



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

初版：2020年8月20日

最終更新：2022年2月16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 1
	目標 1
	マニュアルの変更履歴 1
	通信、サービス、およびその他の情報 2

第 2 章	最初にお読みください 3
-------	--------------

第 3 章	概要 5
-------	------

第 4 章	ソフトウェアの実装およびアーキテクチャ 7
	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 7
	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 7
	統合パッケージ 7
	統合パッケージについての重要事項 8
	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 8
	個別のサブパッケージに関する重要事項 9
	プロビジョニング ファイル 9
	プロビジョニング ファイルについての重要事項 9
	ROMmon イメージ 10
	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 10
	プロセスの概要 11
	プロセスとしての IOS 11
	デュアル IOS プロセス 11
	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 11

自動生成されるファイルディレクトリおよびファイル 12

自動生成されるディレクトリに関する重要事項 13

第 5 章

IOS-XE と SDWAN の展開 15

概要 15

機能制限 15

自律モードまたはコントローラモード 15

コントローラモードと自律モードの切り替え 16

PnP 検出プロセス 16

第 6 章

Cisco IOS XE ソフトウェアの使用 17

ルータ コンソールを使用して CLI にアクセスする方法 17

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 17

コンソールポートとの接続 18

コンソールインターフェイスの使用方法 18

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 19

Telnet を使用してルータコンソールに接続するための準備 20

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 20

キーボードショートカットの使用方法 22

履歴バッファによるコマンドの呼び出し 22

コマンドモードの概要 23

ヘルプの表示 25

コマンドオプションの検索 25

コマンドの no 形式および default 形式の使用 29

コンフィギュレーションの変更の保存 29

コンフィギュレーションファイルの管理 30

show および more コマンド出力のフィルタリング 31

前面パネルの USB ポートの無効化 32

前面パネルの USB ポートの無効化の設定例 32

前面パネルの USB ポートの無効化の確認 33

ルータの電源切断 33

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 33

 Cisco Feature Navigator の使用 33

 Software Advisor の使用 34

 ソフトウェア リリース ノートの使用 34

第 7 章

ベイ構成 35

 ベイ構成 C8500-12X4QC 35

 ベイ構成の例 37

 例 37

 ブレイクアウト サポート 42

 ブレイクアウトサポートの理解 42

 ブレイクアウト サポート 43

 ブレイクアウトサポートを設定するためのコマンド例 44

 ベイ構成 C8500-12X 44

第 8 章

ライセンスとライセンスモデル 45

 使用可能なライセンスとライセンスモデルの機能情報 45

 使用可能なライセンス 47

 Cisco DNA ライセンス 47

 Cisco DNA ライセンスの使用に関するガイドライン 48

 Cisco DNA ライセンスの発注時の考慮事項 49

 高セキュリティライセンス 50

 HSECK9 ライセンスの使用に関するガイドライン 50

 HSECK9 ライセンスの発注時の考慮事項 51

 Cisco CUBE ライセンス 51

 Cisco Unified CME ライセンス 51

 Cisco Unified SRST ライセンス 52

 スループット 52

 数値としてのスループット 53

 自律モードでのスループットとシステム ハードウェア スロットリングの仕様 54

SD-WAN コントローラモードでのスループットとシステム ハードウェア スロットリングの仕様	57
階層としてのスループット	58
数値と階層ベースのスループットの設定	60
使用可能なライセンスとスループットの設定方法	63
ブートレベルライセンスの設定	64
HSECK9 ライセンス用の SLAC のインストール	67
数値のスループットの設定	67
階層ベースのスループットの設定	71
数値のスループット値から階層への変換	75
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	78
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	79
使用可能なライセンスモデル	80
<hr/>	
第 9 章	統合パッケージの管理 83
	Cisco Catalyst 8500 シリーズ エッジ プラットフォームの実行 : 概要 83
	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 83
	Cisco Catalyst 8500 シリーズ エッジ プラットフォームの実行 : 概要 84
	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 84
	request platform コマンドセット 84
	copy コマンド 85
	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 85
	クイック スタート ソフトウェア アップグレード 85
	統合パッケージで実行するルータの管理および設定 86
	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 86
	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 87
	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 88
	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 88

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	89
インストールモードのプロセスフロー	89
プラットフォームをインストールモードで起動	96
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	97
3 ステップインストール	98
インストールモードでのアップグレード	100
インストールモードでのダウングレード	100
ソフトウェアインストールの終了	101
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	101
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	114

第 10 章 ソフトウェア アップグレード プロセス 115

第 11 章 高可用性の概要 117

この章で紹介する機能情報の入手方法	117
目次	118
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	118
ソフトウェア冗長性の概要	118
2 つの Cisco IOS プロセスの設定	118
例	119
ステートフル スイッチオーバー	120
SSO 認識プロトコルおよびアプリケーション	120
IPsec フェールオーバー	120
双方向フォワーディング検出	121

第 12 章 管理イーサネット インターフェイスの使用 123

この章で紹介する機能情報の入手方法	123
目次	123
ギガビット イーサネット管理インターフェイスの概要	124
ギガビット イーサネット ポートの番号	124

ROMmon および管理イーサネット ポートの IP アドレス処理	124
ギガビット イーサネット管理インターフェイスの VRF	125
共通のイーサネット管理タスク	125
VRF 設定の表示	126
管理イーサネット VRF の詳細な VRF 情報の表示	126
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	126
管理イーサネット IP アドレスの設定	126
管理イーサネット インターフェイス上での Telnet 接続	127
管理イーサネット インターフェイス上での PING の実行	127
TFTP または FTP を使用したコピー	127
NTP サーバー	128
SYSLOG サーバー	128
SNMP 関連サービス	128
ドメイン名の割り当て	128
DNS サービス	128
RADIUS サーバーまたは TACACS+ サーバー	129
ACL を使用した VTY 回線	129
<hr/>	
第 13 章	ブリッジドメイン インターフェイスの設定 131
	ブリッジドメイン インターフェイスの制約事項 131
	ブリッジドメイン インターフェイスに関する情報 132
	イーサネット仮想回線の概要 132
	ブリッジドメイン インターフェイスのカプセル化 133
	MAC アドレスの割り当て 133
	IP プロトコルのサポート 134
	IP 転送のサポート 134
	パケット転送 134
	レイヤ 2 から 3 134
	レイヤ 3 からレイヤ 2 135
	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 135
	BDI の初期状態 135

	BDI のリンク状態	136
	ブリッジ ドメイン インターフェイスの統計情報	136
	ブリッジ ドメイン インターフェイスの作成または削除	136
	ブリッジ ドメイン インターフェイスのスケラビリティ	137
	ブリッジドメイン仮想 IP インターフェイス	137
	ブリッジ ドメイン インターフェイスの設定方法	138
	例	140
	ブリッジ ドメイン インターフェイス設定の表示と確認	140
	ブリッジドメイン仮想 IP インターフェイスの設定	141
	VIF インターフェイスのブリッジ ドメインへの関連付け	142
	ブリッジドメイン仮想 IP インターフェイスの確認	142
	ブリッジドメイン仮想 IP インターフェイスの設定例	142
<hr/>		
第 14 章	SR-TE 優先パスを介した EVPN VPWS	143
	SR-TE 優先パスを介した EVPN VPWS の機能情報	143
	SR-TE 優先パスを介した EVPN VPWS の制約事項	144
	SR-TE 優先パスを介した EVPN VPWS に関する情報	144
	SR-TE 優先パスを介した EVPN VPWS の設定方法	144
	SR-TE 優先パスを介した EVPN VPWS の設定	145
	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	145
	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	145
	SR-TE 優先パス設定を介した EVPN VPWS の無効化	145
	SR-TE 優先パスを介した EVPN VPWS の確認	146
<hr/>		
第 15 章	SFP+ の設定	149
<hr/>		
第 16 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	151
	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	151
	Cisco ThousandEyes Enterprise エージェント アプリケーションの機能情報	152
	サポートされるプラットフォームとシステム要件	153
	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	153

Cisco ThousandEyes アプリケーションをホストするワークフロー	154
デバイスへのイメージのダウンロードとコピー	156
Cisco ThousandEyes エージェントとコントローラの接続	157
エージェントのパラメータの変更	158
アプリケーションのアンインストール	158
Cisco ThousandEyes アプリケーションのトラブルシューティング	158



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 \(1 ページ\)](#)
- [マニュアルの変更履歴 \(1 ページ\)](#)
- [通信、サービス、およびその他の情報 \(2 ページ\)](#)

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、[シスコサービス](#) 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、[シスコ サポート](#) 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。

Cisco 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、[シスコサービス](#) 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、[シスコ サポート](#) 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 and C8500-12X)
- Catalyst 8500L プラットフォーム (C8500L-8S4X)

機能	C8500-12X4QC	C8500-12X	C8500L-8S4X
In-Service Software Upgrade (ISSU) のサポート	サポートあり	サポートあり	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
統合脅威防御 (UTD) のサポート	-	-	サポートあり
Fast Reroute (FRR) のサポート	サポートあり	サポートあり	サポート対象外



第 4 章

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 \(7 ページ\)](#)
- [プロセスの概要 \(11 ページ\)](#)

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

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、RPCControl、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。

表 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。
RPCControl	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。

サブパッケージ	目的
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



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

Cisco 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使用して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は、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の方が簡単です。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。

