Cisco Nexus 5000 シリーズ NX-OS セキュリティ コマンド リファレンス

Cisco NX-OS Release 4.x、5.x

初版：2008 年 10 月
最終更新日：2011 年 12 月

Text Part Number: OL-25833-01-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、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

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 5000 シリーズ NX-OS セキュリティ コマンド リファレンス

CONTENTS

はじめに

ここでは、Cisco Nexus 5000 シリーズ NX-OS セキュリティ コマンド リファレンスの対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

この前書きは、次のセクションで構成されています。

対象読者

このマニュアルは、Cisco NX-OS デバイスを設定および管理する経験豊富なユーザの方を対象としています。

サポートされるスイッチ

ここでは、次の内容について説明します。

Cisco Nexus 5000 プラットフォーム スイッチ

表 1 に、Cisco Nexus 5000 プラットフォームでサポートされる Cisco スイッチを示します。

（注） これらのスイッチの詳細については、次の URL にある『*Cisco Nexus 5500 Platform and Cisco Nexus 5000 Platform Hardware Installation Guide*』を参照してください。
http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

表 1　サポートされる Cisco Nexus 5000 プラットフォーム スイッチ

スイッチ	説明
Cisco Nexus 5010 スイッチ	Cisco Nexus 5010 は、1 Rack Unit（RU; ラック ユニット）スイッチです。このスイッチは、従来の環境、仮想化環境、統合環境、ハイパフォーマンス コンピューティング（HPC）環境に対し、500 Gbps ワイヤ速度のスイッチング機能を提供します。
Cisco Nexus 5020 スイッチ	Cisco Nexus 5020 は、2 Rack Unit（RU; ラック ユニット）スイッチです。このスイッチは、従来の環境、仮想化環境、統合環境、HPC 環境に対し、1+ Tbps ワイヤ速度のスイッチング機能を提供します。

（注）　Cisco Nexus 5000 プラットフォーム スイッチは、インターネット グループ管理プロトコル（IGMP）スヌーピングのみをサポートします。
IGMP、Protocol Independent Multicast（PIM）、Multicast Source Discovery Protocol（MSDP）は、Cisco Nexus 5000 プラットフォーム スイッチではサポートされません。

Cisco Nexus 5500 プラットフォーム スイッチ

表 2 に、Cisco Nexus 5500 プラットフォームでサポートされる Cisco スイッチを示します。

（注）　これらのスイッチの詳細については、次の URL にある『*Cisco Nexus 5500 Platform and Cisco Nexus 5000 Platform Hardware Installation Guide*』を参照してください。
http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

表 2　サポートされる Cisco Nexus 5500 プラットフォーム スイッチ

スイッチ	説明
Cisco Nexus 5548P スイッチ	Cisco Nexus 5548P スイッチは、Cisco Nexus 5500 プラットフォームの最初のスイッチです。このスイッチは、1 Rack-Unit（1 RU）の 10 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）スイッチであり、最大 960 Gbps スループットおよび最大 48 ポートを提供します。
Cisco Nexus 5596P スイッチ	Cisco Nexus 5596P スイッチは、Top-of-Rack の 10 ギガビット イーサネットおよび FCoE スイッチであり、最大 1920 ギガビット スループットおよび最大 96 ポートを提供します。

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。

章タイトル	説明
「新機能および変更された機能に関する情報」	新しい Cisco NX-OS ソフトウェア リリースの新機能および変更された機能について説明します。
「A コマンド」	B で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「C コマンド」	C で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「D コマンド」	D で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「E コマンド」	E で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「F コマンド」	F で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「I コマンド」	I で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「M コマンド」	M で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「P コマンド」	P で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「R コマンド」	R で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「S コマンド」	S で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「show コマンド」	Cisco NX-OS セキュリティの **show** コマンドについて説明します。
「T コマンド」	T で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「U コマンド」	U で始まる Cisco NX-OS セキュリティ コマンドについて説明します。
「V コマンド」	V で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

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。

表記法	説明
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。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string 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 string 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`	スイッチに表示され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、山カッコ（< >）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、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

Cisco Nexus 5000 シリーズ スイッチおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダ のマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

次に、Cisco Nexus 5000 シリーズおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダに関連するマニュアルを示します。

リリース ノート

『Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes』

『Cisco Nexus 5000 Series Switch Release Notes』

コンフィギュレーション ガイド

『Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(2)N1(1)』

『Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1) and Release 4.2(1)N2(1)』

『Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide』

『Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Security Configuration Guide』

『Cisco Nexus 5000 Series NX-OS System Management Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide』

『Cisco Nexus 5000 Series Switch NX-OS Software Configuration Guide』

『Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)』

『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x』

『Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide』

メンテナンスおよび操作ガイド

『Cisco Nexus 5000 Series NX-OS Operations Guide』

インストレーション ガイドおよびアップグレード ガイド

『Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide』

『Cisco Nexus 2000 Series Hardware Installation Guide』

『Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.2(1)N1(1)』

『Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders』

ライセンス ガイド

『Cisco NX-OS Licensing Guide』

コマンド リファレンス

『Cisco Nexus 5000 Series NX-OS FabricPath Command Reference』

『Cisco Nexus 5000 Series NX-OS Fabric Extender Command Reference』

『Cisco Nexus 5000 Series NX-OS Fibre Channel Command Reference』

『Cisco Nexus 5000 Series NX-OS Fundamentals Command Reference』

『Cisco Nexus 5000 Series NX-OS Layer 2 Interfaces Command Reference』

『Cisco Nexus 5000 Series NX-OS Multicast Routing Command Reference』

『Cisco Nexus 5000 Series NX-OS QoS Command Reference』

『Cisco Nexus 5000 シリーズ NX-OS セキュリティ コマンド リファレンス』

『Cisco Nexus 5000 Series NX-OS System Management Command Reference』

『Cisco Nexus 5000 Series NX-OS TrustSec Command Reference』

『Cisco Nexus 5000 Series NX-OS Unicast Routing Command Reference』

『Cisco Nexus 5000 Series NX-OS vPC Command Reference』

テクニカル リファレンス

『Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender MIBs Reference』

エラー メッセージおよびシステム メッセージ

『Cisco NX-OS System Messages Reference』

トラブルシューティング ガイド

『Cisco Nexus 5000 Troubleshooting Guide』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

新機能および変更された機能に関する情報

この章では、Cisco Nexus 5000 シリーズ NX-OS セキュリティ コマンド リファレンスの新機能および変更された機能に関するリリース固有の情報を示します。このマニュアルの最新バージョンは、次のシスコ Web サイトから入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

この Cisco NX-OS リリースに関する追加情報を確認するには、次のシスコ Web サイトから入手できる『*Cisco Nexus 5000 Series Switch Release Notes*』を参照してください。

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

Cisco NX-OS リリースの新機能および変更された機能に関する情報

ここでは、次の内容について説明します。

Cisco NX-OS Release 5.1(3)N1(1) の新機能および変更された機能に関する情報

表 1 では、Cisco NX-OS Release 5.1(3)N1(1) の新機能および変更された機能を要約し、その参照先を示しています。

表 1　Release 5.1(3)N1(1) の新機能および変更された機能に関する情報

機能	説明	参照先
アダプタ ファブリック エクステンダ（Adapter-FEX）	•	
コントロール プレーン ポリシング（CoPP）	この機能が導入されました。	arp access-list deny（ARP） permit（ARP） show arp access-lists
IP ARP 同期		show ip arp sync-entries
仮想イーサネット インターフェイスのサポート	次のコマンドは、仮想イーサネット インターフェイス設定のサポートを拡張するために更新されました。 • **ip port access-group** • **ipv6 port traffic-filter** • **mac port access-group** • **show ip arp**	ip port access-group ipv6 port traffic-filter mac port access-group show ip arp

Cisco NX-OS Release 5.0(3)N2(1) の新機能および変更された機能に関する情報

Cisco NX-OS Release 5.0(3)N2(1) には、新機能および変更された機能はありません。

Cisco NX-OS Release 5.0(3)N1(1) の新機能および変更された機能に関する情報

表 2 では、Cisco NX-OS Release 5.0(3)N1(1) の新機能および変更された機能を要約し、その参照先を示しています。

表 2　Release 5.0(3)N1(1) の新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
IP アクセス グループ	ルータ ACL としてインターフェイスに IPv4 アクセス コントロール リスト（ACL）を適用するために、**ip access-group** コマンドが追加されました。	5.0(3)N1(1)	ip access-group
IPSG	この機能が導入されました。 レイヤ 2 イーサネット インターフェイス用に次の IP ソース ガード コマンドが導入されました。 • **ip verify source dhcp-snooping-vlan** • **show ip verify source**	5.0(3)N1(1)	ip verify source dhcp-snooping-vlan show ip verify source
Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）	この機能が導入されました。 Cisco NX-OS スイッチにダイナミック アドレス解決プロトコル インスペクション（ダイナミック ARP インスペクション）（DAI）を設定するために、次のコマンドが追加されました。 • **ip arp inspection log-buffer** • **ip arp inspection validate** • **ip arp inspection vlan**	5.0(3)N1(1)	clear ip arp inspection log clear ip arp inspection statistics vlan ip arp inspection log-buffer ip arp inspection validate ip arp inspection vlan show ip arp inspection show ip arp inspection interfaces show ip arp inspection log show ip arp inspection statistics
ユニキャスト RPF	インターフェイスで Unicast Reverse Path Forwarding（ユニキャスト RPF）を設定するために、**ip verify unicast source reachable-via** コマンドが追加されました。	5.0(3)N1(1)	ip verify unicast source reachable-via

Cisco NX-OS Release 5.0(2)N2(1) の新機能および変更された機能に関する情報

表 3 では、Cisco NX-OS Release 5.0(2)N2(1) の新機能および変更された機能を要約し、その参照先を示しています。

表 3　Release 5.0(2)N2(1) の新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
Release 5.0(2)N2(1)			
DHCP スヌーピング	DHCP スヌーピングはスイッチと VLAN に対して設定できます。	5.0(2)N2(1)	clear ip dhcp snooping binding clear ip dhcp snooping statistics feature dhcp ip dhcp packet strict-validation ip dhcp snooping ip dhcp snooping information option ip dhcp snooping trust ip dhcp snooping verify mac-address ip dhcp snooping vlan ip source binding show ip dhcp snooping show ip dhcp snooping binding show ip dhcp snooping statistics show running-config dhcp show startup-config dhcp

Cisco NX-OS Release 5.0(2)N1(1) の新機能および変更された機能に関する情報

表 4 では、Cisco NX-OS Release 5.0(2)N1(1) の新機能および変更された機能を要約し、その参照先を示しています。

表 4　Release 5.0(2)N1(1) の新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
Release 5.0(2)N1(1)			
HTTP サーバのサポート	スイッチで HTTP または Hypertext Transfer Protocol Secure（HTTPS）をイネーブルにできます。	5.0(2)N1(1)	feature http-server

表 4　Release 5.0(2)N1(1) の新機能および変更された機能に関する情報 （続き）

機能	説明	変更されたリリース	参照先
権限レベル	RADIUS および TACACS+ サーバの役割のコマンド認可に対するロールの累積権限をイネーブルにできます。 また、高い権限レベルに移行できるようにすることも、特定の権限レベルのパスワードを設定することもできます。	5.0(2)N1(1)	enable enable secret feature privilege role name rule show privilege
VTY での ACL	仮想端末回線（VTY）の着信または発信トラフィックを制限するアクセス クラスを設定できます。	5.0(2)N1(1)	access-class ip access-class ipv6 access-class show running-config aclmgr show startup-config aclmgr
チェックポイントおよびロールバック	現在の実行コンフィギュレーションのスナップショットを取得するか、または指定されたチェックポイントにロールバックし、システムのアクティブ コンフィギュレーションを復元できます。	5.0(2)N1(1)	checkpoint clear checkpoint database rollback running-config show checkpoint show checkpoint summary show checkpoint system show checkpoint user show diff rollback-patch checkpoint show diff rollback-patch file show diff rollback-patch running-config show diff rollback-patch startup-config show rollback log

A コマンド

この章では、A で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

aaa accounting default

アカウンティングの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）方式を設定するには、**aaa accounting default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa accounting default {**group** {*group-list*} | **local**}

no aaa accounting default {**group** {*group-list*} | **local**}

構文の説明

group	サーバ グループをアカウンティングで使用するように指定します。
group-list	1 つ以上の設定済みの RADIUS サーバ グループを指定する空白で区切られたリストです。
local	ローカル データベースをアカウンティングで使用するように指定します。

コマンド デフォルト

ローカル データベースがデフォルトです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

group *group-list* メソッドは、以前に定義された一連の RADIUS サーバまたは TACACS+ サーバを参照します。ホスト サーバを設定するには、**radius server-host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

group 方式または **local** 方式を指定した場合にその方式が失敗すると、アカウンティング認証は失敗する可能性があります。

例

次に、AAA アカウンティングに任意の RADIUS サーバを設定する例を示します。

```
switch(config)# aaa accounting default group
```

関連コマンド

コマンド	説明
aaa group server radius	AAA RADIUS サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa accounting	AAA アカウンティング ステータス情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login console

コンソール ログインの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）認証方式を設定するには、**aaa authentication login console** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login console {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login console {**group** *group-list* [**none**] | **local** | **none**}

構文の説明

group	認証にサーバ グループを使用するように指定します。
group-list	RADIUS サーバ グループまたは TACACS+ サーバ グループのスペースで区切られたリストを指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • **tacacs+**：設定済みのすべての TACACS+ サーバ • 設定済みの任意の RADIUS サーバまたは TACACS+ サーバのサーバ グループ名
none	（任意）認証にユーザ名を使用するように指定します。
local	（任意）認証にローカル データベースを使用するように指定します。

コマンド デフォルト

ローカル データベース

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

group radius、**group tacacs+**、および **group** *group-list* の各方式は、以前に定義された一連の RADIUS または TACACS+ サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

group 方式または **local** 方式を指定した場合にその方式が失敗すると、認証は失敗する可能性があります。**none** 方式を単独または **group** 方式の後ろに指定した場合、認証は常に成功します。

例

次に、コンソール ログインの AAA 認証方式を設定する例を示します。

```
switch(config)# aaa authentication login console group radius
```

次に、デフォルトのコンソール ログインの AAA 認証方式に戻す例を示します。

```
switch(config)# no aaa authentication login console group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login default

デフォルトの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）認証方式を設定するには、**aaa authentication login default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

構文の説明

group	サーバ グループを認証で使用するように指定します。
group-list	RADIUS サーバ グループまたは TACACS+ サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • **tacacs+**：設定済みのすべての TACACS+ サーバ • 設定済みの任意の RADIUS サーバまたは TACACS+ サーバのサーバ グループ名
none	（任意）ユーザ名を認証で使用するように指定します。
local	（任意）ローカル データベースを認証で使用するように指定します。

コマンド デフォルト

ローカル データベース

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

group radius、**group tacacs+**、および **group** *group-list* の各方式は、以前に定義された一連の RADIUS または TACACS+ サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

group 方式または **local** 方式を指定した場合にその方式が失敗すると、認証は失敗します。**none** 方式を単独または **group** 方式の後ろに指定した場合、認証は常に成功します。

例

次に、コンソール ログインの AAA 認証方式を設定する例を示します。

```
switch(config)# aaa authentication login default group radius
```

次に、デフォルトのコンソール ログインの AAA 認証方式に戻す例を示します。

```
switch(config)# no aaa authentication login default group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login error-enable

コンソールに Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）認証失敗メッセージが表示されるように設定するには、**aaa authentication login error-enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login error-enable

no aaa authentication login error-enable

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

ログイン時にリモート AAA サーバからの応答がない場合には、ローカル ユーザ データベースへのロールオーバーによってログインが処理されます。このような状況では、ログイン失敗メッセージの表示がイネーブルに設定されている場合、次のメッセージが表示されます。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

例

次に、AAA 認証失敗メッセージのコンソールへの表示をイネーブルにする例を示します。

```
switch(config)# aaa authentication login error-enable
```

次に、AAA 認証失敗メッセージのコンソールへの表示をディセーブルにする例を示します。

```
switch(config)# no aaa authentication login error-enable
```

関連コマンド

コマンド	説明
show aaa authentication	AAA 認証失敗メッセージ表示のステータスを表示します。

aaa authentication login mschap enable

ログイン時の Microsoft Challenge Handshake Authentication Protocol（MS-CHAP; マイクロソフト チャレンジ ハンドシェーク認証プロトコル）認証をイネーブルにするには、**aaa authentication login mschap enable** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login mschap enable

no aaa authentication login mschap enable

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、MS-CHAP 認証をイネーブルにする例を示します。

```
switch(config)# aaa authentication login mschap enable
```

次に、MS-CHAP 認証をディセーブルにする例を示します。

```
switch(config)# no aaa authentication login mschap enable
```

関連コマンド

コマンド	説明
show aaa authentication	MS-CHAP 認証のステータスを表示します。

aaa authorization commands default

すべての EXEC コマンドでデフォルトの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）認可方式を設定するには、**aaa authorization commands default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authorization commands default [**group** *group-list*] [**local** | **none**]

no aaa authorization commands default [**group** *group-list*] [**local** | **none**]

構文の説明

group	（任意）認可にサーバ グループを使用するように指定します。
group-list	サーバ グループのリストです。 リストには、次のようなサーバ グループを含めることができます。 • **tacacs+**：設定済みのすべての TACACS+ サーバ • 設定済みの任意の TACACS+ サーバ グループ名 この名前は、サーバ グループのスペースで区切られたリストで指定でき、最大文字数は 127 です。
local	（任意）認可にローカル ロールベース データベースを使用するように指定します。
none	（任意）認可にデータベースを使用しないように指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.2(1)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

group tacacs+ 方式および **group** *group-list* 方式は、以前に定義された一連の TACACS+ サーバを指します。ホスト サーバを設定するには、**tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** または **none** を設定済みの場合、local 方式または none 方式だけが使用されます。

group 方式または **local** 方式を指定した場合にその方式が失敗すると、認可は失敗する可能性があります。**none** 方式を単独または **group** 方式の後ろに指定した場合、認可は常に成功します。

例

次に、EXEC コマンドでデフォルト AAA 認可方式を設定する例を示します。

```
switch(config)# aaa authorization commands default group TacGroup local
switch(config)#
```

次に、EXEC コマンドでデフォルト AAA 認可方式に戻す例を示します。

```
switch(config)# no aaa authorization commands default group TacGroup local
switch(config)#
```

関連コマンド

コマンド	説明
aaa authorization config-commands default	コンフィギュレーション コマンドでデフォルト AAA 認可方式を設定します。
aaa server group	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authorization config-commands default

すべてのコンフィギュレーション コマンドでデフォルトの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）認可方式を設定するには、**aaa authorization config-commands default** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authorization config-commands default [**group** *group-list*] [**local** | **none**]

no aaa authorization config-commands default [**group** *group-list*] [**local** | **none**]

構文の説明

group	（任意）認可にサーバ グループを使用するように指定します。
group-list	サーバ グループのリストです。 リストには、次のようなサーバ グループを含めることができます。 • **tacacs+**：設定済みのすべての TACACS+ サーバ • 設定済みの任意の TACACS+ サーバ グループ名 この名前は、サーバ グループのスペースで区切られたリストで指定でき、最大文字数は 127 です。
local	（任意）認可にローカル ロールベース データベースを使用するように指定します。
none	（任意）認可にデータベースを使用しないように指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.2(1)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

group tacacs+ 方式および **group** *group-list* 方式は、以前に定義された一連の TACACS+ サーバを指します。ホスト サーバを設定するには、**tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** または **none** を設定済みの場合、local 方式または none 方式だけが使用されます。

group 方式または **local** 方式を指定した場合にその方式が失敗すると、認可は失敗する可能性があります。**none** 方式を単独または **group** 方式の後ろに指定した場合、認可は常に成功します。

例

次に、コンフィギュレーション コマンドでデフォルト AAA 認可方式を設定する例を示します。

```
switch(config)# aaa authorization config-commands default group TacGroup local
switch(config)#
```

次に、コンフィギュレーション コマンドでデフォルト AAA 認可方式に戻す例を示します。

```
switch(config)# no aaa authorization config-commands default group TacGroup local
switch(config)#
```

関連コマンド

コマンド	説明
aaa authorization commands default	EXEC コマンドでデフォルト AAA 認可方式を設定します。
aaa server group	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authorization ssh-certificate

TACACS+ サーバのデフォルト認証、許可、およびアカウンティング（AAA）認可方式を設定するには、**aaa authorization ssh-certificate** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization ssh-certificate default {**group** *group-list* | **local**}

no aaa authorization ssh-certificate default {**group** *group-list* | **local**}

構文の説明

group	認可にサーバ グループを使用するように指定します。
group-list	サーバ グループのスペースで区切られたリスト。リストには、次のようなサーバ グループを含めることができます。 • **tacacs+**：設定済みのすべての TACACS+ サーバ • 設定済みの任意の TACACS+ サーバ グループ名 サーバ グループの名前は最大 127 文字です。
local	認証にローカル データベースを使用するように指定します。

コマンド デフォルト

local

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature tacacs+** コマンドを使用して TACACS+ 機能をイネーブルにする必要があります。

group tacacs+ 方式および **group** *group-list* 方式は、以前に定義された一連の TACACS+ サーバおよび LDAP サーバを指します。ホスト サーバを設定するには、**tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。デバイス上のサーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** を設定済みの場合、**local** 方式だけが使用されます。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認可は失敗する可能性があります。TACACS+ または LDAP サーバ グループ方式の後に、フォールバック方式を設定していない場合、すべてのサーバ グループが応答に失敗すると、認可が失敗します。

このコマンドには、ライセンスは必要ありません。

例

次に、デフォルトの AAA 認可方式として、証明書認証を使用してローカル データベースを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authorization ssh-certificate default local
switch(config)#
```

関連コマンド

コマンド	説明
aaa authorization ssh-publickey	デフォルト AAA 認可方式として、SSH 公開キーを使用したローカル認可を設定します。
feature tacacs+	TACACS+ 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。

aaa authorization ssh-publickey

TACACS+ サーバのデフォルトの AAA 許可方式として Secure Shell（SSH）公開キーでローカル認可を設定するには、**aaa authorization ssh-publickey** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authorization ssh-publickey default {**group** *group-list* | **local**}

no aaa authorization ssh-publickey default {**group** *group-list* | **local**}

構文の説明

group	認可にサーバ グループを使用するように指定します。
group-list	サーバ グループのスペースで区切られたリスト。サーバ グループの名前は最大 127 文字です。
local	認証にローカル データベースを使用するように指定します。

コマンド デフォルト

local

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。設定済みのすべてのサーバ グループで応答に失敗し、フォールバック方式として **local** を設定済みの場合、**local** 方式だけが使用されます。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認可は失敗する可能性があります。サーバ グループの方式のあとにフォールバック方式を設定していないと、すべてのサーバ グループから応答が得られなかった場合は認可が失敗します。

このコマンドには、ライセンスは必要ありません。

例

次に、デフォルトの AAA 認可方式として、SSH 公開キーを使用したローカル認可を設定する例を示します。

```
switch# configure terminal
switch(config)# aaa authorization ssh-publickey default local
switch(config)#
```

関連コマンド

コマンド	説明
aaa authorization ssh-certificate	デフォルト AAA 認可方式として、証明書認証を使用したローカル認可を設定します。
show aaa authorization	AAA 認可設定を表示します。

aaa group server radius

RADIUS サーバ グループを作成して、RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。RADIUS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa group server radius *group-name*

no aaa group server radius *group-name*

構文の説明

group-name	RADIUS サーバ グループ名です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、RADIUS サーバ グループを作成し、RADIUS サーバ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

次に、RADIUS サーバ グループを削除する例を示します。

```
switch(config)# no aaa group server radius RadServer
```

関連コマンド

コマンド	説明
show aaa groups	サーバ グループ情報を表示します。

aaa user default-role

リモート認証の Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サーバ管理者により割り当てられるデフォルト ロールをイネーブルにするには、**aaa user default-role** コマンドを使用します。デフォルト ロールをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa user default-role

no aaa user default-role

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、リモート認証の AAA サーバ管理者により割り当てられるデフォルト ロールをイネーブルにする例を示します。

```
switch(config)# aaa user default-role
switch(config)#
```

次に、リモート認証の AAA サーバ管理者により割り当てられるデフォルト ロールをディセーブルにする例を示します。

```
switch(config)# no aaa user default-role
switch(config)#
```

関連コマンド

コマンド	説明
show aaa user default-role	デフォルト ユーザのリモート認証のステータスを表示します。
show aaa authentication	AAA 認証情報を表示します。

access-class

特定の VTY（Cisco Nexus 5000 シリーズ スイッチ）とアクセス リスト内のアドレス間の着信および発信接続を制限するには、**access-class** コマンドを使用します。アクセス制限を解除するには、このコマンドの **no** 形式を使用します。

access-class *access-list-name* {**in** | **out**}

no access-class *access-list-name* {**in** | **out**}

構文の説明

access-list-name	IPv4 ACL クラスの名前。この名前には最大 64 文字までの英数字を指定できます。名前にはスペースまたは引用符を含めることはできません。
in	着信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。
out	発信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。

コマンド デフォルト

なし

コマンド モード

ライン コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

シスコ デバイスに対する Telnet または SSH を受け入れると、アクセス クラスを VTY にバインドしてデバイスへのアクセスを確保できます。

特定の端末ラインのアクセス リストを表示するには、**show line** コマンドを使用します。

例

次の例では、着信パケットを制限するために VTY 回線のアクセス クラスを設定する例を示します。

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# access-class ozi2 in
switch(config-line)#
```

次の例では、着信パケットを制限するアクセス クラスを削除する例を示します。

```
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)#
```

関連コマンド

コマンド	説明
ip access-class	IPv4 アクセス クラスを設定します。
show access-class	スイッチで設定されるアクセス リストを表示します。
show line	特定の端末ラインのアクセス リストを表示します。
show running-config aclmgr	ACL の実行コンフィギュレーションを表示します。
ssh	IPv4 を使用して SSH セッションを開始します。
telnet	IPv4 を使用して Telnet セッションを開始します。

action

パケットが VLAN アクセス コントロール リスト（VACL）の **permit** コマンドと一致した場合にスイッチが実行する処理を指定するには、**action** コマンドを使用します。**action** コマンドを削除するには、このコマンドの **no** 形式を使用します。

action {**drop forward**}

no action {**drop forward**}

構文の説明

drop	スイッチがパケットをドロップするように指定します。
forward	スイッチがパケットを、その宛先ポートに転送するように指定します。

コマンド デフォルト

なし

コマンド モード

VLAN アクセスマップ コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

action コマンドでは、**match** コマンドによって指定された ACL 内の条件にパケットが一致した場合に、デバイスが実行する処理を指定します。

例

次に、vlan-map-01 という名前で VLAN アクセス マップを作成して、そのマップに ip-acl-01 という名前の IPv4 ACL を割り当て、スイッチが ACL に一致するパケットを転送するよう指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
statistics	アクセス コントロール リストまたは VLAN アクセス マップの統計情報をイネーブルにします。

コマンド	説明
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

arp access-list

Address Resolution Protocol（ARP; アドレス解決プロトコル）ACL を作成するか、特定の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始するには、**arp access-list** コマンドを使用します。ARP ACL を削除するには、このコマンドの **no** 形式を使用します。

arp access-list *access-list-name*

no arp access-list *access-list-name*

構文の説明

access-list-name	ARP ACL の名前。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。名前にはスペースまたは引用符を含めることはできません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

（注） Cisco NX-OS Release 5.1(3)N1(1) 以降、ARP アクセス リストは、Control Plane Policing（CoPP）に対してだけサポートされます。

DHCP スヌーピングを使用できない場合は、ARP ACL を使用して ARP トラフィックをフィルタリングします。

デフォルトでは、ARP ACL は定義されていません。

例

次に、copp-arp-acl という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# arp access-list copp-arp-acl
switch(config-arp-acl)#
```

関連コマンド

コマンド	説明
deny（ARP）	ARP ACL に拒否（deny）ルールを設定します。

コマンド	説明
permit（ARP）	ARP ACL の許可ルールを設定します。
show arp access-lists	すべての ARP ACL または特定の ARP ACL を表示します。

C コマンド

この章では、C で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

checkpoint

現在の実行コンフィギュレーションのスナップショットを作成し、ASCII 形式のファイル システムにスナップショットを保存するには、**checkpoint** コマンドを使用します。

checkpoint [*checkpoint-name* [**description** *descp-text* [*...***description** *descp-text*]] | **description** *descp-text* | **file** {**bootflash:** | **volatile:**}[*//server*][*directory/*][*filename*]]

no checkpoint [*checkpoint-name* | **description** *descp-text* | **file** {**bootflash:** | **volatile:**}[*//server*][*directory/*][*filename*]]

構文の説明

checkpoint-name	（任意）チェックポイント名。名前は、最大 32 文字まで指定できます。
description *descp-text*	（任意）指定されたチェックポイントの説明を指定します。テキストは最大 80 文字で、スペースを含めることができます。
file	（任意）コンフィギュレーション ロールバック チェックポイントを保存するファイルが作成されるように指定します。
bootflash:	書き込み可能なブートフラッシュ ローカル ストレージ ファイル システムを指定します。
volatile:	揮発性の書き込み可能なローカル ストレージ ファイル システムを指定します。
//server	（任意）サーバの名前。有効な値は、**///**、**//module-1/**、**//sup-1/**、**//sup-active/** または **//sup-local/** です。2 個のスラッシュ（//）を含む必要があります。
directory/	（任意）ディレクトリの名前。ディレクトリ名では、大文字と小文字が区別されます。
filename	（任意）チェックポイント コンフィギュレーション ファイルの名前。ファイル名では、大文字と小文字が区別されます。

（注） *filesystem*://*server*/*directory*/*filename* ストリングにはスペースを含めることはできません。この文字列の各要素は、コロン（:）とスラッシュ（/）で区切ります。

コマンド デフォルト

自動的にチェックポイント名（user-checkpoint-*number*）を生成します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

チェックポイントはスイッチに対してローカルです。チェックポイントを作成すると、現在の実行コンフィギュレーションのスナップショットがチェックポイント ファイルに保存されます。チェックポイント名を指定しなかった場合、Cisco NX-OS はチェックポイント名を **user-checkpoint-***number* に設定します。ここで *number* は 1 ～ 10 の値です。

Fibre Channel over Ethernet（FCoE）がスイッチでイネーブルになっている場合、アクティブ コンフィギュレーションをチェックポイント状態に復元できません。FCoE がイネーブルのスイッチでチェックポイントを作成すると、次のエラー メッセージが表示されます。

```
switch# checkpoint chkpoint-1
ERROR: ascii-cfg: FCOE is enabled. Disbaling rollback module (err_id 0x405F004C)
switch#
```

FCoE がディセーブルのスイッチでチェックポイントを作成すると、次のメッセージが表示されます。

```
switch# checkpoint chkpoint-1
...Done
switch#
```

1 つのスイッチで作成できるコンフィギュレーションの最大チェックポイント数は 10 です。チェックポイント数が上限に達すると、最も古いエントリが削除されます。

あるスイッチのチェックポイント ファイルを別のスイッチに適用することはできません。チェックポイントのファイル名の先頭を *system* にすることはできません。

チェックポイント ファイルは、直接アクセスまたは変更できないテキスト ファイルとして保存されます。チェックポイントがシステムから消去されると、関連するチェックポイント コンフィギュレーション ファイルが削除されます。

例

次に、チェックポイントを作成する例を示します。

```
switch# checkpoint
...
user-checkpoint-4 created Successfully

Done
switch#
```

次に chkpnt-1 という名前のチェックポイントを作成する例を示します。目的を定義します。

```
switch# checkpoint chkpnt-1 description Checkpoint to save current configuration, Sep 9
10:02 A.M.
switch#
```

次に、ブートフラッシュ ストレージ システムに chkpnt_configSep9-1.txt という名前のチェックポイント コンフィギュレーション ファイルを作成する例を示します。

```
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
switch#
```

次に chkpnt-1 という名前のチェックポイントを削除する例を示します。

```
switch# no checkpoint chkpnt-1
switch#
```

関連コマンド

コマンド	説明
clear checkpoint	スイッチ上でチェックポイントをクリアします。
rollback	保存されたすべてのチェックポイントにスイッチをロールバックします。

コマンド	説明
show checkpoint all	スイッチに設定されているすべてのチェックポイントを表示します。
show checkpoint summary	スイッチに設定されているすべてのチェックポイントの要約を表示します。
show checkpoint summary user	ユーザによって作成されたすべてのチェックポイントを表示します。
show checkpoint system	システムで自動的に作成されたすべてのチェックポイントを表示します。

clear access-list counters

すべてまたは 1 つの IPv4 アクセス コントロール リスト（ACL）のカウンタをクリアするには、**clear access-list counters** コマンドを使用します。

clear access-list counters [*access-list-name*]

構文の説明

access-list-name	（任意）スイッチがそのカウンタをクリアする IPv4 ACL の名前です。この名前には最大 64 文字までの英数字を指定できます。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、すべての IPv4 ACL のカウンタをクリアする例を示します。

```
switch# clear access-list counters
```

次に、acl-ipv4-01 という名前の IPv4 ACL のカウンタをクリアする例を示します。

```
switch# clear access-list counters acl-ipv4-01
```

関連コマンド

コマンド	説明
access-class	IPv4 ACL を VTY 回線に適用します。
ip access-group	IPv4 ACL をインターフェイスに適用します。
ip access-list	IPv4 ACL を設定します。
show access-lists	1 つまたはすべての IPv4 ACL、IPv6 ACL、および MAC ACL に関する情報を表示します。
show ip access-lists	1 つまたはすべての IPv4 ACL に関する情報を表示します。

clear accounting log

アカウンティング ログをクリアするには、**clear accounting log** コマンドを使用します。

clear accounting log

構文の説明　このコマンドには、引数またはキーワードはありません。

コマンド デフォルト　なし

コマンド モード　EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例　次に、アカウンティング ログをクリアする例を示します。

```
switch# clear accounting log
```

関連コマンド

コマンド	説明
show accounting log	アカウンティング ログを表示します。

clear checkpoint database

スイッチで設定されたチェックポイントをクリアするには、**clear checkpoint database** コマンドを使用します。

clear checkpoint database [**system** | **user**]

構文の説明

system	システム チェックポイントのコンフィギュレーション ロールバック チェックポイント データベースをクリアします。
user	ユーザ チェックポイントのコンフィギュレーション ロールバック チェックポイント データベースをクリアします。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、設定済みチェックポイントをクリアする例を示します。

