Cisco Configuration Guide, Release 4.1

初版：2008 年 09 月 24 日

最終更新：2008 年 09 月 24 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: 123-456

【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。

目次

New and Changed Information

表 1：*New and Changed Features*

Feature	Description	Changed in Release	Where Documented

Preface

This preface describes the audience, organization, and conventions of the Cisco NX-OS Security Configuration Guide, Release . It also provides information on how to obtain related documentation.

Audience

Test

Document Organization

This document is organized into the following chapters:

Chapter	Description

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element(keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Screen examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

（注） Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

注意 Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Cisco NX-OS documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html

The documentation set for Cisco NX-OS includes the following documents:

Release Notes

NX-OS Configuration Guides

-
-

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

第 1 章

Configuring IP ACLs

This chapter describes how to configure IP access control lists (ACLs) on NX-OS devices. Unless otherwise specified, the term IP ACL refers to IPv4 and IPv6 ACLs.

（注） Although we fully support IPv6 ACLs, we recommend that you perform thorough validation testing of your IPv6 ACL implementation prior to deploying it in a production environment

QA test First Level TopicHead Check that this appears in TOC and in Chapter 1 miniTOC

Additional References

Related documents

Related Topic	Document Title
Concepts about VACLs	Example Configuration for IP ACLs， （15 ページ）
IP ACL commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco NX-OS Security Command Reference*

Related Topic	Document Title
Object group commands: complete command sytax, command modes, command history, defaults, usage guidelines, and examples	*Cisco NX-OS Security Command Reference*
Time range commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco NX-OS Security Command Reference*

Standards

Standard/RFC	Title
No New or modified standards are supported by this feature, and support for existing standards has not been modifed by thei feature.	—

MIBs

表 ***2***：***MIBs***

MIB	MIBs Link
This is a test for MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

QA Test: Check that the Figure numbers appear in sequence

図 ***1*** : ***There is a Figure Tag here***

はじめる前に

This is a test for figures.

手順の概要

1.

手順の詳細

	コマンドまたはアクション	目的
ステップ **1**	例：	There are 2 figure tags withing this Purpose Column 図 ***2*** : ***This is another Figure Tag here*** 図 ***3*** : ***There is another Figure Tag here***

```
This is an Example
```

QA Test First Level Topic head II Check that this appears in TOC and in Chapter 1 miniTOC

About Rules and indexes and conref tests

QA Test: **Check t**hat all the links below work in both PDF and html renditions and take you to the correct place

- internal xref to table 表 4：Table for xref, （4 ページ）
- internal xref to fig 図 4：This is a Fig Tag, （6 ページ）
- Xref to another topic Additional Filtering Options, （6 ページ）
- xref to table in another topic表 2：MIBs, （2 ページ）
- cross chapter xref to table 表 8：Conref Table, （19 ページ）
- cross chapter xref to topicLicensing Requirements for AAA, （19 ページ）

Rules are what you create, modify, and remove when you configure how an ACL filters network traffic. Rules appear in the running configuration. When you apply an ACL to an interface or change a rule within an ACL that is already applied to an interface, the supervisor module creates ACL entries from the rules in the running configuration and sends those ACL entries to the applicable I/O module. Depending upon how you configure the ACL, there may be more ACL entries than rules, especially if you use object groups when you configure rules. For more information, see the

You can create rules in ACLs and tYou can create rules in access-list configuration mode by using the **permit** or **deny** command. The device allows traffic that matches the criteria in a permit rule and blocks trafic that matches the criteria in a deny rule. You have many options for configuring the criteria that traffic must meet in order to match the rule

QA Test: Check that the following conreffed table renders
QA Test CSCsw88625 This description should appear before the table title in BOTH html and PDF renditions. Previously this was getting concatenated with the table title

表 ***3*** : ***Conref Table***

Product	**License Requirement**
NX-OS	AAA requires no license.Cisco Unified MeetingPlace Any feature not included in a license package is bundled with the Cisco NX-OS system images and is Cisco Unified MeetingPlaceprovided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide, Release 4.0.Cisco Unified IP Phone

QA Test: The index link should be generated on the fifth level and the second level because the second level is the last indexterm on the policy based ACLs topic. Go to the index and look at the first index - fifth index.