ROMmon イメージ

個別の ROMmon イメージは、統合パッケージまたはその他のソフトウェアリリースとは別に、定期的にリリースされています。

各 ROMmon イメージの詳細については、ROMmon に付属のマニュアルを参照してください。ROMmon の詳細については、『Cisco Catalyst 8500 Series Edge Platforms Maintain and Operate Guide』を参照してください。

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 3.1.0S 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。

Field-Programmable ハードウェアデバイスのアップグレードの詳細については、『Upgrading Field Programmable Hardware Devices for Cisco Catalyst 8500 Series Edge Platforms』を参照してください。

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 番目の 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。

表 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
nvrnram:	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。

表 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。

ファイルまたはディレクトリ	説明
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。



第 5 章

IOS-XE と SDWAN の展開

- 概要 (15 ページ)
- 機能制限 (15 ページ)
- 自律モードまたはコントローラモード (15 ページ)
- コントローラモードと自律モードの切り替え (16 ページ)
- PnP 検出プロセス (16 ページ)

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



第 6 章

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 \(17 ページ\)](#)
- [キーボードショートカットの使用法 \(22 ページ\)](#)
- [履歴バッファによるコマンドの呼び出し \(22 ページ\)](#)
- [コマンドモードの概要 \(23 ページ\)](#)
- [ヘルプの表示 \(25 ページ\)](#)
- [コマンドの no 形式および default 形式の使用 \(29 ページ\)](#)
- [コンフィギュレーションの変更の保存 \(29 ページ\)](#)
- [コンフィギュレーションファイルの管理 \(30 ページ\)](#)
- [show および more コマンド出力のフィルタリング \(31 ページ\)](#)
- [前面パネルの USB ポートの無効化 \(32 ページ\)](#)
- [ルータの電源切断 \(33 ページ\)](#)
- [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 \(33 ページ\)](#)

ルータ コンソールを使用して CLI にアクセスする方法

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。

手順の概要

1. 端末エミュレーションソフトウェアを次のように設定します。
2. RJ-45/RJ-45 ケーブルと RJ-45/DB-25 DTE（データ端末装置）アダプタ、または RJ-45/DB-9 DTE アダプタ（「Terminal」のラベル）を使用して、ポートに接続します。

手順の詳細

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。

手順の概要

1. ルータのコンソールポートに端末ハードウェアを接続し、端末エミュレーションソフトウェアを適切に設定すると、次のプロンプトが表示されます。
2. **Return** を押して、ユーザー EXEC モードを開始します。次のプロンプトが表示されます。
3. ユーザー EXEC モードで、次のように **enable** コマンドを入力します。
4. パスワードプロンプトに、システムパスワードを入力します。システムで有効なパスワードが設定されていない場合、この手順は省略します。次に、「enablepass」というパスワードを入力する例を示します。
5. 有効なパスワードが許可されると、特権 EXEC モードプロンプトが表示されます。
6. これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。
7. コンソールセッションを終了するには、次のように **quit** コマンドを入力します。

手順の詳細

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

例：

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

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

例：

```
Router>
```

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

例：

```
Router> enable
```

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

例：

```
Password: enablepass
```

ステップ 5 有効なパスワードが許可されると、特権 EXEC モードプロンプトが表示されます。

例：

```
Router#
```

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

ステップ 7 コンソールセッションを終了するには、次のように **quit** コマンドを入力します。

例：

```
Router# quit
```

Telnet を使用してリモートコンソールから CLI にアクセスする方法

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

Telnet を使用してルータ コンソールに接続するための準備

TCP/IP ネットワークから Telnet を使用してルータにリモートアクセスする前に、**line vty** グローバル コンフィギュレーション コマンドを使用して、仮想端末回線 (vty) をサポートするようにルータを設定する必要があります。また、ログインを要求するように **vty** を設定し、パスワードを指定する必要があります。



- (注) 回線上でログインがディセーブル化されないようにするには、**login** ライン コンフィギュレーション コマンドを設定するときに、**password** コマンドでパスワードを指定する必要があります。認証、許可、アカウントिंग (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があります。AAA サービスの詳細については、『Cisco IOS XE Security Configuration Guide』および『Cisco IOS Security Command Reference Guide』を参照してください。

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

Telnet を使用してコンソール インターフェイスにアクセスする方法

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

手順の概要

1. 端末または PC から次のいずれかのコマンドを入力します。
2. パスワード プロンプトで、ログイン パスワードを入力します。次に、**mypass** というパスワードを入力する例を示します。
3. ユーザー EXEC モードで、次のように **enable** コマンドを入力します。
4. パスワード プロンプトに、システム パスワードを入力します。次に、**enablepass** というパスワードを入力する例を示します。
5. 有効なパスワードが許可されると、特権 EXEC モード プロンプトが表示されます。
6. これで、特権 EXEC モードの CLI へのアクセスが可能になりました。必要なコマンドを入力して、必要なタスクを実行できます。
7. Telnet セッションを終了するには、次の例のように **exit** または **logout** コマンドを使用します。

手順の詳細

ステップ 1 端末または PC から次のいずれかのコマンドを入力します。

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

この構文では、*host*にはルータのホスト名またはIPアドレスを指定し、*port*には10進数のポート番号（デフォルトは23）を指定します。また、*keyword*にはサポートされるキーワードを指定します。詳細については、『Cisco IOS Configuration Fundamentals Command Reference Guide』を参照してください。

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

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

例：

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

ステップ 2 パスワードプロンプトで、ログインパスワードを入力します。次に、**mypass** というパスワードを入力する例を示します。

例：

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

（注） パスワードが設定されていない場合は、**Return** を押します。

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

例：

```
Router> enable
```

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

例：

```
Password: enablepass
```

ステップ 5 有効なパスワードが許可されると、特権 EXEC モードプロンプトが表示されます。

例：

```
Router#
```

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

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

例：

Router# **logout**

キーボードショートカットの使用方法

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

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

表 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、履歴置換コマンドの一覧を示します。

表 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。

コマンド	目的
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のモードです。ソフトウェアの起動時、または起動時にコンフィギュレーションファイルが破損している場合に、有効なソフトウェアイメージが見つからなければ、ソフトウェアは ROM モニタ モードを開始することがあります。

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

表 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。
診断	<p>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。</p> <p>場合によっては、IOS プロセスで障害が発生したときに、診断モードを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。</p> <p>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、診断モードを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。</p> <p>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。</p> <p>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。</p>	Router (diag) #	<p>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。</p> <p>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。</p> <p>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。</p>

コマンドモード	アクセス方法	プロンプト	終了方法
ROM モニタ	特権 EXEC モードから、 reload 特権 EXEC コマンドを使用します。システムの起動時、最初の 60 秒以内に Break キーを押します。	>	ROM モニターモードを終了する場合は、 continue コマンドを使用します。

ヘルプの表示

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

コマンドモード、コマンド、キーワード、または引数に固有のヘルプを参照するには、次の表に記載されているコマンドのいずれかを使用します。

表 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。
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くてもください)。
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があるキーワードまたは引数が表示されます (コマンドと疑問符の間にスペースを入れてください)。

コマンドオプションの検索

ここでは、コマンドの構文を表示する方法の例を示します。コマンド構文には、任意または必須のキーワードおよび引数が含まれています。コマンドのキーワードおよび引数を表示するには、疑問符 (?) をコンフィギュレーションプロンプトで入力するか、またはコマンドの一部を入力した後に 1 スペース空けて入力します。Cisco IOS XE ソフトウェアでは、使用可能なキーワードおよび引数のリストと簡単な説明が表示されます。たとえば、グローバルコンフィギュレーションモードから **arap** コマンドのすべてのキーワードまたは引数を表示する場合は、**arap ?** と入力します。

コマンドヘルプ出力の中の<cr>記号は「改行」を表します。古いキーボードでは、CRキーはReturnキーです。最近のキーボードでは、CRキーはEnterキーです。コマンドヘルプの最後の<cr>記号は、**Enter**を押してコマンドを完成させるオプションがあること、および<cr>記号に先行するリスト内の引数およびキーワードはオプションであることを示します。<cr>記号自体は、使用できる引数とキーワードがないため、**Enter**を押してコマンドを終了する必要があることを示します。

次の表に、疑問符(?)を使ったコマンド入力のアシスト方法を示します。

表 8: コマンドオプションの検索

コマンド	コメント
<pre>Router> enable Password: <password> Router#</pre>	<p>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「#」に変わったなら（例：Router> から Router#）、特権 EXEC モードに切り替わっています。</p>
<pre>Router# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#</pre>	<p>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。</p>
<pre>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)#</pre>	<p>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。</p> <p>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。</p> <p><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。</p> <p>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。</p>

コマンド	コメント
<pre> 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 . 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 . no name-caching defaults Negate a command or set its nrzi-encoding Enable use of NRZI encoding ntp Configure NTP . . . Router(config-if)# </pre>	<p>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。</p>

コマンド	コメント
<pre>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 cgmpp 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</pre>	<p>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。</p> <p>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。</p>
<pre>Router(config-if)# ip address ? A.B.C.D IP address negotiated IP Address negotiated over PPP Router(config-if)# ip address</pre>	<p>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。</p> <p>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。</p> <p>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。</p>
<pre>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</pre>	<p>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。</p> <p>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。</p> <p><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。</p>

コマンド	コメント
<pre>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</pre>	<p>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。</p> <p>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。</p> <p><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。</p>
<pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>	<p>この例では、Enter を押してコマンドを完了しています。</p>