```
switch# clear checkpoint database
.Done
switch#
```

関連コマンド

コマンド	変更内容
checkpoint	チェックポイントを作成します。
show checkpoint	すべての設定済みチェックポイントを表示します。

clear ip arp

Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブルおよび統計情報をクリアするには、**clear ip arp** コマンドを使用します。

clear ip arp [**vlan** *vlan-id* [**force-delete** | **vrf** {*vrf-name* | **all** | **default** | **management**}]]

構文の説明

vlan *vlan-id*	（任意）指定した VLAN の ARP 情報をクリアします。内部使用に予約されている VLAN を除き、有効な範囲は 1 ～ 4094 秒です。
force-delete	（任意）更新せずに ARP テーブルからエントリをクリアします。
vrf	（任意）ARP テーブルからクリアする Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）を指定します。
vrf-name	VRF 名。名前は最大 32 文字の英数字で、大文字と小文字が区別されます。
all	ARP テーブルからすべての VRF エントリがクリアされるよう指定します。
default	ARP テーブルからデフォルトの VRF エントリがクリアされるよう指定します。
management	ARP テーブルから管理 VRF エントリがクリアされるよう指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
4.2(1)N1(1)	このコマンドが追加されました。

例

次に、ARP テーブル統計情報をクリアする例を示します。

```
switch# clear ip arp
switch#
```

次に、VRF vlan-vrf を持つ VLAN 10 の ARP テーブル統計情報をクリアする例を示します。

```
switch# clear ip arp vlan 10 vrf vlan-vrf
switch#
```

関連コマンド

コマンド	説明
show ip arp	ARP 設定ステータスを表示します。

clear ip arp inspection log

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）ログ バッファをクリアするには、**clear ip arp inspection log** コマンドを使用します。

clear ip arp inspection log

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

例

次に、DAI ロギング バッファをクリアする例を示します。

```
switch# clear ip arp inspection log
switch#
```

関連コマンド

コマンド	説明
ip arp inspection log-buffer entries	DAI のログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection log	DAI のログ設定を表示します。
show ip arp inspection statistics	DAI 統計情報を表示します。

clear ip arp inspection statistics vlan

指定の VLAN のダイナミック ARP インスペクション（DAI）統計情報をクリアするには、**clear ip arp inspection statistics vlan** コマンドを使用します。

clear ip arp inspection statistics vlan *vlan-list*

構文の説明

vlan *vlan-list*	このコマンドによってその DAI 統計情報がクリアされる VLAN を指定します。*vlan-list* 引数は 1 つの VLAN ID、VLAN ID の範囲、カンマ区切りの ID と範囲を指定できます。有効な VLAN ID は 1 ～ 4094 です。内部スイッチ用に予約されている VLAN は除きます。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

例

次に、VLAN 2 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 2
switch#
```

次に、VLAN 5 ～ 12 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 5-12
switch#
```

次に、VLAN 2 および VLAN 5 ～ 12 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 2,5-12
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ロギング バッファをクリアします。
ip arp inspection log-buffer	DAI のログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection vlan	VLAN の指定されたリストの DAI ステータスを表示します。

clear ip dhcp snooping binding

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング バインディング データベースをクリアするには、**clear ip dhcp snooping binding** コマンドを使用します。

clear ip dhcp snooping binding [**vlan** *vlan-id* [**mac** *mac-address* **ip** *ip-address*] [**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*}]]

構文の説明

vlan *vlan-id*	（任意）クリアする DHCP スヌーピング バインディング データベース エントリの VLAN ID を指定します。有効な VLAN ID は 1 ～ 4094 です。内部スイッチ用に予約されている VLAN は除きます。
mac-address *mac-address*	（任意）クリアするバインディング データベース エントリの MAC アドレスを指定します。ドット付き 16 進表記で *mac-address* 引数を入力します。
ip *ip-address*	（任意）クリアするバインディング データベース エントリの IPv4 アドレスを指定します。ドット付き 10 進表記で *ip-address* 引数を入力します。
interface	（任意）Ethernet または EtherChannel インターフェイスを指定します。
ethernet *slot*/*port*	（任意）クリアするバインディング データベース エントリのイーサネット インターフェイスを指定します。
port-channel *channel-number*	（任意）クリアするバインディング データベース エントリのイーサネット ポート チャネルを指定します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

例

次に、DHCP スヌーピング バインディング データベースをクリアする例を示します。

```
switch# clear ip dhcp snooping binding
switch#
```

次に、DHCP スヌーピング バインディング データベースの特定のエントリをクリアする例を示します。

```
switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface
ethernet 2/11
switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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。
show ip dhcp snooping binding	スタティック IP ソース エントリを含めて、IP-MAC アドレス バインディングを表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

clear ip dhcp snooping statistics

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング統計情報をクリアするには、**clear ip dhcp snooping statistics** コマンドを使用します。

clear ip dhcp snooping statistics

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

例

次に、DHCP 統計情報をクリアする例を示します。

```
switch# clear ip dhcp snooping statistics
switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

D コマンド

この章では、D で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

deadtime

RADIUS または TACACS+ サーバ グループのデッド タイム間隔を設定するには、**deadtime** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

deadtime *minutes*

no deadtime *minutes*

構文の説明

minutes	間隔の分数です。有効な範囲は 0 ～ 1440 分です。デッド タイム間隔をゼロ（0）に設定すると、タイマーがディセーブルになります。

コマンド デフォルト

0 分

コマンド モード

RADlUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、RADIUS サーバ グループのデッド タイム間隔を 2 分に設定する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

次に、TACACS+ サーバ グループのデッド タイム間隔を 5 分に設定する例を示します。

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
```

次に、デッド タイム間隔をデフォルト値に戻す例を示します。

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ グループ情報を表示します。

コマンド	説明
show tacacs-server groups	TACACS+ サーバ グループ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

deny（ARP）

条件に一致する ARP トラフィックを拒否する ARP ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本構文

[*sequence-number*] **deny ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

no *sequence-number*

no deny ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

構文の説明

sequence-number	（任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にデバイスがコマンドを挿入します。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しないと、デバイスによって、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
ip	ルールの IP アドレス部分を指定します。
any	（任意）任意のホストがルールの **any** キーワードが含まれる部分に一致するように指定します。**any** を使用すると、送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、および宛先 MAC アドレスを指定できます。
host *sender-IP*	（任意）ARP パケットの送信元 IP アドレスが *sender-IP* 引数の値に一致する場合だけ、ルールが ARP パケットに一致するように指定します。*sender-IP* 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。
sender-IP *sender-IP-mask*	（任意）パケットの送信元 IP アドレスが一致する可能性のある IPv4 アドレスおよび IPv4 アドレス セットのマスク。*sender-IP* 引数と *sender-IP-mask* 引数は、ドット付き 10 進表記で指定する必要があります。*sender-IP-mask* 引数に 255.255.255.255 を指定すると、**host** キーワードを使用した場合と同じ結果になります。
mac	ルールの MAC アドレスの部分を指定します。

コマンド デフォルト

なし

コマンド モード

ARP ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

（注） Cisco NX-OS Release 5.1(3)N1(1) 以降、ARP アクセス リストは、Control Plane Policing（CoPP）に対してだけサポートされます。**deny** コマンドは CoPP ARP ACL では無視されます。

新しく作成した ARP ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号がルールに割り当てられます。

パケットに ARP ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、デバイスはシーケンス番号が最も低いルールを施行します。

例

次に、copp-arp-acl という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始し、192.0.32.14/24 サブネット内にある送信者の IP アドレスを含み、それを copp-arp-acl クラスに関連づける ARP 要求メッセージを拒否するルールを追加する例を示します。

```
switch# configure terminal
switch(config)# arp access-list copp-arp-acl
switch(config-arp-acl)# deny ip 192.0.32.14 255.255.255.0 mac any
switch(config-arp-acl)#
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を設定します。
permit（ARP）	ARP ACL の許可ルールを設定します。
remark	ACL に備考を設定します。
show arp access-lists	すべての ARP ACL または 1 つの ARP ACL を表示します。

deny（IPv4）

条件と一致するトラフィックを拒否する IPv4 アクセス コントロール リスト（ACL）ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本構文

[*sequence-number*] **deny** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no deny *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

インターネット制御メッセージ プロトコル

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

インターネット グループ管理プロトコル

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

インターネット プロトコル v4（IPv4）

[*sequence-number*] **deny ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

伝送制御プロトコル（TCP）

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*] [*flags*] [**established**]

ユーザ データグラム プロトコル

[*sequence-number*] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

構文の説明

sequence-number	（任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にスイッチがコマンドを挿入します。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、スイッチは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
protocol	ルールで一致させるパケットのプロトコルの名前または番号。有効な番号は、0 ～ 255 です。有効なプロトコル名は、次のキーワードです。 • **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数を使用できます。 • **igmp**：ルールを IGMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*igmp-type* 引数を使用できます。 • **ip**：ルールをすべての IPv4 トラフィックに適用するように指定します。このキーワードを使用する場合は、すべての IPv4 プロトコルに適用される他のキーワードおよび引数だけを使用できます。使用できるキーワードには次のものがあります。 – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **tcp**：ルールを TCP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*flags* 引数および *operator* 引数、**portgroup** キーワードおよび **established** キーワードを使用できます。 • **udp**：ルールを UDP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。
source	ルールで一致させる送信元 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。

dscp *dscp*	（任意）IP ヘッダーの DSCP フィールドに特定の 6 ビット diffserv（ディファレンシエーテッド サービス）値が設定されているパケットだけをルールと一致させるように指定します。*dscp* 引数には、次の数値またはキーワードのいずれかを指定します。 • 0 ～ 63：DSCP フィールドの 6 ビットと同等の 10 進数。たとえば 10 を指定した場合、ルールは DSCP フィールドのビットが 001010 であるパケットだけに一致します。 • **af11**：Assured Forwarding（AF）クラス 1、低い廃棄確率（001010） • **af12**：AF クラス 1、中程度の廃棄確率（001100） • **af13**：AF クラス 1、高い廃棄確率（001110） • **af21**：AF クラス 2、低い廃棄確率（010010） • **af22**：AF クラス 2、中程度の廃棄確率（010100） • **af23**：AF クラス 2、高い廃棄確率（010110） • **af31**：AF クラス 3、低い廃棄確率（011010） • **af32**：AF クラス 3、中程度の廃棄確率（011100） • **af33**：AF クラス 3、高い廃棄確率（011110） • **af41**：AF クラス 4、低い廃棄確率（100010） • **af42**：AF クラス 4、中程度の廃棄確率（100100） • **af43**：AF クラス 4、高い廃棄確率（100110） • **cs1**：Class-selector（CS）1、優先順位 1（001000） • **cs2**：CS2、優先順位 2（010000） • **cs3**：CS3、優先順位 3（011000） • **cs4**：CS4、優先順位 4（100000） • **cs5**：CS5、優先順位 5（101000） • **cs6**：CS6、優先順位 6（110000） • **cs7**：CS7、優先順位 7（111000） • **default**：デフォルトの DSCP 値（000000） • **ef**：Expedited Forwarding（EF; 緊急転送）（101110）

precedence *precedence*	（任意）*precedence* 引数で指定された値が IP Precedence フィールドに設定されているパケットだけをルールと一致させるように指定します。*precedence* 引数には、次の数値またはキーワードを指定します。 • 0 ～ 7 : IP Precedence フィールドの 3 ビットと同等の 10 進数。たとえば、3 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します : 011 • **critical** : 優先順位 5（101） • **flash** : 優先順位 3（011） • **flash-override** : 優先順位 4（100） • **immediate** : 優先順位 2（010） • **internet** : 優先順位 6（110） • **network** : 優先順位 7（111） • **priority** : 優先順位 1（001） • **routine** : 優先順位 0（000）
fragments	（任意）非初期フラグメントであるパケットだけをルールと一致させるように指定します。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定したルールには指定できません。これらのオプションをスイッチが評価するために必要な情報は、初期フラグメントだけに含まれているからです。
time-range *time-range-name*	（任意）このルールに適用する時間範囲を指定します。**time-range** コマンドを使用して時間範囲を設定できます。
icmp-message	（任意 : IGMP 限定）指定した ICMP メッセージ タイプのパケットだけに対して一致するルールです。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」の「ICMP メッセージ タイプ」にリストされているキーワードの 1 つを指定します。
igmp-message	（任意 : IGMP 限定）指定した IGMP メッセージ タイプのパケットだけに対して一致するルールです。*igmp-message* 引数には、0 ～ 15 の整数である IGMP メッセージ番号を指定します。また、次のいずれかのキーワードを指定できます。 • **dvmrp** : Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル） • **host-query** : ホスト クエリー • **host-report** : ホスト レポート • **pim** : Protocol Independent Multicast（PIM） • **trace** : マルチキャスト トレース

operator port [*port*]	（任意：TCP および UDP 限定）*operator* 引数および *port* 引数の条件と一致する送信元ポートから送信されたパケット、または一致する宛先ポートに送信されたパケットだけを、ルールと一致させます。これらの引数が送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定します。有効な番号は 0 ～ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の *port* 引数は、*operator* 引数が範囲である場合だけ必要です。 *operator* 引数には、次のいずれかのキーワードを指定する必要があります。 • **eq**：パケットのポートが *port* 引数と同等である場合だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数以上で、2 番目の *port* 引数以下である場合だけ一致します。
portgroup *portgroup*	（任意：TCP および UDP 限定）*portgroup* 引数で指定された IP ポート グループ オブジェクトのメンバである送信元ポートから送信されたパケット、またはメンバである宛先ポートに送信されたパケットだけを、ルールと一致させるように指定します。ポート グループ オブジェクトが送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 IP ポート グループ オブジェクトを作成および変更するには、**object-group ip port** コマンドを使用します。
flags	（任意：TCP 限定）特定の TCP コントロール ビット フラグがオンに設定されたパケットだけを、ルールと一致させます。*flags* 引数の値には、次の 1 つ以上のキーワードを指定する必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	（任意：TCP 限定）確立された TCP 接続に属するパケットだけをルールと一致させるように指定します。スイッチは、ACK または RST ビットが設定されている TCP パケットが、確立された接続に属していると見なします。

コマンド デフォルト　新しく作成した IPv4 ACL には、ルールは含まれていません。

シーケンス番号を指定しない場合は、スイッチによって ACL の最後のルールのシーケンス番号よりも 10 大きい番号がルールに割り当てられます。

コマンド モード　IPv4 ACL コンフィギュレーション

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン　スイッチは、パケットに IPv4 ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。スイッチで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、スイッチはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。各ルールでは、これらの引数の 1 つを指定する際に使用した方法が、他の引数の指定方法に影響を与えることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびネットワーク ワイルドカード：IPv4 アドレスおよびネットワーク ワイルドカードを使用して、送信元または宛先とするホストまたはネットワークを指定できます。構文は次のとおりです。

  IPv4-address network-wildcard

  次に、192.168.67.0 サブネットの IPv4 アドレスおよびネットワーク ワイルドカードを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
  ```

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）: IPv4 アドレスおよび VLSM を使用して、送信元または宛先とするホストまたはネットワークを指定できます。構文は次のとおりです。

  IPv4-address/prefix-len

  次に、192.168.67.0 サブネットの IPv4 アドレスおよび VLSM を使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny udp 192.168.67.0/24 any
  ```

- ホスト アドレス：**host** キーワードおよび IPv4 アドレスを使用して、送信元または宛先とするホストを指定できます。構文は次のとおりです。

  host *IPv4-address*

  この構文は、*IPv4-address*/32 および *IPv4-address* 0.0.0.0 と同じです。

  次に、**host** キーワードおよび 192.168.67.132 IPv4 アドレスを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny icmp host 192.168.67.132 any
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先として任意の IPv4 アドレスを指定できます。**any** キーワードの使用例は、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

ICMP メッセージ タイプ

igmp-message 引数には、0 ～ 255 の整数である ICMP メッセージ番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **administratively-prohibited**：管理上の禁止
- **alternate-address**：代替アドレス
- **conversion-error**：データグラム変換
- **dod-host-prohibited**：ホスト禁止
- **dod-net-prohibited**：ネット禁止
- **echo**：エコー（ping）
- **echo-reply**：エコー応答
- **general-parameter-problem**：パラメータの問題
- **host-isolated**：ホスト分離
- **host-precedence-unreachable**：優先順位のホスト到達不能
- **host-redirect**：ホスト リダイレクト
- **host-tos-redirect**：ToS ホスト リダイレクト
- **host-tos-unreachable**：ToS ホスト到達不能
- **host-unknown**：ホスト未知
- **host-unreachable**：ホスト到達不能
- **information-reply**：情報応答
- **information-request**：情報要求
- **mask-reply**：マスク応答
- **mask-request**：マスク要求
- **mobile-redirect**：モバイル ホスト リダイレクト
- **net-redirect**：ネットワーク リダイレクト
- **net-tos-redirect**：ToS ネット リダイレクト
- **net-tos-unreachable**：ToS ネット到達不能
- **net-unreachable**：ネット到達不能
- **network-unknown**：ネットワーク未知
- **no-room-for-option**：パラメータが必要だが空きなし
- **option-missing**：パラメータが必要だが存在しない
- **packet-too-big**：フラグメンテーションが必要、DF 設定
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：ポート到達不能
- **precedence-unreachable**：優先順位カットオフ
- **protocol-unreachable**：プロトコル到達不能
- **reassembly-timeout**：再構成タイムアウト
- **redirect**：すべてのリダイレクト
- **router-advertisement**：ルータ ディスカバリ アドバタイズメント
- **router-solicitation**：ルータ ディスカバリ要求
- **source-quench**：送信元抑制
- **source-route-failed**：送信元ルート障害

- **time-exceeded**：すべての時間超過メッセージ
- **timestamp-reply**：タイム スタンプ付きの応答
- **timestamp-request**：タイム スタンプ付きの要求
- **traceroute**：トレースルート
- **ttl-exceeded**：TTL 超過
- **unreachable**：すべての到達不能

TCP ポート名

protocol 引数に **tcp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である TCP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **bgp**：Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）
- **chargen**：キャラクタ ジェネレータ（19）
- **cmd**：リモート コマンド（rcmd、514）
- **daytime**：デイタイム（13）
- **discard**：廃棄（9）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **drip**：Dynamic Routing Information Protocol（DRIP; ダイナミック ルーティング情報プロトコル）（3949）
- **echo**：エコー（7）
- **exec**：EXEC（rsh、512）
- **finger**：フィンガー（79）
- **ftp**：File Transfer Protocol（FTP; ファイル転送プロトコル）（21）
- **ftp-data**：FTP データ接続（2）
- **gopher**：Gopher（7）
- **hostname**：NIC ホストネーム サーバ（11）
- **ident**：Ident プロトコル（113）
- **irc**：Internet Relay Chat（IRC; インターネット リレー チャット）（194）
- **klogin**：Kerberos ログイン（543）
- **kshell**：Kerberos シェル（544）
- **login**：ログイン（rlogin、513）
- **lpd**：プリンタ サービス（515）
- **nntp**：Network News Transport Protocol（NNTP）（119）
- **pim-auto-rp**：PIM Auto-RP（496）
- **pop2**：Post Office Protocol v2（POP2）（19）
- **pop3**：Post Office Protocol v3（POP3）（11）
- **smtp**：Simple Mail Transport Protocol（SMTP; シンプル メール転送プロトコル）（25）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）

- **telnet**：Telnet（23）
- **time**：Time（37）
- **uucp**：UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）（54）
- **whois**：WHOIS/NICNAME（43）
- **www**：World Wide Web（HTTP、8）

UDP ポート名

protocol 引数に **udp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である UDP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **biff**：BIFF（メール通知、comsat、512）
- **bootpc**：Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）
- **bootps**：ブートストラップ プロトコル（BOOTP）サーバ（67）
- **discard**：廃棄（9）
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **echo**：エコー（7）
- **isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（5）
- **mobile-ip**：モバイル IP レジストレーション（434）
- **nameserver**：IEN116 ネーム サービス（旧式、42）
- **netbios-dgm**：NetBIOS データグラム サービス（138）
- **netbios-ns**：NetBIOS ネーム サービス（137）
- **netbios-ss**：NetBIOS セッション サービス（139）
- **non500-isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（45）
- **ntp**：Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）
- **pim-auto-rp**：PIM Auto-RP（496）
- **rip**：Routing Information Protocol（RIP）（ルータ、in.routed、52）
- **snmp**：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）
- **snmptrap**：SNMP トラップ（162）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **syslog**：システム ロギング（514）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）
- **tftp**：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（69）
- **time**：Time（37）
- **who**：Who サービス（rwho、513）
- **xdmcp**：X Display Manager Control Protocol（XDMCP）（177）

例

次に、10.23.0.0 および 192.168.37.0 ネットワークから 10.176.0.0 ネットワークへのすべての TCP と UDP のトラフィックを拒否するルール、およびその他のすべての IPv4 トラフィックを許可する最後のルールを持つ、acl-lab-01 という名前の IPv4 ACL を設定する例を示します。

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# deny udp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
permit（IPv4）	IPv4 ACL に許可（permit）ルールを設定します。
remark	IPv4 ACL でリマークを設定します。
show ip access-list	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。

deny（IPv6）

条件と一致するトラフィックを拒否する IPv6 アクセス コントロール リスト（ACL）ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。条件と一致するトラフィックを拒否する IPv6 ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本構文

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

no deny *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**]
[**time-range** *time-range-name*]

no *sequence-number*

インターネット制御メッセージ プロトコル

[*sequence-number* | **no**] **deny icmp** *source destination* [*icmp-message*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

インターネット プロトコル v6（IPv6）

[*sequence-number*] **deny ipv6** *source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*]
[**fragments**] [**time-range** *time-range-name*]

Stream Control Transmission Protocol

[*sequence-number* | **no**] **deny sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

伝送制御プロトコル（TCP）

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*] [*flags*]
[**established**]

ユーザ データグラム プロトコル

[*sequence-number* | **no**] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

構文の説明

sequence-number	（任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にデバイスがコマンドを挿入します。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しないと、デバイスによって、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
protocol	ルールで一致させるパケットのプロトコルの名前または番号。有効な番号は、0 ～ 255 です。有効なプロトコル名は、次のキーワードです。 • **ahp**：ルールを Authentication Header Protocol（AHP; 認証ヘッダー プロトコル）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **esp**：ルールを Encapsulating Security Payload（ESP）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数を使用できます。 • **ipv6**：ルールをすべての IPv6 トラフィックに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **pcp**：ルールを Payload Compression Protocol（PCP; ペイロード圧縮プロトコル）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **sctp**：ルールを Stream Control Transmission Protocol（SCTP）トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。 • **tcp**：ルールを TCP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*flags* 引数および *operator* 引数、**portgroup** キーワードおよび **established** キーワードを使用できます。 • **udp**：ルールを UDP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。
source	ルールで一致させる送信元 IPv6 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。

destination	ルールで一致させる宛先 IPv6 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
dscp *dscp*	（任意）IPv6 ヘッダーの DSCP フィールドに特定の 6 ビット diffserv（ディファレンシエーテッド サービス）値が設定されているパケットだけをルールと一致させるように指定します。*dscp* 引数には、次の数値またはキーワードのいずれかを指定します。 • 0 ～ 63 : DSCP フィールドの 6 ビットと同等の 10 進数。たとえば、10 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します : 001010 • **af11** : Assured Forwarding（AF）クラス 1、低い廃棄確率（001010） • **af12** : AF クラス 1、中程度の廃棄確率（001100） • **af13** : AF クラス 1、高い廃棄確率（001110） • **af21** : AF クラス 2、低い廃棄確率（010010） • **af22** : AF クラス 2、中程度の廃棄確率（010100） • **af23** : AF クラス 2、高い廃棄確率（010110） • **af31** : AF クラス 3、低い廃棄確率（011010） • **af32** : AF クラス 3、中程度の廃棄確率（011100） • **af33** : AF クラス 3、高い廃棄確率（011110） • **af41** : AF クラス 4、低い廃棄確率（100010） • **af42** : AF クラス 4、中程度の廃棄確率（100100） • **af43** : AF クラス 4、高い廃棄確率（100110） • **cs1** : Class-selector（CS）1、優先順位 1（001000） • **cs2** : CS2、優先順位 2（010000） • **cs3** : CS3、優先順位 3（011000） • **cs4** : CS4、優先順位 4（100000） • **cs5** : CS5、優先順位 5（101000） • **cs6** : CS6、優先順位 6（110000） • **cs7** : CS7、優先順位 7（111000） • **default** : デフォルトの DSCP 値（000000） • **ef** : Expedited Forwarding（EF; 緊急転送）（101110）
flow-label *flow-label-value*	（任意）*flow-label-value* 引数で指定された値がフロー ラベル ヘッダー フィールドに設定されている IPv6 パケットだけをルールと一致させるように指定します。*flow-label-value* 引数は、0 ～ 1048575 の整数です。
fragments	（任意）非初期フラグメントであるパケットだけをルールと一致させるように指定します。デバイスでは、非初期フラグメントであるパケットが、ゼロと同等ではないフラグメント オフセットが含まれるフラグメント拡張ヘッダーを持つパケットと見なされます。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定したルールには指定できません。これらのオプションをデバイスが評価するために必要な情報は、初期フラグメントだけに含まれているためです。
time-range *time-range-name*	（任意）このルールに適用する時間範囲を指定します。**time-range** コマンドを使用して時間範囲を設定できます。

icmp-message	（ICMP 限定：任意）ルールと一致させる ICMPv6 メッセージのタイプ。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」の「ICMPv6 メッセージ タイプ」にリストされているキーワードの 1 つを指定します。
operator port [*port*]	（任意：TCP、UDP および SCTP 限定）*operator* 引数および *port* 引数の条件と一致する送信元ポートから送信されたパケット、または一致する宛先ポートに送信されたパケットだけを、ルールと一致させます。これらの引数が送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定します。有効な番号は 0 ～ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の *port* 引数は、*operator* 引数が範囲である場合だけ必要です。 *operator* 引数には、次のいずれかのキーワードを指定する必要があります。 • **eq**：パケットのポートが *port* 引数と同等である場合だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数以上で、2 番目の *port* 引数以下である場合だけ一致します。
portgroup *portgroup*	（任意：TCP、UDP、および SCTP 限定）*portgroup* 引数で指定された IP ポート グループ オブジェクトのメンバである送信元ポートから送信されたパケット、またはメンバである宛先ポートに送信されたパケットだけを、ルールと一致させるように指定します。ポート グループ オブジェクトが送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 IP ポート グループ オブジェクトを作成および変更するには、**object-group ip port** コマンドを使用します。
flags	（TCP 限定：任意）特定の TCP コントロール ビット フラグがオンに設定されたパケットだけを、ルールと一致させます。*flags* 引数の値には、次の 1 つ以上のキーワードを指定する必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	（TCP 限定：任意）確立された TCP 接続に属すパケットだけをルールと一致させるように指定します。デバイスは、ACK または RST ビットが設定されている TCP パケットが、確立された接続に属していると見なします。

コマンド デフォルト なし

コマンド モード　IPv6 ACL コンフィギュレーション

コマンド履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン　新しく作成した IPv6 ACL には、ルールは含まれていません。

デバイスは、パケットに IPv6 ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。デバイスで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、デバイスはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、1 つの引数の指定方法によって、他の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）: IPv6 アドレスおよび VLSM を使用して、送信元または宛先とするホストまたはネットワークを指定できます。構文は次のとおりです。

  IPv6-address/prefix-len

  次に、2001:0db8:85a3:: ネットワークの IPv6 アドレスおよび VLSM を使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny udp 2001:0db8:85a3::/48 any
  ```

- ホスト アドレス：**host** キーワードおよび IPv6 アドレスを使用して、送信元または宛先とするホストを指定できます。構文は次のとおりです。

  host *IPv6-address*

  この構文は、*IPv6-address*/128 と同じです。

  次に、**host** キーワードおよび 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 アドレスを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先として任意の IPv6 アドレスを指定できます。**any** キーワードの使用例は、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

ICMPv6 メッセージ タイプ

igmp-message 引数には、0 ～ 255 の整数である ICMPv6 メッセージ番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **beyond-scope**：範囲外の宛先
- **destination-unreachable**：宛先アドレスに到達不能
- **echo-reply**：エコー応答
- **echo-request**：エコー要求（ping）
- **header**：パラメータ ヘッダーの問題
- **hop-limit**：中継時にホップ制限を超過

- **mld-query**：マルチキャスト リスナー ディスカバリ クエリー
- **mld-reduction**：マルチキャスト リスナー ディスカバリ リダクション
- **mld-reduction**：マルチキャスト リスナー ディスカバリ レポート
- **nd-na**：ネイバー探索のネイバー アドバタイズメント
- **nd-ns**：ネイバー探索のネイバー送信要求
- **next-header**：パラメータの次のヘッダーの問題
- **no-admin**：管理者が宛先を禁止
- **no-route**：宛先へのルートなし
- **packet-too-big**：パケット サイズ超過
- **parameter-option**：パラメータ オプションの問題
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：ポート到達不能
- **reassembly-timeout**：再構成タイムアウト
- **redirect**：ネイバーのリダイレクト
- **renum-command**：ルータの番号付けコマンド
- **renum-result**：ルータの番号付けの結果
- **renum-seq-number**：ルータの番号付けのシーケンス番号リセット
- **router-advertisement**：ネイバー探索のルータ アドバタイズメント
- **router-renumbering**：すべてのルータの再番号付け
- **router-solicitation**：ネイバー探索のルータ送信要求
- **time-exceeded**：すべてのタイム超過メッセージ
- **unreachable**：すべての到達不能

TCP ポート名

protocol 引数に **tcp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である TCP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **bgp**：Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）
- **chargen**：キャラクタ ジェネレータ（19）
- **cmd**：リモート コマンド（rcmd、514）
- **daytime**：デイタイム（13）
- **discard**：廃棄（9）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **drip**：Dynamic Routing Information Protocol（DRIP; ダイナミック ルーティング情報プロトコル）（3949）
- **echo**：エコー（7）
- **exec**：Exec（rsh、512）
- **finger**：フィンガー（79）
- **ftp**：File Transfer Protocol（FTP; ファイル転送プロトコル）（21）
- **ftp-data**：FTP データ接続（2）

- **gopher**：Gopher（7）
- **hostname**：NIC ホストネーム サーバ（11）
- **ident**：Ident プロトコル（113）
- **irc**：Internet Relay Chat（IRC; インターネット リレー チャット）（194）
- **klogin**：Kerberos ログイン（543）
- **kshell**：Kerberos シェル（544）
- **login**：ログイン（rlogin、513）
- **lpd**：プリンタ サービス（515）
- **nntp**：Network News Transport Protocol（NNTP）（119）
- **pim-auto-rp**：PIM Auto-RP（496）
- **pop2**：Post Office Protocol v2（POP2）（19）
- **pop3**：Post Office Protocol v3（POP3）（11）
- **smtp**：Simple Mail Transport Protocol（SMTP; シンプル メール転送プロトコル）（25）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）
- **telnet**：Telnet（23）
- **time**：Time（37）
- **uucp**：UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）（54）
- **whois**：WHOIS/NICNAME（43）
- **www**：World Wide Web（HTTP、8）

UDP ポート名

protocol 引数に **udp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である UDP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **biff**：BIFF（メール通知、comsat、512）
- **bootpc**：Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）
- **bootps**：ブートストラップ プロトコル（BOOTP）サーバ（67）
- **discard**：廃棄（9）
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **echo**：エコー（7）
- **isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（5）
- **mobile-ip**：モバイル IP レジストレーション（434）
- **nameserver**：IEN116 ネーム サービス（旧式、42）
- **netbios-dgm**：NetBIOS データグラム サービス（138）
- **netbios-ns**：NetBIOS ネーム サービス（137）
- **netbios-ss**：NetBIOS セッション サービス（139）
- **non500-isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（45）

- **ntp**：Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）
- **pim-auto-rp**：PIM Auto-RP（496）
- **rip**：Routing Information Protocol（RIP）（ルータ、in.routed、52）
- **snmp**：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）
- **snmptrap**：SNMP トラップ（162）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **syslog**：システム ロギング（514）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）
- **tftp**：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（69）
- **time**：Time（37）
- **who**：Who サービス（rwho、513）
- **xdmcp**：X Display Manager Control Protocol（XDMCP）（177）

例

次に、acl-lab13-ipv6 という IPv6 ACL を作成し、2001:0db8:85a3:: ネットワークおよび 2001:0db8:69f2:: ネットワークから 2001:0db8:be03:2112:: ネットワークへのすべての TCP トラフィックおよび UDP トラフィックを拒否するルールを設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

次に、ipv6-eng-to-marketing という IPv6 ACL を作成し、eng_ipv6 という IPv6 アドレス オブジェクト グループから marketing_group という IPv6 アドレス オブジェクト グループへのすべての IPv6 トラフィックを拒否するルールを設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# deny ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 ACL を設定します。
permit（IPv6）	IPv6 ACL に許可（permit）ルールを設定します。
remark	ACL に備考を設定します。
time-range	時間範囲を設定します。

deny（MAC）

条件に一致するトラフィックを拒否する Media Access Control（MAC; メディア アクセス コントロール）アクセス コントロール リスト（ACL）+ ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no deny *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no *sequence-number*

構文の説明

sequence-number	（任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にスイッチがコマンドを挿入します。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、スイッチは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
source	ルールで一致させる送信元 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
protocol	（任意）ルールで一致させるプロトコルの番号。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なプロトコル名のリストは、「使用上のガイドライン」の「MAC プロトコル」を参照してください。
cos *cos-value*	（任意）IEEE 802.1Q ヘッダーに、*cos-value* 引数で指定したサービス クラス（CoS）値が含まれているパケットだけにルールが一致するように指定します。*cos-value* 引数は、0 ～ 7 の整数です。
vlan *vlan-id*	（任意）IEEE 802.1Q ヘッダーに、指定した VLAN ID が含まれているパケットだけにルールが一致するように指定します。*vlan-id* 引数は、1 ～ 4094 の整数に指定できます。

コマンド デフォルト

新しく作成した MAC ACL には、ルールは含まれていません。

シーケンス番号を指定しない場合は、スイッチによって ACL の最後のルールのシーケンス番号よりも 10 大きい番号がルールに割り当てられます。

コマンド モード

MAC ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは、パケットに MAC ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。スイッチで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、スイッチはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。各ルールでは、これらの引数の 1 つを指定する際に使用した方法が、他の引数の指定方法に影響を与えることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびマスク：MAC アドレスの後にマスクを指定して、1 つのアドレスまたはアドレスグループを指定できます。構文は次のとおりです。

  ```
  MAC-address MAC-mask
  ```

