



Protocol-Independent MAC ACL Filtering on the Cisco 12000 Series Internet Router

Part Number OL-142368-01 (Rev A0), January 19, 2006

The Protocol-Independent MAC ACL Filtering feature allows you to create Layer 2 access control lists (ACLs) that filter incoming Ethernet packets. You can configure Protocol-Independent MAC ACL Filtering on a Cisco 12000 series Internet router that is deployed as a provider-edge (PE) router to filter customer traffic based on the source MAC address in the Layer 2 header of Ethernet, 802.1Q VLAN, and 802.1Q-in-Q packets.

History for the Protocol-Independent MAC ACL Filtering Feature

Release	Modification
12.0(32)S	This feature was introduced on the Cisco 12000 series Internet router on 4-port Gigabit Ethernet IP Services Engine (ISE) line cards.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Protocol-Independent MAC ACL Filtering, page 2](#)
- [Restrictions for Protocol-Independent MAC ACL Filtering, page 2](#)
- [Information About Protocol-Independent MAC ACL Filtering, page 3](#)
- [Configuring Protocol-Independent MAC ACL Filtering, page 4](#)
- [Configuration Example for Protocol-Independent MAC ACL Filtering, page 8](#)
- [Additional References, page 9](#)
- [Command Reference, page 10](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

Prerequisites for Protocol-Independent MAC ACL Filtering

When you use the Protocol-Independent MAC ACL Filtering feature on the Cisco 12000 series Internet router, note the following prerequisites:

- Starting in Cisco IOS Release 12.0(32)S, the Protocol-Independent MAC ACL Filtering feature is supported only on 4-port Gigabit Ethernet ISE line cards in a Cisco 12000 series Internet router.
- To enable a MAC ACL on a subinterface, the subinterface must already be configured for 802.1Q VLAN or stacked VLAN (802.1Q-in-Q) operation.

Restrictions for Protocol-Independent MAC ACL Filtering

The Protocol-Independent MAC ACL Filtering feature is implemented on the Cisco 12000 series Internet router with the following restrictions:

- MAC ACLs are supported only on ingress interfaces and subinterfaces.
- Only MAC ACLs that specify a source MAC address without an address mask are supported.
- Only one MAC ACL is supported on an interface or subinterface. You can also apply Layer 3 ACLs on an interface on which a MAC ACL is configured.
- A MAC ACL is not supported as a match criteria in:
 - A class map configured using the modular Quality-of-Service (QoS) command-line interface (MQC).
 - Committed Access Rate (CAR) values configured using the **rate-limit** command.
- Up to one hundred MAC ACLs in the range 700 to 799 are supported on an interface or subinterface.

The following additional restrictions apply to a MAC ACL applied on an interface or subinterface on a 4-Port Gigabit Ethernet ISE line card:

- By default, a MAC ACL applied to an interface can contain up to 1960 access control entries (ACEs); a MAC ACL applied to an 802.1Q VLAN or stacked VLAN (802.1Q-in-Q) subinterface can contain up to 7200 ACEs.
- When applied to a subinterface configured for stacked VLAN (802.1Q-in-Q) processing, a MAC ACL is applied to traffic received on all 802.1Q-in-Q subinterfaces that have the service-provider VLAN ID (SP-VLAN ID).
- The MAC counters maintained by the source address-based MAC accounting feature may not be accurate for incoming traffic on an interface on which you configure a MAC ACL.

Information About Protocol-Independent MAC ACL Filtering

To configure the Protocol-Independent MAC ACL Filtering feature, you should understand the following concepts:

- [Access Control Lists, page 3](#)
- [Layer 2 Access Control Lists, page 3](#)

Access Control Lists

Cisco provides basic traffic filtering capabilities with access control lists (ACLs, also referred to as access lists). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router.

You configure access lists on a router to filter traffic and provide basic security for your network. Access lists can prevent certain traffic from entering or exiting a network. If you do not configure ACLs, all packets passing through the router could be allowed on all parts of the network. You can use ACLs to control which hosts can access different parts of a network or to decide which types of traffic are forwarded or blocked at router interfaces. For example, you can allow e-mail traffic to be forwarded but not Telnet traffic. ACLs can be configured to block inbound traffic, outbound traffic, or both. However, on Layer 2 interfaces, you can apply ACLs only in the inbound direction.