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 `nvrn:` 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 lg_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-config]? /auto/tftp-users/user/startup-config
!!
3517 bytes copied in 0.122 secs (28828 bytes/sec)
```

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

show および more コマンド出力のフィルタリング

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

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

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

この出力は、コンフィギュレーションファイル内の情報の特定の行に一致します。次に、**show interface** コマンドに出力修飾子を使用して、「protocol」という表現が現れる行のみを出力する例を示します。

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

前面パネルの USB ポートの無効化

手順の概要

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

手順の詳細

	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があります。

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。



第 7 章

ベイ構成

- [ベイ構成 C8500-12X4QC \(35 ページ\)](#)
- [ブレイクアウト サポート \(42 ページ\)](#)
- [ベイ構成 C8500-12X \(44 ページ\)](#)

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。 <ul style="list-style-type: none"> • 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



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

デフォルトでは、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
*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 FortyGigabitEthernet0/2/0 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
```

ブレイクアウト サポート

ブレイクアウトサポートの理解

ポートのブレイ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、ブレイクアウトサポートは、ブレイクアウト対応の 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。ブレイクアウトサポートは 4X10G で、3 タプルアプローチを使用します。

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

表 9: ブレイ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 ブレイ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 ブレイクアウトモードの 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 ブレイクアウトモードの 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 ブレイ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ブレイ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 ブレイクアウトモードの 2 番目のネイティブポート 10G ブレイクアウトモードの 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 ブレイクアウトモードの最初のネイティブポート 10G ブレイクアウトモードの 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 ブレイ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 ブレイクアウトモードの 3 番目のネイティブポート