  次に、MAC アドレス 00c0.4f03.0a72 を持つ *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
  ```

  次に、*destination* 引数に、MAC ベンダー コードが 00603e のすべてのホストの MAC アドレスを指定する例を示します。

  ```
  switch(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先として任意の MAC アドレスを指定できます。**any** キーワードの使用例は、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

MAC プロトコル

protocol 引数には、MAC プロトコルの番号またはキーワードを指定します。プロトコル番号は、先頭に 0x が付く 4 バイトの 16 進数です。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なキーワードは、次のとおりです。

- **aarp**：Appletalk ARP（0x80f3）
- **appletalk**：Appletalk（0x809b）
- **decnet-iv**：DECnet Phase IV（0x6003）
- **diagnostic**：DEC 診断プロトコル（0x6005）
- **etype-6000**：Ethertype 0x6000（0x6000）
- **etype-8042**：Ethertype 0x8042（0x8042）
- **ip**：インターネット プロトコル v4（0x0800）
- **lat**：DEC LAT（0x6004）
- **lavc-sca**：DEC LAVC、SCA（0x6007）
- **mop-console**：DEC MOP リモート コンソール（0x6002）
- **mop-dump**：DEC MOP ダンプ（0x6001）
- **vines-echo**：VINES エコー（0x0baf）

例

次に、2 つの MAC アドレス グループ間で非 IPv4 トラフィックを許可するルールが含まれる mac-ip-filter という名前の MAC ACL を設定する例を示します。

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)# permit any any
```

関連コマンド

コマンド	説明
mac access-list	MAC ACL を設定します。
permit（MAC）	MAC ACL に拒否（deny）ルールを設定します。
remark	ACL に備考を設定します。
show mac access-list	すべての MAC ACL または 1 つの MAC ACL を表示します。

description（ユーザ ロール）

ユーザ ロールの説明を設定するには、**description** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

description *text*

no description

構文の説明

text	ユーザ ロールについて説明するテキスト ストリング。最大 128 の英数字まで指定可能です。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

ユーザ ロールの説明テキストには、空白スペースを使用できます。

例

次に、ユーザ ロールの説明を設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

次に、ユーザ ロールから説明を削除する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# no description
```

関連コマンド

コマンド	説明
show role	ユーザ ロール設定に関する情報を表示します。

E コマンド

この章では、E で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

enable

ユーザがシークレット パスワードの入力を求められた後に、高い権限レベルに移行できるようにするには、**enable** コマンドを使用します。

enable *level*

構文の説明

level	ユーザがログインする必要がある権限レベル。指定できるレベルは 15 だけです。

コマンド デフォルト

権限レベル 15

コマンド モード

EXEC コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature privilege** コマンドを使用して、TACACS+ サーバでのコマンド認可にロールの累積権限をイネーブルにする必要があります。

例

次に、ユーザがシークレット パスワードの入力を求められた後に、高い権限レベルに移行できるようにする例を示します。

```
switch# enable 15
switch#
```

関連コマンド

コマンド	説明
enable secret	特定の権限レベルのシークレット パスワードをイネーブルにします。
feature privilege	TACACS+ サーバでのコマンド認可に対するロールの累積権限をイネーブルにします。
show privilege	現在の特権レベル、ユーザ名、および累積権限サポートのステータスを表示します。
username	ユーザが認可に権限レベルを使用できるようにします。

enable secret

特定の権限レベルのシークレット パスワードをイネーブルにするには、**enable secret** コマンドを使用します。パスワードをディセーブルにするには、このコマンドの **no** 形式を使用します。

enable secret [**0** | **5**] *password* [**all** | **priv-lvl** *priv-lvl*]

no enable secret [**0** | **5**] *password* [**all** | **priv-lvl** *priv-lvl*]

構文の説明

0	（任意）パスワードがクリア テキストであること指定します。
5	（任意）パスワードが暗号化形式であること指定します。
password	ユーザ権限エスカレーション用のパスワード。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
all	（任意）すべての権限レベルのシークレットを追加または削除します。
priv-lvl *priv-lvl*	（任意）シークレットが属する権限レベル。指定できる範囲は 1 ～ 15 です。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature privilege** コマンドを使用して、TACACS+ サーバでのコマンド認可にロールの累積権限をイネーブルにする必要があります。

例

次に、特定の権限レベルのシークレット パスワードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret 5 def456 priv-lvl 15
switch(config)# username user2 priv-lvl 15
switch(config)#
```

関連コマンド

コマンド	説明
enable	ユーザがシークレット パスワードの入力を求められた後に、高い権限レベルに移行できるようにします。
feature privilege	TACACS+ サーバでのコマンド認可に対するロールの累積権限をイネーブルにします。

コマンド	説明
show privilege	現在の特権レベル、ユーザ名、および累積権限サポートのステータスを表示します。
username	ユーザが認可に権限レベルを使用できるようにします。

F コマンド

この章では、F で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

feature（ユーザ ロール機能グループ）

ユーザ ロール機能グループに機能を設定するには、**feature** コマンドを使用します。ユーザ ロール機能グループから機能を削除するには、このコマンドの **no** 形式を使用します。

feature *feature-name*

no feature *feature-name*

構文の説明

feature-name	**show role feature** コマンドの出力に表示されるスイッチ機能名。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール機能グループ コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

このコマンドで使用できる有効な機能名を表示するには、**show role feature** コマンドを使用します。

例

次に、ユーザ ロール機能グループに機能を追加する例を示します。

```
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

次に、ユーザ ロール機能グループから機能を削除する例を示します。

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)# no feature callhome
```

関連コマンド

コマンド	説明
role feature-group name	ユーザ ロール機能グループを作成または設定します。
show role feature-group	ユーザ ロール機能グループを表示します。

feature dhcp

デバイスのダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング機能をイネーブルにするには、**feature dhcp** コマンドを使用します。DHCP スヌーピング機能をディセーブルして DHCP スヌーピングに関連するすべてのコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

feature dhcp

no feature dhcp

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

DHCP スヌーピング機能は、デフォルトではディセーブルです。DHCP スヌーピングするは、VLAN のイネーブルまたはディセーブルにできます。

DHCP スヌーピング機能をイネーブルにしないと、DHCP スヌーピングの関連コマンドを使用できません。

ダイナミック APR インスペクションおよび IP ソース ガードは、DHCP スヌーピング機能に依存します。

DHCP スヌーピング機能をディセーブルにすると、次の機能を含む、DHCP スヌーピング設定に関連するデバイス上のすべての設定が廃棄されます。

- DHCP スヌーピング
- DHCP リレー
- Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）
- IPSG

DHCP スヌーピング設定を保持したまま、DHCP スヌーピング機能をオフにしたい場合には、**no ip dhcp snooping** コマンドを使用して、DHCP スヌーピングをグローバルにディセーブルにします。

DHCP スヌーピング機能がイネーブルのときには、アクセス コントロール リスト（ACL）の統計情報はサポートされません。

例

次の例では、DHCP スヌーピングをイネーブルにする方法を示します。

```
switch(config)# feature dhcp
```

```
switch(config)#
```

次の例では、DHCP スヌーピングをディセーブルにする方法を示します。

```
switch(config)# no feature dhcp
switch(config)#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

feature http-server

スイッチで HTTP または Hypertext Transfer Protocol Secure（HTTPS）をイネーブルにするには、**feature http-server** コマンドを使用します。HTTP または HTTPS サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

feature http-server

no feature http-server

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS Release 5.0(2)N1(1) よりも前のリリースでは、デフォルトで HTTP および HTTPS がスイッチ上でイネーブルになっています。

例

次に、スイッチ上で HTTP サーバをイネーブルにし、HTTP サーバのステータスを確認する例を示します。

```
switch(config)# feature http-server
switch(config)# exit
switch# show feature
Feature Name          Instance  State
--------------------  --------  --------
assoc_mgr             1         enabled
cimserver             1         disabled
dhcp-snooping         1         disabled
fabric-binding        1         disabled
fc-port-security      1         disabled
fcoe                  1         enabled
fcsp                  1         disabled
fex                   1         enabled
fport-channel-trunk   1         disabled
http-server           1         enabled
interface-vlan        1         enabled
lacp                  1         enabled
ldap                  1         disabled
lldp                  1         enabled
niv                   1         disabled
npiv                  1         disabled
npv                   1         disabled
otv                   1         disabled
```

```
port_track            1         disabled
private-vlan          1         enabled
privilege             1         enabled
sshServer             1         enabled
tacacs                1         enabled
telnetServer          1         enabled
udld                  1         enabled
vpc                   1         enabled
vtp                   1         enabled
switch# show http-server
http-server enabled
switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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。
show feature	スイッチでイネーブルまたはディセーブルである機能を表示します。
show http-server	HTTP または HTTPS サーバの設定を表示します。

feature privilege

RADIUS サーバと TACACS+ サーバでのコマンド認可に対するロールの累積権限をイネーブルにするには、**feature privilege** コマンドを使用します。ロールの累積権限をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature privilege

no feature privilege

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

feature privilege コマンドをイネーブルにすると、権限ロールは低いレベルの権限ロールの権限を継承します。

例

次に、ロールの累積権限をイネーブルにする例を示します。

```
switch(config)# feature privilege
switch(config)#
```

次に、ロールの累積権限をディセーブルにする例を示します。

```
switch(config)# no feature privilege
switch(config)#
```

関連コマンド

コマンド	説明
enable	上位の特権レベルへのユーザの昇格をイネーブルにします。
enable secret priv-lvl	特定の権限レベルのシークレット パスワードをイネーブルにします。
show feature	スイッチでイネーブルまたはディセーブルである機能を表示します。
show privilege	現在の特権レベル、ユーザ名、および累積権限サポートのステータスを表示します。
username	ユーザが認可に権限レベルを使用できるようにします。

feature tacacs+

TACACS+ をイネーブルにするには、**feature tacacs+** コマンドを使用します。TACACS+ をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature tacacs+

no feature tacacs+

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

（注） TACACS+ をディセーブルにすると、Cisco NX-OS ソフトウェアにより TACACS+ 設定が削除されます。

例

次に、TACACS+ をイネーブルにする例を示します。

```
switch(config)# feature tacacs+
```

次に、TACACS+ をディセーブルにする例を示します。

```
switch(config)# no feature tacacs+
```

関連コマンド

コマンド	説明
show feature	TACACS+ がスイッチでイネーブルになっているかどうかを表示します。
show tacacs+	TACACS+ 情報を表示します。

I コマンド

この章では、I で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

interface policy deny

ユーザ ロールに対してインターフェイス ポリシー コンフィギュレーション モードを開始するには、**interface policy deny** コマンドを使用します。ユーザ ロールのインターフェイス ポリシーをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

interface policy deny

no interface policy deny

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

すべてのインターフェイス

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールのインターフェイス ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

次に、ユーザ ロールのインターフェイス ポリシーをデフォルト設定に戻す例を示します。

```
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

ip access-class

仮想端末回線（VTY）の着信または発信トラフィックを制限するために IPv4 アクセス クラスを作成または設定するには、**ip access-class** コマンドを使用します。アクセス クラスを削除するには、このコマンドの **no** 形式を使用します。

ip access-class *access-list-name* {**in** | **out**}

no ip access-class *access-list-name* {**in** | **out**}

構文の説明

access-list-name	IPv4 ACL クラスの名前。名前は、最大 64 文字まで指定できます。名前には、文字、数字、ハイフン、および下線を使用できます。名前にはスペースまたは引用符を含めることはできません。
in	着信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。
out	発信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。

コマンド デフォルト

なし

コマンド モード

ライン コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次の例では、着信パケットを制限するために VTY 回線の IP アクセス クラスを設定する例を示します。

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# ip access-class VTY_ACCESS in
switch(config-line)#
```

次の例では、着信パケットを制限する IP アクセス クラスを削除する例を示します。

```
switch(config)# line vty
switch(config-line)# no ip access-class VTY_ACCESS in
switch(config-line)#
```

関連コマンド

コマンド	説明
access-class	VTY のアクセス クラスを設定します。
copy running-config startup-config	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 ファイルにコピーします。
show line	特定の端末ラインのアクセス リストを表示します。

コマンド	説明
show running-config aclmgr	ACL の実行コンフィギュレーションを表示します。
show startup-config aclmgr	ACL のスタートアップ コンフィギュレーションを表示します。
ssh	IPv4 を使用して SSH セッションを開始します。
telnet	IPv4 を使用して Telnet セッションを開始します。

ip access-group

ルータの ACL としてレイヤ 3 インターフェイスに IPv4 アクセス コントロール リスト（ACL）を適用するには、**ip access-group** コマンドを使用します。インターフェイスから IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-group *access-list-name* {**in** | **out**}

no ip access-group *access-list-name* {**in** | **out**}

構文の説明

access-list-name	IPv4 ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
in	ACL を着信トラフィックに適用するように指定します。
out	ACL を発信トラフィックに適用するように指定します。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード
サブインターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、IPv4 ACL はレイヤ 3 ルーテッド インターフェイスには適用されません。

ip access-group コマンドを使用することにより、次のインターフェイス タイプに対して、IPv4 ACL をルータ ACL として適用できます。

- VLAN インターフェイス
- レイヤ 3 イーサネット インターフェイス
- レイヤ 3 イーサネット サブインターフェイス
- レイヤ 3 イーサネット ポート チャネル インターフェイスおよびサブインターフェイス
- ループバック インターフェイス
- 管理インターフェイス

また、**ip access-group** コマンドを使用することにより、次のインターフェイス タイプに対して、IPv4 ACL をルータ ACL として適用できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 イーサネット ポート チャネル インターフェイス

ただし、**ip access-group** コマンドを使用してレイヤ 2 に適用した ACL は、ポート モードをルーテッド（レイヤ 3）モードに変更しない限り、アクティブになりません。

デバイスから特定の ACL を削除した場合、インターフェイスからその ACL を削除しなくても、削除した ACL はインターフェイス上のトラフィックには影響しません。

このコマンドには、ライセンスは必要ありません。

例

次に、レイヤ 3 イーサネット インターフェイス 1/2 に対して、ip-acl-01 という IPv4 ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip access-group ip-acl-01 in
```

次に、イーサネット インターフェイス 2/1 から、ip-acl-01 という IPv4 ACL を削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# no switchport
switch(config-if)# ip access-group ip-acl-01 in
switch(config-if)# no ip access-group ip-acl-01 in
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
show access-lists	すべての ACL を表示します。
show ip access-lists	特定の IPv4 ACL またはすべての IPv4 ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定の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。

ipv6 access-class

仮想端末回線（VTY）の着信または発信トラフィックを制限するために IPv6 アクセス クラスを作成または設定するには、**ipv6 access-class** コマンドを使用します。アクセス クラスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-class *access-list-name* {**in** | **out**}

no ipv6 access-class *access-list-name* {**in** | **out**}

構文の説明

access-list-name	IPv6 ACL クラスの名前。名前は、最大 64 文字まで指定できます。名前には、文字、数字、ハイフン、および下線を使用できます。名前にはスペースまたは引用符を含めることはできません。
in	着信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。
out	発信接続が特定の Cisco Nexus 5000 シリーズ スイッチとアクセス リストのアドレス間で制限されていることを指定します。

コマンド デフォルト

なし

コマンド モード

ライン コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、着信パケットを制限するために VTY 回線の IPv6 アクセス クラスを設定する例を示します。

```
switch# configure terminal
switch(config)# line vty
switch(config-line)# ipv6 access-class VTY_I6ACCESS in
switch(config-line)#
```

次に、着信パケットの数を制限する IPv6 アクセス クラスを削除する例を示します。

```
switch(config)# line vty
switch(config-line)# no ipv6 access-class VTY_I6ACCESS in
switch(config-line)#
```

関連コマンド

コマンド	説明
access-class	VTY のアクセス クラスを設定します。
copy running-config startup-config	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 ファイルにコピーします。
show ipv6 access-class	IPv6 アクセス クラスを表示します。

コマンド	説明
show line	特定の端末ラインのアクセス リストを表示します。
show running-config aclmgr	ACL の実行コンフィギュレーションを表示します。
show startup-config aclmgr	ACL のスタートアップ コンフィギュレーションを表示します。
ssh6	IPv6 を使用して SSH セッションを開始します。
telnet6	IPv6 を使用して Telnet セッションを開始します。

ip access-list

IPv4 アクセス コントロール リスト（ACL）を作成して、特定の ACL の IP アクセス リスト コンフィギュレーション モードを開始するには、**ip access-list** コマンドを使用します。IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-list *access-list-name*

no ip access-list *access-list-name*

構文の説明

access-list-name	IPv4 ACL の名前で、最大 64 の英数字です。名前にはスペースまたは引用符を含めることはできません。

コマンド デフォルト

デフォルトでは、IPv4 ACL は定義されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

IPv4 トラフィックをフィルタリングするには、IPv4 ACL を使用します。

ip access-list コマンドを使用すると、スイッチで IP アクセス リスト コンフィギュレーション モードが開始されます。このモードで、IPv4 **deny** コマンドおよび **permit** コマンドを使用し、ACL のルールを設定します。指定した ACL が存在しない場合、このコマンドの入力時にスイッチで新しい ACL が作成されます。

ACL をインターフェイスに適用するには、**ip access-group** コマンドを使用します。

すべての IPv4 ACL は、最終ルールとして、次の暗黙ルールが設定されます。

```
deny ip any any
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

IPv4 ACL には、ネイバー探索プロセスをイネーブルにする暗黙ルールは追加されません。IPv4 では、IPv6 ネイバー探索プロセスと同等の Address Resolution Protocol（ARP; アドレス解決プロトコル）は、別のデータリンク層プロトコルを使用します。デフォルトでは、IPv4 ACL は、インターフェイス上での ARP パケットの送受信を暗黙で許可します。

例

次に、ip-acl-01 という IPv4 ACL の IP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch(config)# ip access-list ip-acl-01
switch(config-acl)#
```

関連コマンド

コマンド	説明
access-class	IPv4 ACL を VTY 回線に適用します。
deny（IPv4）	IPv4 ACL に拒否（deny）ルールを設定します。
ip access-group	IPv4 ACL をインターフェイスに適用します。
permit（IPv4）	IPv4 ACL に許可（permit）ルールを設定します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。

ip arp event-history errors

イベント履歴バッファにアドレス解決プロトコル（ARP）のデバッグ イベントをログに記録するには、**ip arp event-history errors** コマンドを使用します。

ip arp event-history errors size {**disabled** | **large** | **medium** | **small**}

no ip arp event-history errors size {**disabled** | **large** | **medium** | **small**}

構文の説明

size	イベント履歴バッファ サイズを設定するように指定します。
disabled	イベント履歴バッファ サイズをディセーブルに指定します。
large	イベント履歴バッファ サイズが大であることを指定します。
medium	イベント履歴バッファ サイズが中であることを指定します。
small	イベント履歴バッファ サイズが小であることを指定します。これがデフォルトのバッファ サイズです。

コマンド デフォルト

デフォルトでは、イベント履歴バッファは小になります。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、サイズが「中」の ARP イベント履歴バッファを設定する例を示します。

```
switch(config)# ip arp event-history errors size medium
switch(config)#
```

次に、ARP イベント履歴バッファをデフォルトに設定する例を示します。

```
switch(config)# no ip arp event-history errors size medium
switch(config)#
```

関連コマンド

コマンド	説明
show running-config arp all	デフォルト設定を含む ARP 設定を表示します。

ip arp inspection log-buffer

ダイナミック ARP インスペクション（DAI）ロギング バッファ サイズを設定するには、**ip arp inspection log-buffer** コマンドを使用します。DAI ロギング バッファをデフォルトのサイズに戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection log-buffer entries *number*

no ip arp inspection log-buffer entries *number*

構文の説明

entries *number*	1 ～ 1024 メッセージの範囲で、バッファ サイズを指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する前に、**feature dhcp** コマンドを使用して、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをイネーブルにしてください。

DAI ロギング バッファのデフォルトのサイズは、32 メッセージです。

例

次に、DAI ロギング バッファのサイズを設定する例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection log-buffer entries 64
switch(config)#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ロギング バッファをクリアします。
feature dhcp	DHCP スヌーピングをイネーブルにします。
show ip arp inspection log	DAI のログ設定を表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection validate

追加の Dynamic ARP Inspection（DAI）検証をイネーブルにするには、**ip arp inspection validate** コマンドを使用します。追加の DAI をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

ip arp inspection validate {**ip** [**dst-mac**] [**src-mac**]}

ip arp inspection validate {**src-mac** [**dst-mac**] [**ip**]}

no ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

no ip arp inspection validate {**ip** [**dst-mac**] [**src-mac**]}

no ip arp inspection validate {**src-mac** [**dst-mac**] [**ip**]}

構文の説明

dst-mac	（任意）イーサネット ヘッダーの宛先 MAC アドレスを、ARP 応答の ARP 本文にあるターゲット MAC アドレスと照合します。MAC アドレスが一致していないパケットは無効として分類され、ドロップされます。
ip	（任意）ARP 本文が有効で、予期された IP アドレスかどうかを検証します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。すべての ARP 要求と ARP 応答で送信者 IP アドレスを検査し、ARP 応答でターゲット IP アドレスのみを検査します。
src-mac	（任意）イーサネット ヘッダーの送信元 MAC アドレスを、ARP 要求および応答の ARP 本文にある送信側 MAC アドレスと照合します。MAC アドレスが一致していないパケットは無効として分類され、ドロップされます。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する前に、**feature dhcp** コマンドを使用して、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをイネーブルにしてください。

最小限、1 つのキーワードを指定する必要があります。複数のキーワードを指定する場合、順序は影響しません。

送信元 MAC 検証をイネーブルにすると、ARP パケットはパケット本体の送信側イーサネット アドレスが ARP フレーム ヘッダーの送信側イーサネット アドレスと同じである場合にだけ有効と見なされます。宛先 MAC 検証をイネーブルにすると、ARP 要求フレームはターゲット イーサネット アドレスが ARP フレーム ヘッダーの宛先イーサネット アドレスと同じである場合にだけ有効と見なされます。

例

次に、追加の DAI 検証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

次に、追加の DAI 検証をディセーブルにする例を示します。

```
switch(config)# no ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	DHCP スヌーピングをイネーブルにします。
show ip arp inspection	DAI 設定ステータスを表示します。
show running-config dhcp	DAI 設定を含めて、DHCP スヌーピング設定を表示します。

ip arp inspection vlan

VLAN リストに対して Dynamic ARP Inspection（DAI）をイネーブルにするには、**ip arp inspection vlan** コマンドを使用します。VLAN リストの DAI をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit** | **all** | **none**}]

no ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit** | **all** | **none**}]

構文の説明

vlan-list	DAI をアクティブにする VLAN。vlan-list 引数は 1 つの VLAN ID、VLAN ID の範囲、カンマ区切りの ID と範囲を指定できます（「例」を参照）。有効な VLAN ID は、1 ～ 4096 です。
logging	（任意）指定した VLAN の DAI ロギングをイネーブルにします。 • **all**：ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）バインディングと一致するすべてのパケットをロギングします。 • **none**：DHCP バインディング パケットをロギングしません（このオプションは、ロギングをディセーブルにする場合に使用します）。 • **permit**：DHCP バインディングで許可されたパケットをロギングします。
dhcp-bindings	DHCP バインディングの一致に基づくロギングをイネーブルにします。
permit	DHCP バインディング一致による許可パケットのロギングをイネーブルにします。
all	すべてのパケットのロギングをイネーブルにします。
none	ロギングをディセーブルにします。

コマンド デフォルト

ドロップされたパケットのロギング

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、デバイスは DAI によって検査され、ドロップされたパケットをロギングします。

このコマンドには、ライセンスは必要ありません。

例

次に、VLAN 13、15、および 17 ～ 23 で DAI をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection vlan 13,15,17-23
switch(config)#
```

関連コマンド

コマンド	説明
ip arp inspection validate	追加の DAI 検証をイネーブルにします。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection vlan	VLAN の指定されたリストの DAI ステータスを表示します。
show running-config dhcp	DAI 設定を含めて、DHCP スヌーピング設定を表示します。

ip arp inspection trust

レイヤ 2 インターフェイスを信頼できる ARP インターフェイスとして設定するには、**ip arp inspection trust** コマンドを使用します。レイヤ 2 インターフェイスを信頼できない ARP インターフェイスとして設定するには、このコマンドの **no** 形式を使用します。

ip arp inspection trust

no ip arp inspection trust

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、すべてのインターフェイスが信頼できない ARP インターフェイスです。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

信頼できる ARP インターフェイスとして設定できるのは、レイヤ 2 イーサネット インターフェイスだけです。

このコマンドには、ライセンスは必要ありません。

例

次に、レイヤ 2 インターフェイスを信頼できる ARP インターフェイスとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip arp inspection trust
switch(config-if)#
```

関連コマンド

コマンド	説明
show ip arp inspection	Dynamic ARP Inspection（DAI）の設定ステータスを表示します。
show ip arp inspection interface	指定されたインターフェイスの信頼状態および ARP パケット レートを表示します。
show running-config dhcp	DAI 設定を含めて、DHCP スヌーピング設定を表示します。

ip dhcp packet strict-validation

DHCP スヌーピング機能によるダイナミック ホスト コンフィギュレーション プロトコル（DHCP）パケットの厳密な検証をイネーブルにするには、**ip dhcp packet strict-validation** コマンドを使用します。DHCP パケットの厳密な検証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp packet strict-validation

no ip dhcp packet strict-validation

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

ip dhcp packet strict-validation コマンドを使用する前に、DHCP スヌーピングをイネーブルにする必要があります。

DHCP パケットの厳密な検証では、DHCP パケットの DHCP オプション フィールドの先頭 4 バイトの「magic cookie」値を含め、このオプション フィールドが有効であるかをチェックします。DHCP パケットの厳密な検証がイネーブルにされている場合、デバイスは検証に失敗した DHCP パケットをドロップします。

例

次に、DHCP パケットの厳密な検証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp packet strict-validation
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	現在の DHCP 設定を表示します。

ip dhcp snooping

デバイスでダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをグローバルにイネーブルにするには、**ip dhcp snooping** コマンドを使用します。DHCP スヌーピングをグローバルでディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping

no ip dhcp snooping

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、DHCP スヌーピングはグローバルにディセーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature dhcp** コマンドを使用して DHCP スヌーピング機能をイネーブルにする必要があります。

no ip dhcp snooping コマンドを使用して DHCP スヌーピングをディセーブルにすると、デバイスの DHCP スヌーピング設定が保持されます。

例

次に、DHCP スヌーピングをグローバルにイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

ip dhcp snooping information option

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）パケットの option-82 情報の挿入および削除をイネーブルにするには、**ip dhcp snooping information option** コマンドを使用します。option-82 情報の挿入および削除をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option

no ip dhcp snooping information option

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、option-82 情報の挿入および削除は実行されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature dhcp** コマンドを使用して DHCP スヌーピング機能をイネーブルにする必要があります。

例

次に、DHCP スヌーピングをグローバルにイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping information option
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

ip dhcp snooping trust

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）メッセージの信頼できる送信元としてインターフェイスを設定するには、**ip dhcp snooping trust** コマンドを使用します。インターフェイスを DHCP メッセージの信頼できない送信元として設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping trust

no ip dhcp snooping trust

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

デフォルトでは、DHCP メッセージの信頼できる送信元として設定されるインターフェイスはありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 3 イーサネット インターフェイスおよびサブインターフェイス
- レイヤ 2 イーサネット インターフェイス
- プライベート VLAN インターフェイス

例

次に、インターフェイスを DHCP メッセージの信頼できる送信元として設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip dhcp snooping trust
switch(config-if)#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。

コマンド	説明
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

ip dhcp snooping verify mac-address

MAC アドレス検証のダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをイネーブルにするには **ip dhcp snooping verify mac-address** コマンドを使用します。DHCP スヌーピングの MAC アドレス検証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、DHCP スヌーピングでの MAC アドレス検証はディセーブルです。

このコマンドを使用するには、**feature dhcp** コマンドを使用して DHCP スヌーピング機能をイネーブルにする必要があります。

信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合、アドレス検証によってデバイスはパケットをドロップします。

例

次の例では、DHCP スヌーピングを MAC アドレス検証でイネーブルにする方法を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping verify mac-address
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
show running-config dhcp	DHCP スヌーピングの設定を表示します。

ip dhcp snooping vlan

1 つ以上の VLAN でダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをイネーブルにするには **ip dhcp snooping vlan** コマンドを使用します。1 つまたは複数の VLAN 上で DHCP スヌーピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping vlan *vlan-list*

no ip dhcp snooping vlan *vlan-list*

構文の説明

vlan-list	DHCP スヌーピングをイネーブルにする VLAN 範囲。*vlan-list* 引数は 1 つの VLAN ID、VLAN ID の範囲、カンマ区切りの ID と範囲を指定できます。有効な VLAN ID は 1 ～ 4094 です。内部用に予約されている VLAN は除きます。 ハイフン（-）を使用して、VLAN ID の範囲の開始 ID と終了 ID を区別します（たとえば、70-100）。 カンマ（,）を使用して、各 VLAN ID および VLAN ID の範囲を区別します（たとえば、20,70-100,142）。

コマンド デフォルト

デフォルトでは、すべての VLAN 上で DHCP スヌーピングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature dhcp** コマンドを使用して DHCP スヌーピング機能をイネーブルにする必要があります。

例

次に、VLAN 100、200、および 250 ～ 252 で DHCP スヌーピングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

ip port access-group

IPv4 アクセス コントロール リスト（ACL）をインターフェイスのポート ACL として適用するには、**ip port access-group** コマンドを使用します。インターフェイスから IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip port access-group *access-list-name* **in**

no ip port access-group *access-list-name* **in**

構文の説明

access-list-name	IPv4 ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
in	ACL を着信トラフィックに適用するように指定します。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード
仮想イーサネット インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.1(3)N1(1)	このコマンドのサポートが、仮想イーサネット インターフェイスに導入されました。

使用上のガイドライン

デフォルトでは、インターフェイスに IPv4 ACL は適用されません。

ip port access-group コマンドを使用することにより、次のインターフェイス タイプに対して、IPv4 ACL をポート ACL として適用できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 EtherChannel インターフェイス
- 仮想イーサネット インターフェイス

IPv4 ACL を VLAN ACL として適用することもできます。詳細については、**match** コマンドを参照してください。

スイッチでポート ACL が適用されるのは、着信トラフィックだけです。着信パケットは、スイッチ上で ACL のルールに対してチェックされます。最初の一致ルールによってパケットが許可されると、そのパケットはスイッチで引き続き処理されます。最初の一致ルールによってパケットが拒否されると、そのパケットはスイッチで廃棄され、ICMP ホスト到達不能メッセージが戻されます。

スイッチから特定の ACL を削除した場合、インターフェイスからその ACL を削除しなくても、削除した ACL はインターフェイス上のトラフィックには影響しません。

例

次に、イーサネット インターフェイス 1/2 に対して、ip-acl-01 という IPv4 ACL をポート ACL として適用する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip port access-group ip-acl-01 in
```

次に、イーサネット インターフェイス 1/2 から、ip-acl-01 という IPv4 ACL を削除する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# no ip port access-group ip-acl-01 in
switch(config-if)#
```

次に、仮想イーサネット インターフェイス 1 に対して、ip-acl-03 という IPv4 ACL をポート ACL として適用する例を示します。

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ip port access-group ip-acl-03 in
switch(config-if)#
```

関連コマンド

コマンド	説明
interface vethernet	仮想イーサネット インターフェイスを設定します。
ip access-list	IPv4 ACL を設定します。
show access-lists	すべての ACL を表示します。
show ip access-lists	特定の IPv4 ACL またはすべての IPv4 ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定の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。

ip source binding

レイヤ 2 イーサネット インターフェイス用の固定 IP ソース エントリを作成するには、**ip source binding** コマンドを使用します。固定 IP ソース エントリをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip source binding *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot*/*port* | **port-channel** *channel-no*}

no ip source binding *IP-address MAC-address* **vlan** *vlan-id* {**interface ethernet** *slot*/*port* | **port-channel** *channel-no*}

構文の説明

IP-address	特定のインターフェイス上で使用する IPv4 アドレス。有効なエントリは、ドット付き 10 進表記です。
MAC-address	特定のインターフェイス上で使用する MAC アドレス。有効なエントリは、ドット付き 16 進表記です。
vlan *vlan-id*	IP ソース エントリに関連付ける VLAN を指定します。
interface ethernet *slot*/*port*	固定 IP エントリに関連付けるレイヤ 2 イーサネット インターフェイスを指定します。スロット番号には 1 ～ 255、ポート番号には 1 ～ 128 を指定できます。
port-channel *channel-no*	EtherChannel インターフェイスを指定します。番号は、1 ～ 4096 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、固定 IP ソース エントリは作成されません。

このコマンドを使用するには、**feature dhcp** コマンドを使用してダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング機能をイネーブルにする必要があります。

例

次に、イーサネット インターフェイス 2/3 上に、VLAN 100 に関連付ける固定 IP ソース エントリを作成する例を示します。

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet 2/3
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
show ip verify source	IP と MAC アドレスのバインディングを表示します。
show interface	インターフェイス コンフィギュレーションを表示します。
show running-config dhcp	DHCP スヌーピング設定情報を表示します。

ip verify source dhcp-snooping-vlan

レイヤ 2 イーサネット インターフェイス上で IP ソース ガードをイネーブルにするには、**ip verify source dhcp-snooping-vlan** コマンドを使用します。レイヤ 2 イーサネット インターフェイス上で IP ソース ガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify source dhcp-snooping-vlan

no ip verify source dhcp-snooping-vlan

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する前に、**feature dhcp** コマンドを使用して、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングをイネーブルにしてください。

IP ソース ガードは、インターフェイス上の IP トラフィックを、IP-MAC アドレス バインディング テーブル エントリまたはスタティック IP ソース エントリに送信元が含まれているトラフィックだけに制限します。

IP ソース ガードの機能は、DHCP スヌーピング（IP-MAC アドレス バインディング テーブルの構築および維持に関して）、またはスタティック IP ソース エントリの手動での維持に依存しています。