An ACL is an ordered list of access control entries (ACEs). Each ACE specifies permit or deny and a set of conditions the packet must satisfy in order to match the ACE. The meaning of permit or deny depends on the context in which the ACL is used. When a packet is received on an interface, the router compares the fields in the packet against any applied ACLs to verify that the packet has the permissions required to be forwarded, based on the conditions specified in the access lists.

An ACL tests the packets against the ACEs in its list one-by-one. Because the first match determines whether the router accepts or rejects packets, the order of permit and deny conditions in the list is critical. If no conditions match, the router drops the packet; if there are no restrictions, the router forwards the packet.

The Cisco 12000 series Internet router supports two types of ACLs:

- Layer 2 ACLs filter traffic based on the Layer 2 MAC address in packet headers.
- Layer 3 ACLs filter traffic based on the Layer 3 IP address in packet headers.

Layer 2 Access Control Lists

Layer 2 ACLs allow a router to filter ingress and egress traffic based on the source or destination MAC address in the Layer 2 header of a packet. A MAC address is a standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use MAC addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long.

Starting in Cisco IOS Release 12.0(32)S, Layer 2 ACLs based on the source MAC address are supported on the ingress interfaces and subinterfaces of 4-port Gigabit Ethernet IP Services Engine (ISE) line cards in the Cisco 12000 series Internet router.

When applied to an interface or subinterface, a MAC ACL filters incoming Ethernet, VLAN, and 802.1Q-in-Q packets based on the source MAC address in Layer 2 packet headers. MAC ACLs filter all types of ingress traffic, including IPv4, IPv6, and Layer 2 tunneling protocols, such as Ethernet over MPLS (EoMPLS) and Virtual Private LAN Service (VPLS).

When you create an ACL based on the source MAC address using the **access-list** command, the valid values for the access-list number are from 700 to 799.

In addition, you can configure QoS policies (using the MQC interface) and CAR values (using the **rate-limit** command) on an interface or subinterface on which you apply a MAC ACL.

Configuring Protocol-Independent MAC ACL Filtering

This section contains the following procedures:

- [Creating a MAC ACL, page 4](#)
- [Applying a MAC ACL on a Gigabit Ethernet Interface or Subinterface, page 5](#)
- [Displaying MAC ACL Statistics, page 6](#)
- [Clearing MAC ACL Statistics, page 7](#)

Creating a MAC ACL

To create a MAC ACL which you can later apply on a Gigabit Ethernet interface, an 802.1Q VLAN subinterface, or a stacked VLAN (802.1Q-in-Q) subinterface, follow these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} {*mac-address* | **any**}
4. Repeat Step 3 to configure additional permit and deny entries in the MAC ACL.

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	access-list <i>access-list-number</i> {deny permit} { <i>mac-address</i> any} Example: Router(config)# access-list 700 permit 0003.fdb.8700	Creates an access list based on a source MAC address, where: <i>access-list-number</i> assigns the number of a MAC ACL in the range 700 to 799. deny discards a packet if the conditions are matched. permit forwards a packet if the conditions are matched. <i>mac-address</i> defines the source MAC address to use to filter packets. MAC addresses are 6 bytes long. any includes all source MAC addresses that are not specified in a permit or deny entry in the ACL as match criteria.

Applying a MAC ACL on a Gigabit Ethernet Interface or Subinterface

To apply a MAC ACL on a Gigabit Ethernet interface, an 802.1Q VLAN subinterface, or a stacked VLAN (802.1Q-in-Q) subinterface, follow these steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port/subinterface-number*
4. **mac access-group** *access-list-number in*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot/port.subinterface-number</i> Example: Router(config)# interface gigabitethernet 1/0.2	Enters interface or subinterface configuration mode and specifies the Gigabit Ethernet interface, 802.1Q VLAN subinterface, or stacked VLAN (802.1Q-in-Q) subinterface on which you want to apply a MAC ACL.