ブレイクアウト サポート



(注) ブレイ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
```

ブレイ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 ブレイクアウトにあり、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イクアウト設定がある場合

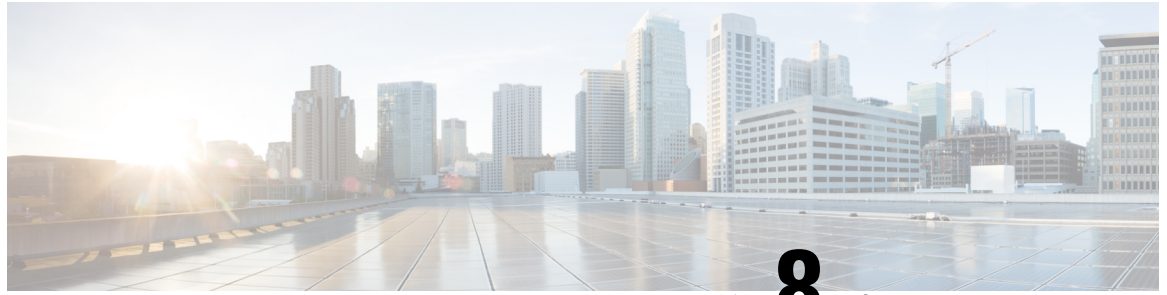
```
hw-module subslot 0/2 breakout 10g port all
hw-module subslot 0/2 breakout none port all
```

すべてのポートからブレイ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。



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 ファミリー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 ファミリー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 \(45 ページ\)](#)
- [使用可能なライセンス \(47 ページ\)](#)
- [スループット \(52 ページ\)](#)
- [使用可能なライセンスとスループットの設定方法 \(63 ページ\)](#)
- [使用可能なライセンスモデル \(80 ページ\)](#)

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、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 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
総スループットのスロットリング	Cisco IOS XE Cupertino 17.8.1a	<p>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。</p> <p>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。</p> <p>数値としてのスループット (53 ページ) および 階層としてのスループット (58 ページ) を参照してください。</p>
階層ベースライセンス	Cisco IOS XE Cupertino 17.7.1a	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
Cisco Digital Network Architecture (Cisco DNA) ライセンス	Cisco IOS XE Amsterdam 17.3.2	<p>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。</p> <p>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。</p>

機能名	リリース	機能情報
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ーで導入されました。
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ーで導入されました

使用可能なライセンス

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ー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 \(49 ページ\)](#)』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。
 - 新しいハードウェアを購入する際に Cisco DNA ライセンスを注文した場合、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 IOS XE Cupertino 17.7.1a からサポートされている階層ベースのスループットを設定する場合、Network Essentials および Cisco DNA Essentials ライセンスでは階層 3 (T3) はサポートされません。

つまり、T3 (スループットが 2.5 G 以上) を設定するには、Network Advantage や Cisco DNA Advantage、または Network Premier や Cisco DNA Premier をブートレベルライセンスとして設定する必要があります。

これは、T3 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。

- 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 (security9、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。

ライセンス PID は、使用できるスループットも示します。スループットは、数値または階層で表すことができます。次に例を示します。

- Cisco DNA-C-10M-E-3Y は、スループットが数値で表されるライセンス PID です。10M は、10 Mbps の双方向スループットを使用できることを意味します。

スループットの数値と関連する概念の詳細については、[スループット \(52 ページ\)](#) と [数値としてのスループット \(53 ページ\)](#) のセクションを参照してください。

- Cisco DNA-C-T0-E-3Yは、スループットが階層値で表されるライセンスPIDです。T0は、最大 15 Mbps の双方向スループットを使用できることを意味します。

階層ベースのスループットの数値と関連する概念の詳細については、[スループット \(52 ページ\)](#) と [階層としてのスループット \(58 ページ\)](#) のセクションを参照してください。

注文するスループットが 250Mbps を超える場合、または階層 2 以上の階層の場合は、HSECK9 ライセンスも必要です。「[高セキュリティライセンス \(50 ページ\)](#)」を参照してください。

高セキュリティライセンス

高セキュリティ (HSECK9) ライセンスは、輸出規制ライセンスです。これは、完全な暗号化機能と、250 Mbps を超える、または階層 2 以上の階層のスループットの使用を許可します。



- (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。

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 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 ライセンスの使用に関するガイドライン

輸出規制ライセンスは、米国の取引規制法の制限対象であり使用前に承認が必要です。この承認は、Smart Licensing Authorization Code (SLAC) の形式であり、完全な暗号化機能が使用可能になり、スループットの制限が解除される前に、デバイスにインストールする必要があります。使用する HSECK9 ライセンスごとに SLAC が必要です。詳細については、この章の設定のセクションで説明しています。

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設定で 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。

Catalyst 8000 ハードウェアプラットフォームとは別の設定で 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設定で HSECK9 ライセンスを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 を工場ですべて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 Cisco UBE 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 UBE 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、デバイス上で転送できるデータの量を示します。この値は、自律モードで設定できます。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。

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。

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とは、スループットに対する制限の適用を指します。

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。



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。さらに、物理プラットフォームでは、非暗号化スループットはデフォルトでスロットルされません。

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。

スループット値

使用できるスループットは、Cisco DNA ライセンスを注文するときにライセンス製品ID (PID) で表されます。

- 数値のスループット値を持つライセンス PID の例：Cisco DNA-C-**10M**-E-3Y
- 階層ベースのスループット値を持つライセンス PID の例：Cisco DNA-C-**T0**-E-3Y

詳細については、デバイスで実行されているソフトウェアバージョンと、購入したライセンス PID に応じて、以下の対応するセクションを参照してください。

数値としてのスループット

ライセンス PID の数値のスループット値は双方向です。これは、各方向（アップストリームとダウンストリーム）で許可される最大スループットです。総スループットは両方向のスループットの合計であるため、双方向のスループットが2倍になります。

たとえば、ライセンス PID Cisco DNA-C-**10M**-E-3Y を注文した場合、10 Mbps は双方向スループットであり、デバイスで設定するスループット値です。この値を設定すると、最大 10 Mbps のアップストリームと 10 Mbps のダウンストリーム スループットがサポートされます。使用可能な総スループットは 20 Mbps です。

Cisco IOS XE Cupertino 17.8.1a 以降、スループットレベルが 250 Mbps を超える場合、デバイスで双方向スループット値を設定すると、総スループットの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。これは、物理プラットフォームでのみサポートされています。

- **例：スループットが 250 Mbps を超える場合のロットリング**

ライセンス PID Cisco DNA-C-**500M**-A-3Y を注文します。500 Mbps は双方向スループットで、1Gbps は総スループットです。リリースごとの設定と動作は次のとおりです。

- Cisco IOS XE Cupertino 17.7.x までの物理プラットフォームおよび仮想プラットフォーム：デバイスで 500 Mbps のスループットを設定し、最大 500 Mbps のアップストリームと 500 Mbps のダウンストリーム スループットがサポートされます。
- Cisco IOS XE Cupertino 17.8.1a 以降：

物理プラットフォームでは、デバイスで 500 Mbps のスループットを設定します。最大 1 Gbps のアップストリームトラフィックと 0 Mbps のダウンストリームトラフィック、または 100 Mbps のアップストリームトラフィックと 900 Mbps のダウンストリームトラフィック、または合計 1 Gbps の制限内のその他の比率がサポートされます。

仮想プラットフォームでは、デバイスで 500 Mbps のスループットを設定します。最大 500 Mbps のアップストリームおよび 500 Mbps のダウンストリームスループットがサポートされます。

• **例：スループットが 250 Mbps 以下の場合のスロットリング**

ライセンス PID Cisco DNA-C-**250M**-A-3Y を注文します。250 Mbps は双方向スループット、500 Mbps は総スループットです。リリースごとの設定と動作は次のとおりです。

すべてのリリースの物理プラットフォームと仮想プラットフォームで、デバイスで 250 Mbps のスループットを設定します。最大 250 Mbps のアップストリームと 250 Mbps のダウンストリームスループットが使用可能です。



- (注) 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) を設定すると、500 Mbps を任意のアップストリームとダウンストリームの比率で使用できます。

ネットワークに必要なスループットに到達するための推奨される方法は、最初に総スループット (アップストリームとダウンストリーム) を計算し、それを 2 で割って双方向スループット値に到達することです。最後に、双方向スループット以上のライセンス PID を選択します。

次の表は、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のスループットの仕様を示しています。



- (注) 自律モードと SD-WAN コントローラモードのスループットの仕様については、別の表が用意されています。

自律モードでのスループットとシステムハードウェアスロットリングの仕様

- サポートされるスループット：デバイスで設定できるスループット値。これらは、指定されたデバイスで設定できる唯一のスループット値です。
- ハードウェアスロットルスループット：サポートされているスループットレベルに対して、システムのハードウェアによって課されるスロットリング制限。以下の表のこの列は、サポートされているスループットレベルごとにハードウェアがスロットルされているかどうか、およびそのハードウェアのスロットルレベルが何であるかを示しています。値がスロットルされていないと表示されている場合は、制限を設定してもスループットがスロットルされないことを意味します。

- HSECK9 が必要か：サポートされているスループットレベルに HSECK9 ライセンスが必要かどうかを示します（250 Mbps 以下の場合、HSECK9 は必要ありません）。
- スループットタイプ：表内のすべてのスループット値は双方向です。これは、わかりやすくするために表にも記載されています。この列は、スループット値が暗号化されているかどうか、物理プラットフォームで暗号化されているか、仮想プラットフォームで暗号化されているかどうかを確認します。

PID	サポートされるスループット	ハードウェアスロットルスループット	サポートされるリリース	HSECK9 が必要か	スループットタイプ
C8300-1N1S-4T2X (デフォルトは 10M)	10M、15M、25M、50M、100M、250M	250M	>= 17.4.1	いいえ	双方向、暗号化
	500M	500M	>= 17.4.1	はい	
	1G	1G	>= 17.4.1	はい	
	2.5G	スロットルなし	>= 17.4.1	はい	
C8300-2N2S-6T (デフォルトは 10M)	10M、15M、25M、50M、100M、250M	250M	>= 17.4.1	いいえ	双方向、暗号化
	500M	500M	>= 17.4.1	はい	
	1G	1G	>= 17.4.1	はい	
C8300-1N1S-6T (デフォルトは 10M)	10M、15M、25M、50M、100M、250M	250M	>= 17.4.1	いいえ	双方向、暗号化
	500M	500M	>= 17.4.1	はい	
	1G	1G	>= 17.4.1	はい	
C8300-2N2S-4T2X (デフォルトは 10M)	10M、15M、25M、50M、100M、250M	250M	>= 17.4.1	いいえ	双方向、暗号化
	500M	500M	>= 17.4.1	はい	
	1G	1G	>= 17.4.1	はい	
	2.5G	スロットルなし	>= 17.4.1	はい	

PID	サポートされるスループット	ハードウェアスロットルスループット	サポートされるリリース	HSECK9が 必要か	スルー プット タイプ
C8200-1N-4T (デフォルトは 10M)	10M、15M、 25M、50M、 100M、250M	250M	>= 17.4.1	いいえ	双方 向、暗 号化
	500M	500M	>= 17.4.1	はい	
C8200-1N-4T-L (デフォルトは 10M)	10M、15M、 25M、50M、 100M、250M	250M	>= 17.5.1	いいえ	双方 向、暗 号化
C8500-12X4QC (デフォルトは 2.5G)	2.5G	2.5G	>= 17.4.1	はい	双方 向、暗 号化
	5G	5G	>= 17.4.1	はい	
	10G	スロットルな し	>= 17.4.1	はい	
C8500-12X (デフォルトは 2.5G)	2.5G	2.5G	>= 17.4.1	はい	双方 向、暗 号化
	5G	5G	>= 17.4.1	はい	
	10G	スロットルな し	>= 17.4.1	はい	
C8500L-8S4X (デフォルトは 1G)	1G	1G	>= 17.5.1	はい	双方 向、暗 号化
	2.5G	2.5G	>= 17.5.1	はい	
	5G	5G	>= 17.5.1	はい	
	10G	スロットルな し	>= 17.5.1	はい	

PID	サポートされるスループット	ハードウェアスロットルスループット	サポートされるリリース	HSECK9が必要か	スループットタイプ
C8000v (デフォルトは10M)	10M	10M	>= 17.4.1	いいえ	双方向、暗号化および非暗号化スループット
	25M	25M	>= 17.4.1	いいえ	
	50M	50M	>= 17.4.1	いいえ	
	100M	100M	>= 17.4.1	いいえ	
	250M	250M	>= 17.4.1	いいえ	
	500M	500M	>= 17.4.1	はい	
	1G	1G	>= 17.4.1	はい	
	2.5G	2.5G	>= 17.4.1	はい	
	5G	5G	>= 17.4.1	はい	
	10G	10G	>= 17.4.1	はい	

SD-WAN コントローラモードでのスループットとシステムハードウェアスロットリングの仕様

PID	HSECK9なしのスループット	HSECK9ありのスループット	サポートされるリリース	スループットタイプ
C8300-1N1S-4T2X (デフォルトは250M)	250M	スロットルなし	>=17.4.1	双方向、暗号化
C8300-2N2S-6T (デフォルトは250M)	250M	1G	>=17.4.1	双方向、暗号化
C8300-1N1S-6T (デフォルトは250M)	250M	1G	>=17.4.1	双方向、暗号化
C8300-2N2S-4T2X (デフォルトは250M)	250M	スロットルなし	>=17.4.1	双方向、暗号化
C8200-1N-4T (デフォルトは250M)	250M	500M	>=17.4.1	双方向、暗号化

PID	HSECK9 なし のスループット	HSECK9 ありの スループット	サポートさ れるリリー ス	スループットタイプ
C8200-1N-4T-L (デフォルトは 250M)	250M	250M	>=17.5.1	双方向、暗号化
C8500-12X4QC (デフォルトはスロットル なし)	スロットルな し	スロットルな し	>=17.4.1	双方向、暗号化
C8500-12X (デフォルトはスロットル なし)	スロットルな し	スロットルな し	>=17.4.1	双方向、暗号化
C8500L-8S4X (デフォルトはスロットル なし)	スロットルな し	スロットルな し	>=17.5.1	双方向、暗号化
C8000v (デフォルトは 250M)	250M	スロットルな し	>=17.4.1	双方向、暗号化およ び非暗号化スルー プット

階層としてのスループット

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。

階層はスループットレベルを表します。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) です。T2 以上の階層は、HSECK9 ライセンスが必要です。

ライセンス PID の階層ベースのスループット値は双方向です。これは、各方向（アップストリームとダウンストリーム）で許可される最大スループットです。総スループットは両方向のスループットの合計であるため、双方向のスループットが 2 倍になります。

たとえば、ライセンス PID Cisco DNA-C-T0-A-3Y を注文した場合、T0 は双方向スループットであり、デバイスで設定するスループット値です。この値を設定すると、T0 アップストリームと T0 ダウンストリームがサポートされます。T0 階層は、最大 15 Mbps のスループットをサポートします。したがって、総スループットは 30 Mbps です。

数値のスループット値がどのように階層にマッピングされるか、およびそれぞれの Cisco DNA ライセンスでどの階層が使用できるかについては、[階層および数値スループットのマッピング](#)の表を参照してください。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 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。これは階層および数値のスループットのマッピングの表で説明しています。

- プラットフォームによってサポートする最大スループットレベルは異なるため、それぞれの階層はプラットフォームによって異なる値になります。たとえば、T2は、C8300-2N2S-4T2の場合は1G スループット、C8200-1N-4Tの場合は500M、C8200-1N-4T-Lの場合は250Mになります。これは階層および数値のスループットのマッピングの表で説明しています。

Cisco IOS XE Cupertino 17.8.1a 以降、T2 以上の階層を設定すると、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。これは、物理プラットフォームでのみサポートされています。

• 例：スループットが T2 以上の階層の場合のスロットリング

ライセンス PID Cisco DNA-C-T2-A-3Y を注文します。T2 では、双方向スループットは最大 1 Gbps で、総スループットは最大 2 Gbps です。リリースごとの設定と動作は次のとおりです。

- Cisco IOS XE Cupertino 17.7.x までの物理プラットフォームおよび仮想プラットフォーム：デバイスで T2 を設定し、デバイスに応じて、最大 1 Gbps のアップストリームと最大 1 Gbps のダウンストリーム スループットがサポートされます。

- Cisco IOS XE Cupertino 17.8.1a 以降：

物理プラットフォームでは、T2 を設定し、デバイスに応じて、アップストリームとダウンストリームの比率で最大 2 Gbps の総スループットを使用できます。