このコマンドには、ライセンスは必要ありません。

例

次に、レイヤ 2 インターフェイスの IP ソース ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# ip verify source dhcp-snooping-vlan
switch(config-if)#
```

次に、レイヤ 2 インターフェイスの IP ソース ガードをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# no ip verify source dhcp-snooping-vlan
switch(config-if)#
```

関連コマンド

コマンド	説明
feature dhcp	スイッチをスヌーピングする DHCP をイネーブルにします。
ip source binding	レイヤ 2 イーサネット インターフェイスのスタティック IP ソース エントリを作成します。
show ip verify source	インターフェイスの IP と MAC アドレスのバインディングを表示します。
show running-config dhcp	実行コンフィギュレーションの IP 設定を表示します。
show running-config interface ethernet	実行コンフィギュレーション内のインターフェイスの設定を表示します。

ip verify unicast source reachable-via

インターフェイス上でユニキャスト リバース パス転送（ユニキャスト RPF）を設定するには、**ip verify unicast source reachable-via** コマンドを使用します。インターフェイスからユニキャスト RPF を削除するには、このコマンドの **no** 形式を使用します。

ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

no ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

構文の説明

any	ルーズ チェックを指定します。
allow-default	（任意）特定のインターフェイス上で使用する MAC アドレスを指定します。
rx	ストリクト チェックを指定します。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

入力インターフェイスに次のいずれかのユニキャスト RPF モードを設定できます。

- ストリクト ユニキャスト RPF モード : ストリクト モード チェックは、次の一致が検出された場合に成功します。
  - ユニキャスト RPF が、Forwarding Information Base（FIB; 転送情報ベース）でパケット送信元アドレスの一致を検出。
  - パケットを受信した入力側インターフェイスが、FIB 一致のユニキャスト PRF インターフェイスの 1 つと一致。

  これらのチェックに失敗すると、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケット フローが対称であると予想される場合に使用できます。
- ルーズ ユニキャスト RPF モード : ルーズ モード チェックは、FIB でのパケット送信元アドレスの検索が一致し、最低 1 つの実インターフェイスを経由して送信元に到達可能であるという FIB 結果が示された場合に成功します。パケットを受信した入力インターフェイスが FIB 内のインターフェイスのいずれかと一致する必要はありません。

このコマンドには、ライセンスは必要ありません。

例

次に、インターフェイス上にルーズ ユニキャスト RPF チェックを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
```

```
switch(config-if)# ip verify unicast source reachable-via any
```

次に、インターフェイス上にストリクト ユニキャスト RPF チェックを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ip verify unicast source reachable-via rx
```

関連コマンド

コマンド	説明
show ip interface ethernet	インターフェイスの IP 関連情報を表示します。
show running-config interface ethernet	実行コンフィギュレーション内のインターフェイスの設定を表示します。
show running-config ip	実行コンフィギュレーションの IP 設定を表示します。

ipv6 access-list

IPv6 アクセス コントロール リスト（ACL）を作成して、特定の ACL の IP アクセス リスト コンフィギュレーション モードを開始するには、**ipv6 access-list** コマンドを使用します。IPv6 ACL を削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

構文の説明

access-list-name	IPv6 ACL の名前で、最大 64 の英数字です。名前にはスペースまたは引用符を含めることはできません。

コマンド デフォルト

デフォルトでは、IPv6 ACL は定義されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 トラフィックをフィルタリングするには、IPv6 ACL を使用します。

ipv6 access-list コマンドを使用すると、スイッチで IP アクセス リスト コンフィギュレーション モードが開始されます。このモードで、IPv6 の **deny** コマンドおよび **permit** コマンドを使用し、ACL のルールを設定します。指定した ACL が存在しない場合、このコマンドの入力時にスイッチで新しい ACL が作成されます。

すべての IPv6 ACL は、最終ルールとして、次の暗黙ルールが設定されます。

```
deny ipv6 any any
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

例

次に、ipv6-acl-01 という名前の IPv6 ACL の IP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch(config)# ipv6 access-list ipv6-acl-01
switch(config-ipv6-acl)#
```

関連コマンド

コマンド	説明
deny（IPv6）	IPv6 ACL に拒否（deny）ルールを設定します。
permit（IPv6）	IPv6 ACL に許可（permit）ルールを設定します。

ipv6 port traffic-filter

IPv6 アクセス コントロール リスト（ACL）をインターフェイスのポート ACL として適用するには、**ipv6 port traffic-filter** コマンドを使用します。インターフェイスから IPv6 ACL を削除するには、このコマンドの **no** 形式を使用します。

ipv6 port traffic-filter *access-list-name* **in**

no ipv6 port traffic-filter *access-list-name* **in**

構文の説明

access-list-name	IPv6 ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
in	デバイスが ACL を着信トラフィックに適用するように指定します。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード
仮想イーサネット インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。
5.1(3)N1(1)	このコマンドのサポートが、仮想イーサネット インターフェイスに導入されました。

使用上のガイドライン

デフォルトでは、インターフェイスに IPv6 ACL は適用されません。

ipv6 port traffic-filter コマンドを使用することにより、次のインターフェイス タイプに対して、IPv6 ACL をポート ACL として適用できます。

- イーサネット インターフェイス
- EtherChannel インターフェイス
- 仮想イーサネット インターフェイス

ipv6 port traffic-filter コマンドを使用することにより、次のインターフェイス タイプに対して、IPv6 ACL をポート ACL として適用もできます。

- VLAN インターフェイス

（注） VLAN インターフェイスを設定する前に、VLAN インターフェイスをグローバルでイネーブルにする必要があります。詳細については、**feature interface-vlan** コマンドを参照してください。

スイッチでポート ACL が適用されるのは、着信トラフィックだけです。着信パケットは、スイッチ上で ACL のルールに対してチェックされます。最初の一致ルールによってパケットが許可されると、そのパケットはスイッチで引き続き処理されます。最初の一致ルールによってパケットが拒否されると、そのパケットはスイッチで廃棄され、ICMP ホスト到達不能メッセージが戻されます。

デバイスから特定の ACL を削除した場合、インターフェイスからその ACL を削除しなくても、削除した ACL はインターフェイス上のトラフィックには影響しません。

例

次に、イーサネット インターフェイス 1/3 に対して、ipv6-acl という IPv6 ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 port traffic-filter ipv6-acl in
switch(config-if)#
```

次に、イーサネット インターフェイス 1/3 から、ipv6-acl という IPv6 ACL を削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 port traffic-filter ipv6-acl in
switch(config-if)#
```

次に、特定の仮想イーサネット インターフェイスに対して、ipv6-acl-03 という名前の IPv6 ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# ipv6 port traffic-filter ipv6-acl-03 in
switch(config-if)#
```

関連コマンド

コマンド	説明
interface vethernet	仮想イーサネット インターフェイスを設定します。
ipv6 access-list	IPv6 ACL を設定します。
show access-lists	すべての ACL を表示します。
show ipv6 access-lists	特定の IPv6 ACL またはすべての IPv6 ACL を表示します。

M コマンド

この章では、M で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

mac access-list

Media Access Control（MAC; メディア アクセス コントロール）アクセス コントロール リスト（ACL）を作成するか、または特定の ACL の MAC アクセス リスト コンフィギュレーション モードを開始するには、**mac access-list** コマンドを使用します。MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

mac access-list *access-list-name*

no mac access-list *access-list-name*

構文の説明

access-list-name	MAC ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。

コマンド デフォルト

デフォルトでは、MAC ACL は定義されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

非 IP トラフィックをフィルタリングするには、MAC ACL を使用します。

mac access-list コマンドを使用すると、スイッチで MAC アクセス リスト コンフィギュレーション モードが開始されます。このモードで、MAC **deny** コマンドおよび **permit** コマンドを使用し、ACL のルールを設定します。指定した ACL が存在しない場合は、このコマンドの入力時にスイッチで新しい ACL が作成されます。

ACL をインターフェイスに適用するには、**mac access-group** コマンドを使用します。

すべての MAC ACL は、最終ルールとして、次の暗黙ルールが設定されます。

```
deny any any protocol
```

この暗黙のルールにより、トラフィックのレイヤ 2 ヘッダーに指定されたプロトコルに関係なく、一致しないトラフィックがスイッチによって確実に拒否されます。

例

次に、mac-acl-01 という MAC ACL の MAC アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch(config)# mac access-list mac-acl-01
switch(config-acl)#
```

関連コマンド

コマンド	説明
deny（MAC）	MAC ACL に拒否（deny）ルールを設定します。
mac access-group	MAC ACL をインターフェイスに適用します。
permit（MAC）	MAC ACL に許可（permit）ルールを設定します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。

mac port access-group

MAC アクセス コントロール リスト（ACL）をインターフェイスに適用するには、**mac port access-group** コマンドを使用します。インターフェイスから MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

構文の説明

access-list-name	MAC ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。

コマンド デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード
仮想イーサネット インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.1(3)N1(1)	このコマンドのサポートが、仮想イーサネット インターフェイスに追加されました。

使用上のガイドライン

デフォルトでは、インターフェイスに MAC ACL は適用されません。

MAC ACL を非 IP トラフィックに適用します。

mac port access-group コマンドを使用することにより、次のインターフェイス タイプに対して、MAC ACL をポート ACL として適用できます。

- レイヤ 2 インターフェイス
- レイヤ 2 EtherChannel インターフェイス
- 仮想イーサネット インターフェイス

MAC ACL を VLAN ACL として適用することもできます。詳細については、**match** コマンドを参照してください。

スイッチで MAC ACL が適用されるのは、着信トラフィックだけです。スイッチは、MAC ACL を適用すると、パケットを ACL のルールに対してチェックします。最初の一致ルールによってパケットが許可されると、そのパケットはスイッチで引き続き処理されます。最初の一致ルールによってパケットが拒否されると、そのパケットはスイッチで廃棄され、ICMP ホスト到達不能メッセージが戻されます。

スイッチから特定の ACL を削除した場合、インターフェイスからその ACL を削除しなくても、削除した ACL はインターフェイス上のトラフィックには影響しません。

例

次に、イーサネット インターフェイス 1/2 に対して、mac-acl-01 という MAC ACL を適用する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# mac port access-group mac-acl-01
switch(config-if)#
```

次に、イーサネット インターフェイス 1/2 から、mac-acl-01 という MAC ACL を削除する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# no mac port access-group mac-acl-01
switch(config-if)#
```

次に、特定の仮想イーサネット インターフェイスに対して、mac-acl-03 という名前の MAC ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface vethernet 1
switch(config-if)# mac port access-group mac-acl-03
switch(config-if)#
```

関連コマンド

コマンド	説明
interface vethernet	仮想イーサネット インターフェイスを設定します。
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL を表示します。
show mac access-lists	特定の MAC ACL またはすべての MAC ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定の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。

match

VLAN アクセス マップ内のトラフィック フィルタリング用としてアクセス コントロール リスト（ACL）を指定するには、**match** コマンドを使用します。VLAN アクセス マップから **match** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match {**ip** | **ipv6** | **mac**} **address** *access-list-name*

no match {**ip** | **ipv6** | **mac**} **address** *access-list-name*

構文の説明

ip	IPv4 ACL を指定します。
ipv6	IPv6 ACL を指定します。
mac	MAC ACL を指定します。
address *access-list-name*	IPv4 アドレス、IPv6 アドレス、または MAC アドレス、およびアクセス リスト名を指定します。名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。

コマンド デフォルト

デフォルトでは、スイッチによりトラフィックが分類され、IPv4 トラフィックには IPv4 ACL が、その他のすべてのトラフィックには MAC ACL が適用されます。

コマンド モード

VLAN アクセスマップ コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

指定できる **match** コマンドは、アクセス マップごとに 1 つだけです。

例

次に、vlan-map-01 という名前で VLAN アクセス マップを作成して、そのマップに ip-acl-01 という名前の IPv4 ACL を割り当て、スイッチが ACL に一致するパケットを転送するよう指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。

コマンド	説明
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

P コマンド

この章では、P で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

permit（ARP）

条件と一致する ARP トラフィックを許可する ARP ACL ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本構文

[*sequence-number*] **permit ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

no *sequence-number*

no permit ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。デバイスによってアクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しないと、デバイスによって、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
ip	ルールの IP アドレス部分を指定します。
any	任意のホストが、ルールの **any** キーワードを含む部分と一致するように指定します。送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、および宛先 MAC アドレスの指定に、**any** を使用できます。
host *sender-IP*	ARP パケットの送信元 IP アドレスが *sender-IP* 引数の値と一致する場合だけ、パケットを一致させるルールを指定します。*sender-IP* 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。
sender-IP sender-IP-mask	パケットの送信元 IP アドレスと一致させる IPv4 アドレス セットの IPv4 アドレスおよびマスク。*sender-IP* 引数および *sender-IP-mask* 引数は、ドット付き 10 進表記で指定する必要があります。*sender-IP-mask* 引数に 255.255.255.255 を指定すると、**host** キーワードを使用した場合と同じ結果になります。
mac	ルールの MAC アドレスの部分を指定します。

コマンド デフォルト

なし

コマンド モード

ARP ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

（注） Cisco NX-OS Release 5.1(3)N1(1) 以降、ARP アクセス リストは、Control Plane Policing（CoPP）に対してだけサポートされます。**permit** コマンドは CoPP ARP ACL では無視されます。

新しく作成した ARP ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、デバイスは ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号を割り当てます。

パケットに ARP ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、デバイスはシーケンス番号が最も低いルールを施行します。

例

次に、copp-arp-acl という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始し、192.0.32.14/24 サブネット内にある送信者の IP アドレスを含み、それを copp-arp-acl クラスに関連づける ARP 要求メッセージを許可するルールを追加する例を示します。

```
switch# configure terminal
switch(config)# arp access-list copp-arp-acl
switch(config-arp-acl)# permit ip 192.0.32.14 255.255.255.0 mac any
switch(config-arp-acl)#
```

関連コマンド

コマンド	説明
deny（ARP）	ARP ACL に拒否（deny）ルールを設定します。
arp access-list	ARP ACL を設定します。
remark	ACL に備考を設定します。
show arp access-lists	すべての ARP ACL または 1 つの ARP ACL を表示します。

permit（IPv4）

条件と一致するトラフィックを許可する IPv4 アクセス コントロール リスト（ACL）ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本構文

[*sequence-number*] **permit** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no permit *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

インターネット制御メッセージ プロトコル

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

インターネット グループ管理プロトコル

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

インターネット プロトコル v4（IPv4）

[*sequence-number*] **permit ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

伝送制御プロトコル（TCP）

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*] [*flags*] [**established**]

ユーザ データグラム プロトコル

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。スイッチによってアクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、スイッチは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
protocol	ルールで一致させるパケットのプロトコルの名前または番号。有効な番号は、0 ～ 255 です。有効なプロトコル名は、次のキーワードです。 • **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数を使用できます。 • **igmp**：ルールを IGMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*igmp-type* 引数を使用できます。 • **ip**：ルールをすべての IPv4 トラフィックに適用するように指定します。このキーワードを使用する場合は、すべての IPv4 プロトコルに適用される他のキーワードおよび引数だけを使用できます。使用できるキーワードには次のものがあります。 – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **tcp**：ルールを TCP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*flags* 引数および *operator* 引数、**portgroup** キーワードおよび **established** キーワードを使用できます。 • **udp**：ルールを UDP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。
source	ルールで一致させる送信元 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。

dscp *dscp*	（任意）IP ヘッダーの DSCP フィールドに特定の 6 ビット diffserv（ディファレンシエーテッド サービス）値が設定されているパケットだけをルールと一致させるように指定します。*dscp* 引数には、次の数値またはキーワードのいずれかを指定します。 • 0 ～ 63：DSCP フィールドの 6 ビットと同等の 10 進数。たとえば 10 を指定した場合、ルールは DSCP フィールドのビットが 001010 であるパケットだけに一致します。 • **af11**：Assured Forwarding（AF）クラス 1、低い廃棄確率（001010） • **af12**：AF クラス 1、中程度の廃棄確率（001100） • **af13**：AF クラス 1、高い廃棄確率（001110） • **af21**：AF クラス 2、低い廃棄確率（010010） • **af22**：AF クラス 2、中程度の廃棄確率（010100） • **af23**：AF クラス 2、高い廃棄確率（010110） • **af31**：AF クラス 3、低い廃棄確率（011010） • **af32**：AF クラス 3、中程度の廃棄確率（011100） • **af33**：AF クラス 3、高い廃棄確率（011110） • **af41**：AF クラス 4、低い廃棄確率（100010） • **af42**：AF クラス 4、中程度の廃棄確率（100100） • **af43**：AF クラス 4、高い廃棄確率（100110） • **cs1**：Class-selector（CS）1、優先順位 1（001000） • **cs2**：CS2、優先順位 2（010000） • **cs3**：CS3、優先順位 3（011000） • **cs4**：CS4、優先順位 4（100000） • **cs5**：CS5、優先順位 5（101000） • **cs6**：CS6、優先順位 6（110000） • **cs7**：CS7、優先順位 7（111000） • **default**：デフォルトの DSCP 値（000000） • **ef**：Expedited Forwarding（EF; 緊急転送）（101110）

precedence *precedence*	（任意）*precedence* 引数で指定された値が IP Precedence フィールドに設定されているパケットだけをルールと一致させるように指定します。*precedence* 引数には、次の数値またはキーワードを指定します。 • 0 ～ 7 : IP Precedence フィールドの 3 ビットと同等の 10 進数。たとえば、3 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します : 011 • **critical** : 優先順位 5（101） • **flash** : 優先順位 3（011） • **flash-override** : 優先順位 4（100） • **immediate** : 優先順位 2（010） • **internet** : 優先順位 6（110） • **network** : 優先順位 7（111） • **priority** : 優先順位 1（001） • **routine** : 優先順位 0（000）
fragments	（任意）非初期フラグメントであるパケットだけをルールと一致させるように指定します。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定したルールには指定できません。これらのオプションをスイッチが評価するために必要な情報は、初期フラグメントだけに含まれているからです。
time-range *time-range-name*	（任意）このルールに適用する時間範囲を指定します。**time-range** コマンドを使用して時間範囲を設定できます。
icmp-message	（任意 : IGMP 限定）指定した ICMP メッセージ タイプのパケットだけに対して一致するルールです。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」の「ICMP メッセージ タイプ」にリストされているキーワードの 1 つを指定します。
igmp-message	（任意 : IGMP 限定）指定した IGMP メッセージ タイプのパケットだけに対して一致するルールです。*igmp-message* 引数には、0 ～ 15 の整数である IGMP メッセージ番号を指定します。また、次のいずれかのキーワードを指定できます。 • **dvmrp** : Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル） • **host-query** : ホスト クエリー • **host-report** : ホスト レポート • **pim** : Protocol Independent Multicast（PIM） • **trace** : マルチキャスト トレース

operator port [*port*]	（任意：TCP および UDP 限定）*operator* 引数および *port* 引数の条件と一致する送信元ポートから送信されたパケット、または一致する宛先ポートに送信されたパケットだけを、ルールと一致させます。これらの引数が送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定します。有効な番号は 0 ～ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の *port* 引数は、*operator* 引数が範囲である場合だけ必要です。 *operator* 引数には、次のいずれかのキーワードを指定する必要があります。 • **eq**：パケットのポートが *port* 引数と同等である場合だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数以上で、2 番目の *port* 引数以下である場合だけ一致します。
portgroup *portgroup*	（任意：TCP および UDP 限定）*portgroup* 引数で指定された IP ポート グループ オブジェクトのメンバである送信元ポートから送信されたパケット、またはメンバである宛先ポートに送信されたパケットだけを、ルールと一致させるように指定します。ポート グループ オブジェクトが送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 IP ポート グループ オブジェクトを作成および変更するには、**object-group ip port** コマンドを使用します。
flags	（任意：TCP 限定）特定の TCP コントロール ビット フラグがオンに設定されたパケットだけを、ルールと一致させます。*flags* 引数の値には、次の 1 つ以上のキーワードを指定する必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	（任意：TCP 限定）確立された TCP 接続に属するパケットだけをルールと一致させるように指定します。スイッチは、ACK または RST ビットが設定されている TCP パケットが、確立された接続に属していると見なします。

コマンド デフォルト　新しく作成した IPv4 ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、デバイスは ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号を割り当てます。

コマンド モード　IPv4 ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン　スイッチは、パケットに IPv4 ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。スイッチで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、スイッチはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。各ルールでは、これらの引数の 1 つを指定する際に使用した方法が、他の引数の指定方法に影響を与えることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびネットワーク ワイルドカード：IPv4 アドレスおよびネットワーク ワイルドカードを使用して、送信元または宛先とするホストまたはネットワークを指定できます。構文は次のとおりです。

  IPv4-address network-wildcard

  次に、192.168.67.0 サブネットの IPv4 アドレスおよびネットワーク ワイルドカードを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit tcp 192.168.67.0 0.0.0.255 any
  ```

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）: IPv4 アドレスおよび VLSM を使用して、送信元または宛先とするホストまたはネットワークを指定できます。構文は次のとおりです。

  IPv4-address/prefix-len

  次に、192.168.67.0 サブネットの IPv4 アドレスおよび VLSM を使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit udp 192.168.67.0/24 any
  ```

- ホスト アドレス：**host** キーワードおよび IPv4 アドレスを使用して、送信元または宛先とするホストを指定できます。構文は次のとおりです。

  host *IPv4-address*

  この構文は、*IPv4-address*/32 および *IPv4-address* 0.0.0.0 と同じです。

  次に、**host** キーワードおよび 192.168.67.132 IPv4 アドレスを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit icmp host 192.168.67.132 any
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先として任意の IPv4 アドレスを指定できます。**any** キーワードの使用例は、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

ICMP メッセージ タイプ

igmp-message 引数には、0 ～ 255 の整数である ICMP メッセージ番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **administratively-prohibited**：管理上の禁止
- **alternate-address**：代替アドレス
- **conversion-error**：データグラム変換
- **dod-host-prohibited**：ホスト禁止
- **dod-net-prohibited**：ネット禁止
- **echo**：エコー（ping）
- **echo-reply**：エコー応答
- **general-parameter-problem**：パラメータの問題
- **host-isolated**：ホスト分離
- **host-precedence-unreachable**：優先順位のホスト到達不能
- **host-redirect**：ホスト リダイレクト
- **host-tos-redirect**：ToS ホスト リダイレクト
- **host-tos-unreachable**：ToS ホスト到達不能
- **host-unknown**：ホスト未知
- **host-unreachable**：ホスト到達不能
- **information-reply**：情報応答
- **information-request**：情報要求
- **mask-reply**：マスク応答
- **mask-request**：マスク要求
- **mobile-redirect**：モバイル ホスト リダイレクト
- **net-redirect**：ネットワーク リダイレクト
- **net-tos-redirect**：ToS ネット リダイレクト
- **net-tos-unreachable**：ToS ネット到達不能
- **net-unreachable**：ネット到達不能
- **network-unknown**：ネットワーク未知
- **no-room-for-option**：パラメータが必要だが空きなし
- **option-missing**：パラメータが必要だが存在しない
- **packet-too-big**：フラグメンテーションが必要、DF 設定
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：ポート到達不能
- **precedence-unreachable**：優先順位カットオフ
- **protocol-unreachable**：プロトコル到達不能
- **reassembly-timeout**：再構成タイムアウト
- **redirect**：すべてのリダイレクト
- **router-advertisement**：ルータ ディスカバリ アドバタイズメント
- **router-solicitation**：ルータ ディスカバリ要求
- **source-quench**：送信元抑制
- **source-route-failed**：送信元ルート障害

- **time-exceeded**：すべての時間超過メッセージ
- **timestamp-reply**：タイム スタンプ付きの応答
- **timestamp-request**：タイム スタンプ付きの要求
- **traceroute**：トレースルート
- **ttl-exceeded**：TTL 超過
- **unreachable**：すべての到達不能

TCP ポート名

protocol 引数に **tcp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である TCP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **bgp**：Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）
- **chargen**：キャラクタ ジェネレータ（19）
- **cmd**：リモート コマンド（rcmd、514）
- **daytime**：デイタイム（13）
- **discard**：廃棄（9）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **drip**：Dynamic Routing Information Protocol（DRIP; ダイナミック ルーティング情報プロトコル）（3949）
- **echo**：エコー（7）
- **exec**：EXEC（rsh、512）
- **finger**：フィンガー（79）
- **ftp**：File Transfer Protocol（FTP; ファイル転送プロトコル）（21）
- **ftp-data**：FTP データ接続（2）
- **gopher**：Gopher（7）
- **hostname**：NIC ホストネーム サーバ（11）
- **ident**：Ident プロトコル（113）
- **irc**：Internet Relay Chat（IRC; インターネット リレー チャット）（194）
- **klogin**：Kerberos ログイン（543）
- **kshell**：Kerberos シェル（544）
- **login**：ログイン（rlogin、513）
- **lpd**：プリンタ サービス（515）
- **nntp**：Network News Transport Protocol（NNTP）（119）
- **pim-auto-rp**：PIM Auto-RP（496）
- **pop2**：Post Office Protocol v2（POP2）（19）
- **pop3**：Post Office Protocol v3（POP3）（11）
- **smtp**：Simple Mail Transport Protocol（SMTP; シンプル メール転送プロトコル）（25）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）

- **telnet**：Telnet（23）
- **time**：Time（37）
- **uucp**：UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）（54）
- **whois**：WHOIS/NICNAME（43）
- **www**：World Wide Web（HTTP、8）

UDP ポート名

protocol 引数に **udp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である UDP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **biff**：BIFF（メール通知、comsat、512）
- **bootpc**：Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）
- **bootps**：ブートストラップ プロトコル（BOOTP）サーバ（67）
- **discard**：廃棄（9）
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **echo**：エコー（7）
- **isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（5）
- **mobile-ip**：モバイル IP レジストレーション（434）
- **nameserver**：IEN116 ネーム サービス（旧式、42）
- **netbios-dgm**：NetBIOS データグラム サービス（138）
- **netbios-ns**：NetBIOS ネーム サービス（137）
- **netbios-ss**：NetBIOS セッション サービス（139）
- **non500-isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（45）
- **ntp**：Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）
- **pim-auto-rp**：PIM Auto-RP（496）
- **rip**：Routing Information Protocol（RIP）（ルータ、in.routed、52）
- **snmp**：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）
- **snmptrap**：SNMP トラップ（162）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **syslog**：システム ロギング（514）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）
- **tftp**：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（69）
- **time**：Time（37）
- **who**：Who サービス（rwho、513）
- **xdmcp**：X Display Manager Control Protocol（XDMCP）（177）

例

次に、acl-lab-01 という IPv4 ACL を作成し、10.23.0.0 および 192.168.37.0 ネットワークから 10.176.0.0 ネットワークへのすべての TCP および UDP トラフィックを許可するルールを設定する例を示します。

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit udp 192.168.37.0/16 10.176.0.0/16
```

関連コマンド

コマンド	説明
deny（IPv4）	IPv4 ACL に拒否（deny）ルールを設定します。
ip access-list	IPv4 ACL を設定します。
remark	ACL に備考を設定します。
show ip access-lists	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。

permit（IPv6）

条件と一致するトラフィックを許可する IPv6 アクセス コントロール リスト（ACL）ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本構文

[*sequence-number*] **permit** *protocol source destination* [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

no permit *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*]
[**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

インターネット制御メッセージ プロトコル

[*sequence-number* | **no**] **permit icmp** *source destination* [*icmp-message*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

インターネット プロトコル v6（IPv6）

[*sequence-number*] **permit ipv6** *source destination* [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Stream Control Transmission Protocol

[*sequence-number* | **no**] **permit sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

伝送制御プロトコル（TCP）

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*] [*flags*]
[**established**]

ユーザ データグラム プロトコル

[*sequence-number* | **no**] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。デバイスによってアクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しないと、デバイスによって、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
protocol	ルールで一致させるパケットのプロトコルの名前または番号。有効な番号は、0 ～ 255 です。有効なプロトコル名は、次のキーワードです。 • **ahp**：ルールを Authentication Header Protocol（AHP; 認証ヘッダー プロトコル）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **esp**：ルールを Encapsulating Security Payload（ESP）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数を使用できます。 • **ipv6**：ルールをすべての IPv6 トラフィックに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **pcp**：ルールを Payload Compression Protocol（PCP; ペイロード圧縮プロトコル）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **sctp**：ルールを Stream Control Transmission Protocol（SCTP）トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。 • **tcp**：ルールを TCP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*flags* 引数および *operator* 引数、**portgroup** キーワードおよび **established** キーワードを使用できます。 • **udp**：ルールを UDP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。
source	ルールで一致させる送信元 IPv6 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。

destination	ルールで一致させる宛先 IPv6 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
dscp *dscp*	（任意）IPv6 ヘッダーの DSCP フィールドに特定の 6 ビット diffserv（ディファレンシエーテッド サービス）値が設定されているパケットだけをルールと一致させるように指定します。*dscp* 引数には、次の数値またはキーワードのいずれかを指定します。 • 0 ～ 63 : DSCP フィールドの 6 ビットと同等の 10 進数。たとえば、10 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します : 001010 • **af11** : Assured Forwarding（AF）クラス 1、低い廃棄確率（001010） • **af12** : AF クラス 1、中程度の廃棄確率（001100） • **af13** : AF クラス 1、高い廃棄確率（001110） • **af21** : AF クラス 2、低い廃棄確率（010010） • **af22** : AF クラス 2、中程度の廃棄確率（010100） • **af23** : AF クラス 2、高い廃棄確率（010110） • **af31** : AF クラス 3、低い廃棄確率（011010） • **af32** : AF クラス 3、中程度の廃棄確率（011100） • **af33** : AF クラス 3、高い廃棄確率（011110） • **af41** : AF クラス 4、低い廃棄確率（100010） • **af42** : AF クラス 4、中程度の廃棄確率（100100） • **af43** : AF クラス 4、高い廃棄確率（100110） • **cs1** : Class-selector（CS）1、優先順位 1（001000） • **cs2** : CS2、優先順位 2（010000） • **cs3** : CS3、優先順位 3（011000） • **cs4** : CS4、優先順位 4（100000） • **cs5** : CS5、優先順位 5（101000） • **cs6** : CS6、優先順位 6（110000） • **cs7** : CS7、優先順位 7（111000） • **default** : デフォルトの DSCP 値（000000） • **ef** : Expedited Forwarding（EF; 緊急転送）（101110）
flow-label *flow-label-value*	（任意）*flow-label-value* 引数で指定された値がフロー ラベル ヘッダー フィールドに設定されている IPv6 パケットだけをルールと一致させるように指定します。*flow-label-value* 引数は、0 ～ 1048575 の整数です。
fragments	（任意）非初期フラグメントであるパケットだけをルールと一致させるように指定します。デバイスでは、非初期フラグメントであるパケットが、ゼロと同等ではないフラグメント オフセットが含まれるフラグメント拡張ヘッダーを持つパケットと見なされます。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定したルールには指定できません。これらのオプションをデバイスが評価するために必要な情報は、初期フラグメントだけに含まれているためです。
time-range *time-range-name*	（任意）このルールに適用する時間範囲を指定します。**time-range** コマンドを使用して時間範囲を設定できます。

icmp-message	（ICMP 限定：任意）ルールと一致させる ICMPv6 メッセージのタイプ。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」の「ICMPv6 メッセージ タイプ」にリストされているキーワードの 1 つを指定します。
operator port [*port*]	（任意：TCP、UDP および SCTP 限定）*operator* 引数および *port* 引数の条件と一致する送信元ポートから送信されたパケット、または一致する宛先ポートに送信されたパケットだけを、ルールと一致させます。これらの引数が送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定します。有効な番号は 0 ～ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の *port* 引数は、*operator* 引数が範囲である場合だけ必要です。 *operator* 引数には、次のいずれかのキーワードを指定する必要があります。 • **eq**：パケットのポートが *port* 引数と同等である場合だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数以上で、2 番目の *port* 引数以下である場合だけ一致します。
portgroup *portgroup*	（任意：TCP、UDP、および SCTP 限定）*portgroup* 引数で指定された IP ポート グループ オブジェクトのメンバである送信元ポートから送信されたパケット、またはメンバである宛先ポートに送信されたパケットだけを、ルールと一致させるように指定します。ポート グループ オブジェクトが送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 IP ポート グループ オブジェクトを作成および変更するには、**object-group ip port** コマンドを使用します。
flags	（TCP 限定：任意）特定の TCP コントロール ビット フラグがオンに設定されたパケットだけを、ルールと一致させます。*flags* 引数の値には、次の 1 つ以上のキーワードを指定する必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	（TCP 限定：任意）確立された TCP 接続に属すパケットだけをルールと一致させるように指定します。デバイスは、ACK または RST ビットが設定されている TCP パケットが、確立された接続に属していると見なします。

コマンド デフォルト なし

コマンド モード　IPv6 ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン　新しく作成した IPv6 ACL には、ルールは含まれていません。

デバイスは、パケットに IPv6 ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。デバイスで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、デバイスはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、1 つの引数の指定方法によって、他の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）: IPv6 アドレスおよび VLSM を使用して、送信元または宛先とするホストまたはネットワークを指定できます。構文は次のとおりです。