This section describes some of the options that you can use when you configure a rule. For information about every option, see the applicable **permit** and **deny** commands in the *Cisco NX-OS Security Command Reference*

QA Test: CSCsx53724 In the next paragraph, there should be no space after the text "Cisco Unified MeetingPlace" and the period that follows it.

This is Cisco Unified MeetingPlace.

QA Test : CSCsz10127 This is a xref to a step, it should render in both HTML and PDFステップ 2, （11 ページ）

表 ***4*** : ***Table for xref***

table head	**Desc**
this is a table	for xref

QA Test: CSCtd75733. Check that the following double bytesmart quotes appear while rendering: “smart quotes”. Edit ths topic (c_About_Rules.xml) and see the the double byte smart quotes appear correctly. Export this topic and see if the double byte smart quotes are still in tact.

Profiling Tests

-
-
-
-
-
- Supress Feature ID FTS2345
-
-
-
-
-
-
-
-
-
-
-

New profile values added after phase 2

New profile values added in Sprint 6

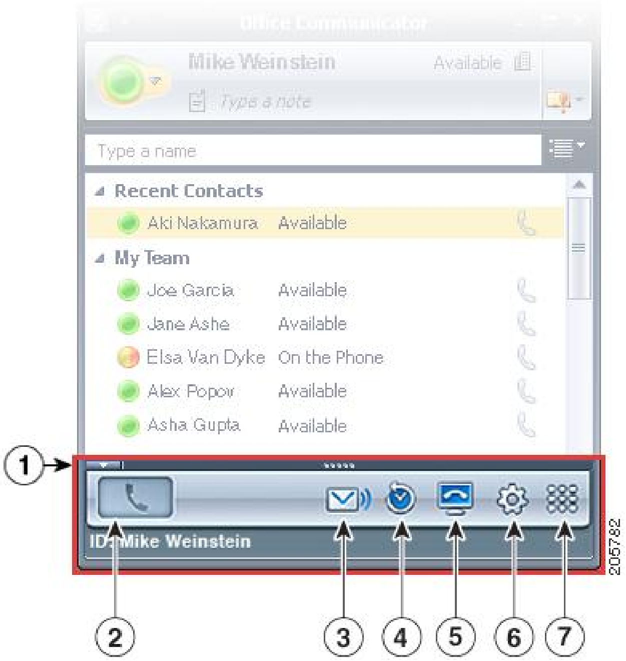
-
-
-
-
-
-
-
-
-
-

This is a simple table	blah blah blach
QA Test CSCte43613: Test that the note below appears correctly （注） I am a very long note and i like ot be very very long and i dont like to runn across a table and i like messing things up and I create problems for everyone becuase i am an note in a simpletable	（注） I am a very long note and i like ot be very very long and i dont like to runn across a table and i like messing things up and I create problems for everyone becuase i am an note in a simpletable

Image test

図 *4* : ***This is a Fig Tag***

図 *5* : ***This is a Fig Tag***



Office Communicator

Mike Weinstein Available

Type a note

Type a name

Recent Contacts

Aki Nakamura	Available

My Team

Joe Garcia	Available
Jane Ashe	Available
Elsa Van Dyke	On the Phone
Alex Popov	Available
Asha Gupta	Available

ID: Mike Weinstein

図 *6* : ***This is fig 3***

WIP

Additional Filtering Options

You can identify traffic by using additional options. These options differ by ACL type. The following list includes most but not all additional filtering options:

- IPv4 ACLs support the following additional filtering options:
    - Layer 4 protocol
    - TCP and UDP ports
    - ICMP types and codes

    - IGMP types
    - Precedence level
    - Differentiated Services Code Point (DSCP) value
    - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
    - Established TCP connections

- IPv6 ACLs support the following additional filtering options:
    - Layer 4 protocol
    - Authentication Header Protocol
    - Encapsulating Security Payload
    - Payload Compression Protocol
    - Stream Control Transmission Protocol (SCTP)
    - SCTP, TCP, and UDP ports
    - ICMP types and codes
    - IGMP types
    - Flow label
    - DSCP value
    - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
    - Established TCP connections

