Cisco Nexus 1000V System Management コンフィギュレーション ガイド リリース 4.0

Cisco Nexus 1000V System Management Configuration Guide, Release 4.0

2009 年 11 月 6 日

Text Part Number: OL-19419-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Nexus 1000V System Management コンフィギュレーション ガイド リリース 4.0

CONTENTS

はじめに

この『*Cisco Nexus 1000V System Management コンフィギュレーション ガイド リリース 4.0*』マニュアルでは、システム管理の手順について説明します。

ここでは、次の内容について説明します。

対象読者

このマニュアルは、ネットワーク システムの上級ユーザを対象としています。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章およびタイトル	説明
第 1 章「システム管理の概要」	利用可能なシステム管理機能について説明します。
第 2 章「CDP の設定」	他の接続したデバイスとの情報送受信用の Cisco Discovery Protocol（CDP）を設定するための手順を説明しています。
第 3 章「ドメインの設定」	ドメインの作成と VLAN の割り当てを含む Cisco Nexus 1000V ドメインの設定方法について説明します。
第 4 章「サーバ接続の管理」	接続を確立してサーバに接続する方法、サーバから切断する方法、およびサーバ接続を表示する方法について説明します。
第 5 章「コンフィギュレーションの管理」	コンフィギュレーション ファイルの管理方法について説明します。
第 6 章「ファイルの使用」	ファイルのコピーと移動を含むファイルを管理する方法を説明しています。

章およびタイトル	説明
第 7 章「ユーザの管理」	現在のユーザの表示およびユーザへのメッセージの送信を含むシステム上でユーザを管理する方法を説明しています。
第 8 章「NTP の設定」	Network Time Protocol（NTP; ネットワーク タイム プロトコル）を設定して、一連の分散したタイム サーバおよびクライアント間での計時を同期化するための手順を説明しています。この同期によって、複数のネットワーク デバイスからシステム ログおよびその他の時刻特定イベントを受信したときに、イベントを相互に関連付けることができます。
第 9 章「ローカル SPAN および ER SPAN の設定」	イーサネット Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）を設定する方法を説明しています。
第 10 章「SNMP の設定」	ユーザ、メッセージ 暗号化、通知、TCP での認証などを含む SNMP を設定する方法を説明しています。
第 11 章「NetFlow の設定」	NetFlow を設定する方法を説明しています。
第 12 章「システム メッセージ ロギングの設定」	システム メッセージ ロギングを設定する方法を説明しています。

表記法

コマンドの説明では、次の表記法を使用しています。

太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
{ }	波カッコの中の要素は、必須の選択要素です。
[ ]	角カッコの中の要素は、省略可能です。
x | y | z	いずれか 1 つを選択する要素は、縦線で区切って示されます。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

出力例では、次の表記法を使用しています。

`screen フォント`	デバイスが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、かぎカッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、注釈および注意に次の表記法を使用しています。

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

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

関連資料

次に示す Cisco Nexus 1000V の関連資料は、Cisco.com から入手できます。

一般情報

『*Cisco Nexus 1000V Release Notes, Release 4.0*』

インストール & アップグレード

『*Cisco Nexus 1000V Software Installation Guide, Release 4.0*』

『*Cisco Nexus 1000V Virtual Ethernet Module Software Installation Guide, Release 4.0*』

コンフィギュレーション

『*Cisco Nexus 1000V License Configuration Guide, Release 4.0*』

『*Cisco Nexus 1000V Getting Started Guide, Release 4.0*』

『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0*』

『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0*』

『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0*』

『*Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0*』

『*Cisco Nexus 1000V Security Configuration Guide, Release 4.0*』

『*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0*』

『*Cisco Nexus 1000V High Availability and Redundancy Reference, Release 4.0*』

リファレンス

『*Cisco Nexus 1000V Command Reference, Release 4.0*』

『*Cisco Nexus 1000V MIB Quick Reference*』

トラブルシューティング & アラート

『*Cisco Nexus 1000V Troubleshooting Guide, Release 4.0*』

『*Cisco Nexus 1000V Password Recovery Guide*』

『*Cisco NX-OS System Messages Reference*』

CHAPTER 1

システム管理の概要

この章では、次のシステム管理機能について説明します。

ドメイン

Cisco Nexus 1000V 用のドメイン名を作成し、通信および管理用の制御 VLAN とパケット VLAN を追加する必要があります。この処理は、ソフトウェアをインストールする際の Cisco Nexus 1000V の初期セットアップの一部です。後でドメインを作成する必要がある場合は、**setup** コマンドを使用するか、「ドメインの設定」（P.3-1）に記載されている手順を実行します。

サーバ接続

vCenter サーバまたは ESX サーバに接続するためには、まず、Cisco Nexus 1000V で次のものを含む接続を定義する必要があります。

- 接続名
- 使用するプロトコル
- サーバの IP アドレス
- サーバの DNS 名

- データセンター名

第 4 章「サーバ接続の管理」では、vCenter サーバに接続する方法と vCenter サーバから切断する方法、接続を表示する方法について記載されています。

Cisco Discovery Protocol（CDP）

Cisco Discovery Protocol（CDP）は、データ リンク層の上で動作し、接続されているすべてのシスコ製デバイスに情報をアドバタイズし、接続されているシスコ製デバイスに関する情報を検出および表示するために使用されます。CDP は、シスコ製のすべての機器で動作します。

CDP の詳細については、「CDP の設定」（P.2-1）を参照してください。

コンフィギュレーションの管理

コンフィギュレーションを管理するには、次の手順を実行します。

- 「スイッチ名の変更」（P.5-1）
- 「Message of the Day の設定」（P.5-2）
- 「コンフィギュレーションの表示」（P.5-2）
- 「コンフィギュレーションの保存」（P.5-11）
- 「コンフィギュレーションの削除」（P.5-11）

コンフィギュレーションの管理の詳細については、「コンフィギュレーションの管理」（P.5-1）を参照してください。

ファイルの使用

単一のインターフェイスを使用して、次のものを含むファイル システムを管理できます。

- フラッシュ メモリ ファイル システム
- ネットワーク ファイル システム（TFTP および FTP）
- データを読み書きするためのその他のエンドポイント（NVRAM や実行コンフィギュレーションなど）

ファイルの使用方法の詳細については、「ファイルの使用」（P.6-1）を参照してください。

ユーザの管理

デバイスに現在接続されているユーザを識別し、単一のユーザまたはすべてのユーザにメッセージを送信することができます。詳細については、「ユーザの管理」（P.7-1）を参照してください。

ネットワーク タイム プロトコル（NTP）

Network Time Protocol（NTP; ネットワーク タイム プロトコル）は、分散している一連のタイム サーバおよびクライアント間で、計時を同期させます。この同期によって、複数のネットワーク デバイスからシステム ログおよびその他の時刻特定イベントを受信したときに、イベントを相互に関連付けることができます。

NTP の詳細については、「NTP の設定」（P.8-1）を参照してください。

システム メッセージ

システム メッセージ ロギングを使用すると、システム プロセスが生成するメッセージの宛先を制御し、重大度に基づいてメッセージをフィルタリングできます。端末セッション、ログ ファイル、およびリモート システム上の syslog サーバへのロギングを設定できます。

システム メッセージ ロギングは RFC 3164 に準拠しています。システム メッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。

システム メッセージ設定については、「システム メッセージ ロギングの設定」（P.12-1）を参照してください。

簡易ネットワーク管理プロトコル（SNMP）

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）は、SNMP マネージャとエージェント間の通信用メッセージ フォーマットを提供する、アプリケーション レイヤ プロトコルです。SNMP はネットワーク デバイスの監視や管理に使用される、標準化されたフレームワークと共通言語を提供します。

SNMP の詳細については、「SNMP の設定」（P.10-1）を参照してください。

スイッチド ポート アナライザ（SPAN）

イーサネット Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）を使用すると、デバイスの入出力トラフィックを監視したり、送信元ポートから宛先ポートへのパケットを複製できます。

SPAN の設定については、「ローカル SPAN および ER SPAN の設定」（P.9-1）を参照してください。

NetFlow

NetFlow を使用すると、送信元、宛先、タイミング、アプリケーション情報に基づいて IP トラフィックの特徴を明確にすることで、仮想スイッチを通過するトラフィックを視覚化することができます。この情報は、ネットワークの可用性とパフォーマンスの評価、法的な要求事項の満足（コンプライアンス）、トラブルシューティングに役立てることができます。

詳細については、「NetFlow の設定」（P.11-1）を参照してください。

トラブルシューティング

ping と traceroute は、利用可能なトラブルシューティング ツールです。

詳細については、『*Cisco Nexus 1000V Troubleshooting Guide, Release 4.0*』を参照してください。

CHAPTER 2

CDP の設定

この章では、Cisco Discovery Protocol（CDP）の設定方法について、次の内容を説明します。

CDP の概要

ここでは、次の内容について説明します。

CDP の概要

Cisco Discovery Protocol（CDP）は、データ リンク層の上で動作し、接続されているすべてのシスコ製デバイスに情報をアドバタイズし、接続されているシスコ製デバイスに関する情報を検出および表示するために使用されます。CDP は、シスコ製のすべての機器で動作します。

CDP はネイバー デバイスのプロトコル アドレスを収集し、各デバイスのプラットフォームを検出します。CDP の動作はデータ リンク レイヤ上に限定されます。異なるレイヤ 3 プロトコルをサポートする 2 つのシステムで相互学習が可能です。

CDP が設定された各デバイスは、マルチキャスト アドレスに定期的にアドバタイズメントを送信します。各デバイスは SNMP メッセージを受信できるアドレスを最低 1 つはアドバタイズします。アドバタイズメントには保持時間情報も含まれます。保持時間は、受信デバイスが CDP 情報を破棄するまでに保持する時間の長さを表します。アドバタイズメントまたはリフレッシュ タイマーおよびホールド タイマーを設定できます。

CDP Version 2（CDPv2）では、接続デバイス間でネイティブ VLAN ID またはポート デュプレックス ステートが一致していないインスタンスを追跡できます。

CDP では、次の Type-Length-Value（TLV）フィールドがアドバタイズされます。

- Device ID
- Address
- Port ID
- Capabilities
- Version
- Platform
- Native VLAN
- Full/Half Duplex
- MTU
- SysName
- SysObjectID
- Management Address
- Physical Location

すべての CDP パケットに VLAN ID が含まれます。レイヤ 2 アクセス ポート上で CDP を設定した場合、そのアクセス ポートから送信される CDP パケットには、アクセス ポートの VLAN ID が含まれます。レイヤ 2 トランク ポート上で CDP を設定した場合は、そのトランク ポートから送信される CDP パケットに、トランク ポート上で許可設定されている最小の VLAN ID が含まれます。トランク ポートは、そのトランク ポートの許可 VLAN リストに指定されている VLAN ID であれば、どの VLAN ID が含まれている CDP パケットでも受信できます。VLAN の詳細については、『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0*』を参照してください。

ハイ アベイラビリティ

CDP ではステートレス リスタートがサポートされています。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。

設定時の注意事項および制約事項

CDP に関する設定時の注意事項および制約事項は、次のとおりです。

- 接続数が 256 のハブにポートを接続した場合、CDP はポートあたり最大 256 のネイバーを検出できます。
- CDP を設定する前に、CDP 機能がグローバルにイネーブルになっている必要があります。CDP は、デフォルトでグローバルにイネーブルになっていますが、「CDP 機能のグローバルなディセーブル化」の手順（P.2-3）を使用してディセーブルにできます。
- CDP を設定できるのは、物理インターフェイスおよびポート チャネル上に限られます。

CDP の設定

ここでは、次の内容について説明します。

CDP 機能のグローバルなイネーブル化

CDP をグローバルにイネーブルにするには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- CDP を設定する前に CDP をイネーブルにしておく必要があります。
- CDP はデフォルトでグローバルにイネーブルになっています。

手順の概要

1. **config t**
2. **enable cdp**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cdp enable** **例：** `n1000v(config)# cdp enable`	CDP 機能をグローバルにイネーブルにします。

CDP 機能のグローバルなディセーブル化

CDP をグローバルにディセーブルにするには、ここに示す手順を実行します

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- CDP 機能をグローバルにディセーブルにすると、すべての CDP コンフィギュレーションもディセーブルになります。
- CDP が現在グローバルにイネーブルになっています。

- CDP は、デフォルトで各インターフェイス上でイネーブルになっています。

手順の概要

1. **config t**
2. **no cdp enable**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no cdp enable** **例：** `n1000v(config)# no cdp enable`	CDP 機能をディセーブルにして、関連する CDP コンフィギュレーションをすべて削除します。

インターフェイス上での CDP のイネーブル化

特定のインターフェイス上で CDP をイネーブルにするには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- CDP 機能がグローバルにイネーブルになっていること。CDP はデフォルトでイネーブルになっていますが、「CDP 機能のグローバルなイネーブル化」の手順（P.2-3）を使用して再度イネーブルにすることもできます。
- CDP が、デフォルトですべてのインターフェイス上でイネーブルになっていること。
- CDP が、設定対象のインターフェイスで現在ディセーブルになっていること。
- CDP の詳細については、「CDP の概要」（P.2-1）を参照してください。

手順の概要

1. **config t**
2. **interface** *interface-type slot/port*
3. **no cdp enable**
4. **cdp enable**
5. **show cdp interface** *interface-type slot/port*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type slot/port*
	
	例：
	`n1000v(config)# interface mgmt0`
	`n1000v(config-if)#`
		CLI を特定のインターフェイスに対するインターフェイス コンフィギュレーション モードにします。

ステップ 3	**no cdp enable** **例：** `n1000v(config-if)# no cdp enable`	このインターフェイスで CDP をディセーブルにします。
ステップ 4	**cdp enable** **例：** `n1000v(config-if)# cdp enable`	このインターフェイスで CDP をイネーブルにします。

ステップ 5	**show cdp interface** *interface-type slot/port*
	
	例：
	`n1000v(config-if)# show cdp interface mgmt0`
	`mgmt0 is up`
	`    CDP disabled on interface`
	`    Sending CDP packets every 60 seconds`
	`    Holdtime is 180 seconds`
		（任意）指定したインターフェイスの CDP 情報を表示します。

ステップ 6	**copy running-config startup-config**
	
	例：
	`n1000v(config-if)# copy running-config`
	`startup-config`
		（任意）この設定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ます。

ポート チャネル 2 で CDP をイネーブルにする例を示します。

例：

```
n1000v# config t
n1000v(config)# interface port-channel 2
n1000v(config-if)# cdp enable
n1000v(config-if)# copy running-config startup-config
```

インターフェイス上での CDP のディセーブル化

インターフェイス上で CDP をディセーブルにするには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- CDP がデバイス上で現在イネーブルになっていること。

（注） CDP がデバイス上でディセーブルになっている場合、すべてのインターフェイスでもディセーブルになっています。

- CDP が、設定対象のインターフェイスで現在イネーブルになっていること。
- CDP の詳細については、「CDP の概要」（P.2-1）を参照してください。

手順の概要

1. **config t**
2. **interface** *interface-type slot/port*
3. **no cdp enable**
4. （任意）**show cdp interface** *interface-type slot/port*
5. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type slot/port*
	
	例：
	`n1000v(config)# interface mgmt0`
	`n1000v(config-if)#`
		指定したインターフェイスに対する CLI インターフェイス コンフィギュレーション モードにします。

ステップ 3	**no cdp enable** **例：** `n1000v(config-if)# no cdp enable`	指定したインターフェイス上で CDP をディセーブルにします。

	コマンド	目的
ステップ 4	**show cdp interface** *interface-type slot/port* **例：** `n1000v(config-if)# show cdp interface mgmt0`	（任意）インターフェイスの CDP 情報を表示します。
ステップ 5	**copy running-config startup-config** **例：** `n1000v(config-if)# copy running-config startup-config`	（任意）この設定変更を保存します。

次に、mgmt0 上で CDP をディセーブルにする例を示します。

```
n1000v# config t
n1000v(config)# interface mgmt0
n1000v(config-if)# no cdp enable
n1000v(config-if)# show cdp interface mgmt0
mgmt0 is up
    CDP disabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
n1000v(config-if)# copy running-config startup-config
```

グローバル CDP バージョンの割り当て

デバイス上でアドバイスする CDP バージョンを割り当てるには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- デバイス上で現在サポートされている CDP のバージョンを知っておく必要があります。
- 一度にアドバタイズされるのは 1 つのバージョンの CDP（バージョン 1 またはバージョン 2）だけです。
- CDP の詳細については、「CDP の概要」（P.2-1）を参照してください。

手順の概要

1. **config t**
2. **cdp advertise {v1 | v2}**
3. （任意）**show cdp global**
4. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cdp advertise {v1 | v2}**
	
	例 1：
	`n1000v(config)# cdp advertise v1`
	`n1000v(config)#`
	
	例 2：
	`n1000v(config)# cdp advertise v2`
	`n1000v(config)#`
		アドバタイズする CDP バージョンを割り当てます。
		• CDP バージョン 1
		• CDP バージョン 2

ステップ 3	**show cdp global**	（任意）CDPv2 がイネーブルになっているかどうかを示す CDP コンフィギュレーションを表示します。

例 1：

```
n1000v(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is disabled
    Sending DeviceID TLV in Default Format
```

例 2：

```
n1000v(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
    Sending DeviceID TLV in Default Format
```

ステップ 4	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）この設定変更を保存します。

CDP オプション パラメータの設定

次の CDP パラメータを設定するには、ここに示す手順を実行します。

- デバイス ID

- ネイバー情報の最大保持時間
- 送信アドバタイズメントのリフレッシュ タイム

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- デバイス ID を割り当てる場合、MAC アドレス、シャーシ シリアル番号、Organizationally Unique Identifier（OUI; 組織固有識別子）のどれを使用するかがわかっていること。
- 保持時間を設定する場合、CDP がネイバー情報を保持する時間がわかっていること。
- アップストリーム cat6k スイッチからの出力を表示するには、**show cdp neighbor** コマンドを使用すること。
- CDP タイマーを設定する場合は、CDP がアドバタイズする頻度がわかっていること。
- CDP の詳細については、「CDP の概要」（P.2-1）を参照してください。

手順の概要

1. **config t**
2. （任意）**cdp format device-id** {**mac-address** | **other** | **serial-number**}
3. **show cdp neighbors** from the upstream device
4. **show cdp neighbors** from your device
5. （任意）**cdp timer** *seconds*
6. （任意）**cdp holdtime** *seconds*
7. （任意）**show cdp global**
8. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cdp format device-id** {**mac-address** | **other** | **serial-number**} **例：** `n1000v(config)# cdp format device-id mac-address`	（任意）次のいずれかのオプションとともに CDP デバイス ID を割り当てます。 • mac-address：シャーシの MAC アドレス • other：シャーシのシリアル番号（デフォルト） • serial-number：シャーシのシリアル番号/組織固有識別子（OUI）
ステップ 3	**show cdp neighbors**	アップストリーム デバイスから自デバイスを表示します。

コマンド	目的

例：
`swordfish-6k-2#show cdp neighbors`
`Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge`
`S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone`
 	
`Device ID Local Intrfce Holdtme Capability Platform Port ID`
 	
`02000c000000 Gig 1/16 14 S Soft Swit Eth 2/4`
`02000c000000 Gig 1/17 14 S Soft Swit Eth 2/5`
`02000c000000 Gig 1/14 14 S Soft Swit Eth 2/2`
`02000c000000 Gig 1/15 14 S Soft Swit Eth 2/3`
`02000c000000 Gig 1/18 13 S Soft Swit`	

ステップ 4　**show cdp neighbors**	自デバイスからアップストリーム デバイスを表示します。

`n1000v(config)# show cdp neighbors`
`Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge`
`S - Switch, H - Host, I - IGMP, r - Repeater,`
`V - VoIP-Phone, D - Remotely-Managed-Device,`
`s - Supports-STP-Dispute`
 	
`Device ID Local Intrfce Hldtme Capability Platform Port ID`
 	
`swordfish-6k-2 Eth2/2 169 R S I WS-C6503-E Gig1/14`
`swordfish-6k-2 Eth2/3 139 R S I WS-C6503-E Gig1/15`
`swordfish-6k-2 Eth2/4 135 R S I WS-C6503-E Gig1/16`
`swordfish-6k-2 Eth2/5 177 R S I WS-C6503-E Gig1/17`
`swordfish-6k-2 Eth2/6 141 R S I WS-C6503-E Gig1/18`	

ステップ 5　**cdp holdtime** *seconds* **例：** `n1000v(config)# cdp holdtime 10`	（任意）CDP がネイバー情報を破棄するまでにそれを保持する最大時間を設定します。 • 範囲は 10 ～ 255 秒です。 • デフォルト値は 180 秒です。
ステップ 6　**cdp timer** *seconds* **例：** `n1000v(config)# cdp timer 5`	（任意）CDP がネイバーにアドバタイズメントを送信するリフレッシュ タイムを設定します。 • 範囲は 5 ～ 254 秒です。 • デフォルト値は 60 秒です。
ステップ 7　**show cdp global**	グローバル CDP コンフィギュレーションを表示します。

例：
`n1000v(config)# show cdp global`
`Global CDP information:`
`CDP enabled globally`
`Sending CDP packets every 5 seconds`
`Sending a holdtime value of 10 seconds`
`Sending CDPv2 advertisements is disabled`
`Sending DeviceID TLV in Mac Address Format`	

ステップ 8　**copy running-config startup-config** **例：** `n1000v(config-if)# copy running-config startup-config`	（任意）この設定変更を保存します。

CDP 統計情報の消去

CDP 統計情報を消去するには、次のいずれかのコマンドを使用します。

コマンド	目的
clear cdp counters	インターフェイスの CDP 統計情報を消去します。
clear cdp table	1 つまたはすべてのインターフェイスの CDP キャッシュを消去します。

CDP コンフィギュレーションの確認

CDP コンフィギュレーション情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
show cdp all	CDP がイネーブルになっているすべてのインターフェイスを表示します。 例 2-1（P.2-11）を参照してください。
show cdp entry {**all** | **name** *entry-name*}	CDP データベース エントリを表示します。 例 2-2（P.2-12）を参照してください。
show cdp global	CDP グローバル パラメータを表示します。 例 2-4（P.2-14）を参照してください。
show cdp interface *interface-type slot/port*	CDP インターフェイスのステータスを表示します。 例 2-5（P.2-14）を参照してください。
show cdp neighbors {**detail** | **interface** *interface-type slot/port*}	CDP ネイバーのステータスを表示します。 例 2-6（P.2-14）を参照してください。
show cdp traffic interface *interface-type slot/port*	インターフェイスの CDP トラフィック統計を表示します。 例 2-7（P.2-14）を参照してください。

例 2-1　show cdp all

```
n1000v# show cdp all
Ethernet2/2 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/3 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/4 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/5 is up
```

```
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/6 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
mgmt0 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

例 2-2　show cdp entry *name*

```
n1000v# show cdp entry name swordfish-6k-2
----------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 172.28.30.2
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/2, Port ID (outgoing port): GigabitEthernet1/14
Holdtime: 152 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team
```

例 2-3　show cdp entry all

```
n1000v# show cdp entry all
----------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 172.28.30.2
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/2, Port ID (outgoing port): GigabitEthernet1/14
Holdtime: 140 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1

----------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 172.28.30.2
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/3, Port ID (outgoing port): GigabitEthernet1/15
Holdtime: 129 sec
```

```
Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1

---------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 7.7.8.1
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/4, Port ID (outgoing port): GigabitEthernet1/16
Holdtime: 154 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1

---------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 7.7.8.1
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/5, Port ID (outgoing port): GigabitEthernet1/17
Holdtime: 156 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1

---------------------------------------
Device ID:swordfish-6k-2
System Name:
Interface address(es):
    IPv4 Address: 172.28.15.229
Platform: cisco WS-C6503-E, Capabilities: Router Switch IGMP Filtering
Interface: Ethernet2/6, Port ID (outgoing port): GigabitEthernet1/18
Holdtime: 171 sec

Version:
Cisco IOS Software, s72033_rp Software (s72033_rp-IPBASE-M), Version 12.2(33)SXH2a,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Fri 25-Apr-08 09:11 by prod_rel_team

Advertisement Version: 1
```

例 2-4　show cdp global

```
n1000v(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is disabled
    Sending DeviceID TLV in Default Format
```

例 2-5　show cdp interface

```
n1000v(config)# show cdp interface ethernet 2/3
Ethernet2/3 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

例 2-6　show cdp neighbors interface

```
n1000v(config)# show cdp neighbors interface ethernet 2/3
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID

swordfish-6k-2         Eth2/3          173     R S I    WS-C6503-E    Gig1/15
```

例 2-7　show cdp traffic interface

```
n1000v(config)# show cdp traffic interface ethernet 2/3
----------------------------------------
Traffic statistics for Ethernet2/3
Input Statistics:
    Total Packets: 98
    Valid CDP Packets: 49
        CDP v1 Packets: 49
        CDP v2 Packets: 0
    Invalid CDP Packets: 49
        Unsupported Version: 49
        Checksum Errors: 0
        Malformed Packets: 0

Output Statistics:
    Total Packets: 47
        CDP v1 Packets: 47
        CDP v2 Packets: 0
    Send Errors: 0
```

CDP の設定例

CDP 機能をイネーブルにして、リフレッシュ タイマーおよびホールド タイマーを設定する例を示します。

```
config t
cdp enable
cdp timer 50
cdp holdtime 100
```

デフォルト設定

表 2-1 に、CDP パラメータのデフォルト設定を示します。

表 2-1　デフォルトの CDP パラメータ

パラメータ	デフォルト
CDP	グローバルおよびすべてのインターフェイスでイネーブル
CDP version	バージョン 2
CDP device ID	シリアル番号
CDP timer	60 秒
CDP hold timer	180 秒

その他の関連資料

ここでは、CDP に関する次の追加情報について説明します。

- 「関連資料」（P.2-15）
- 「標準規格」（P.2-15）

関連資料

関連項目	マニュアル タイトル
VLAN	『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

CHAPTER 3

ドメインの設定

この章では、ドメインの作成や VLAN の割り当てなど、Cisco Nexus 1000V ドメインの設定方法について説明します。

この章では、次の内容について説明します。

ドメインの作成

ドメインを作成するには、ここに示す手順を実行します。

始める前に

- EXEC モードで CLI にログインします。

手順の概要

1. **config t**
2. **svs-domain**
3. **domain id** *domain-id*
4. **control vlan** *vlan-id*
5. **packet vlan** *vlan-id*
6. **exit**
7. **show svs-domain**
8. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**svs-domain**
	
	例：
	`n1000v(config)# svs-domain`
	`n1000v(config-svs-domain)#`
		ドメインを作成し、CLI SVS ドメイン コンフィギュレーション モードにします。

ステップ 3	**domain id** *32*
	
	例：
	`n1000v(config-svs-domain)# domain id 32`
	`n1000v(config-svs-domain)#`
		ドメイン ID を割り当てます。

ステップ 4	**control vlan** *70*
	
	例：
	`n1000v(config-svs-domain)# control vlan 70`
	`n1000v(config-vlan)#`
		制御 VLAN をドメインに割り当てます。

ステップ 5	**packet vlan** *71*
	
	例：
	`n1000v(config-vlan)# packet vlan 71`
	`n1000v(config-vlan)#`
		パケット VLAN をドメインに割り当てます。

ステップ 6	**show svs-domain** **例：** `n1000v(config-vlan)# show svs-domain`	ドメイン コンフィギュレーションを表示します。

	コマンド	目的

ステップ 7	**exit**
	
	例：
	`n1000v(config-vlan)# exit`
	`n1000v(config)#`
		CLI 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 8	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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コピーします。