  IPv6-address/prefix-len

  次に、2001:0db8:85a3:: ネットワークの IPv6 アドレスおよび VLSM を使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit udp 2001:0db8:85a3::/48 any
  ```

- ホスト アドレス：**host** キーワードおよび IPv6 アドレスを使用して、送信元または宛先とするホストを指定できます。構文は次のとおりです。

  host *IPv6-address*

  この構文は、*IPv6-address*/128 と同じです。

  次に、**host** キーワードおよび 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 アドレスを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先として任意の IPv6 アドレスを指定できます。**any** キーワードの使用例は、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

ICMPv6 メッセージ タイプ

igmp-message 引数には、0 ～ 255 の整数である ICMPv6 メッセージ番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **beyond-scope**：範囲外の宛先
- **destination-unreachable**：宛先アドレスに到達不能
- **echo-reply**：エコー応答
- **echo-request**：エコー要求（ping）
- **header**：パラメータ ヘッダーの問題
- **hop-limit**：中継時にホップ制限を超過

- **mld-query**：マルチキャスト リスナー ディスカバリ クエリー
- **mld-reduction**：マルチキャスト リスナー ディスカバリ リダクション
- **mld-reduction**：マルチキャスト リスナー ディスカバリ レポート
- **nd-na**：ネイバー探索のネイバー アドバタイズメント
- **nd-ns**：ネイバー探索のネイバー送信要求
- **next-header**：パラメータの次のヘッダーの問題
- **no-admin**：管理者が宛先を禁止
- **no-route**：宛先へのルートなし
- **packet-too-big**：パケット サイズ超過
- **parameter-option**：パラメータ オプションの問題
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：ポート到達不能
- **reassembly-timeout**：再構成タイムアウト
- **redirect**：ネイバーのリダイレクト
- **renum-command**：ルータの番号付けコマンド
- **renum-result**：ルータの番号付けの結果
- **renum-seq-number**：ルータの番号付けのシーケンス番号リセット
- **router-advertisement**：ネイバー探索のルータ アドバタイズメント
- **router-renumbering**：すべてのルータの再番号付け
- **router-solicitation**：ネイバー探索のルータ送信要求
- **time-exceeded**：すべてのタイム超過メッセージ
- **unreachable**：すべての到達不能

TCP ポート名

protocol 引数に **tcp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である TCP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **bgp**：Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）
- **chargen**：キャラクタ ジェネレータ（19）
- **cmd**：リモート コマンド（rcmd、514）
- **daytime**：デイタイム（13）
- **discard**：廃棄（9）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **drip**：Dynamic Routing Information Protocol（DRIP; ダイナミック ルーティング情報プロトコル）（3949）
- **echo**：エコー（7）
- **exec**：Exec（rsh、512）
- **finger**：フィンガー（79）
- **ftp**：File Transfer Protocol（FTP; ファイル転送プロトコル）（21）
- **ftp-data**：FTP データ接続（2）

- **gopher**：Gopher（7）
- **hostname**：NIC ホストネーム サーバ（11）
- **ident**：Ident プロトコル（113）
- **irc**：Internet Relay Chat（IRC; インターネット リレー チャット）（194）
- **klogin**：Kerberos ログイン（543）
- **kshell**：Kerberos シェル（544）
- **login**：ログイン（rlogin、513）
- **lpd**：プリンタ サービス（515）
- **nntp**：Network News Transport Protocol（NNTP）（119）
- **pim-auto-rp**：PIM Auto-RP（496）
- **pop2**：Post Office Protocol v2（POP2）（19）
- **pop3**：Post Office Protocol v3（POP3）（11）
- **smtp**：Simple Mail Transport Protocol（SMTP; シンプル メール転送プロトコル）（25）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）
- **telnet**：Telnet（23）
- **time**：Time（37）
- **uucp**：UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）（54）
- **whois**：WHOIS/NICNAME（43）
- **www**：World Wide Web（HTTP、8）

UDP ポート名

protocol 引数に **udp** を指定した場合、*port* 引数として 0 ～ 65535 の整数である UDP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- **biff**：BIFF（メール通知、comsat、512）
- **bootpc**：Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）
- **bootps**：ブートストラップ プロトコル（BOOTP）サーバ（67）
- **discard**：廃棄（9）
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **echo**：エコー（7）
- **isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（5）
- **mobile-ip**：モバイル IP レジストレーション（434）
- **nameserver**：IEN116 ネーム サービス（旧式、42）
- **netbios-dgm**：NetBIOS データグラム サービス（138）
- **netbios-ns**：NetBIOS ネーム サービス（137）
- **netbios-ss**：NetBIOS セッション サービス（139）
- **non500-isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（45）

- **ntp**：Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）
- **pim-auto-rp**：PIM Auto-RP（496）
- **rip**：Routing Information Protocol（RIP）（ルータ、in.routed、52）
- **snmp**：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）
- **snmptrap**：SNMP トラップ（162）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **syslog**：システム ロギング（514）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）
- **tftp**：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（69）
- **time**：Time（37）
- **who**：Who サービス（rwho、513）
- **xdmcp**：X Display Manager Control Protocol（XDMCP）（177）

例

次に、acl-lab13-ipv6 という IPv6 ACL を作成し、2001:0db8:85a3:: ネットワークおよび 2001:0db8:69f2:: ネットワークから 2001:0db8:be03:2112:: ネットワークへのすべての TCP トラフィックおよび UDP トラフィックを許可するルールを設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

次に、ipv6-eng-to-marketing という IPv6 ACL を作成し、eng_ipv6 という IPv6 アドレス オブジェクト グループから marketing_group という IPv6 アドレス オブジェクト グループへのすべての IPv6 トラフィックを許可するルールを設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

関連コマンド

コマンド	説明
deny（IPv6）	IPv6 ACL に拒否（deny）ルールを設定します。
ipv6 access-list	IPv6 ACL を設定します。
remark	ACL に備考を設定します。

permit（MAC）

条件と一致するトラフィックを許可する MAC アクセス コントロール リスト（ACL）ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no permit *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no *sequence-number*

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。スイッチによってアクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、スイッチは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
source	ルールで一致させる送信元 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
protocol	（任意）ルールで一致させるプロトコルの番号。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なプロトコル名のリストは、「使用上のガイドライン」の「MAC プロトコル」を参照してください。
cos *cos-value*	（任意）IEEE 802.1Q ヘッダーに、*cos-value* 引数で指定したサービス クラス（CoS）値が含まれているパケットだけにルールが一致するように指定します。*cos-value* 引数は、0 ～ 7 の整数です。
vlan *vlan-id*	（任意）IEEE 802.1Q ヘッダーに、指定した VLAN ID が含まれているパケットだけにルールが一致するように指定します。*vlan-id* 引数は、1 ～ 4094 の整数に指定できます。

コマンド デフォルト

新しく作成した MAC ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、スイッチで ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号が割り当てられます。

コマンド モード

MAC ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは、パケットに MAC ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。スイッチで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、スイッチはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、1 つの引数の指定方法によって、他の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびマスク：MAC アドレスの後にマスクを指定して、1 つのアドレスまたはアドレスグループを指定できます。構文は次のとおりです。

  MAC-address MAC-mask

  次に、MAC アドレス 00c0.4f03.0a72 を持つ *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
  ```

  次に、*destination* 引数に、MAC ベンダー コードが 00603e のすべてのホストの MAC アドレスを指定する例を示します。

  ```
  switch(config-acl)# permit any 0060.3e00.0000 0000.0000.0000
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先として任意の MAC アドレスを指定できます。**any** キーワードの使用例は、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

MAC プロトコル

protocol 引数には、MAC プロトコルの番号またはキーワードを指定します。プロトコル番号は、プレフィックスが 0x である 4 バイト 16 進数です。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なキーワードは、次のとおりです。

- **aarp**：Appletalk ARP（0x80f3）
- **appletalk**：Appletalk（0x809b）
- **decnet-iv**：DECnet Phase IV（0x6003）
- **diagnostic**：DEC 診断プロトコル（0x6005）
- **etype-6000**：EtherType 0x6000（0x6000）
- **etype-8042**：EtherType 0x8042（0x8042）
- **ip**：インターネット プロトコル v4（0x0800）
- **lat**：DEC LAT（0x6004）
- **lavc-sca**：DEC LAVC、SCA（0x6007）
- **mop-console**：DEC MOP リモート コンソール（0x6002）
- **mop-dump**：DEC MOP ダンプ（0x6001）
- **vines-echo**：VINES エコー（0x0baf）

例

次に、2 つの MAC アドレス グループ間ですべての IPv4 トラフィックを許可するルールが含まれる mac-ip-filter という名前の MAC ACL を作成する例を示します。

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)#
```

関連コマンド

コマンド	説明
deny（MAC）	MAC ACL に拒否（deny）ルールを設定します。
mac access-list	MAC ACL を設定します。
remark	ACL に備考を設定します。
show mac access-list	すべての MAC ACL または 1 つの MAC ACL を表示します。

permit interface

ユーザ ロール インターフェイス ポリシーでインターフェイスを追加するには、**permit interface** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

permit interface *interface-list*

no permit interface

構文の説明

interface-list	ユーザ ロールがアクセスを許可されているインターフェイスのリストです。

コマンド デフォルト

すべてのインターフェイス

コマンド モード

インターフェイス ポリシー コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

permit interface ステートメントを機能させるには、次の例のように、コマンド ルールを設定してインターフェイス アクセスを許可する必要があります。

```
switch(config-role)# rule number permit command configure terminal ; interface *
```

例

次に、ユーザ ロール インターフェイス ポリシーでインターフェイス範囲を設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/2 - 8
```

次に、ユーザ ロール インターフェイス ポリシーでインターフェイスのリストを設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5
```

次に、ユーザ ロール インターフェイス ポリシーからインターフェイスを削除する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 1/2
```

関連コマンド

コマンド	説明
interface policy deny	ユーザ ロールのインターフェイス ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

permit vlan

ユーザ ロール VLAN ポリシーで VLAN を追加するには、**permit vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

permit vlan *vlan-list*

no permit vlan

構文の説明

vlan-list	ユーザ ロールがアクセスを許可されている VLAN のリストです。

コマンド デフォルト

すべての VLAN

コマンド モード

VLAN ポリシー コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

permit vlan ステートメントを機能させるには、次の例のように、コマンド **rule** を設定して VLAN アクセスを許可する必要があります。

```
switch(config-role)# rule number permit command configure terminal ; vlan *
```

例

次に、ユーザ ロール VLAN ポリシーで VLAN の範囲を設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

次に、ユーザ ロール VLAN ポリシーで VLAN のリストを設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
```

次に、ユーザ ロール VLAN ポリシーから VLAN を削除する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
```

関連コマンド

コマンド	説明
vlan policy deny	ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

permit vrf

ユーザ ロール VRF ポリシーで、Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスを追加するには、**permit vrf** コマンドを使用します。VRF を削除するには、このコマンドの **no** 形式を使用します。

permit vrf *vrf-list*

no permit vrf

構文の説明

vrf-list	ユーザ ロールがアクセスを許可されている VRF のリストです。

コマンド デフォルト

すべての VRF

コマンド モード

VRF ポリシー コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール VRF ポリシーで VRF の範囲を設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
```

関連コマンド

コマンド	説明
vrf policy deny	ユーザ ロールの VRF ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

permit vsan

ユーザ ロールに VSAN ポリシーへのアクセスを許可するには、**permit vsan** コマンドを使用します。ユーザ ロールのデフォルトの VSAN ポリシー設定に戻すには、このコマンドの **no** 形式を使用します。

permit vsan *vsan-list*

no permit vsan *vsan-list*

構文の説明

vsan-list	ユーザ ロールがアクセスできる VSAN の範囲です。有効な範囲は 1 ～ 4093 です。 次の区切り記号を使用して範囲を区切ることができます。 • **,** は、1-5, 10, 12, 100-201 のように複数の範囲を区切る記号です。 • **-** は、101-201 のように範囲を区切る記号です。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**vsan policy deny** コマンドを使用して VSAN ポリシーを拒否した後にのみイネーブルになります。

例

次に、ユーザ ロールに VSAN ポリシーへのアクセスを許可する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# permit vsan 10, 12, 100-104
switch(config-role-vsan)#
```

関連コマンド

コマンド	説明
vsan policy deny	ユーザの VSAN ポリシーへのアクセスを拒否します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

R コマンド

この章では、R で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

radius-server deadtime

Cisco Nexus 5000 シリーズ スイッチにすべての RADIUS サーバのデッド タイム間隔を設定するには、**radius-server deadtime** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

構文の説明

minutes	デッド タイム間隔の分数。有効な範囲は 1 ～ 1440 分です。

コマンド デフォルト

0 分

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

デッド タイム間隔は、応答のなかった RADIUS サーバをスイッチが確認するまでの分数です。

（注） アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

例

次に、すべての RADIUS サーバの定期的なモニタリングを実行するグローバル デッド タイム間隔を設定する例を示します。

```
switch(config)# radius-server deadtime 5
```

次に、すべての RADIUS サーバのグローバル デッド タイム間隔をデフォルトに戻して、サーバの定期的なモニタリングをディセーブルにする例を示します。

```
switch(config)# no radius-server deadtime 5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server directed-request

ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにするには、**radius-server directed-request** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server directed-request

no radius-server directed-request

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

設定した RADIUS サーバ グループに認証要求を送信します。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

ログイン時、*username@vrfname*:*hostname* を指定できます。*vrfname* は使用する VRF、*hostname* は設定した RADIUS サーバ名です。ユーザ名が認証用に RADIUS サーバに送信されます。

例

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにする例を示します。

```
switch(config)# radius-server directed-request
```

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できないようにする例を示します。

```
switch(config)# no radius-server directed-request
```

関連コマンド

コマンド	説明
show radius-server directed-request	指定要求 RADIUS サーバ設定を表示します。

radius-server host

RADIUS サーバ パラメータを設定するには、**radius-server host** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

構文の説明

hostname	RADIUS サーバの Domain Name Server（DNS; ドメイン ネーム サーバ）名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。
ipv4-address	*A.B.C.D* 形式の RADIUS サーバの IPv4 アドレス。
ipv6-address	*X:X:X:X* フォーマットの RADIUS サーバの IPv6 アドレス。
key	（任意）RADIUS サーバ事前共有秘密キーを設定します。
0	（任意）RADIUS クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有キーを設定します。これはデフォルトです。
7	（任意）RADIUS クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有キー（7 で表示）を設定します。
shared-secret	RADIUS クライアントとサーバ間の通信を認証する事前共有キー。事前共有キーには、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。大文字と小文字が区別され、最大文字数は 63 です。
pac	（任意）Cisco TrustSec と連動させるために、RADIUS Cisco ACS サーバで Protected Access Credentials（PAC）の生成をイネーブルにします。
accounting	（任意）アカウンティングを設定します。
acct-port *port-number*	（任意）アカウンティング用の RADIUS サーバのポートを設定します。指定できる範囲は 0 ～ 65535 です。
auth-port *port-number*	（任意）認証用の RADIUS サーバのポートを設定します。指定できる範囲は 0 ～ 65535 です。
authentication	（任意）認証を設定します。
retransmit *count*	（任意）スイッチがローカル認証に戻る前に RADIUS サーバへの接続試行を行う回数を設定します。有効な範囲は 1 ～ 5 回で、デフォルトは 1 回です。
test	（任意）テスト パケットを RADIUS サーバに送信するようにパラメータを設定します。
idle-time *time*	サーバをモニタリングするための時間間隔を分で指定します。有効な範囲は 1 ～ 1440 分です。
password *password*	テスト パケット内のユーザ パスワードを指定します。パスワードは、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。

username *name*	テスト パケット内のユーザ名を指定します。ユーザ名は、英数字で指定します。大文字と小文字の区別がなく、最大文字数は 32 です。
timeout *seconds*	RADIUS サーバへの再送信タイムアウト（秒単位）を指定します。デフォルトは 1 秒です。有効な範囲は 1 ～ 60 秒です。

コマンド デフォルト

アカウンティング ポート：1813
認証ポート：1812
アカウンティング：イネーブル
認証：イネーブル
再送信数：1
アイドル時間：0
サーバ モニタリング：ディセーブル
タイムアウト：5 秒
テスト ユーザ名：test
テスト パスワード：test

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

例

次に、RADIUS サーバの認証とアカウンティングのパラメータを設定する例を示します。

```
switch(config)# radius-server host 192.168.2.3 key HostKey
switch(config)# radius-server host 192.168.2.3 auth-port 2003
switch(config)# radius-server host 192.168.2.3 acct-port 2004
switch(config)# radius-server host 192.168.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 192.168.2.3 test idle-time 10
switch(config)# radius-server host 192.168.2.3 test username tester
switch(config)# radius-server host 192.168.2.3 test password 2B9ka5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server key

RADIUS 共有秘密キーを設定するには、**radius-server key** コマンドを使用します。設定した共有秘密キーを削除するには、このコマンドの **no** 形式を使用します。

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

構文の説明

0	（任意）RADIUS クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有キーを設定します。
7	（任意）RADIUS クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有キーを設定します。
shared-secret	RADIUS クライアントとサーバ間の通信を認証するために使用される事前共有キー。事前共有キーには、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。大文字と小文字が区別され、最大文字数は 63 です。

コマンド デフォルト

クリア テキスト認証

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

RADIUS 事前共有キーを設定して、RADIUS サーバに対してスイッチを認証する必要があります。キーの長さは 65 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。グローバル キーは、スイッチにあるすべての RADIUS サーバ コンフィギュレーションで使用するよう設定できます。**radius-server host** コマンドで **key** キーワードを使用することでこのグローバル キーの割り当てを上書きできます。

例

次に、RADIUS 認証を設定する各種のシナリオを提供する例を示します。

```
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server retransmit

スイッチが RADIUS サーバで要求を試行する回数を指定するには、**radius-server retransmit** コマンドを使用する必要があります。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server retransmit *count*

no radius-server retransmit *count*

構文の説明

count	スイッチがローカル認証に戻る前に RADIUS サーバへの接続試行を行う回数。有効な範囲は 1 ～ 5 回です。

コマンド デフォルト

再送信 1 回

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、RADIUS サーバに再送信回数を設定する例を示します。

```
switch(config)# radius-server retransmit 3
```

次に、RADIUS サーバに再送信のデフォルト数を設定する例を示します。

```
switch(config)# no radius-server retransmit 3
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server timeout

RADIUS サーバへの再送信間隔を指定するには、**radius-server timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server timeout *seconds*

no radius-server timeout *seconds*

構文の説明

seconds	RADIUS サーバへの再送信間隔の秒数。有効な範囲は 1 ～ 60 秒です。

コマンド デフォルト

1 秒

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、タイムアウト間隔を設定する例を示します。

```
switch(config)# radius-server timeout 30
```

次に、デフォルトの間隔に戻す例を示します。

```
switch(config)# no radius-server timeout 30
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

remark

IPv4 または MAC アクセス コントロール リスト（ACL）にコメントを入力するには、**remark** コマンドを使用します。**remark** コマンドを削除するには、このコマンドの no 形式を使用します。

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

構文の説明

sequence-number	（任意）**remark** コマンドのシーケンス番号。これにより、スイッチはアクセス リストの番号が指定された位置にコマンドを挿入します。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、スイッチは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 **resequence** コマンドを使用して、シーケンス番号をリマークとルールに再度割り当てます。
remark	リマークのテキスト。引数に使用できる文字数は最大 100 文字です。

コマンド デフォルト

デフォルトでは、ACL にリマークが含まれません。

コマンド モード

IPv4 ACL コンフィギュレーション モード
MAC ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

remark 引数には、最大 100 文字を指定できます。*remark* 引数に 100 を超える文字を入力すると、スイッチは最初の 100 文字を受け入れ、後の文字を廃棄します。

例

次に、IPv4 ACL にリマークを作成して、結果を表示する例を示します。

```
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-list	すべての ACL または 1 つの ACL を表示します。

resequence

アクセス コントロール リスト（ACL）のすべてのルールまたは時間の範囲にシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。

resequence *access-list-type* access-list *access-list-name starting-number increment*

resequence time-range *time-range-name starting-number increment*

構文の説明

access-list-type	ACL のタイプ。この引数の有効値は、次のキーワードです。 • **arp** • **ip** • **mac**
access-list *access-list-name*	ACL の名前を指定します。
time-range *time-range-name*	時間範囲の名前を指定します。
starting-number	ACL の最初のルールまたは時間の範囲のシーケンス番号。
increment	スイッチが後続の各シーケンス番号に追加する数。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

resequence コマンドを使用すると、ACL のルールまたは時間の範囲にシーケンス番号を再度割り当てることができます。最初のルールの新しいシーケンス番号は、*starting-number* 引数によって決まります。その他の各ルールは、*increment* 引数によって決まる新しいシーケンス番号を受け取ります。最大シーケンス番号がシーケンス番号の許容最大値を超えると、シーケンスが実行されず、次のメッセージが表示されます。

```
ERROR: Exceeded maximum sequence number.
```

最大シーケンス番号は、4294967295 です。

例

次に、**show ip access-lists** コマンドを使用して、100 のシーケンス番号で開始し、10 ずつ増える ip-acl-01 という名前の IPv4 ACL のシーケンスを再度実行し、**resequence** コマンドの使用の前後のシーケンス番号を確認する例を示します。

```
switch(config)# show ip access-lists ip-acl-01
```

```
IP access list ip-acl-01
        7 permit tcp 128.0.0.0/16 any eq www
        10 permit udp 128.0.0.0/16 any
        13 permit icmp 128.0.0.0/16 any eq echo
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp 128.0.0.0/16 any eq www
        110 permit udp 128.0.0.0/16 any
        120 permit icmp 128.0.0.0/16 any eq echo
        130 deny igmp any any
switch(config)#
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。

role feature-group name

ユーザ ロール機能グループを作成または指定し、ユーザ ロール機能グループ コンフィギュレーション モードを開始するには、**role feature-group name** コマンドを使用します。ユーザ ロール機能グループを削除するには、このコマンドの **no** 形式を使用します。

role feature-group name *group-name*

no role feature-group name *group-name*

構文の説明

group-name	ユーザ ロール機能グループ名。*group-name* の最大文字数は 32 で、大文字と小文字が区別され、英数字文字列で指定します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール機能グループを作成して、ユーザ ロール機能グループ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

次に、ユーザ ロール機能グループを削除する例を示します。

```
switch(config)# no role feature-group name MyGroup
switch(config)#
```

関連コマンド

コマンド	説明
feature-group name	ユーザ ロール機能グループを指定または作成して、ユーザ ロール機能グループ コンフィギュレーション モードを開始します。
show role feature-group	ユーザ ロール機能グループを表示します。

role name

ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始するには、**role name** コマンドを使用します。ユーザ ロールを削除するには、このコマンドの **no** 形式を使用します。

role name {*role-name* | **default-role** | *privilege-role*}

no role name {*role-name* | **default-role** | *privilege-role*}

構文の説明

role-name	ユーザ ロール名。*role-name* の最大文字数は 16 で、大文字と小文字が区別され、英数字文字列で指定します。
default-role	デフォルトのユーザ ロール名を指定します。
privilege-role	特権のあるユーザ ロール。次のいずれかの値になります。 • priv-0 • priv-1 • priv-2 • priv-3 • priv-4 • priv-5 • priv-6 • priv-7 • priv-8 • priv-9 • priv-10 • priv-11 • priv-12 • priv-13

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.0(2)N1(1)	権限ロール作成のサポートが追加されました。

使用上のガイドライン

Cisco Nexus 5000 シリーズ スイッチには、次のデフォルトのユーザ ロールがあります。

- ネットワーク管理者：スイッチ全体の読み取りおよび書き込みアクセスを完了します。
- スイッチ全体の読み取りアクセスを完了します。

デフォルトのユーザ ロールは変更または削除できません。

特権レベルのロールを表示するには、**feature privilege** コマンドを使用して TACACS+ サーバでのコマンド認可にロールの累積権限をイネーブルにする必要があります。権限ロールは、レベルが低い方の権限ロールの権限を継承します。

例

次に、ユーザ ロールを作成して、ユーザ ロール コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)#
```

次に、特権レベル 1 のユーザ ロールを作成して、ユーザ ロール コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name priv-1
switch(config-role)#
```

次に、ユーザ ロールを削除する例を示します。

```
switch(config)# no role name MyRole
```

関連コマンド

コマンド	説明
feature privilege	TACACS+ サーバでのコマンド認可に対するロールの累積権限をイネーブルにします。
rule	ユーザ ロールのルールを設定します。
show role	ユーザ ロールを表示します。

rollback running-config

実行コンフィギュレーションをロールバックするには、**rollback running-config** コマンドを使用します。

rollback running-config {**checkpoint** *checkpoint-name* | **file** {**bootflash:** | **volatile:**}[*//server*][*directory/*][*filename*] [**atomic**] [**verbose**]}

構文の説明

checkpoint	実行コンフィギュレーションがチェックポイントにロールバックされるよう指定します。
checkpoint-name	チェックポイント名。名前は、最大 32 文字まで指定できます。
file	実行コンフィギュレーションがコンフィギュレーション ファイルにロールバックされるよう指定します。
bootflash:	書き込み可能なブートフラッシュ ローカル ストレージ ファイル システムを指定します。
volatile:	揮発性の書き込み可能なローカル ストレージ ファイル システムを指定します。
//server	サーバの名前。有効な値は、**///**、**//module-1/**、**//sup-1/**、**//sup-active/** または **//sup-local/** です。2 個のスラッシュ（//）を含む必要があります。
directory/	ディレクトリの名前。ディレクトリ名では、大文字と小文字が区別されます。
filename	チェックポイント コンフィギュレーション ファイルの名前。ファイル名では、大文字と小文字が区別されます。
atomic	（任意）パッチの適用中に初めて失敗すると、ロールバック実行を中止するように指定します。これは、デフォルトのモードです。
verbose	（任意）ロールバック実行手順がロールバック操作中に表示されるように指定します。

（注） *filesystem*://*server*/*directory*/*filename* ストリングにはスペースを含めることはできません。この文字列の各要素は、コロン（:）とスラッシュ（/）で区切ります。

コマンド デフォルト

アトミック ロールバック

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

チェックポイント名またはファイルにロールバックできます。ロールバックする前に、**show diff rollback-patch** コマンドを使用して、現在のコンフィギュレーションまたは保存されているコンフィギュレーションを参照している送信元と宛先のチェックポイント間の差異を表示できます。

指定されたチェックポイントへのロールバックがチェックポイント コンフィギュレーションにシステムのアクティブ コンフィギュレーションを復元します。

ブートフラッシュ時のファイルへのロールバックは、**checkpoint** *checkpoint_name* コマンドを使用して作成されたファイルでのみサポートされます。他の ASCII タイプのファイルではサポートされません。

（注） atomic ロールバック中に設定を変更すると、ロールバックは失敗します。手動でエラーを修正し、**rollback** コマンドを実行する必要があります。

例

次に、verbose モードで chkpnt-1 という名前のチェックポイントに実行コンフィギュレーションをロールバックする例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration--->
switch# rollback running-config chkpnt-1 verbose
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
#Generating Rollback Patch
Rollback Patch is Empty

Rollback completed successfully.

switch#
```

次に、ブートフラッシュ ストレージ システムの chkpnt_configSep9-1.txt というチェックポイント コンフィギュレーション ファイルに実行コンフィギュレーションをロールバックする例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
switch# rollback running-config file bootflash:///chkpnt_configSep9-1.txt
switch#
```

関連コマンド

コマンド	説明
rollback	保存されたすべてのチェックポイントにスイッチをロールバックします。
show checkpoint	チェックポイント情報を表示します。
show diff rollback-patch checkpoint	現在のチェックポイントと保存済みコンフィギュレーションの差異を表示します。

コマンド	説明
show diff rollback-patch file	現在のチェックポイント ファイルと保存済みコンフィギュレーションの差異を表示します。
show diff rollback-patch running-config	現在の実行コンフィギュレーションと保存済みチェックポイント コンフィギュレーションの差異を表示します。

rule

ユーザ ロールのルールを設定するには、**rule** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

構文の説明

number	ルールのシーケンス番号。スイッチは、最初に最大値を使用してルールを適用し、以降は降順で適用されます。
deny	コマンドまたは機能へのアクセスを拒否します。
permit	コマンドまたは機能へのアクセスを許可します。
command *command-string*	コマンド ストリングを指定します。コマンド文字列は最大 128 文字で、スペースを含めることができます。
read	読み取りアクセスを指定します。
read-write	読み取りおよび書き込みアクセスを指定します。
feature *feature-name*	（任意）機能名を指定します。スイッチの機能名を表示するには、**show role feature** コマンドを使用します。
feature-group *group-name*	（任意）機能グループを指定します。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.0(2)N1(1)	拒否ルールを特権 0（priv-0）ロールに追加できます。

使用上のガイドライン

ロールごとに最大 256 のルールを設定できます。

指定するルール番号は、適用したルールの順序を決めます。ルールは降順で適用されます。たとえば、ロールに 3 つのルールがある場合、ルール 3、ルール 2、ルール 1 の順に適用されます。

拒否（deny）ルールは、どの権限ロールにも追加できません（特権レベル 0（priv-0）のロールを除きます）。

例

次に、ユーザ ロールにルールを追加する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

次に、特権レベル 0 のユーザ ロールにルールを追加する例を示します。

```
switch(config)# role name priv-0
switch(config-role)# rule 1 deny command clear users
switch(config-role)#
```

次に、ユーザ ロールからルールを削除する例を示します。

```
switch(config)# role MyRole
switch(config-role)# no rule 10
```

関連コマンド

コマンド	説明
role name	ユーザ ロール名を作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールを表示します。

S コマンド

この章では、S で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

server

RADIUS サーバ グループまたは TACACS+ サーバ グループにサーバを追加するには、**server** コマンドを使用します。サーバ グループからサーバを削除するには、このコマンドの **no** 形式を使用します。

server {*ipv4-address* | *ipv6-address* | *hostname*}

no server {*ipv4-address* | *ipv6-address* | *hostname*}

構文の説明

ipv4-address	*A.B.C.D* 形式のサーバの IPv4 アドレス
ipv6-address	*X:X:X::X* 形式のサーバの IPv6 アドレス
hostname	サーバ名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。

コマンド デフォルト

なし

コマンド モード

RADIUS サーバ グループ コンフィギュレーション モード
TACACS+ サーバ グループ コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

サーバ グループには、最大 64 のサーバを設定できます。

RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。

サーバを検索できなかった場合、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してサーバを設定します。

（注） TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、RADIUS サーバ グループにサーバを追加する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 192.168.1.1
```

次に、RADIUS サーバ グループからサーバを削除する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 192.168.1.1
```

次に、TACACS+ サーバ グループにサーバを追加する例を示します。

```
switch(config)# feature tacacs+
```

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 192.168.2.2
```

次に、TACACS+ サーバ グループからサーバを削除する例を示します。

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 192.168.2.2
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ グループ情報を表示します。
show tacacs-server groups	TACACS+ サーバ グループ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

ssh

IPv4 を使用してセキュア シェル（SSH）セッションを作成するには、**ssh** コマンドを使用します。

ssh [*username@*]{*ipv4-address* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}]

構文の説明

username	（任意）SSH セッションのユーザ名。ユーザ名は、大文字と小文字の区別がなく、最大文字数は 64 です。
ipv4-address	リモート ホストの IPv4 アドレスです。
hostname	リモート ホストのホスト名です。ホスト名は、大文字と小文字が区別され、最大文字数は 64 です。
vrf *vrf-name*	（任意）SSH セッションで使用する Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）名を指定します。この名前には最大 32 文字までの英数字を指定できます。
default	デフォルト VRF を指定します。
management	管理 VRF を指定します。

コマンド デフォルト

デフォルト VRF

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

次に、IPv4 を使用して SSH セッションを開始する例を示します。

```
switch# ssh 192.168.1.1 vrf management
```

関連コマンド

コマンド	説明
clear ssh session	SSH セッションを消去します。
ssh server enable	SSH サーバをイネーブルにします。
ssh6	IPv6 アドレスを使用して SSH セッションを開始します。

ssh6

IPv6 を使用してセキュア シェル（SSH）セッションを作成するには、**ssh6** コマンドを使用します。

ssh6 [*username@*]{*ipv6-address* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}]

構文の説明

username	（任意）SSH セッションのユーザ名。ユーザ名は、大文字と小文字の区別がなく、最大文字数は 64 です。
ipv6-address	リモート ホストの IPv6 アドレスです。
hostname	リモート ホストのホスト名です。ホスト名は、大文字と小文字が区別され、最大文字数は 64 です。
vrf *vrf-name*	（任意）SSH IPv6 セッションで使用する Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）名を指定します。この名前には最大 32 文字までの英数字を指定できます。
default	デフォルト VRF を指定します。
management	管理 VRF を指定します。

コマンド デフォルト

デフォルト VRF

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

次に、IPv6 を使用して SSH セッションを開始する例を示します。

```
switch# ssh6 2001:0DB8::200C:417A vrf management
```

関連コマンド

コマンド	説明
clear ssh session	SSH セッションを消去します。
ssh	IPv4 アドレスを使用して SSH セッションを開始します。
ssh server enable	SSH サーバをイネーブルにします。

ssh key

セキュア シェル（SSH）サーバ キーを作成するには、**ssh key** コマンドを使用します。SSH サーバ キーを削除するには、このコマンドの **no** 形式を使用します。

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

構文の説明

dsa	Digital System Algorithm（DSA）SSH サーバ キーを指定します。
force	（任意）以前のイベントが存在する場合に、DSA SSH キー イベントを強制的に生成します。
rsa	Rivest, Shamir, and Adelman（RSA）公開キー暗号法の SSH サーバ キーを指定します。
length	（任意）SSH サーバ キーを作成するときに使用するビット数。有効な範囲は 768 ～ 2048 です。

コマンド デフォルト

1024 ビットの長さ

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS ソフトウェアは SSH バージョン 2 をサポートしています。

SSH サーバ キーを削除または交換する場合、**no ssh server enable** コマンドを使用してまず SSH サーバをディセーブルにする必要があります。

例

次に、デフォルトのキーの長さで RSA を使用して SSH サーバ キーを作成する例を示します。

```
switch(config)# ssh key rsa
```

次に、指定したキーの長さで RSA を使用して SSH サーバ キーを作成する例を示します。

```
switch(config)# ssh key rsa 768
```

次に、force オプションで DSA を使用して SSH サーバ キーを交換する例を示します。

```
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

次に、DSA SSH サーバ キーを削除する例を示します。

```
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
```

```
switch(config)# ssh server enable
```

次に、すべての SSH サーバ キーを削除する例を示します。

```
switch(config)# no ssh server enable
switch(config)# no ssh key
switch(config)# ssh server enable
```

関連コマンド

コマンド	説明
show ssh key	SSH サーバ キーの情報を表示します。
ssh server enable	SSH サーバをイネーブルにします。

ssh server enable

セキュア シェル（SSH）サーバをイネーブルにするには、**ssh server enable** コマンドを使用します。SSH サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh server enable

no ssh server enable

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

次に、SSH サーバをイネーブルにする例を示します。

```
switch(config)# ssh server enable
```

次に、SSH サーバをディセーブルにする例を示します。

```
switch(config)# no ssh server enable
```

関連コマンド

コマンド	説明
show ssh server	SSH サーバ キーの情報を表示します。

storm-control level

トラフィック ストーム制御の抑制レベルを設定するには、**storm-control level** コマンドを使用します。抑制モードをオフにしたり、デフォルトの設定に戻したりするには、このコマンドの **no** 形式を使用します。

storm-control {**broadcast** | **multicast** | **unicast**} **level** *percentage*[.*fraction*]

no storm-control {**broadcast** | **multicast** | **unicast**} **level**

構文の説明

broadcast	ブロードキャスト トラフィックを指定します。
multicast	マルチキャスト トラフィックを指定します。
unicast	ユニキャスト トラフィックを指定します。
level *percentage*	抑制レベルの割合を指定します。有効な範囲は 0 ～ 100% です。
fraction	（任意）抑制レベルの端数。有効な範囲は 0 ～ 99 です。