- MAC ACLs support the following additional filtering options:
    - Layer 3 protocol
    - VLAN ID
    - Class of Service (CoS)

For information about all filtering options available in rules, see the applicable**permit**and**deny**commands in the *Cisco NX-OS Security Command References*

Policy-Based ACLs

The device supports policy-based ACLs (PBACLs), which allow you to apply access control policies across object groups. An object group is a group of IP addresses or a group of TCP or UDP ports. When you create a rule, you specify the object groups rather than specifying IP addresses or ports.

uicontrolUsing object groups when you configure IPv4 or IPv6 ACLs can help of updating to add or remove addresses or ports from the source or destination of rules. For example, if three rules reference the same IP address group object,rules

QA: Testing font for <ph> elementPBACLs do not reduce the resources required by an ACL when you apply it to an interface. When you apply a PBACL or update a PBACL that is already applied, *italics*the device expands each rule that refers to object groups into one ACL entry per object within the group. If a rule specifies the source and destination both with object groups, the number of ACL entries created on the I/O module when you apply the PBACL is equal to the number of objects in the source group multiplied by the number of objects in the destination group**QA Test: This <b> should render in bold**

- QA Test: This ph should render in regular fonts
  QA Test: Check that the following emdash renders— **permit** or **deny** command to configure a rule, the addrgroupkeyword allows you to specify an object group for the source or destination

  italics
- IPv6 address object groups—Can be used with IPv6 ACL rules to specify source or destination addresses. When you use the **permit** or **deny** command to configure a rule, the addregroupkeyword allows you to specify an object group for the source or destinationuicontrol.

Configuring IP ACLs

This Figure shows the IPv4 ACL content

図 *7* : ***IPv4 ACL Content Pane***

QA Test: CSCsx68329:Check that the Second level bullets looks different from first level bullets

- a first level bullet
- another first level bullet
  - second level bullet

This section includes the following topics:

Forth Level Topic

Using object groups when you configure IPv4 or IPv6 ACLs can help reduce the complexity of updating ACLs when you need to add or remove addresses or ports from the source or destination of rules. For example, if three rules reference the same IP address group object, you can add an IP address to the object instead of changing all three rules

QA Test: This Section title should render in bold heading

PBACLs do not reduce the resources required by an ACL when you apply it to an interface. When you apply a PBACL or update a PBACL that is already applied, the device expands each rule that refers to object groups into one ACL entry per object within the group. If a rule specifies the source and destination both with object groups, the number of ACL entries created on the I/O module when you apply the PBACL is equal to the number of objects in the source group multiplied by the number of objects in the destination group

https://ciscoshare.cisco.com/alfext/ui/#/library/b6b987cb-05ec-4b2e-87fe-87b1108ed944

https://www.youtube.com/watch?v=I8vzbIuvhoo

Audience, （vii ページ）

QA Test: This Example title should render in bold heading

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

Fifth Level References Topic

QA Test: Check that this Section title renders as a bold heading

表 *5*：*Table Title*

Product	License Requirement
NX-OS	AAA requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide, Release 4.0.

表 *6*：*Technical Assistance*

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

QA Test: Check that this example heading renders as a bold heading

You can apply an IPv4 or IPv6 ACL to a Layer 2 interface, which can be a physical port or a port channel. ACLs applied to these interface types are considered port ACLs.

Task with no summary steps

You can apply an IPv4 or IPv6 ACL to a Layer 2 interface, which can be a physical port or a port channel. ACLs applied to these interface types are considered port ACLs.