- (注) C8200-1N-4T-L では、T2 を設定すると、500 Mbps を任意のアップストリームおよびダウンストリームの比率で使用できます。ただし、250Mの数値を設定すると、各方向で最大250 Mbps が使用可能になります。

仮想プラットフォームでは、デバイスで T2 のスループットを設定します。最大 1 Gbps のアップストリームおよび 1 Gbps のダウンストリーム スループットが使用可能です。

• 例：スループットが T0 または T1 の場合のスロットリング

ライセンス PID Cisco DNA-C-T1-A-3Y を注文します。T1 では、100 Mbps が双方向スループット、200 Mbps が総スループットです。リリースごとの設定と動作は次のとおりです。

すべてのリリースの物理プラットフォームと仮想プラットフォームで、デバイスで T1 のスループットを設定します。最大 100 Mbps のアップストリームと 100 Mbps のダウンストリーム スループットが使用可能です。

階層および数値のスループットのマッピング

Y : Network Premium および Cisco DNA Premium

■ : Network Advantage および Cisco DNA Advantage

■ : Network Essentials および Cisco DNA Essentials

PID	T0		T1			T2*			T3*			
	10M	15 M	25M	50M	100M	250M	500M	1G	2.5G	5G	10G	
	*HSECK9 ライセンスが必要											
C8300-1N1S-6T	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■				
C8300-2N2S-6T	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■				
C8300-1N1S-4T2X	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■			
C8300-2N2S-4T2X	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■			
C8200-1N-4T	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■					
C8200-1N-4T-L	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■						
C8500-12X									■ ■	■ ■	■ ■	
C8500-12X4QC									■ ■	■ ■	■ ■	
C8500L-8S4X								■ ■	■ ■	■ ■	■ ■	
C8000v	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■ ■	■ ■	■ ■		

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。

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。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、アカウントの数値および階層ベースのライセンスを表示します。図 1: CSSM Web UI に表示される数値と階層の値 (62 ページ) は、この 2 つを区別する方法を示しています。

- 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 (67 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 \(71 ページ\)](#) または [数値のスループットの設定 \(67 ページ\)](#) 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。
-

図 1: CSSM Web UI に表示される数値と階層の値

+	Routing DNA Advantage: Tier 2	→ Tier-Based	Prepaid
+	Routing DNA Advantage: Tier 2: 1G	→ Numeric	Prepaid
+	Routing DNA Advantage: Tier 2: 250M		Prepaid
+	Routing DNA Advantage: Tier 2: 500M		Prepaid
+	Routing DNA Advantage: Tier 3		Prepaid
+	Routing DNA Advantage: Tier 3: 5G		Prepaid
+	Routing DNA Advantage: Tier 4		Prepaid
+	Routing DNA Essentials: Tier 1: 100M		Prepaid
+	Routing DNA Essentials: Tier 2		Prepaid
+	Routing DNA Essentials: Tier 2: 1G		Prepaid
+	Routing DNA Essentials: Tier 2: 250M		Prepaid
+	Routing DNA Essentials: Tier 2: 500M		Prepaid
+	Routing DNA Essentials: Tier 3		Prepaid
+	Routing DNA Premier: Tier 1: 100M		Prepaid
+	Routing DNA Premier: Tier 2: 1G		Prepaid

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 \(75 ページ\)](#)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 \(78 ページ\)](#)』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 \(79 ページ\)](#)」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ーで使用可能なライセンスについて、使用を開始する前に完了する必要があるタスク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)]。

³ SLAC がシスコの工場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。

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。

手順の概要

1. **show version**
2. **configure terminal**
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} }**
4. **exit**
5. **copy running-config startup-config**
6. **reload**
7. **show version**
8. **show license summary**
9. 完全な使用状況レポート（必要な場合）

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	show version 例： <pre>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 <output truncated></pre>	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。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	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。 <ul style="list-style-type: none"> 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} } 例 : Device (config)# license boot level network-premier addon dna-premier % use 'write' command to make license boot config take effect on next boot	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。
ステップ 4	exit 例 : Device# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	copy running-config startup-config 例 : Device# copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK] <output truncated>	コンフィギュレーションファイルに設定を保存します。
ステップ 6	reload 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>	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。
ステップ 7	show version 例 : Device# show version <output truncated> Technology Package License Information:	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。

	コマンドまたはアクション	目的
	<pre> 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> </pre>	
ステップ 8	<p>show license summary</p> <p>例 :</p> <pre> 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 </pre>	<p>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。</p>
ステップ 9	<p>完全な使用状況レポート（必要な場合）</p>	<p>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。</p> <ul style="list-style-type: none"> • レポートが必要であることを示すシステムメッセージ 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。

	コマンドまたはアクション	目的
		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。

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

- [数値としてのスループット \(53 ページ\)](#) および [数値と階層ベースのスループットの設定 \(60 ページ\)](#) 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。 [ブートレベルライセンスの設定 \(64 ページ\)](#) 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、Smart Licensing Using Policy 環境のトポロジに適用されるメソッドに従って、Smart Licensing Authorization Code (SLAC) がすでに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 \(67 ページ\)](#) 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。

手順の概要

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**
2. **configure terminal**
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}**
4. **exit**
5. **copy running-config startup-config**
6. **reload**
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**

手順の詳細

	コマンドまたはアクション	目的
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。 <ul style="list-style-type: none"> • 物理プラットフォームの場合：show platform hardware throughput crypto 	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。 添付の例：

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> 仮想プラットフォームの場合：show platform hardware throughput level <p>例：</p> <pre>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</pre>	<ul style="list-style-type: none"> 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。
ステップ 2	<p>configure terminal</p> <p>例：</p> <pre>Device# configure terminal</pre>	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	<p>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。</p> <ul style="list-style-type: none"> 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} <p>例：</p> <pre>Device(config)# platform hardware throughput crypto ? 100M 100 mbps bidirectional thput 10M 10 mbps bidirectional thput 15M 15 mbps bidirectionalthput 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</pre>	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 少なくとも、ネットワークスタックライセンスを設定しておく必要があります。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。 250 Mbps を超えるスループットを設定する場合は、SLAC をインストールしておく必要があります。250 Mbps を超えるオプションは、SLAC がインストールされている場合にのみ表示されます。 <p>添付の例：</p> <ul style="list-style-type: none"> 物理プラットフォームで 1 Gbps が設定されています。総スループットのスロットリング (Cisco IOS XE Cupertino 17.8.1a 以降) が有効です。再起動後、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に関係なく、総スループットの 2 Gbps の制限が有効になります。

	コマンドまたはアクション	目的
	<pre>% 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.</pre>	<ul style="list-style-type: none"> 仮想プラットフォームで 5000 Mbps が設定されています。最大 5000 Mbps のアップストリームおよび 5000 Mbps のダウンストリーム スループットがサポートされます。
ステップ 4	<p>exit</p> <p>例 :</p> <pre>Device# exit</pre>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	コンフィギュレーションファイルに設定を保存します。
ステップ 6	<p>reload</p> <p>例 :</p> <pre>Device# reload</pre>	<p>デバイスがリロードされます。</p> <p>(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 (Catalyst 8200、8300、および 8500 シリーズ エッジ プラットフォーム) である場合にのみ、この手順を実行します。</p> <p>仮想プラットフォーム (Catalyst 8000V エッジソフトウェア) 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。</p>
ステップ 7	<p>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。</p> <ul style="list-style-type: none"> 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 <p>例 :</p> <pre>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</pre>	<p>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。</p> <p>(注) 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。</p>

コマンドまたはアクション	目的
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

- [階層としてのスループット（58 ページ）](#) および [数値と階層ベースのスループットの設定（60 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。[ブートレベルライセンスの設定（64 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、ライセンスが指定されていることを確認します。
- 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 は、Network Essentials および Cisco DNA Essentials ではサポートされていません。
- 階層 2（T2）以上の階層を設定する場合は、Smart Licensing Using Policy 環境のトポロジに適用されるメソッドに従って、Smart Licensing Authorization Code（SLAC）がすでに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（67 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。
- 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。

手順の概要

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**
2. **show license authorization**
 3. **configure terminal**
 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}**
 - 仮想プラットフォームの場合 : **platform hardware throughput level MB {T0 | T1 | T2 | T3}**
 5. **exit**
 6. **copy running-config startup-config**
 7. **reload**
 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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>例 :</p> <pre>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</pre>	<p>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。</p> <p>添付の例 :</p> <ul style="list-style-type: none"> • 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。
ステップ 2	<p>show license authorization</p> <p>例 :</p> <pre>Device# show license authorization Overall status:</pre>	<p>(オプション) 製品インスタンスの SLAC 情報を表示します。</p> <p>添付の例 :</p>

	コマンドまたはアクション	目的
	<pre> 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 </pre>	<ul style="list-style-type: none"> • 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、後続の手順で 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。
<p>ステップ 3</p>	<p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre>	<p>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。</p>
<p>ステップ 4</p>	<p>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。</p> <ul style="list-style-type: none"> • 物理プラットフォームの場合 : platform hardware throughput crypto {T0 T1 T2 T3} • 仮想プラットフォームの場合 : platform hardware throughput level MB {T0 T1 T2 T3} <p>例 :</p> <pre>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</pre>	<p>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。</p> <p>(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。</p> <p>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。</p> <ul style="list-style-type: none"> • ブートレベルライセンスはすでに設定されています。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。

