 シリーズ Embedded Services Processor（ESP）
- • Cisco ASR 1000 シリーズ SPA インターフェイスプロセッサ（SIP）またはモジュラ インターフェイス プロセッサ

Cisco ASR 1000 シリーズ ルータは、ハードウェアアーキテクチャとして Cisco Quantum Flow Processor（QFP）を導入しています。QFP ベースのアーキテクチャでは、すべてのパケットが ESP を介して転送されるため、ESP で問題が発生すると、転送が停止します。

パケットドロップの表示

Cisco IOS XE 17.6 以降では、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	**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。

（注） ラッパーコマンド **show drops history qfp** は、Catalyst 8500L エッジプラットフォームでは使用できません。

```
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

Cisco IOS XE 17.14 以降では、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	**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	**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。 • ラッパーコマンド **show drops thresholds** は現在、Catalyst 8500L エッジプラットフォームでは使用できません。

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
```

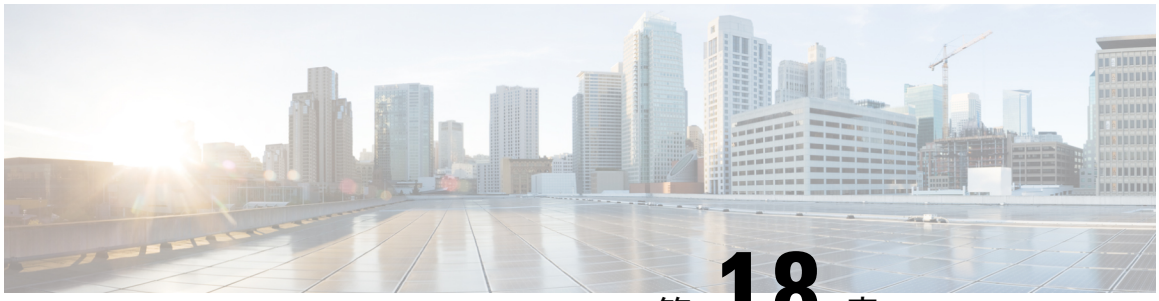
パケットドロップの機能情報

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 *31* : パケットドロップの機能情報

機能名	リリース	機能情報
パケットドロップ情報の表示	Cisco IOS XE 17.13.1a	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。
QFP ドロップのしきい値と警告	IOS XE 17.14.1a	Cisco IOS XE 17.14.1a 以降では、この機能により、各ドロップ原因の警告しきい値と、1 秒あたりの QFP ドロップ合計数を設定できます。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。 Cisco ASR 1000 シリーズおよび Catalyst 8500 シリーズ エッジ プラットフォームでは、**platform qfp drops threshold** コマンドを使用してしきい値を設定できます。
パケットドロップ履歴	IOS XE 17.13.1a	Cisco IOS XE 17.13.1a 以降では、**show drops history qfp** コマンドを使用して、Cisco ASR 1000 シリーズおよび Catalyst 8500 シリーズエッジプラットフォームでの QFP ドロップの履歴を表示できます。



第 18 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 *32 : 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 17.7.1a	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

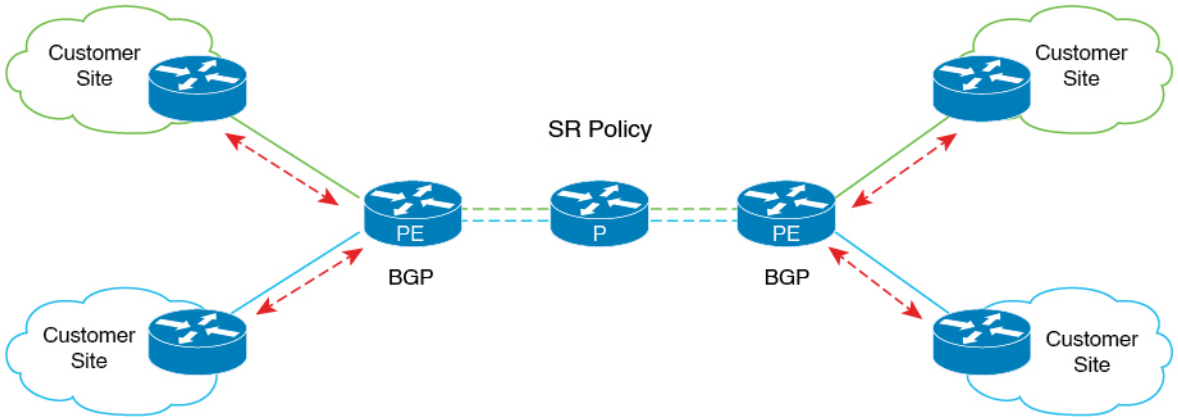
- SR オンデマンドネクストホップ（ODN）ポリシーはサポートされていません。SR 静的ポリシーのみがサポートされます。
- SR フロー単位ポリシー（PFP）はサポートされていません。SR 宛先単位ポリシー（PDP）のみがサポートされています。
- 内部ゲートウェイプロトコル（IGP）は Intermediate System-to-Intermediate system（IS-IS）です。