CSCsw89155 The following procedure should render without any summary steps when rendering a topic. When rendering the whole book, it may show. There is a different cdets case open to track that

はじめる前に

Ensure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application. For more information, see the or the

手順の詳細

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td>ステップ 1</td><td><b>config t</b>
例：
<code>switch# config t</code>
<code>switch(config)#</code></td><td>Enters global configuration mode.</td></tr>
<tr><td>ステップ 2</td><td><b>interface ethernet</b> <i>slot</i>/<i>port</i>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>QA Test:CSCsu72601: This choicetable should not be dropped</td><td>choice table description</td></tr>
</table>
例：
<code>switch(config)# interface ethernet 2/3</code>
<code>switch(config-if)#</code></td><td>Enters interface configuration mode for a Layer 2 or Layer 3 physical interface</td></tr>
<tr><td>ステップ 3</td><td><b>ip port access-group|ipv6 port traffic-filter</b> <i>access-list</i> <b>in</b>
例：
<code>switch(config-if)# ip port access-group</code>
<code>acl-12-marketing-group in</code></td><td>Applies an IPv4 or IPv6 ACL to the interface or port channel. Only inbound filtering is supported with port ACLs. You can apply one port ACL to an interface.</td></tr>
<tr><td>ステップ 4</td><td><b>show running-config aclmgr</b>
例：
<code>switch(config-if)# show running-config aclmgr</code></td><td>（任意） QA Test: Optional Step Test. Make sure that the word (Optional) appears Here</td></tr>
<tr><td>ステップ 5</td><td><b>copy running-config startup-config</b>
例：
<code>switch(config-if)# copy running-config</code>
<code>startup-config</code></td><td>（任意） QA Test: The following info is followed by a Step Result. Check that the Step Result is not Dropped CSCsy00824: This is a step result. It should render.</td></tr>
</table>

QA Test: Check that this Step Example is rendered in a bold heading

To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.

Creating an IP ACL

You can create an IPv4 ACL or IPv6 ACL on the device and add rules to it.

はじめる前に

Ensure that you are in the correct VDC (or use the **switchto vdc** command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

手順の概要

1. （任意） **config t**
2. **ipipv6access-list***name*
3. *sequence-number***permitdeny***protocolsourcedestination*
4. **statistics per-entry**
5. **show ip access-lists***name*
6. **copy running-config startup-config**
7. <b> inside <codeblock> should render in yellow highlights

手順の詳細

ステップ1 （任意） **config t**

例：

QA test CSCsz39546: This First Step Should render with "(Optional)"

```
switch# config t
switch(config)#
```

.

Enters global configuration mode.

ステップ2 **ipipv6access-list***name*

例：

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

Creates the IP ACL and enters IP ACL configuration mode. The name argument can be up to 64 characters.

ステップ3 *sequence-number***permitdeny***protocolsourcedestination*

例：

```
switch(config-acl)# permit ip 192.168.2.0/24 any
```

Creates a rule in the IP ACL. You can create many rules. The sequence-number argument can be a whole number between 1 and 4294967295.

The**permit**and**deny**commands support many ways of identifying traffic. For more information, see the *Cisco NX-OS Security Command Reference*

ステップ4 **statistics per-entry**

例：

```
switch(config-acl)# statistics per-entry
```

Specifies that the device maintains global statistics for packets that match the rules in the ACL.

ステップ 5 **show ip access-lists***name*

例：

```
switch(config-acl)# show ip access-lists acl-01
```

Displays the IP ACL configuration.

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

例：

```
switch(config-acl)# copy running-config startup-config
```

Copies the running configuration to the startup configuration.

ステップ 7 <b> inside <codeblock> should render in yellow highlights

例：

```
QA Test: This bold should render in yellow highlights
```

Task with No table

You can change, reorder, add, and remove rules in an existing IPv4 or IPv6 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.*QA Test: This text should render in italics*

QA Test: check that this cmdName is rendered in bold command to reassign sequence numbers. For more information, see the .QA Test: Check that this <uicontrol is rendered in bold

はじめる前に

Ensure that you are in the correct VDC (or use the **switchto vdc** command). Because ACL names can be repeated in different VDCs, we recommend that you confirm which VDC you are working in.