	コマンドまたはアクション	目的
	<pre> 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 </pre>	<p>(注) 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。</p> <p>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ています。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。</p> <p>添付の例：</p> <ul style="list-style-type: none"> 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、階層T2以上が表示されます。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。 <p>さらに、総スループットのスロットリング (Cisco IOS XE Cupertino 17.8.1a以降) が有効です。再起動後、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に関係なく、総スループットの2 Gbpsの制限がサポートされます。</p> <ul style="list-style-type: none"> 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。
ステップ 5	<pre> exit 例 : Device# exit </pre>	<p>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。</p>
ステップ 6	<pre> copy running-config startup-config 例 : </pre>	<p>コンフィギュレーションファイルに設定を保存します。</p>

	コマンドまたはアクション	目的
	<pre>Device# copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]</pre>	
ステップ 7	<p>reload</p> <p>例 :</p> <pre>Device# reload Proceed with reload? [confirm] *Mar 02 05:07:00.979: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.</pre>	<p>デバイスがリロードされます。</p> <p>(注) リロードは、物理プラットフォームでのみ必要です。</p>
ステップ 8	<p>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。</p> <ul style="list-style-type: none"> 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 <p>例 :</p> <pre>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</pre>	<p>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。</p> <p>添付の例 :</p> <ul style="list-style-type: none"> 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。 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。 <p>(注) 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。</p>

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](#)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（60 ページ）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 \(67 ページ\)](#) を参照してください。
- この製品インスタン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。

手順の概要

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**
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**
3. **copy running-config startup-config**
4. **reload**
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**
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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>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。</p> <ul style="list-style-type: none"> • 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 <p>例：</p> <pre>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</pre> <p>OR</p>	<p>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。</p>

	コマンドまたはアクション	目的
	<pre>Device# show platform hardware throughput level The current throughput level is 100000 kb/s</pre>	
ステップ 2	<p>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。</p> <ul style="list-style-type: none"> 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 <p>例：</p> <pre>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</pre>	<p>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。</p>
ステップ 3	<p>copy running-config startup-config</p> <p>例：</p> <pre>Device# copy running-config startup-config Destination filename [startup-config]? Building configuration... [OK]</pre>	<p>コンフィギュレーションファイルに設定を保存します。</p> <p>(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。</p>
ステップ 4	<p>reload</p> <p>例：</p> <pre>Device# reload Proceed with reload? [confirm] *Dec 8 03:24:09.534: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command</pre>	<p>デバイスがリロードされます。</p> <p>(注) リロードは、物理プラットフォームでのみ必要です。</p>

	コマンドまたはアクション	目的
ステップ 5	<p>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。</p> <ul style="list-style-type: none"> 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 <p>例：</p> <pre>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</pre> <p>OR</p> <pre>Device# show platform hardware throughput level The current throughput level is 100000 kb/s</pre>	<p>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。</p>
ステップ 6	<p>変換が完了したことを確認します。</p> <ul style="list-style-type: none"> 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 <p>例：</p> <pre>Device# license throughput crypto auto-convert Crypto throughput is already tier based, no need to convert.</pre> <p>OR</p> <pre>Device# license throughput level auto-convert % Tier conversion not possible since the device is already in tier licensing</pre>	<p>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せん。</p>

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 (75 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 (75 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 (75 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 (67 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。その後、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、シスコのマネージド サービス プロバイダー ビジネス向けに設計された消費ベースのソフトウェア ライセンス モデルです。

- 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。

ここでは、まずシスコと MSLA を締結し、サブスクリプション ID でライセンスを購入します。

サブスクリプション ID 付きのライセンスは、[Cisco commerce workspace](#) (CCW) で注文できます。注文したライセンスは、対応するサブスクリプション ID とともに、CSSM の指定されたスマートアカウントおよびバーチャルアカウントに保管されます。

ライセンスのワークフローを完了するには、サポートされているトポロジを実装する必要があります。CSSM がライセンス使用情報を受け取ると、スループットと、アクティブ化され使用中の Cisco DNA サブスクリプション階層に基づいて課金されます。詳細については、[MSLA](#) および [ユーティリティモード](#) を参照してください。



第 9 章

統合パッケージの管理

この章では、統合パッケージがどのように管理され、Cisco 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。



(注) 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 \(83 ページ\)](#)
- [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 \(84 ページ\)](#)
- [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 \(85 ページ\)](#)
- [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 \(88 ページ\)](#)

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であることを前提とします。

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

クイック スタート バージョンを使用してソフトウェアをアップグレードするには、次の手順を実行します。

手順の概要

1. **copy URL-to-image bootflash:** コマンドを使用して、統合パッケージを bootflash: にコピーします。
2. **dir bootflash:** コマンドを入力して、bootflash: ディレクトリ内の統合パッケージを確認します。
3. ブート用のブートパラメータを設定します。**config-register 0x2102** グローバルコンフィギュレーションコマンドを入力して、コンフィギュレーションレジスタを 0x2 に設定し、**boot system flash bootflash:image-name** を入力します。
4. **copy running-config startup-config** を入力して設定を保存します。
5. **reload** コマンドを入力して、ルータをリロードし、ブートを終了します。リロード完了時には、アップグレードされたソフトウェアが実行されています。

手順の詳細

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**



- (注) 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 \(86ページ\)](#) 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 11: バンドルモードとインストールモード

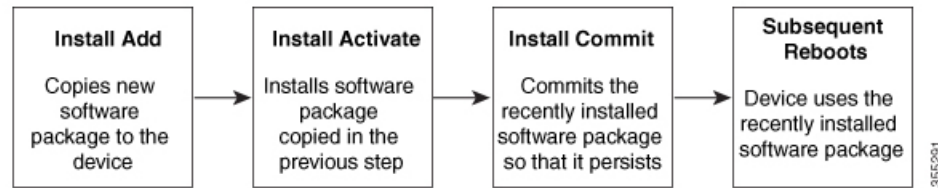
バンドルモード	インストールモード
このモードでは、ローカル（ハードディスク、フラッシュ）またはリモート（TFTP）の .bin イメージを使用して、統合されたブートプロセスが提供されます。	このモードでは、ブートプロセスにローカル（ブートフラッシュ）の packages.conf ファイルを使用します。
このモードでは、1つの .bin ファイルを使用します。	このモードでは、.bin ファイルは拡張された .pkg ファイルに置き換えられます。
CLI : <pre>#boot system file <filename></pre>	CLI : <pre>#install add file bootflash: [activate commit]</pre>
このモードでアップグレードするには、ブートシステムを新しいイメージにポイントします。	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。

Process with Install Commit



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` ファイルに抽出します。またファイルを検証して、イメージファイルがインストールされているプラットフォームに固有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 12: 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 <i>location:filename.bin</i>	<p>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。</p> <ul style="list-style-type: none"> • 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 に抽出します。 • 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	<p>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。</p> <ul style="list-style-type: none"> • 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>	<p>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終了し、システムは最後にコミットされた状態に戻ります。</p> <ul style="list-style-type: none"> • 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エーションでのみ有効です。
install commit	install commit	<p>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。</p> <ul style="list-style-type: none"> • 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	<p>インストールを終了し、システムを最後にコミットされた状態に戻します。</p> <ul style="list-style-type: none"> 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優先バージョンに戻ります。
install remove	install remove {file <filename> inactive}	<p>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。</p> <ul style="list-style-type: none"> 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}	<p>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。</p> <ul style="list-style-type: none"> • 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。 <p>(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、以前のイメージをインストールモードでインストールする必要があります。バンドルモードでは SMU ロールバックのみが可能です。</p>
install deactivate	install deactivate file <filename>	<p>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。</p> <ul style="list-style-type: none"> • 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 13: *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。 <ul style="list-style-type: none"> • 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。 <p>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。</p>

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ステップのバリエーション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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device>enable	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	install add file location: filename [activate commit] 例 : <pre>Device#install add file bootflash:c8000e-universalk9_EBD_V177_THROTTLE_LATEST_20211021_031123_V17_7_0_117.SSA.bin activate commit</pre>	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 ファイルに抽出します。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 : <pre>Device#exit</pre>	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

	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:c8000e-universalk9-ED_V177_THR01TE_IABEST_20211027_030841_V17 7.0 120.SPA.bin	ソフトウェア インストール パッケージをリモートの場所（FTP、HTTP、HTTPS、または TFTP 経由）からプラットフォームにコピーし、.package ファイルの個々のコンポーネントをサブパッケージおよび packages.conf ファイルに抽出します。
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。 <ul style="list-style-type: none"> • 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エーションでは、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終了し、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。 <ul style="list-style-type: none"> • 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。

	コマンドまたはアクション	目的
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。 <ul style="list-style-type: none"> • 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終了

ソフトウェアパッケージのアクティブ化は次の方法で終了できます。

- 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エーションでは **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
```

