



# システムアップグレードの実行および機能パッケージのインストール

システムアップグレードおよびパッケージインストールプロセスを実行するには、ルータで **install** コマンドを使用します。これらのプロセスでは、iso イメージ (.iso)、機能パッケージをルータ上で追加およびアクティブ化します。ネットワークサーバーからこれらのファイルにアクセスし、ルータ上でアクティブ化します。インストールしたパッケージまたは SMU が原因でルータに問題が発生した場合は、アンインストールすることができます。

この章で説明する内容は次のとおりです。

- [システムのアップグレード \(1 ページ\)](#)
- [サポートされているソフトウェアのアップグレードまたはダウングレードバージョンの表示 \(3 ページ\)](#)
- [機能のアップグレード \(8 ページ\)](#)
- [最適化されたインストールイメージのサイズ \(9 ページ\)](#)
- [準備済みパッケージのインストール \(11 ページ\)](#)
- [パッケージのインストール \(14 ページ\)](#)
- [パッケージのアンインストール \(18 ページ\)](#)
- [プラットフォームでサポートされている機能の表示 \(20 ページ\)](#)

## システムのアップグレード

システムのアップグレードとは、ルータに新しいバージョンの Cisco IOS XR オペレーティングシステムをインストールするプロセスです。ルータには Cisco IOS XR イメージがプリインストールされています。ただし、ルータ機能を最新の状態に保つために新しいバージョンをインストールすることができます。システムアップグレード操作は XR VM から実行しますが、システムアップグレードの間に、XR VM とシステム管理 VM の両方で実行しているソフトウェアがアップグレードされます。



(注) ルータ上のインターフェイスに関する設定がなく、**no-shut** 操作を実行して起動した場合、ルータのリロード時にインターフェイスの状態が自動的に **admin-shutdown** に変更されます。



- (注)
- 十分なディスク容量があることを確認します。
  - **fsck** コマンドを実行してファイルシステムのステータスを確認し、IOS XR が正常にアップグレードされていることを確認します。**fsck** コマンドは、システム管理パッケージをインストールする場合はシステム管理 EXEC モードで、XR パッケージをインストールする場合は XR EXEC モードで実行する必要があります。
  - すべての **install** コマンドは、システム管理 EXEC モードと XR EXEC モードの両方で適用できます。システム管理のインストール操作は XR EXEC モードで実行します。

システムアップグレードは、基本パッケージ (Cisco IOS XR ユニキャストルーティング コアバンドル) をインストールして実行します。このバンドルをインストールするには、**install** コマンドを実行します。Cisco IOS XR ユニキャストルーティング コアバンドルのファイル名は、*asr9k-mini-x.iso* です。



**注意** ルータのリロード時はインストール操作を実行しないでください。  
アップグレード操作中はルータをリロードしないでください。



(注) CSMサーバーは、Web ベースのサーバー側の自動化およびオーケストレーションフレームワークです。サービスプロバイダーは、クリックするだけの簡単な Web インターフェイスを使用して、複数の SMU を同時にスケジュールして展開し、何百台ものルータでソフトウェアのアップグレードをスケジュールどおりに実行できます。詳細については、[Cisco Software Manager](#) を参照してください。



(注) **install commit** コマンドを使用してトランザクションを完了せずに手動または自動のシステムリロードを実行すると、インストールトランザクションが開始される前の状態 (設定の変更を含む) にシステムが復元されます。デバッグ用に保存されるのはログのみです。

このアクションにより、使用可能なすべてのコンフィギュレーション ロールバック ポイントがクリアされます。インストールロールバックイベントが発生するまでは、実行されたコミットにロールバックしたり、コミットを表示したりはできません。インストール ロールバックイベント後に実行された新しいコミットは、コミット ID 1000000001 から開始されます。



- (注) ISSUを使用してシャーシを古いソフトウェアバージョンから IOS XR リリース 7.6.x 以降にアップグレード後、ハードウェアプログラミングを有効にするには、シャーシのリロードを開始します。該当するインターフェイスで最大伝送ユニット (MTU) 値の 9646 を有効にする必要がある場合、シャーシのリロードは必須です。

## サポートされているソフトウェアのアップグレードまたはダウングレードバージョンの表示

表 1: 機能の履歴 (表)

機能名	リリース情報	説明
サポートされている IOS XR ソフトウェアのアップグレードまたはダウングレードバージョン	リリース 7.5.1	この機能を使用して、ソフトウェアバージョンを別の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るかどうかを判断できます。実際のアップグレードやダウングレードプロセスを実行する前に、アップグレードやダウングレードが失敗する原因となるハードウェアまたはソフトウェアの制限を確認することもできます。この機能は、正常なソフトウェアのアップグレードやダウングレードを計画するのに役立ちます。  この機能では、 <b>show install upgrade-matrix</b> コマンドが導入されています。

Cisco ルータには、IOS XR ソフトウェアがプリインストールされています。ソフトウェアリリースをアップグレードして新機能とソフトウェア修正を使用するか、ソフトウェアをダウングレードします。追加された新機能または提供されているソフトウェア修正を活用するには、ルータを最新バージョンにアップグレードすることが重要です。

この機能を使用すると、シスコ認定のアップグレードおよびダウングレードパスに適合する Cisco IOS XR ソフトウェアリリースを選択するための次の質問に対する回答を得られます。

- 現在のリリースでサポートされているアップグレードまたはダウングレードリリースは何か。

- リリース X からリリース Y にアップグレードする予定です。使用中のルータではリリース Y へのアップグレードがサポートされていますか。
- ソフトウェアをアップグレードする前にインストールする必要があるブリッジング SMU はありますか。

この機能には、現在のリリースがターゲットリリースへのアップグレードをサポートしているかどうかを判断するメカニズムがあります。このタスクは、**install replace** コマンドを使用したソフトウェアのアップグレードまたはダウングレードの開始時に実行されます。検証に失敗すると、ソフトウェアのアップグレードはブロックされ、失敗の理由が表示されます。この機能を使用すると、特定のリリースにアップグレードまたはダウングレードできるかどうかをプロアクティブに検査でき、ソフトウェアの計画とアップグレードにかかる時間と労力を節約できます。