コマンド デフォルト

すべてのパケットが渡されます。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

storm-control level コマンドを入力して、インターフェイス上のトラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、インターフェイスでイネーブルにされているすべてのトラフィック ストーム制御モードにトラフィック ストーム制御レベルを適用します。

端数の抑制レベルを入力する場合、ピリオド（.）が必要になります。

抑制レベルは、合計帯域幅の割合です。100% のしきい値は、トラフィックに制限がないことを意味します。0 または 0.0（端数）% のしきい値は、指定されたすべてのトラフィックがポートでブロックされることを意味します。

廃棄カウントを表示するには、**show interfaces counters storm-control** コマンドを使用します。

指定したトラフィック タイプの抑制をオフにするには、次のいずれかの方式を使用します。

- 指定したトラフィック タイプのレベルを 100% に設定する。
- このコマンドの **no** 形式を使用する。

例

次に、ブロードキャスト トラフィックの抑制をイネーブルにし、抑制しきい値レベルを設定する例を示します。

```
switch(config-if)# storm-control broadcast level 30
```

次に、マルチキャスト トラフィックの抑制モードをディセーブルにする例を示します。

```
switch(config-if)# no storm-control multicast level
```

関連コマンド

コマンド	説明
show interface	インターフェイスのストーム制御抑制カウンタを表示します。
show running-config	インターフェイスの設定を表示します。

show コマンド

この章では、Cisco NX-OS セキュリティの **show** コマンドについて説明します。

show aaa accounting

Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）のアカウンティング設定を表示するには、**show aaa accounting** コマンドを使用します。

show aaa accounting

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、アカウンティング ログの設定を表示する例を示します。

```
switch# show aaa accounting
         default: local
switch#
```

関連コマンド

コマンド	説明
aaa accounting default	アカウンティングの AAA 方式を設定します。

show aaa authentication

Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）の認証設定情報を表示するには、**show aaa authentication** コマンドを使用します。

show aaa authentication login [**error-enable** | **mschap**]

構文の説明

error-enable	（任意）認証ログイン エラー メッセージ イネーブル コンフィギュレーションを表示します。
mschap	（任意）認証ログイン マイクロソフト チャレンジ ハンドシェーク認証プロトコル（MS-CHAP）イネーブル コンフィギュレーションを表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、設定された認証パラメータを表示する例を示します。

```
switch# show aaa authentication
         default: group t1
         console: group t1
switch#
```

次に、認証ログイン エラー イネーブル コンフィギュレーションを表示する例を示します。

```
switch# show aaa authentication login error-enable
disabled
switch#
```

次に、認証ログイン MS-CHAP コンフィギュレーションを表示する例を示します。

```
switch# show aaa authentication login mschap
MSCHAP is disabled
switch#
```

関連コマンド

コマンド	説明
aaa authentication	AAA 認証方式を設定します。

show aaa authorization

AAA 認可設定情報を表示するには、**show aaa authorization** コマンドを使用します。

show aaa authorization [**all**]

構文の説明

all	（任意）設定されている値とデフォルトの値を表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.2(1)N1(1)	このコマンドが追加されました。

例

次に、設定されている認可方式を表示する例を示します。

```
switch# show aaa authorization
AAA command authorization:
         default authorization for config-commands: none

switch#
```

関連コマンド

コマンド	説明
aaa authorization commands default	EXEC コマンドでデフォルト AAA 認可方式を設定します。
aaa authorization config-commands default	コンフィギュレーション コマンドでデフォルト AAA 認可方式を設定します。

show aaa groups

Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サーバ グループ コンフィギュレーションを表示するには、**show aaa groups** コマンドを使用します。

show aaa groups

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、AAA グループ情報を表示する例を示します。

```
switch# show aaa groups
radius
t1
tacacs
rad1
switch#
```

関連コマンド

コマンド	説明
aaa group server radius	RADIUS サーバ グループを作成します。

show aaa user

リモート認証の Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）サーバ管理者により割り当てられるデフォルト ロールのステータスを表示するには、**show aaa user** コマンドを使用します。

show aaa user default-role

構文の説明

default-role	デフォルト AAA ロールのステータスを表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、リモート認証の AAA サーバ管理者により割り当てられるデフォルト ロールのステータスを表示する例を示します。

```
switch# show aaa user default-role
enabled
switch#
```

関連コマンド

コマンド	説明
aaa user default-role	リモート認証のデフォルト ユーザを設定します。
show aaa authentication	AAA 認証情報を表示します。

show access-lists

すべての IPv4 アクセス コントロール リスト（ACL）および MAC ACL、または特定の ACL を表示するには、**show access-lists** コマンドを使用します。

show access-lists [*access-list-name*]

構文の説明

access-list-name	（任意）ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

コマンド デフォルト

access-list-name 引数を使用して ACL を指定する場合を除いて、スイッチはすべての ACL を表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スイッチ上のすべての IPv4 ACL および MAC ACL を表示する例を示します。

```
switch# show access-lists
```

Cisco NX-OS Release 5.0(2)N1(1) では、次の出力が表示されます。

```
switch# show access-lists

IP access list BulkData
        10 deny ip any any
IP access list CriticalData
        10 deny ip any any
IP access list Scavenger
        10 deny ip any any
MAC access list acl-mac
        10 permit any any
IP access list denyv4
        20 deny ip 10.10.10.0/24 10.20.10.0/24 fragments
        30 permit udp 10.10.10.0/24 10.20.10.0/24 lt 400
        40 permit icmp any any router-advertisement
        60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
        70 permit igmp any any host-report
        80 deny tcp any any rst
        90 deny tcp any any ack
        100 permit tcp any any fin
        110 permit tcp any gt 300 any lt 400
        130 deny tcp any range 200 300 any lt 600
        140 deny tcp any range 200 300 any lt 600
IP access list dot
        statistics per-entry
        10 permit ip 20.1.1.1 255.255.255.0 20.10.1.1 255.255.255.0 precedence f
lash-override
        20 deny ip 20.1.1.1/24 20.10.1.1/24 fragments
```

```
        30 permit tcp any any fragments
        40 deny tcp any eq 400 any eq 500
IP access list ipPacl
        statistics per-entry
        10 deny tcp any eq 400 any eq 500
IP access list ipv4
        10 permit ip 10.10.10.1 225.255.255.0 any fragments
        20 permit ip any any dscp ef
IP access list ipv4Acl
        10 permit ip 10.10.10.1/32 10.10.10.2/32
MAC access list test
        statistics per-entry
        10 deny 0000.1111.2222 0000.0000.0000 0000.1111.3333 ffff.0000.0000
IP access list voice
        10 remark - avaya rtp range
        20 permit udp any range 49072 50175 any range 49072 50175 dscp ef
        30 permit udp any range 49072 50175 any range 50176 50353 dscp ef
        40 permit udp any range 50176 50353 any range 49072 50175 dscp ef
        50 permit udp any range 50176 50353 any range 50176 50353 dscp ef
        60 permit udp any range 2048 2815 any range 2048 2815 dscp ef
        70 permit udp any range 2048 2815 any range 2816 3028 dscp ef
        80 permit udp any range 2816 3028 any range 2816 3028 dscp ef
        90 permit udp any range 2816 3028 any range 2048 2815 dscp ef
        100 remark -- cisco rtp range
switch#
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。

show accounting log

アカウンティングのログ内容を表示するには、**show accounting log** コマンドを使用します。

show accounting log [*size*] [**start-time** *year month day HH*:*MM*:*SS*] [**end-time** *year month day HH*:*MM*:*SS*]

構文の説明

size	（任意）表示するログの量（バイト単位）。有効な範囲は 0 ～ 250000 です。
start-time *year month day HH*:*MM*:*SS*	（任意）開始時刻を指定します。*year* 引数は、*yyyy* 形式です。*month* 引数は、3 文字の英語の略語です。*day* 引数の範囲は 1 ～ 31 です。*HH*:*MM*:*SS* 引数は、標準 24 時間形式です。
end-time *year month day HH*:*MM*:*SS*	（任意）終了時刻を指定します。*year* 引数は、*yyyy* 形式です。*month* 引数は、3 文字の英語の略語です。*day* 引数の範囲は 1 ～ 31 です。*HH*:*MM*:*SS* 引数は、標準 24 時間形式です。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、アカウンティング ログ全体を表示する例を示します。

```
switch# show accounting log
```

Cisco NX-OS Release では、このコマンドにより次の出力が表示されます。

```
switch# show accounting log

Mon Aug 16 09:37:43 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; interface vfc3 ; bind interface Ethernet1/12 (SUCCESS)
Mon Aug 16 09:38:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; interface vfc3 ; no shutdown (REDIRECT)
Mon Aug 16 09:38:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=Inte
rface vfc3 state updated to up
Mon Aug 16 09:38:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; interface vfc3 ; no shutdown (SUCCESS)
Mon Aug 16 09:38:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; interface vfc3 ; no shutdown (SUCCESS)
Mon Aug 16 09:48:05 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; interface Ethernet2/1 (SUCCESS)
Mon Aug 16 09:55:27 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; vtp mode client (FAILURE)
Mon Aug 16 09:55:35 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; vtp mode server (FAILURE)
Mon Aug 16 10:03:46 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; no vtp mode (FAILURE)
Mon Aug 16 10:04:11 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
```

```
igure terminal ; vtp mode transparent (SUCCESS)
Mon Aug 16 10:04:20 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; vtp domain MyDomain (SUCCESS)
Mon Aug 16 10:04:39 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; vtp password MyPass (SUCCESS)
Mon Aug 16 10:05:17 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; no vtp password (SUCCESS)
Mon Aug 16 10:06:46 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; vtp pruning (SUCCESS)
Mon Aug 16 10:09:11 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=conf
igure terminal ; interface Ethernet1/12 (SUCCESS)
Mon Aug 16 10:32:33 2010:type=update:id=72.163.177.184@pts/0:user=admin:cmd=clea
r vtp counters (SUCCESS)
Mon Aug 16 10:35:20 2010:type=stop:id=72.163.177.184@pts/0:user=admin:cmd=shell
terminated because of telnet closed
--More--
switch#
```

次に、アカウンティング ログの 400 バイトを表示する例を示します。

```
switch# show accounting log 400
```

次に、2008 年 2 月 16 日の 16:00:00 に開始するアカウンティング ログを表示する例を示します。

```
switch# show accounting log start-time 2008 Feb 16 16:00:00
```

次に、2008 年 2 月 1 日 15:59:59 に開始し、2008 年 2 月 29 日 16:00:00 に終了するアカウンティング ログを表示する例を示します。

```
switch# show accounting log start-time 2008 Feb 1 15:59:59 end-time 2008 Feb 29 16:00:00
```

関連コマンド

コマンド	説明
clear accounting log	アカウンティング ログを消去します。

show arp access-lists

すべての ARP アクセス コントロール リスト（ACL）または特定の ARP ACL を表示するには、**show arp access-lists** コマンドを使用します。

show arp access-lists [*access-list-name*]

構文の説明

access-list-name	（任意）ARP ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

（注） Cisco NX-OS Release 5.1(3)N1(1) 以降、ARP アクセス リストは、Control Plane Policing（CoPP）に対してだけサポートされます。

access-list-name 引数を使用して ACL を指定する場合を除いて、デバイスはすべての ARP ACL を表示します。

このコマンドには、ライセンスは必要ありません。

例

次に、スイッチ上のすべての ARP ACL を表示する例を示します。

```
switch# show arp access-lists
```

次に、arp-permit-all という名前の ARP ACL を表示する例を示します。

```
switch# show arp access-lists arp-permit-all
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を設定します。

show checkpoint

チェックポイントが実装されたときに設定を表示するには、**show checkpoint** コマンドを使用します。

show checkpoint [*checkpoint-name*] [**all** [**system** | **user**]]

構文の説明

checkpoint-name	（任意）チェックポイント名。名前は、最大 32 文字まで指定できます。
all	（任意）ユーザ設定チェック ポイントおよびシステム設定済みチェック ポイントを表示します。
system	（任意）すべてのシステム設定済みチェック ポイントを表示します。
user	（任意）すべてのユーザ設定チェック ポイントを表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

コマンド出力は、最新（最大 10）のチェックポイント ID の履歴を表示します。チェック ポイント ID はユーザがチェックポイントの設定にシステムを復元できるロールバック ポイントを表します。

例

次に、ローカル スイッチで設定されたロールバック チェックポイントを表示する例を示します。

```
switch# show checkpoint
--------------------------------------------------------------------------------
Name: chkpnt-1


!Command: Checkpoint cmd vdc 1
!Time: Mon Sep  6 09:40:47 2010

version 5.0(2)N1(1)
feature telnet
feature tacacs+
cfs eth distribute
feature private-vlan
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex

username adminbackup password 5 !  role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCAd7Nkhktzebsg5/0  role network-admin
no password strength-check
```

```
ip domain-lookup
ip domain-lookup
hostname switch
ip access-list ip1
class-map type qos class-fcoe
  match cos 4
class-map type qos match-all cq1
  match cos 4
  match precedence 7
class-map type qos match-all cq2
  match cos 5
  match dscp 10
class-map type qos match-any cq3
  match precedence 7

<--output truncated-->
switch#
```

次に、特定のチェックポイントに関する情報を表示する例を示します。

```
switch# show checkpoint chkpnt-1
------------------------------------------------------------------------------
Name: chkpnt-1


!Command: Checkpoint cmd vdc 1
!Time: Mon Sep  6 09:40:47 2010

version 5.0(2)N1(1)
feature telnet
feature tacacs+
cfs eth distribute
feature private-vlan
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex

username adminbackup password 5 !  role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCAd7Nkhktzebsg5/0  role network-admin
no password strength-check
ip domain-lookup
ip domain-lookup
hostname switch
ip access-list ip1
class-map type qos class-fcoe
  match cos 4
class-map type qos match-all cq1
  match cos 4
  match precedence 7
--More--
switch#
```

次に、設定済みのすべてのロールバック チェックポイントを表示する例を示します。

```
switch# show checkpoint all
```

関連コマンド

コマンド	説明
checkpoint	チェックポイントを作成します。
rollback	保存されたすべてのチェックポイントに設定をロールバックします。
show checkpoint summary	コンフィギュレーション ロールバック チェックポイントのサマリーを表示します。
show checkpoint system	システム定義のロールバック チェックポイントを表示します。
show checkpoint user	ユーザ設定のロールバック チェックポイントを表示します。

show checkpoint summary

設定済みチェックポイントの要約を表示するには、**show checkpoint summary** コマンドを使用します。

show checkpoint summary [**system** | **user**]

構文の説明

system	（任意）システム設定チェックポイントの要約を表示します。
user	（任意）ユーザ設定チェックポイントの要約を表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、コンフィギュレーション ロールバック チェックポイントのサマリーを表示する例を示します。

```
switch# show checkpoint summary
User Checkpoint Summary
User Checkpoint Summary
--------------------------------------------------------------------------------
1) chkpnt-1:
Created by admin
Created at Tue, 08:10:23 14 Sep 2010
Size is 21,508 bytes
Description: Checkpoint to save current configuration, Sep 9 10:02 A.M.

2) chkpnt-2:
Created by admin
Created at Tue, 08:11:46 14 Sep 2010
Size is 21,536 bytes
Description: None

3) user-checkpoint-4:
Created by admin
Created at Tue, 08:16:48 14 Sep 2010
Size is 21,526 bytes
Description: None

switch#
```

次に、システム設定のロールバック チェックポイントの要約を表示する例を示します。

```
switch# show checkpoint summary system
```

次に、ユーザ設定のロールバック チェックポイントの要約を表示する例を示します。

```
switch# show checkpoint summary user
--------------------------------------------------------------------------------
```

```
1) chkpnt-1:
Created by admin
Created at Tue, 08:10:23 14 Sep 2010
Size is 21,508 bytes
Description: Checkpoint to save current configuration, Sep 9 10:02 A.M.

2) chkpnt-2:
Created by admin
Created at Tue, 08:11:46 14 Sep 2010
Size is 21,536 bytes
Description: None

3) user-checkpoint-4:
Created by admin
Created at Tue, 08:16:48 14 Sep 2010
Size is 21,526 bytes
Description: None

switch#
```

関連コマンド

コマンド	説明
checkpoint	チェックポイントを作成します。
rollback	保存されたすべてのチェックポイントに設定をロールバックします。
show checkpoint	ロールバック チェックポイントを表示します。
show checkpoint system	システム定義のロールバック チェックポイントを表示します。
show checkpoint user	ユーザ設定のロールバック チェックポイントを表示します。

show checkpoint system

システム設定のチェックポイントのみを表示するには、**show checkpoint system** コマンドを使用します。

show checkpoint system

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、システムによって定義されているロールバック チェックポイントを表示する例を示します。

```
switch# show checkpoint system
```

関連コマンド

コマンド	説明
checkpoint	チェックポイントを作成します。
rollback	保存されたすべてのチェックポイントに設定をロールバックします。
show checkpoint	ロールバック チェックポイントを表示します。
show checkpoint user	ユーザ設定のロールバック チェックポイントを表示します。

show checkpoint user

ユーザ設定チェックポイントだけを表示するには、**show checkpoint user** コマンドを使用します。

show checkpoint user

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、現在のユーザが設定したロールバック チェックポイントを表示する例を示します。

```
switch# show checkpoint user
!--------------------------------------------------------------------------------
Name: myChkpoint


!Command: Checkpoint cmd vdc 1
!Time: Mon Sep  6 09:40:47 2010

version 5.0(2)N1(1)
feature telnet
feature tacacs+
cfs eth distribute
feature private-vlan
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp
feature fex

username adminbackup password 5 !  role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCAd7Nkhktzebsg5/0  role network-admin
no password strength-check
ip domain-lookup
ip domain-lookup
hostname switch
ip access-list ip1
class-map type qos class-fcoe
  match cos 4
class-map type qos match-all cq1
  match cos 4
  match precedence 7

<--output truncated-->
```

```
switch#
```

関連コマンド

コマンド	説明
checkpoint	チェックポイントを作成します。
rollback	保存されたすべてのチェックポイントに設定をロールバックします。
show checkpoint	ロールバック チェックポイントを表示します。
show checkpoint summary	すべての設定済みロールバック チェックポイントのサマリーを表示します。
show checkpoint system	システム定義のロールバック チェックポイントを表示します。

show diff rollback-patch checkpoint

2 つのチェックポイント間での設定の違いを表示するには、**show diff rollback-patch checkpoint** コマンドを使用します。

show diff rollback-patch checkpoint *src-checkpoint-name* **checkpoint** *dest-checkpoint-name*

構文の説明

src-checkpoint-name	送信元ソース チェックポイント名。名前は、最大 32 文字まで指定できます。
dest-checkpoint-name	宛先チェックポイント名。名前は、最大 32 文字まで指定できます。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、現在のコンフィギュレーションまたは保存済みコンフィギュレーションを参照している送信元と宛先のチェックポイント間の差異を表示するために使用します。コンフィギュレーションの差異は、現在の実行コンフィギュレーションとチェックポイントが設定されているコンフィギュレーションに基づき、システムの動作状態を復元するために、システムに適用されます。

例

次に、chkpnt-1 と chkpnt-2 の 2 つのチェックポイント間の変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration--->
switch# checkpoint
...
user-checkpoint-4 created Successfully

Done
switch#
<-- modify configuration in running configuration--->
switch# show diff rollback-patch checkpoint user-checkpoint-4 checkpoint chkpnt-1
#Generating Rollback Patch

!!
interface Ethernet1/2
  no untagged cos
  no description Sample config
  exit
!
interface Ethernet1/2
```

```
 channel-group 1
!
line vty
switch# rollback chkpnt-1
switch#
```

関連コマンド

コマンド	説明
checkpoint	チェックポイントを作成します。
rollback	保存されたすべてのチェックポイントに設定をロールバックします。
show checkpoint	チェックポイント情報を表示します。
show diff rollback-patch file	現在のチェックポイント ファイルと保存済みコンフィギュレーションの差異を表示します。
show diff rollback-patch running-config	現在の実行コンフィギュレーションと保存済みチェックポイント コンフィギュレーションの差異を表示します。

show diff rollback-patch file

2 つのチェックポイント コンフィギュレーション ファイルの差異を表示するには、**show diff rollback-patch file** コマンドを使用します。

show diff rollback-patch file {**bootflash:** | **volatile:**}[*//server*][*directory/*][*src-filename*] {**checkpoint** *dest-checkpoint-name* | **file** {**bootflash:** | **volatile:**}[*//server*][*directory/*][*dest-filename*] | **running-config** | **startup-config**}

構文の説明

bootflash:	書き込み可能なブートフラッシュ ローカル ストレージ ファイル システムを指定します。
volatile:	揮発性の書き込み可能なローカル ストレージ ファイル システムを指定します。
//server	（任意）サーバの名前。有効な値は、**///**、**//module-1/**、**//sup-1/**、**//sup-active/** または **//sup-local/** です。2 個のスラッシュ（//）を含む必要があります。
directory/	（任意）ディレクトリの名前。ディレクトリ名では、大文字と小文字が区別されます。
src-filename	（任意）送信元のチェックポイント コンフィギュレーション ファイルの名前。ファイル名では、大文字と小文字が区別されます。
dest-filename	（任意）宛先チェックポイント コンフィギュレーション ファイルの名前。ファイル名では、大文字と小文字が区別されます。
checkpoint	宛先チェックポイントを指定します。
dest-checkpoint-name	宛先チェックポイント名。名前は、最大 32 文字まで指定できます。
file	宛先チェックポイント ファイルを指定します。
running-config	実行コンフィギュレーションを宛先として使用するよう指定します。
startup-config	スタートアップ コンフィギュレーションを宛先として使用するように指定します。

（注） *filesystem*://*server*/*directory*/*filename* ストリングにはスペースを含めることはできません。この文字列の各要素は、コロン（:）とスラッシュ（/）で区切ります。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

現在、または保存された設定を参照している送信元と宛先のチェックポイント コンフィギュレーション ファイルの差異を表示するには、このコマンドを使用します。コンフィギュレーションの差異は、現在の実行コンフィギュレーションとチェックポイントが設定されているコンフィギュレーションに基づき、システムの動作状態を復元するために、システムに適用されます。

例

次に、ブートフラッシュのストレージ システムにあるファイルに保存されている 2 つのチェックポイント コンフィギュレーション間の差異を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
switch# show diff rollback-patch file bootflash:///chkpnt_configSep9-2.txt file
bootflash:///chkpnt_configSep9-1.txt

switch# rollback file bootflash:///chkpnt_configSep9-1.txt
switch#
```

関連コマンド

コマンド	説明
rollback	保存されたすべてのチェックポイントにスイッチをロールバックします。
show checkpoint	チェックポイント情報を表示します。
show diff rollback-patch checkpoint	現在のチェックポイントと保存済みコンフィギュレーションの差異を表示します。
show diff rollback-patch running-config	現在の実行コンフィギュレーションと保存済みチェックポイント コンフィギュレーションの差異を表示します。

show diff rollback-patch running-config

現在の実行コンフィギュレーションと保存済み（チェックポイントが設定されている）コンフィギュレーションの差異を表示するには、**show diff rollback-patch running-config** コマンドを使用します。

show diff rollback-patch running-config {**checkpoint** *checkpoint-name* | **file** {**bootflash:** | **volatile:**}[*//server*][*directory/*][*filename*] | **running-config** | **startup-config**}

構文の説明

checkpoint	比較においてチェックポイントを宛先と使用するよう指定します。
checkpoint-name	チェックポイント名。名前は、最大 32 文字まで指定できます。
file	比較においてチェックポイント コンフィギュレーション ファイルを宛先として使用するよう指定します。
bootflash:	書き込み可能なブートフラッシュ ローカル ストレージ ファイル システムを指定します。
volatile:	揮発性の書き込み可能なローカル ストレージ ファイル システムを指定します。
//server	（任意）サーバの名前。有効な値は、**///**、**//module-1/**、**//sup-1/**、**//sup-active/** または **//sup-local/** です。2 個のスラッシュ（//）を含む必要があります。
directory/	（任意）ディレクトリの名前。ディレクトリ名では、大文字と小文字が区別されます。
filename	（任意）チェックポイント コンフィギュレーション ファイルの名前。ファイル名では、大文字と小文字が区別されます。
running-config	実行コンフィギュレーションを比較での宛先として使用するように指定します。
startup-config	スタートアップ コンフィギュレーションを比較での宛先として使用するように指定します。

（注） *filesystem*://*server*/*directory*/*filename* ストリングにはスペースを含めることはできません。この文字列の各要素は、コロン（:）とスラッシュ（/）で区切ります。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、保存済みコンフィギュレーションを参照している現在の実行コンフィギュレーションと宛先チェックポイントの差異を表示するために使用します。コンフィギュレーションの差異は、現在の実行コンフィギュレーションとチェックポイントが設定されているコンフィギュレーションに基づき、システムの動作状態を復元するために、システムに適用されます。

例

次に、現在の実行コンフィギュレーションと chkpnt-1 という名前のチェックポイントの間の設定変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration--->
switch# show diff rollback-patch running-config checkpoint chkpnt-1
Collecting Running-Config
#Generating Rollback Patch

!!
interface Ethernet1/2
  no description Sample config
  exit
switch#
```

次に、現在の実行コンフィギュレーションとブートフラッシュ ストレージ システムの保存済みコンフィギュレーションの間での設定変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# show diff rollback-patch running-config file chkpnt_configSep9-1.txt
```

次に、現在の実行コンフィギュレーションと、チェックポイントが設定された実行コンフィギュレーションの間の設定変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# show diff rollback-patch running-config running-config
```

次に、現在の実行コンフィギュレーションと保存済みスタートアップ コンフィギュレーションの間の設定変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# copy running-config startup-config
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
switch# show diff rollback-patch running-config startup-config
Collecting Running-Config
Collecting Startup-Config
#Generating Rollback Patch

!!
```

```
interface Ethernet1/2
  no untagged cos
  no description Sample config
  exit
password strength-check
no username admin
no username adminbackup
!
interface Ethernet1/2
 channel-group 1
no feature ssh
no feature telnet
switch#
```

関連コマンド

コマンド	説明
rollback	保存されたすべてのチェックポイントにスイッチをロールバックします。
show checkpoint	チェックポイント情報を表示します。
show diff rollback-patch checkpoint	現在のチェックポイントと保存済みコンフィギュレーションの差異を表示します。
show diff rollback-patch file	現在のチェックポイント ファイルと保存済みコンフィギュレーションの差異を表示します。
show diff rollback-patch startup-config	現在のスタートアップ コンフィギュレーションと保存済みチェックポイント コンフィギュレーションの差異を表示します。

show diff rollback-patch startup-config

現在のスタートアップ コンフィギュレーションと保存済み（チェックポイントが設定されている）コンフィギュレーションの差異を表示するには、**show diff rollback-patch startup-config** コマンドを使用します。

show diff rollback-patch startup-config {**checkpoint** *checkpoint-name* | **file** {**bootflash:** | **volatile:**}[*//server*][*directory/*][*filename*] | **running-config** | **startup-config**}

構文の説明

checkpoint	比較においてチェックポイントを宛先と使用するよう指定します。
checkpoint-name	チェックポイント名。名前は、最大 32 文字まで指定できます。
file	比較においてチェックポイント コンフィギュレーション ファイルを宛先として使用するよう指定します。
bootflash:	書き込み可能なブートフラッシュ ローカル ストレージ ファイル システムを指定します。
volatile:	揮発性の書き込み可能なローカル ストレージ ファイル システムを指定します。
//server	（任意）サーバの名前。有効な値は、**///**、**//module-1/**、**//sup-1/**、**//sup-active/** または **//sup-local/** です。2 個のスラッシュ（//）を含む必要があります。
directory/	（任意）ディレクトリの名前。ディレクトリ名では、大文字と小文字が区別されます。
filename	（任意）チェックポイント コンフィギュレーション ファイルの名前。ファイル名では、大文字と小文字が区別されます。
running-config	実行コンフィギュレーションを比較での宛先として使用するように指定します。
startup-config	スタートアップ コンフィギュレーションを比較での宛先として使用するように指定します。

（注） *filesystem*://*server*/*directory*/*filename* ストリングにはスペースを含めることはできません。この文字列の各要素は、コロン（:）とスラッシュ（/）で区切ります。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、保存済みコンフィギュレーションを参照している現在のスタートアップ コンフィギュレーションと宛先チェックポイントの差異を表示するために使用します。コンフィギュレーションの差異は、現在の実行コンフィギュレーションとチェックポイントが設定されているコンフィギュレーションに基づき、システムの動作状態を復元するために、システムに適用されます。

例

次に、現在のスタートアップ コンフィギュレーションと chkpnt-1 という名前のチェックポイントの間の設定変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration--->
switch# copy running-config startup-config
switch# show diff rollback-patch startup-config checkpoint chkpnt-1
Collecting Startup-Config
#Generating Rollback Patch

!!
!
feature telnet
feature ssh
username adminbackup password 5 ! role network-operator
username admin password 5 $1$KIPRDtFF$7eUMjCAd7Nkhktzebsg5/0 role network-admin
no password strength-check
switch#
```

次に、現在のスタートアップ コンフィギュレーションとブートフラッシュ ストレージ システムの保存済みコンフィギュレーションの間での設定変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# copy running-config startup-config
switch# show diff rollback-patch startup-config file chkpnt_configSep9-1.txt

switch#
```

次に、現在のスタートアップ コンフィギュレーションと、チェックポイントが設定された実行コンフィギュレーションの間の設定変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# copy running-config startup-config
<-- modify configuration in running configuration--->
switch# show diff rollback-patch startup-config running-config
Collecting Running-Config
Collecting Startup-Config
#Generating Rollback Patch

!!
!
feature telnet
feature ssh
username adminbackup password 5 ! role network-operator
```

```
username admin password 5 $1$KIPRDtFF$7eUMjCAd7Nkhktzebsg5/0 role network-admin
no password strength-check
switch#
```

次に、現在のスタートアップ コンフィギュレーションと保存済みスタートアップ コンフィギュレーションの間の設定変更を表示する例を示します。

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# copy running-config startup-config
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# show diff rollback-patch startup-config startup-config
Collecting Startup-Config
#Generating Rollback Patch
Rollback Patch is Empty
switch#
```

関連コマンド

コマンド	説明
rollback	保存されたすべてのチェックポイントにスイッチをロールバックします。
show checkpoint	チェックポイント情報を表示します。
show diff rollback-patch checkpoint	現在のチェックポイントと保存済みコンフィギュレーションの差異を表示します。
show diff rollback-patch file	現在のチェックポイント ファイルと保存済みコンフィギュレーションの差異を表示します。
show diff rollback-patch running-config	現在の実行コンフィギュレーションと保存済みチェックポイント コンフィギュレーションの差異を表示します。

show http-server

HTTP または HTTPS 設定に関する情報を表示するには、**show http-server** コマンドを使用します。

show http-server

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS Release 5.0(2)N1(1) よりも前のリリースでは、デフォルトで HTTP または HTTPS がスイッチ上でイネーブルになっています。

例

次に、HTTP サーバのステータスを表示する例を示します。

```
switch# show http-server
http-server enabled
switch#
```

関連コマンド

コマンド	説明
feature http-server	スイッチの HTTP または HTTPS サーバをイネーブルまたはディセーブルにします。

show ip access-lists

すべての IPv4 アクセス コントロール リスト（ACL）または特定の IPv4 ACL を表示するには、**show ip access-lists** コマンドを使用します。

show ip access-lists [*access-list-name*]

構文の説明

access-list-name	（任意）IPv4 ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

コマンド デフォルト

access-list-name 引数を使用して ACL を指定する場合を除いて、スイッチはすべての IPv4 ACL を表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、このコマンドはスイッチの IPv4 ACL 設定を表示します。このコマンドは、IPv4 ACL が管理（mgmt0）インターフェイスに割り当てられている場合に限り、IPv4 ACL の統計情報を表示します。ACL が SVI インターフェイスまたは QoS クラス マップ内に割り当てられている場合、このコマンドにより表示される統計情報はありません。

例

次に、スイッチ上のすべての IPv4 ACL を表示する例を示します。

```
switch# show ip access-lists
```

次に、Cisco NX-OS Release 5.0(2)N1(1) でスイッチ上のすべての IPv4 ACL を表示する例を示します。

```
switch# show ip access-lists
IP access list BulkData
        10 deny ip any any
IP access list CriticalData
        10 deny ip any any
IP access list Scavenger
        10 deny ip any any
IP access list denyv4
        20 deny ip 10.10.10.0/24 10.20.10.0/24 fragments
        30 permit udp 10.10.10.0/24 10.20.10.0/24 lt 400
        40 permit icmp any any router-advertisement
        60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
        70 permit igmp any any host-report
        80 deny tcp any any rst
        90 deny tcp any any ack
        100 permit tcp any any fin
        110 permit tcp any gt 300 any lt 400
        130 deny tcp any range 200 300 any lt 600
        140 deny tcp any range 200 300 any lt 600
```

```
IP access list dot
        statistics per-entry
        10 permit ip 20.1.1.1 255.255.255.0 20.10.1.1 255.255.255.0 precedence f
lash-override
        20 deny ip 20.1.1.1/24 20.10.1.1/24 fragments
        30 permit tcp any any fragments
        40 deny tcp any eq 400 any eq 500
IP access list ipPacl
        statistics per-entry
        10 deny tcp any eq 400 any eq 500
IP access list ipv4
        10 permit ip 10.10.10.1 225.255.255.0 any fragments
        20 permit ip any any dscp ef
IP access list ipv4Acl
        10 permit ip 10.10.10.1/32 10.10.10.2/32
IP access list voice
--More--
switch#
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。

show ip arp

Address Resolution Protocol（ARP; アドレス解決プロトコル）テーブル統計情報を表示するには、**show ip arp** コマンドを使用します。

show ip arp [**client** | [**statistics** | **summary**] [**ethernet** *slot*/*port* | **loopback** *intf-num* | **mgmt** *mgmt-intf-num* | **port-channel** *channel-num* | **vlan** *vlan-id*] [**fhrp-non-active-learn**] [**static**] [**detail**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]]

構文の説明

client	（任意）ARP クライアントの ARP 情報を表示します。
statistics	（任意）スイッチのグローバルな ARP 統計情報またはインターフェイスの ARP 統計情報を表示します。
summary	（任意）ARP 隣接サマリー情報を表示します。
ethernet *slot*/*port*	（任意）イーサネット インターフェイスの ARP 情報を表示します。スロット番号は 1 ～ 255、ポート番号は 1 ～ 128 です。
loopback *intf-num*	（任意）ループバック インターフェイスの ARP 情報を表示します。ループバック インターフェイスの番号は 0 ～ 1023 です。
mgmt *mgmt-intf-num*	（任意）管理インターフェイスの ARP 情報を表示します。インターフェイス番号は 0 です。
port-channel *channel-num*	（任意）EtherChannel インターフェイスの ARP 情報を表示します。チャネル番号の範囲は 1 ～ 4096 です。
vlan *vlan-id*	（任意）指定した VLAN の詳細な ARP 情報を表示します。内部使用に予約されている VLAN を除き、有効な範囲は 1 ～ 4094 秒です。
fhrp-non-active-learn	（任意）非アクティブな Cisco First Hop Redundancy Protocol（FHRP）アドレスに対する要求のみによって学習した ARP テーブル情報を表示します。
static	（任意）スタティック ARP エントリを表示します。
detail	（任意）詳細な ARP 情報を表示します。
vrf	（任意）使用する仮想ルーティングおよび転送（VRF）を指定します。
vrf-name	VRF 名。名前は最大 32 文字の英数字で、大文字と小文字が区別されます。
all	ARP テーブル内の指定された VLAN のすべての VRF エントリを表示します。
default	指定された VLAN のデフォルト VRF エントリを表示します。
management	指定された VLAN の管理 VRF エントリを表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.2(1)N1(1)	このコマンドが追加されました。
5.1(3)N1(1)	**client**、**ethernet**、**fhrp-non-active-learn**、**loopback**、**mgmt**、**port-channel**、**static**、**statistics**、および **summary** キーワードが追加されました。

使用上のガイドライン

VLAN インターフェイスの ARP 情報を表示する前に、**feature interface-vlan** コマンドを使用する必要があります。

例

次に、ARP テーブルを表示する例を示します。