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

```

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_tle1.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_tle1.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]
--- 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
```

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

```

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_lt3e3.17.06.01a.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 Current  Technology-package Next Reboot
-----
Smart License   Perpetual     None          None
Smart License   Subscription  None          None
-----
```

```
The current crypto throughput level is 250000 kbps
```

```
Smart Licensing Status: Registration Not Applicable/Not Applicable
```

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

```
Configuration register is 0x2102
```

以下は、ソフトウェアのインストールを終了する例です。

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



```

This install abort would require a reload. Do you want to proceed? [y/n]
*Oct 29
02:42:52.789: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install aborty
--- Starting Abort ---
Performing Abort on Active/Standby

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

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

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

Initializing Hardware ...

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

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

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

□

Press RETURN to get started!

□

```

以下は、show コマンドの出力例です。

show install log

```

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

```

show install summary

```

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

```

show install package *filesystem: filename*

```

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

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

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

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

Package is bootable from media and tftp.
Package contents:

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

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

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

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

```

```

Raw disk-file SHA1sum:
  a57bed4ddecfd08af3b456f69d11aaeb962865ea
Header size:      1116 bytes
Package type:     40000
Package flags:    0
Header version:   3

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

```

Package is not bootable.

show install active

```

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

```

show install inactive

```

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

```

show install committed

```

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

```

show install uncommitted

```

Device# show install uncommitted
[ R0 ] Uncommitted Package(s) Information:

```

```

State (St): I - Inactive, U - Activated & Uncommitted,
           C - Activated & Committed, D - Deactivated & Uncommitted
-----
Type  St   Filename/Version
-----
No Uncommitted Packages

```

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

問題 ソフトウェアインストールのトラブルシューティング

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

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

問題 インストールに関するその他の問題

解決法 インストールに関する問題を解決するには、次のコマンドを使用します。

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



第 10 章

ソフトウェア アップグレード プロセス

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

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



第 11 章

高可用性の概要

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

Cisco 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（117 ページ）](#)
- [目次（118 ページ）](#)
- [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（118 ページ）](#)
- [ステートフル スイッチオーバー（120 ページ）](#)
- [IPsec フェールオーバー（120 ページ）](#)
- [双方向フォワーディング検出（121 ページ）](#)

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。

手順の概要

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

4. mode SSO
5. exit
6. reload

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	redundancy 例： Router(config)# redundancy	冗長コンフィギュレーションモードを開始します。
ステップ 4	mode SSO 例： Router(config)# mode SSO	SSO を設定します。このコマンドが入力されると、冗長スーパーバイザエンジンがリロードされ、SSO モードで動作を開始します。
ステップ 5	exit 例： Router(config)# exit 例： Router #	コンフィギュレーションモードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	reload 例： Router # reload	IOS をリロードします。

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witch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 とボーダー ゲートウェイ プロトコル (BGP) 用の BFD がサポートされます。

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



第 12 章

管理イーサネット インターフェイスの使用

Cisco 8500 シリーズ 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 (123 ページ)
- 目次 (123 ページ)
- ギガビットイーサネット管理インターフェイスの概要 (124 ページ)
- ギガビットイーサネット ポートの番号 (124 ページ)
- ROMmon および管理イーサネット ポートの IP アドレス処理 (124 ページ)
- ギガビットイーサネット管理インターフェイスの VRF (125 ページ)
- 共通のイーサネット管理タスク (125 ページ)

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つたりしますが、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 \(125 ページ\)](#) を参照してください。

ギガビットイーサネット ポートの番号

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

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
```

管理イーサネット インターフェイス上での Telnet 接続

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

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

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

管理イーサネット インターフェイス上での PING の実行

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

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

```
Router# ping vrf Mgmt-intf 172.17.1.1

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

TFTP または FTP を使用したコピー

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

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

TFTP の例

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

FTP の例

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

NTP サーバー

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

次の CLI では、このプロシージャの例を示します。

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

SYSLOG サーバー

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

次の CLI では、このプロシージャの例を示します。

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

SNMP 関連サービス

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

次の CLI では、このプロシージャの例を示します。

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

ドメイン名の割り当て

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

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

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

DNS サービス

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

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

RADIUS サーバーまたは TACACS+ サーバー

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

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

RADIUS サーバーグループの設定

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

TACACS+ サーバーグループの例

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

ACL を使用した VTY 回線

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

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




第 13 章

ブリッジ ドメイン インターフェイスの設定

Cisco 8500 シリーズ 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 \(131 ページ\)](#)
- [ブリッジ ドメイン インターフェイスに関する情報 \(132 ページ\)](#)
- [ブリッジドメイン仮想 IP インターフェイスの設定 \(141 ページ\)](#)

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 packets 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プングが有効になり、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。



- (注) `mac-address` コマンドを使用して、ブリッジドメインインターフェイスにスタティック MAC アドレスを設定できます。

IP プロトコルのサポート

ブリッジドメインインターフェイスは、Cisco 8500 シリーズ 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。



- (注) MAC アドレス ラーニングは、ブリッジドメイン上のインターフェイスで実行できません。

レイヤ3からレイヤ2

パケットがルータの物理インターフェイスのレイヤ3に到達すると、ルート検索アクションが実行されます。ルート検索がブリッジドメインインターフェイスに向かうと、ブリッジドメインインターフェイスはレイヤ2カプセル化を追加し、対応するブリッジドメインにフレームを転送します。バイトカウンタが更新されます。

ブリッジドメインインターフェイスが属するブリッジドメインでのレイヤ2検索中に、ブリッジドメインは、宛先MACアドレスに基づいて適切なサービスインスタンスにパケットを転送します。

ブリッジドメインとブリッジドメインインターフェイスのステートをリンクする

ブリッジドメインインターフェイスはレイヤ3のルーティング可能なIOSインターフェイスおよびブリッジドメインのポートとして機能します。ブリッジドメインインターフェイスとブリッジドメインのいずれも、個々の管理状態で動作します。

ブリッジドメインインターフェイスをシャットダウンすると、レイヤ3データサービスは停止しますが、関連するブリッジドメインの状態は上書きされず、影響を受けません。

ブリッジドメインをシャットダウンすると、サービスインスタンスやブリッジドメインインターフェイスを含むすべての関連メンバへのレイヤ2転送が停止します。関連するサービスインスタンスはブリッジドメインの動作状態に影響を与えます。ブリッジドメインインターフェイスは、関連するサービスインスタンスの1つが起動しない限り、動作することはできません。



- (注) ブリッジドメインインターフェイスは内部インターフェイスであるため、ブリッジドメインインターフェイスの動作状態はブリッジドメインの動作状態には影響しません。

BDIの初期状態

BDI最初の管理ステータスは、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タを表示するには、`show interface <if-name>` コマンドを使用します。

ブリッジドメインインターフェイスの作成または削除

Cisco IOS ルータのインターフェイスまたはサブインターフェイスを定義する場合は、名前を付け、どのようにIPアドレスに割り当てられるかを指定します。システムへブリッジドメインを追加する前にブリッジドメインインターフェイスを作成できます。この新しいブリッジドメインインターフェイスは、関連するブリッジドメインの設定後にアクティブになります。



- (注) ブリッジドメインインターフェイスが作成されると、ブリッジドメインが自動的に作成されます。

ブリッジドメインインターフェイスとブリッジドメインを作成すると、システムは、ブリッジドメインとブリッジドメインインターフェイスのペアをマッピングするために必要なアソシエーションを保持します。

ブリッジドメインとブリッジドメインインターフェイスのマッピングはシステムに保持されます。ブリッジドメインインターフェイスは、アソシエーションを示すために関連するブリッジドメインのインデックスを使用されます。

ブリッジドメインインターフェイスのスケラビリティ

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ラビリティの数値を示します。

表 14: 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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Router# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	interface BDI { <i>interface number</i> }	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 < <i>first-tag</i> > [<i>second-dot1q</i> < <i>second-tag</i> >] 例：	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。

	コマンドまたはアクション	目的
	Router(config-if)# encapsulation dot1q 1 second-dot1q 2	
ステップ 5	次のいずれかを実行します。 例： ip address <i>ip-address mask</i> 例： 例： ipv6 address { <i>X:X:X:X::X link-local</i> <i>X:X:X:X::X/prefix [anycast eui-64]</i> autoconfig [default] } 例： Router(config-if)# ip address 2.2.2.1 255.255.255.0 例： 例： Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64	ブリッジドメインインターフェイスのIPv4 または IPv6 アドレスを指定します。
ステップ 6	match security-group destination tag sgt-number 例： Router(config-route-map)# match security-group destination tag 150	security-group destination security tag の値を設定します。
ステップ 7	mac address {mac-address} 例： Router(config-if)# mac-address 1.1.3	ブリッジドメインインターフェイスのMACアドレスを指定します。
ステップ 8	no shut 例： Router(config-if)# no shut	Cisco 8500 シリーズ 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 例： 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

手順の概要

1. **enable**
2. **show interfaces bdi**
3. **show platform software interface fp active name**
4. **show platform hardware qfp active interface if-name**
5. **debug platform hardware qfp feature**
6. **platform trace runtime process forwarding-manager module**
7. **platform trace boottime process forwarding-manager module interfaces**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	show interfaces bdi 例： Router# show interfaces BDI3	対応する BDI の設定の概要を表示します。
ステップ 3	show platform software interface fp active name 例： Router# show platform software interface fp active name BDI4	フォワーディングプロセッサのブリッジドメインインターフェイス設定を表示します。
ステップ 4	show platform hardware qfp active interface if-name 例：	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。

	コマンドまたはアクション	目的
	Router# show platform hardware qfp active interface if-name BDI4	
ステップ 5	debug platform hardware qfp feature 例 : Router# debug platform hardware qfp active feature l2bd client all	選択した CPP L2BD Client のデバッグがオンになります。
ステップ 6	platform trace runtime process forwarding-manager module 例 : Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module interfaces level info	Forwarding Manager プロセスの Forwarding Manager Route Processor および Embedded Service Processor のトレースメッセージを有効にします。
ステップ 7	platform trace boottime process forwarding-manager module interfaces 例 : Router(config)# platform trace boottime slot R0 bay 1 process forwarding-manager forwarding-manager level max	ブートアップ中の、Route Processor Forwarding Manager プロセスの Forwarding Manager Route Processor および Embedded Service Processor のトレースメッセージを有効にします。