手順の概要

1. uicontrolQA Test: This cmd should render in regular fonts**QA Test: Check that this wd is rendered in bold**
2. **ip**|**ipv6 access-list** *name*
3. *sequence-number* **permit**|**deny** *protocol source destination*
4. **no** {*sequence-number*} {**permit**|**deny**} *protocol source destination*
5. [**no**] **statistics per-entry**
6. **show ip access-lists** *name*
7. **copy running-config startup-config**

手順の詳細

ステップ 1 uicontrolQA Test: This cmd should render in regular fonts**QA Test: Check that this wd is rendered in bold**

例：

```
switch# config t
switch(config)#
```

Enters global configuration mode. uicontrol font

ステップ 2 **ip**|**ipv6 access-list** *name*

例：

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

Enters IP ACL configuration mode for the ACL that you specify by name.

ステップ 3 *sequence-number* **permit**|**deny** *protocol source destination*

例：

```
switch(config-acl)# 100 permit ip 192.168.2.0/24 any
```

Creates a rule in the IP ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The sequence-number argument can be a whole number between 1 and 4294967295.

The **permit** and **deny** commands support many ways of identifying traffic. *italics*For more information, see the QA: Check this is font for <cite>*QA Test: Check this cite is rendered in italics*

ステップ 4 **no** {*sequence-number*} {**permit**|**deny**} *protocol source destination*

例：

switch (config-acl) # no 80

Removes the rule that you specified from the IP ACL.

ステップ 5 [**no**] **statistics per-entry**

例：

```
switch (config-acl) # statistics per-entry
```

Specifies that the device maintains global statistics for packets that match the rules in the ACL.

The nouicontrol option stops the device from maintaining global statistics for the ACL.

ステップ 6 **show ip access-lists** *name*

例：

```
switch (config-acl)# show ip access-lists acl-01
```

Displays the IP ACL configuration.

ステップ 7 **copy running-config startup-config**

例：

```
switch (config-acl) # copy running-config startup-config
```

Copies the running configuration to the startup configuration.

Applying an ACL as a VACL

You can apply an IP ACL as a VACL. For information about how to create a VACL using an IPv4 or IPv6 ACL, see the “Creating or Changing a VACL” section on page 12-3.

Order of ACL Application with Figures

When the device processes a packet, it determines the forwarding path of the packet. The path determines which ACLs that the device applies to the traffic. The device applies the ACLs in the following order:

1. Port ACL
2. Ingress VACL
3. Ingress router ACL
4. SGACL
5. Egress router ACL
6. Egress VACL

If the packet is bridged within the ingress VLAN, the device does not apply router ACLs.

The Following fgure shows the order in which the device applies ACLS.

図 *8*： ***Order of ACL Application***

The following figure shows where the device applies ACLs, depending upon the type of ACL. The red path indicates a packet sent to a destination on a different interface than its source. The blue path indicates a packet that is bridged within its VLAN.

図 *9*： ***ACLs and Packet Flow***

Second level topichead

Information About ACLs

An ACL is an ordered set of rules that you can use to filter traffic. Each rule specifies a set of conditions that a packet must satisfy to match the rule. When the device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first matching rule determines whether the packet is permitted or denied. If there is no match, the device applies the applicable default rule. The device continues processing packets that are permitted and drops packets that are denied. For more information, see the Order of ACL Application with Figures, （14 ページ）

sem title

Error Message `QA test: CSCsx38952 This should render in courier fonts with heading "Error Message"`

Explanation QA Test: This should render in regular fonts with heading "Explanation"

Recommended Action QA Test: This should render in regular fonts with Heading"Recommended Action"

Example Configuration for IP ACLs

Example 1

The following example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL to Ethernet interface 2/1, which is a Layer 2 interface:

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

Example 2

The following example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL to Ethernet interface 2/1, which is a Layer 2 interface:

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

Example 3

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

Feature History for IP ACLs

表 *7*：***This is a regular table***

heading	heading	heading
content	content	content
content	content	content

Feature Name	Releases	Feature Information
statistics	4.0(3)	The Name of the **statistics** command was changed to **statistics bug entry**
QA Test: This Feature History table should render as a wide table in PDF		

Feature Name	Releases	Feature Information
statistics	4.0(3)	The Name of the **statistics** command was changed to **statistics bug entry**
QA Test: This Feature Information table should render as a wide table in PDF		

第 I 部

QA Test: The following conref in title should appear in High Nav in HTML preview Conref

第 2 章

Configuring AAA

Information About AAA

Prerequisites for AAA

Remote AAA servers have the following prerequisites:

- Ensure that at least one RADIUS or TACACS+ server is IP reachable (see the “Configuring RADIUS Server Hosts” section on page 3-6 and the “Configuring TACACS+ Server Hosts” section on page 4-8).
- Ensure that the NX-OS device is configured as a client of the AAA servers.