```
switch# show ip arp

IP ARP Table for context default
Total number of entries: 1
Address         Age       MAC Address     Interface
90.10.10.2      00:03:11  000d.ece7.df7c  Vlan900
switch#
```

次に、詳細な ARP テーブルを表示する例を示します。

```
switch# show ip arp detail

IP ARP Table for context default
Total number of entries: 1
Address         Age       MAC Address     Interface        Physical Interface
90.10.10.2      00:02:55  000d.ece7.df7c  Vlan900          Ethernet1/12
switch#
```

次に、VLAN 10 およびすべての VRF の ARP テーブルを表示する例を示します。

```
switch# show ip arp vlan 10 vrf all
```

表 1 に、上記の出力で表示されるフィールドの説明を示します。

表 1　show ip arp フィールドの説明

フィールド	説明
IP ARP Table	ARP テーブルを適用するコンテキスト。
Total number of entries	ARP テーブルの ARP エントリまたはメッセージの合計数。
Address	ARP テーブルがスイッチの MAC アドレスに自動的にマッピングするスイッチの IP アドレス。
Age	MAC アドレスを持つスイッチが IP アドレスにマッピングされてからの期間。
MAC Address	スイッチの MAC アドレス。
Interface	パケットが転送されるスイッチ インターフェイス。
Physical Interface	物理インターフェイス（イーサネット、ループバック、EtherChannel、管理、または VLAN）。

関連コマンド

コマンド	説明
clear ip arp	ARP キャッシュおよび ARP テーブルをクリアします。
feature interface-vlan	VLAN インターフェイスの作成をイネーブルにします。
show running-config arp	実行 ARP コンフィギュレーションを表示します。

show ip arp inspection

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）設定ステータスを表示するには、**show ip arp inspection** コマンドを使用します。

show ip arp inspection

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

例

次に、DAI 設定のステータスを表示する例を示します。

```
switch# show ip arp inspection
```

関連コマンド

コマンド	説明
ip arp inspection vlan	VLAN の指定されたリストの DAI をイネーブルにします。
show ip arp inspection interface	指定されたインターフェイスの信頼状態および ARP パケット レートを表示します。
show ip arp inspection log	DAI のログ設定を表示します。
show ip arp inspection statistics	DAI 統計情報を表示します。
show ip arp inspection vlan	VLAN の指定されたリストの DAI ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

show ip arp inspection interfaces

指定されたインターフェイスの信頼状態を表示するには、**show ip arp inspection interfaces** コマンドを使用します。

show ip arp inspection interfaces {**ethernet** *slot*/*port* | **port-channel** *channel-number*}

構文の説明

ethernet *slot*/*port*	（任意）出力がイーサネット インターフェイス用になるように指定します。
port-channel *channel-number*	（任意）出力がポートチャネル インターフェイス用になるように指定します。有効なポートチャネル番号は、1 ～ 4096 です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

例

次に、信頼できるインターフェイスの信頼状態を表示する例を示します。

```
switch# show ip arp inspection interfaces ethernet 2/1
```

関連コマンド

コマンド	説明
ip arp inspection vlan	VLAN の指定されたリストの Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）をイネーブルにします。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection vlan	VLAN の指定されたリストの DAI ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

show ip arp inspection log

Dynamic ARP Inspection（DAI）ログ設定を表示するには、**show ip arp inspection log** コマンドを使用します。

show ip arp inspection log

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

例

次に、DAI ログ設定を表示する例を示します。

```
switch# show ip arp inspection log

Syslog Buffer Size : 12
Syslog Rate        : 5 entries per 1 seconds
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ロギング バッファをクリアします。
ip arp inspection log-buffer	DAI のログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

show ip arp inspection statistics

ダイナミック ARP インスペクション（DAI）統計情報を表示するには、**show ip arp inspection statistics** コマンドを使用します。

show ip arp inspection statistics [**vlan** *vlan-list*]

構文の説明

vlan *vlan-list*	（任意）DAI 統計情報を表示する VLAN のリストを指定します。指定できる VLAN ID は 1 ～ 4094 です。1 つの VLAN または VLAN の範囲を指定できます。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

例

次に、VLAN 1 の DAI 統計情報を表示する例を示します。

```
switch# show ip arp inspection statistics vlan 1
```

関連コマンド

コマンド	説明
clear ip arp inspection statistics vlan	指定された VLAN の DAI 統計情報を消去します。
show ip arp inspection log	DAI のログ設定を表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

show ip arp inspection vlan

VLAN の指定されたリストのダイナミック ARP インスペクション（DAI）ステータスを表示するには、**show ip arp inspection vlan** コマンドを使用します。

show ip arp inspection vlan *vlan-list*

構文の説明

vlan-list	DAI ステータスがある VLAN のリスト。*vlan-list* 引数は 1 つの VLAN ID、VLAN ID の範囲、カンマ区切りの ID と範囲を指定できます。指定できる VLAN ID は 1 ～ 4094 です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

例

次に、VLAN 1 の DAI ステータスを表示する例を示します。

```
switch# show ip arp inspection vlan 1

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

Vlan : 1
-----------
Configuration        : Disabled
Operation State      : Inactive
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection statistics vlan	指定された VLAN の DAI 統計情報を消去します。
ip arp inspection vlan	VLAN の指定されたリストの DAI をイネーブルにします。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection interface	指定されたインターフェイスの信頼状態および ARP パケット レートを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

show ip arp sync-entries

アドレス解決プロトコル（ARP）テーブルの同期後に ARP テーブル情報を表示するには、**show ip arp sync-entries** コマンドを使用します。

show ip arp sync-entries [**detail** | **vrf** {*vrf-name* | **all** | **default** | **management**}]

構文の説明

detail	（任意）ARP テーブルに関する詳細情報を表示します。
vrf	（任意）仮想ルーティングおよび転送（VRF）インスタンスの ARP テーブル情報を表示します。
vrf-name	VRF 名。名前は最大 32 文字の英数字で、大文字と小文字が区別されます。
all	すべての VRF エントリの ARP テーブル情報を表示します。
default	デフォルトの VRF エントリの ARP テーブル情報を表示します。
management	管理 VRF エントリの ARP テーブル情報を表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.1(3)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、仮想ポート チャネル（vPC）のグローバルな ARP 統計情報を表示する例を示します。

```
switch# show ip arp sync-entries
```

関連コマンド

コマンド	説明
ip arp synchronize	vPC ドメインでの ARP 同期をイネーブルにします。
show running-config arp	ARP テーブルの実行コンフィギュレーション情報を表示します。

show ip dhcp snooping

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングの一般的なステータス情報を表示するには、**show ip dhcp snooping** コマンドを使用します。

show ip dhcp snooping

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

例

次に、DHCP スヌーピングに関する一般ステータス情報を表示する例を示します。

```
switch# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted
------------          -------
Ethernet2/3           Yes

switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報を表示します。
show running-config dhcp	DHCP スヌーピング設定を表示します。

show ip dhcp snooping binding

すべてのインターフェイスまたは特定のインターフェイスの IP-to-MAC アドレス バインディングを表示するには、**show ip dhcp snooping binding** コマンドを使用します。

show ip dhcp snooping binding [*IP-address*] [*MAC-address*] [**interface ethernet** *slot*/*port*] [**vlan** *vlan-id*]

show ip dhcp snooping binding [**dynamic**]

show ip dhcp snooping binding [**static**]

構文の説明

IP-address	（任意）表示されるバインディングに含める IPv4 アドレス。有効なエントリは、ドット付き 10 進表記です。
MAC-address	（任意）表示されるバインディングに含める MAC アドレス。有効なエントリは、ドット付き 16 進表記です。
interface ethernet *slot*/*port*	（任意）表示されるバインディングに関連付けるイーサネット インターフェイスを指定します。スロット番号は 1 ～ 255、ポート番号は 1 ～ 128 です。
vlan *vlan-id*	（任意）表示されるバインディングに関連付ける VLAN ID を指定します。有効な VLAN ID は 1 ～ 4094 です。内部用に予約されている VLAN は除きます。 ハイフン（-）を使用して、VLAN ID の範囲の開始 ID と終了 ID を区別します（たとえば、70-100）。 カンマ（,）を使用して、各 VLAN ID および VLAN ID の範囲を区別します（たとえば、20,70-100,142）。
dynamic	（任意）すべてのダイナミック IP-MAC アドレス バインディングに出力を制限します。
static	（任意）すべてのスタティック IP-MAC アドレス バインディングに出力を制限します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

バインディング インターフェイスには、スタティック IP ソース エントリが含まれます。スタティック エントリは、Type 列に「static」と表示されます。

例

次に、すべてのバインディングを表示する例を示します。

```
switch# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type        VLAN  Interface
------------------  ---------------  --------  ----------  ----  -------------
0f:00:60:b3:23:33   10.3.2.2         infinite  static      13    Ethernet2/46
0f:00:60:b3:23:35   10.2.2.2         infinite  static      100   Ethernet2/10
switch#
```

関連コマンド

コマンド	説明
clear ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを消去します。
copy running-config startup-config	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。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
ip source binding	レイヤ 2 イーサネット インターフェイスのスタティック IP ソース エントリを作成します。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

show ip dhcp snooping statistics

ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング統計情報を表示するには、**show ip dhcp snooping statistics** コマンドを使用します。

show ip dhcp snooping statistics

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

例

次に、DHCP スヌーピング統計情報を表示する例を示します。

```
switch# show ip dhcp snooping statistics
Packets processed 61343
Packets received through cfsoe 0
Packets forwarded 0
Packets forwarded on cfsoe 0
Total packets dropped 61343
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to dhcp relay not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 61343
Packets dropped due to max hops exceeded 0
switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
show running-config dhcp	DHCP スヌーピング設定を表示します。

show ipv6 access-lists

すべての IPv6 アクセス コントロール リスト（ACL）または特定の IPv6 ACL を表示するには、**show ipv6 access-lists** コマンドを使用します。

show ipv6 access-lists [*access-list-name*] [**expanded** | **summary**]

構文の説明

access-list-name	（任意）IPv6 ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
expanded	（任意）オブジェクト グループの名前だけでなく、IPv6 アドレス グループまたはポート グループの内容を表示するように指定します。
summary	（任意）コマンドが ACL 設定ではなく、ACL に関する情報を表示するように指定します。詳細については、「使用上のガイドライン」の項を参照してください。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

access-list-name 引数を使用して ACL を指定する場合を除いて、デバイスはすべての IPv6 ACL を表示します。

summary キーワードを使用すると、ACL 設定ではなく ACL に関する情報を表示できます。表示される情報には、次の内容が含まれます。

- エントリ単位の統計情報が ACL に対して設定されているかどうか。
- ACL 設定内のルール数。この数は、デバイスがインターフェイスに適用されるときに ACL 内に含まれるエントリ数を反映しません。ACL 内のルールがオブジェクト グループを使用する場合、適用されるときの ACL 内のエントリ数は、ルール数よりはるかに大きくなることがあります。
- ACL が適用されているインターフェイス。
- ACL がアクティブ状態のインターフェイス。

show ipv6 access-lists コマンドは、次の両方の状態が真の場合に、ACL 内の各エントリの統計情報を表示します。

- ACL 設定に statistics per-entry コマンドが含まれている。
- 管理上アップ状態のインターフェイスに ACL が適用されている。

例

次に、スイッチ上のすべての IPv6 ACL を表示する例を示します。

```
switch# show ipv6 access-lists
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 ACL を設定します。

show ip verify source

IP ソース ガードがイネーブルになっているインターフェイス、および IP と MAC アドレスのバインディングを表示するには、**show ip verify source** コマンドを使用します。

show ip verify source [**interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*}]

構文の説明

interface	（任意）出力が特定のインターフェイスの IP-to-MAC アドレス バインディングに制限されるように指定します。
ethernet *slot*/*port*	（任意）出力が所定のイーサネット インターフェイスのバインディングに制限されるように指定します。スロット番号は 1 ～ 255、ポート番号は 1 ～ 128 です。
port-channel *channel-number*	（任意）出力が所定のポートチャネル インターフェイスのバインディングに制限されるように指定します。有効なポートチャネル番号は、1 ～ 4096 です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(3)N1(1)	このコマンドが追加されました。

例

次に、スイッチで IP ソース ガードがイネーブルになっているインターフェイス、および IP と MAC アドレスのバインディングを表示する例を示します。

```
switch# show ip verify source
IP source guard is enabled on the following interfaces:
-------------------------------------------------------
        Ethernet1/2
        Ethernet1/5


IP source guard operational entries:
------------------------------------
Interface         Filter-mode             IP-address     Mac-address       Vlan
------------      -----------             ----------     --------------    ----
Ethernet1/2       inactive-no-snoop-vlan
Ethernet1/5       inactive-no-snoop-vlan
switch#
```

関連コマンド

コマンド	説明
ip source binding	指定したイーサネット インターフェイスのスタティック IP ソース エントリを作成します。
ip verify source dhcp-snooping-vlan	インターフェイスの IP ソース ガードをイネーブルにします。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

show mac access-lists

すべてのメディア アクセス コントロール（MAC）アクセス コントロール リスト（ACL）または特定の MAC ACL を表示するには、**show mac access-lists** コマンドを使用します。

show mac access-lists [*access-list-name*]

構文の説明

access-list-name	（任意）MAC ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

コマンド デフォルト

access-list-name 引数を使用して ACL を指定する場合を除いて、スイッチはすべての MAC ACL を表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スイッチ上のすべての MAC ACL を表示する例を示します。

```
switch# show mac access-lists

MAC access list acl-mac
        10 permit any any
MAC access list test
        statistics per-entry
        10 deny 0000.1111.2222 0000.0000.0000 0000.1111.3333 ffff.0000.0000
switch#
```

関連コマンド

コマンド	説明
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。

show privilege

現在の権限レベル、ユーザ名、および累積権限サポートのステータスを表示するには、**show privilege** コマンドを使用します。

show privilege

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

feature privilege コマンドをイネーブルにすると、権限ロールは低いレベルの権限ロールの権限を継承します。

例

次に、累積権限サポートの現在の特権レベル、ユーザ名、およびステータスを表示する例を示します。

```
switch# show privilege
User name: admin
Current privilege level: -1
Feature privilege: Enabled
switch#
```

関連コマンド

コマンド	説明
enable	上位の特権レベルへのユーザの昇格をイネーブルにします。
enable secret priv-lvl	特定の権限レベルのシークレット パスワードをイネーブルにします。
feature privilege	RADIUS および TACACS+ サーバでのコマンド認可に対するロールの累積権限をイネーブルにします。
username	ユーザが認可に権限レベルを使用できるようにします。

show radius-server

RADIUS サーバ情報を表示するには、**show radius-server** コマンドを表示します。

show radius-server [*hostname* | *ipv4-address* | *ipv6-address*] [**directed-request** | groups [*group-name*] | sorted | statistics *hostname* | *ipv4-address* | *ipv6-address*]

構文の説明

hostname	（任意）RADIUS サーバの Domain Name Server（DNS; ドメイン ネーム サーバ）名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。
ipv4-address	（任意）*A.B.C.D* 形式の RADIUS サーバの IPv4 アドレス。
ipv6-address	（任意）*X:X::X:X* フォーマットの RADIUS サーバの IPv6 アドレス。
directed-request	（任意）指定要求設定を表示します。
groups [*group-name*]	（任意）設定された RADIUS サーバ グループに関する情報を表示します。*group-name* を入力して、特定の RADIUS サーバ グループに関する情報を表示します。
sorted	（任意）RADIUS サーバに関する名前でソートされた情報を表示します。
statistics	（任意）RADIUS サーバの RADIUS 統計情報を表示します。ホスト名または IP アドレスが必要です。

コマンド デフォルト

グローバル RADIUS サーバ設定を表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

RADIUS 事前共有キーは、**show radius-server** コマンド出力には表示されません。RADIUS 事前共有キーを表示するには、**show running-config radius** コマンドを使用します。

例

次に、すべての RADIUS サーバの情報を表示する例を示します。

```
switch# show radius-server
retransmission count:1
timeout value:5
deadtime value:0
source interface:any available
total number of servers:1

following RADIUS servers are configured:
        192.168.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:********
switch#
```

次に、指定された RADIUS サーバの情報を表示する例を示します。

```
switch# show radius-server 192.168.1.1
        192.168.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:********
                idle time:0
                test user:test
                test password:********
switch#
```

次に、RADIUS 指定要求設定を表示する例を示します。

```
switch# show radius-server directed-request
disabled
switch#
```

次に、RADIUS サーバ グループの情報を表示する例を示します。

```
switch# show radius-server groups
total number of groups:2

following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
                deadtime is 0
        group RadServer:
                server: 192.168.1.1 on auth-port 1812, acct-port 1813
                deadtime is 0
switch#
```

次に、指定された RADIUS サーバ グループの情報を表示する例を示します。

```
switch# show radius-server groups RadServer
        group RadServer:
                server: 10.193.128.5 on auth-port 1812, acct-port 1813
                deadtime is 0
switch#
```

次に、すべての RADIUS サーバのソートされた情報を表示する例を示します。

```
switch# show radius-server sorted
timeout value:5
retransmission count:1
deadtime value:0
source interface:any available
total number of servers:1

following RADIUS servers are configured:
        192.168.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:********
switch#
```

次に、指定された RADIUS サーバの統計情報を表示する例を示します。

```
switch# show radius-server statistics 192.168.1.1
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
```

```
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
switch#
```

関連コマンド

コマンド	説明
show running-config radius	実行コンフィギュレーション ファイルの RADIUS 情報を表示します。

show role

ユーザ ロール設定を表示するには、**show role** コマンドを使用します。

show role [**name** *role-name*]

構文の説明

name *role-name*	（任意）特定のユーザ ロール名の情報を表示します。

コマンド デフォルト

すべてのユーザ ロールの情報を表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、特定のユーザ ロールの情報を表示する例を示します。

```
switch# show role name MyRole

Role: MyRole
  Description: new role
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       deny    command                         pwd
switch#
```

次に、すべてのユーザ ロールの情報を表示する例を示します。

```
switch# show role
```

Cisco NX-OS Release 5.0(2)N1(1) では、次の出力が表示されます。

```
switch# show role

Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       permit  read-write

Role: network-operator
  Description: Predefined network operator role has access to all read
  commands on the switch
  ----------------------------------------------------------------------
```

```
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       permit  read

Role: vdc-admin
  Description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       permit  read-write

Role: vdc-operator
  Description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       permit  read

Role: priv-14
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  1       permit  read-write

Role: priv-13
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-12
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-11
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-10
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-9
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
```

```
  Vrf policy: permit (default)

Role: priv-8
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-7
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-6
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-5
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-4
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-3
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-2
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-1
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-0
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
```

```
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  10      permit  command                         traceroute6 *
  9       permit  command                         traceroute *
  8       permit  command                         telnet6 *
  7       permit  command                         telnet *
  6       permit  command                         ping6 *
  5       permit  command                         ping *
  4       permit  command                         ssh6 *
  3       permit  command                         ssh *
  2       permit  command                         enable *

Role: default-role
  Description: This is a system defined role and applies to all users.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  5       permit  command                         feature environment
  4       permit  command                         feature hardware
  3       permit  command                         feature module
  2       permit  command                         feature snmp
  1       permit  command                         feature system

Role: priv-15
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: MyRole
  Description: new role
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       deny    command                         pwd
switch#
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを設定します。

show role feature

ユーザ ロール機能を表示するには、**show role feature** コマンドを使用します。

show role feature [**detail** | **name** *feature-name*]

構文の説明

detail	（任意）すべての機能の詳細情報を表示します。
name *feature-name*	（任意）特定の機能の詳細情報を表示します。名前は最大 16 文字の英数字で、大文字と小文字が区別されます。

コマンド デフォルト

ユーザ ロール機能名のリストを表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール機能を表示する例を示します。

```
switch# show role feature
```

Cisco NX-OS Release 5.0(2)N1(1) では、次の出力が表示されます。

```
aaa             (AAA service related commands)
arp             (ARP protocol related commands)
cdp             (Cisco Discovery Protocol related commands)
l3vm            (Layer 3 virtualization related commands)
ping            (Network reachability test commands)
snmp            (SNMP related commands)
radius          (Radius configuration and show commands)
syslog          (Syslog related commands)
tacacs          (TACACS configuration and show commands)
install         (Software install related commands)
license         (License related commands)
callhome        (Callhome configuration and show commands)
platform        (Platform configuration and show commands)
access-list     (IP access list related commands)
svi             (Interface VLAN related commands)
vlan            (Virtual LAN related commands)
eth-span        (Ethernet SPAN related commands)
ethanalyzer     (Ethernet Analyzer)
spanning-tree   (Spanning Tree protocol related commands)
acl             (FC ACL related commands)
sfm             (ISCSI flow related commands)
fcns            (Fibre Channel Name Server related commands)
fcsp            (Fibre Channel Security Protocol related commands)
fdmi            (FDMI related commands)
fspf            (Fabric Shortest Path First protocol related commands)
rlir            (Registered Link Incident Report related commands)
rscn            (Registered State Change Notification related commands)
```

```
span            (SPAN session relate commands)
vsan            (VSAN configuration and show commands)
wwnm            (WorldWide Name related commands)
zone            (Zone related commands)
fcanalyzer      (FC analyzer related commands)
switch#
```

次に、すべてのユーザ ロール機能の詳細情報を表示する例を示します。

```
switch# show role feature detail
```

Cisco NX-OS Release 5.0(2)N1(1) では、次の出力が表示されます。

```
aaa             (AAA service related commands)
  show aaa *
  config t ; aaa *
  aaa *
  clear aaa *
  debug aaa *
  show accounting *
  config t ; accounting *
  accounting *
  clear accounting *
  debug accounting *
arp             (ARP protocol related commands)
  show ip arp *
  config t; ip arp *
  clear ip arp *
  debug ip arp *
  debug-filter ip arp *
cdp             (Cisco Discovery Protocol related commands)
  show cdp *
  config t ; cdp *
  cdp *
  clear cdp *
  debug cdp *
l3vm            (Layer 3 virtualization related commands)
  show vrf *
  config t ; vrf *
  routing-context vrf *
ping            (Network reachability test commands)
  show ping *
  config t ; ping *
  ping *
  clear ping *
  debug ping *
  show ping6 *
  config t ; ping6 *
  ping6 *
  clear ping6 *
  debug ping6 *
  show traceroute *
  config t ; traceroute *
--More--
switch#
```

次に、arp という名前の特定のユーザ ロール機能の詳細情報を表示する例を示します。

```
switch# show role feature name arp
```

Cisco NX-OS Release 5.0(2)N1(1) では、このコマンドによって、次の出力を表示します。

```
arp             (ARP protocol related commands)
  show ip arp *
  config t; ip arp *
```

```
  clear ip arp *
  debug ip arp *
  debug-filter ip arp *
switch#
```

関連コマンド

コマンド	説明
role feature-group	ユーザ ロールの機能グループを設定します。
rule	ユーザ ロールのルールを設定します。

show role feature-group

ユーザ ロール機能グループを表示するには、**show role feature-group** コマンドを使用します。

show role feature-group [**detail** | **name** *group-name*]

構文の説明

detail	（任意）すべての機能グループの詳細情報を表示します。
name *group-name*	（任意）特定の機能グループの詳細情報を表示します。

コマンド デフォルト

ユーザ ロール機能グループのリストを表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール機能グループを表示する例を示します。

```
switch# show role feature-group
```

次に、すべてのユーザ ロール機能グループに関する詳細情報を表示する例を示します。

```
switch# show role feature-group detail
```

次に、特定のユーザ ロール機能グループの情報を表示する例を示します。

```
switch# show role feature-group name SecGroup
```

関連コマンド

コマンド	説明
role feature-group	ユーザ ロールの機能グループを設定します。
rule	ユーザ ロールのルールを設定します。

show rollback log

スイッチのコンフィギュレーション ロールバックのログを表示するには、**show rollback log** コマンドを使用します。

show rollback log {**exec** | **verify**}

構文の説明

exec	ロールバック実行ログを表示します。
verify	ロールバック確認ログを表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

使用上のガイドライン

ロールバック ログが空の場合、次のメッセージが表示されます。

```
ERROR: Log Not Available
```

例

次に、ロールバック実行ログを表示する例を示します。

```
switch# show rolback log exec
------------------------------------------------------------------------------
time: Mon, 06:16:02 06 Sep 2010
Status: success
------------------------------------------------------------------------------
time: Mon, 07:58:36 06 Sep 2010
Status: success
------------------------------------------------------------------------------
time: Mon, 09:48:58 06 Sep 2010
Status: success
switch#
```

次に、ロールバック確認ログを表示する例を示します。

```
switch# show rollback log verify
------------------------------------------------------------------------------
time: Mon, 09:48:56 06 Sep 2010
Status: success
------------------------------------------------------------------------------
time: Mon, 09:48:58 06 Sep 2010
Status: success
switch#
```

関連コマンド

コマンド	説明
rollback	アクティブ コンフィギュレーションをチェックポイント状態に復元します。

show running-config aaa

実行コンフィギュレーションの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）設定情報を表示するには、**show running-config aaa** コマンドを使用します。

show running-config aaa [**all**]

構文の説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、実行コンフィギュレーションの設定済み AAA 情報を表示する例を示します。

```
switch# show running-config aaa
```

関連コマンド

コマンド	説明
aaa accounting default	アカウンティングの AAA 方式を設定します。
aaa authentication login console	コンソール ログインの AAA 認証方式を設定します。
aaa authentication login default	デフォルトの AAA 認証方式を設定します。
aaa authentication login error-enable	AAA 認証失敗メッセージをコンソールに表示するように設定します。
aaa authorization commands default	デフォルトの AAA 認証方式を設定します。
aaa authorization config-commands default	すべてのコンフィギュレーション コマンドのデフォルトの AAA 認証方式を設定します。
aaa group server radius	RADIUS サーバ グループを作成します。
aaa user default-role	リモート認証のために AAA サーバ管理者により割り当てられるデフォルト ロールをイネーブルにします。

show running-config aclmgr

実行コンフィギュレーションのアクセス コントロール リスト（ACL）の設定を表示するには、**show running-config aclmgr** コマンドを使用します。

show running-config aclmgr [**all**]

構文の説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、ACL の実行コンフィギュレーションを表示する例を示します。

```
switch# show running-config aclmgr

!Command: show running-config aclmgr
!Time: Tue Aug 31 05:01:56 2010

version 5.0(2)N1(1)
ip access-list BulkData
  10 deny ip any any
ip access-list CriticalData
  10 deny ip any any
ip access-list Scavenger
  10 deny ip any any
mac access-list acl-mac
  10 permit any any
ip access-list denyv4
  20 deny ip 10.10.10.0/24 10.20.10.0/24 fragments
  30 permit udp 10.10.10.0/24 10.20.10.0/24 lt 400
  40 permit icmp any any router-advertisement
  60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
  70 permit igmp any any host-report
  80 deny tcp any any rst
  90 deny tcp any any ack
  100 permit tcp any any fin
  110 permit tcp any gt 300 any lt 400
  130 deny tcp any range 200 300 any lt 600
  140 deny tcp any range 200 300 any lt 600
ip access-list dot
  statistics per-entry
  10 permit ip 20.1.1.1 255.255.255.0 20.10.1.1 255.255.255.0 precedence flash-o
verride
:
<snip>
:
```

```
vlan access-map vacl-mac
  match mac address acl-mac
  action forward
  statistics per-entry
vlan filter vacl-mac vlan-list 300

interface Ethernet1/1
  ipv6 port traffic-filter denv6 in

interface Ethernet1/2
  ip port access-group voice in

interface Ethernet1/9
  ipv6 port traffic-filter denv6 in

interface Ethernet1/10
  ipv6 port traffic-filter denv6 in

line vty
  access-class myACList in
  access-class myACList out
  ipv6 access-class myI6List out

switch#
```

次に、VTY の実行コンフィギュレーションのみを表示する例を示します。

```
switch# show running-config aclmgr | begin vty
line vty
  access-class myACList in
  access-class myACList out
  ipv6 access-class myI6List out

switch#
```

関連コマンド

コマンド	説明
access-class	VTY のアクセス クラスを設定します。
copy running-config startup-config	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 ファイルにコピーします。
ip access-class	VTY の IPv4 アクセス クラスを設定します。
ipv6 access-class	VTY の IPv6 アクセス クラスを設定します。
show startup-config aclmgr	ACL のスタートアップ コンフィギュレーションを表示します。

show running-config arp

実行コンフィギュレーションのアドレス解決プロトコル（ARP）の設定を表示するには、**show running-config arp** コマンドを使用します。

show running-config arp [**all**]

構文の説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、ARP 設定を表示する例を示します。

```
switch# show running-config arp

!Command: show running-config arp
!Time: Mon Aug 23 07:33:15 2010

version 5.0(2)N1(1)
ip arp timeout 2100
ip arp event-history errors size medium

interface Vlan10
  ip arp 10.193.131.37 00C0.4F00.0000

switch#
```

次に、デフォルト情報を含む ARP 設定を表示する例を示します。

```
switch# show running-config arp all

!Command: show running-config arp all
!Time: Mon Aug 23 07:33:52 2010

version 5.0(2)N1(1)
ip arp timeout 1500
ip arp event-history cli size small
ip arp event-history snmp size small
ip arp event-history client-errors size small
ip arp event-history client-event size small
ip arp event-history lcache-errors size small
ip arp event-history lcache size small
ip arp event-history errors size small
ip arp event-history ha size small
ip arp event-history event size small
ip arp event-history packet size small
```

```
interface Vlan10
  ip arp 10.193.131.37 00C0.4F00.0000
  ip arp gratuitous update
  ip arp gratuitous request

switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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 ファイルにコピーします。
ip arp event-history errors	イベント履歴バッファに ARP デバッグ イベントをロギングします。
ip arp timeout	ARP タイムアウトを設定します。
ip arp inspection	DHCP スヌーピングに関する一般的な情報を表示します。
show startup-config arp	ARP のスタートアップ コンフィギュレーションを表示します。

show running-config dhcp

実行コンフィギュレーションのダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング設定を表示するには、**show running-config dhcp** コマンドを使用します。

show running-config dhcp [**all**]

構文の説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature dhcp** コマンドを使用して DHCP スヌーピング機能をイネーブルにする必要があります。

例

次の例では、DHCP スヌーピング設定を表示する方法を示します。

```
switch# show running-config dhcp

!Command: show running-config dhcp
!Time: Mon Aug 23 09:09:11 2010

version 5.0(2)N1(1)
feature dhcp

ip dhcp snooping
ip dhcp snooping information option
service dhcp
ip dhcp relay
ip dhcp relay information option

ip arp inspection filter arp-acl-01 vlan 15,37-48

switch#
```

次に、デフォルト情報の DHCP スヌーピング設定を表示する例を示します。

```
switch# show running-config dhcp all

!Command: show running-config dhcp all
!Time: Mon Aug 23 09:10:11 2010

version 5.0(2)N1(1)
feature dhcp
```

```
ip dhcp snooping
ip dhcp snooping information option
ip dhcp snooping verify mac-address
service dhcp
ip dhcp relay
ip dhcp relay information option
no ip dhcp relay sub-option type cisco
no ip dhcp relay information option vpn
no ip arp inspection validate src-mac dst-mac ip
ip arp inspection log-buffer entries 32
no ip dhcp packet strict-validation


interface port-channel23
  no ip dhcp snooping trust
  no ip arp inspection trust
  no ip verify source dhcp-snooping-vlan

interface port-channel67
  no ip dhcp snooping trust
  no ip arp inspection trust
  no ip verify source dhcp-snooping-vlan

interface port-channel150
  no ip dhcp snooping trust
  no ip arp inspection trust
  no ip verify source dhcp-snooping-vlan

interface port-channel400
  no ip dhcp snooping trust
  no ip arp inspection trust
  no ip verify source dhcp-snooping-vlan

<--output truncated-->
switch#
```

次に、Cisco NX-OS Release 5.0(3)N1(1) を実行するスイッチ上の DHCP スヌーピング設定および IP ソース ガード情報を表示する例を示します。

```
switch# show running-config dhcp

!Command: show running-config dhcp
!Time: Sat Apr 19 06:18:33 2008

version 5.0(3)N1(1)
feature dhcp

ip dhcp snooping
ip dhcp snooping information option


interface Ethernet1/2
  ip dhcp snooping trust
  ip verify source dhcp-snooping-vlan

interface Ethernet1/5
  ip verify source dhcp-snooping-vlan
ip source binding 10.0.0.7 002f.23bd.0014 vlan 5 interface Ethernet1/2
ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface Ethernet1/5


switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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。
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
ip verify source	レイヤ 2 インターフェイスの IP ソース ガードをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show ip verify source	IP-MAC アドレス バインディングを表示します。
show startup-config dhcp	DHCP のスタートアップ コンフィギュレーションを表示します。

show running-config radius

実行コンフィギュレーションの RADIUS サーバ情報を表示するには、**show running-config radius** コマンドを使用します。

show running-config radius [**all**]

構文の説明

all	（任意）デフォルトの RADIUS 設定情報を表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、実行コンフィギュレーションの RADIUS の情報を表示する例を示します。