この機能は、特定のソフトウェアのアップグレードまたはダウングレードに関連する前提条件や制限事項を理解するのに役立つ次の情報を提供します。

- 必要なブリッジング SMU RPM
- SMU RPM のブロッキング
- サポートされていないハードウェア
- 注意事項または制限事項

**install replace** コマンドで **force** キーワードを使用すると、自動検証を上書きできます。このオプションを使用すると、アップグレードが失敗したときに警告メッセージが表示されますが、ソフトウェアのアップグレードはブロックされません。**force?** キーワードを使用して、ソフトウェアのアップグレードまたはダウングレードでサポートされるリリースを決定するこのプロセスの無効化以外のシステム機能に対する他の影響を理解します。

次の **show** コマンドを使用するか、運用データからサポート情報を表示できます。

コマンド	説明
<b>show install upgrade-matrix running</b>	実行中のシステムにインストールされているサポートデータに従って、現在のバージョンからのサポートされている全ソフトウェアアップグレードを表示します。
<b>show install upgrade-matrix iso path-to-ISO</b>	実行中のシステムと ISO イメージの両方のサポートデータに従って、現在のバージョンからターゲット ISO のバージョンへのソフトウェアのアップグレードに関する詳細を表示します。
<b>show install upgrade-matrix iso path-to-ISO all</b>	ターゲット ISO イメージのサポートデータに従って、任意のバージョンからのサポートされている全ソフトウェアアップグレードを表示します。

コマンド	説明
<b>show install upgrade-matrix iso path-to-ISO from-running</b>	実行中のシステムとターゲット ISO イメージの両方のサポートマトリックスに従って、現在のバージョンから ISO のバージョンへのソフトウェアのアップグレードに関する詳細を表示します。

### 実行中のバージョンからのサポートされている全ソフトウェアアップグレードの表示

次に、ルータの現在のバージョン7.5.1からのアップグレードでサポートされている全リリースの例を示します。

```
Router#show install upgrade-matrix running
```

```
Fri Jul 29 10:18:43.413 IST
```

```
This may take a while ...
```

```
The current software [7.5.1] can be upgraded from and downgraded to the following releases:
```

```
=====
```

From	To	Bridge SMUs Required	Caveats
7.0.2	7.5.1	r702.CSCvw57276	None
6.5.3	7.5.1	r653.CSCvw57276	None
7.5.1	7.0.2	None	None
7.5.1	6.5.3	None	- <a href="https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-4/system-security/configuration/guide/b-system-security-cg-asr9000-74x/configuring-aaa-services.html#id_128191">https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-4/system-security/configuration/guide/b-system-security-cg-asr9000-74x/configuring-aaa-services.html#id_128191</a>
7.5.1	7.4.1	None	None
7.5.1	7.1.25	None	None
7.5.1	7.1.3	None	None
7.5.1	7.1.2	None	None
7.5.1	7.3.1	None	None
7.5.1	6.6.3	None	- <a href="https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-4/system-security/configuration/guide/b-system-security-cg-asr9000-74x/configuring-aaa-services.html#id_128191">https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-4/system-security/configuration/guide/b-system-security-cg-asr9000-74x/configuring-aaa-services.html#id_128191</a>
7.5.1	7.3.2	None	None
7.4.1	7.5.1	None	None

```
=====
```

## サポートされているソフトウェアのアップグレードまたはダウングレードバージョンの表示

7.1.25	7.5.1	None	None
7.1.3	7.5.1	None	None
7.1.2	7.5.1	None	None
7.3.1	7.5.1	None	None
6.6.3	7.5.1	r663.CSCvw57276	None
7.3.2	7.5.1	None	None

## 現在のバージョンからターゲットバージョンにソフトウェアをアップグレードするためにサポートされているリリースの表示

次に、ソフトウェアを現在のバージョンからターゲットバージョンにアップグレードするためにサポートされているリリースの例を示します。

```
Router#show install upgrade-matrix iso /harddisk:/asr9k-goldenk9-x64-7.5.2-rev1.iso
```

```
Fri Jul 29 10:19:24.185 IST
This may take a while ...
Upgrade from the current software [7.5.1] to 7.5.2 is supported
=====
From      To      Bridge SMUs Required      Caveats
=====
7.5.1     7.5.2   None                       None
=====
```

現在のイメージには、サポートされているアップグレードまたは特定のバージョンへのダウングレードバージョンのみを指定するアップグレードマトリックスがあります。現在のマトリックスのバージョンよりも新しいバージョンのISOのアップグレードパスを決定する場合は、新しいISOのアップグレードマトリックスに、サポートされているアップグレードまたはダウングレードパスが記載されています。

## 現在のバージョンからISOバージョンへのサポートされているリリースの表示

次に、ソフトウェアアップグレードパス、ダウングレードパス、および現在のバージョンからターゲットISOバージョンへのアップグレードの制限事項の例を示します。

```
Router#show install upgrade-matrix iso /harddisk:/ asr9k-goldenk9-x64-7.5.2-rev1.iso all
Fri Jul 29 10:20:10.961 IST
This may take a while ...
```

```
7.5.2 can be upgraded from and downgraded to the following releases:
```

7.0.2	7.5.2	r702.CSCvw57276	None
7.5.1	7.5.2	None	None
7.4.2	7.5.2	None	None
7.4.1	7.5.2	None	None

7.5.2	7.0.2	None	None
7.5.2	6.5.3	None	- <a href="https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-4/system-security/configuration/guide/b-system-security-cg-asr9000-74x/configuring-aaa-services.html#id_128191">https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-4/system-security/configuration/guide/b-system-security-cg-asr9000-74x/configuring-aaa-services.html#id_128191</a>
7.5.2	7.1.25	None	None
7.5.2	7.4.2	None	None
7.5.2	7.6.1	None	None
7.5.2	7.4.1	None	None
7.5.2	7.1.3	None	None
7.5.2	7.1.2	None	None
7.5.2	7.3.1	None	None
7.5.2	6.6.3	None	- <a href="https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-4/system-security/configuration/guide/b-system-security-cg-asr9000-74x/configuring-aaa-services.html#id_128191">https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r7-4/system-security/configuration/guide/b-system-security-cg-asr9000-74x/configuring-aaa-services.html#id_128191</a>
7.5.2	7.3.2	None	None
7.1.25	7.5.2	None	None
7.1.3	7.5.2	None	None
7.1.2	7.5.2	None	None
7.6.1	7.5.2	None	None
6.5.3	7.5.2	r653.CSCvw57276	None
7.3.1	7.5.2	None	None
6.6.3	7.5.2	r663.CSCvw57276	None
7.3.2	7.5.2	None	None