	Command or Action	Purpose
Step 4	<pre>mac access-group access-list-number in</pre> <p>Example: Router(config-subif)# interface gigabitethernet 1/0.2 </p>	Applies the MAC ACL to the interface or subinterface on ingress traffic.
Step 5	<pre>end</pre> <p>Example: Router(config-if)# end </p>	Exits interface configuration mode and returns to privileged EXEC mode.

Displaying MAC ACL Statistics

To display the configuration and statistics for one or all MAC ACLs applied to the Gigabit Ethernet interfaces and subinterfaces on a Cisco 12000 series Internet router or line card, use the **show mac access-lists** command in privileged EXEC or line-card configuration mode.

To display MAC ACL statistics for a specified Cisco 12000 series line card, you must connect to the line card in either of the following ways:

- Enter the **attach slot-number** command in privileged EXEC mode.
- Enter the **execute-on slot slot-number** command in privileged EXEC mode as a prefix to the **show** command to connect directly to the image on the line card.

Command	Purpose
<pre>Router# show mac access-lists [access-list-number]</pre> <p>Or</p> <pre>Router# attach slot-number LC-Slot# show mac access-lists [access-list-number]</pre> <p>Or</p> <pre>Router# execute-on slot slot-number show mac access-lists [access-list-number]</pre> <p>Example: Router# execute-on slot 4 show access-lists </p>	Displays the contents of one or all MAC access lists applied on all line cards on the router or on a specified line card.

Clearing MAC ACL Statistics

To clear the statistics for a specific or all MAC ACLs on a Cisco 12000 series Internet router or line card, follow these steps:

SUMMARY STEPS

1. **enable**
2. **clear mac access-list counters** [*access-list-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<pre>clear mac access-list counters [access-list-number]</pre> <p>Or</p> <pre>Router# attach slot-number LC-Slot# clear mac access-list counters [access-list-number]</pre> <p>Or</p> <pre>Router# execute-on slot slot-number clear mac access-list counters [access-list-number]</pre> <p>Example: Router# clear mac access-list counters 701 </p>	<p>Clears the statistical counters for a specified MAC ACL or for all current MAC ACLs, and resets them to zero.</p> <p><i>access-list-number</i> identifies the number of a MAC ACL in the range 700 to 799. If you do not enter an access-list number, statistics for all MAC ACLs on the router or line card are cleared.</p>

Configuration Example for Protocol-Independent MAC ACL Filtering

The following example shows how to configure a MAC ACL to receive inbound traffic from three customer devices on a VLAN subinterface on a 4-Port Gigabit Ethernet ISE line card and deny traffic from all other devices:

MAC ACL configuration

```
Router> enable
Router# configure terminal
Router(config)# access-list 700 permit 0003.fd1b.8700
Router(config)# access-list 700 permit 0003.fd1b.8701
Router(config)# access-list 700 permit 0003.fd1b.8702
Router(config)# access-list 700 deny any
```

Apply MAC ACL to Gigabit Ethernet VLAN subinterface

```
Router(config)# interface gigabitethernet 6/0.1
Router(config-subif)# mac access-group 700 in
Router(config-subif)# end
```

Additional References

The following sections provide references related to Protocol-Independent MAC ACL Filtering.

Related Documents

Related Topic	Document Title
Overview description of how to use access control lists to filter network traffic	Access Control Lists: Overview and Guidelines
Detailed description of how to configure and use access control lists to filter IP traffic	“Configuring IP Services” chapter in the Cisco IOS IP Configuration Guide “IP Services Commands” chapters in the Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services , Release 12.2
Detailed description of how to configure and use access control lists on Cisco 12000 series line cards	Implementing Access Lists on Cisco 12000 Series Internet Routers
Configuration commands and procedures for Cisco IOS security features	Cisco IOS Security Configuration Guide , Release 12.3 Cisco IOS Security Command Reference , Release 12.3
Description of software functionality and commands supported on the 4-Port Gigabit Ethernet ISE line card	4-Port Gigabit Ethernet ISE Line Card for Cisco 12000 Series Internet Router

Standards

Standard	Title
No new or modified standards are supported by this feature.	