次に、制御 VLAN とパケット VLAN を作成する例を示します。

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# domain id 32
n1000v(config-svs-domain)# control vlan 70
n1000v(config-svs-domain)# packet vlan 71
n1000v(config-vlan)# exit
n1000v(config)# show svs-domain

n1000v (config)# show svs domain
SVS domain config:
  Domain id:    98
  Control vlan: 70
  Packet vlan:  71
  Sync state:  -

n1000v(config)#
n1000v(config)# copy run start
[########################################] 100%
n1000v(config)#
```

ドメインの制御 VLAN の作成

ドメインに制御 VLAN を追加するには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- 必要な Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）を設定しイネーブルにしてあること（『*Cisco Nexus 1000V Interface Configuration Guide, Beta 2 Release*』を参照）。SVI は VLAN インターフェイスとも呼ばれ、複数の VLAN 間の通信を可能にします。
- VLAN が番号付けされる方法について知っていること。詳細については、『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0*』を参照してください。
- 新たに作成した VLAN は、レイヤ 2 ポートを割り当てるまで使用されないままになります。

手順の概要

1. **config t**
2. **vlan** *vlan-id*
3. **name** *vlan-name*
4. **state** *vlan-state*
5. **exit**
6. **show vlan id** *vlan-id*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vlan** *30*
	
	例：
	`n1000v(config)# vlan 30`
	`n1000v(config-vlan)#`
		制御トラフィック用の VLAN ID 30 を作成し、CLI VLAN コンフィギュレーション モードにします。
		（注） 内部的に割り当てられた VLAN に割り当て済みの VLAN ID を入力した場合、エラー メッセージが返されます。

ステップ 3	**name** *cp_control*
	
	例：
	`n1000v(config-vlan)# name cp_control`
	`n1000v(config-vlan)#`
		説明用の名前 cp_control をこの VLAN に追加します。

ステップ 4	**state** *active*
	
	例：
	`n1000v(config-vlan)# state active`
	`n1000v(config-vlan)#`
		VLAN の動作状態をアクティブに変更します。

ステップ 5	**show vlan id** *30* **例：** `n1000v(config-vlan)# show vlan-id 30`	VLAN ID 30 のコンフィギュレーションを表示します。

	コマンド	目的

ステップ 6	**exit**
	
	例：
	`n1000v(config-vlan)# exit`
	`n1000v(config)#`
		CLI 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 7	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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コピーします。

次に、制御トラフィック用の VLAN 30 を作成する例を示します。

```
n1000v# config t
n1000v(config)# vlan 30
n1000v(config-vlan)# name cp_control
n1000v(config-vlan)# state active
n1000v(config-vlan)# exit
n1000v(config)# show vlan-id 30

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
30   cp_control                       active

VLAN Type MTU
---- -----
5    enet 1500

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type              Ports
-------  ---------  ----------------  ------------------------------------------

n1000v(config)# copy run start
[########################################] 100%
n1000v(config)#
```

ドメインのパケット VLAN の作成

ドメインにパケット VLAN を追加するには、次の手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- EXEC モードで CLI にログインしていること。
- 『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0*』に従って、必要なスイッチ仮想インターフェイス（SVI）を設定しイネーブルにしてあること。SVI は VLAN インターフェイスとも呼ばれ、複数の VLAN 間の通信を可能にします。

- VLAN が番号付けされる方法について知っていること。詳細については、『*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0*』を参照してください。

- 新たに作成した VLAN は、レイヤ 2 ポートを割り当てるまで使用されないままになること。

手順の概要

1. **config t**
2. **vlan** *vlan-id*
3. **name** *vlan-name*
4. **state** *vlan-state*
5. **exit**
6. **show vlan id** *vlan-id*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vlan** *31*
	
	例：
	`n1000v(config)# vlan 31`
	`n1000v(config-vlan)#`
		パケット トラフィック用の VLAN ID 31 を作成し、CLI VLAN コンフィギュレーション モードにします。
		（注） 内部的に割り当てられた VLAN に割り当て済みの VLAN ID を入力した場合、エラー メッセージが返されます。

ステップ 3	**name** *cp_packet*
	
	例：
	`n1000v(config-vlan)# name cp_packet`
	`n1000v(config-vlan)#`
		説明用の名前 cp_packet をこの VLAN に追加します。

ステップ 4	**state** *active*
	
	例：
	`n1000v(config-vlan)# state active`
	`n1000v(config-vlan)#`
		VLAN の動作状態をアクティブに変更します。

ステップ 5	**show vlan id** *31* **例：** `n1000v(config-vlan)# show vlan-id 30`	VLAN ID 31 のコンフィギュレーションを表示します。

	コマンド	目的

ステップ 6	**exit**
	
	例：
	`n1000v(config-vlan)# exit`
	`n1000v(config)#`
		CLI 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 7	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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コピーします。

次に、パケット トラフィック用の VLAN 31 を作成する例を示します。

```
n1000v# config t
n1000v(config)# vlan 31
n1000v(config-vlan)# name cp_packet
n1000v(config-vlan)# state active
n1000v(config-vlan)# exit
n1000v(config)# show vlan-id 31

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
31   cp_packet                        active

VLAN Type MTU
---- -----
5    enet 1500

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type              Ports
-------  ---------  ----------------  ------------------------------------------

n1000v(config)# copy run start
[########################################] 100%
n1000v(config)#
```

CHAPTER 4

サーバ接続の管理

この章では、接続を確立してサーバに接続する方法、サーバから切断する方法、およびサーバ接続を表示する方法について説明します。

この章では、次の内容について説明します。

vCenter Server への接続

この手順を使用して、接続を設定して、vCenter Server または ESX サーバに接続します。

始める前に

- EXEC モードで CLI にログインします。
- vCenter Server 管理ステーションをインストールして実行します。
- ESX サーバをインストールして実行します。
- 管理ポートを設定します。
- Cisco Nexus 1000V から vCenter Server にアクセスできるようにします。
- Cisco Nexus 1000V アプライアンスをインストールします。
- ホスト名を使用して接続を設定している場合は、DNS を設定しておきます。

手順の概要

1. **config t**
2. **svs connection** *name*
3. **protocol vmware-vim**
4. **remote {ip address** *address*| **hostname** *name*}
5. **vmware dvs datacenter-name** *name*
6. **connect**

手順の詳細

	コマンド	説明

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**svs connection** *name*
	
	例：
	`n1000v (config#) svs connection vcWest`
	`n1000v(config-svs-conn#)`
		Cisco Nexus 1000V と特定の ESX サーバまたは vCenter Server 間にこの接続を追加するための、接続コンフィギュレーション モードに切り替えます。名前を使用して、複数接続情報をコンフィギュレーションに格納できます。

ステップ 3	**protocol vmware-vim** [http]
	
	例：
	`n1000v(config-svs-conn#) protocol vmware-vim`
	`n1000v(config-svs-conn#)`
		この接続が VIM プロトコルを使用するように指定します。このコマンドはローカルに格納されます。
		• **http**：VIM プロトコルが HTTP で実行されるように指定します。デフォルトでは HTTP over SSL（HTTPS）を使用します。

ステップ 4	次のいずれかを実行します。 • IP アドレスを設定している場合は、ステップ 5 を参照してください。 • ホスト名を設定している場合は、ステップ 6 を参照してください。	

ステップ 5	**remote ip address** *ipaddress*
	
	例：
	`n1000v(config-svs-conn#) remote ip address 10.86.194.225`
	`n1000v(config-svs-conn#)`
	
	ステップ 7 を参照してください。
		この接続で使用する ESX サーバまたは vCenter Server の IP アドレスを指定します。このコマンドはローカルに格納されます。

ステップ 6	**remote hostname** *hostname*
	
	例：
	`n1000v(config-svs-conn#) remote hostname vcMain`
	`n1000v(config-svs-conn#)`
		この接続で使用する ESX サーバまたは vCenter Server の DNS 名を指定します。このコマンドはローカルに格納されます。
		（注）　DNS はすでに設定されています。

	コマンド	説明

ステップ 7	**vmware dvs datacenter-name** *name*
	
	例：
	`n1000v(config-svs-conn#) vmware dvs datacenter-name HamiltonDC`
	`n1000v(config-svs-conn#)`
		Cisco Nexus 1000V が Distributed Virtual Switch（DVS; 分散仮想スイッチ）として作成される vCenter Server のデータセンター名を指定します。接続前または接続後に、このコマンドを使用できます。データセンター名はローカルに格納されます。

ステップ 8	**connect** **例：** `n1000v(config-svs-conn#) connect`	接続を開始します。この接続のユーザ名とパスワードが設定されていない場合は、ユーザ名とパスワード入力プロンプトが表示されます。 デフォルトは no connect です。一度にアクティブにできる接続は 1 つだけです。以前に定義した接続が確立している場合は、no connect を入力して以前の接続を終了するまでは、エラー メッセージが表示され、コマンドは拒否されます。

vCenter Server からの切断

この手順を使用して、vCenter Server 設定の修正後などに vCenter Server から切断します。

始める前に

- EXEC モードで Cisco Nexus 1000V にログインします。
- 「vCenter Server への接続」の手順（P.4-1）を参照して、Cisco Nexus 1000V 接続を設定します。
- Cisco Nexus 1000V を vCenter Server または ESX に接続します。

手順の詳細

	コマンド	説明

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**svs connection** *name*
	
	例：
	`n1000v (config#) svs connection vcWest`
	`n1000v(config-svs-conn)#`
		vCenter Server に接続するために、CLI グローバル コンフィギュレーション サブモードに切り替えます。

ステップ 3	**no connect**
	
	例：
	`n1000v(config-svs-conn)# no connect`
	`n1000v(config-svs-conn)#`
		接続を終了します。

vCenter Server からの DVS の削除

この手順を使用して、vCenter Server から DVS を削除します。

始める前に

- EXEC モードで CLI にログインします。
- 「vCenter Server への接続」の手順（P.4-1）を参照して、接続を設定します。
- Cisco Nexus 1000V を vCenter Server または ESX に接続します。
- Server Administrator を Cisco Nexus 1000V に接続しているすべてのホストの VI クライアントから削除しておきます。詳細については、VMware のマニュアルを参照してください。

手順の詳細

	コマンド	説明

ステップ 1	`config t`
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**svs connection** *name*
	
	例：
	`n1000v(config#) svs connection vcWest`
	`n1000v(config-svs-conn)#`
		vCenter Server に接続するために、CLI グローバル コンフィギュレーション サブモードに切り替えます。

ステップ 3	**no vmware dvs**
	
	例：
	`n1000v(config-svs-conn)# no vmware dvs`
	`n1000v(config-svs-conn)#`
		指定された接続に関連付けられている DVS を vCenter Server から削除します。

接続の表示

この手順を使用して、接続を表示します。

始める前に

- 任意のコマンド モードで CLI にログインします。
- 「vCenter Server への接続」の手順（P.4-1）を参照して、接続設定を行います。
- Cisco Nexus 1000V を vCenter Server または ESX に接続します。

手順の詳細

	コマンド	説明
ステップ 1	**show svs connections** [*name*]	現在の Cisco Nexus 1000V への接続を表示します。 **（注）** ネットワーク接続の問題により、vCenter Server への接続がシャットダウンされる場合があります。ネットワーク接続が復元しても、Cisco Nexus 1000V では自動的に接続は復元されません。この場合、次のコマンド シーケンスを使用して、手動で接続を復元する必要があります。 **no connect** connect

例：

```
n1000v# show svs connections vc
Connection vc:
IP address: 172.28.15.206
Protocol: vmware-vim https
vmware dvs datacenter-name: HamiltonDC
ConfigStatus: Enabled
OperStatus: Connected
n1000v#
```

ドメインの表示

この手順を使用して、設定されたドメインを表示します。

始める前に

- 任意のコマンド モードで CLI にログインします。
- 「ドメインの作成」の手順（P.3-1）を参照して、ドメインを設定します。

手順の詳細

	コマンド	説明

ステップ 1	**show svs-domain**
	
	例：
	`n1000v# show svs-domain`
	
	`n1000v (config)# show svs domain`
	`SVS domain config:`
	`  Domain id:    98`
	`  Control vlan: 70`
	`  Packet vlan:  71`
	`  Sync state:  -`
	
	`n1000v#`
		Cisco Nexus 1000V で設定されたドメインを表示します。

コンフィギュレーションの表示

この手順を使用して、実行コンフィギュレーションを表示します。

始める前に

- 任意のコマンド モードで CLI にログインします。
- 「vCenter Server への接続」の手順（P.4-1）を参照して、Cisco Nexus 1000V 接続を設定します。
- Cisco Nexus 1000V を vCenter Server または ESX に接続します。

手順の詳細

	コマンド	説明
ステップ 1	**show running-config**	現在の設定を表示します。 Cisco Nexus 1000V が vCenter Server または ESX サーバに接続していない場合は、接続関連情報だけが出力されます。

例：

```
n1000v(config-acl)# show running-config
version 4.0(1)
feature port-security
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network-operator
username admin password 5 $1$N1mX5tLD$daXpuxlAPcIHoz53PBhy6/  role network-admin
telnet server enable
ssh key rsa 1024 force
kernel core target 0.0.0.0
kernel core limit 1
```

```
system default switchport
ip access-list my66
  10 permit ip 1.1.1.1/32 1.1.1.2/32
snmp-server user admin network-admin auth md5 0x90f3798f3e894496a11ec42ce2efec9c priv
0x90f3798f3e894496a11ec42ce2efec9c localizedkey
snmp-server enable traps entity fru
snmp-server enable traps license
vrf context management
  ip route 0.0.0.0/0 172.28.15.1
switchname srini-cp
vlan 40-43,45-48
vdc srini-cp id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 32
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 192
  limit-resource u4route-mem minimum 32 maximum 256
  limit-resource u6route-mem minimum 16 maximum 256

interface Ethernet6/2
  inherit port-profile uplinkportprofile1

interface Ethernet6/3
  inherit port-profile uplinkportprofile2

interface Ethernet6/4
  inherit port-profile uplinportprofile3

interface Ethernet7/2
  inherit port-profile uplinkportprofile1

interface mgmt0
  ip address 172.28.15.163/24

interface Vethernet1


  inherit port-profile vm100

interface Vethernet2


  inherit port-profile vm100

interface Vethernet3


  inherit port-profile vm100

interface Vethernet4


  inherit port-profile vm100

interface Vethernet5

interface Vethernet6
boot kickstart bootflash:/svs-kickstart-mzg.4.0.1a.S1.0.82.bin sup-1
boot system bootflash:/svs-mzg.4.0.1a.S1.0.82.bin sup-1
boot system bootflash:/isan.bin sup-1
boot kickstart bootflash:/svs-kickstart-mzg.4.0.1a.S1.0.82.bin sup-2
boot system bootflash:/svs-mzg.4.0.1a.S1.0.82.bin sup-2
boot system bootflash:/isan.bin sup-2
ip route 0.0.0.0/0 172.28.15.1
```

```
port-profile uplinkportprofile1
  capability uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 1,40-43
  no shutdown
  system vlan 1,40-43
  state enabled
port-profile vm100
  vmware port-group
  switchport mode access
  switchport access vlan 43
  ip port access-group my100 out
  ip port access-group my66 in
  no shutdown
  state enabled
port-profile uplinkportprofile2
  capability uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 45-46
  no shutdown
  state enabled
port-profile uplinportprofile3
  capability uplink
  vmware port-group
  switchport trunk allowed vlan 47-48
  state enabled
port-profile uplinkportprofile3
  no shutdown
svs-domain
  domain id 163
  control vlan 41
  packet vlan 42
svs connection VCR5
  protocol vmware-vim
  remote ip address 172.28.30.83
  vmware dvs datacenter-name cisco-DC
  connect
n1000v(config-acl)#
```

モジュール情報の表示

この手順を使用して、Cisco Nexus 1000V から DVS のビューを含むモジュール情報を表示します。

始める前に

- 任意のコマンド モードで CLI にログインします。
- 「vCenter Server への接続」の手順（P.4-1）を参照して、Cisco Nexus 1000V 接続を設定します。
- Cisco Nexus 1000V を vCenter Server または ESX に接続します。
- Server Administrator で、Cisco Nexus 1000V を実行しているホストを、vCenter Server の DVS に追加しておきます。

手順の概要

1. **show module**

2. **show server-info**
3. **show interface brief**
4. **show interface virtual**

手順の詳細

	コマンド	説明
ステップ 1	**show module** **例：** `n1000v# show module`	モジュール情報を表示します。
ステップ 2	**show server_info** **例：** `n1000v# show server_info`	サーバ情報を表示します。
ステップ 3	**show interface brief** **例：** `n1000v# show interface brief`	vCenter Server へのアップリンクを含むインターフェイス情報を表示します。
ステップ 4	**show interface virtual** **例：** `n1000v# show interface virtual`	仮想インターフェイス情報を表示します。

例：

```
n1000v# show  module
Mod  Ports  Module-Type                       Model              Status
---  -----  --------------------------------- ------------------ ------------
1    1      Virtual Supervisor Module         Nexus1000V         active *
2    48     Virtual Ethernet Module                              ok
3    48     Virtual Ethernet Module                              ok

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
1    4.0(0)S1(0.82)  0.0     --
2    NA              0.0     --
3    NA              0.0     --

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA
2    02-00-0c-00-02-00 to 02-00-0c-00-02-80  NA
3    02-00-0c-00-03-00 to 02-00-0c-00-03-80  NA

Mod  Server-IP        Server-UUID                            Server-Name
---  ---------------  -------------------------------------  --------------------
1    172.18.217.180                                          esx-1
2    172.18.117.44    487701ee-6e87-c9e8-fb62-001a64d20a20  esx-2
```

```
3    172.18.217.3     4876efdd-b563-9873-8b39-001a64644a24  esx-3

* this terminal session
```

例：

```
n1000v# show  server_info

Mod     Status          UUID
---     -----------     ----
  2      powered-up     34303734-3239-5347-4838-323130344654
  3      absent              371e5916-8505-3833-a02b-74a4122fc476
  4      powered-up     4880a7a7-7b51-dd96-5561-001e4f3a22f9
  5      absent              48840e85-e6f9-e298-85fc-001e4f3a2326
  6      powered-up     eb084ba6-3b35-3031-a6fe-255506d10cd0
n1000v#
```

例：

```
n1000v# show interface brief

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     172.28.15.211                           1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth2/2        1      eth  trunk  up      none                     a-1000(D) --

--------------------------------------------------------------------------------
Interface     VLAN   Type Mode   Status  Reason                   MTU
--------------------------------------------------------------------------------
```

例：

```
n1000v# show interface virtual

--------------------------------------------------------------------------------
Port        Adapter        Owner                    Mod Host
--------------------------------------------------------------------------------
Veth49                     R-VM-1                   2   mcs-srvr35
```

CHAPTER 5

コンフィギュレーションの管理

この章では、次の内容について説明します。

スイッチ名の変更

スイッチ名またはプロンプトをデフォルト（switch#）から別のストリングに変更するには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- コンフィギュレーション モードで CLI にログインします。

手順の詳細

	コマンド	目的

ステップ 1	**switchname**
	
	例：
	`n1000v(config)# switchname metro`
	`metro(config)# exit`
	`metro#`
		スイッチ プロンプトを変更します。

Message of the Day の設定

ユーザがログインする際に端末上のログイン プロンプトの前に表示される Message of the Day（MOTD）のメッセージを設定するには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- コンフィギュレーション モードで CLI にログインします。
- バナー メッセージは、最大 40 行、行あたり最大 80 文字です。
- デリミタを選ぶ際には、次のガイドラインに従ってください。
  - *メッセージストリング中ではデリミタを使用しないでください。*
  - **"** および **%** をデリミタとして使用しないでください。
- Message of the Day の中では次のトークンを使用できます。
  - `$(hostname)` を使用すると、スイッチのホスト名が表示されます。
  - `$(line)` を使用すると、vty または tty のラインまたは名前が表示されます。

手順の詳細

	コマンド	目的

ステップ 1	**banner motd [***delimiting-character message delimiting-character***]**
	
	例：
	`n1000v(config)# banner motd #April 16, 2008`
	`Welcome to the svs#`
	`n1000v(config)#`
		バナー Message of the Day を設定します。
		• 最大 40 行
		• 行あたり最大 80 文字
		• # などのデリミタで囲む
		• 複数行にまたがることが可能
		• トークンを使用可能

ステップ 2	**show banner motd**
	
	例：
	`n1000v(config)# show banner motd`
	`April 16, 2008 Welcome to the Switch`
		設定されているバナー メッセージを表示します。

コンフィギュレーションの表示

スイッチのコンフィギュレーションを表示するには、ここで説明する方法を使用します。ここでは、次の内容について説明します。

- 「ソフトウェアとハードウェアのバージョンの表示」（P.5-3）
- 「実行コンフィギュレーションの表示」（P.5-4）
- 「スタートアップ コンフィギュレーションと実行コンフィギュレーションの比較」（P.5-6）
- 「インターフェイス コンフィギュレーションの表示」（P.5-7）

ソフトウェアとハードウェアのバージョンの表示

アップグレードの前後でバージョンを確認するためなど、システム上のソフトウェアとハードウェアのバージョンを表示するには、ここに示すコマンドを使用します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

システムで動作しているソフトウェアとハードウェアのバージョンを表示するには、次の手順を実行します。

	コマンド	説明
ステップ 1	**show version** **例：** `n1000v# show version`	現在スイッチで動作しているシステム ソフトウェアとハードウェアのバージョンを表示します。

例：

```
n1000v(config-acl)# show ver
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  loader:    version 1.2(2) [last: image booted through mgmt0]
  kickstart: version 4.0(1) [build 4.0(1a)S1(0.122)]
  system:    version 4.0(1) [build 4.0(1a)S1(0.82)] [gdb]
  kickstart image file is:
  kickstart compile time:  10/19/2008 4:00:00
  system image file is:    bootflash:/isan.bin
  system compile time:     9/2/2008 1:00:00 [10/24/2008 05:12:58]


Hardware
  Cisco Nexus1000V ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU         with 1034780 kB of memory.
  Processor Board ID T5056807B1E

  Device name: n1000v
  bootflash:          0 kB
  slot0:              0 kB (expansion flash)

Kernel uptime is 3 day(s), 15 hour(s), 21 minute(s), 53 second(s)
```

```
plugin
  Core Plugin, Ethernet Plugin

n1000v#
```

実行コンフィギュレーションの表示

現在システムで動作しているコンフィギュレーションを表示するには、ここに示す方法を使用します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**show running-config** **例：** `n1000v# show running-config`	現在スイッチで動作しているシステム ソフトウェアとハードウェアのバージョンを表示します。

例：

```
n1000v(config-acl)# show running-config
version 4.0(1)
feature port-security
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role network-operator
username admin password 5 $1$N1mX5tLD$daXpuxlAPcIHoz53PBhy6/  role network-admin
telnet server enable
ssh key rsa 1024 force
kernel core target 0.0.0.0
kernel core limit 1
system default switchport
ip access-list my66
  10 permit ip 1.1.1.1/32 1.1.1.2/32
snmp-server user admin network-admin auth md5 0x90f3798f3e894496a11ec42ce2efec9c priv
0x90f3798f3e894496a11ec42ce2efec9c localizedkey
snmp-server enable traps entity fru
snmp-server enable traps license
vrf context management
  ip route 0.0.0.0/0 172.28.15.1
switchname srini-cp
vlan 40-43,45-48
vdc srini-cp id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource monitor-session minimum 0 maximum 32
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 192
  limit-resource u4route-mem minimum 32 maximum 256
  limit-resource u6route-mem minimum 16 maximum 256
```

```
interface Ethernet6/2
  inherit port-profile uplinkportprofile1

interface Ethernet6/3
  inherit port-profile uplinkportprofile2

interface Ethernet6/4
  inherit port-profile uplinportprofile3

interface Ethernet7/2
  inherit port-profile uplinkportprofile1

interface mgmt0
  ip address 172.28.15.163/24

interface Vethernet1


  inherit port-profile vm100

interface Vethernet2


  inherit port-profile vm100

interface Vethernet3


  inherit port-profile vm100

interface Vethernet4


  inherit port-profile vm100

interface Vethernet5

interface Vethernet6
boot kickstart bootflash:/svs-kickstart-mzg.4.0.1a.S1.0.82.bin sup-1
boot system bootflash:/svs-mzg.4.0.1a.S1.0.82.bin sup-1
boot system bootflash:/isan.bin sup-1
boot kickstart bootflash:/svs-kickstart-mzg.4.0.1a.S1.0.82.bin sup-2
boot system bootflash:/svs-mzg.4.0.1a.S1.0.82.bin sup-2
boot system bootflash:/isan.bin sup-2
ip route 0.0.0.0/0 172.28.15.1
port-profile uplinkportprofile1
  capability uplink
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 1,40-43
  no shutdown
  system vlan 1,40-43
  state enabled
port-profile vm100
  vmware port-group
  switchport mode access
  switchport access vlan 43
  ip port access-group my100 out
  ip port access-group my66 in
  no shutdown
  state enabled
port-profile uplinkportprofile2
  capability uplink
```

```
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 45-46
  no shutdown
  state enabled
port-profile uplinportprofile3
  capability uplink
  vmware port-group
  switchport trunk allowed vlan 47-48
  state enabled
port-profile uplinkportprofile3
  no shutdown
svs-domain
  domain id 163
  control vlan 41
  packet vlan 42
svs connection VCR5
  protocol vmware-vim
  remote ip address 172.28.30.83
  vmware dvs datacenter-name cisco-DC
  connect
```

スタートアップ コンフィギュレーションと実行コンフィギュレーションの比較

スタートアップ コンフィギュレーションと実行コンフィギュレーションの違いを表示するには、ここに示す手順を実行します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**show running-config diff** **例：** `n1000v# show running-config diff`	現在のシステムのスタートアップ コンフィギュレーションと実行コンフィギュレーションの差違を表示します。

例 5-1　　show running-config diff のコマンド出力

```
n1000v# show running-config diff
*** Startup-config
--- Running-config
***************
*** 1,7 ****
  version 4.0(1)
- system mem-thresholds minor 0 severe 0 critical 0
  vrf context management
```

```
    ip route 0.0.0.0/0 10.78.1.1
  switchname DCOS-112-S10
  vlan 80,110-111,150,160,170
  vdc DCOS-112-S10 id 1
--- 1,6 ----
***************
*** 116,131 ****
    ip address 10.78.1.112/24

  interface Vethernet49
    inherit port-profile vlan160

- interface Vethernet65
-   inherit port-profile vlan170
-
  interface Vethernet50
    inherit port-profile vlan160

  interface Vethernet66
    inherit port-profile vlan170
  ip route 0.0.0.0/0 10.78.1.1
  vlan 80-80, 110-110, 111-111, 150-150, 160-160, 170-170

--- 115,130 ----
    ip address 10.78.1.112/24

  interface Vethernet49
    inherit port-profile vlan160

  interface Vethernet50
    inherit port-profile vlan160

+ interface Vethernet65
+   inherit port-profile vlan170
+
  interface Vethernet66
    inherit port-profile vlan170
  ip route 0.0.0.0/0 10.78.1.1
  vlan 80-80, 110-110, 111-111, 150-150, 160-160, 170-170

n1000v#
```

インターフェイス コンフィギュレーションの表示

ここでは、次の手順について説明します。

- 「インターフェイス コンフィギュレーションの要約の表示」（P.5-7）
- 「インターフェイス コンフィギュレーションの詳細の表示」（P.5-8）
- 「全インターフェイスの要約の表示」（P.5-9）
- 「全インターフェイスの実行コンフィギュレーションの表示」（P.5-10）

インターフェイスの表示の詳細については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0*』を参照してください。

インターフェイス コンフィギュレーションの要約の表示

インターフェイス コンフィギュレーションの要約を表示するには、ここに示す手順を実行します。

始める前に

この手順を実行する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

システム上のインターフェイス コンフィギュレーションの要約を表示するには、次の手順を実行します。

	コマンド	説明
ステップ 1	**show interface** {*type*} {*name*} **brief**	指定したインターフェイス コンフィギュレーションに関する要約情報を表示します。

例：

```
n1000v# show interface mgmt 0 brief

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     10.78.1.63                              1000     1500
n1000v#
```

インターフェイス コンフィギュレーションの詳細の表示

インターフェイス コンフィギュレーションの詳細を表示するには、ここに示す手順を実行します。

始める前に

ここに示すコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

システム上の特定のインターフェイス コンフィギュレーションの詳細を表示するには、次の手順を実行します。

	コマンド	説明
ステップ 1	**show interface** {*type*} {*name*}	指定したインターフェイス コンフィギュレーションに関する詳細を表示します。

例：