### 実行中のバージョンから ISO バージョンへのサポートされているリリースの表示

次に、実行中のシステムとターゲット ISO イメージの両方のサポートマトリックスに従った現在のバージョンから ISO のバージョンへのソフトウェアのアップグレードに関する詳細を表示する例を示します。

```
Router#show install upgrade-matrix iso /harddisk:/asr9k-goldenk9-x64-7.5.2-rev1.iso
from-running
Fri Jul 29 10:21:31.957 IST
```

```
This may take a while ...
Upgrade from the current software [7.5.1] to 7.5.2 is supported
```

From	To	Bridge SMUs Required	Caveats
7.5.1	7.5.2	None	None

## 機能のアップグレード

機能のアップグレードとは、ルータに新機能とソフトウェアパッチを導入するプロセスです。パッケージをインストールして機能のアップグレードを実行します。ソフトウェアパッチのインストールは、ソフトウェアメンテナンスアップグレード（SMU）ファイルをインストールして実行します。

ルータにパッケージをインストールすると、そのパッケージに含まれる特定の機能がインストールされます。Cisco IOS XR ソフトウェアはさまざまなソフトウェアパッケージに分割されているため、ルータで実行する機能を選択できます。各パッケージには、ルーティングやセキュリティなど、特定のルータ機能のセットを実行するコンポーネントが含まれています。

たとえば、ルーティングパッケージのコンポーネントは、BGP や OSPF など、個別の RPM に分かれています。BGP は基本ソフトウェアバージョンの一部であり、必須 RPM なので削除できません。ただし、OSPF などの任意の RPM は、必要に応じて追加および削除できます。

パッケージの命名規則は <platform>-<pkg>-<pkg version>-<release version>.<architecture>.rpm です。

次に例を示します。

```
asr9k-9000v-nV-x64-1.0.0.0-r702.x86_64.rpm
```

**install** コマンドを使用して、パッケージと SMU をインストールします。インストールプロセスの詳細については、[パッケージのインストール（14 ページ）](#) を参照してください。



- (注)
- 十分なディスク容量があることを確認します。
  - fsck** コマンドを実行してファイルシステムのステータスを確認し、IOS XR が正常にアップグレードされていることを確認します。**fsck** コマンドは、システム管理パッケージをインストールする場合はシステム管理 EXEC モードで、XR パッケージをインストールする場合は XR EXEC モードで実行する必要があります。
  - すべての **install** コマンドは、システム管理 EXEC モードと XR EXEC モードの両方で適用できます。システム管理のインストール操作は XR EXEC モードで実行します。

XR VM とシステム管理 VM 用の個別のパッケージと SMU があります。それぞれをそのファイル名で識別できます。

たとえば、asr9k-px-7.9.1.CSCvu59908.pie は XR VM のパッケージの例です。asr9k-sysadmin-7.9.1.pie は、システム管理 VM に関連付けられます。



XR パッケージや SMU は XR VM からアクティブ化されますが、システム管理パッケージや SMU はシステム管理 VM からアクティブ化されます。

または、XR からシステム管理パッケージと SMU をアクティブ化または非アクティブ化することで、クロス VM 操作を実行できます。

## 最適化されたインストールイメージのサイズ

表 2: 機能の履歴 (表)

機能名	リリース情報	説明
最適化されたインストールイメージのサイズ	リリース 7.3.1	このリリースでは、ルータにインストールされている Cisco ISO イメージのサイズが約 300 MB 縮小されているため、ルータのディスク容量が解放され、パッケージのインストールにかかる時間が短縮されます。

Cisco IOS XR リリース 7.3.1 では、イメージ全体のサイズが約 300 MB 縮小され、最適化されたバージョンの mini-x ISO イメージが導入されています。この最適化された ISO により、インストール操作にかかる時間が短縮され、インストールリポジトリに保存されているファイルのディスク容量の使用率が削減されます。

この最適化された ISO は、次の方法を使用したルータの起動をサポートしています。

- iPXE ブート
- USB ブート
- システムのアップグレード
- In-Service Software Upgrade (ISSU)

ISSU の場合、下位バージョンからリリース 7.3.1 以降にアップグレードするには、実行中の下位バージョンにブリッジ SMU が必要です。一方、リリース 7.3.1 以降から下位バージョンへのロールバックには、ブリッジ SMU は必要ありません。SMU がインストールされているリリース 7.3.1 から古いバージョンにダウングレードする場合、SMU に依存関係はありません。ブリッジ SMU は必須の前提条件であり、リリース 7.3.1 以降へのアップグレードを実行する前に、実行中のバージョンにインストールする必要があります。

次に、下位の実行中のバージョンにインストールする必要があるホスト、XR、およびシステム管理用のブリッジ SMU を示します。たとえば、リリース 7.1.1 の場合は次のようになります。

- asr9k-iosxr-infra-64-3.0.0.2-r711.CSCvq46421.x86\_64.rpm

- asr9k-iosxr-os-64-3.0.0.2-r711.CSCvq46421.x86\_64.rpm
- asr9k-sysadmin-system-7.1.1-r711.CSCvq46421.x86\_64.rpm

ブリッジ SMU は、Download Software Center にある特定のリリースの Cisco IOS XR ソフトウェアの tar バンドルに含まれています。

インストール操作に関連するコマンドでは、common という用語を含む新しいパッケージが表示されます。共通パッケージは、NETCONF YANG モードを使用して実行した場合、install コマンドの出力にも表示されます。



(注) **show install active summary** および **show install committed summary** コマンドの common 用語はリストされていません。

共通パッケージは、システム管理 VM の /misc/disk1/tftpboot にあります。

common という用語は、システム管理 VM および XR VM の **show install repository** または **show install repository all** コマンドの出力にも表示されます。