次のタスク

各コマンドに使用できるコマンドおよびオプションの詳細については、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-channell
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-channell service-instance 1756
member bd-vif5001
member bd-vif5002
```




第 14 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 (143 ページ)
- SR-TE 優先パスを介した EVPN VPWS の制約事項 (144 ページ)
- SR-TE 優先パスを介した EVPN VPWS に関する情報 (144 ページ)
- SR-TE 優先パスを介した EVPN VPWS の設定方法 (144 ページ)
- SR-TE 優先パスを介した EVPN VPWS の確認 (146 ページ)

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 15: 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

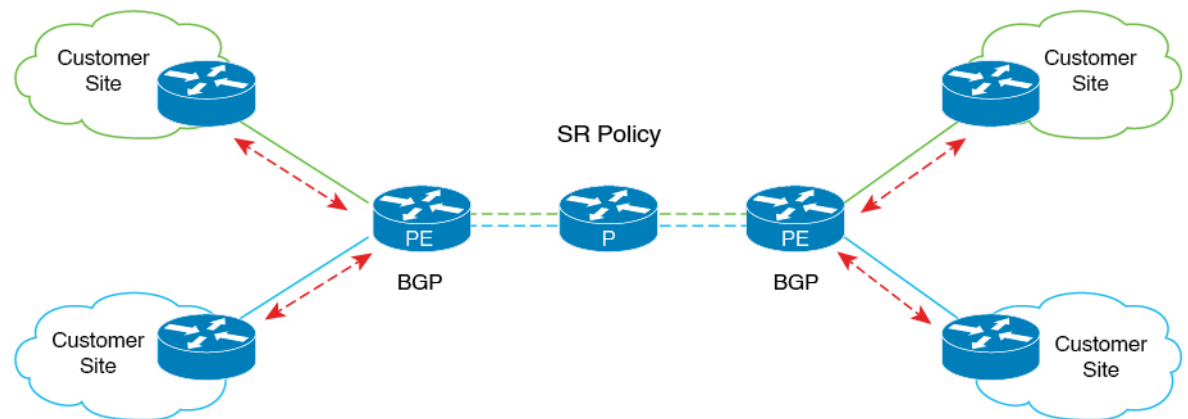
- SR オンデマンドネクストホップ (ODN) ポリシーはサポートされていません。SR 静的ポリシーのみがサポートされます。
- SR フロー単位ポリシー (PFP) はサポートされていません。SR 宛先単位ポリシー (PDP) のみがサポートされています。
- 内部ゲートウェイプロトコル (IGP) は Intermediate System-to-Intermediate system (IS-IS) です。

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



357625

SR-TE 優先パスを介した EVPN VPWS の設定方法

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

SR-TE 優先パスを介した EVPN VPWS の設定

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

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

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

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

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

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

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

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

SR-TE 優先パス設定を介した EVPN VPWS の無効化

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

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

SR-TE 優先パスを介した EVPN VPWS の確認

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

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

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

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

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

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

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

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

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

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




第 15 章

SFP+ の設定

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable <i>source-interface gigabitethernet slot/port</i> 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。
ステップ 3	interface tengigabitethernet <i>slot/port</i> 例 : Router(config)# interface tengigabitethernet 4/11	設定する 10 ギガビット イーサネット インターフェイスを指定します。 ここで、各変数は次のように定義されます。 slot/port : インターフェイスの場所を指定します。



第 16 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 \(151 ページ\)](#)
- [サポートされるプラットフォームとシステム要件 \(153 ページ\)](#)
- [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 \(153 ページ\)](#)
- [エージェントのパラメータの変更 \(158 ページ\)](#)
- [アプリケーションのアンインストール \(158 ページ\)](#)
- [Cisco ThousandEyes アプリケーションのトラブルシューティング \(158 ページ\)](#)

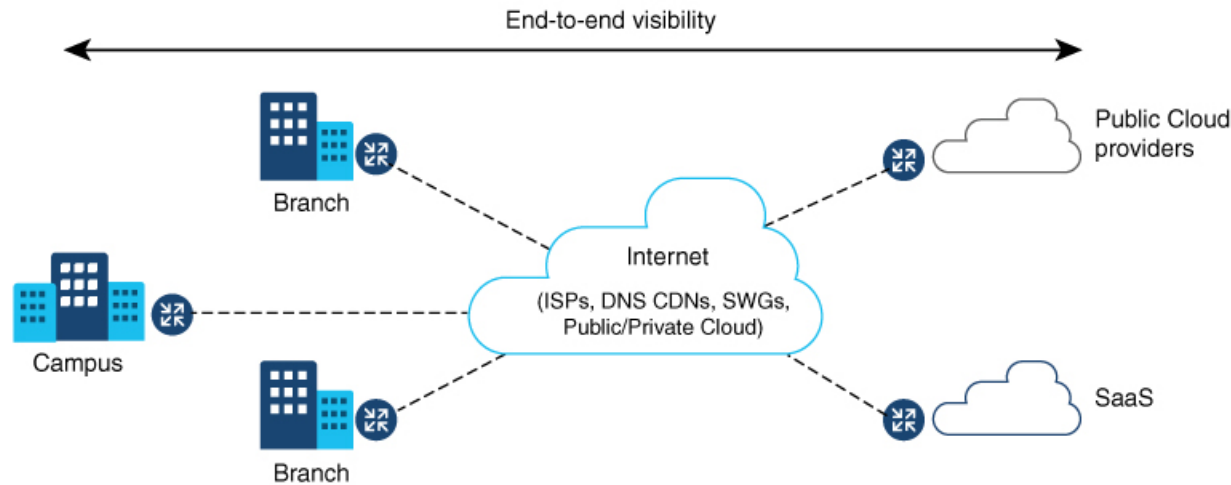
Cisco ThousandEyes エンタープライズ エージェント アプリケーションのホスティング

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 16: 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.2USB 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。

- 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 \(158 ページ\)](#) 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。

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。

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: tel1000
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: tel1000 started
successfully Current state is RUNNING
```

```
Device#show app-hosting detail appid tel1000 (Details of Application)
App id          : tel1000
Owner           : iox
State          : RUNNING
Application
  Type          : docker
  Name          : ThousandEyes Enterprise Agent
  Version       : 4.0
  Author        : ThousandEyes <support@thousandeyes.com>
  Path          : bootflash:thousandeyes-enterprise-agent-4.0-22.cisco.tar
Resource reservation
  Memory        : 500 MB
  Disk          : 1 MB
  CPU           : 1500 units
  CPU-percent   : 70 %
```

- b) デバイスにプロキシサーバーがある場合は、イメージを `bootflash:/apps` に手動でコピーします。
- c) [ソフトウェアのダウンロード](#) ページから Cisco ThousandEyes アプリケーションパッケージをダウンロードし、エージェントバージョン 4.0.2 を使用していることを確認します。
- d) `bootflash:` にアプリケーションディレクトリを作成し、イメージをコピーします。

```
Device# mkdir bootflash:apps
Create directory filename [apps]?
Created dir bootflash:/apps
```

- e) Cisco ThousandEyes イメージを `bootflash:apps` ディレクトリにコピーします。
- f) `verify` コマンドを使用してイメージを検証します。

```
verify /md5 bootflash:apps/<file name>
```

Cisco ThousandEyes エージェントとコントローラの接続

始める前に

エージェントをコントローラに接続する前に、インターネットに接続していることを確認します。

Cisco ThousandEyes アプリケーションが稼働状態になると、エージェント (ThousandEyes エージェント) プロセスがクラウド環境で実行されているコントローラに接続します。

- (注) 接続に関連する問題がある場合、関連するエラーメッセージがアプリケーション固有のログ (`/var/logs`) に記録されます。

エージェントのパラメータの変更

エージェントのパラメータを変更するには、次のアクションを実行します。

-
- ステップ1 **app-hosting stop appid appid** コマンドを使用して、アプリケーションを停止します。
 - ステップ2 **app-hosting deactivate appid appid** コマンドを使用して、アプリケーションを非アクティブ化します。
 - ステップ3 アプリケーション ホスティングの設定に必要な変更を加えます。
 - ステップ4 **app-hosting activate appid appid** コマンドを使用して、アプリケーションをアクティブ化します。
 - ステップ5 **app-hosting start appid appid** コマンドを使用して、アプリケーションを起動します。
-

アプリケーションのアンインストール

アプリケーションをアンインストールするには、次の手順を実行します。

-
- ステップ1 **app-hosting stop appid te** コマンドを使用して、アプリケーションを停止します。
 - ステップ2 **show app-hosting list** コマンドを使用して、アプリケーションがアクティブ状態であるかどうかを確認します。
 - ステップ3 **app-hosting deactivate appid te** コマンドを使用して、アプリケーションを非アクティブ化します。
 - ステップ4 アプリケーションがアクティブ状態でないことを確認します。 **show app-hosting list** コマンドを使用して、アプリケーションのステータスを確認します。
 - ステップ5 **app-hosting install appid te** コマンドを使用して、アプリケーションをアンインストールします。
 - ステップ6 アンインストールプロセスが完了したら、 **show app-hosting list** コマンドを使用して、アプリケーションが正常にアンインストールされたかどうかを確認します。
-

Cisco ThousandEyes アプリケーションのトラブルシューティング

Cisco ThousandEyes アプリケーションをトラブルシューティングするには、次の手順を実行します。

1. **app-hosting connect appid appid session /bin/bash** コマンドを使用して、Cisco ThousandEyes エージェント アプリケーションに接続します。
2. 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せん。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 [elf03700] [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 scl.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。