```
n1000v# show interface mgmt 0
mgmt0 is up
    Hardware is GigabitEthernet, address is 0000.0000.0000 (bia 0050.5681.5578)
    Internet Address is 10.78.1.63/24
    MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
       reliability 255/255, txload 1/255, rxload 1/255
```

```
    Encapsulation ARPA
    full-duplex, 1000 Mb/s
    Beacon is turned off
    Auto-Negotiation is turned on
    Input flow-control is off, output flow-control is off
    59914 packets input, 10411045 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun, 0 fifo
    6317 packets output, 1390631 bytes
    0 underrun, 0 output errors, 0 collisions
    0 fifo, 0 carrier errors

n1000v#
```

全インターフェイスの要約の表示

システム上で設定されているすべてのインターフェイスの要約を表示するには、ここに示す手順を実行します。

始める前に

この手順を実行する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**show interface brief**	システム上の全インターフェイス コンフィギュレーションの要約を表示します。

例：

```
n1000v# show interface brief

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     10.78.1.63                              1000     1500

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth3/2        1      eth  trunk  up      none                     a-1000(D) --
Eth3/6        150    eth  trunk  up      none                     a-1000(D) --
Eth6/2        1      eth  trunk  up      none                     a-1000(D) --

--------------------------------------------------------------------------------
Interface     VLAN   Type Mode   Status  Reason                   MTU
--------------------------------------------------------------------------------
Veth81        630    virt access up      none                     1500
Veth82        630    virt access up      none                     1500
Veth224       631    virt access up      none                     1500
Veth225       1      virt access nonPcpt nonParticipating         1500
n1000v#
```

全インターフェイスの実行コンフィギュレーションの表示

システム上の全インターフェイスの実行コンフィギュレーションを表示するには、ここに示す手順を実行します。

始める前に

この手順を実行する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。
- コマンド **show running-config interface** の出力は、コマンド **show interface** の出力と異なります。

手順の詳細

	コマンド	説明
ステップ 1	**show running-config interface**	システム上の全インターフェイスの実行コンフィギュレーションを表示します。

例：

```
n1000v# show running-config interface
version 4.0(1)

interface Ethernet3/2
  switchport
  inherit port-profile sftrunk

interface Ethernet3/6
  switchport
  inherit port-profile vmuplink

interface Ethernet6/2
  switchport
  inherit port-profile alluplink

interface mgmt0
  ip address 10.78.1.63/24

interface Vethernet81
  inherit port-profile vm630

interface Vethernet82
  inherit port-profile vm630

interface Vethernet224
  inherit port-profile vm631

interface Vethernet225

n1000v#
```

コンフィギュレーションの保存

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するには、ここに示す手順を実行します。これにより、コンフィギュレーション ファイルに変更内容が保存され、次回システムを起動したときに有効になります。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。

手順の詳細

	コマンド	説明
ステップ 1	**copy running-config startup-config**	新しいコンフィギュレーションを不揮発性ストレージに保存します。これにより、実行コンフィギュレーションとスタートアップ コンフィギュレーションが同じになります。

例：

```
n1000v(config)# copy run start
[########################################] 100%
n1000v(config)#
```

コンフィギュレーションの削除

スタートアップ コンフィギュレーションを削除するには、ここに示す手順を実行します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

注意　**write erase** コマンドを実行すると、ローダ機能を除き、スタートアップ コンフィギュレーション全体が削除されます。

- CLI にログインします。
- このコマンドでは次のパラメータが使用されます。
  - boot：ブート変数と mgmt0 IP コンフィギュレーションを削除します。
  - debug：デバッグ コンフィギュレーションを削除します。

手順の詳細

	コマンド	説明
ステップ 1	**write erase** [boot | debug]	既存のスタートアップ コンフィギュレーションが完全に削除され、すべての設定が工場出荷時のデフォルトに戻ります。 実行コンフィギュレーションは影響を受けません。

CHAPTER 6

ファイルの使用

ここでは、Cisco Nexus 1000V のファイル システムについて説明します。このファイル システムは、スイッチが使用する次のようなファイル システムすべてに対する単一のインターフェイスを提供します。

- フラッシュ メモリ ファイル システム
- ネットワーク ファイル システム（TFTP および FTP）
- データを読み書きするためのその他のエンドポイント（NVRAM や実行コンフィギュレーションなど）

ここでは、次の内容について説明します。

ファイル システム内の移動

ここでは、ファイル システム内の移動方法について説明します。具体的な内容は次のとおりです。

ファイル システムの指定

ファイル システムを指定するための構文は、*<file system name>*:[//server/] です。表 6-1 にファイル システムの構文を示します。

表 6-1　ファイル システムの構文の構成要素

ファイル システム名	サーバ	説明
bootflash	sup-active sup-local sup-1 module-5 module-7	アクティブ スーパーバイザにあり、システム イメージ、コンフィギュレーション ファイル、その他のファイルを格納するために使用される、内部 CompactFlash メモリ。
	sup-standby sup-remote sup-2 module-6[1] module-8[2]	スタンバイ スーパーバイザにあり、システム イメージ、コンフィギュレーション ファイル、その他のファイルを格納するために使用される、内部 CompactFlash メモリ。
volatile	—	スーパーバイザ モジュールにある、一時的または保留中の変更のために使用される、Volatile Random-Access Memory（VRAM; 揮発性 RAM）。Cisco Nexus 1000V CLI ではデフォルトで volatile: ファイル システムになります。
modflash	slot-*slot*	Storage Services Module（SSM）にある、SSI ブート イメージを格納するために使用される CompactFlash。

作業ディレクトリの特定

CLI の現在のディレクトリ名を表示するには、ここに示す手順を実行します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。

手順の詳細

手順	コマンド	目的

ステップ 1	**pwd**
	
	例：
	`n1000v# pwd`
	`bootflash:`
		現在の作業ディレクトリを表示します。

ディレクトリの変更

CLI で、あるディレクトリまたはファイル システムから別のディレクトリまたはファイル システムに場所を変更するには、ここに示す手順を実行します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- 任意のコマンド モードで CLI にログインします。
- Cisco Nexus 1000V CLI ではデフォルトで volatile: ファイル システムになります。

ヒント volatile: ファイル システムに保存されたファイルは、スイッチのリブート時にすべて消去されます。

手順の詳細

手順	コマンド	目的

ステップ 1	**pwd**
	
	例：
	`n1000v# pwd`
	`volatile:`
	`n1000v#`
		CLI の現在のディレクトリ名を表示します。

ステップ 2	**cd** *directory name*	CLI の場所を指定したディレクトリに変更します
	例： `n1000v# cd bootflash:`	CLI の場所を、bootflash: ファイル システムのルート ディレクトリに変更します。
	例： `n1000v# cd bootflash:mydir`	CLI の場所を、bootflash: ファイル システムの mydir ディレクトリに変更します。
	例： `n1000v# cd mystorage`	CLI の場所を、現在のディレクトリの中にある mystorage ディレクトリに変更します。 現在のディレクトリが bootflash: mydir だった場合、このコマンドを実行すると、現在のディレクトリが bootflash: mydir/mystorage に変更されます。

ファイル システム内のファイルの一覧表示

ディレクトリまたはファイルの内容を表示するには、ここに示す手順を実行します。

手順の詳細

手順	コマンド	目的
ステップ 1	**dir** [*directory* | *filename*]	ディレクトリまたはファイルの内容を表示します。

例：

```
DCOS-112-R5# dir lost+found/
      49241     Jul 01 09:30:00 2008  diagclient_log.2613
      12861     Jul 01 09:29:34 2008  diagmgr_log.2580
         31     Jul 01 09:28:47 2008  dmesg
       1811     Jul 01 09:28:58 2008  example_test.2633
         89     Jul 01 09:28:58 2008  libdiag.2633
      42136     Jul 01 16:34:34 2008  messages
         65     Jul 01 09:29:00 2008  otm.log
        741     Jul 01 09:29:07 2008  sal.log
         87     Jul 01 09:28:50 2008  startupdebug

Usage for log://sup-local
   51408896 bytes used
  158306304 bytes free
  209715200 bytes total
DCOS-112-R5#
```

ファイルをコピーするために使用できるファイル システムの特定

コピー先またはコピー元として使用できるファイル システムを特定するには、ここに示す手順を実行します。

始める前に

この手順を実行する前に、次の点を理解または実行しておく必要があります。

- EXEC モードで CLI にログインします。

手順の詳細

手順	コマンド	目的
ステップ 1	**copy ?**	copy コマンドで使用できるコピー元ファイル システムを表示します。
ステップ 2	**copy filename ?**	copy コマンドで特定のファイルに対して使用できるコピー先ファイル システムを表示します。

例：

```
n1000v# copy ?
  bootflash:      Select source filesystem
  core:           Select source filesystem
  debug:          Select source filesystem
  ftp:            Select source filesystem
  licenses        Backup license files
  log:            Select source filesystem
  modflash:       Select source filesystem
  nvram:          Select source filesystem
  running-config  Copy running configuration to destination
  scp:            Select source filesystem
  sftp:           Select source filesystem
  startup-config  Copy startup configuration to destination
  system:         Select source filesystem
  tftp:           Select source filesystem
```

```
  volatile:       Select source filesystem
n1000v# copy filename ?
  bootflash:      Select destination filesystem
  ftp:            Select destination filesystem
  modflash:       Select destination filesystem
  nvram:          Select destination filesystem
  running-config  Copy from source to running configuration
  scp:            Select destination filesystem
  sftp:           Select destination filesystem
  system:         Select destination filesystem
  tftp:           Select destination filesystem
  volatile:       Select destination filesystem
n1000v#
```

ファイルのコピーとバックアップ

保存のためや別の場所で再利用するために、コンフィギュレーション ファイルなどのファイルをコピーするには、ここに示す手順を実行します。内部ファイル システムが壊れると、コンフィギュレーションが失われるおそれがあります。コンフィギュレーション ファイルは定期的に保存およびバックアップしてください。また、新しいソフトウェア コンフィギュレーションをインストールしたり、新しいソフトウェア コンフィギュレーションに移行する前に、既存のコンフィギュレーション ファイルをバックアップしてください。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- Telnet または SSH 接続を通じて CLI にログインしていること。
- 離れた場所にコピーする場合は、デバイスから宛先に到達できるルートがあること。サブネット間でトラフィックをルーティングするルータまたはデフォルト ゲートウェイがない場合は、使用デバイスとリモートのコピー先が同じサブネットワーク内にあることが必要です。
- ping コマンドを使用して、デバイスがコピー先に接続できること。
- コピー元のコンフィギュレーション ファイルがリモート サーバ上の正しいディレクトリにあること。
- コピー元ファイルのアクセス権が正しく設定されていること。ファイルのアクセス権は、誰でも読み取り可能に設定されている必要があります。

（注）　**dir** コマンドを使用して、コピー先のファイル システムに十分なスペースがあることを確認してください。十分なスペースがない場合は、**delete** コマンドを使用して不要なファイルを削除してください。

ファイル システム	サーバ	ファイル名
bootflash	sup-active sup-standby sup-1 または module-5 sup-2 または module-6 sup-local sup-remote	ユーザ指定
volatile	—	ユーザ指定
nvram	—	startup-config または snapshot-config

ファイル システム	サーバ	ファイル名
system	—	running-config
tftp[1]	IPv4 アドレス、IPv6 アドレス、または DNS 名	ユーザ指定
ftp		
scp（secure copy）		
sftp		
core	*slot-number*	プロセス識別番号

1. ファイルのダウンロードとアップロードを行う際には、TFTP の制限により、TFTP クライアントではファイル サイズが 32 MB に制限され、一部の TFTP サーバでは 16 MB に制限されます。

手順の詳細

手順	コマンド	目的
ステップ 1	**copy** [*source filesystem:*] *filename* [*destination filesystem:*] *filename*	指定したコピー元から指定したコピー先にファイルをコピーします。
	例： `n1000v# copy system:running-config tftp://10.10.1.1/home/configs/switch3-run.cfg`	実行コンフィギュレーションのコピーをリモートのスイッチに保存します。
	例： `copy nvram:startup-config SCP://10.10.1.1/home/configs/switch3-run.cfg`	スタートアップ コンフィギュレーションのコピーをリモートのスイッチに保存します。
	例： `n1000v# copy bootflash:system_image bootflash://sup-2/system_image`	アクティブ スーパーバイザ モジュールのブートフラッシュから、スタンバイ スーパーバイザ モジュールのブートフラッシュにファイルをコピーします。

	例：
	`n1000v# copy nvram:snapshot-config nvram:startup-config`
	`Warning: this command is going to overwrite your current startup-config.`
	`Do you wish to continue? {y/n} [y] y`
		NVRAM 内の既存のコンフィギュレーションの内容を上書きします。

	例： `n1000v# copy system:running-config bootflash:my-config`	実行コンフィギュレーションを bootflash: ファイル システムにコピーします。
	例： `n1000v# copy scp://user@10.1.7.2/system-image bootflash:system-image`	IPv4 アドレスで識別される SCP サーバからシステム イメージ ファイルをブートフラッシュにコピーします。
	例： `n1000v# copy sftp://172.16.10.100/myscript.txt volatile:myscript.txt`	IPv4 アドレスで識別される SFTP サーバからスクリプト ファイルを volatile: ファイル システムにコピーします。
	例： `n1000v# copy nvram:startup-config nvram:snapshot-config`	スタートアップ コンフィギュレーションのスナップショットを、スイッチ上の事前に定義された場所に作成します（バイナリ ファイル）。

手順	コマンド	目的
	例： `n1000v# copy nvram:startup-config bootflash:my-config`	スタートアップ コンフィギュレーションのバックアップ コピーを bootflash: ファイル システムに格納します（ASCII ファイル）。
	例： `n1000v# copy nvram:startup-config tftp://172.16.10.100/my-config`	スタートアップ コンフィギュレーションのバックアップ コピーを TFTP サーバに格納します（ASCII ファイル）。
	例： `n1000v# copy system:running-config bootflash:my-config`	実行コンフィギュレーションのバックアップ コピーを bootflash: ファイル システムに格納します（ASCII ファイル）。
	例： `n1000v# copy bootflash:samplefile bootflash:mystorage/samplefile`	samplefile という名前のファイルを、bootflash: ファイル システムのルート ディレクトリから mystorage ディレクトリにコピーします。
	例： `n1000v# copy samplefile mystorage/samplefile`	現在のファイル システム内でファイルをコピーします。
	例： `n1000v# copy tftp://10.10.1.1/home/configs/switch3-run.cfg system:running-config`	コピー元ファイルをスイッチの実行コンフィギュレーションにコピーします。ファイルは行単位で解析され、スイッチが設定されます。

タブ補完の使用

CLI でコマンド中の部分的なファイル名を補完するには、次に示す手順を実行します。

	コマンド	目的

ステップ 1	**show file** ***filesystem name: partial filename*** <Tab>
	
	例：
	`n1000v# show file bootflash:svs-`
	`bootflash:svs-dplug-mzg.4.0.0.S1.0.34.bin`
	`bootflash:svs-kickstart-mzg.4.0.0.S1.0.34.bin`
	`bootflash:svs-mzg.4.0.0.S1.0.34.bin`
	`n1000v# show file bootflash:svs-`
		部分的なファイル名を入力して Tab キーを押すと、入力した文字が単一のファイルに一致する場合、CLI によりファイル名が補完されます。
		一致しない場合は、入力した文字に一致するファイル名の選択肢の一覧が表示されます。
		その後、ファイル名が一意になるような十分な文字を入力することで、CLI によりファイル名が補完されます。

ステップ 2	**show file bootflash:c** <Tab>
	
	例：
	`n1000v# show file bootflash:c<Tab>`
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIICXgIBAAKBgQDSq93BrlHcg3bX1jXDMY5c9+yZSST3VhuQ`
	`BqogvCPDGeLecA+j`
	`...`
	`...`
	`n1000v#`
		CLI によりファイル名が補完されます。

ディレクトリの作成

現在のディレクトリ レベルまたは指定したディレクトリ レベルにディレクトリを作成するには、次の手順を実行します。

手順	コマンド	目的
ステップ 1	**mkdir** *directory name* **dir** *filename*	現在のディレクトリ レベルにディレクトリを作成します。

	例：
	`n1000v# mkdir bootflash:test`
	`n1000v#`
		test という名前のディレクトリを bootflash: ディレクトリに作成します。

	例：
	`n1000v# mkdir test`
	`n1000v#`
		test という名前のディレクトリを現在のディレクトリ レベルに作成します。現在のディレクトリが bootflash:mydir の場合、このコマンドを実行すると、bootflash:mydir/test というディレクトリが作成されます。

既存のディレクトリの削除

フラッシュ ファイル システムから既存のディレクトリを削除するには、次の手順を実行します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。
- このコマンドは、フラッシュ ファイル システムでだけ有効であること。
- ディレクトリを削除するには、ディレクトリが空であること。

手順の詳細

手順	コマンド	目的
ステップ 1	**rmdir** {bootflash: | modflash: | volatile:} *directory*	ディレクトリを削除します。

	例：
	`n1000v# rmdir bootflash:test`
	`n1000v#`
		bootflash ディレクトリ内の test という名前のディレクトリを削除します。

	例：
	`n1000v# rmdir test`
	`n1000v#`
		現在のディレクトリ レベルにある test という名前のディレクトリを削除します。現在のディレクトリが bootflash:mydir の場合、このコマンドを実行すると、bootflash:mydir/test ディレクトリが削除されます。

ファイルの移動

ある場所から別の場所にファイルを移動するには、次の手順を実行します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。
- 移動先のディレクトリに十分なスペースがない場合、コピーは完了しないこと。

注意　移動先のディレクトリに同じ名前のファイルがすでに存在する場合、そのファイルは移動したファイルで上書きされます。

手順の詳細

手順	コマンド	目的
ステップ 1	**move** {*source path and filename*}　{*destination path and filename*}	ディレクトリを削除します。
	例： `n1000v# move slot0:samplefile bootflash:mystorage/samplefile`	あるディレクトリから同じファイル システム（bootflash:）内の別のディレクトリにファイルを移動します。
	例： `n1000v# move samplefile mystorage/samplefile`	現在のファイル システム内であるディレクトリから別のディレクトリにファイルを移動します。

ファイルまたはディレクトリの削除

フラッシュ メモリ デバイス上のファイルまたはディレクトリを削除するには、ここに示す手順を実行します。

始める前に

注意　削除する際にファイル名の代わりにディレクトリ名を指定すると、ディレクトリとその内容がすべて削除されます。

- ファイルを削除する場合、ソフトウェアによってファイルが消去されます。
- 環境変数 CONFIG_FILE または BOOTLDR で指定されているコンフィギュレーション ファイルまたはイメージを削除しようとすると、削除を確認するプロンプトが表示されます。
- BOOT 環境変数で指定されている最後の有効なシステム イメージを削除しようとすると、削除を確認するプロンプトが表示されます。

手順の詳細

手順	コマンド	目的
ステップ 1	delete [bootflash: | debug: | log: | modflash: | volatile:] *filename or directory name* **例：** `n1000v# delete bootflash:dns_config.cfg`	指定したファイルまたはディレクトリを削除します。
	例： `n1000v# delete dns_config.cfg`	指定したファイルを現在の作業ディレクトリから削除します。
	例： `n1000v# delete bootflash:my-dir`	指定したディレクトリとその内容を削除します。

ファイルの圧縮

LZ77 符号化を使用して指定したファイルを圧縮（zip）するには、ここに示す手順を実行します。

始める前に

- CLI にログインしていること。

手順の詳細

手順	コマンド	目的

ステップ 1	**show** *command* > [*path*] *filename*
	
	例：
	`n1000v# show l2fm internal event-history errors > errorsfile`
	`n1000v#`
		show コマンドの出力をファイルに保存します。

ステップ 2	`dir`
	
	例：
	`n1000v# dir`
		最初の手順で作成した新しいファイルを含め、現在のディレクトリの内容を表示します。

手順　コマンド	目的
ステップ 3　**gzip** *[path] filename* **例：** n1000v# gzip bootflash:errorsfile n1000v#	指定したファイルを圧縮します。
ステップ 4　**dir** **例：** n1000v# dir	新たに圧縮したファイルを含め、指定したディレクトリの内容を表示します。新たに圧縮したファイルのファイル サイズの違いを表示します。

例：

```
n1000v# show l2fm internal event-history errors > errorsfile
n1000v# dir
       1681     Jun 30 05:21:08 2008  cisco_svs_certificate.pem
       2687     Jul 01 18:17:20 2008  errorsfile
      16384     Jun 30 05:17:51 2008  lost+found/
       4096     Jun 30 05:18:29 2008  routing-sw/
         49     Jul 01 17:09:18 2008  sample_test.txt
    1322843     Jun 30 05:17:56 2008  svs-dplug-mzg.4.0.0.S1.0.34.bin
   21629952     Jun 30 05:18:02 2008  svs-kickstart-mzg.4.0.0.S1.0.34.bin
   39289400     Jun 30 05:18:14 2008  svs-mzg.4.0.0.S1.0.34.bin

Usage for bootflash://
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
n1000v# gzip bootflash:errorsfile
n1000v# dir
       1681     Jun 30 05:21:08 2008  cisco_svs_certificate.pem
        703     Jul 01 18:17:20 2008  errorsfile.gz
      16384     Jun 30 05:17:51 2008  lost+found/
       4096     Jun 30 05:18:29 2008  routing-sw/
         49     Jul 01 17:09:18 2008  sample_test.txt
    1322843     Jun 30 05:17:56 2008  svs-dplug-mzg.4.0.0.S1.0.34.bin
   21629952     Jun 30 05:18:02 2008  svs-kickstart-mzg.4.0.0.S1.0.34.bin
   39289400     Jun 30 05:18:14 2008  svs-mzg.4.0.0.S1.0.34.bin

Usage for bootflash://
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
n1000v#
```

ファイルの圧縮解除

LZ77 符号化を使用して圧縮された、指定したファイルを圧縮解除（unzip）するには、ここに示す手順を実行します。

始める前に

- CLI にログインしていること。

手順の詳細

手順	コマンド	目的
ステップ 1	**gunzip** [path] *filename*	指定したファイルを圧縮解除します。
ステップ 2	**dir**	新たに圧縮解除したファイルを含め、ディレクトリの内容を表示します。

例：

```
n1000v# gunzip bootflash:errorsfile.gz
n1000v# dir bootflash:
       1681     Jun 30 05:21:08 2008  cisco_svs_certificate.pem
       2687     Jul 01 18:17:20 2008  errorsfile
      16384     Jun 30 05:17:51 2008  lost+found/
       4096     Jun 30 05:18:29 2008  routing-sw/
         49     Jul 01 17:09:18 2008  sample_test.txt
    1322843     Jun 30 05:17:56 2008  svs-dplug-mzg.4.0.0.S1.0.34.bin
   21629952     Jun 30 05:18:02 2008  svs-kickstart-mzg.4.0.0.S1.0.34.bin
   39289400     Jun 30 05:18:14 2008  svs-mzg.4.0.0.S1.0.34.bin

Usage for bootflash://sup-local
  258408448 bytes used
 2939531264 bytes free
 3197939712 bytes total
DCOS-112-R5#
```

コマンド出力のファイル保存

コマンド出力をファイルに保存するには、次の手順を実行します。

手順の詳細

手順	コマンド	目的
ステップ 1	**show running-config >** [*path* | *filename*]	コマンド **show running-config** の出力を、指定したパスおよびファイル名に保存します。
	例： `n1000v# show running-config > volatile:switch1-run.cfg`	コマンド **show running-config** の出力を、volatile: ファイル システム上のファイル switch1-run.cfg に保存します。
	例： `n1000v# show running-config > bootflash:switch2-run.cfg`	コマンド **show running-config** の出力を、ブートフラッシュ上のファイル switch2-run.cfg に保存します。
	例： `n1000v# show running-config > tftp://10.10.1.1/home/configs/switch3-run.cfg`	コマンド **show running-config** の出力を、TFTP サーバ上のファイル switch3-run.cfg に保存します。
	例： `n1000v# show interface > samplefile`	コマンド show interface の出力を、ブートフラッシュなど、同じディレクトリ レベルのファイル samplefile に保存します。

ロード前のコンフィギュレーション ファイルの確認

イメージをロードする前にその完全性を確認するには、ここに示す手順を実行します。このコマンドは、システム イメージとキックスタート イメージの両方に使用できます。

手順の詳細

手順	コマンド	目的
ステップ 1	**copy** *source path and file* **system:running-config** **例：** `n1000v# copy tftp://10.10.1.1/home/configs/switch3-run.cfg system:running-config`	コピー元ファイルをスイッチの実行コンフィギュレーションにコピーします。ファイルは行単位で解析され、スイッチが設定されます。
ステップ 2	**show version image** [bootflash: | modflash: |volatile:]	指定したイメージを検証します。

例：

```
n1000v# show version image bootflash:
Md5 Verification Failed
Image integrity check failed
```

スタートアップ コンフィギュレーション ファイルのロック解除

アプリケーションまたはスイッチによって行われているスタートアップ コンフィギュレーション ファイルのロックを表示または解除するには、次の手順を実行します。

手順の詳細

手順	コマンド	目的
ステップ 1	**show system internal sysmgr startup-config locks** **例：** `n1000v# show system internal sysmgr startup-config locks`	スイッチ上のアプリケーションによりスタートアップ コンフィギュレーション ファイルに対して行われているロックを表示します。
ステップ 2	**system startup-config unlock** {*lock id*} **例：** `n1000v# system startup-config unlock 10`	スタートアップ コンフィギュレーション ファイルから指定したロック ID を削除します。 指定可能なロック ID の範囲は、0 ～ 65536 です。

例：

```
n1000v# show system internal sysmgr startup-config locks
There are no startup-config locks acquired.
```

以前のコンフィギュレーションへのロールバック

以前保存したコンフィギュレーションからコンフィギュレーションを復元するには、ここに示す手順を実行します。

始める前に

（注） **copy running-config startup-config** コマンドを実行するたびに、バイナリ ファイルが作成され、ASCII ファイルが更新されます。有効なバイナリ コンフィギュレーション ファイルを使用すると、ブート全体の時間が大幅に短縮されます。バイナリ ファイルはアップロードできませんが、その内容を使用して既存のスタートアップ コンフィギュレーションを上書きできます。**write erase** コマンドを実行すると、バイナリ ファイルが消去されます。

手順の詳細

手順	コマンド	目的
ステップ 1	**copy running-config bootflash:** {*filename*} **例：** `n1000v# copy running-config bootflash:June03-Running`	以前保存した実行コンフィギュレーションのスナップショット コピー（バイナリ ファイル）に戻します。

	`copy bootflash:` {*filename*} `nvram:startup-config`
	
	例：
	`n1000v# copy bootflash:my-config nvram:startup-config`
		bootflash: ファイル システムに以前保存したコンフィギュレーションのコピー（ASCII ファイル）に戻します。

ファイルの表示

ここでは、ファイルに関する情報の表示方法について説明します。具体的には次の手順について説明します。

- 「ファイルの圧縮」（P.6-10）
- 「ファイル チェックサムの表示」（P.6-16）
- 「ファイル チェックサムの表示」（P.6-16）
- 「ファイルの最後の行の表示」（P.6-16）

ファイルの内容の表示

指定したファイルの内容を表示するには、次の手順を実行します。

始める前に

- CLI にログインしていること。

手順の詳細

手順	コマンド	目的

ステップ 1	**show file [bootflash: | modflash: | volatile:]** *filename*
	
	例：
	`n1000v# show file bootflash:sample_test.txt`
	`config t`
	`Int veth1/1`
	`no shut`
	`end`
	`show int veth1/1`
	
	`n1000v#`
		指定したファイルの内容を表示します。

ディレクトリの内容の表示

ディレクトリまたはファイル システムの内容を表示するには、ここに示す手順を実行します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。

手順	コマンド	目的

ステップ 1	**pwd**
	
	例：
	`n1000v# pwd`
	`bootflash:`
		現在の作業ディレクトリを表示します。

ステップ 2	**dir**	ディレクトリの内容を表示します。

例：

```
n1000v# pwd
bootflash:
n1000v# dir

Usage for volatile://
          0 bytes used
   20971520 bytes free
```

```
   20971520 bytes total
n1000v#
```

ファイル チェックサムの表示

ファイルの完全性を確認するためにチェックサムを表示するには、次の手順を実行します。

手順	コマンド	目的

ステップ 1	**show file** *filename* [**cksum** | **md5sum**]
	
	例：
	`n1000v# show file bootflash:cisco_svs_certificate.pem cksum`
	`266988670`
		元のファイルと比較するために、ファイルのチェックサムまたは Message-Digest Algorithm 5（MD5）チェックサムを表示します。

	例：
	`n1000v# show file bootflash:cisco_svs_certificate.pem md5sum`
	`d3013f73aea3fda329f7ea5851ae81ff`
	`n1000v#`
		ファイルの Message-Digest Algorithm 5（MD5）チェックサムを表示します。MD5 はファイルの電子的なフィンガープリントです。

ファイルの最後の行の表示

指定したファイルの最後の行（末尾）を表示するには、ここに示すコマンドを使用します。

始める前に

- EXEC モードで CLI にログインします。

手順の詳細

手順　コマンド	目的
ステップ 1　**tail** {*path*}[*filename*] {*Number of lines*}	指定したファイルの末尾から、要求された数の行を表示します。 行数に指定できる範囲は 0 ～ 80 です。

例：

```
n1000v# tail bootflash:errorsfile 5

20) Event:E_DEBUG, length:34, at 171590 usecs after Tue Jul  1 09:29:05 2008
    [102] main(326): stateless restart


n1000v#
```

CHAPTER 7

ユーザの管理

ここでは、次の手順について説明します。

スイッチにアクセスしているユーザ情報の表示

この手順を使用して、現在スイッチにアクセスしているすべてのユーザを表示します。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。

手順の詳細

	コマンド	説明
ステップ 1	**show users**	現在システムにアクセスしているユーザのリストを表示します。

例：

```
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    pts/0        Jul  1 04:40 03:29        2915 (::ffff:64.103.145.136)
admin    pts/2        Jul  1 10:06 03:37        6413 (::ffff:64.103.145.136)
admin    pts/3        Jul  1 13:49    .         8835 (171.71.55.196)*
n1000v#
```

ユーザへのメッセージ送信

このコマンドを使用して、現在システムを使用しているすべてのアクティブな CLI ユーザにメッセージを送信できます。

始める前に

このコマンドを使用する前に、次の点を理解または実行しておく必要があります。

- CLI にログインしていること。

手順の詳細

	コマンド	説明
ステップ 1	**send** {line | session *device*} *string*	現在システムにログインしているユーザにメッセージを送信します。 • **line**：すべての開かれているセッションにメッセージ（行）を送信します。 • **session**：指定された pts または tty デバイス タイプにメッセージを送信します。 • **string**：メッセージ（最長 80 文字までの英数文字）。

例：

```
n1000v# send line Hello. Shutting down the system in 10 minutes.