次に、システム管理 VM からの出力例を示します。

```
sysadmin-vm:0_RSP0# show install repository
Sat May 2 16:33:25.200 UTC+00:00
Admin repository
-----
asr9k-common-7.3.1
asr9k-goldenk9-x64-7.3.1-supersetOptInstallSmu
asr9k-mini-x64-7.3.1
asr9k-sysadmin-7.3.1
asr9k-sysadmin-hostos-7.3.1-r731.admin.x86_64
asr9k-sysadmin-hostos-7.3.1-r731.host.x86_64
asr9k-sysadmin-hostos-7.3.1-r731.CSCho77777.admin.x86_64
asr9k-sysadmin-hostos-7.3.1-r731.CSCho77777.host.x86_64
asr9k-sysadmin-hostos-7.3.1-r731.admin.x86_64
asr9k-sysadmin-hostos-7.3.1-r731.host.x86_64
asr9k-sysadmin-hostos-7.3.1-r731.CSCho77777.admin.x86_64
asr9k-sysadmin-hostos-7.3.1-r731.CSCho77777.host.x86_64
asr9k-sysadmin-shared-7.3.1-r731.CSCcv33333.x86_64
asr9k-sysadmin-shared-7.3.1-r731.CSCcv33333.x86_64
asr9k-sysadmin-system-7.3.1-r731.CSCcv11111.x86_64
asr9k-sysadmin-system-7.3.1-r731.CSCcv22222.x86_64
----- Truncated for Brevity -----
```

次に、XR VM からの出力例を示します。

```
Router#show install repository
Sat May 2 13:55:59.996 UTC
26 package(s) in XR repository:
asr9k-iosxr-infra-64-1.0.0.1-r731.CSCxr22222.x86_64
asr9k-iosxr-infra-64-1.0.0.2-r731.CSCxr44444.x86_64
asr9k-k9sec-x64-2.1.0.0-r731.x86_64
asr9k-optic-x64-1.0.0.0-r731.x86_64
asr9k-mgbl-x64-2.0.0.0-r731.x86_64
asr9k-mpls-te-rsvp-x64-2.1.0.0-r731.x86_64
asr9k-common-7.3.1
asr9k-goldenk9-x64-7.3.1-supersetOptInstallSmu
```

```
asr9k-bng-x64-1.0.0.0-r731.x86_64
asr9k-mini-x64-7.3.1
asr9k-mpls-x64-2.0.0.0-r731.x86_64
asr9k-li-x64-1.1.0.0-r73104I.x86_64
----- Truncated for Brevity -----
```

コマンド出力の `asr9k-common-7.3.1` は、イメージサイズを縮小するために最適化されたパッケージを表します。

## 準備済みパッケージのインストール

システムアップグレードまたは機能アップグレードは、ISO イメージファイル、パッケージ、および SMU をアクティブ化することで実行します。アクティベーション前にこれらのインストール可能なファイルを準備することができます。準備フェーズでは、アクティベーション前のチェックが実行され、インストール可能なファイルのコンポーネントがルータ設定にロードされます。準備プロセスはバックグラウンドで実行されるため、その間もルータをフルに利用できます。準備フェーズが完了したら、すべての準備済みファイルを即座にアクティブ化できます。アクティベーション前の準備には、次の利点があります。

- インストール可能なファイルが破損していると、準備プロセスは失敗します。これによって問題が早期に警告されます。破損したファイルが直接アクティブ化されると、ルータの誤動作を招く可能性があります。
- システムアップグレード用の ISO イメージを直接アクティブ化するには時間がかかり、その間にルータを使用できなくなります。ただし、アクティベーション前にイメージを準備すると、準備プロセスが非同期で実行されるだけでなく、準備済みのイメージを後でアクティブ化するとき、アクティベーションプロセスにかかる時間も短縮されます。その結果、ルータのダウンタイムが大幅に削減されます。
- 正常な操作に必要なディスク容量チェックが実行されるため、ディスク容量の不足が定量化され、ファイルシステムの領域を解放するための可能な代替手段が提供されます。
- パッケージの互換性チェックが実行されるため、必要なすべてのインストールパッケージが使用可能になります。パッケージ互換性チェックエラーの場合、パッケージとバージョンの詳細がログに記録されます。

システムのアップグレードおよびパッケージのインストールに準備動作を利用するには、次のタスクを実行します。



- (注) システム管理パッケージまたは XR パッケージのどちらをインストールするかによって、それぞれ `install` モードまたは `install` モードで `install` コマンドを実行します。すべての `install` コマンドは両方のモードで使用できます。システム管理のインストール動作は XR モードで実行できます。

**ステップ 1** 必要な ISO イメージおよびパッケージをリポジトリに追加します。

詳細については、[パッケージのインストール \(14 ページ\)](#) を参照してください。

## ステップ2 show install repository

例：

```
RP/0/RSP0/cpu 0: router#show install repository
```

必要なインストール可能ファイルがリポジトリ内にあることを確認するには、この手順を実行します。パッケージは「install add」動作の完了後にのみ表示されます。

## ステップ3 show install request

例：

```
RP/0/RSP0/cpu 0: router#show install request
```

(任意) 追加動作の動作 ID とステータスを表示します。動作 ID は、後で **activate** コマンドを実行する際に使用できます。

```
Install operation 8 is still in progress
```

## ステップ4 次のいずれかを実行します。

- **install prepare** *package\_name*
- **install prepare id** *operation\_id*

例：

準備プロセスが開始されます。この動作は非同期モードで実行されます。**install prepare** コマンドはバックグラウンドで実行され、EXEC プロンプトは最短で返されます。

動作 ID を使用すると、指定した動作に追加されたすべてのパッケージの準備がまとめて行われます。たとえば 5 つのパッケージが動作 8 に追加されている場合、**install prepare id 8** を実行すると、5 つのパッケージがすべてまとめて準備されます。パッケージを個別に準備する必要はありません。

## ステップ5 show install prepare

例：

```
RP/0/RSP0/cpu 0: router#show install prepare
```

準備済みのパッケージを表示します。この結果で、必要なすべてのパッケージが準備されていることを確認します。

## ステップ6 install activate

例：

```
RP/0/RSP0/cpu 0: router#install activate
```

準備の完了したすべてのパッケージをまとめてアクティブ化し、ルータでパッケージ設定をアクティブにします。

(注) CLI でパッケージ名または動作 ID を指定しないでください。

SMU によっては、アクティベーション時にルータの手動リロードが必要な場合があります。このような SMU をアクティブ化すると、リロードを実行するための警告メッセージが表示されます。SMU のコンポーネントは、リロードの完了後にのみアクティブ化されます。**install activate** コマンドの完了後すぐにルータのリロードを実行します。