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	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

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0S command reference publications.

- [access-list \(MAC\), page 11](#)
- [clear mac access-list counters, page 14](#)
- [mac access-group, page 16](#)
- [show mac access-list, page 18](#)

access-list (MAC)

To define an access list (ACL) that filters packets based on the source MAC address in Layer 2 packet headers, use the MAC version of the **access-list** command in global configuration mode. To remove a MAC access list or a specific MAC ACL entry, use the **no** form of this command.

```
access-list access-list-number {deny | permit} {mac-address | any}
```

```
no access-list access-list-number
```

Or

```
no access-list access-list-number {deny | permit} {mac-address | any}
```

Syntax Description	
<i>access-list-number</i>	Number of a MAC access list. This is a decimal number from 700 to 799.
deny	Discards a packet if the conditions are matched.
permit	Forwards a packet if the conditions are matched.
<i>mac-address</i>	48-bit MAC address written as a dotted triplet of four-digit hexadecimal numbers in the format <i>xxxx.xxxx.xxxx</i> .
	Note The MAC version of the access-list command does not support the <i>source-wildcard</i> argument, which specifies the wildcard bits to be applied to the source.
any	Includes all source MAC addresses that are not specified in a permit or deny entry in the ACL as match criteria.
	Note You can enter the access-list command with the any keyword anywhere in a MAC ACL. When a MAC ACL is processed, access-list command entries which use the any keyword are automatically moved to the bottom of the list and processed last.

Defaults

A MAC ACL defaults to an implicit deny statement for all inbound packets.

To change the default behavior and allow incoming traffic from all source MAC addresses that are not specifically configured in a **deny** statement, enter the **access-list permit any** command at the end of the MAC ACL.

Command Modes

Global configuration

Command History

Release	Modification
12.0(32)S	This command was introduced on the Cisco 12000 series Internet router.

Usage Guidelines

You can use a MAC ACL to control the transmission of packets on a Gigabit Ethernet interface, an 802.1Q VLAN subinterface, or a stacked VLAN (802.1Q-in-Q) subinterface, including packets with broadcast and multicast MAC addresses which match the source address specified in the MAC ACL. A MAC ACL filters incoming traffic only. Only one MAC ACL is supported on an interface.

MAC ACLs are applied on Gigabit Ethernet interfaces and VLAN subinterfaces. After receiving a packet, the Cisco IOS software checks the source MAC address of the Gigabit Ethernet, 802.1Q VLAN, or 802.1Q-in-Q packet against the access list. If the MAC access list permits the address, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an ICMP host unreachable message.

An ACL tests the packets against its permit and deny entries in the order in which the entries are listed. Therefore, plan your access conditions carefully. The first match on a source MAC address determines whether the router accepts or rejects the packets. Because the router stops testing packets from a source MAC address after the first match, the order of permit and deny conditions in the ACL is critical.

**Note**

You can enter the **access-list** command with the **any** keyword anywhere in a MAC ACL. When a MAC ACL is processed, **access-list** command entries which use the **any** keyword are automatically moved to the bottom of the list and processed last.

There is an implicit deny entry (**access-list access-list-number deny any**) at the end of a MAC ACL. If no permit and deny conditions match, the router drops a packet. To change the implicit **deny any** entry, you must enter an explicit **permit any** statement. To later reconfigure a **deny any** or **permit any** entry at the end of the MAC ACL, follow these steps:

1. Remove the final **access-list access-list-number {deny | permit} any** statement by entering the **no** form of the command:
no access-list access-list-number {deny | permit} any
2. Enter the new **access-list access-list-number {deny | permit} any** statement.

On a VLAN subinterface on which no MAC ACL is configured, the default behavior is to permit all VLAN packets.

If you apply a MAC ACL on a Gigabit Ethernet interface on which EoMPLS tunneling is enabled, the MAC ACL filters all incoming traffic. ACLs applied to a subinterface are ignored.