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 *2 : 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。

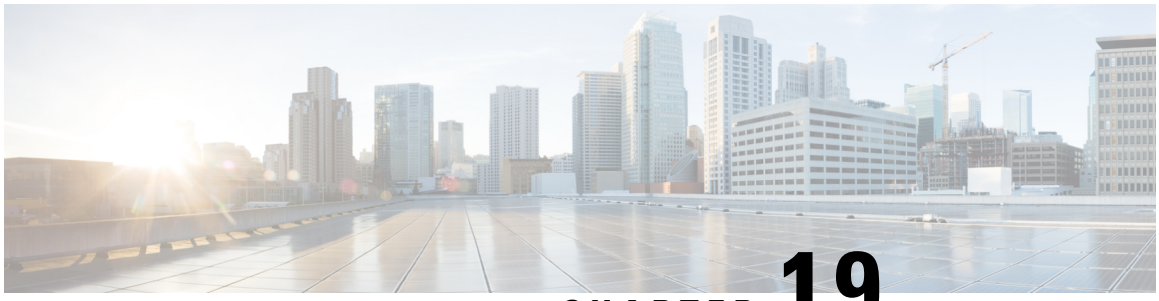
```
device# show l2vpn evpn vpws VC ID 100 detail
EVPN name: vc100, state: up, type: point-to-point
  EVPN ID: 100
  VPWS Service Instance ID: Source 1, Target 2
  Labels: Local 17, Remote 17
  Next Hop Address: 6.6.6.6
  Associated member interface Gi0/0/3 up, Gi0/0/3:3000 status is up
  Output interface: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



CHAPTER 19

SFP+ の設定

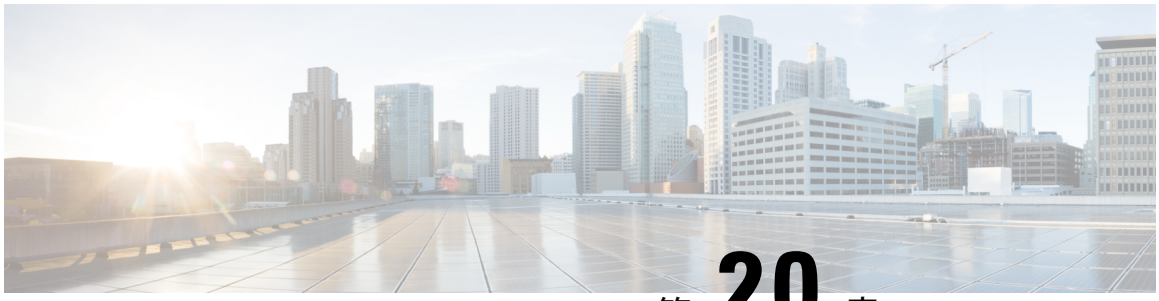
SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	**enable** *source-interface gigabitethernet slot/port* **Example:** `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** **Example:** `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* **Example:** `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。



第 20 章

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

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

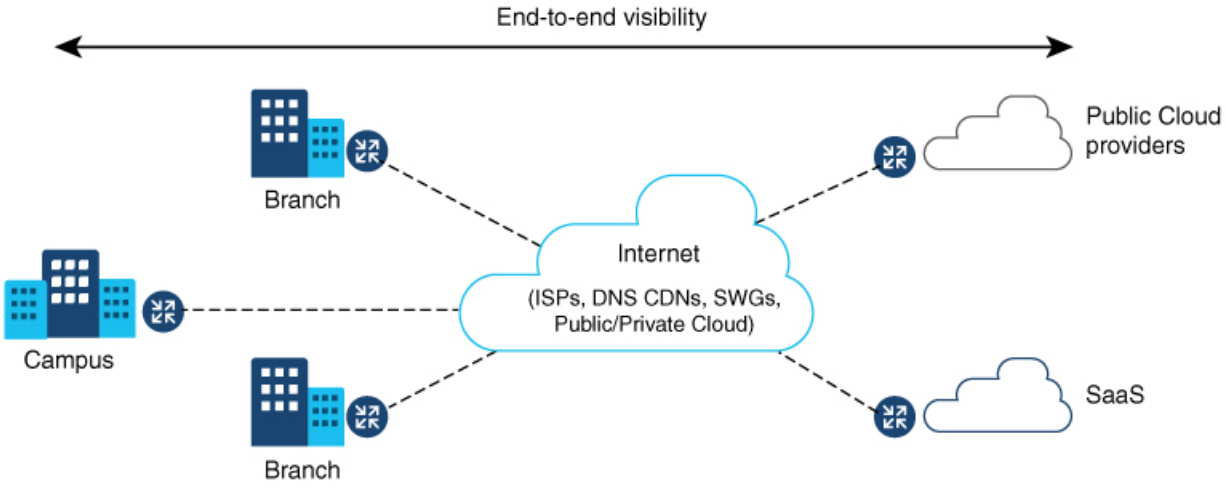
Cisco ThousandEyes エンタープライズ エージェント アプリケーションのホスティング

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

Cisco IOS XE リリース 17.8.1 以降、アプリケーション ホスティング機能を使用して、Cisco ThousandEyes エンタープライズ エージェントをコンテナアプリケーションとして Cisco Catalyst 8500 および Catalyst 8500L シリーズ エッジ プラットフォームに展開できます。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 *3 : ThousandEyes* アプリケーションによるネットワークの表示



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

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

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

表 *33 : 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 17.8.1	アプリケーション ホスティング機能をコンテナとして使用して、ルーティング プラットフォームで実行される ThousandEyes エージェント アプリケーションを統合することで、インターネット、クラウドプロバイダー、およびエンタープライズ ネットワークに関する詳細な分析情報を用いてアプリケーション エクスペリエンスを可視化できます。

サポートされるプラットフォームとシステム要件

次の表に、サポートされるプラットフォームとシステム要件を示します。

プラットフォーム	ブートフラッシュ	FRU ストレージ	DRAM
Cisco Catalyst 8500 シリーズ エッジプラットフォーム			
C8500-12X4QC	32 GB	（デフォルト）32 GB eUSB（オプション）HDD	16 GB