## ステップ7 show install active

例：

```
RP/0/RSP0/cpu 0: router#show install active
```

アクティブなパッケージを表示します。

この結果で、すべての RP と LC でイメージおよびパッケージの同じバージョンがアクティブになっていることを確認します。

## ステップ 8 install commit

例：

```
RP/0/RSP0/cpu 0: router#install commit
```

### パッケージのインストール：関連コマンド

関連コマンド	目的
<b>show install log</b>	インストールプロセスのログ情報を表示します。これはインストールが失敗した場合のトラブルシューティングに使用できます。
<b>show install package</b>	リポジトリに追加されたパッケージの詳細を表示します。このコマンドは、パッケージの個々のコンポーネントを識別する際に使用します。
<b>install prepare clean</b>	準備動作をクリアし、すべてのパッケージを準備済み状態から削除します。

### 次のタスク

- システムのアップグレードの実行後、システム管理 モードから **upgrade hw-module location all fpd all** コマンドを使用して FPD をアップグレードします。FPD アップグレードプロセスの進捗状況は、システム管理 モードで **show hw-module fpd** コマンドを使用してモニターできます。FPD アップグレードが完了したら、ルータをリロードします。
- **install verify packages** コマンドを使用してインストールを確認します。
- インストールによってルータに問題が発生した場合は、該当するパッケージまたは SMU をアンインストールしてください。[パッケージのアンインストール](#)を参照してください。



(注) ISO イメージはアンインストールできません。ただし、旧バージョンの ISO をインストールすることでシステムダウングレードを実行することができます。

## パッケージのインストール

システムをアップグレードするか、パッチをインストールするには、このタスクを完了します。システムアップグレードは ISO イメージファイルを使用して行いますが、パッチインストールの場合はパッケージおよび SMU を使用します。アップグレード操作には、ミニ ISO とともに SMU も含めることができます。

.rpm ファイルをインストールする際もこのタスクを使用します。rpm ファイルには、1つのファイルに統合された複数のパッケージと SMU が含まれています。カードタイプにかかわらず、パッケージ形式によってコンポーネントごとに 1つの RPM が定義されます。



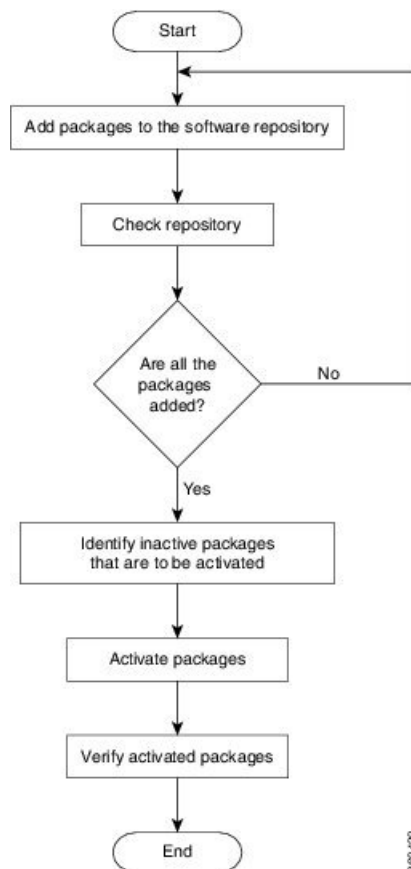
- (注)
- 十分なディスク容量があることを確認します。
  - **fsck** コマンドを実行してファイルシステムのステータスを確認し、IOS XR が正常にアップグレードされていることを確認します。**fsck** コマンドは、システム管理パッケージをインストールする場合はシステム管理 EXEC モードで、XR パッケージをインストールする場合は XR EXEC モードでを実行する必要があります。
  - すべての **install** コマンドは、システム管理 EXEC モードと XR EXEC モードの両方で適用できます。システム管理のインストール操作は XR EXEC モードで実行します。



- (注)
- システムアップグレードは、XR EXEC モードからのみサポートされています。
  - システム管理パッケージはシステム管理 EXEC モードおよび XR EXEC モードで **install** コマンドを使用して実行できますが、XR パッケージは XR EXEC モードで **install** コマンドを使用してのみ実行できます。すべての **install** コマンドは両方のモードで使用できます。
  - システム管理 SMU はシステム管理 EXEC モードおよび XR EXEC モードでインストールできますが、XR SMU は XR EXEC モードでのみインストールできます。
  - IPv6 を介したインストール操作はサポートされていません。

パッケージをインストールするためのワークフローを次のフローチャートに示します。

図 1: パッケージインストールのワークフロー



### 始める前に

- 管理ポートを設定して接続します。インストール可能なファイルには管理ポートからアクセスできます。
- インストールするパッケージを、ルータのハードディスク、またはルータがアクセスできるネットワーク サーバーにコピーします。

**ステップ 1** 次のいずれかを実行します。

- **install add source** <http or shttp transfer protocol>/package\_path/ filename1 filename2 ...
- **install add source** <tftp transfer protocol>/package\_path/ filename1 filename2 ...
- **install add source** <ftp or sftp transfer protocol>/user@server:/package\_path/ filename1 filename2 ...

例 :

```
RP/0/RSP0/cpu 0: router#install add source /harddisk:/ asr9k-mpls-x64-2.1.0.0-r731.x86_64.rpm
asr9k-mpls-x64-2.1.0.0-r732.x86_64.rpm
```

または

```
RP/0/RSP0/cpu 0: router#install add source sftp://root@8.33.5.15:/auto/ncs/package/
asr9k-mcast-1.0.0.0-731.x86_64.rpm asr9k-iosxr-mpls-1.0.0.0-732.x86_64.rpm
```

または

```
RP/0/RSP0/cpu 0: router#install add source /harddisk:/
asr9k-mpls-x64-2.1.0.0-<release-number>.x86_64.rpm asr9k-mpls-x64-2.1.0.0-<release-number>.x86_64.rpm
```

または

```
RP/0/RSP0/cpu 0: router#install add source sftp://root@8.33.5.15:/auto/ncs/package/
asr9k-mcast-1.0.0.0-<release-number>.x86_64.rpm asr9k-iosxr-mpls-1.0.0.0-<release-number>.x86_64.rpm
```

(注) *package\_path* と *filename* の間にはスペースが必要です。

パッケージからソフトウェアファイルが展開され、検証されてからソフトウェアリポジトリに追加されます。追加するファイルのサイズによっては、この処理に時間がかかる場合があります。動作は非同期モードで実行されます。**install add** コマンドはバックグラウンドで実行され、すべてのファイルが展開されると EXEC プロンプトが返されます。