Configuring a MAC ACL on an interface or subinterface does not affect the scalability of VLAN, Layer 2 Tunnel Protocol (L2TP), and MAC accounting (based on the source address or destination address).

You can apply MAC ACLs and Layer 3 ACLs on the same Gigabit Ethernet interface. Layer 3 ACLs are not supported on a VLAN subinterface.

Use the **show mac access-lists** command to display the contents and statistics of one or all MAC ACLs.

To delete a MAC ACL, use the **no access-list access-list-number** command. To delete a MAC ACL entry, use the **no access-list access-list-number {deny | permit} {mac-address | any}** command.

Examples

The following example of a MAC ACL allows access for packets received from three customer devices. Packets transmitted from any other source address that does not match the source MAC addresses in these access list statements are rejected.

```
Router> enable
Router# configure terminal
Router(config)# access-list 1 permit 00aa.00aa.00aa
Router(config)# access-list 1 permit 00bb.00bb.00bb
Router(config)# access-list 1 permit 00cc.00cc.00cc
! (Note: all other access implicitly denied)
```

The following example of a MAC ACL allows access for traffic from all devices except the source MAC address 00dd.00dd.00d.

```
Router> enable
Router# configure terminal
Router(config)# access-list 1 permit 00aa.00aa.00aa
Router(config)# access-list 1 permit 00bb.00bb.00bb
Router(config)# access-list 1 permit 00cc.00cc.00cc
Router(config)# access-list 1 deny 00dd.00dd.00dd
Router(config)# access-list 1 permit any
```

To delete the MAC ACL entry that rejects packets from the source MAC address 00dd.00dd.00d, enter the following command:

```
Router(config)# no access-list 1 deny 00dd.00dd.00dd
```

Related Commands

Command	Description
clear mac access-list counters	Clears the counters of a MAC ACL.
mac access-group	Controls access to an interface according to the source MAC address in a Layer 2 packet header.
show mac access-list	Displays the contents of one or all MAC ACLs.

clear mac access-list counters

To clear the counters of one or all MAC access lists on a router or specified line card, use the **clear mac access-list counters** command in privileged EXEC or line-card configuration mode.

clear mac access-list counters [*access-list-number*]

Syntax Description	<i>access-list-number</i>	(Optional) Number of the MAC access list from 700 to 799 for which to clear the counters. If you do not enter an access-list number, statistics for all MAC ACLs on the router or line card are cleared.
---------------------------	---------------------------	--

Command Modes	Privileged EXEC Line-card configuration
----------------------	--

Command History	Release	Modification
	12.0(32)S	This command was introduced on the Cisco 12000 series Internet router.

Usage Guidelines Some access lists use counters to count the number of packets that pass each line of the access list. The **show mac access-list** command displays the counters as a number of matches.

Use the **clear mac access-list counters** command to reset the counters to 0 for a particular MAC ACL or all MAC ACLs.

Use the **clear mac access-list counters** command in privileged EXEC mode to clear the counters for one or all MAC ACLs configured on a router. To clear MAC ACL counters on a specified line card, do one of the following:

- Use the **attach slot-number** command in privileged EXEC mode to connect to a line card. Then, from line-card configuration mode, enter the **clear mac access-list counters** command. For example:

```
Router# attach 2
LC-Slot2# clear mac access-list counters
```

- Use the **execute-on slot-number** command as a prefix to the **clear mac access-list counters** command in privileged EXEC mode. For example:

```
Router# execute-on 2 clear mac access-list counters
```

Examples

The following example clears the counters for MAC access list 101 on a router:

```
Router# clear mac access-list counters 101
```

The following examples clear the counters for access list 101 configured on the line card installed in slot 4:

```
Router# execute-on 4 clear mac access-list counters 101
```

```
Router# attach 4
LC-SLOT4# clear mac access-list counters 101
```

Related Commands

Command	Description
show mac access-list	Displays the contents of MAC ACLs.

mac access-group

To use a MAC access list (ACL) to control the reception of incoming traffic on a Gigabit Ethernet interface, an 802.1Q VLAN subinterface, or an 802.1Q-in-Q stacked VLAN subinterface, use the **mac access-group** command in interface or subinterface configuration mode. To remove a MAC ACL, use the **no** form of this command.

mac access-group {*access-list-number*} **in**

no mac access-group {*access-list-number*} **in**

Syntax Description	<i>access-list-number</i>	Number of a MAC ACL to apply to an interface or subinterface (as specified by a access-list (MAC) command). This is a decimal number from 700 to 799.
	in	Filters on inbound packets.