C8500-12X	32 GB	（デフォルト）32 GB eUSB（オプション）HDD	16 GB
Cisco Catalyst 8500L シリーズ エッジ プラットフォーム			
C8500L-8S4X	16 GB	（デフォルト）32GB M.2 USB	16 GB

（注） Cisco ThousandEyes エンタープライズ エージェントを実行するための最小限の DRAM およびブートフラッシュストレージ要件は 8GB です。デバイスに十分なメモリまたはストレージがない場合は、DRAM をアップグレードするか、SSD/M.2 USB などの外部ストレージを追加することを推奨します。使用可能なリソースが他のアプリケーションを実行するのに十分でない場合、Cisco IOx はエラーメッセージを生成します。

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

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

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 4.2.2 を使用していることを確認します。

ステップ 3 デバイスでイメージをコピーします。

ステップ 4 イメージをインストールして起動します。

ステップ 5 エージェントをコントローラに接続します。

（注） Cisco IOS XE 17.8.1 ソフトウェアとともに Cisco ThousandEyes アプリケーションパッケージをサポートするプラットフォームを注文した場合、Cisco ThousandEyes アプリケーションパッケージはデバイスのブートフラッシュで使用できます。

Cisco ThousandEyes アプリケーションをホストするワークフロー

アプリケーションをインストールして起動するには、次の手順を実行します。

始める前に

Cisco ThousandEyes ポータルで新しいアカウントを作成し、トークンを生成します。Cisco ThousandEyes エージェント アプリケーションは、このトークンを使用して認証し、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 （211 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 C8500-L プラットフォームでは、次のコマンドを使用してデバイスを app-heavy モードに変換し、デバイスをリロードします。

```
Device(config)#platform resource app-heavy
Please reboot to activate this template

C8500L(config)#end
C8500L#wr mem
```

```
Building configuration...
[OK]
C8500L#

C8500L#reload
Proceed with reload? [confirm]
```

ステップ 8 ThousandEyes アプリケーションをインストールします。

```
app-hosting install appid <appid> package [bootflash: | harddisk: | https:]
```

次のオプションから ThousandEyes アプリケーションをインストールする場所を選択します。

```
Device# app-hosting install appid te package ?
          bootflash:  Package path □ ISR4K case if image is locally available in bootflash:
          harddisk:   Package path □ Cat8K case if image is locally available in M.2 USB
          https:      Package path □ Download over the internet if image is not locally present in
 router. URL to ThousandEyes site hosting agent image to be provided here
```

ステップ 9 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。