



Lock-and-Key Commands

This chapter describes lock-and-key commands. Lock-and-key security is a traffic filtering security feature that uses dynamic access lists. Lock-and-key is available for IP traffic only.

Refer to the *Command Reference Master Index* or search online to find complete descriptions of other commands used when configuring lock-and-key.

For lock-and-key configuration information, refer to the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the *Security Configuration Guide*.

access-enable

To enable the router to create a temporary access list entry in a dynamic access list, use the **access-enable** EXEC command.

access-enable [**host**] [**timeout** *minutes*]

Syntax Description

| | |
|-------------------------------|---|
| host | (Optional) Tells the software to enable access only for the host from which the Telnet session originated. If not specified, the software allows all hosts on the defined network to gain access. The dynamic access list contains the network mask to use for enabling the new network. |
| timeout <i>minutes</i> | (Optional) Specifies an idle timeout for the temporary access list entry. If the access list entry is not accessed within this period, it is automatically deleted and requires the user to authenticate again. The default is for the entries to remain permanently. We recommend that this value equal the idle timeout set for the WAN connection. |

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command enables the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the temporary access list entry will remain, even after the user terminates the session.

Use the **autocommand** command with the **access-enable** command to cause the **access-enable** command to execute when a user Telnets into the router.

Example

The following example causes the software to create a temporary access list entry and tells the software to enable access only for the host from which the Telnet session originated. If the access list entry is not accessed within 2 minutes, it is deleted.

```
autocommand access-enable host timeout 2
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (extended)
autocommand

access-template

To manually place a temporary access list entry on a router to which you are connected, use the **access-template EXEC** command.

access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*] [**timeout** *minutes*]

Syntax Description

| | |
|-------------------------------|--|
| <i>access-list-number</i> | Number of the dynamic access list. |
| <i>name</i> | Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists. |
| <i>dynamic-name</i> | (Optional) Name of a dynamic access list. |
| <i>source</i> | (Optional) Source address in a dynamic access list. The keywords host and any are allowed. All other attributes are inherited from the original access-list entry. |
| <i>destination</i> | (Optional) Destination address in a dynamic access list. The keywords host and any are allowed. All other attributes are inherited from the original access-list entry. |
| timeout <i>minutes</i> | (Optional) Specifies a maximum time limit for each entry within this dynamic list. This is an absolute time, from creation, that an entry can reside in the list. The default is an infinite time limit and allows an entry to remain permanently. |

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command provides a way to enable the lock-and-key access feature.

You should always define either an idle timeout (with the **timeout** keyword in this command) or an absolute timeout (with the **timeout** keyword in the **access-list** command). Otherwise, the dynamic access list will remain, even after the user has terminated the session.

Example

In the following example, the software enables IP access on incoming packets in which the source address is 172.29.1.129 and the destination address is 192.168.52.12. All other source and destination pairs are discarded.

```
access-template 101 payroll host 172.29.1.129 host 192.168.52.12 timeout 2
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (extended)

autocommand

clear access-template

clear access-template

To manually clear a temporary access list entry from a dynamic access list, use the **clear access-template EXEC** command.

clear access-template [*access-list-number* | *name*] [*dynamic-name*] [*source*] [*destination*]

Syntax Description

| | |
|---------------------------|--|
| <i>access-list-number</i> | (Optional) Number of the dynamic access list from which the entry is to be deleted. |
| <i>name</i> | Name of an IP access list from which the entry is to be deleted. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists. |
| <i>dynamic-name</i> | (Optional) Name of the dynamic access list from which the entry is to be deleted. |
| <i>source</i> | (Optional) Source address in a temporary access list entry to be deleted. |
| <i>destination</i> | (Optional) Destination address in a temporary access list entry to be deleted. |

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command is related to the lock-and-key access feature. It clears any temporary access list entries that match the parameters you define.