Broadcast Message from admin@switch
        (/dev/pts/34) at 8:58 ...

line Hello. Shutting down the system in 10 minutes.


n1000v#
```

CHAPTER 8

NTP の設定

この章では、Network Time Protocol（NTP; ネットワーク タイム プロトコル）の設定方法について説明し、次の内容が含まれます。

NTP の概要

ここでは、次の内容について説明します。

NTP の概要

ネットワーク タイム プロトコル（NTP）は、分散している一連のタイム サーバおよびクライアント間で、計時を同期させます。この同期によって、複数のネットワーク デバイスからシステム ログおよびその他の時刻特定イベントを受信したときに、イベントを相互に関連付けることができます。

NTP ではトランスポート プロトコルとして、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用します。すべての NTP 通信で Universal Time Coordinated（UTC; 協定世界時）規格を使用します。NTP サーバは通常、タイム サーバに接続されたラジオ クロック、アトミック クロックなど、信頼できる時刻源から時刻を受信します。NTP はこの時刻をネットワーク全体に配信します。NTP はきわめて効率的です。毎分 1 パケット以下で、2 台のマシンが相互に 1 ミリ秒以内で同期します。

NTP では層（stratum）を使用して、ネットワーク デバイスが正規の時刻源から NTP ホップ数にしてどれだけ離れているかを表します。Stratum 1 タイム サーバは、正規の時刻源（アトミック クロックなど）が直接接続されています。Stratum 2 の NTP サーバは、Stratum 1 NTP サーバから NTP を使用して時刻を受信し、それによって正規の時刻源に接続します。

NTP は正確な時刻を維持している可能性のあるネットワーク デバイスへの同期を回避します。また、NTP は順番どおりに同期しないシステムには、同期しません。NTP は複数のネットワーク デバイスから伝えられた時刻を比較し、時刻が他と大きく異なっているネットワーク デバイスには、下位の層であっても同期しません。

Cisco NX-OS は Stratum 1 サーバとして動作しません。したがって、ラジオ クロックまたはアトミック クロックには接続できません。インターネット上で利用できる、パブリックな NTP サーバに由来するタイム サービスをネットワークに使用することを推奨します。

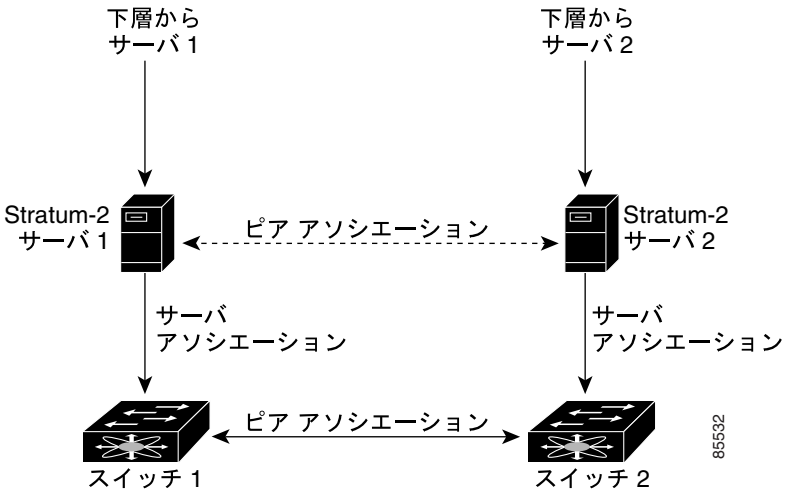
ネットワークがインターネットから切り離されている場合、Cisco NX-OS ではネットワーク デバイスが実際には他の方法で時刻を決定している場合でも、NTP によって同期しているものとして動作するように、ネットワーク デバイスを設定できます。その後、NTP を使用して、そのネットワーク デバイスに他のネットワーク デバイスを同期させることができます。

NTP ピア

NTP を使用すると、2 つのネットワーキング デバイス間にピア関係を設定できます。ピアはそのままで時刻を提供することも、または NTP サーバに接続することもできます。ローカル デバイスとリモート ピアの両方がそれぞれ異なる NTP サーバに接続すると、NTP サービスの信頼性が高くなります。ローカル デバイスはピアから得た時刻を使用することによって、接続先の NTP サーバに障害が発生した場合でも、正確な時刻を維持できます。

図 8-1 に、2 台の NTP Stratum 2 サーバおよび 2 台のスイッチからなるネットワークを示します。

図 8-1　NTP ピアおよびサーバのアソシエーション



この構成では、スイッチ 1 とスイッチ 2 は NTP ピアになっています。スイッチ 1 は Stratum-2 サーバ 1 を使用し、スイッチ 2 は Stratum-2 サーバ 2 を使用します。Stratum-2 サーバ 1 に障害が発生すると、サーバ 1 はスイッチ 2 に関連付けられたピア経由で正しい時刻を維持します。

ハイ アベイラビリティ

NTP はステートレス リスタートをサポートします。リブート後またはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションが適用されます。

NTP ピアを設定すると、NTP サーバ障害の発生時に冗長性が得られます。

NTP の前提条件

NTP を設定する場合は、NTP が動作している 1 つ以上のサーバに接続できなければなりません。

設定時の注意事項および制約事項

NTP に関する設定時の注意事項および制約事項は、次のとおりです。

- 別のデバイスとの間にピア アソシエーションを設定できるのは、使用するクロックの信頼性が確実な場合（つまり、信頼できる NTP サーバのクライアントである場合）に限られます。
- 単独で設定したピアは、サーバの役割を担いますが、バックアップとして使用する必要があります。サーバが 2 台ある場合、一部のデバイスが一方のサーバに接続し、残りのデバイスが他方のサーバに接続するように設定できます。その後、2 台のサーバ間にピア アソシエーションを設定すると、信頼性の高い NTP 構成になります。
- サーバが 1 台だけの場合は、すべてのデバイスをそのサーバのクライアントとして設定する必要があります。
- 設定できる NTP エンティティ（サーバおよびピア）は、最大 64 です。

NTP サーバおよびピアの設定

この手順を使用して、NTP サーバとピアを設定します。

始める前に

- NTP を設定するには、IPv4 アドレスまたはドメイン ネーム サーバ（DNS）名を使用します。

手順の概要

1. **config t**
2. **ntp server** {*ip-address* | *ipv6-address* | *dns-name*}
3. **ntp peer** {*ip-address* | *ipv6-address* | *dns-name*}
4. **show ntp peers**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ntp server** {*ip-address* | *ipv6-address* | *dns-name*} **例：** `n1000v(config)# ntp server 192.0.2.10`	サーバとのアソシエーションを作成します。
ステップ 3	**ntp peer** {*ip-address* | *dns-name*} `n1000v(config)# ntp peer 2001:0db8::4101`	ピアとのアソシエーションを作成します。複数のピア アソシエーションを指定できます。
ステップ 4	**show ntp peers** **例：** `n1000v(config)# show ntp peers`	（任意）設定済みのサーバおよびピアを表示します。 **（注）** ドメイン名が解決されるのは、DNS サーバが設定されている場合だけです。
ステップ 5	**copy running-config startup-config** **例：** `n1000v(config-if)# copy running-config startup-config`	（任意）この設定変更を保存します。

次に、NTP サーバとピアを設定する例を示します。

```
n1000v# config t
n1000v(config)# ntp server 192.0.2.10
n1000v(config# ntp peer 2001:0db8::4101
```

NTP 統計のクリア

次のコマンドを使用して、NTP 統計をクリアします。

コマンド	目的
clear ntp statistics	NTP 統計をクリアします。

NTP セッションのクリア

次のコマンドを使用して、NTP セッションをクリアします。

コマンド	目的
clear ntp session	NTP セッションをクリアします。

NTP の設定確認

NTP の設定情報を表示するには、次のコマンドのいずれかを使用します。

コマンド	目的
show ntp peer-status	すべての NTP サーバおよびピアのステータスを表示します。
show ntp peers	すべての NTP ピアを表示します。
show ntp statistics {**io** | **local** | **memory** | **peer** {*ip-address* | *dns-name*}}	NTP 統計を表示します。
show ntp status	NTP 配信ステータスを表示します。
show ntp timestamp status	タイムスタンプ チェックがイネーブルかどうかを表示します。

NTP の設定例

NTP サーバの設定例を示します。