(注) XR VM とシステム管理 VM のリポジトリは異なります。ルーティングパッケージは XR VM リポジトリに、システム管理パッケージはシステム管理 VM リポジトリに自動的に追加されます。

## ステップ 2 show install request

例：

```
RP/0/RSP0/cpu 0: router#show install request
```

(任意) 追加動作の動作 ID とステータスを表示します。動作 ID は、後で **activate** コマンドを実行する際に使用できます。

```
Install operation 8 is still in progress
```

## ステップ 3 show install repository

例：

```
RP/0/RSP0/cpu 0: router#show install repository
```

リポジトリに追加されるパッケージを表示します。パッケージは **install add** 動作の完了後にのみ表示されます。

## ステップ 4 show install inactive

例：

```
RP/0/RSP0/cpu 0: router#show install inactive
```

リポジトリ内に存在する非アクティブなパッケージを表示します。アクティブ化できるのは非アクティブなパッケージだけです。

ステップ 5 次のいずれかを実行します。

- **install activate** *package\_name*
- **install activate id** *operation\_id*

例：



`operation_id` は **install add** 操作の ID です。 [パッケージのインストール \(14 ページ\)](#) の [ステップステップ 2 \(16 ページ\)](#) を参照してください。このコマンドは、システム管理モードからも実行できます。パッケージ設定がルータでアクティブになります。その結果、新機能とソフトウェア修正が有効になります。この操作は、デフォルトの非同期モードで実行されます。**install activate** コマンドはバックグラウンドで実行され、EXEC プロンプトが返されます。

同期モードを使用するか、CLI から `[sync]` オプションを選択して、アクティブ化操作を実行できます。

動作 ID を使用すると、指定した動作に追加されたすべてのパッケージがまとめてアクティブ化されます。たとえば、5 つのパッケージが動作 ID 8 に追加されている場合、**install activate id 8** を実行すると、5 つのパッケージがすべてまとめてアクティブ化されます。パッケージを個別にアクティブ化する必要はありません。

アクティベーションは瞬時には完了せず、ある程度の時間がかかります。アクティブ化が完了すると、システムが自動的にリロードします。再起動 SMU アクティベーションの場合、SMU の影響を受けるプロセスが再起動されると、SMU が有効になります。

SMU が XR VM とシステム管理 VM の両方と依存関係がある場合は、両方の VM で SMU をアクティブ化した後でリロードを実行すると、両方で同時に反映されます。ルータをリロードするには、システム管理 EXEC モードから **hw-module location all reload** コマンドを使用します。

## ステップ 6 show install active

例：

```
RP/0/RSP0/cpu 0: router#show install active
```

アクティブなパッケージを表示します。

この結果で、すべての RP と LC でイメージおよびパッケージの同じバージョンがアクティブになっていることを確認します。

表 3: 例：パッケージのインストール：関連コマンド

関連コマンド	目的
<b>show install log</b>	インストールプロセスのログ情報を表示します。これはインストールが失敗した場合のトラブルシューティングに使用できます。
<b>show install package</b>	リポジトリに追加されたパッケージの詳細を表示します。このコマンドは、パッケージの個々のコンポーネントを識別する際に使用します。
<b>install prepare</b>	アクティベーションの準備として、非アクティブなパッケージに対してアクティベーション前のチェックを実行します。
<b>show install prepare</b>	準備が完了してアクティベーション可能になったパッケージのリストを表示します。

## ステップ 7 install commit

例：

```
RP/0/RSP0/cpu 0: router#install commit
```

ホスト、XR、およびシステム管理で新たにアクティブになったソフトウェアをコミットします。

- (注) マルチ SDR モードでは、**install commit sdr** を使用して、CLI がトリガーされている場所から SDR のみをコミットできます。詳細については、「[Secure Domain Router Commands](#)」を参照してください。

### 次のタスク

- システムのアップグレードの実行後、システム管理 モードから **upgrade hw-module location all fpd all** コマンドを使用して FPD をアップグレードします。FPD アップグレードプロセスの進捗状況は、システム管理 モードで **show hw-module fpd** コマンドを使用してモニターできます。FPD アップグレードが完了したら、ルータをリロードします。
- **install verify packages** コマンドを使用してインストールを確認します。
- インストールによってルータに問題が発生した場合は、該当するパッケージまたは SMU をアンインストールしてください。[パッケージのアンインストール \(18 ページ\)](#) を参照してください。

## パッケージのアンインストール

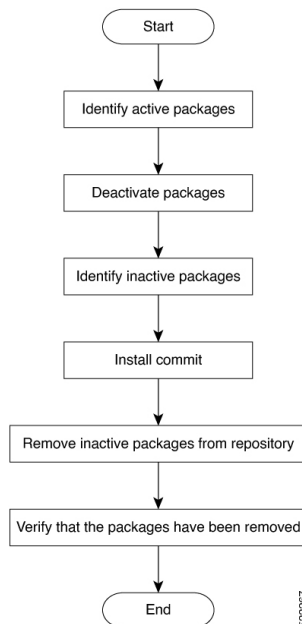
パッケージをアンインストールするには、次のタスクを実行します。アンインストールしたパッケージに含まれるすべてのルータ機能は非アクティブ化されます。XR VM で追加したパッケージは、システム管理 VM からはアンインストールできません。ただし、クロス VM 操作では、XR からシステム管理パッケージを非アクティブ化できます。



- (注) インストール済みの ISO イメージはアンインストールできません。また、ホスト、XR VM、およびシステム管理 VM でサードパーティ製 SMU をインストールするカーネル SMU もアンインストールできません。ただし、ISO イメージまたはカーネル SMU を新たにインストールすると既存のインストールが上書きされます。

パッケージをアンインストールするためのワークフローを次のフローチャートに示します。

図 2: パッケージアンインストールのワークフロー



このタスクでは、XR VM パッケージをアンインストールします。システム管理パッケージをアンインストールする場合は、同じコマンドを `mode` で実行します。

### ステップ 1 `show install active`

例 :

```
RP/0/RSP0/cpu 0: router#show install active
```

アクティブなパッケージを表示します。非アクティブ化できるのはアクティブなパッケージだけです。

ステップ 2 次のいずれかを実行します。

- `install deactivate package_name`
- `install deactivate id operation_id`

例 :

`operation_id` は `install add` 動作の ID です。パッケージに関連するすべての機能およびソフトウェアパッチが非アクティブ化されます。複数のパッケージ名を指定して同時に非アクティブ化できます。