```
switch# show running-config radius
```

Cisco NX-OS Release 5.0(2)N1(1) では、次の出力が表示されます。

```
!Command: show running-config radius
!Time: Wed Aug 25 10:25:41 2010

version 5.0(2)N1(1)
radius-server host 192.168.1.1 key 7 "KkwyCet" authentication accounting
aaa group server radius r1
    server 192.168.1.1


switch#
```

関連コマンド

コマンド	説明
show radius-server	RADIUS 情報を表示します。

show running-config security

実行コンフィギュレーションのユーザ アカウント、セキュア シェル（SSH）サーバ、および Telnet サーバ情報を表示するには、**show running-config security** コマンドを使用します。

show running-config security [**all**]

構文の説明

all	（任意）デフォルトのユーザ アカウント、SSH サーバ、および Telnet サーバ コンフィギュレーション情報を表示します。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、実行コンフィギュレーションのユーザ アカウント、SSH サーバ、および Telnet サーバ情報を表示する例を示します。

```
switch# show running-config security
```

Cisco NX-OS Release 5.0(2)N1(1) では、次の出力が表示されます。

```
!Command: show running-config security
!Time: Wed Aug 25 10:27:20 2010

version 5.0(2)N1(1)
feature telnet

username admin password 5 $1$eKzwPRms$5QB0PxpkXdp6ZKkME/vSS1  role network-admin
username praveena password 5 $1$9w6ZnM/R$Pg5OfsV/vkOaAGW.f.RyP.  role network-op
erator
username install password 5 !  role network-admin
username user1 password 5 !  role priv-5
no password strength-check


switch#
```

関連コマンド

コマンド	説明
ssh	IPv4 を使用してセキュア シェル（SSH）接続を作成します。
ssh6	IPv6 を使用してセキュア シェル（SSH）接続を作成します。
telnet	IPv4 を使用して Telnet セッションを作成します。

コマンド	説明
telnet6	IPv6 を使用して Telnet セッションを作成します。
username	ユーザ アカウントを設定します。

show ssh key

セキュア シェル（SSH）サーバ キーを表示するには、**show ssh key** コマンドを使用します。

show ssh key

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**ssh server enable** コマンドを使用して SSH がイネーブルのときだけ使用できます。

例

次に、SSH サーバ キーを表示する例を示します。

```
switch# show ssh key
```

Cisco NX-OS Release 5.0(2)N1(1) では、次の出力が表示されます。

```
**************************************
rsa Keys generated:Mon Aug  2 22:49:27 2010

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA0iACA1fHAeIaY6PD5fSBLqGX3MIn+k72qhdvLNib7dL7
8CRQVS1AlQiDDTrvyIfRZ5yHMDQndvcmRfkJzluSCW2FP8vokZ66aXFk8TBTFc5Bn3NUiUyPZyhPtFD2
LaHBCkxl0MxEP+nmPJ6Qf6mBzZVAIdLw8Nd64ZwqVHHjeFc=

bitcount:1024
fingerprint:
bb:bf:a4:c0:22:3b:70:15:e4:2b:2b:bb:08:41:82:d4
**************************************
could not retrieve dsa key information
**************************************
switch#
```

関連コマンド

コマンド	説明
ssh server key	SSH サーバ キーを設定します。

show ssh server

セキュア シェル（SSH）サーバ ステータスを表示するには、**sshow ssh server** コマンドを使用します。

show ssh server

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、SSH サーバ ステータスを表示する例を示します。

```
switch# show ssh server
ssh version 2 is enabled
switch#
```

関連コマンド

コマンド	説明
ssh server enable	SSH サーバをイネーブルにします。

show startup-config aaa

スタートアップ コンフィギュレーションの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）設定情報を表示するには、**show startup-config aaa** コマンドを使用します。

show startup-config aaa

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スタートアップ コンフィギュレーションの AAA 情報を表示する例を示します。

```
switch# show startup-config aaa
```

関連コマンド

コマンド	説明
show running-config aaa	実行コンフィギュレーションの AAA コンフィギュレーション情報を表示します。

show startup-config aclmgr

スタートアップ コンフィギュレーションのアクセス コントロール リスト（ACL）の設定を表示するには、**show startup-config aclmgr** コマンドを使用します。

show startup-config aclmgr [**all**]

構文の説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、ACL スタートアップ コンフィギュレーションを表示する例を示します。

```
switch# show startup-config aclmgr

!Command: show startup-config aclmgr
!Time: Tue Aug 31 05:01:58 2010

version 5.0(2)N1(1)
ip access-list BulkData
  10 deny ip any any
ip access-list CriticalData
  10 deny ip any any
ip access-list Scavenger
  10 deny ip any any
mac access-list acl-mac
  10 permit any any
ip access-list denyv4
  20 deny ip 10.10.10.0/24 10.20.10.0/24 fragments
  30 permit udp 10.10.10.0/24 10.20.10.0/24 lt 400
  40 permit icmp any any router-advertisement
  60 deny tcp 10.10.10.0/24 10.20.10.0/24 syn
  70 permit igmp any any host-report
  80 deny tcp any any rst
  90 deny tcp any any ack
  100 permit tcp any any fin
  110 permit tcp any gt 300 any lt 400
  130 deny tcp any range 200 300 any lt 600
  140 deny tcp any range 200 300 any lt 600
:
<snip>
:
vlan access-map vacl-mac
  match mac address acl-mac
  action forward
  statistics per-entry
```

```
vlan filter vacl-mac vlan-list 300

interface Ethernet1/1
  ipv6 port traffic-filter denv6 in

interface Ethernet1/2
  ip port access-group voice in

interface Ethernet1/9
  ipv6 port traffic-filter denv6 in

interface Ethernet1/10
  ipv6 port traffic-filter denv6 in

line vty
  access-class myACList in
  access-class myACList out
  ipv6 access-class myI6List out

switch#
```

次に、VTY スタートアップ コンフィギュレーションを表示する例を示します。

```
switch# show startup-config aclmgr | begin vty
line vty
  access-class myACList in
  access-class myACList out
  ipv6 access-class myI6List out

switch#
```

関連コマンド

コマンド	説明
access-class	VTY のアクセス クラスを設定します。
copy running-config startup-config	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 ファイルにコピーします。
ip access-class	VTY の IPv4 アクセス クラスを設定します。
ipv6 access-class	VTY の IPv6 アクセス クラスを設定します。
show running-config aclmgr	ACL の実行コンフィギュレーションを表示します。

show startup-config arp

スタートアップ コンフィギュレーションのアドレス解決プロトコル（ARP）の設定を表示するには、**show startup-config arp** コマンドを使用します。

show startup-config arp [**all**]

構文の説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N1(1)	このコマンドが追加されました。

例

次に、ARP スタートアップ コンフィギュレーションを表示する例を示します。

```
switch# show startup-config arp

!Command: show running-config arp
!Time: Mon Aug 23 07:33:15 2010

version 5.0(2)N1(1)
ip arp timeout 2100
ip arp event-history errors size medium

interface Vlan10
  ip arp 10.193.131.37 00C0.4F00.0000

switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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 ファイルにコピーします。
ip arp event-history errors	イベント履歴バッファに ARP デバッグ イベントをロギングします。
ip arp timeout	ARP タイムアウトを設定します。
ip arp inspection	DHCP スヌーピングに関する一般的な情報を表示します。
show running-config arp	ARP の実行コンフィギュレーションを表示します。

show startup-config dhcp

スタートアップ コンフィギュレーションのダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピング設定を表示するには、**show running-config dhcp** コマンドを使用します。

show running-config dhcp [**all**]

構文の説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.0(2)N2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**feature dhcp** コマンドを使用して DHCP スヌーピング機能をイネーブルにする必要があります。

例

次に、スタートアップ コンフィギュレーション ファイルの DHCP スヌーピング設定を表示する例を示します。

```
switch# show startup-config dhcp

!Command: show startup-config dhcp
!Time: Mon Aug 23 09:09:14 2010

version 5.0(2)N1(1)
feature dhcp

ip dhcp snooping
ip dhcp snooping information option
service dhcp
ip dhcp relay
ip dhcp relay information option

ip arp inspection filter arp-acl-01 vlan 15,37-48

switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	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。

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
show running-config dhcp	DHCP の実行コンフィギュレーションを表示します。

show startup-config radius

スタートアップ コンフィギュレーションの RADIUS 設定情報を表示するには、**show startup-config radius** コマンドを使用します。

show startup-config radius

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スタートアップ コンフィギュレーションの RADIUS 情報を表示する例を示します。

```
switch# show startup-config radius
```

関連コマンド

コマンド	説明
show running-config radius	実行コンフィギュレーションの RADIUS サーバ情報を表示します。

show startup-config security

スタートアップ コンフィギュレーションのユーザ アカウント、セキュア シェル（SSH）サーバ、および Telnet サーバ コンフィギュレーション情報を表示するには、**show startup-config security** コマンドを使用します。

show startup-config security

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スタートアップ コンフィギュレーションのユーザ アカウント、SSH サーバ、および Telnet サーバ情報を表示する例を示します。

```
switch# show startup-config security
```

関連コマンド

コマンド	説明
show running-config security	実行コンフィギュレーションのユーザ アカウント、セキュア シェル（SSH）サーバ、および Telnet サーバ情報を表示します。

show tacacs-server

TACACS+ サーバ情報を表示するには、**show tacacs-server** コマンドを表示します。

show tacacs-server [*hostname* | *ip4-address* | *ip6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]

構文の説明

hostname	（任意）TACACS+ サーバのドメイン ネーム サーバ（DNS）名。最大文字サイズは 256 です。
ipv4-address	（任意）*A.B.C.D* 形式の TACACS+ サーバの IPv4 アドレス。
ipv6-address	（任意）*X:X:X::X* 形式の TACACS+ サーバの IPv6 アドレス。
directed-request	（任意）指定要求設定を表示します。
groups	（任意）設定された TACACS+ サーバ グループに関する情報を表示します。
sorted	（任意）TACACS+ サーバに関する名前でソートされた情報を表示します。
statistics	（任意）TACACS+ サーバの TACACS+ 統計情報を表示します。

コマンド デフォルト

グローバル TACACS+ サーバ設定を表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ 事前共有キーは、**show tacacs-server** コマンド出力には表示されません。TACACS+ 事前共有キーを表示するには、**show running-config tacacs+** コマンドを使用します。

TACACS+ 情報を表示する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、すべての TACACS+ サーバの情報を表示する例を示します。

```
switch# show tacacs-server
```

次に、指定された TACACS+ サーバの情報を表示する例を示します。

```
switch# show tacacs-server 192.168.2.2
```

次に、TACACS+ 指定要求設定を表示する例を示します。

```
switch# show tacacs-server directed-request
```

次に、TACACS+ サーバ グループの情報を表示する例を示します。

```
switch# show tacacs-server groups
```

次に、指定された TACACS+ サーバ グループの情報を表示する例を示します。

```
switch# show tacacs-server groups TacServer
```

次に、すべての TACACS+ サーバのソートされた情報を表示する例を示します。

```
switch# show tacacs-server sorted
```

次に、指定された TACACS+ サーバの統計情報を表示する例を示します。

```
switch# show tacacs-server statistics 192.168.2.2
```

関連コマンド

コマンド	説明
show running-config tacacs+	実行コンフィギュレーション ファイルの TACACS+ 情報を表示します。

show telnet server

Telnet サーバ ステータスを表示するには、**show telnet server** コマンドを使用します。

show telnet server

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、Telnet サーバ ステータスを表示する例を示します。

```
switch# show telnet server
```

関連コマンド

コマンド	説明
telnet server enable	Telnet サーバをイネーブルにします。

show user-account

スイッチ上のユーザ アカウントに関する情報を表示するには、**show user-account** コマンドを使用します。

show user-account [*name*]

構文の説明

name	（任意）指定したユーザ アカウントだけに関する情報です。

コマンド デフォルト

スイッチで定義されているすべてのユーザ アカウントに関する情報を表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

スイッチで定義されているすべてのユーザ アカウントに関する情報を表示する例を示します。

```
switch# show user-account

user:admin
        this user account has no expiry date
        roles:network-admin
user:mable
        this user account has no expiry date
        roles:network-operator
user:install
        this user account has no expiry date
        roles:network-admin
no password set. Local login not allowed
Remote login through RADIUS/TACACS+ is possible
user:user1
        this user account has no expiry date
        roles:priv-5
no password set. Local login not allowed
Remote login through RADIUS/TACACS+ is possible
switch#
```

次に、特定のユーザ アカウントに関する情報を表示する例を示します。

```
switch# show user-account admin
user:admin
        this user account has no expiry date
        roles:network-admin
switch#
```

関連コマンド

コマンド	説明
username	ユーザ アカウントを設定します。

show users

現在スイッチにログインしているユーザを表示するには、**show users** コマンドを使用します。

show users

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、現在スイッチにログインしているすべてのユーザを表示する例を示します。

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    ttyS0        Aug 24 22:19 10:41        4681
admin    pts/0        Aug 25 03:39   .          8890 (72.163.177.191) *
switch#
```

関連コマンド

コマンド	説明
clear user	特定のユーザをログアウトします。
username	ユーザ アカウントを作成および設定します。

show vlan access-list

IPv4 アクセス コントロール リスト（ACL）の内容、または特定の VLAN アクセス マップに関連付けられている MAC ACL を表示するには、**show vlan access-list** コマンドを使用します。

show vlan access-list *map-name*

構文の説明

map-name	表示する VLAN アクセス リストです。

コマンド デフォルト

なし

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

指定した VLAN アクセス マップについて、スイッチはアクセス マップ名とマップに関連付けられた ACL の内容を表示します。

例

次に、指定した VLAN アクセス マップに関連付けられた ACL の内容を表示する例を示します。

```
switch# show vlan access-list vlan1map
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を作成または設定します。
mac access-list	MAC ACL を作成または設定します。
show access-lists	VLAN アクセス マップが適用されている方法に関する情報を表示します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。
vlan access-map	VLAN アクセス マップを設定します。

show vlan access-map

すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示するには、**show vlan access-map** コマンドを使用します。

show vlan access-map [*map-name*]

構文の説明

map-name	（任意）表示する VLAN アクセス マップです。

コマンド デフォルト

map-name 引数を使用して特定のアクセス マップを選択する場合を除いて、スイッチはすべての VLAN アクセス マップを表示します。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

表示される各 VLAN アクセス マップに対して、スイッチはアクセス マップ名、**match** コマンドで指定された ACL、および **action** コマンドで指定された処理を表示します。

VLAN アクセス マップが適用されている VLAN を確認するには、**show vlan filter** コマンドを使用します。

例

次に、特定の VLAN アクセス マップを表示する例を示します。

```
switch# show vlan access-map vlan1map
```

次に、すべての VLAN アクセス マップを表示する例を示します。

```
switch# show vlan access-map
Vlan access-map vacl-mac
        match mac: acl-mac
        action: forward
        statistics per-entry

switch#
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。

コマンド	説明
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

show vlan filter

コマンドによって影響される VLAN アクセス マップおよび VLAN ID を含めて、**vlan filter** コマンドのインスタンスに関する情報を表示するには、**show vlan filter** コマンドを使用します。

show vlan filter [**access-map** *map-name* | **vlan** *vlan-id*]

構文の説明

access-map *map-name*	（任意）指定されたアクセス マップが適用されている VLAN に出力を制限します。
vlan *vlan-id*	（任意）指定された VLAN だけに適用されているアクセス マップに出力を制限します。

コマンド デフォルト

access-map キーワードを使用してアクセス マップを指定する場合、または **vlan** キーワードを使用して VLAN ID を指定する場合を除いて、VLAN に適用されている VLAN アクセス マップのすべてのインスタンスが表示されます。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スイッチのすべての VLAN アクセス マップ情報を表示する例を示します。

```
switch# show vlan filter

vlan map vacl-mac:
        Configured on VLANs:    300
switch#
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

T コマンド

この章では、T で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

tacacs-server deadtime

応答性について到達不能（非応答）TACACS+ サーバをモニタする定期的な時間間隔を設定するには、**tacacs-server deadtime** コマンドを使用します。非応答 TACACS+ サーバのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

構文の説明

time	分単位の時間間隔です。有効な範囲は 1 ～ 1440 です。

コマンド デフォルト

0 分

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

時間間隔の設定をゼロにすると、タイマーがディセーブルになります。個別の TACACS+ サーバのデッド タイム間隔がゼロ（0）よりも大きい場合は、サーバ グループに設定された値よりもその値が優先されます。

デッド タイム間隔が 0 分の場合、TACACS+ サーバがサーバ グループの一部でグループのデッド タイム間隔が 0 分を超えていない限り、TACACS+ サーバ モニタリングは実行されません。

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、デッド タイム間隔を設定して、定期的なモニタリングをイネーブルにする例を示します。

```
switch(config)# tacacs-server deadtime 10
```

次に、デッド タイム間隔をデフォルトに戻して、定期的なモニタリングをディセーブルにする例を示します。

```
switch(config)# no tacacs-server deadtime 10
```

関連コマンド

コマンド	説明
deadtime	非応答 RADIUS サーバ グループまたは TACACS+ サーバ グループをモニタリングするデッド タイム間隔を設定します。
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server	TACACS+ サーバ情報を表示します。

tacacs-server directed-request

ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できるようにするには、**tacacs-server directed-request** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server directed-request

no tacacs-server directed-request

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

設定した TACACS+ サーバ グループに認証要求を送信します。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

ログイン中に *username@vrfname:hostname* を指定できます。*vrfname* は使用する VRF、*hostname* は設定された TACACS+ サーバ名です。ユーザ名が認証用にサーバ名に送信されます。

例

次に、ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できるようにする例を示します。

```
switch(config)# tacacs-server directed-request
```

次に、ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できないようにする例を示します。

```
switch(config)# no tacacs-server directed-request
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server directed request	指定要求 TACACS+ サーバ コンフィギュレーションを表示します。

tacacs-server host

TACACS+ サーバ ホスト パラメータを設定するには、**tacacs-server host** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

no tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

構文の説明

hostname	TACACS+ サーバの Domain Name Server（DNS; ドメイン ネーム サーバ）名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。
ipv4-address	*A.B.C.D* フォーマットの TACACS+ サーバの IPv4 アドレスです。
ipv6-address	*X:X:X::X* フォーマットの TACACS+ サーバの IPv6 アドレスです。
key	（任意）TACACS+ サーバ用の共有秘密キーを設定します。
0	（任意）TACACS+ クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有キー（0 で表示）を設定します。これはデフォルトです。
7	（任意）TACACS+ クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有キー（7 で表示）を設定します。
shared-secret	TACACS+ クライアントとサーバ間の通信を認証する事前共有キー。事前共有キーは、英数字で指定します。大文字と小文字が区別され、最大文字数は 63 です。
port *port-number*	（任意）認証用の TACACS+ サーバのポートを設定します。有効な範囲は 1 ～ 65535 です。
test	（任意）テスト パケットを TACACS+ サーバに送信するようにパラメータを設定します。
idle-time *time*	（任意）サーバをモニタリングするための時間間隔を分数で指定します。時間の範囲は 1 ～ 1440 分です。
password *password*	（任意）テスト パケット内のユーザ パスワードを指定します。パスワードは、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。
username *name*	（任意）テスト パケット内のユーザ名を指定します。ユーザ名は、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。
timeout *seconds*	（任意）TACACS+ サーバへの再送信 TACACS+ サーバ タイムアウト期間（秒単位）を設定します。有効な範囲は 1 ～ 60 秒です。

コマンド デフォルト

アイドル時間：ディセーブル
サーバ モニタリング：ディセーブル
タイムアウト：1 秒
テスト ユーザ名：test
テスト パスワード：test

コマンド モード　グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン　TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

アイドル時間間隔が 0 分の場合、TACACS+ サーバの定期モニタリングは実行されません。

例　次に、TACACS+ サーバ ホスト パラメータを設定する例を示します。

```
switch(config)# tacacs-server host 192.168.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 192.168.2.3 test idle-time 10
switch(config)# tacacs-server host 192.168.2.3 test username tester
switch(config)# tacacs-server host 192.168.2.3 test password 2B9ka5
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server	TACACS+ サーバ情報を表示します。

tacacs-server key

グローバル TACACS+ 共有秘密キーを設定するには、**tacacs-server key** コマンドを使用します。設定した共有秘密キーを削除するには、このコマンドの **no** 形式を使用します。

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

構文の説明

0	（任意）TACACS+ クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有キーを設定します。これはデフォルトです。
7	（任意）TACACS+ クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有キーを設定します。
shared-secret	TACACS+ クライアントとサーバ間の通信を認証する事前共有キー。事前共有キーは、英数字で指定します。大文字と小文字が区別され、最大文字数は 63 です。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ サーバに対してスイッチを認証するには、TACACS+ 事前共有キーを設定する必要があります。キーの長さは 65 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。グローバル キーを設定して、スイッチにあるすべての TACACS+ サーバ コンフィギュレーションで使用するようにできます。**tacacs-server host** コマンドで **key** キーワードを使用することで、このグローバル キーの割り当てを上書きできます。

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、TACACS+ サーバ共有キーを表示および設定する例を示します。

```
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server	TACACS+ サーバ情報を表示します。

tacacs-server timeout

TACACS+ サーバへの再送信間隔を指定するには、**tacacs-server timeout** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

構文の説明

seconds	TACACS+ サーバへの再送信間隔を秒単位で設定します。有効な範囲は 1 ～ 60 秒です。

コマンド デフォルト

1 秒

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、TACACS+ サーバのタイムアウト値を設定する例を示します。

```
switch(config)# tacacs-server timeout 3
```

次に、デフォルトの TACACS+ サーバのタイムアウト値に戻す例を示します。

```
switch(config)# no tacacs-server timeout 3
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server	TACACS+ サーバ情報を表示します。

telnet

スイッチで IPv4 を使用して Telnet セッションを作成するには、**telnet** コマンドを使用します。Cisco Nexus 5000 シリーズ

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** {*vrf-name* | **default** | **management**}]

構文の説明

ipv4-address	リモート スイッチの IPv4 アドレス。
hostname	リモート スイッチのホスト名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 64 です。
port-number	（任意）Telnet セッションのポート番号。有効な範囲は 1 ～ 65535 です。
vrf *vrf-name*	（任意）Telnet セッションで使用する Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）名を指定します。名前は最大 32 文字の英数字で、大文字と小文字が区別されます。
default	デフォルト VRF を指定します。
management	管理 VRF を指定します。

コマンド デフォルト

ポート 23 がデフォルト ポートです。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

IPv6 アドレスで Telnet セッションを作成するには、**telnet6** コマンドを使用します。

例

次に、IPv4 を使用して Telnet セッションを開始する例を示します。

```
switch# telnet 192.168.1.1 vrf management
switch#
```

関連コマンド

コマンド	説明
clear line	Telnet セッションを消去します。
telnet server enable	Telnet サーバをイネーブルにします。
telnet6	IPv6 アドレスで Telnet セッションを作成します。

telnet server enable

Telnet サーバをイネーブルにするには、**telnet server enable** コマンドを使用します。Telnet サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

telnet server enable

no telnet server enable

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、Telnet サーバをイネーブルにする例を示します。

```
switch(config)# telnet server enable
```

次に、Telnet サーバをディセーブルにする例を示します。

```
switch(config)# no telnet server enable
```

関連コマンド

コマンド	説明
show telnet server	Telnet サーバのステータスを表示します。

telnet6

Cisco NX-OS スイッチで IPv6 を使用して Telnet セッションを作成するには **telnet6** コマンドを使用します。

telnet6 {*ipv6-address* | *hostname*} [*port-number*] [**vrf** {*vrf-name* | **default** | **management**}]

構文の説明

ipv6-address	リモート デバイスの IPv6 アドレス。
hostname	リモート デバイスのホスト名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 64 です。
port-number	（任意）Telnet セッションのポート番号。有効な範囲は 1 ～ 65535 です。
vrf *vrf-name*	（任意）Telnet セッションで使用する Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）名を指定します。名前は最大 32 文字の英数字で、大文字と小文字が区別されます。
default	デフォルト VRF を指定します。
management	管理 VRF を指定します。

コマンド デフォルト

ポート 23 がデフォルト ポートです。デフォルトの VRF が使用されます。

コマンド モード

EXEC モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**telnet server enable** コマンドを使用して Telnet サーバをイネーブルにする必要があります。

IPv4 アドレスで Telnet セッションを作成するには、**telnet** コマンドを使用します。

例

次に、IPv6 アドレスで Telnet セッションを開始する例を示します。

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
switch#
```

関連コマンド

コマンド	説明
clear line	Telnet セッションを消去します。
telnet	IPv4 アドレスで Telnet セッションを作成します。
telnet server enable	Telnet サーバをイネーブルにします。

U コマンド

この章では、U で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

use-vrf

RADIUS または TACACS+ サーバ グループの Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスを指定するには、**use-vrf** コマンドを使用します。VRF インスタンスを削除するには、このコマンドの **no** 形式を使用します。

use-vrf {*vrf-name* | **default** | **management**}

no use-vrf {*vrf-name* | **default** | **management**}

構文の説明

vrf-name	VRF インスタンス名です。名前は最大 32 文字の英数字で、大文字と小文字が区別されます。
default	デフォルト VRF を指定します。
management	管理 VRF を指定します。

コマンド デフォルト

なし

コマンド モード

RADIUS サーバ グループ コンフィギュレーション モード
TACACS+ サーバ グループ コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

サーバ グループに設定できるのは、1 つの VRF インスタンスだけです。

RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。あるいは、TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。

サーバを検索できなかった場合、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してサーバを設定します。

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、RADIUS サーバ グループの VRF インスタンスを指定する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf management
```

次に、TACACS+ サーバ グループの VRF インスタンスを指定する例を示します。

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf management
```

次に、TACACS+ サーバ グループから VRF インスタンスを削除する例を示します。

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf management
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ情報を表示します。
show tacacs-server groups	TACACS+ サーバ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。
vrf	VRF インスタンスを設定します。

username

ユーザ アカウントを作成および設定するには、**username** コマンドを使用します。ユーザ アカウントを削除するには、このコマンドの **no** 形式を使用します。

username *user-id* [**expire** *date*] [**password** {**0** | **5**} *password*] [**role** *role-name*] [**priv-lvl** *level*]

username *user-id* **sshkey** {*key* | **filename** *filename*}

no username *user-id*

構文の説明

user-id	ユーザ アカウントのユーザ ID。*user-id* 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。 **（注）** Cisco NX-OS ソフトウェアでは、*user-id* 引数の文字列に、「#」文字と「@」文字は使用できません。
expire *date*	（任意）ユーザ アカウントが満了する日付を指定します。*date* 引数の形式は、YYYY-MM-DD です。
password	（任意）アカウントのパスワードを指定します。デフォルトでは、パスワードは設定されていません。
0	パスワードがクリア テキストであることを指定します。これは、デフォルトのモードです。
5	パスワードが暗号化されることを指定します。
password	ユーザのパスワード（クリア テキスト）。パスワードは、最大 64 文字まで指定できます。 **（注）** クリア テキスト パスワードには、パスワードのいずれの部分にも、ドル記号（$）またはスペースを含めることはできません。また、パスワードの先頭には、引用符（" または '）、垂直バー（|）、または右山カッコ（>）の特殊文字を含めることはできません。
role *role-name*	（任意）ユーザに割り当てられるロールを指定します。有効な値は次のとおりです。 • **default-role** - ユーザ ロール • **network-admin** - システムで設定されたロール • **network-operator** - システムで設定されたロール • **priv-0** - 権限ロール • **priv-1** - 権限ロール • **priv-2** - 権限ロール • **priv-3** - 権限ロール • **priv-4** - 権限ロール • **priv-5** - 権限ロール • **priv-6** - 権限ロール • **priv-7** - 権限ロール • **priv-8** - 権限ロール • **priv-9** - 権限ロール

	• **priv-10** - 権限ロール • **priv-11** - 権限ロール • **priv-12** - 権限ロール • **priv-13** - 権限ロール • **priv-14** - 権限ロール • **priv-15** - 権限ロール • **vdc-admin** - システムで設定されたロール • **vdc-operator** - システムで設定されたロール
priv-lvl *level*	（任意）特権レベルをユーザを割り当てるように指定します。有効値は、0 ～ 15 です。
sshkey	（任意）ユーザ アカウントの SSH キーを指定します。
key	SSH キーの文字列。
filename *filename*	SSH キーの文字列を含むファイル名を指定します。

コマンド デフォルト　有効期限、パスワード、SSH キーはありません。

コマンド モード　グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。
5.0(2)N1(1)	**priv-lvl** キーワードが追加されました。

使用上のガイドライン　スイッチは強力なパスワードだけを受け入れます。強力なパスワードは、次の特性を備えています。

- 長さが 8 文字以上である
- 複数の連続する文字（「abcd」など）を含んでいない
- 複数の同じ文字の繰返し（「aaabbb」など）を含んでいない
- 辞書に載っている単語を含んでいない
- 固有名詞を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

注意　ユーザ アカウントのパスワードを指定しない場合、そのユーザはアカウントにログインできない可能性があります。

priv-lvl キーワードを表示するには、feature privilege コマンドを使用して TACACS+ サーバの累積権限ロールをイネーブルにする必要があります。

例

次に、パスワードを使用してユーザ アカウントを作成する例を示します。

```
switch(config)# username user1 password Ci5co321
switch(config)#
```

次に、ユーザ アカウントの SSH キーを設定する例を示します。

```
switch(config)# username user1 sshkey file bootflash:key_file
switch(config)#
```

次に、ユーザ アカウントの特権レベルを設定する例を示します。

```
switch(config)# username user1 priv-lvl 15
switch(config)#
```

関連コマンド

コマンド	説明
feature privilege	TACACS+ サーバでのコマンド認可に対するロールの累積権限をイネーブルにします。
show privilege	ユーザの累積権限サポートの現在の特権レベル、ユーザ名、およびステータスを表示します。
show user-account	ユーザ アカウントの設定を表示します。

V コマンド

この章では、V で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

vlan access-map

新規の VLAN アクセス マップを作成したり、既存の VLAN アクセス マップを設定したりするには、**vlan access-map** コマンドを使用します。VLAN アクセス マップを削除するには、このコマンドの **no** 形式を使用します。

vlan access-map *map-name*

no vlan access-map *map-name*

構文の説明

map-name	作成または設定する VLAN アクセス マップ名 名前では最大 64 文字までの英数字を使用でき、大文字と小文字が区別されます。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

各 VLAN アクセス マップには、1 つの **match** コマンドと 1 つの **action** コマンドを含めることができます。

例

次に、vlan-map-01 という名前で VLAN アクセス マップを作成して、そのマップに ip-acl-01 という名前の IPv4 ACL を割り当て、スイッチが ACL に一致するパケットを転送するよう指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

vlan filter

VLAN アクセス マップを 1 つ以上の VLAN に適用するには、**vlan filter** コマンドを使用します。VLAN アクセス マップの適用を解除するには、このコマンドの **no** 形式を使用します。

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* [**vlan-list** *VLAN-list*]

構文の説明

map-name	作成または設定する VLAN アクセス マップ名
vlan-list *VLAN-list*	VLAN アクセス マップがトラフィックをフィルタリングする 1 つ以上の VLAN の ID を指定します。 ハイフン（-）を使用して、VLAN ID の範囲の開始 ID と終了 ID を区別します（たとえば、70-100）。 カンマ（,）を使用して、各 VLAN ID および VLAN ID の範囲を区別します（たとえば、20,70-100,142）。 **（注）** このコマンドの **no** 形式を使用する場合、*VLAN-list* 引数を省略できます。この引数を省略する場合、スイッチはアクセス マップが適用されているすべての VLAN からアクセス マップを削除します。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

1 つ以上の VLAN に VLAN アクセス マップを適用できます。

VLAN に適用できるのは、1 つの VLAN アクセス マップだけです。

このコマンドの **no** 形式を使用すると、アクセス マップを適用したときに指定したすべてまたは一部分の VLAN リストから VLAN アクセス マップの適用を解除できます。適用されたすべての VLAN からアクセス マップの適用を解除する場合、*VLAN-list* 引数を省略できます。現在適用されている VLAN のサブセットからアクセス マップの適用を解除する場合、*VLAN-list* 引数を使用して、アクセス マップを削除する必要がある VLAN を指定します。

例

次に、vlan-map-01 という名前の VLAN アクセス マップを VLAN 20 ～ 45 に適用する例を示します。

```
switch(config)# vlan filter vlan-map-01 20-45
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。

vlan policy deny

ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始するには、**vlan policy deny** コマンドを使用します。ユーザ ロールのデフォルトの VLAN ポリシーに戻すには、このコマンドの **no** 形式を使用します。

vlan policy deny

no vlan policy deny

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

すべての VLAN

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

次に、ユーザ ロールのデフォルトの VLAN ポリシーに戻す例を示します。

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

vrf policy deny

ユーザの Virtual Forwarding and Routing（VRF; 仮想ルーティングおよび転送）インスタンス ポリシーへの拒否アクセスを設定するには、**vrf policy deny** コマンドを使用します。ユーザ ロールのデフォルトの VRF ポリシー設定に戻すには、このコマンドの **no** 形式を使用します。

vrf policy deny

no vrf policy deny

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールの VRF ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

次に、ユーザ ロールのデフォルトの VRF ポリシーに戻す例を示します。

```
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

vsan policy deny

ユーザ ロールの VSAN ポリシーへの拒否アクセスを設定するには、**vsan policy deny** コマンドを使用します。ユーザ ロールのデフォルトの VSAN ポリシー設定に戻すには、このコマンドの **no** 形式を使用します。

vsan policy deny

no vsan policy deny

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

VSAN ポリシーへのアクセスを許可するには、**permit vsan** コマンドを使用します。

例

次に、ユーザ ロールの VSAN ポリシーへのアクセスを拒否する方法の例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)#
```

次に、ユーザ ロールのデフォルトの VSAN ポリシー設定に戻す例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# no vsan policy deny
switch(config-role)#
```

関連コマンド

コマンド	説明
permit vsan	ユーザの VSAN ポリシーへの許可アクセスを設定します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。