```
config t
ntp server 192.0.2.10
```

デフォルト設定

次のテーブルは、CDP および NTP パラメータのデフォルト設定をリスト表示しています。

パラメータ	デフォルト
NTP	イネーブル

その他の関連資料

NTP に関する詳細情報については、次の項を参照してください。

- 「関連資料」（P.8-6）
- 「標準規格」（P.8-6）

関連資料

関連項目	マニュアル タイトル
インターフェイス	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

CHAPTER 9

ローカル SPAN および ER SPAN の設定

この章では、ローカルおよび ER イーサネット Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）機能を設定して、トラフィックを監視する方法を説明します。また、次の内容が含まれます。

SPAN の概要

スイッチド ポート アナライザ（SPAN）機能（ポート ミラーリングまたはポート モニタリングとも呼ばれます）では、Cisco SwitchProbe やその他の Remote Monitoring（RMON; リモート モニタリング）プローブなどのネットワーク アナライザを使用して、ネットワーク トラフィックを分析できます。

SPAN では、1 つ以上のポートまたは 1 つ以上の VLAN 上のトラフィックを監視して、ネットワーク アナライザが接続されている 1 つ以上の宛先ポートに、監視されたトラフィックを送信できます。

ここでは、次の内容について説明します。

SPAN 送信元

トラフィックを監視できるインターフェイスは、SPAN 送信元と呼ばれます。SPAN 送信元には、イーサネット、仮想イーサネット、ポートチャネル、VLAN があります。VLAN が SPAN 送信元として指定されると、VLAN でサポートされているすべてのインターフェイスは、SPAN 送信元となります。トラフィックは、受信方向、送信方向で監視できます。また、イーサネットおよび仮想イーサネット送信元インターフェイスの場合は、双方向で監視できます。

- 受信ソース（Rx）：この送信元ポート経由でスイッチに入るトラフィックは、SPAN 宛先ポートにコピーされます。

- 送信ソース（Tx）：この送信元ポート経由でスイッチから出るトラフィックは、SPAN 宛先ポートにコピーされます。

送信元ポートの特徴

Cisco Nexus 1000V がサポートする送信元ポート数は無制限（最大数はスイッチで利用可能なポート数）です。サポートする送信元 VLAN 数も無制限です。

送信元ポートには次の特徴があります。

- イーサネット、仮想イーサネット、ポートチャネル、VLAN のいずれかのポート タイプを使用できます。
- 宛先ポートとしての使用はできません。
- トラフィックの方向（受信、送信、双方向）を監視するように設定できます。
- 送信元ポートは同じ VLAN にも異なる VLAN にも配置できます。
- VLAN SPAN 送信元の場合、送信元 VLAN のすべてのアクティブなポートが送信元ポートとして含まれます。
- ローカル SPAN 送信元は、宛先ポートと同じホスト（ラインカード）上になければなりません。

SPAN 宛先

SPAN 宛先とは、送信元ポートを監視するインターフェイスを指します。Cisco Nexus 1000V では、宛先は必ずポートになります。Cisco Nexus 1000V は、SPAN 宛先として、イーサネットおよび仮想イーサネット インターフェイスをサポートします。この項には次の内容が含まれます。

ローカル SPAN 宛先ポートの特徴

各ローカル SPAN セッションには、送信元ポートまたは VLAN からトラフィックのコピーを受信するために、1 つ以上の宛先ポート（モニタリング ポートとも呼ばれます）が必要です。宛先ポートには次の特徴があります。

- 物理または仮想イーサネット ポートまたはポート チャネルとして使用できます。
- 送信元ポートとしての使用はできません。
- SPAN セッションの送信元 VLAN に属する場合、送信元リストから除外され、監視されません。
- すべての監視された送信元ポートでの送受信トラフィックのコピーを受信します。宛先ポートがオーバーサブスクライブ状態になっている場合、輻輳する可能性があります。この輻輳は 1 つ以上の送信元ポートでのトラフィック転送に影響する可能性があります。
- 送信元ポートと同じホスト（ラインカード）上になければなりません。
- ローカル SPAN では、送信元インターフェイスおよび宛先インターフェイスは、同じデバイス上になければなりません。
  図 9-1 およびローカル SPAN を参照してください。

ER SPAN 宛先ポートの特徴

- ERSPAN では、送信元 SPAN インターフェイスおよび宛先 SPAN インターフェイスは、IP ネットワークで相互接続した異なるデバイス上にある場合があります。ERSPAN トラフィックは GRE によってカプセル化されています。図 9-2 およびERSPAN を参照してください。

ローカル SPAN

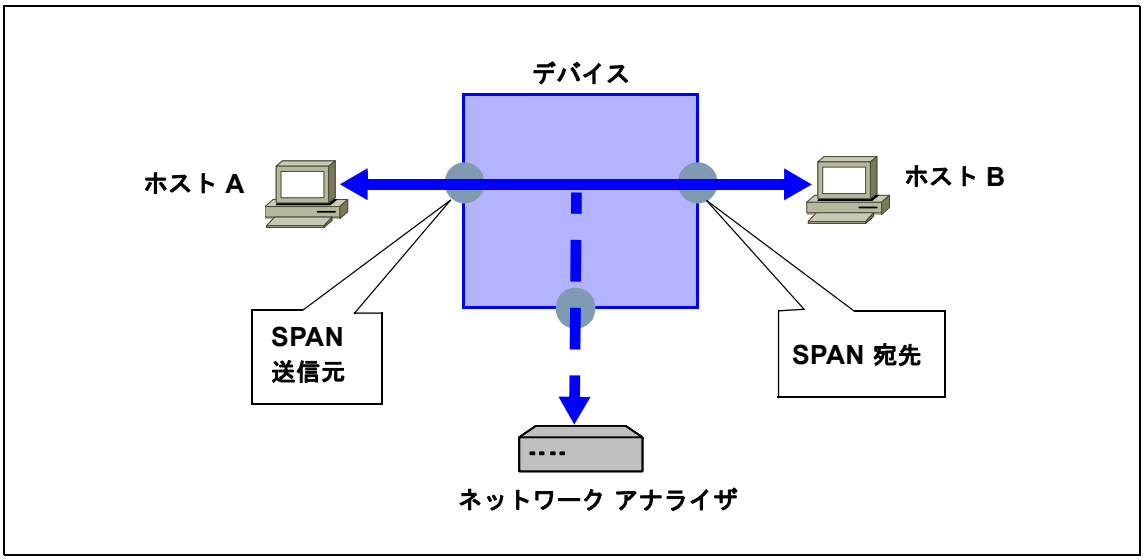
ローカル SPAN では、送信元インターフェイスおよび宛先インターフェイスは、同じデバイス上になければなりません。ネットワーク アナライザは、SPAN 宛先ポートに直接接続しています。SPAN 送信元は、VLAN インターフェイスのポートとして使用できます。宛先は、通常はポートですが、VLAN としても使用できます。

図 9-1 では、ホスト A から送信されたトラフィックが、SPAN 送信元インターフェイスで受信されます。トラフィック（ACL、QoS など）は、通常どおり処理されます。その後、トラフィックが複製されます。元のパケットは、ホスト B に対して転送されます。次に、複製されたパケットは、モニタが接続されている宛先 SPAN インターフェイスに送信されます。

ローカル SPAN は、1 つ以上の宛先ポートに複製できます。トラフィックをフィルタリングできるため、必要なトラフィックだけが宛先 SPAN インターフェイスを送信します。

ローカル SPAN は、BPDU を含む送信元インターフェイスで受信されるすべてのトラフィックを監視できます。

図 9-1　　ローカル SPAN

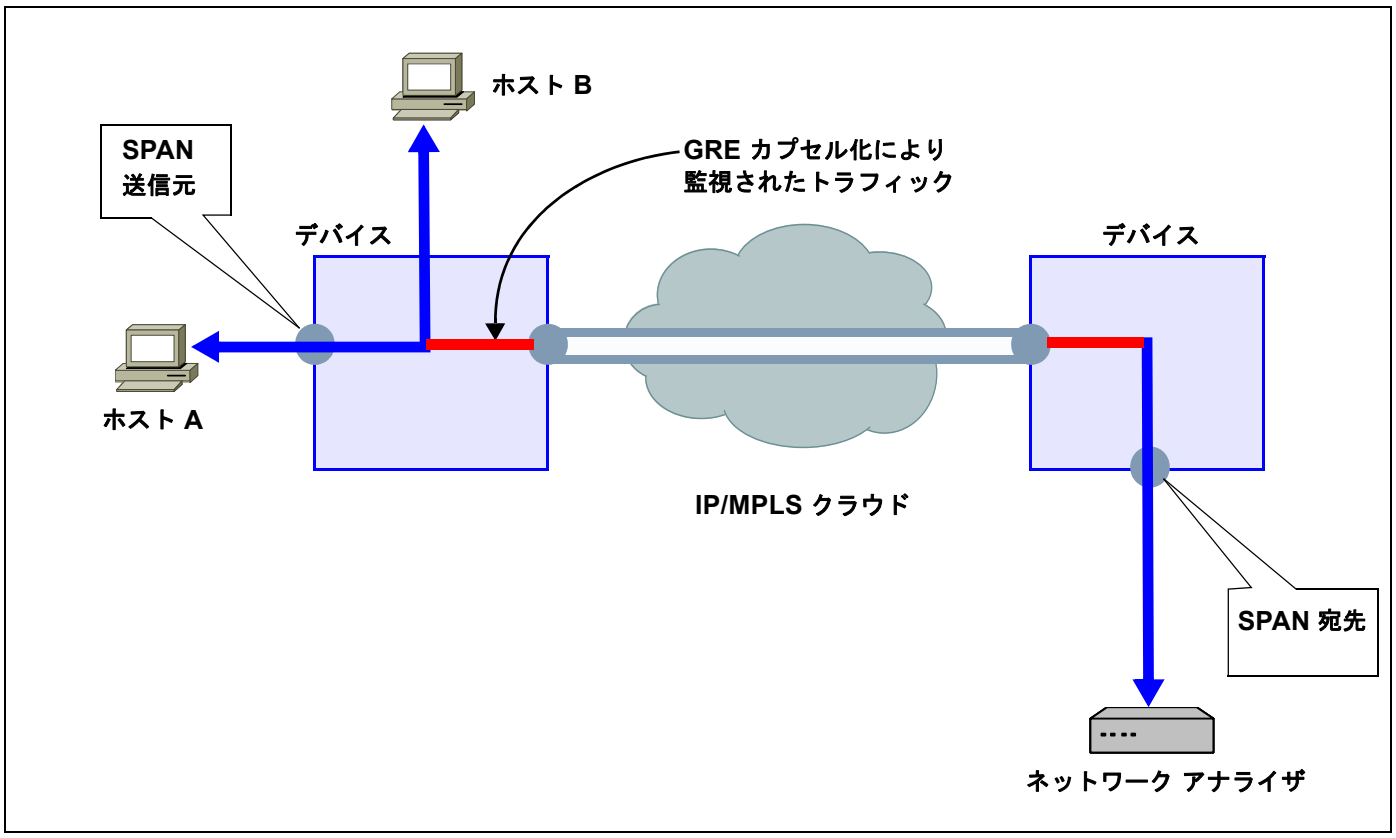


カプセル化リモート SPAN

Encapsulated remote（ER; カプセル化リモート）SPAN は、IP ネットワーク全体の複数のネットワーク デバイスのトラフィックを監視し、カプセル化エンベロープにあるトラフィックを宛先アナライザに送信します。これとは対照的に、ローカル Local SPAN は、IP ネットワーク経由でトラフィックを転送できません。ERSPAN を使用して、リモートでトラフィックを監視できます。ERSPAN 送信元には、ポートまたは VLAN を設定できます。

図 9-2 では、ホスト A の入出力トラフィックが ERSPAN によって監視されています。カプセル化された ERSPAN パケットは、ルーティングされたネットワーク経由で、ホスト A から宛先デバイスにルーティングされます。宛先デバイスでは、ERSPAN パケットのカプセルを解除して、接続しているネットワーク アナライザに転送します。宛先は送信元と同じ L2 ネットワークにすることもできます。

図 9-2　ERSPAN



SPAN セッション

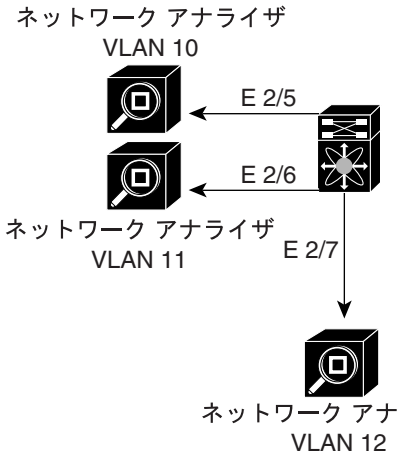
最大合計 64 の SPAN セッション（ローカル SPAN と ER SPAN）をローカル デバイス上に作成できます。

SPAN セッションを作成すると、複数の VLAN 送信元を監視し、必要な VLAN だけを選択して、複数の宛先ポートに送信できます。たとえば、トランク ポートで SPAN を設定し、さまざまな宛先ポート上でのさまざまな VLAN からのトラフィックを監視できます。

図 9-3 では、3 つの VLAN から 3 つの指定された宛先ポートにトラフィックをコピーする VLAN ベースの SPAN 設定を示しています。各宛先ポートで許可する VLAN を選択して、トラフィックの送信を制限できます。図 9-3 では、デバイスは各宛先ポートへ、1 つの VLAN からのパケットを送信します。

（注）　VLAN ベースの SPAN セッションでは、パケットが宛先で必要かどうかに関係なく、すべての送信元パケットがすべての宛先にコピーされます。VLAN トラフィック フィルタリングは、送信宛先ポートで実行されます。

図 9-3　VLAN ベースの SPAN 設定



送信元 VLAN	トラフィックの方向	宛先ポート
10	Rx	E 2/5 E 2/6 E 2/7
11	Rx, Tx	
12	Tx	

186284

Rx は受信
Tx は送信

SPAN 注意事項および制約事項

SPAN に関する設定時の注意事項および制約事項は、次のとおりです。

- 最大 64 の SPAN セッション（ローカル SPAN と ERSPAN）を VSM で設定できます。
- 最大 32 の送信元 VLAN がセッションで許可されます。
- 最大 128 の送信元インターフェイスがセッションで許可されます。

注意　**オーバーロードの可能性**
アップリンク ポートのオーバーロードを回避するために、ERSPAN の設定時、特に送信元 VLAN 設定時には注意が必要です。

- ポートは最大 4 つの SPAN セッションで設定できます。
- 1 つの SPAN セッションで使用される宛先ポートは、別の SPAN セッションの宛先ポートとしても使用できません。
- 1 つのポートを送信元ポートと宛先ポートの両方に設定できません。
- SPAN セッションに複数の出力側送信元ポートが含まれている場合、これらのポートが受信するパケットは、そのポートで送信しない場合でも複製される可能性があります。送信元ポートでこの動作が生じる例の一部を示します。
  - フラッディングから生じたトラフィック
  - ブロードキャストおよびマルチキャスト トラフィック

- 送受信の両方が設定された同じ VLAN でスイッチされる VLAN SPAN セッションの場合、宛先ポートから 2 つのパケット（受信から 1 つ、送信から 1 つ）が転送されます。

SPAN の設定

この項では、SPAN を設定する方法を説明し、次の手順が含まれています。

ローカル SPAN セッションの設定

この手順を使用して、SPAN セッションを設定します。

（注）　ERSPAN を設定している場合は、「ERSPAN セッションの設定」の手順（P.9-13）を参照してください。

始める前に

- EXEC モードで CLI にログインします。
- 設定する SPAN セッションの数を確認します。
- 送信元および宛先ポートは、アクセスまたはトランク モードで設定しておきます。詳細については、『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0*』を参照してください。
- 宛先インターフェイスは、スイッチポート トランク モードで設定しておく必要があります。
- デフォルトでは、SPAN セッションはシャット ステートで作成されます。
- 既存の SPAN セッションを作成する場合は、追加の設定がセッションに追加されます。確実にセッションの以前の設定をクリアするには、まず、セッションを削除する必要があります（ステップ 2 の **no monitor session** を参照）。
- この手順には、モニタ コンフィギュレーション モードでの SPAN セッションの作成と、インターフェイス コンフィギュレーション モードでの実行 VLAN の設定が含まれます。

手順の概要

1. **config t**
2. **no monitor session** *session-number*
3. **monitor session** *session-number*
4. **description** *description*
5. **source** {**interface** ***type*** | **vlan**} {*number* | *range*} [**rx** | **tx** | **both**]
6. （任意）ステップ 5 を繰り返して、追加の SPAN 送信元を設定します。

7. （任意）**filter vlan** {*number* | *range*}
8. （任意）ステップ 7 を繰り返して、フィルタリングするすべての送信元 VLAN を設定します。
9. **destination interface** *type* {*number* | *range*}
10. （任意）ステップ 9 を繰り返して、すべての SPAN 宛先ポートを設定します。
11. **no shut**
12. （任意）**exit**
13. （任意）**interface ethernet** *slot*/*port*[-*port*]
14. （任意）**switchport trunk allowed vlan** {*vlan-range* | **add** *vlan-range* | **except** *vlan-range* | **remove** *vlan-range* | **all** | **none**}
15. （任意）ステップ 13 およびステップ 14 を繰り返して、各宛先ポートで許可された VLAN を設定します。
16. （任意）**show interface ethernet** *slot*/*port*[-*port*] **trunk**
17. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no monitor session** *session-number* **例：** `n1000v(config)# no monitor session 3`	指定されたセッションをクリアします。

ステップ 3	**monitor session** *session-number*
	
	例：
	`n1000v(config)# monitor session 3`
	`n1000v(config-monitor)#`
		任意のセッション番号でセッションを作成して、CLI モニタ コンフィギュレーション モードに切り替え、セッションを設定します。

ステップ 4	**description** *description* **例：** `n1000v(config-monitor)# description my_span_session_3`	指定された SPAN セッションの場合は、説明を追加します。 • description：最大 32 文字の英数字 デフォルト = ブランク（no description）

	コマンド	目的

ステップ 5	**source** {**interface** *type* | **vlan**} {*number* | *range*} [**rx** | **tx** | **both**]
	
	例 1：
	`n1000v(config-monitor)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	
	例 2：
	`n1000v(config-monitor)# source interface port-channel 2`
	
	例 3：
	`n1000v(config-monitor)# source interface vethernet 12 both`
	
	例 4：
	`n1000v(config-monitor)# source vlan 3, 6-8 tx`
		指定されたセッションの場合は、監視するトラフィックの送信元と方向を設定します。
		• type：インターフェイス タイプ（イーサネット、ポートチャネル、仮想イーサネット）を指定します。
		• number：監視するインターフェイス スロットおよびポートまたはポート範囲、VLAN 番号または VLAN 範囲を指定します。
		• traffic direction：次の方向のいずれかになるように、トラフィック 監視を指定します。
		– 受信（rx）（VLAN デフォルト）
		– 送信（tx）
		– 双方向（インターフェイス デフォルト）

ステップ 6	（任意）ステップ 5 を繰り返して、追加の SPAN 送信元を設定します。	
ステップ 7	**filter vlan** {*number* | *range*} **例：** `n1000v(config-monitor)# filter vlan 3-5, 7`	（任意）指定された SPAN セッションの場合、送信元 VLAN の中からフィルタを設定します。
ステップ 8	（任意）ステップ 7 を繰り返して、フィルタリングするすべての送信元 VLAN を設定します。	
ステップ 9	**destination interface** *type* {*number* | *range*} **例：** `n1000v(config-monitor)# destination interface ethernet 2/5, ethernet 3/7`	指定された SPAN セッションの場合、コピーされた送信元パケットの宛先として動作するポートを指定します。 • type：インターフェイス タイプ（イーサネットまたは仮想イーサネット）を指定します。 • number：監視するインターフェイス スロットおよびポートを指定します。 • range：監視するインターフェイス範囲を指定します。 **（注）** SPAN 宛先ポートはアクセスまたはトランク ポートとして設定しておく必要があります。
ステップ 10	（任意）ステップ 9 を繰り返して、すべての SPAN 宛先ポートを設定します。	
ステップ 11	**no shut** **例：** `n1000v(config-monitor)# no shut`	SPAN セッションをイネーブルにします。デフォルトでは、セッションはシャット ステートで作成されます。

	コマンド	目的

ステップ 12	**exit**
	
	例：
	`n1000v(config-monitor)# exit`
	`n1000v(config)#`
		（任意）モニタ コンフィギュレーション モードを終了して、CLI コンフィギュレーション モードに切り替えます。

ステップ 13	**interface ethernet** *slot/port*[*-port*]
	
	例：
	`n1000v(config)# interface ethernet 2/5`
	`n1000v(config-if)#`
		（任意）指定されたインターフェイスの CLI インターフェイス コンフィギュレーション モードに切り替えます。

ステップ 14	**switchport trunk allowed vlan** {*vlan-range* | **add** *vlan-range* | **except** *vlan-range* | **remove** *vlan-range* | **all** | **none**} **例：** `n1000v(config-if)# switchport trunk allowed vlan 3-5`	（任意）指定されたインターフェイス用。インターフェイスで許可する VLAN の範囲を設定します。デフォルトでは、インターフェイス上ですべての VLAN が許可されます。 • **vlan-range**：インターフェイスで許可する VLAN の範囲を指定します。 • **add vlan-range**：インターフェイスで許可されている既存の VLAN を追加します。 • **except vlan-range**：インターフェイスで許可されている VLAN から VLAN の範囲を除外します。 • **remove vlan-range**：インターフェイスで許可されている VLAN から VLAN の範囲を削除します。 • **all**：インターフェイスですべての VLAN を許可します。 これはデフォルトです。 • **none**：インターフェイスで VLAN を許可しません。
ステップ 15	（任意）ステップ 13 およびステップ 14 を繰り返して、各宛先ポートで許可された VLAN を設定します。	
ステップ 16	**show interface ethernet** *slot/port*[*-port*] **trunk** **例：** `n1000v(config-if)# show interface ethernet 2/5 trunk`	（任意）選択したスロットおよびポートまたはポート範囲に対応するインターフェイス トランキング設定を表示します。
ステップ 17	**copy running-config startup-config** **例：** `n1000v(config-if)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

ERSPAN ポート プロファイルの設定

この手順を使用して、VSM 上のポート プロファイルを設定し、ERSPAN パケットを IP ネットワーク経由で、リモート宛先アナライザに 転送します。

始める前に

- EXEC モードで CLI にログインします。
- vCenter Server のすべてのホストに対して、この設定を完了する必要があります。
- このポート プロファイルに使用する名前を確認します。

（注）　ポート プロファイル名は、各 ESX ホストで必要な VMKNIC を設定するために使用されます。

- このプロファイルをマッピングする VMware ポート グループ名を確認します。
- 新しい仮想アダプタを追加するための VMware マニュアルを手元に用意します。
- この設定で使用するシステム VLAN の ID を確認します。

手順の概要

1. **config t**
1. **port-profile** *port_profile_name*
2. **capability l3control**
3. **vmware port-group** *pg_name*
4. **switchport access vlan** *vlan_id*
5. **no shutdown**
6. **system vlan** *vlan_id*
7. **state enabled**
8. （任意）**show port-profile name** *port_profile_name*
9. （任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**port-profile** *port_profile_name*
	
	例：
	`n1000v(config)# port-profile erspan_profile`
	`n1000v(config-port-prof)#`
		ポート プロファイルを作成し、指定されたポート プロファイルの CLI グローバル コンフィギュレーション モードに切り替えます。実行コンフィギュレーションに、ポート プロファイルを保存します。
		port-profile name は、最大 80 文字で、Cisco Nexus 1000V の各ポート プロファイルで一意でなければなりません。

ステップ 3	**capability l3control**
	
	例：
	`n1000v(config-port-prof)# capability l3control`
	`n1000v(config-port-prof)#`
		port-profile を設定して、ERSPAN トラフィックを転送し、実行コンフィギュレーションに保存します。

ステップ 4	**vmware port-group** *pg_name*
	
	例：
	`n1000v(config-port-prof)#vmware port-group erspan`
	`n1000v(config-port-prof)#`
		ポート プロファイルを VMware ポート グループとして指定し、このプロファイルがマッピングする VMware ポート グループ名を追加します。実行コンフィギュレーションに、設定を保存します。
		ポート プロファイルは、同じ名前の VMware ポート グループにマッピングされます。vCenter Server 接続が確立すると、Cisco Nexus 1000V で作成されたポート グループは、vCenter Server の仮想スイッチに配信されます。
		• **pg-name**：ポート グループ名。pg-name を指定しない場合、ポート グループ名は、ポート プロファイル名と同じになります。ポート プロファイルを異なるポート グループ名にマッピングする場合は、pg-name オプションのあとに別の名前を続けます。

ステップ 5	**switchport access vlan** *vlan_id*
	
	例 1：
	`n1000v(config-port-prof)# switchport access vlan 2`
	`n1000v(config-port-prof)#`
		VLAN ID をこのポート プロファイルのアクセス ポートに割り当て、実行コンフィギュレーションに設定を保存します。

ステップ 6	**no shutdown**
	
	例：
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		実行コンフィギュレーションのインターフェイスをイネーブルにします。

	コマンド	目的

ステップ 7	**system vlan** *vlan_id*
	
	例：
	`n1000v(config-port-prof)# system vlan 2`
	`n1000v(config-port-prof)#`
		システム VLAN ID をポート プロファイルに関連付け、実行コンフィギュレーションに保存します。
		アクセス ポートに割り当てられた VLAN ID と一致しなければなりません。一致しない場合は、次のエラー メッセージが表示されます。
		ERROR: System vlan being set does not match the switchport access vlan 2

ステップ 8	**state enabled**
	
	例：
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		実行コンフィギュレーションで、ポート プロファイルをイネーブルにします。
		これで、このポート プロファイルは、ERSPAN 送信元を持つすべての ESX ホストの ERSPAN パケットを送信できます。

ステップ 9	**show port-profile name** *port_profile_name*
	
	例：
	`n1000v(config-port-prof)# show port-profile name erspan`
	`port-profile erspan`
	`  description:`
	`  status: enabled`
	`  capability uplink: no`
	`  capability l3control: yes`
	`  system vlans: 2`
	`  port-group: access`
	`  max-ports: 32`
	`  inherit:`
	`  config attributes:`
	`  switchport access vlan 2`
	`  no shutdown`
	`  evaluated config attributes:`
	`  switchport access vlan 2`
	`  no shutdown`
	`  assigned interfaces:`
	
	`n1000v(config-port-prof)#`
		（任意）指定されたポート プロファイルの設定を、実行コンフィギュレーションにあるとおりに表示します。

ステップ 10	**copy running-config startup-config**
	
	例：
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################]`
	`100%`
	`n1000v(config-port-prof)#`
		（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

ステップ 11	VMware のマニュアルを参照して、vSphere Client クライアントで、各 ESX ホストの VMKNIC を設定します。必ず**新しい仮想アダプタ**として、VMKNIC がこのポート プロファイルを参照するようにします。	

ERSPAN セッションの設定

この手順を使用して、ERSPAN セッションを設定します。

（注）　ローカル SPAN を設定している場合は、「ローカル SPAN セッションの設定」の手順（P.9-6）を参照してください。

始める前に

- EXEC モードで CLI にログインします。
- 設定する SPAN セッションの数を確認します。
- 「ERSPAN ポート プロファイルの設定」の手順（P.9-10）を参照して、VSM の ERSPAN 対応ポート プロファイルを設定しておきます。
- 新しい仮想アダプタを追加するための VMware マニュアルを使用して、各 ESX ホスト上に必要な VMKNIC を設定しておきます。
- デフォルトでは、SPAN セッションはシャット ステートで作成されます。
- 既存の SPAN セッションを作成する場合は、追加の設定がセッションに追加されます。確実にセッションの以前の設定をクリアするには、まず、セッションを削除する必要があります（ステップ 2 の **no monitor session** を参照）。
- この手順には、ERSPAN 送信元コンフィギュレーション モードでの SPAN セッションの作成と、インターフェイス コンフィギュレーション モードでの実行 VLAN の設定が含まれます。

手順の概要

1. **config t**
2. **no monitor session** *session-number*
3. **monitor session** *session-number* **type erspan-source**
4. **description** *description*
5. **source** {**interface** ***type*** | **vlan**} {*number* | *range*} [**rx** | **tx** | **both**]
6. （任意）ステップ 5 を繰り返して、追加の ERSPAN 送信元を設定します。
7. （任意）**filter vlan** {*number* | *range*}
8. （任意）ステップ 7 を繰り返して、フィルタリングするすべての送信元 VLAN を設定します。
9. **destination ip** *ip_address*
10. **ip ttl** *ttl_value*
11. **ip prec** *ipp_value*
12. **ip dscp** *dscp_value*
13. **mtu** *mtu_value*
14. （任意）ステップ 9 からステップ 13 まで繰り返して、すべての ERSPAN 宛先を設定します。
15. （任意）**erspan-id flow_id**
16. **no shut**
17. （任意）**show monitor session session_id**
18. （任意）**exit**

19.（任意）**copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no monitor session** *session-number* **例：** `n1000v(config)# no monitor session 3`	指定されたセッションをクリアします。

ステップ 3	**monitor session** *session-number* **type erspan-source**
	
	例：
	`n1000v(config)# monitor session 3 type erspan`
	`n1000v(config-erspan-src)#`
		任意のセッション番号でセッションを作成し、CLI ERSPAN 送信元コンフィギュレーション モードに切り替えます。この設定は、実行コンフィギュレーションに保存されます。

ステップ 4	**description** *description*
	
	例：
	`n1000v(config-erspan-src)# description my_erspan_session_3`
	`n1000v(config-erspan-src)#`
		指定された ERSPAN セッションの場合、説明を追加して、実行コンフィギュレーションに保存します。
		• description：最大 32 文字の英数字
		デフォルト = ブランク（no description）

ステップ 5	**source** {**interface** *type* | **vlan**} {*number* | *range*} [**rx** | **tx** | **both**]
	
	例 1：
	`n1000v(config-erspan-src)# source interface ethernet 2/1-3, ethernet 3/1 rx`
	
	例 2：
	`n1000v(config-erspan-src)# source interface port-channel 2`
	
	例 3：
	`n1000v(config-erspan-src)# source interface vethernet 12 both`
	
	例 4：
	`n1000v(config-erspan-src)# source vlan 3, 6-8 tx`
		指定されたセッションの場合、監視する送信元とトラフィックの方向を設定し、実行コンフィギュレーションに保存します。
		• type：インターフェイス タイプ（イーサネット、ポートチャネル、仮想イーサネット）を指定します。
		• number：監視するインターフェイス スロットおよびポートまたはポート範囲、VLAN 番号または VLAN 範囲を指定します。
		• traffic direction：次の方向のいずれかになるように、トラフィック 監視を指定します。
		– 受信（rx）（VLAN デフォルト）
		– 送信（tx）
		– 双方向（インターフェイス デフォルト）

ステップ 6	（任意）ステップ 5 を繰り返して、追加の ERSPAN 送信元を設定します。	

	コマンド	目的
ステップ 7	**filter vlan** {*number* | *range*} **例：** `n1000v(config-erspan-src)# filter vlan 3-5, 7`	（任意）指定された ERSPAN セッションの場合、監視する VLAN、VLAN リスト、VLAN 範囲のいずれかを設定して、実行コンフィギュレーションに保存します。 モニタ ポート上では、VLAN フィルタ リストと一致する VLAN からのトラフィックだけが宛先に複製されます。
ステップ 8	（任意）ステップ 7 を繰り返して、フィルタリングするすべての送信元 VLAN を設定します。	

ステップ 9	**destination ip** *ip_address*
	
	例：
	`n1000v(config-erspan-src)# destination interface ethernet 2/5, ethernet 3/7`
	`n1000v(config-monitor-erspan-src)#`
		カプセル化されたトラフィックが送信されるホストの IP アドレスを設定し、実行コンフィギュレーションに保存します。

ステップ 10	**ip ttl** *ttl_value*
	
	例：
	`n1000v(config-monitor-erspan-src)# ip ttl 64`
	`n1000v(config-monitor-erspan-src)#`
		（任意）ERSPAN のパケットに対し、1 ～ 255 の範囲で IP 有効期限値を指定し、実行コンフィギュレーションに保存します。

ステップ 11	**ip prec** *precedence_value*
	
	例：
	`n1000v(config-monitor-erspan-src)# ip prec 1`
	`n1000v(config-monitor-erspan-src)#`
		（任意）ERSPAN のパケットに対し、0 ～ 7 の範囲で IP precedence 値を指定し、実行コンフィギュレーションに保存します。

ステップ 12	**ip dscp** *dscp_value*
	
	例：
	`n1000v(config-monitor-erspan-src)# ip dscp 24`
	`n1000v(config-monitor-erspan-src)#`
		（任意）0 ～ 63 の範囲で IP DSCP 値を指定します。ERSPAN トラフィックのパケットの場合は、実行コンフィギュレーションに保存します。

ステップ 13	**mtu** *mtu_value*
	
	例：
	`n1000v(config-monitor-erspan-src)# mtu 1000`
	`n1000v(config-monitor-erspan-src)#`
		（任意）ERSPAN トラフィックの MTU サイズを指定し、実行コンフィギュレーションに保存します。

ステップ 14	（任意）ステップ 9 からステップ 13 までを繰り返して、すべての SPAN 宛先ポートを設定します。	
ステップ 15	**erspan-id** *flow_id* **例：** `n1000v(config-erspan-src)# erspan_id 51`	ERSPAN ID（1 ～ 1023）をセッション設定に追加して、実行コンフィギュレーションに保存します。 セッション ERSPAN ID を、カプセル化されたフレームの ERSPAN ヘッダーに追加し、終端ボックスで使用して、さまざまな トラフィックの ERSPAN ストリームを識別できます。

	コマンド	目的
ステップ 16	**no shut** **例：** `n1000v(config-erspan-src)# no shut`	ERSPAN セッションをイネーブルにし、実行コンフィギュレーションに保存します。 デフォルトでは、セッションはシャット ステートで作成されます。
ステップ 17	**show monitor session** *session_id* **例：** `n1000v(config-erspan-src)# show monitor session 3`	（任意）実行コンフィギュレーションにあるとおりに、ERSPAN セッション設定を表示します。

ステップ 18	**exit**
	
	例：
	`n1000v(config-erspan-src)# exit`
	`n1000v(config)#`
		（任意）ERSPAN 送信元コンフィギュレーション モードを終了し、CLI コンフィギュレーション モードに戻ります。

ステップ 19	**copy running-config startup-config** **例：** `n1000v(config-if)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

SPAN セッションのシャットダウン

この手順を使用して、SPAN セッションのパケットのコピーを中止します。1 つの送信元および宛先からのパケットのコピーを中止し、別の送信元および宛先で再開できます。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- EXEC モードで CLI にログインします。
- シャットダウンする SPAN セッションを確認します。
- グローバル コンフィギュレーション モードまたはモニタ コンフィギュレーション モードで、SPAN セッションをシャットダウンできます。

手順の概要

グローバル コンフィギュレーション モードから：

1. **config t**
2. **monitor session** {*session-number* | *session-range* | **all**} **shut**
3. **show monitor**
4. **copy running-config startup-config**

モニタ コンフィギュレーション モードから：

1. **config t**
2. **monitor session** {*session-number* | *session-range* | **all**}
3. **shut**
4. **show monitor**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**monitor session** {*session-number* | *session-range* | **all**} **shut**
	
	例：
	`n1000v(config)# monitor session 3 shut`
	`n1000v(config)#`
	
	例：
	`n1000v(config)# monitor session 3`
	`n1000v(config-monitor)# shut`
		グローバル コンフィギュレーション モードまたはモニタ コンフィギュレーション モードで、指定された SPAN モニタ セッションをシャットダウンします。
		• session-number：特定の SPAN セッション番号を指定します。
		• session range：SPAN セッションの範囲を指定します（許可されている範囲は 1 ～ 16）。
		• all：すべての SPAN モニタ セッションを指定します。

ステップ 3	**show monitor** **例：** `n1000v(config-monitor)# show monitor`	（任意）SPAN セッションの状況を表示します。
ステップ 4	**copy running-config startup-config** **例：** `n1000v(config-monitor)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

SPAN セッションの再開

この手順を使用して、SPAN セッションのパケットのコピーを再開します。1 つの送信元および宛先からのパケットのコピーを中止し、別の送信元および宛先で再開できます。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- EXEC モードで CLI にログインします。
- 設定する SPAN セッションを確認します。
- グローバル コンフィギュレーション モードまたはモニタ コンフィギュレーション モードで、SPAN セッションを再開できます。

手順の概要

グローバル コンフィギュレーション モードから：

1. **config t**
2. **no monitor session** {*session-number* | *session-range* | **all**} **shut**
3. **show monitor**
4. **copy running-config startup-config**

モニタ コンフィギュレーション モードから：

1. **config t**
2. **monitor session** {*session-number* | *session-range* | **all**}
3. **no shut**
4. **show monitor**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] monitor session** {*session-number* *session-range* | **all**} **shut**
	
	例：
	`n1000v(config)# no monitor session 3 shut`
	`n1000v(config)#`
	
	例：
	`n1000v(config)# monitor session 3`
	`n1000v(config-monitor)# no shut`
		グローバル コンフィギュレーション モードまたはモニタ コンフィギュレーション モードで、指定された SPAN モニタ セッションを開始します。
		• session-number：特定の SPAN セッション番号を指定します。
		• session range：SPAN セッションの範囲を指定します（許可されている範囲は 1 ～ 16）。
		• all：すべての SPAN モニタ セッションを指定します。

ステップ 3	**show monitor** **例：** `n1000v(config-monitor)# show monitor`	（任意）SPAN セッションの状況を表示します。
ステップ 4	**copy running-config startup-config** **例：** `n1000v(config-monitor)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

SPAN の設定確認

SPAN 設定を表示するには、次のコマンドを使用します。

コマンド	目的
show monitor session {**all** | *session-number* | **range** *session-range*} [**brief**]	SPAN セッションの設定を表示します。
show monitor	イーサネット SPAN 情報を表示します。
module vem module-number execute vemcmd show span //	VEM モジュールで設定された SPAN セッションを表示します。
show port-profile name *port_profile_name*	ERSPAN で必要なレイヤ 3 対応ポート プロファイルを表示します。

設定例

この項には、次の設定例が含まれています。

SPAN セッションの設定例

SPAN セッションを設定する手順は、次のとおりです。

ステップ 1　アクセス モードまたはトランク モードで宛先ポートを設定し、SPAN モニタリングをイネーブルにします。

```
n1000v# config t
  n1000v(config)# interface ethernet 2/5
    n1000v(config-if)# switchport
    n1000v(config-if)# switchport mode trunk
    n1000v(config-if)# no shut
    n1000v(config-if)# exit
  n1000v(config)#
```

ステップ 2　SPAN セッションを設定します。

```
  n1000v(config)# no monitor session 3
  n1000v(config)# monitor session 3
    n1000v(config-monitor)# source interface ethernet 2/1-3
    n1000v(config-monitor)# source interface port-channel 2
    n1000v(config-monitor)# source vlan 3, 6-8 tx
    n1000v(config-monitor)# filter vlan 3-5, 7
    n1000v(config-monitor)# destination interface ethernet 2/5
    n1000v(config-monitor)# no shut
    n1000v(config-monitor)# exit
  n1000v(config)# show monitor session 3
  n1000v(config)# copy running-config startup-config
```

ERSPAN セッションの設定例

次の例では、送信元イーサネット インターフェイスと宛先 IP アドレスに対して、双方向 ERSPAN セッションを作成する方法を示しています。宛先 IP に到達するパケットは、ヘッダーの ID 999 で特定されます。

```
n1000v(config)# monitor session 1 type erspan-source
n1000v(config-erspan-src)# source interface ethernet 3/3
n1000v(config-erspan-src)# destination ip 10.54.54.1
n1000v(config-erspan-src)# erspan-id 999
n1000v(config-erspan-src)# mtu 1000
n1000v(config-erspan-src)# no shut

n1000v(config)# show monitor session 1
   session 1
---------------
type              : erspan-source
state             : up
source intf       :
```

```
    rx            : Eth3/3
    tx            : Eth3/3
    both          : Eth3/3
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
destination IP    : 10.54.54.1
ERSPAN ID         : 999
ERSPAN TTL        : 64
ERSPAN IP Prec.   : 0
ERSPAN DSCP       : 0
ERSPAN MTU        : 1000