Defaults No access list is applied to the interface or subinterface.

Command Modes Interface configuration
Subinterface configuration

Command History	Release	Modification
	12.0(32)S	This command was introduced on the Cisco 12000 series Internet router.

Usage Guidelines MAC ACLs are applied on incoming traffic on Gigabit Ethernet interfaces and VLAN subinterfaces. After receiving a packet, the Cisco IOS software checks the source MAC address of the Gigabit Ethernet, 802.1Q VLAN, or 802.1Q-in-Q packet against the access list. If the MAC access list permits the address, the software continues to process the packet. If the access list denies the address, the software discards the packet and returns an ICMP host unreachable message.

If the specified MAC access list does not exist on the interface or subinterface, all packets are passed.



Note

The **mac access-group** command is supported on a VLAN subinterface only if a VLAN is already configured on the subinterface.

Examples

The following example applies MAC ACL 101 on incoming traffic received on Gigabit Ethernet interface 0:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# mac access-group 101 in
```

Related Commands

Command	Description
access-list (MAC)	Defines a MAC access list.
clear mac access-list counters	Clears the counters of a MAC ACL.
show mac access-list	Displays the contents of one or all MAC ACLs.

show mac access-list

To display the contents and statistics of one or all MAC access lists (ACLs) on a router or specified line card, use the **show mac access-list** command in privileged EXEC or line-card configuration mode.

show mac access-list [*access-list-number*]

Syntax Description	<i>access-list-number</i> (Optional) Number of the MAC ACL to display. If you do not enter an access-list number, the contents of all MAC ACLs on the router or line card are displayed.
---------------------------	--

Defaults	The contents of all MAC ACLs are displayed.
-----------------	---

Command Modes	Privileged EXEC Line-card configuration
----------------------	--

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.0(32)S</td> <td>This command was introduced on the Cisco 12000 series Internet router.</td> </tr> </tbody> </table>	Release	Modification	12.0(32)S	This command was introduced on the Cisco 12000 series Internet router.
Release	Modification				
12.0(32)S	This command was introduced on the Cisco 12000 series Internet router.				

Usage Guidelines Use the **show mac access-list** command in privileged EXEC mode to display the contents and statistics for one or all MAC ACLs configured on a router or line card. To display information about the MAC ACLs configured on a specific line card, do one of the following:

- Use the **attach slot-number** command in privileged EXEC mode to connect to a line card. Then, from line-card configuration mode, enter the **show mac access-list** command. For example:

```
Router# attach 2
LC-SLot2# show mac access-list 101
```

- Use the **execute-on slot-number** command as a prefix to the **show mac access-list** command in privileged EXEC mode. For example:

```
Router# execute-on 2 show mac access-list 101
```

The **show mac access-list** command provides output identical to the **show access-lists** command, except that it is MAC ACL-specific and allows you to specify a particular MAC access list.

Examples

The following is sample output from the **show mac access-list** command for MAC ACL 701:

```
Router# show mac access-list 701

Standard MAC access list 701
 1 permit 0001.0001.0001 (44890496 matches)
 2 permit 0001.0001.0003 (44890500 matches)
 3 permit 0000.0000.eeee
 4 permit 0000.0000.ffff
 0 deny any (default) (44890509 matches)
Aggregated hardware matches: permit/deny 89780996/44890509
```

Related Commands

Command	Description
access-list (MAC)	Defines a MAC ACL.
clear mac access-list counters	Clears the counters for a MAC ACL.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CDDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2006 Cisco Systems, Inc. All rights reserved.