# Standard IP Access List Logging

The Standard IP Access List Logging feature provides the ability to log messages about packets that are permitted or denied by a standard IP access list. Any packet that matches the access list logs an information message about the packet at the device console.

This module provides information about standard IP access list logging.

### Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

### Contents

# Hardware Compatibility Matrix for the Cisco cBR Series Routers

**Note**

The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

*Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers*

| Cisco CMTS Platform | Processor Engine | Interface Cards |
|---|---|---|
| Cisco cBR-8 Converged Broadband Router | **Cisco IOS-XE Release 16.5.1 and Later Releases**<br><br>Cisco cBR-8 Supervisor:<br><br> • PID—CBR-SUP-250G<br><br> • PID—CBR-CCAP-SUP-160G<br><br> • PID—CBR-CCAP-SUP-60G | **Cisco IOS-XE Release 16.5.1 and Later Releases**<br><br>Cisco cBR-8 CCAP Line Cards:<br><br> • PID—CBR-LC-8D30-16U30<br><br> • PID—CBR-LC-8D31-16U30<br><br> • PID—CBR-RF-PIC<br><br> • PID—CBR-RF-PROT-PIC<br><br> • PID—CBR-CCAP-LC-40G<br><br> • PID—CBR-CCAP-LC-40G-R<br><br> • PID—CBR-SUP-8X10G-PIC<br><br> • PID—CBR-2X100G-PIC<br><br>Digital PICs:<br><br> • PID—CBR-DPIC-8X10G<br><br> • PID—CBR-DPIC-2X100G<br><br>Cisco cBR-8 Downstream PHY Module:<br><br> • PID—CBR-D31-DS-MOD<br><br>Cisco cBR-8 Upstream PHY Modules:<br><br> • PID—CBR-D31-US-MOD |

# Restrictions for Standard IP Access List Logging

IP access list logging is supported only for routed interfaces or router access control lists (ACLs).

# Information About Standard IP Access List Logging

## Standard IP Access List Logging

The Standard IP Access List Logging feature provides the ability to log messages about packets that are permitted or denied by a standard IP access list. Any packet that matches the access list causes an information

log message about the packet to be sent to the device console. The log level of messages that are printed to the device console is controlled by the **logging console** command.

The first packet that the access list inspects triggers the access list to log a message at the device console. Subsequent packets are collected over 5-minute intervals before they are displayed or logged. Log messages include information about the access list number, the source IP address of packets, the number of packets from the same source that were permitted or denied in the previous 5-minute interval, and whether a packet was permitted or denied. You can also monitor the number of packets that are permitted or denied by a particular access list, including the source address of each packet.

# How to Configure Standard IP Access List Logging

## Creating a Standard IP Access List Using Numbers

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} **host** *address* [**log**]
4. **access-list** *access-list-number* {**deny** | **permit**} **any** [**log**]
5. **interface** *type number*
6. **ip access-group** *access-list-number* {**in** | **out**}
7. **end**

### DETAILED STEPS

|  | **Command or Action** | **Purpose** |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **access-list** *access-list-number* {**deny** | **permit**} **host** *address* [**log**]<br><br>**Example:**<br>`Device(config)# access-list 1 permit host 10.1.1.1 log` | Defines a standard numbered IP access list using a source address and wildcard, and configures the logging of informational messages about packets that match the access list entry at the device console. |
| **Step 4** | **access-list** *access-list-number* {**deny** | **permit**} **any** [**log**]<br><br>**Example:**<br>`Device(config)# access-list 1 permit any log` | Defines a standard numbered IP access list by using an abbreviation for the source and source mask 0.0.0.0 255.255.255.255. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **interface** *type number*<br><br>**Example:**<br><br>`Device(config)# interface TenGigabitEthernet4/1/0` | Configures an interface and enters interface configuration mode. |
| **Step 6** | **ip access-group** *access-list-number* {**in** \| **out**}<br><br>**Example:**<br><br>`Device(config-if)# ip access-group 1 in` | Applies the specified numbered access list to the incoming or outgoing interface.<br><br>• When you filter based on source addresses, you typically apply the access list to an incoming interface. |
| **Step 7** | **end**<br><br>**Example:**<br><br>`Device(config-if)# end` | Exits interface configuration mode and enters privileged EXEC mode. |

# Creating a Standard IP Access List Using Names

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip access-list standard** *name*
4. {**deny** \| **permit**} {**host** *address* \| **any**} **log**
5. **exit**
6. **interface** *type number*
7. **ip access-group** *access-list-name* {**in** \| **out**}
8. **end**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Device> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip access-list standard** *name*<br><br>**Example:**<br><br>`Device(config)# ip access-list standard acl1` | Defines a standard IP access list and enters standard named access list configuration mode. |
| **Step 4** | {**deny** \| **permit**} {**host** *address* \| **any**} **log**<br><br>**Example:** | Sets conditions in a named IP access list that will deny packets from entering a network or permit packets to enter |

| | Command or Action | Purpose |
|---|---|---|
| | Device(config-std-nacl)# permit host 10.1.1.1 log | a network, and configures the logging of informational messages about packets that match the access list entry at the device console. |
| Step 5 | **exit**<br><br>**Example:**<br><br>Device(config-std-nacl)# exit | Exits standard named access list configuration mode and enters global configuration mode. |
| Step 6 | **interface** *type number*<br><br>**Example:**<br><br>Device(config)# interface TenGigabitEthernet4/1/0 | Configures an interface and enters interface configuration mode. |
| Step 7 | **ip access-group** *access-list-name* {**in** \| **out**}<br><br>**Example:**<br><br>Device(config-if)# ip access-group acl1 in | Applies the specified access list to the incoming or outgoing interface.<br><br>• When you filter based on source addresses, you typically apply the access list to an incoming interface. |
| Step 8 | **end**<br><br>**Example:**<br><br>Device(config-if)# end | Exits interface configuration mode and enters privileged EXEC mode. |

# Configuration Examples for Standard IP Access List Logging

## Example: Limiting Debug Output

The following sample configuration uses an access list to limit the **debug** command output. Limiting the **debug** output restricts the volume of data to what you are interested in, saving you time and resources.

```
Device(config)# ip access-list acl1
Device(config-std-nacl)# remark Displays only advertisements for LDP peer in acl1
Device(config-std-nacl)# permit host 10.0.0.44

Device# debug mpls ldp advertisements peer-acl acl1

tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.17.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.16.0.31
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.22.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.1
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.3
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.1.33
```

# Additional References for Standard IP Access List Logging

**Related Documents**

| Related Topic | Document Title |
|---|---|
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br><br>• Cisco IOS Security Command Reference: Commands D to L<br><br>• Cisco IOS Security Command Reference: Commands M to R<br><br>• Cisco IOS Security Command Reference: Commands S to Z |

**Technical Assistance**

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

# Feature Information for Standard IP Access List Logging

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

**Note** The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

*Table 2: Feature Information for Standard IP Access List Logging*

| Feature Name | Releases | Feature Information |
|---|---|---|
| IP Access Lists | Cisco IOS XE Fuji 16.7.1 | This feature was integrated into Cisco IOS XE Fuji 16.7.1 on the Cisco cBR Series Converged Broadband Routers. |