n1000v# module vem 3 execute vemcmd show span

VEM SOURCE IP: 10.54.54.10

HW SSN ID            DST LTL/IP    ERSPAN ID
        0            10.54.54.1          999
        1                    48        local
```

その他の関連資料

SPAN の実装に関する詳細情報については、次の項を参照してください。

- 「関連資料」（P.9-21）
- 「標準規格」（P.9-21）

関連資料

関連項目	マニュアル タイトル
ポート プロファイル設定	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0*』
インターフェイス	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0*』
SPAN コマンド	『*Cisco Nexus 1000V Command Reference, Release 4.0*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

その他の関連資料

CHAPTER 10

SNMP の設定

この章では、ユーザ、メッセージ暗号化、通知、TCP での認証などを含む SNMP を設定する方法を説明します。

ここでは、次の内容について説明します。

SNMP に関する情報

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）は、SNMP マネージャとエージェント間の通信用メッセージ フォーマットを提供する、アプリケーションレイヤ プロトコルです。SNMP はネットワーク デバイスの監視や管理に使用される、標準化されたフレームワークと共通言語を提供します。

ここでは、次の内容について説明します。

SNMP 機能の概要

SNMP フレームワークは、3 つの部分からなります。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスの動作を制御および監視するためのシステム。

- SNMP エージェント：管理デバイス内部のソフトウェア コンポーネントで、デバイスに関するデータを維持し、必要に応じてこれらのデータを管理システムに伝えます。Cisco Nexus 1000V はエージェントと MIB をサポートします。SNMP エージェントをイネーブルにするには、マネージャとエージェント間の関係を定義する必要があります。
- Managed Information Base（MIB; 管理情報ベース）：SNMP エージェント上の管理対象オブジェクトのコレクション。

SNMP は RFC 3411 ～ 3418 で定義されています。

（注）　SNMP セットはサポートされていません。

SNMPv1、SNMPv2c、および SNMPv3 です。SNMPv1 および SNMPv2c の両方により、コミュニティベースのセキュリティ形式の使用がサポートされています。

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を作成できるということです。これらの通知は、SNMP マネージャからの要求送信を必要としません。通知によって、不正なユーザ認証、再起動、接続の終了、ネイバー ルータとの接続切断、またはその他の重要イベントを示すことができます。

SNMP 通知は、トラップまたは応答要求として生成されます。トラップは、エージェントからホスト レシーバー テーブルで指定された SNMP マネージャに送信される、非同期の非確認応答メッセージです。応答要求は、SNMP エージェントから SNMP マネージャに送信される非同期メッセージで、マネージャは受信したという確認応答が必要です。

トラップの信頼性は、応答要求よりも低くなります。これは、SNMP マネージャがトラップを受信するときには、確認応答を送信しないためです。Cisco Nexus 1000V では、トラップを受信したかどうかを判断できません。応答要求を受信した場合、SNMP マネージャは SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）を使用して、メッセージを確認します。応答がなかった場合、Cisco Nexus 1000V はもう一度、応答要求を送信します。

複数のホスト レシーバーに通知を送信するように、Cisco Nexus 1000V を設定できます。ホスト レシーバーの詳細については、「SNMP 通知レシーバーの設定」（P.10-8）を参照してください。

SNMPv3

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。SNMPv3 が提供するセキュリティ機能は、次のとおりです。

- メッセージの完全性：パケットが伝送中に改ざんされていないことを保証します。
- 認証：有効な送信元からのメッセージであることを判別します。
- 暗号化：パケット内容のスクランブルによって、不正な送信元で判読できないようにします。

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方を提供します。セキュリティ モデルは、ユーザおよびユーザに与えられている役割に合わせて設定される認証方式です。セキュリティ レベルは、セキュリティ モデル内で許可されるセキュリティ レベルです。セキュリティ モデルとセキュリティ レベルのコンビネーションによって、SNMP パケットを取り扱うときに使用するセキュリティ メカニズムが決まります。

ここでは、次の内容について説明します。

- 「SNMPv1、v2、v3 のセキュリティ モデルおよびセキュリティ レベル」（P.10-3）

SNMPv1、v2、v3 のセキュリティ モデルおよびセキュリティ レベル

セキュリティ レベルによって、SNMP メッセージを開示から保護する必要があるか、メッセージの認証が必要かどうかが決定されます。セキュリティ モデル内に存在する各種セキュリティ レベルは、次のとおりです。

- noAuthNoPriv：認証も暗号化も行わないセキュリティ レベル
- authNoPriv：認証は行うが暗号化は行わないセキュリティ レベル
- authPriv：認証と暗号化の両方を行うセキュリティ レベル

SNMPv1、SNMPv2c、SNMPv3 の 3 つのセキュリティ モデルが利用できます。セキュリティ レベルと組み合わされたセキュリティ モデルによって、SNMP メッセージの処理時に適用されるセキュリティ メカニズムが決まります。

表 10-1 に、セキュリティ モデルとセキュリティ レベルのコンビネーションが何を意味するかを示します。

表 10-1　SNMP セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	動作
v1	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	なし	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	ユーザ名	なし	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	なし	Hash-Based Message Authentication Code（HMAC）Message Digest 5（MD5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）に基づいて認証します。
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC MD5 または HMAC SHA アルゴリズムに基づいて認証します。Cipher Block Chaining（CBC; 暗号ブロック連鎖）DES（DES-56）規格に基づいた認証に加え、Data Encryption Standard（DES; データ暗号規格）56 ビット暗号化を行います。

User-Based Security Model

SNMPv3 User-Based Security Model（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されず、データ シーケンスが悪意なく起こり得る範囲を超えて変更されていないことを保証します。

- メッセージ起点認証：ユーザのために受信したデータの起点として主張されたアイデンティティが確認されていることを保証します。
- メッセージの機密性：不正な個人、エンティティ、またはプロセスに対して、情報が使用可能になったり開示されたりしていないことを保証します。

SNMPv3 は、設定ユーザによる管理操作だけを許可し、SNMP メッセージを暗号化します。

Cisco Nexus 1000V では、SNMPv3 に対応する 2 種類の認証プロトコルを使用します。

- HMAC-MD5-96 認証プロトコル
- HMAC-SHA-96 認証プロトコル

Cisco Nexus 1000V は、SNMPv3 メッセージ暗号化用プライバシー プロトコルの 1 つとして、Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠します。

priv オプションで、SNMP セキュリティ暗号化に DES を使用するか、それとも 128 ビット AES 暗号化を使用するかを選択できます。**priv** オプションと **aes-128** トークンを組み合わせた場合は、このプライバシー パスワードが 128 ビットの AES 鍵を作成するためのものであることを意味します。AES priv パスワードは、8 文字以上の長さにできます。パスフレーズをクリア テキストで指定する場合は、大文字と小文字を区別して、最大 64 文字の英数字を指定できます。ローカライズした鍵を使用する場合は、130 文字まで指定できます。

（注）　外部 AAA（認証、認可、アカウンティング）サーバを使用する SNMPv3 動作の場合は、外部 AAA サーバ上のユーザ コンフィギュレーションで、プライバシー プロトコルとして AES を使用する必要があります。

CLI および SNMP ユーザの同期

SNMPv3 のユーザ管理は、Access Authentication and Accounting（AAA）サーバ レベルで集中させることができます。この集中ユーザ管理によって、Cisco Nexus 1000V の SNMP エージェントは AAA サーバのユーザ認証サービスを活用できます。ユーザ認証が確認されると、SNMP PDU がさらに処理されます。また、ユーザ グループ名の保管に AAA サーバも使用されます。SNMP ではグループ名を使用して、スイッチでローカルに使用できるアクセス/ロール ポリシーを適用します。

ユーザ グループ、ロール、またはパスワードの設定を変更すると、SNMP と AAA の両方について、データベースの同期が図られます。

Cisco Nexus 1000V では次のように、ユーザ設定を同期させます。

- **snmp-server user** コマンドで指定された認証パスフレーズが CLI ユーザのパスワードになります
- **username** コマンドで指定されたパスワードが SNMP ユーザの認証およびプライバシーパスフレーズになります。
- SNMP または CLI を使用してユーザを削除すると、SNMP と CLI の両方でユーザが削除されます。
- ユーザとロール（役割）間のマッピング変更は、SNMP と CLI で同期します。
- CLI から行ったロール変更（削除または変更）は、SNMP と同期します。

（注）　パスフレーズまたはパスワードをローカライズした鍵または暗号形式で設定した場合、Cisco Nexus 1000V はパスワードを同期させません。

Cisco NX-OS はデフォルトで、同期したユーザ設定を 60 分間維持します。このデフォルト値の変更方法については、「AAA 同期時間の変更」（P.10-14）を参照してください。

グループベースの SNMP アクセス

（注）　グループが業界全体で使用されている標準 SNMP 用語なので、この SNMP の項では、ロールのことをグループと言います。

SNMP のアクセス権は、グループ別に編成されます。SNMP の各グループは、CLI でのロールと同様です。各グループは読み取りアクセス権または読み取りと書き込みアクセス権を指定して定義します。

自分のユーザ名を作成すると、エージェントとの通信を開始し、管理者に自分のロールを設定してもらい、そのロールに自分を追加してもらうことができます。

ハイ アベイラビリティ

SNMP ではステートレス リスタートがサポートされています。リブートまたはスーパーバイザ スイッチオーバー後に、実行コンフィギュレーションを適用します。

SNMP の前提条件

SNMP の前提条件は、次のとおりです。

注意事項および制約事項

SNMP に関する設定時の注意事項および制約事項は、次のとおりです。

- 一部の SNMP MIB に対する読み取り専用アクセスがサポートされています。詳細については次の URL にアクセスして、Cisco NX-OS の MIB サポート リストを参照してください。

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

SNMP の設定

ここでは、次の内容について説明します。

- 「SNMP のディセーブル化」（P.10-13）
- 「AAA 同期時間の変更」（P.10-14）

（注）　この機能に対応する Cisco NX-OS コマンドは、Cisco IOS で使用されているコマンドと異なる場合があるので注意してください。

SNMP ユーザの設定

この手順を使用して、SNMP のユーザを設定します。

始める前に

- EXEC モードで CLI にログインします。

手順の概要

1. **config t**
2. **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]
3. **show snmp user**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`switch(config)#`
		グローバル コンフィギュレーション モードに切り替えます。

ステップ 2	**snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]] **例：** `switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh`	認証およびプライバシー パラメータを指定して、SNMP ユーザを設定します。パスフレーズには最大 64 文字の英数字を使用できます。大文字と小文字を区別します。**localizekey** キーワードを使用する場合は、パスフレーズに大文字と小文字を区別した英数字を 130 文字まで使用できます。 engineID の形式は、12 桁のコロンで区切った 10 進数字です。

	コマンド	目的
ステップ 3	**show snmp user** **例：** `switch(config-callhome)# show snmp user`	（任意）1 つ以上の SNMP ユーザに関する情報を表示します。
ステップ 4	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

SNMP のコンタクトおよびロケーション情報を設定する例を示します。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

SNMP メッセージ暗号化の強制

着信要求の認証または暗号化を求めるように、SNMP を設定できます。デフォルトでは、SNMP エージェントは認証および暗号化を行わないでも SNMPv3 メッセージを受け付けます。プライバシーを強化する場合、Cisco Nexus 1000V は noAuthoNoPriv または authNoPriv の securityLevel パラメータを使用している SNMPv3 PDU 要求に、authorizationError で応答します。

SNMP メッセージの暗号化をユーザに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server user *name* **enforcePriv** **例：** `switch(config)# snmp-server user Admin enforcePriv`	このユーザに SNMP メッセージの暗号化を強制します。

SNMP メッセージの暗号化をすべてのユーザに強制するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server globalEnforcePriv **例：** `switch(config)# snmp-server globalEnforcePriv`	すべてのユーザに SNMP メッセージの暗号化を強制します。

複数のロールへの SNMPv3 ユーザの割り当て

SNMP ユーザの設定後、ユーザに複数のロールを割り当てることができます。

（注）　他のユーザにロールを割り当てることができるのは、network-admin ロールに属しているユーザだけです。

SNMP ユーザにロールを割り当てるには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server user *name group* **例：** `switch(config)# snmp-server user Admin superuser`	この SNMP ユーザを設定済みのユーザ ルールに関連付けます。

SNMP コミュニティの作成

SNMPv1 または SNMPv2c に対応する SNMP コミュニティを作成できます。

SNMP コミュニティ ストリングを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server community *name group* {**ro** | **rw**} **例：** `switch(config)# snmp-server community public ro`	SNMP コミュニティ ストリングを作成します。

SNMP 通知レシーバーの設定

複数のホスト レシーバーに対して SNMP 通知を作成するように、Cisco Nexus 1000V を設定できます。

SNMPv1 トラップのホスト レシーバーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server host *ip-address* **traps version 1** *community* [**udp_port** *number*] **例：** `switch(config)# snmp-server host 192.0.2.1 traps version 1 public`	SNMPv1 トラップのホスト レシーバーを設定します。コミュニティには最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

SNMPv2c トラップまたは応答要求のホスト レシーバーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server host *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*] **例：** `switch(config)# snmp-server host 192.0.2.1 informs version 2c public`	SNMPv2c トラップまたは応答要求のホスト レシーバーを設定します。コミュニティには最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

SNMPv3 トラップまたは応答要求のホスト レシーバーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server host *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*] **例：** `switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS`	SNMPv2c トラップまたは応答要求のホスト レシーバーを設定します。ユーザ名には最大 255 の英数字を使用できます。UDP ポート番号の範囲は 0 ～ 65535 です。

（注） SNMP マネージャは SNMPv3 メッセージを認証して解読するために、Cisco Nexus 1000V デバイスの SNMP engineID に基づいてユーザ クレデンシャル（authKey/PrivKey）を調べる必要があります。

通知ターゲット ユーザの設定

通知ホスト レシーバーに SNMPv3 応答要求通知を送信するには、デバイス上で通知ターゲット ユーザを設定する必要があります。

Cisco Nexus 1000V は通知ターゲット ユーザのクレデンシャルを使用して、設定された通知ホスト レシーバーへの SNMPv3 応答要求通知メッセージを暗号化します。

（注） 受信した INFORM PDU を認証して解読する場合、Cisco Nexus 1000V で設定されているのと同じ、応答要求を認証して解読するユーザ クレデンシャルが通知ホスト レシーバーに必要です。

通知ターゲット ユーザを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server user *name* [**auth** {md5 | sha} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] **例：** `switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03`	通知ホスト レシーバーの engineID を指定して、通知ターゲット ユーザを設定します。engineID の形式は、12 桁のコロンで区切った 10 進数字です。

SNMP 通知のイネーブル化

通知をイネーブルまたはディセーブルにできます。通知の名前を指定しなかった場合、Cisco Nexus 1000V はすべての通知をイネーブルにします。

表 10-2 には、Cisco Nexus 1000V MIB に関する通知をイネーブルにする、CLI コマンドを示します。

（注）　**snmp-server enable traps** コマンドを使用すると、設定されている通知ホスト レシーバーに応じて、トラップおよび応答要求の両方がイネーブルになります。

表 10-2　SNMP 通知のイネーブル化

MIB	関連コマンド
すべての通知	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB	**snmp-server enable traps entity**
CISCO-ENTITY-FRU-CONTROL-MIB	**snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**

ライセンス通知は、デフォルトでイネーブルです。その他の通知はすべて、デフォルトでディセーブルです。

指定した通知をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server enable traps **例：** `switch(config)# snmp-server enable traps`	すべての SNMP 通知をイネーブルにします。
snmp-server enable traps aaa [**server-state-change**] **例：** `switch(config)# snmp-server enable traps aaa`	AAA SNMP 通知をイネーブルにします。
snmp-server enable traps entity [**fru**] **例：** `switch(config)# snmp-server enable traps entity`	ENTITY-MIB SNMP 通知をイネーブルにします。
snmp-server enable traps license **例：** `switch(config)# snmp-server enable traps license`	ライセンス SNMP 通知をイネーブルにします。
snmp-server enable traps link **例：** `switch(config)# snmp-server enable traps link`	リンク SNMP 通知をイネーブルにします。
snmp-server enable traps port-security **例：** `switch(config)# snmp-server enable traps port-security`	ポート セキュリティ SNMP 通知をイネーブルにします。
snmp-server enable traps snmp [**authentication**] **例：** `switch(config)# snmp-server enable traps snmp`	SNMP エージェント通知をイネーブルにします。

インターフェイスに関する linkUp/linkDown 通知のディセーブル化

個々のインターフェイスに関する linkUp および linkDown 通知をディセーブルにできます。これにより、フラッピング インターフェイス（アップとダウン間の移行を繰り返しているインターフェイス）に関する通知を制限できます。

インターフェイスに関する linkUp/linkDown 通知をディセーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no snmp trap link-status **例：** `switch(config-if)# no snmp trap link-status`	インターフェイスの SNMP リンクステート トラップをディセーブルにします。このコマンドは、デフォルトでイネーブルにされています。

TCP による SNMP のワンタイム認証のイネーブル化

TCP セッションでの 1 回限りの SNMP 認証をイネーブルにできます。

TCP による SNMP のワンタイム認証をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server tcp-session [**auth**] **例：** `switch(config)# snmp-server tcp-session`	TCP セッションでの 1 回限りの SNMP 認証をイネーブルにします。デフォルトはディセーブルです。

SNMP スイッチのコンタクトおよびロケーション情報の指定

32 文字までの長さで（スペースを含まない）のスイッチ コンタクト情報を指定できます。さらに、スイッチ ロケーションを指定できます。

始める前に

- EXEC モードで CLI にログインします。

手順の概要

1. **config t**
2. **snmp-server contact** *name*
3. **snmp-server location** *name*
4. **show snmp**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`switch(config)#`
		グローバル コンフィギュレーション モードに切り替えます。

ステップ 2	**snmp-server contact** *name* **例：** `switch(config)# snmp-server contact Admin`	SNMP コンタクト名として sysContact を設定します。
ステップ 3	**snmp-server location** *name* **例：** `switch(config)# snmp-server location Lab-7`	SNMP ロケーションとして sysLocation を設定します。
ステップ 4	**show snmp** **例：** `switch(config)# show snmp`	（任意）1 つ以上の宛先プロファイルに関する情報を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

SNMP のコンタクトおよびロケーション情報を設定する例を示します。

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp contact Admin
switch(config)# snmp location Lab-7
```

SNMP のディセーブル化

デバイス上で SNMP プロトコルをディセーブルにできます。

SNMP プロトコルをディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
no snmp-server protocol enable **例：** `switch(config)# no snmp-server protocol enable`	SNMP プロトコルをディセーブルにします。このコマンドは、デフォルトでイネーブルにされています。

AAA 同期時間の変更

同期したユーザ設定を Cisco NX-OS に維持させる時間の長さを変更できます。

AAA 同期時間を変更するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server aaa-user cache-timeout *seconds* **例：** `switch(config)# snmp-server aaa-user cache-timeout 1200.`	ローカル キャッシュで AAA 同期ユーザ設定を維持する時間を設定します。値の範囲は 1 ～ 86400 秒です。デフォルト値は 3600 です。

SNMP の設定確認

SNMP 設定を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config snmp [**all**]	SNMP の実行コンフィギュレーションを表示します。
show snmp	SNMP ステータスを表示します。
show snmp community	SNMP コミュニティ ストリングを表示します。
show snmp context	SNMP コンテキスト マッピングを表示します。
show snmp engineID	SNMP engineID を表示します。
show snmp group	SNMP ロールを表示します。
show snmp session	SNMP セッションを表示します。
show snmp trap	SNMP 通知がイネーブルなのかディセーブルなのかを表示します。
show snmp user	SNMPv3 ユーザを表示します。

SNMP の設定例

Blue VRF を使用してある通知ホスト レシーバーに Cisco linkUp/linkDown 通知を送信するように設定し、Admin と NMS という 2 つの SNMP ユーザを定義する例を示します。

```
config t
 snmp-server contact Admin@company.com
 snmp-server user Admin auth sha abcd1234 priv abcdefgh
 snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:22:32:15:10:03
 snmp-server host 192.0.2.1 informs version 3 auth NMS
 snmp-server host 192.0.2.1 use-vrf Blue
 snmp-server enable traps link cisco
```

デフォルト設定

表 10-3 に、SNMP パラメータのデフォルト設定をリスト表示します。

表 10-3　デフォルトの SNMP パラメータ

パラメータ	デフォルト
license notifications	イネーブル

その他の関連資料

SNMP の実装に関連する詳細情報については、次の項を参照してください。

- 「標準規格」（P.10-15）
- 「MIB」（P.10-15）

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

MIB

MIB	MIB のリンク
• SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • SNMPv2-MIB	MIB を見つけてダウンロードするには、次の URL を参照してください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

SNMP 機能の履歴

表 10-4 に、この機能のリリース履歴をリスト表示します。

表 10-4　SNMP 機能の履歴

機能名	リリース	機能情報
SNMP	4.0	初回 Cisco Nexus 1000V 製品リリース

CHAPTER 11

NetFlow の設定

この章では、NetFlow を設定して、送信元、トラフィック宛先、タイミング、アプリケーション情報に基づいて、IP トラフィックを特徴付けます。これによって、仮想スイッチを通過するトラフィックを可視化します。この情報を使用して、ネットワーク可用性とパフォーマンスを評価し、規制要件（コンプライアンス）を満たすことができます。また、トラブルシューティングを支援することもできます。

ここでは、次の内容について説明します。

NetFlow 情報

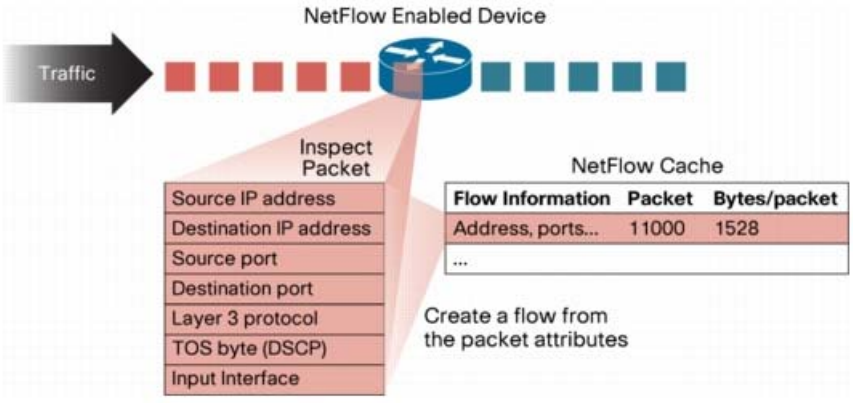
NetFlow は IP トラフィックを評価し、IP トラフィックがフローする方法と場所を把握できます。NetFlow は、アカウンティング、ネットワーク モニタリング、およびネットワーク プランニングで使用できる情報を収集します。

ここでは、次の内容について説明します。

フローとは何か

フローとは、送信元インターフェイス（またはサブインターフェイス）に到着する一方向のパケット ストリームであり、一連の条件と一致します。同じ送信元/宛先 IP アドレス、送信元/宛先ポート、プロトコル インターフェイス、サービス クラスを持つすべてのパケットは、フローにグループ化され、パケットとバイト数が計算されます。これにより、大量のネットワーク情報が、NetFlow キャッシュと呼ばれるデータベースに集約されます。

図 11-1　NetFlow キャッシュでのフローの作成



NetFlow が収集する条件を定義して、フローを作成できます。フローは NetFlow キャッシュに格納されます。

フロー情報には次の内容が含まれます。

- 送信元アドレスは、トラフィックを送信したユーザを示します。
- 宛先アドレスは、トラフィックを受信するユーザを示します。
- ポートはトラフィックを使用するアプリケーションを特定します。
- サービス クラスは、トラフィックのプライオリティを調べます。
- デバイス インターフェイスは、トラフィックがネットワーク デバイスで使用される方法を示します。
- 計算されたパケットとバイト数は、トラフィック量を示します。

フロー レコード定義

フロー レコードは、フロー内のパケットやフローごとに収集されたカウンタのタイプなど、NetFlow が収集する情報を定義します。新しいフロー レコードを定義するか、あらかじめ定義された Cisco Nexus 1000V フロー レコードを使用できます。

レコードを作成するには、「フロー レコードの定義」の手順（P.11-10）を参照してください。

次の表では、フロー レコードで定義される条件を説明します。

フロー レコード条件	説明
Match	フロー レコードのコレクションと一致する情報を定義します。 • **ip**：フロー レコードで収集されるデータは、次の IP オプションのいずれかと一致します。 – protocol – tos（タイプ オブ サービス） • **ipv4**：フロー レコードで収集されるデータは、次の ipv4 アドレス オプションのいずれかと一致します。 – 送信元アドレス – 宛先アドレス • **transport**：フロー レコードで収集されるデータは、次のトランスポート オプションのいずれかと一致します。 – 宛先ポート – 送信元ポート
Collect	フロー レコードが情報を収集する方法を定義します。 • **counter**：次のフォーマットのいずれかで、フロー レコード情報を収集します。 – bytes：32 ビットのカウンタで収集されます（ロングの 64 ビット カウンタが指定されている場合を除く）。 – packets：32 ビットのカウンタで収集されます（ロングの 64 ビット カウンタが指定されている場合を除く）。 • **timestamp sys-uptime**：フローの先頭または最終パケットに関するシステム稼動時間を収集します。 • **transport tcp flags**：フローのパケットの TCP トランスポート レイヤ フラグを収集します。

あらかじめ定義されたフロー レコード

Cisco Nexus 1000V には、次のあらかじめ定義されたフロー レコードが含まれます。

- 「Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow-Original」（P.11-3）
- 「Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow IPv4 Original-Input」（P.11-4）
- 「Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow IPv4 Original-Output」（P.11-5）
- 「Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow IPv4 Protocol-Port」（P.11-5）

例 11-1　Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow-Original

```
n1000v# show flow record netflow-original
Flow record netflow-original:
    Description: Traditional IPv4 input NetFlow with origin ASs
```

```
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
n1000v#
```

（注）　**show flow record** コマンドによる出力結果には、次の行が表示されますが、基になるコマンドは現在 Cisco Nexus 1000V ではサポートされていません。これらのコマンドを使用しても、コンフィギュレーションには影響はありません。

```
collect routing source as
collect routing destination as
collect routing next-hop address ipv4
```

例 11-2　Cisco Nexus 1000V であらかじめ定義されたフロー レコード：Netflow IPv4 Original-Input

```
n1000v# show flow record netflow ipv4 original-input
Flow record ipv4 original-input:
    Description: Traditional IPv4 input NetFlow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
n1000v#
```

例 11-3　Cisco Nexus 1000V であらかじめ定義されたフロー レコード : Netflow IPv4 Original-Output

```
switch# show flow record netflow ipv4 original-output
Flow record ipv4 original-output:
    Description: Traditional IPv4 output NetFlow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 source address
        match ipv4 destination address
        match ip protocol
        match ip tos
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect routing source as
        collect routing destination as
        collect routing next-hop address ipv4
        collect transport tcp flags
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
switch#
```

例 11-4　Cisco Nexus 1000V であらかじめ定義されたフロー レコード : Netflow IPv4 Protocol-Port

```
switch# show flow record netflow ipv4 protocol-port
Flow record ipv4 protocol-port:
    Description: Protocol and Ports aggregation scheme
    No. of users: 0
    Template ID: 0
    Fields:
        match ip protocol
        match transport source-port
        match transport destination-port
        match interface input
        match interface output
        match flow direction
        collect counter bytes
        collect counter packets
        collect timestamp sys-uptime first
        collect timestamp sys-uptime last
switch#
```

NetFlow で生成されるフロー レコードにアクセスする方法

NetFlow データには、主に 2 つの方法を使用してアクセスできます。

- 「コマンドライン インターフェイス（CLI）」（P.11-6）
- 「NetFlow コレクタ」（P.11-7）

コマンドライン インターフェイス（CLI）

現在のネットワーク状態を表示するには、CLI を使用できます。NetFlow CLI はトラブルシューティングの際に非常に有用です。利用可能な show コマンドを表示するには、「NetFlow の設定確認」（P.11-21）を参照してください。

CLI は次のツールを使用して、フロー レコードを取得して、Netflow コレクタにエクスポートします。

- 「フロー モニタ」（P.11-6）
- 「フロー エクスポータ」（P.11-6）

フロー モニタ

フロー モニタは、次の NetFlow コンポーネント間のアソシエーションを作成します。

- フロー レコード：マッチングおよび収集条件から構成されます。
- フロー エクスポータ：エクスポート条件から構成されます。

このフロー モニタ アソシエーションでは、レコードおよびエクスポータから構成されるセットを定義し、それを何度も再利用できます。さまざまなニーズに合わせて、複数のフロー モニタを作成できます。フロー モニタは、特定の方向の、特定のインターフェイスに適用されます。

「フロー モニタの定義」の手順（P.11-16）および「フロー モニタのインターフェイスへの割り当て」の手順（P.11-18）を参照してください。

フロー エクスポータ

フロー エクスポータを使用して、キャッシュから NetFlow コレクタと呼ばれるレポーティング サーバに、フロー レコードが送信される場所と時間を定義します。

エクスポータ定義には、次の内容が含まれます。

- 宛先 IP アドレス
- 送信元インターフェイス
- UDP ポート番号（コレクタが待機するところ）
- エクスポート フォーマット

（注）　NetFlow エクスポート パケットでは、送信元インターフェイスに割り当てられた IP アドレスを使用します。送信元インターフェイスに IP アドレスが割り当てられていない場合、エクスポータはアクティブになりません。

「フロー エクスポータの定義」の手順（P.11-13）を参照してください。

エクスポート フォーマット

Cisco Nexus 1000V は、NetFlow バージョン 9 エクスポート フォーマットをサポートしています。

（注）　Cisco Nexus 1000V は、モニタごとに最大 2 つのエクスポータにデータをエクスポートするトランスポート プロトコルとして、UDP をサポートしています。

NetFlow コレクタ

Cisco Nexus 1000V NetFlow キャッシュから、NetFlow コレクタと呼ばれるレポーティング サーバに、NetFlow をエクスポートできます。NetFlow コレクタは、エクスポートされたフローを再構成し、フローを組み合わせて、トラフィックおよびセキュリティ分析で使用するレポートを生成します。SNMP ポーリングとは異なり、NetFlow エクスポートは定期的に、情報を NetFlow レポーティング コレクタにプッシュします。NetFlow キャッシュには常にフローが入ってきます。Cisco Nexus 1000V はキャッシュ内の終了または期限切れになったフローを検索し、NetFlow コレクタ サーバにエクスポートします。ネットワーク通信が終了すると、フローも終了します。つまり、パケットには、TCP FIN フラグが含まれます。

次は、NetFlow データ レポーティングを実装する手順です。

- NetFlow が収集する情報を定義するように、NetFlow レコードを設定します。
- NetFlow キャッシュへのフロー レコードを取得するように、Netflow モニタを設定します。
- フローをコレクタに送信するように、NetFlow エクスポートを設定します。
- Cisco Nexus 1000V は、NetFlow キャッシュ内の終了したフローを検索し、NetFlow コレクタ サーバにエクスポートします。
- フローは UDP エクスポート パケットで利用可能なスペース、またはエクスポート タイマーに基づいてまとめられます。
- NetFlow コレクタ ソフトウェアは、データからリアルタイムのレポートまたは履歴レポートを作成します。

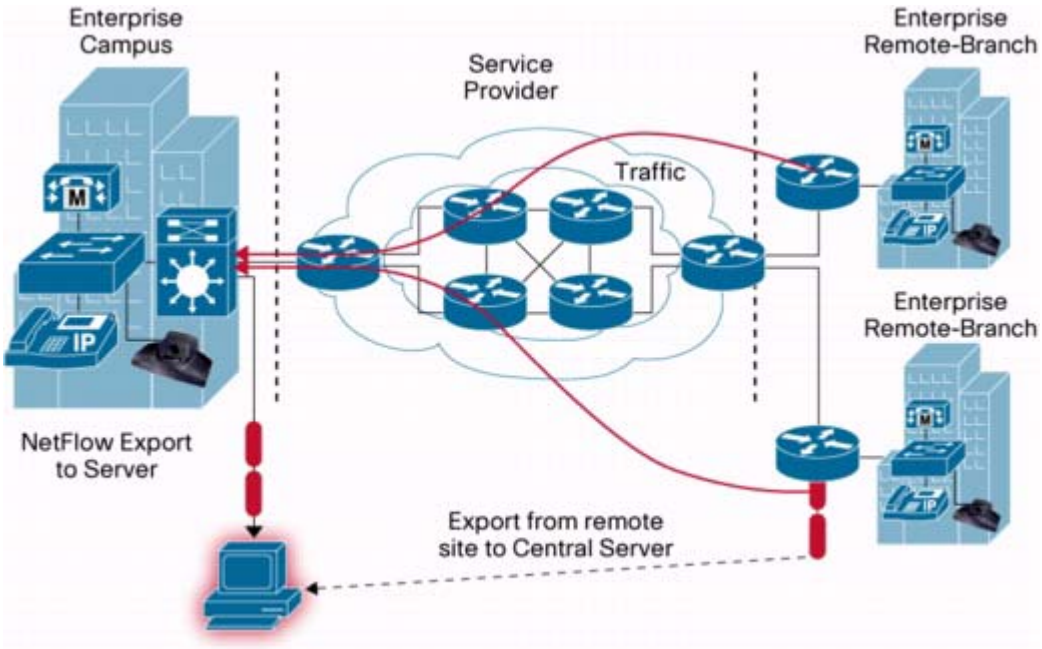
NetFlow コレクタ サーバへのフローのエクスポート

タイマーは、フローが NetFlow コレクタ サーバにエクスポートされるタイミングを判断します。

次のいずれかが発生するときに、フローのエクスポートが可能になります。

- フローが一定時間非アクティブとなり、その間、フローで新しいパケットを受信していない場合。
- 長時間の FTP ダウンロードなど、フローがアクティブなタイマーより長く存在している場合。
- TCP フラグが、フローが終了したことを示している場合。つまり、FIN または RST フラグが表示されている場合です。
- フロー キャッシュが満杯で、一部の古いフローを削除して、新しいフローのための領域を作成する必要がある場合。