動作 ID を使用すると、指定した動作に追加されたすべてのパッケージがまとめて非アクティブ化されません。パッケージを個別に非アクティブ化する必要はありません。`install add` 動作（非アクティブ化で使った ID の動作）の一部として追加されたシステム管理パッケージがある場合、これらも非アクティブ化されます。

### ステップ 3 `show install inactive`

例 :

```
RP/0/RSP0/cpu 0: router#show install inactive
```

非アクティブ化済みのパッケージは、非アクティブなパッケージとして表示されるようになります。非アクティブなパッケージのみリポジトリから削除できます。

#### ステップ 4 `install commit`

#### ステップ 5 `install remove package_name`

例：

非アクティブなパッケージがリポジトリから削除されます。

指定した動作 ID に追加されているすべてのパッケージを削除するには、`id operation-id` キーワードおよび引数を指定して `install remove` コマンドを使用します。

また、`install remove inactive all` を使用して、XR およびシステム管理からすべての非アクティブなパッケージを削除できます。

#### ステップ 6 `show install repository`

例：

```
RP/0/RSP0/cpu 0: router#show install repository
```

リポジトリ内の使用可能なパッケージを表示します。削除されたパッケージは結果に表示されなくなります。

### 次のタスク

必要なパッケージをインストールします。。

## プラットフォームでサポートされている機能の表示

表 4: 機能の履歴 (表)

機能名	リリース情報	説明
プラットフォームでサポートされている機能の表示	リリース 7.5.2	この機能には、ルータのリリースでサポートされている機能とサポートされていない機能のリストが表示されます。この機能を使用すると、サポート情報用の注釈付き機能を使用して、ネットワーク設定をより適切に計画できます。この機能では、 <code>show features</code> コマンドが導入されています。

この機能では、「Is feature X supported on my router?」という質問に対する回答を得られません。

使用しているルータのリリースで機能がサポートされているかどうかを確認できます。サポート情報は、リリースおよびプラットフォーム固有のデータ（ルータに存在するプラットフォームバリエーション、RP、LC など）に基づいています。



- (注) Cisco IOS XR ソフトウェアリリース 7.5.2 では、アクセス制御リスト (ACL) 機能のみがサポートされています。

サポートされているリリースがルータにインストールされている場合、機能情報を決定する機能はデフォルトで有効になっています。

サポートされている機能と機能のリストを表示するには、**show features** コマンドを使用します。機能は、サポート情報の表記とともにツリー構造で表示されます。たとえば、ACL では、多数のアクセス制御エレメント (ACE) に対応するために圧縮を使用する機能がサポートされていますが、IPv6 ACL BNG には、Cisco IOS XR ソフトウェアリリース 7.5.2 のサポートデータがありません。機能に関するこのサポート情報は、ツリー構造の次のキーで表されます。

キー	機能サポート情報	説明
X	Unsupported	機能は、当該リリースのプラットフォームではサポートされていません。
-	サポート対象	機能は、当該リリースのプラットフォームでサポートされています。
?	サポートは不明	機能のサポートについては、当該リリースのプラットフォームでは不明です。機能のオプションパッケージがルータにインストールされていないことが原因である可能性があります。
*	サポートデータがありません	機能のサポートは、当該リリースのプラットフォームでは使用できません。機能がルータに存在しないラインカードに固有であることが原因である可能性があります。

#### サポート対象機能のリストの表示

この例では、ルータでサポートされている機能が表示されます。



- (注) Cisco IOS XR ソフトウェアリリース 7.5.2 では、アクセス制御リスト (ACL) の機能のみがサポートされています。

```
Router#show features
Fri Jun 3 19:16:58.298 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Cisco IOS XR
```

## プラットフォームでサポートされている機能の表示

```

|--[-] XR Protocols
| |--[-] XR Base Protocols
| | |--[-] Services
| | | |--[-] Access Control List (ACL)
| | | | |--[-] IPv6 ACL Support
| | | | | |--[*] IPv6 ACL ABF Track
| | | | | |--[*] IPv6 ACL BNG
| | | | | |--[*] IPv6 ACL Chaining (Meta ACL)
| | | | | |--[-] IPv6 ACL Common ACL
| | | | | |--[-] IPv6 ACL Compression
| | | | | |--[*] IPv6 ACL Default ABF
| | | | | |--[*] IPv6 ACL Fragment
| | | | | |--[-] IPv6 ACL ICMP Off
| | | | | |--[-] IPv6 ACL ICMP Protocol
| | | | | |--[-] IPv6 ACL Interface Statistics
| | | | | |--[-] IPv6 ACL Log Rate
| | | | | |--[-] IPv6 ACL Log Threshold
| | | | | |--[-] IPv6 ACL Logging
| | | | | |--[-] IPv6 ACL MIB
| | | | | |--[-] IPv6 ACL Object Groups (Scale)
| | | | | |--[-] IPv6 ACL Police
| | | | | |--[-] IPv6 ACL Priority
| | | | | |--[*] IPv6 ACL Protocol Range
| | | | | |--[-] IPv6 ACL Set Qos-Group
| | | | | |--[-] IPv6 ACL Set TTL
| | | | | |--[-] IPv6 ACL TCP Flags
| | | | | |--[-] IPv6 ACL TTL Match
| | | | | |--[-] IPv6 ACL UDF
| | | | |--[-] ES-ACL Support (L2 ACL)
| | | |--[-] IPv4 ACL Support
| | | | |--[-] IPv4 ACL Set Qos-group
| | | | |--[*] IPv4 ACL ABF Track
| | | | |--[*] IPv4 ACL BNG
| | | | |--[*] IPv4 ACL Chaining (Meta ACL)
| | | | |--[-] IPv4 ACL Common ACL
| | | | |--[-] IPv4 ACL Compression
| | | | |--[*] IPv4 ACL Default ABF
| | | | |--[*] IPv4 ACL Fragment
| | | | |--[-] IPv4 ACL Fragment Flags
| | | | |--[-] IPv4 ACL ICMP Off
| | | | |--[-] IPv4 ACL ICMP Protocol
| | | | |--[-] IPv4 ACL Interface Statistics
| | | | |--[-] IPv4 ACL Log Rate
| | | | |--[-] IPv4 ACL Log Threshold
| | | | |--[-] IPv4 ACL Logging
| | | | |--[-] IPv4 ACL MIB
| | | | |--[-] IPv4 ACL Object Groups (Scale)
| | | | |--[-] IPv4 ACL Police
| | | | |--[-] IPv4 ACL Priority
| | | | |--[*] IPv4 ACL Protocol Range
| | | | |--[-] IPv4 ACL Set TTL
| | | | |--[-] IPv4 ACL TCP Flags
| | | | |--[-] IPv4 ACL TTL
| | | | |--[-] IPv4 ACL UDF
| | | |--[-] IPv4 Prefix-List
| | |--[-] IPv6 Prefix-List