Example

The following example clears any temporary access list entries with a source of 172.20.1.12 from the dynamic access list named vendor:

```
clear access-template vendor 172.20.1.12
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (extended)

access-template

show ip accounting

To display the active accounting or checkpointed database or to display access-list violations, use the **show ip accounting** privileged EXEC command.

show ip accounting checkpoint [**output-packets** | **access-violations**]

Syntax Description

| | |
|--------------------------|--|
| checkpoint | (Optional) Indicates that the checkpointed database should be displayed. |
| output-packets | (Optional) Indicates that information pertaining to packets that passed access control and were successfully routed should be displayed. This is the default value if neither output-packets nor access-violations is specified. |
| access-violations | (Optional) Indicates that information pertaining to packets that failed access lists and were not routed should be displayed. |

Defaults

If neither the **output-packets** nor **access-violations** keyword is specified, **show ip accounting** displays information pertaining to packets that passed access control and were successfully routed.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

To use this command, you must first enable IP accounting on a per-interface basis.

Sample Displays

Following is sample output from the **show ip accounting** command:

```
Router# show ip accounting
```

| Source | Destination | Packets | Bytes |
|---------------|--------------|---------|---------|
| 172.30.19.40 | 172.30.67.20 | 7 | 306 |
| 172.30.13.55 | 172.30.67.20 | 67 | 2749 |
| 172.30.2.50 | 172.30.33.51 | 17 | 1111 |
| 172.30.2.50 | 172.30.2.1 | 5 | 319 |
| 172.30.2.50 | 172.30.1.2 | 463 | 30991 |
| 172.30.19.40 | 172.30.2.1 | 4 | 262 |
| 172.30.19.40 | 172.30.1.2 | 28 | 2552 |
| 172.30.20.2 | 172.30.6.100 | 39 | 2184 |
| 172.30.13.55 | 172.30.1.2 | 35 | 3020 |
| 172.30.19.40 | 172.30.33.51 | 1986 | 95091 |
| 172.30.2.50 | 172.30.67.20 | 233 | 14908 |
| 172.30.13.28 | 172.30.67.53 | 390 | 24817 |
| 172.30.13.55 | 172.30.33.51 | 214669 | 9806659 |
| 172.30.13.111 | 172.30.6.23 | 27739 | 1126607 |
| 172.30.13.44 | 172.30.33.51 | 35412 | 1523980 |
| 172.30.7.21 | 172.30.1.2 | 11 | 824 |
| 172.30.13.28 | 172.30.33.2 | 21 | 1762 |
| 172.30.2.166 | 172.30.7.130 | 797 | 141054 |
| 172.30.3.11 | 172.30.67.53 | 4 | 246 |
| 172.30.7.21 | 172.30.33.51 | 15696 | 695635 |
| 172.30.7.24 | 172.30.67.20 | 21 | 916 |
| 172.30.13.111 | 172.30.10.1 | 16 | 1137 |

Table 12 describes fields shown in the display.

Table 12 Show IP Accounting Field Descriptions

| Field | Description |
|-------------|---|
| Source | Source address of the packet. |
| Destination | Destination address of the packet. |
| Packets | Number of packets transmitted from the source address to the destination address. |
| Bytes | Number of bytes transmitted from the source address to the destination address. |

Following is sample output from the **show ip accounting access-violations** command. (The following displays information pertaining to packets that failed access lists and were not routed.)

```
Router# show ip accounting access-violations
```

| Source | Destination | Packets | Bytes | ACL |
|--------------|--------------|---------|-------|-----|
| 172.30.19.40 | 172.30.67.20 | 7 | 306 | 77 |
| 172.30.13.55 | 172.30.67.20 | 67 | 2749 | 185 |
| 172.30.2.50 | 172.30.33.51 | 17 | 1111 | 140 |
| 172.30.2.50 | 172.30.2.1 | 5 | 319 | 140 |
| 172.30.19.40 | 172.30.2.1 | 4 | 262 | 77 |

Accounting data age is 41

Table 13 describes fields shown in the display.

Table 13 Show IP Accounting Access-Violation Field Descriptions

| Field | Description |
|-------------|---|
| Source | Source address of the packet. |
| Destination | Destination address of the packet. |
| Packets | For accounting keyword, number of packets transmitted from the source address to the destination address. For access-violations keyword, number of packets transmitted from the source address to the destination address that violated the access control list. |
| Bytes | For accounting keyword, number of bytes transmitted from the source address to the destination address. For access-violations keyword, number of bytes transmitted from the source address to the destination address that violated the access control list. |
| ACL | Number of the access list of the last packet transmitted from the source to the destination that failed an access list. |

Related Commands

You can use the master indexes or search online to find documentation of related commands.

clear ip accounting

ip accounting

ip accounting-list

ip accounting-threshold

ip accounting-transits