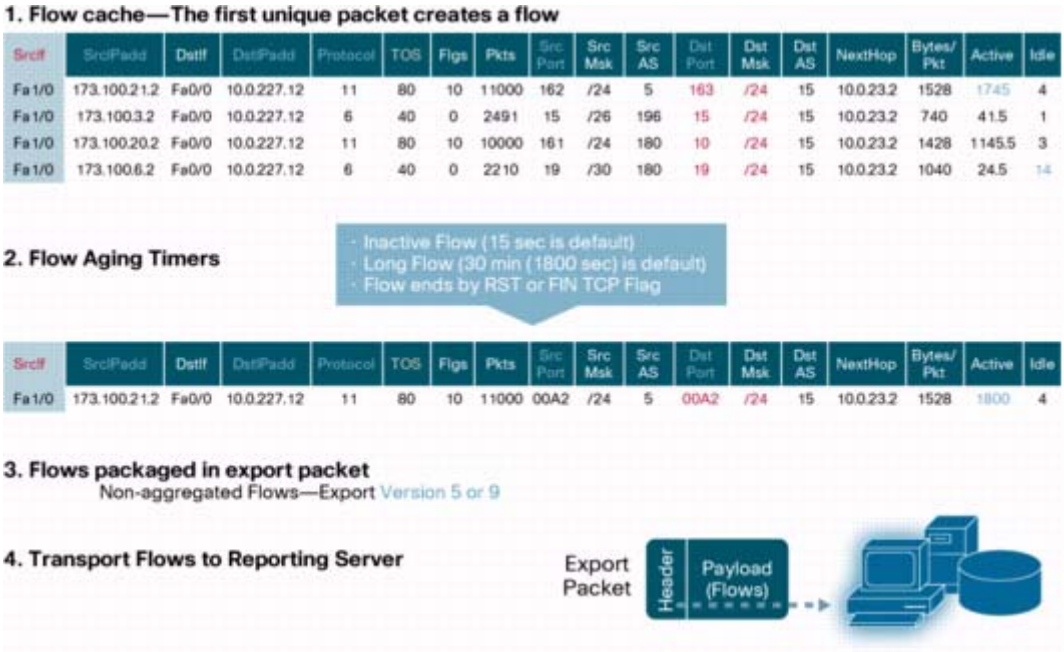
図 11-2　NetFlow コレクタ サーバへのフローのエクスポート



NetFlow データの例

次の図は、NetFlow データの例を示しています。

図 11-3　NetFlow キャッシュの例



ハイ アベイラビリティ

Cisco Nexus 1000V は、NetFlow のステートレス リスタートをサポートします リブートまたはスーパーバイザ スイッチオーバーの後に、Cisco Nexus 1000V は実行コンフィギュレーションを適用します。

NetFlow の前提条件

- NetFlow は追加メモリと CPU リソースを消費するため、リソース要件に注意する必要があります。
- メモリと CPU リソースは、フロー モニタ インターフェイスをホスティングする VEM が提供します。リソースは VEM 上の CPU コアの数によって、制限されています。

設定時の注意事項および制約事項

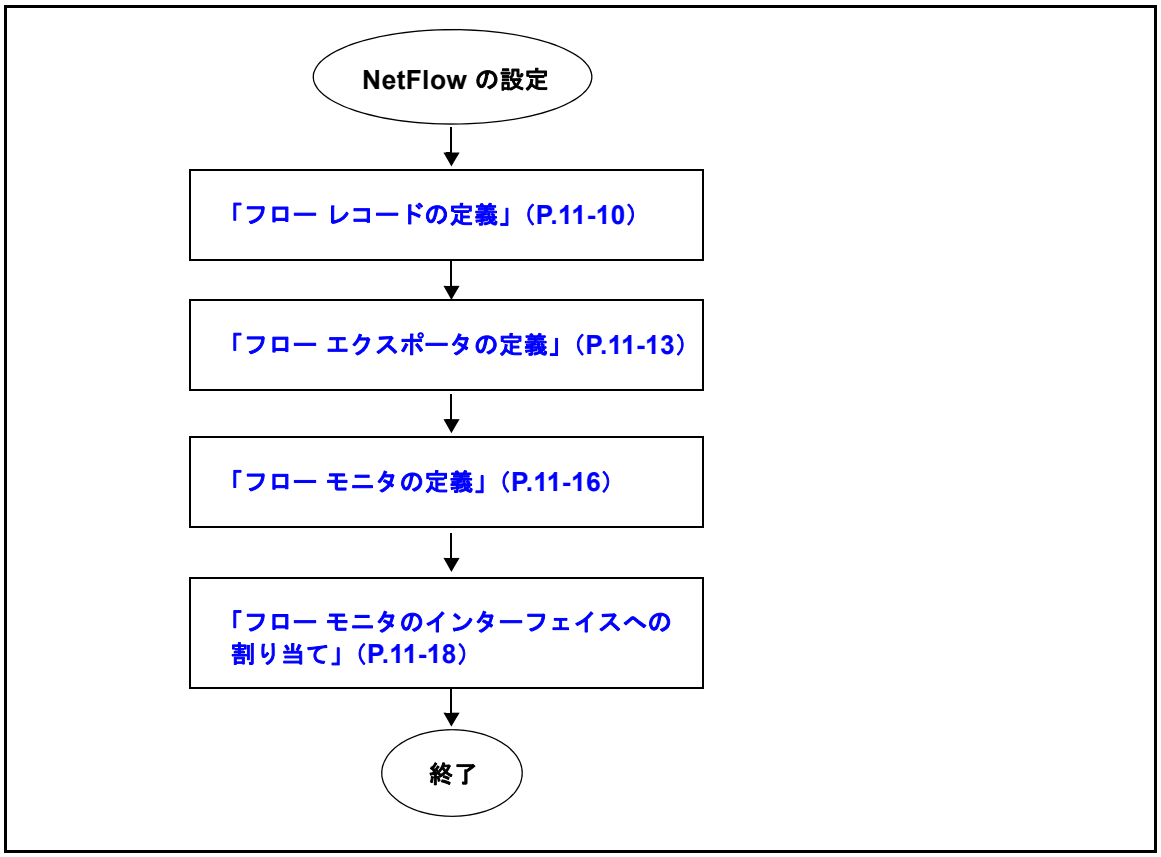
NetFlow に関する設定時の注意事項および制約事項は、次のとおりです。

- 送信元インターフェイスが設定されていない場合、NetFlow エクスポータはディセーブルの状態のままです。
- Cisco Nexus 1000V では、デフォルトで、エクスポータの送信元インターフェイスとして、Mgmt0 インターフェイスが設定されます。必要に応じて、送信元インターフェイスを変更できます。
- Cisco Nexus 1000V には、次のあらかじめ定義されたフロー レコードが含まれているため、新しいフロー レコードを作成する代わりに、これを使用できます。詳細については、「フロー レコード定義」（P.11-2）を参照してください。
  - netflow-original
    Cisco Nexus 1000V のあらかじめ定義された従来の、起点 AS を含む IPv4 入力 NetFlow
  - netflow ipv4 original-input
    Cisco Nexus 1000V のあらかじめ定義された従来の IPv4 入力 NetFlow
  - netflow ipv4 original-output
    Cisco Nexus 1000V のあらかじめ定義された従来の IPv4 出力 NetFlow
  - netflow ipv4 protocol-port
    Cisco Nexus 1000V のあらかじめ定義されたプロトコルおよびポート集約方式
- 最大 1 つのフロー モニタを、各方向の各インターフェイスに対して許可します。
- 最大 2 つのフロー エクスポータを、各モニタに対して許可します。

NetFlow の設定

次のフロー チャートは、NetFlow コンフィギュレーション プロセスを案内するために作成されています。各手順を完了したらこのフロー チャートに戻り、すべての必要な手順を正しい順序で完了したことを確認してください。

フロー チャート：NetFlow の設定



フロー レコードの定義

この手順を使用して、フロー レコードを作成します。

（注）　任意で、「フロー レコード定義」（P.11-2）で説明されている Cisco Nexus 1000V のあらかじめ定義されたレコードを使用できます。「フロー モニタの定義」（P.11-16）を参照して、あらかじめ定義されたレコードを、フロー モニタに適用します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- このフロー レコードが一致するオプションを確認します。
- このフロー レコードが収集するオプションを確認します。

詳細については、「フロー レコード定義」（P.11-2）を参照してください。

（注）　**show flow record** コマンドによる出力結果には、次の行が表示されますが、基になるコマンドは現在 Cisco Nexus 1000V ではサポートされていません。これらのコマンドを使用しても、コンフィギュレーションには影響はありません。
collect routing source as
collect routing destination as
collect routing next-hop address ipv4

手順の概要

1. **config t**
2. **flow record** *name*
3. **description** *string*
4. **match {ip {protocol | tos} | ipv4 {destination address | source address} | transport {destination-port | source-port}}**
5. **collect {counter {bytes [long] | packets [long]} | timestamp sys-uptime | transport tcp flags}**
6. **show flow record** [*name*]
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**flow record** *name*
	
	例：
	`n1000v(config)# flow record RecordTest`
	`n1000v(config-flow-record)#`
		名前ごとにフロー レコードを作成し、特定のレコードで、CLI フロー レコード コンフィギュレーション モードに切り替えます。

ステップ 3	**description** *string* **例：** `n1000v(config-flow-record)# description Ipv4Flow`	（任意）63 文字以内の説明をこのフロー レコードに追加し、実行コンフィギュレーションに保存します。

	コマンド	目的
ステップ 4	**match {ip {protocol | tos} | ipv4 {destination address | source address} | transport {destination-port | source-port}}** **例：** `n1000v(config-flow-record)# match ipv4 destination address`	次のいずれかに一致するフロー レコードを定義し、実行コンフィギュレーションに保存します。 • **ip**：次の IP オプションのいずれかと一致します。 – protocol – tos（タイプ オブ サービス） • **ipv4**：次の ipv4 アドレス オプションのいずれかと一致します。 – 送信元アドレス – 宛先アドレス • **transport**：次のトランスポート オプションのいずれかと一致します。 – 宛先ポート – 送信元ポート
ステップ 5	**collect {counter {bytes [long] | packets [long]} | timestamp sys-uptime | transport tcp flags}** **例：** `n1000v(config-flow-record)# collect counter packets`	収集オプションを指定して、フロー レコードで収集する情報を定義し、実行コンフィギュレーションに保存します。 • **counter**：次のフォーマットのいずれかで、フロー レコード情報を収集します。 – bytes：32 ビットのカウンタで収集されます（ロングの 64 ビット カウンタが指定されている場合を除く）。 – packets：32 ビットのカウンタで収集されます（ロングの 64 ビット カウンタが指定されている場合を除く）。 • **timestamp sys-uptime**：フローの先頭または最終パケットに関するシステム稼動時間を収集します。 • **transport tcp flags**：フローのパケットの TCP トランスポート レイヤ フラグを収集します。
ステップ 6	**show flow record** [*name*] **例：** `n1000v(config-flow-exporter)# show flow record RecordTest`	（任意）フロー レコード情報を表示します。
ステップ 7	**copy running-config startup-config** **例：** `n1000v(config-flow-exporter)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

次に、フロー レコードを作成する例を示します。

```
n1000v# config t
n1000v(config)# flow record RecordTest
```

```
n1000v(config-flow-record)# description Ipv4flow
n1000v(config-flow-record)# match ipv4 destination address
n1000v(config-flow-record)# collect counter packets
n1000v(config-flow-record)# show flow record RecordTest
Flow record RecordTest:
    Description: Ipv4flow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 destination address
        match interface input
        match interface output
        match flow direction
        collect counter packets
n1000v(config-flow-record)#
```

フロー エクスポータの定義

この手順を使用して、フロー レコードが NetFlow コレクタ サーバにエクスポートされる場所と方法を定義する、フロー エクスポータを作成します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- 最大 2 つのフロー エクスポータを、各モニタに対して許可します。
- NetFlow コレクタ サーバの宛先 IP アドレスを確認します。
- フロー レコードが送信される送信元インターフェイスを確認します。
- コレクタが待機しているトランスポート UDP を確認します。
- エクスポート フォーマット バージョン 9 がサポートされているバージョンです。

手順の概要

1. **config t**
2. **flow exporter** *name*
3. **description** *string*
4. **destination** {*ipv4-address* | *ipv6-address*}
5. **dscp** *value*
6. **source mgmt 0** *slot/port*
7. **transport udp number**
8. **version 9**
9. **option** {**exporter-stats** | **interface-table**} **timeout** *seconds*
10. **template data timeout** *seconds*
11. **show flow exporter** [*name*]
12. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**flow exporter** *name*
	
	例：
	`n1000v(config)# flow exporter ExportTest`
	`n1000v(config-flow-exporter)#`
		フロー エクスポータを作成して、実行コンフィギュレーションに保存します。次に、CLI フロー エクスポータ コンフィギュレーション モードに切り替えます。

ステップ 3	**description** *string*
	
	例：
	`n1000v(config-flow-exporter)#`
	`description ExportV9`
		63 文字以内の説明をこのフロー エクスポータに追加し、実行コンフィギュレーションに保存します。

ステップ 4	**destination** {*ipv4-address* | *ipv6-address*}
	
	例：
	`n1000v(config-flow-exporter)#`
	`destination 192.0.2.1`
		このフロー エクスポータの宛先インターフェイスの IP アドレスを指定し、実行コンフィギュレーションに保存します。

ステップ 5	**dscp** *value* **例：** `n1000v(config-flow-exporter)# dscp 0`	このフロー エクスポータの DiffServ コードポイント値を 0 ～ 63 の範囲で指定して、実行コンフィギュレーションに保存します。
ステップ 6	**source mgmt** *interface_number* **例：** `n1000v(config-flow-exporter)# source mgmt 0`	フロー レコードが NetFlow コレクタ サーバに送信されるインターフェイスと数を指定して、実行コンフィギュレーションに保存します。
ステップ 7	**transport udp number** **例：** `n1000v(config-flow-exporter)# transport udp 200`	NetFlow コレクションに到達するために使用する宛先 UDP ポートを、0 ～ 65535 の範囲で指定して、実行コンフィギュレーションに保存します。

ステップ 8	**version** {**9**}
	
	例：
	`n1000v(config-flow-exporter)# version 9`
	`n1000v(config-flow-exporter-version-9)#`
		NetFlow エクスポート バージョン 9 を指定して、実行コンフィギュレーションに保存します。次に、エクスポート バージョン 9 コンフィギュレーション モードに切り替えます。

	コマンド	目的
ステップ 9	**option** {**exporter-stats** | **interface-table** | **sampler-table**} **timeout** *value* **例：** `n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 1200`	次のバージョン 9 のエクスポータ再送タイマーと値のいずれかを、1 ～ 86400 秒の範囲で指定して、実行コンフィギュレーションに保存します。 • **exporter-stats** • **interface-table** • **sampler-table**
ステップ 10	**template data timeout** *seconds* **例：** `n1000v(config-flow-exporter-version-9)# template data timeout 1200`	テンプレート データ再送タイマーと値を、1 ～ 86400 秒の範囲で設定して、実行コンフィギュレーションに保存します。
ステップ 11	**show flow exporter** [*name*] **例：** `n1000v(config-flow-exporter)# show flow exporter`	（任意）フロー エクスポータに関する情報を表示します。
ステップ 12	**copy running-config startup-config** **例：** `n1000v(config-flow-exporter)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

次に、フロー エクスポータを作成する例を示します。

```
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
n1000v(config-flow-exporter)# destination 192.0.2.1
n1000v(config-flow-exporter)# dscp 2
n1000v(config-flow-exporter)# source mgmt 0
n1000v(config-flow-exporter)# transport udp 200
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 1200
n1000v(config-flow-exporter-version-9)# template data timeout 1200
n1000v(config-flow-exporter-version-9)# show flow exporter ExportTest
Flow exporter ExportTest:
    Description: ExportHamilton
    Destination: 192.0.2.1
    VRF: default (1)
    Destination UDP Port 200
    Source Interface Mgmt0
    DSCP 2
    Export Version 9
        Exporter-stats timeout 1200 seconds
        Data template timeout 1200 seconds
    Exporter Statistics
        Number of Flow Records Exported 0
        Number of Templates Exported 0
        Number of Export Packets Sent 0
        Number of Export Bytes Sent 0
        Number of Destination Unreachable Events 0
        Number of No Buffer Events 0
        Number of Packets Dropped (No Route to Host) 0
        Number of Packets Dropped (other) 0
```

```
        Number of Packets Dropped (LC to RP Error) 0
        Number of Packets Dropped (Output Drops) 1
        Time statistics were last cleared: Never
n1000v(config-flow-exporter-version-9)#
```

フロー モニタの定義

この手順を使用して、フロー モニタを作成し、フロー レコードとフロー エクスポータを作成したフロー モニタに関連付けます。

始める前に

- 最大 1 つのフロー モニタを、各方向の各インターフェイスに対して許可します。
- このフロー モニタを関連付ける既存のフロー エクスポータ名を確認します。
- このフロー モニタを関連付ける既存のフロー レコード名を確認します。以前に作成したフロー レコードまたは次の Cisco Nexus 1000V のあらかじめ定義されたフロー レコードのいずれかを使用できます。
  - netflow-original
  - netflow ipv4 original-input
  - netflow ipv4 original-output
  - netflow ipv4 protocol-port

  フロー レコードの詳細については、「フロー レコード定義」（P.11-2）を参照してください。

手順の概要

1. **config t**
2. **flow monitor** *name*
3. **description** *string*
4. **exporter** *name*
5. **record** *name*
6. **timeout** {**active** *value* | **inactive** *value*}
7. **cache** {**size** *value*}
8. **show flow monitor** [*name*]
9. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**flow monitor** *name*
	
	例：
	`n1000v(config)# flow monitor MonitorTest`
	`n1000v(config-flow-monitor)#`
		名前ごとにフロー モニタを作成し、実行コンフィギュレーションに保存します。次に、CLI フロー モニタ コンフィギュレーション モードに切り替えます。

ステップ 3	**description** *string* **例：** `n1000v(config-flow-monitor)# description Ipv4Monitor`	（任意）指定されたフロー モニタの場合は、63 文字以下の英数字で説明用の文字列を追加し、実行コンフィギュレーションに保存します。
ステップ 4	**exporter** *name* **例：** `n1000v(config-flow-monitor)# exporter Exportv9`	指定されたフロー モニタの場合は、既存のフロー エクスポータを追加し、実行コンフィギュレーションに保存します。

ステップ 5	**record {***name* | **netflow** {ipv4}}
	
	Example using Cisco Nexus 1000V pre-defined record:
	`n1000v(config-flow-monitor)# record netflow-original`
	
	Example using user-defined record:
	`n1000v(config-flow-monitor)# record RecordTest`
		指定されたフロー モニタの場合は、既存のフロー レコードを追加し、実行コンフィギュレーションに保存します。
		• **name**：以前に作成したフロー レコード名、またはシスコが提供しているあらかじめ定義されたフロー レコード名。
		• **netflow**：従来の NetFlow 収集方式
		– **ipv4**：従来の IPv4 NetFlow 収集方式

ステップ 6	**timeout** {**active** *value* | **inactive** *value*} **例：** `n1000v(config-flow-monitor)# timeout inactive 600`	（任意）指定されたフロー モニタの場合、古いタイマーとキャッシュからの古いエントリの値を指定し、実行コンフィギュレーションに保存します。 • **active**：アクティブ、ロング、またはタイムアウト。許可されている値は、60 ～ 4092 秒の範囲です。デフォルト値は 1800 秒です。 • **inactive**：非アクティブまたは通常のタイムアウト。許可されている値は、15 ～ 4092 秒の範囲です。デフォルト値は 15 秒です。
ステップ 7	**cache** {**size** *value*} **例：** `n1000v(config-flow-monitor)# cache size 15000`	（任意）指定されたフロー モニタの場合、キャッシュ サイズを 256 ～ 65536 エントリの範囲で指定し、実行コンフィギュレーションに保存します。 **（注）** このオプションは、モニタ キャッシュのメモリとパフォーマンスへの影響を抑えます。

	コマンド	目的
ステップ 8	**show flow monitor** [*name*] **例：** `n1000v(config-flow-monitor)# show flow monitor Monitor Test`	（任意）既存のフロー モニタに関する情報を表示します。
ステップ 9	**copy running-config startup-config** **例：** `n1000v(config-flow-monitor)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

次に、フロー エクスポータを作成する例を示します。

```
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
n1000v(config-flow-monitor)# exporter ExportTest
n1000v(config-flow-monitor)# record RecordTest
n1000v(config-flow-monitor)# cache size 15000
n1000v(config-flow-monitor)# timeout inactive 600
n1000v(config-flow-monitor)# show flow monitor MonitorTest
Flow Monitor monitortest:
    Use count: 0
    Inactive timeout: 600
    Active timeout: 1800
    Cache Size: 15000
n1000v(config-flow-monitor)#
```

フロー モニタのインターフェイスへの割り当て

この手順を使用して、フロー モニタをインターフェイスに割り当てます。

始める前に

- インターフェイスに使用するフロー モニタ名を確認します。
- インターフェイス タイプと数を確認します。

手順の概要

1. **config t**
2. **interface** *interface-type interface-number*
3. **ip flow monitor** *name* {**input** | **output**}
4. **show flow** *interface-type interface-number*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface-type interface-number*
	
	例：
	`n1000v(config)# interface veth 2`
	`n1000v(config-if)#`
		指定されたインターフェイスの CLI インターフェイス コンフィギュレーション モードに切り替えます。

ステップ 3	**ip flow monitor** *name* {**input** | **output**} **例：** `n1000v(config-if)# ip flow monitor MonitorTest output`	指定されたインターフェイスの場合は、入出力パケット用にフロー モニタを割り当て、実行コンフィギュレーションに保存します。
ステップ 4	**show flow** *interface-type interface-number* **例：** `n1000v(config-if# show flow interface veth 2`	（任意）指定されたインターフェイスの場合、NetFlow 設定が表示されます。
ステップ 5	**copy running-config startup-config** **例：** `n1000v(config-if)# copy running-config startup-config`	（任意）実行中の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コピーし、リブートと再起動を行って、永久的に保存します。

次に、フロー モニタをインターフェイスに割り当てる例を示します。

```
n1000v(config)# interface veth 2
n1000v(config-if)# ip flow monitor MonitorTest output
n1000v(config-if)# show flow interface veth 2
Interface veth 2:
    Monitor: MonitorTest
    Direction: Output
n1000v(config-if)#
```

NetFlow の設定例

例 11-5　この例では、新しいフロー レコードを使用して、フロー モニタを定義し、それをインターフェイスに適用します。

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# description Ipv4flow
```

```
n1000v(config-flow-record)# match ipv4 destination address
n1000v(config-flow-record)# collect counter packets
n1000v(config-flow-record)# exit
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
n1000v(config-flow-exporter)# destination 192.0.2.1
n1000v(config-flow-exporter)# dscp 2
n1000v(config-flow-exporter)# source mgmt 0
n1000v(config-flow-exporter)# transport udp 200
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 1200
n1000v(config-flow-exporter-version-9)# template data timeout 1200
n1000v(config-flow-exporter-version-9)# exit
n1000v(config-flow-exporter)# exit
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
n1000v(config-flow-monitor)# exporter ExportTest
n1000v(config-flow-monitor)# record RecordTest
n1000v(config-flow-monitor)# exit
n1000v(config)# interface veth 2/1
n1000v(config-if)# ip flow monitor MonitorTest output
n1000v(config-if)# show flow interface veth 2/1
Interface veth 2/1:
    Monitor: MonitorTest
    Direction: Output
n1000v(config-if)#
```

例 11-6　この例では、あらかじめ定義されたレコードを使用して、フロー モニタを定義し、それをインターフェイスに適用します。

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
n1000v(config-flow-exporter)# destination 192.0.2.1
n1000v(config-flow-exporter)# dscp 2
n1000v(config-flow-exporter)# source mgmt 0
n1000v(config-flow-exporter)# transport udp 200
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 1200
n1000v(config-flow-exporter-version-9)# template data timeout 1200
n1000v(config-flow-exporter-version-9)# exit
n1000v(config-flow-exporter)# exit
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
n1000v(config-flow-monitor)# exporter ExportTest
n1000v(config-flow-monitor)# record netflow-original
n1000v(config-flow-monitor)# exit
n1000v(config)# interface veth 2/1
n1000v(config-if)# ip flow monitor MonitorTest output
n1000v(config-if)# show flow interface veth 2/1
Interface veth 2/1:
    Monitor: MonitorTest
    Direction: Output
n1000v(config-if)#
```

NetFlow の設定確認

NetFlow 設定を確認するには、表 11-1 で説明されているコマンドを使用します。

表 11-1　NetFlow の設定確認

コマンド	目的
show flow exporter [*name*]	NetFlow のフロー エクスポータ マップ情報を表示します。 例 11-7（P.11-21）を参照してください。
show flow interface [*interface-type number*]	NetFlow インターフェイスに関する情報を表示します。 例 11-8（P.11-22）を参照してください。
show flow monitor [*name* [**cache module** *number* |**statistics module** *number*]	NetFlow フロー モニタに関する情報を表示します。 （注）　**show flow monitor cache** コマンドは、キャッシュ エントリも表示するという点で、**show flow monitor statistics** コマンドとは異なります。各プロセッサには独自のキャッシュがあるため、これらのコマンドのすべての出力内容は、サーバ（モジュールまたはホストとも呼ばれます）のプロセッサ数に基づいています。複数のプロセッサを使用して、1 つのフローのパケットを処理している場合、同じフローが各プロセッサに表示されます。 次の例を参照してください。 • 「Show flow monitor」（P.11-22） • 「Show flow monitor cache module」（P.11-22） • 「Show flow monitor statistics module」（P.11-23）
show flow record [*name*]	NetFlow のフロー レコード情報を表示します。

例 11-7　Show flow exporter

```
n1000v(config-flow-exporter-version-9)# show flow exporter ExportTest
Flow exporter ExportTest:
    Description: ExportHamilton
    Destination: 192.0.2.1
    VRF: default (1)
    Destination UDP Port 200
    Source Interface 2
    DSCP 2
    Export Version 9
        Exporter-stats timeout 1200 seconds
        Data template timeout 1200 seconds
    Exporter Statistics
        Number of Flow Records Exported 0
        Number of Templates Exported 0
```

```
        Number of Export Packets Sent 0
        Number of Export Bytes Sent 0
        Number of Destination Unreachable Events 0
        Number of No Buffer Events 0
        Number of Packets Dropped (No Route to Host) 0
        Number of Packets Dropped (other) 0
        Number of Packets Dropped (LC to RP Error) 0
        Number of Packets Dropped (Output Drops) 1
        Time statistics were last cleared: Never
n1000v(config-flow-exporter-version-9)#
```