```

## サポートされている ACL 機能のリストの表示

この例では、ルータの ACL 機能が表示されます。

```
Router#show features acl
Fri Jun 3 19:17:31.635 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Access Control List (ACL)
|--[-] IPv6 ACL Support
| |--[*] IPv6 ACL ABF Track
| |--[*] IPv6 ACL BNG
| |--[*] IPv6 ACL Chaining (Meta ACL)
| |--[-] IPv6 ACL Common ACL
| |--[-] IPv6 ACL Compression
| |--[*] IPv6 ACL Default ABF
| |--[*] IPv6 ACL Fragment
| |--[-] IPv6 ACL ICMP Off
| |--[-] IPv6 ACL ICMP Protocol
| |--[-] IPv6 ACL Interface Statistics
| |--[-] IPv6 ACL Log Rate
| |--[-] IPv6 ACL Log Threshold
| |--[-] IPv6 ACL Logging
| |--[-] IPv6 ACL MIB
| |--[-] IPv6 ACL Object Groups (Scale)
| |--[-] IPv6 ACL Police
| |--[-] IPv6 ACL Priority
| |--[*] IPv6 ACL Protocol Range
| |--[-] IPv6 ACL Set Qos-Group
| |--[-] IPv6 ACL Set TTL
| |--[-] IPv6 ACL TCP Flags
| |--[-] IPv6 ACL TTL Match
| |--[-] IPv6 ACL UDF
|--[-] ES-ACL Support (L2 ACL)
|--[-] IPv4 ACL Support
| |--[-] IPv4 ACL Set Qos-group
| |--[*] IPv4 ACL ABF Track
| |--[*] IPv4 ACL BNG
| |--[*] IPv4 ACL Chaining (Meta ACL)
| |--[-] IPv4 ACL Common ACL
| |--[-] IPv4 ACL Compression
| |--[*] IPv4 ACL Default ABF
| |--[*] IPv4 ACL Fragment
| |--[-] IPv4 ACL Fragment Flags
| |--[-] IPv4 ACL ICMP Off
| |--[-] IPv4 ACL ICMP Protocol
| |--[-] IPv4 ACL Interface Statistics
| |--[-] IPv4 ACL Log Rate
| |--[-] IPv4 ACL Log Threshold
| |--[-] IPv4 ACL Logging
| |--[-] IPv4 ACL MIB
| |--[-] IPv4 ACL Object Groups (Scale)
| |--[-] IPv4 ACL Police
| |--[-] IPv4 ACL Priority
| |--[*] IPv4 ACL Protocol Range
| |--[-] IPv4 ACL Set TTL
| |--[-] IPv4 ACL TCP Flags
| |--[-] IPv4 ACL TTL
| |--[-] IPv4 ACL UDF
|--[-] IPv4 Prefix-List
|--[-] IPv6 Prefix-List
```

## 特定の RP でサポートされている ACL 機能のリストの表示

この例では、RP ロケーション 0/RP0/CPU0 の ACL 機能が表示されます。

```
Router#show features acl detail location 0/RP0/CPU0
Fri Jun 3 19:15:49.889 UTC
Key:
X - Unsupported
- - Supported
? - Support unknown (optional package not installed)
* - Support data not available

[-] Access Control List (ACL)
Cisco provides basic traffic filtering capabilities with access control
lists (also referred to as access lists). User can configure access
control lists (ACLs) for all routed network protocols to filter protocol
packets when these packets pass through a device. User can configure
access lists on your device to control access to a network, access lists
can prevent certain traffic from entering or exiting a network.

|--[-] IPv6 ACL Support
|
| IPv6 based ACL is a list of source IPv6 addresses that use Layer 3 or
| Layer 4 information to permit or deny access to traffic. IPv6 router
| ACLs apply only to IPv6 packets that are routed.. A filter contains the
| rules to match the packet matches, the rule also stipulates if the
| packet should be permitted or denied.
|
|--[*] IPv6 ACL ABF Track
|
| IPv6 ACL ABF Track allows the user to configure a rule with track as
| nextthop inside the ACL rule . ACL Based Forwarding (ABF) denotes the
| ability to forward packets to another next hop router based on the
| criteria defined in the rule. Track takes precedence over VRF and
| IP, if present in the nextthop
|
|--[*] IPv6 ACL BNG
|
| IPv6 ACL BNG is an ACL subscriber BNG feature. It allows the use of
| ACL on dynamic template.
|
|--[*] IPv6 ACL Chaining (Meta ACL)
|
| IPv6 ACL Chaining (Meta ACL) allows the user to apply more than one
| ACL on the interface. is known as Meta ACL or ACL chaining.
|
|--[-] IPv6 ACL Common ACL
|
| IPv6 ACL Common allows the user to apply the ACL on the interface
| using the common keyword. Using this feature the ACL won't be
| applied to the specific interface but it will be common to th entire
| NPU to which the interface belongs.
|
|--[-] IPv6 ACL Compression
|
| IPv6 ACL Compression allows the user to apply the ACL on the
| interface using a compression level. This helps in reducing the
| hardware resources needed to program the ACL.
|
|--[*] IPv6 ACL Default ABF
|
| IPv6 ACL Default ABF allows the user to configure a rule with
| default nextthop inside the ACL rule . ACL Based Forwarding (ABF)
| denotes the ability to forward packets to another next hop router
| based on the criteria defined in the rule
|
|--[*] IPv6 ACL Fragment
|
| IPv6 ACL Fragment allows the user to configure a rule with fragment
| inside the ACL rule and use it as a match criteria to filter traffic.
|
|--[-] IPv6 ACL ICMP Off
|
| IPv6 ACL ICMP Off allows the user to not genearte the ICMP error
| message on a deny action. When configured it will not send the
| packet to FIB to generate ICMP error message.
----- Truncated for Brevity -----
```



## 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。