Licensing Requirements for AAA

QA Test CSCsw88625 This description should appear before the table title in BOTH html and PDF renditions. Previously this was getting concatenated with the table title

表 8 : ***Conref Table***

Product	License Requirement
NX-OS	AAA requires no license.Cisco Unified MeetingPlace Any feature not included in a license package is bundled with the Cisco NX-OS system images and is Cisco Unified MeetingPlaceprovided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the Cisco NX-OS Licensing Guide, Release 4.0.Cisco Unified IP Phone

Placing a Call

手順の概要

1. QA Test: CSCsz92064 The choices list (with the bullets), should render before the step Example
   - This is the first choice
   - This is the second Choice

手順の詳細

QA Test: CSCsz92064 The choices list (with the bullets), should render before the step Example

- This is the first choice
- This is the second Choice

例：

```
This step example should render after  the second choice.
```

トラブルシューティングのヒント

QA Test: The heading for Troubleshooting Tips should display only once in both PDF and html renditions

第 3 章

Wrapper for chapter

Information About AAA

Additional References

Related documents

Related Topic	Document Title
Concepts about VACLs	Example Configuration for IP ACLs, （15 ページ）
IP ACL commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco NX-OS Security Command Reference*
Object group commands: complete command sytax, command modes, command history, defaults, usage guidelines, and examples	*Cisco NX-OS Security Command Reference*
Time range commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco NX-OS Security Command Reference*

Standards

Standard/RFC	Title
No New or modified standards are supported by this feature, and support for existing standards has not been modifed by thei feature.	—

MIBs

表 9：MIBs

MIB	MIBs Link
This is a test for MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

adhoc tests

表 10：QA Test: Table with 16 columns (Check that the footnotes appear in order right after the tables here)

test[1]	ergerg[2]	erger[3]	grer	regreg	erger	egrerg	ergerg	ergerg	egerg	ergerg	egrerg	egerge	egerger	ergerg	egegeg

							middle footnote[4]							ergegr	footnote at the end [5]

[1] first footnote

[2] second footnote

[3] third footnote

[4] footnote in the middle

[5] end footnote

Second table footnote one [6]	Second table footnote 2 [7]
second table footnote three [8]	Second table footnote four [9]

[6] Second table footnote one

[7] Second table footnote two

[8] Second table footnote three

[9] Second table footnote four

para with outputclass set to FID

トラブルシューティングのヒント

para with outputclass set to Troubleshooting

問題　para with outputclass set to problem

考えられる原因　para with outputclass set to possible cause

para with outputclass set to solution

table with outputclass set to Feature info	

表 ***11*** : ***table with outputclass set to feature support***

dsfwe	tewefwfewst

QA Test: Check that the following Draft comment renders in pink when the bookmap is in a state less that review draft. If the bookmap is in a state Final Draft or Published, then the draft comment should not render at all

This topic has outpurclass set to prerequisite

This is a prereq topic

This is a topic with output class set to restrictions

This is restriction topic

This is topic with outputclass set to troubleshooting

output class is set to troubleshooting

付録 A

用語集

Attendant

A person to whom the Cisco Unified MeetingPlace Express system administrator has given privileges to reschedule all meetings and end all meetings via the Meeting Details web page. Attendants can perform limited system administrator tasks, such as viewing alarms and reports, in the Administration Center.

audience

One of three permission levels in a web meeting room. A person who has audience privileges has limited permissions during a meeting. In the full meeting room, audience members can also view shared content, chat messages, and notes, and send chat messages. Moderators and presenters can restrict audience chat messages.

No participant has this permission level by default. However, moderators can demote participants to this permission level during a meeting to restrict the activity of those participants.

Billing Code

The code your company or department uses if it performs bill-backs.

索 引