例 11-8　Show flow interface

```
n1000v(config-if)# show flow interface VEth2
Interface veth2:
    Monitor: MonitorTest
    Direction: Output
n1000v(config-if)#
```

例 11-9　Show flow monitor

```
n1000v(config)# show flow monitor
Flow Monitor MonitorTest:
    Description: Ipv4Monitor
    Use count: 1
    Flow Record: test
    Flow Exporter: ExportTest
    Inactive timeout: 15
    Active timeout: 1800
    Cache Size: 15000
Flow Monitor MonitorIpv4:
    Description: exit
    Use count: 70
    Flow Record: RecordTest
    Flow Exporter: ExportIpv4
    Inactive timeout: 15
    Active timeout: 1800
    Cache Size: 4096
n1000v(config)#
```

例 11-10　Show flow monitor cache module

```
n1000v# show flow monitor test_mon cache module 5
Cache type:                           Normal
Cache size (per-processor):           4096
High Watermark:                       2
Flows added:                          102
Flows aged:                           099
    - Active timeout                  0
    - Inactive timeout                099
    - Event aged                      0
    - Watermark aged                  0
    - Emergency aged                  0
    - Permanent                       0
    - Immediate aged                  0
    - Fast aged                       0

Cache entries on Processor0
    - Active Flows:                   2
    - Free Flows:                     4094
```

```
  IPV4 SRC ADDR    IPV4 DST ADDR  IP PROT            INTF INPUT           INTF OUTPUT  FLOW DIRN
===============  ===============  =======  ====================  ====================  =========
        0.0.0.0  255.255.255.255  17                     Veth1                            Input
   7.192.192.10      7.192.192.2  1                      Veth1                Eth5/2      Input

Cache entries on Processor1
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor2
    - Active Flows:                 1
    - Free Flows:                   4095

  IPV4 SRC ADDR    IPV4 DST ADDR  IP PROT            INTF INPUT           INTF OUTPUT  FLOW DIRN
===============  ===============  =======  ====================  ====================  =========
   7.192.192.10      7.192.192.1  1                      Veth1                Eth5/2      Input

Cache entries on Processor3
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor4
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor5
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor6
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor7
    - Active Flows:                 0
    - Free Flows:                   4096
```

例 11-11　Show flow monitor statistics module

```
NX-1000v# show flow monitor test_mon statistics module 5
Cache type:                           Normal
Cache size (per-processor):           4096
High Watermark:                       2
Flows added:                          105
Flows aged:                           103
    - Active timeout                  0
    - Inactive timeout                103
    - Event aged                      0
    - Watermark aged                  0
    - Emergency aged                  0
    - Permanent                       0
    - Immediate aged                  0
    - Fast aged                       0

Cache entries on Processor0
    - Active Flows:                   0
    - Free Flows:                     4096

Cache entries on Processor1
    - Active Flows:                   1
    - Free Flows:                     4095
```

```
Cache entries on Processor2
    - Active Flows:                 1
    - Free Flows:                   4095

Cache entries on Processor3
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor4
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor5
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor6
    - Active Flows:                 0
    - Free Flows:                   4096

Cache entries on Processor7
    - Active Flows:                 0
    - Free Flows:                   4096
```

例 11-12　Show flow record

```
n1000v(config-flow-record)# show flow record RecordTest
Flow record RecordTest:
    Description: Ipv4flow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 destination address
        match interface input
        match interface output
        match flow direction
        collect counter packets
n1000v(config-flow-record)#
```

デフォルト設定

表 11-2 に、NetFlow パラメータのデフォルト設定をリスト表示します。

表 11-2　デフォルトの NetFlow パラメータ

パラメータ	デフォルト
source interface	mgmt0
match	方向とインターフェイス（着信 / 発信）
flow monitor active timeout	1800
flow monitor inactive timeout	15
flow monitor cache size	4096

その他の関連資料

NetFlow の実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.11-25）
- 「標準規格」（P.11-25）

関連資料

関連項目	マニュアル タイトル
Cisco NetFlow の概要	http://cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

その他の関連資料

CHAPTER 12

システム メッセージ ロギングの設定

この章では、デバイス上でシステム メッセージ ロギングを設定する方法について説明します。

この章では、次の内容について説明します。

システム メッセージ ロギングの概要

システム メッセージ ロギングを使用すると、システム プロセスが生成するメッセージの宛先を制御し、重大度に基づいてメッセージをフィルタリングできます。端末セッション、ログ ファイル、およびリモート システム上の syslog サーバへのロギングを設定できます。

システム メッセージ ロギングは RFC 3164 に準拠しています。システム メッセージのフォーマットおよびデバイスが生成するメッセージの詳細については、『*Cisco NX-OS System Messages Reference*』を参照してください。

デバイスはデフォルトで、端末セッションにメッセージを出力します。端末セッションへのロギングの設定については、「端末セッションへのシステム メッセージ ロギングの設定」（P.12-5）を参照してください。

表 12-1 で、システム メッセージに使用する重大度について説明します。重大度を設定すると、そのレベルとそれより下位レベルのメッセージが出力されます。

表 12-1　　システム メッセージの重大度

レベル	説明
0 ：緊急事態	システムは使用不能
1 ：アラート	即時対処が必要
2 ：クリティカル	クリティカル条件

表 12-1　システム メッセージの重大度 （続き）

レベル	説明
3 ：エラー	エラー条件
4 ：警告	警告条件
5 ：通知	正常だが重要な条件
6 ：情報	情報目的のメッセージ
7 ：デバッグ	デバッグ時限定の表示

デバイスは重大度 0、1、または 2 のメッセージのうち、最新の 100 メッセージを NVRAM ログに記録します。NVRAM へのロギングは設定できません。

メッセージを生成したファシリティとメッセージの重大度に基づいて、記録するシステム メッセージを設定できます。ファシリティについては、「システム メッセージ ロギング ファシリティ」（P.12-2）を参照してください。モジュールおよびファシリティごとの重大度の設定については、「モジュールのシステム メッセージ ロギングの設定」（P.12-7）を参照してください。

syslog サーバは、syslog プロトコルに基づいてシステム メッセージを記録するように設定されたリモート システム上で動作します。最大 3 つの syslog サーバを設定できます。syslog サーバの設定については、「syslog サーバの設定」（P.12-11）を参照してください。

（注）　最初のデバイス初期化時に、メッセージが syslog サーバに送信されるのは、ネットワークの初期化後です。

システム メッセージ ロギング ファシリティ

表 12-2 に、システム メッセージ ロギング コンフィギュレーションで使用できるファシリティの一覧を示します。

表 12-2　システム メッセージ ロギング ファシリティ

ファシリティ	説明
aaa	AAA マネージャ
aclmgr	ACL マネージャ
adjmgr	隣接マネージャ
all	すべてのファシリティを表すキーワード
arbiter	アービター マネージャ
arp	ARP マネージャ
auth	許可システム
authpriv	プライベート許可システム
bootvar	Bootvar
callhome	Call home マネージャ
capability	MIG ユーティリティ デーモン
cdp	CDP マネージャ
cert-enroll	証明書登録デーモン

表 12-2　システム メッセージ ロギング ファシリティ （続き）

ファシリティ	説明
cfs	CFS マネージャ
clis	CLIS マネージャ
cmpproxy	CMP プロキシ マネージャ
copp	CoPP マネージャ
core	コア デーモン
cron	cron および at スケジューリング サービス
daemon	システム デーモン
dhcp	DHCP マネージャ
diagclient	GOLD 診断クライアント マネージャ
diagmgr	GOLD 診断マネージャ
eltm	ELTM マネージャ
ethpm	イーサネット PM マネージャ
evmc	EVMC マネージャ
evms	EVMS マネージャ
feature-mgr	Feature マネージャ
fs-daemon	Fs デーモン
ftp	ファイル転送システム
glbp	GLBP マネージャ
hsrp	HSRP マネージャ
im	IM マネージャ
ipconf	IP コンフィギュレーション マネージャ
ipfib	IP FIB マネージャ
kernel	OS カーネル
l2fm	L2 FM マネージャ
l2nac	L2 NAC マネージャ
l3vm	L3 VM マネージャ
license	ライセンス マネージャ
local0	Local use daemon
local1	Local use daemon
local2	Local use daemon
local3	Local use daemon
local4	Local use daemon
local5	Local use daemon
local6	Local use daemon
local7	Local use daemon
lpr	ライン プリンタ システム
m6rib	M6RIB マネージャ
mail	メール システム

表 12-2　システム メッセージ ロギング ファシリティ （続き）

ファシリティ	説明
mfdm	MFDM マネージャ
module	モジュール マネージャ
monitor	イーサネット SPAN マネージャ
mrib	MRIB マネージャ
mvsh	MVSH マネージャ
news	USENET ニュース
nf	NF マネージャ
ntp	NTP マネージャ
otm	GLBP マネージャ
pblr	PBLR マネージャ
pfstat	PFSTAT マネージャ
pixm	PIXM マネージャ
pixmc	PIXMC マネージャ
pktmgr	パケット マネージャ
platform	プラットフォーム マネージャ
pltfm_config	PLTFM コンフィギュレーション マネージャ
plugin	プラグイン マネージャ
port-channel	ポート チャネル マネージャ
port_client	ポート クライアント マネージャ
port_lb	診断ポート ループバック テスト マネージャ
qengine	Q エンジン マネージャ
radius	RADIUS マネージャ
res_mgr	リソース マネージャ
rpm	RPM マネージャ
security	セキュリティ マネージャ
session	セッション マネージャ
spanning-tree	スパニング ツリー マネージャ
syslog	内部 syslog マネージャ
sysmgr	システム マネージャ
tcpudp	TCP および UDP マネージャ
u2	U2 マネージャ
u6rib	U6RIB マネージャ
ufdm	UFDM マネージャ
urib	URIB マネージャ
user	ユーザ プロセス
uucp	UNIX 間コピー システム
vdc_mgr	VDC マネージャ
vlan_mgr	VLAN マネージャ

表 12-2　システム メッセージ ロギング ファシリティ （続き）

ファシリティ	説明
vmm	VMM マネージャ
vshd	VSHD マネージャ
xbar	XBAR マネージャ
xbar_client	XBAR クライアント マネージャ
xbar_driver	XBAR ドライバ マネージャ
xml	XML エージェント

注意事項および制約事項

システム メッセージは、デフォルトでコンソールおよびログ ファイルに記録されます。

システム メッセージ ロギングの設定

ここでは、次の内容について説明します。

（注）　Cisco Nexus 1000V コマンドは Cisco IOS コマンドと異なる場合があるので注意してください。

端末セッションへのシステム メッセージ ロギングの設定

重大度に基づいて、コンソール、Telnet、および SSH セッションにメッセージを記録するには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次のことを確認または実行しておく必要があります。

- デフォルトでは、端末セッションでのロギングがイネーブルです。

手順の概要

1. **terminal monitor**
2. **config t**
3. **logging console** [*severity-level*]
4. **show logging console**
5. **logging monitor** [*severity-level*]
6. **show logging monitor**
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**terminal monitor**
	
	例：
	`n1000v# terminal monitor`
	`n1000v#`
		デバイスがコンソールにメッセージを記録できるようにします。

ステップ 2	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	**logging console** [*severity-level*]
	
	例：
	`n1000v(config)# logging console 2`
	`n1000v(config)#`
		指定された重大度とそれより上位の重大度のメッセージをコンソール セッションに記録するように、デバイスを設定します。重大度は表 12-1 に示したとおり、0 ～ 7 の範囲で指定できます。重大度を指定しなかった場合は、デフォルトの 2 が使用されます。

ステップ 4	**show logging console**	（任意）コンソール ロギングの設定を表示します。

ステップ 5	**logging monitor** [*severity-level*]
	
	例：
	`n1000v(config)# logging monitor 3`
	`n1000v(config)#`
		デバイスが指定された重大度とそれより上位の重大度のメッセージをモニタに記録できるようにします。この設定は、Telnet および SSH セッションに適用されます。重大度は表 12-1 に示したとおり、0 ～ 7 の範囲で指定できます。重大度を指定しなかった場合は、デフォルトの 2 が使用されます。

ステップ 6	**show logging monitor**	（任意）モニタ ロギングの設定を表示します。
ステップ 7	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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コピーします。

例：

```
n1000v# terminal monitor
n1000v# config t
n1000v(config)# logging console 2
n1000v(config)# show logging console
Logging console:                enabled (Severity: critical)
n1000v(config)# logging monitor 3
n1000v(config)# show logging monitor
Logging monitor:                enabled (Severity: errors)
n1000v(config)#
n1000v(config)# copy running-config startup-config
```

端末セッションのシステム メッセージ ロギングのデフォルトの復元

端末セッションのシステム メッセージ ロギングのデフォルト設定を復元するには、CLI グローバル コンフィギュレーション モードで次のコマンドを実行します。

コマンド	説明

no logging console [*severity-level*]
 	
例：
`n1000v(config)# no logging console`
`n1000v(config)#`
	デバイスによるコンソールへのメッセージのロギングをディセーブルにします。

no logging monitor [*severity-level*]
 	
例：
`n1000v(config)# no logging monitor 3`
`n1000v(config)#`
	Telnet および SSH セッションへのメッセージ ロギングをディセーブルにします。

モジュールのシステム メッセージ ロギングの設定

モジュールごとに記録されるメッセージの重大度とタイムスタンプ ユニットを設定するには、ここに示す手順を実行します。

始める前に

手順の概要

1. **config t**
2. **logging module** [*severity-level*]
3. **show logging module**
4. **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}
5. **show logging timestamp**

6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

ステップ 2	**logging module** [*severity-level*] **例：** `n1000v(config)# logging module 3`	指定された重大度以上のモジュール ログ メッセージをイネーブルにします。重大度は表 12-1 に示したとおり、0 ～ 7 の範囲で指定できます。重大度を指定しなかった場合は、デフォルトの 5 が使用されます。
ステップ 3	**show logging module**	（任意）モジュール ロギング設定を表示します。
ステップ 4	**logging timestamp** {**microseconds** | **milliseconds** | **seconds**} **例：** `n1000v(config)# logging timestamp microseconds`	ロギング タイムスタンプ ユニットを設定します。デフォルトの単位は秒です。
ステップ 5	**show logging timestamp**	（任意）設定されているロギング タイムスタンプ ユニットを表示します。
ステップ 6	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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コピーします。

次に、モジュールのシステム メッセージ ロギングを設定する例を示します。

例：

```
n1000v# config t
n1000v(config)# logging module 3
n1000v(config)# show logging module
Logging linecard:                enabled (Severity: errors)
n1000v(config)# logging timestamp microseconds
n1000v(config)# show logging timestamp
Logging timestamp:               Microseconds
n1000v(config)# copy running-config
```

モジュールのシステム メッセージ ロギングのデフォルトの復元

モジュールのシステム メッセージ ロギングのデフォルト設定を復元するには、CLI グローバル コンフィギュレーション モードで次のコマンドを実行します。

コマンド	説明

no logging module [*severity-level*]
 	
例：
`n1000v(config)# no logging module 3`
`n1000v(config)#`
	モジュールのシステム メッセージ ロギングのデフォルトの重大度を復元します。

no logging timestamp {**microseconds** | **milliseconds** | **seconds**} **例：** `n1000v(config)# no logging timestamp milliseconds`	ロギング タイムスタンプ ユニットをデフォルトの秒にリセットします。

ファシリティのシステム メッセージ ロギングの設定

ファシリティごとに記録されるメッセージの重大度とタイムスタンプ ユニットを設定するには、ここに示す手順を実行します。

始める前に

手順の概要

1. **config t**
2. **logging level** *facility severity-level*
3. **show logging level** [*facility*]
4. **logging timestamp** {**microseconds** | **milliseconds** | **seconds**}
5. **show logging timestamp**
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI グローバル コンフィギュレーション モードを開始します。

	コマンド	目的

ステップ 2	**logging level** *facility severity-level*
	
	例：
	`n1000v(config)# logging level aaa 3`
	`n1000v(config)#`
		指定されたファシリティからの、指定した重大度以上のメッセージ ロギングをイネーブルにします。ファシリティについては、「システム メッセージ ロギング ファシリティ」（P.12-2）を参照してください。重大度は表 12-1 に示したとおり、0 ～ 7 の範囲で指定できます。すべてのファシリティに同じ重大度を適用する場合は、facility に **all** を使用します。デフォルトについては、**show logging level** コマンドを参照してください。

ステップ 3	**show logging level** [*facility*] **例：** `n1000v(config)# show logging level aaa`	（任意）ファシリティ別に、ロギング レベルの設定およびシステム デフォルト レベルを表示します。ファシリティを指定しなかった場合は、すべてのファシリティのレベルが表示されます。
ステップ 4	**logging timestamp** {**microseconds** | **milliseconds** | **seconds**} **例：** `n1000v(config)# logging timestamp microseconds`	ロギング タイムスタンプ ユニットを設定します。デフォルトの単位は秒です。
ステップ 5	**show logging timestamp**	（任意）設定されているロギング タイムスタンプ ユニットを表示します。
ステップ 6	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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コピーします。

ファシリティのシステム メッセージ ロギングの設定例を示します。

例：

```
n1000v# config t
n1000v(config)# logging level aaa 3
n1000v(config)# show logging level aaa
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       3

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
logging timestamp microseconds
n1000v(config)# show logging timestamp
Logging timestamp:              Microseconds
copy running-config startup-config
```

ファシリティのシステム メッセージ ロギングのデフォルトの復元

ファシリティのシステム メッセージ ロギングのデフォルトを復元するには、次のコマンドを使用します。

コマンド	説明

no logging level [*facility severity-level*]
 	
例：
`n1000v(config)# no logging level aaa 3`
`n1000v(config)#`
	指定したファシリティのデフォルトのロギング重大度を復元します。ファシリティおよび重大度を指定しなかった場合、すべてのファシリティがそれぞれのデフォルト重大度にリセットされます。

no logging timestamp {**microseconds** | **milliseconds** | **seconds**} **例：** `n1000v(config)# no logging timestamp milliseconds`	ロギング タイムスタンプ ユニットをデフォルトの秒にリセットします。

syslog サーバの設定

システム メッセージ ロギングのための syslog サーバを設定するには、ここに示す手順を実行します。

手順の概要

1. **config t**
2. **logging server** *host* [*severity-level* [**use_vrf** *vrf-name*]]
3. **show logging server**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**logging server** *host* [*severity-level* [**use-vrf** *vrf-name*]] **例：** `n1000v(config)# logging server 10.10.2.2 7`	指定のホスト名または IPv4/IPv6 アドレスで syslog サーバを設定します。**use_vrf** キーワードを使用すると、メッセージ ロギングを特定の VRF に限定できます。重大度は表 12-1 に示したとおり、0 ～ 7 の範囲で指定できます。デフォルトの発信ファシリティは local7 です。 この例では、ファシリティ local 7 のすべてのメッセージを転送します。

ステップ 3	**show logging server**
	
	例：
	`n1000v(config)# show logging server`
	`Logging server: enabled`
	`{10.10.2.2}`
	`server severity: debugging`
	`server facility: local7`
		（任意）syslog サーバの設定を表示します。

ステップ 4	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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コピーします。

サーバのシステム メッセージ ロギングのデフォルトの復元

サーバのシステム メッセージ ロギングのデフォルトを復元するには、ここに示す手順を実行します。

コマンド	説明
no logging server *host* **例：** `n1000v(config)# no logging server host`	指定されたホストに対応するロギング サーバを削除します。

UNIX または Linux システムを使用したロギングの設定

UNIX または Linux システムでメッセージ ロギングを設定するには、ここに示す手順を実行します。

始める前に

この手順を開始する前に、次の点を理解または実行しておく必要があります。

- 次に示すのは、syslog 用に設定する UNIX または Linux のフィールドです。

フィールド	説明
Facility	メッセージの作成元。auth、authpriv、cron、daemon、kern、lpr、mail、mark、news、syslog、user、local0 ～ local7、またはすべてを表すアスタリスク（*）。これらのファシリティ指定によって、発信元に基づいてメッセージの宛先を制御できます。 **（注）** ローカル ファシリティを使用する前に、コンフィギュレーションを確認してください。
Level	メッセージを記録する最小の重大度。debug、info、notice、warning、err、crit、alert、emerg、またはすべてを表すアスタリスク（*）を指定できます。ファシリティをディセーブルにする場合は、none を使用します。
Action	メッセージの宛先。ファイル名、前に @ 記号を加えたホスト名、ユーザをカンマで区切ったリスト、またはすべてのログイン ユーザを表すアスタリスク（*）を使用できます。

手順の詳細

ステップ 1　UNIX または Linux システムで、次の内容をファイル /var/log/myfile.log に追加します。

```
facility.level <five tab characters> action
```

例：

```
debug.local7            /var/log/myfile.log
```

ステップ 2　シェル プロンプトに次のコマンドを入力し、ログ ファイルを作成します。

```
$ touch /var/log/myfile.log
$ chmod 666 /var/log/myfile.log
```

ステップ 3　コマンド入力後に myfile.log を調べ、システム メッセージ ロギング デーモンが新しい設定変更を読み取ったかどうかを確認します。

```
$ kill -HUP ~cat /etc/syslog.pid~
```

ログ ファイルの表示

ログ ファイル中のメッセージを表示するには、ここに示す手順を実行します。

手順の概要

1. **show logging last** *number-lines*

手順の詳細

	コマンド	目的
ステップ 1	**show logging last** *number-lines*	ログ ファイルの末尾から指定行数を表示します。最終行番号として 1 ～ 9999 を指定できます。

例：

```
n1000v#  show logging last 5
2008 Aug 31 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:04 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
2008 Aug 31 09:37:05 CP-beta2 %KERN-3-SYSTEM_MSG: packet_recvms
g: truncated packet (size=1514 left=1500) - kernel
n1000v#
```

システム メッセージ ロギングの設定確認

システム メッセージ ロギングの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show logging console	コンソール ロギングの設定を表示します。 例 12-1（P.12-15）を参照してください。
show logging info	ロギングの設定を表示します。 例 12-2（P.12-15）を参照してください。
show logging last *number-lines*	ログ ファイルの末尾から指定行数を表示します。 例 12-3（P.12-16）を参照してください。
show logging level [*facility*]	ファシリティ ロギングの重大度の設定を表示します。 例 12-4（P.12-17）を参照してください。
show logging module	モジュール ロギングの設定を表示します。 例 12-5（P.12-17）を参照してください。
show logging monitor	モニタ ロギングの設定を表示します。 例 12-6（P.12-17）を参照してください。
show logging server	syslog サーバの設定を表示します。 例 12-7（P.12-17）を参照してください。

コマンド	目的
show logging session	ロギング セッション ステータスを表示します。 例 12-8（P.12-17）を参照してください。
show logging status	ロギング ステータスを表示します。 例 12-9（P.12-17）を参照してください。
show logging timestamp	設定されているロギング タイムスタンプ ユニットの設定を表示します。 例 12-10（P.12-17）を参照してください。

例 12-1　　show logging console

```
n1000v# show logging console
Logging console:                disabled
n1000v#
```

例 12-2　　show logging info

```
n1000v# show logging info

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: notifications)
Logging linecard:               enabled (Severity: notifications)
Logging timestamp:              Seconds
Logging server:                 disabled
Logging logfile:                enabled
        Name - g/external/messages: Severity - notifications Size - 4194304

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       2
auth                    0                       0
authpriv                3                       3
bootvar                 5                       5
callhome                2                       2
cdp                     2                       2
cert_enroll             2                       2
cfs                     3                       3
confcheck               2                       2
cron                    3                       3
daemon                  3                       3
diagclient              2                       2
diagmgr                 2                       2
eth_port_channel        5                       5
ethpm                   5                       5
evmc                    5                       5
evms                    2                       2
feature-mgr             2                       2
ftp                     3                       3
ifmgr                   5                       5
igmp_1                  3                       3
ip                      2                       2
ipv6                    2                       2
kern                    6                       6
l2fm                    2                       2
licmgr                  6                       6
local0                  3                       3
local1                  3                       3
```

```
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
lpr                     3                       3
mail                    3                       3
mfdm                    2                       2
module                  5                       5
monitor                 7                       7
msp                     2                       2
mvsh                    2                       2
news                    3                       3
ntp                     2                       2
otm                     3                       3
pblr                    2                       2
pixm                    2                       2
pixmc                   2                       2
platform                5                       5
portprofile             5                       5
private-vlan            3                       3
radius                  2                       2
res_mgr                 2                       2
rpm                     2                       2
sal                     2                       2
securityd               2                       2
sksd                    3                       3
stp                     3                       3
syslog                  3                       3
sysmgr                  3                       3
ufdm                    2                       2
urib                    3                       3
user                    3                       3
uucp                    3                       3
vdc_mgr                 6                       6
vim                     5                       5
vlan_mgr                2                       2
vms                     5                       5
vshd                    5                       5
xmlma                   3                       3

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
n1000v$
```

例 12-3　show logging last

```
n1000v# show logging last 5
2008 Jul 29 17:52:42 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/5 is up in mode access
2008 Jul 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/2 is up in mode trunk
2008 Jul 29 17:52:43 S22-DCOS %ETHPORT-5-IF_UP: Interface Ethernet2/4 is up in mode access
2008 Jul 29 17:53:04 S22-DCOS %SYSMGR-3-BASIC_TRACE: process_cfg_write: PID 1858 with
message rcvd cfg_action from
sap 0x545 for vdc 1 at time 1217353984 .
2008 Jul 29 17:53:04 S22-DCOS clis[2558]: CLI-3-NVDB: Batched send failed for component:
clic
n1000v#
```

例 12-4　show logging level aaa

```
n1000v# show logging level aaa
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
aaa                     2                       2

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
n1000v#
```

例 12-5　show logging module

```
n1000v# show logging module
Logging linecard:               enabled (Severity: notifications)
n1000v#
```

例 12-6　show logging monitor

```
n1000v# show logging monitor
Logging monitor:                enabled (Severity: errors)
n1000v#
```

例 12-7　show logging server

```
n1000v# show logging server
Logging server:                 enabled
{10.10.2.2}
        server severity:        debugging
        server facility:        local7
n1000v#
```

例 12-8　show logging session status

```
n1000v# show logging session status
Last Action Time Stamp     : Fri Nov 18 11:28:55 1910
Last Action                : Distribution Enable
Last Action Result         : Success
Last Action Failure Reason : none
n1000v#
```

例 12-9　show logging status

```
n1000v# show logging status
Fabric Distribute     : Enabled
Session State         : IDLE
n1000v#
```

例 12-10　show logging timestamp

```
n1000v# show logging timestamp
Logging timestamp:              Seconds
n1000v#
```

システム メッセージ ロギングの設定例

システム メッセージ ロギングの設定例を示します。

```
config t
  logging console 3
  logging monitor 3
  logging logfile my_log 6
  logging module 3
  logging level aaa 2
  logging timestamp milliseconds
  logging distribute
  logging server 172.28.254.253
  logging server 172.28.254.254 5 local3
  logging commit
  copy running-config startup-config
```

デフォルト設定

表 12-3 に、システム メッセージ ロギング パラメータのデフォルト設定を示します。

表 12-3　システム メッセージ ロギング パラメータのデフォルト設定

パラメータ	デフォルト
コンソール ロギング	重大度 2 でイネーブル
モニタ ロギング	重大度 5 でイネーブル
ログ ファイル ロギング	重大度 5 のメッセージ ロギングがイネーブル
モジュール ロギング	重大度 5 でイネーブル
ファシリティ ロギング	イネーブル。重大度については「システム メッセージ ロギング ファシリティ」（P.12-2）を参照
タイムスタンプ ユニット	秒
syslog サーバ ロギング	ディセーブル
syslog サーバ コンフィギュレーション配布	ディセーブル

その他の関連資料

システム メッセージ ロギングの実装に関連する詳細情報については、次の項を参照してください。

- 「関連資料」（P.12-19）
- 「標準規格」（P.12-19）

関連資料

関連項目	マニュアル タイトル
システム管理 CLI コマンド	『*Cisco Nexus 1000V Command Reference, Release 4.0*』
システム メッセージ	『*Cisco NX-OS System Messages Reference*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

その他の関連資料

INDEX

E

M

N

P

S

V

い

か

け

こ

す

せ

て

と

は

ふ

も

ゆ

ろ