



Configuring Network Security

This chapter contains network security information that is unique to the Catalyst 4006 switch with Supervisor Engine III. It also provides guidelines, procedures, and configuration examples.

This chapter consists of the following sections:

- [Hardware and Software ACL Support, page 16-1](#)
- [Guidelines and Restrictions for Using Layer 4 Operators in ACLs, page 16-2](#)

For network security information and procedures, refer to these publications:

- *Cisco IOS Security Configuration Guide*, Release 12.1, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/index.htm
- *Cisco IOS Security Command Reference*, Release 12.1, at http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_r/index.htm

By default, the Catalyst 4006 switch with Supervisor Engine III sends ICMP unreachable when a packet is denied by an access list; these packets are not dropped in hardware but are forwarded to the switch so that it can generate the ICMP-unreachable message.

To drop access-list denied packets in hardware on the input interface, you must disable ICMP unreachable using the **no ip unreachable** interface configuration command. The **ip unreachable** command is enabled by default, regardless of whether the **ip unreachable** command is enabled.

All packets denied by an output access list are always forwarded to the CPU.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference for the Catalyst 4006 Switch with Supervisor Engine III* and the publications at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>

Hardware and Software ACL Support

This section describes how to determine whether access control lists (ACLs) are processed in hardware or in software:

- Flows that match a *deny* statement in standard and extended ACLs (input and output) are dropped in hardware if ICMP unreachable are disabled.
- Flows that match a *permit* statement in standard and extended ACLs (input and output) are processed in hardware.

- The following ACL types are *not* supported in software:
 - Standard XNS access list
 - Extended XNS access list
 - DECnet access list
 - Extended MAC address access list
 - Protocol type-code access list
 - Standard IPX access list
 - Extended IPX access list

**Note**

Packets that require logging are processed in software. A copy of the packets is sent to the CPU for logging while the actual packets are forwarded in hardware so that nonlogged packet processing is not impacted.

**Note**

When you enter the **show ip access-list** command, the match count displayed is updated every 15 seconds.

Guidelines and Restrictions for Using Layer 4 Operators in ACLs

The following sections describe guidelines and restrictions when configuring ACLs that include Layer 4 port operations:

- [Determining Layer 4 Operation Usage, page 16-2](#)
- [How Access Control List Processing Impacts CPU, page 16-4](#)

Determining Layer 4 Operation Usage

You can specify these operate types, each of which uses one Layer 4 operation in the hardware:

- gt (greater than)
- lt (less than)
- neq (not equal)
- range (inclusive range)

We recommend that you do not specify more than six *different* operations on the same ACL. If you exceed this number, each new operation might cause the affected ACE (access list entry) to be processed in software.

Use the following two guidelines to determine Layer 4 operation usage:

1. Layer 4 operations are considered different if the operator or operand differ. For example, in the following ACL three different Layer 4 operations exist (*gt 10* and *gt 11* are considered two different Layer 4 operations):

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```

**Note**

The *eq* operators can be used an unlimited number of times as this operator does not use a Layer 4 operation in hardware.

2. Layer 4 operations are considered different if the same operator/operand couple applies once to a source port and once to a destination port, as in the following example:

```
... Src gt 10 ...
... Dst gt 10
```

A more detailed example follows:

```
access-list 101
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny

access-list 102
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

The Layer 4 operations usage of access lists 101 and 102 is as follows:

- Access list 101 Layer 4 operations: 5
 - *gt 10 permit* and *gt 10 deny* both use the same operation because they are identical and both operate on the destination port.
- Access list 102 Layer 4 operations: 4
- Total Layer 4 operations: 8 (due to sharing between the two access lists)
 - *neg6 permit* is shared between the two ACLs because they are identical and both operate on the same destination port.
- An explanation of the Layer 4 operations usage is as follows:
 - Layer 4 operation 1 stores *gt 10 permit* and *gt 10 deny* from ACL 101
 - Layer 4 operation 2 stores *lt 9 deny* from ACL 101
 - Layer 4 operation 3 stores *gt 11 deny* from ACL 101
 - Layer 4 operation 4 stores *neg 6 permit* from ACL 101 and 102
 - Layer 4 operation 5 stores *neg 6 deny* from ACL 101
 - Layer 4 operation 6 stores *gt 20 deny* from ACL 102
 - Layer 4 operation 7 stores *lt 9 deny* from ACL 102
 - Layer 4 operation 8 stores *range 11 13 deny* from ACL 102

How Access Control List Processing Impacts CPU

Access control list processing can potentially impact the CPU in two ways:

1. For some packets, access control list matches must be performed by the software when the hardware runs out of resources.
 - TCP flag combinations other than *rst ack* and *syn fin rst* are processed in software. *rst ack* is equivalent to the keyword **established**.
 - You can have up to six Layer 4 operations (*lt*, *gt*, *neq*, and *range*) in an ACL, in order for all operations to be processed in hardware. The *eq* operator does not require any Layer 4 operations and can be used any number of times. In addition, Layer 4 operations can be shared by source and destination operands as even-pairings only, if the total number of Layer 4 operations is six. You can set zero source and six destination operations or two source and four destination operations, but you cannot set three source and three destination operations if you want all six Layer 4 operations performed in hardware. If you use three source and three destination operations, the third access control entry will be handled in software.
 - If the total number of Layer 4 operations in an ACL is less than six, they can be distributed in any way you choose.
 - If the total number of Layer 4 operations in an ACL is greater than six, then the additional Layer 4 operations are processed in software

Examples:

The following access lists will be processed completely in hardware:

```
access-list 104 permit tcp any any established
access-list 105 permit tcp any any rst ack
access-list 107 permit tcp any synfin rst
```



Note Access-lists 104 and 105 are identical; *established* is a shorthand for *rst* and *ack*.

Access list 101 below will be processed completely in software:

```
access-list 101 permit tcp any any urg
```

Because 4 source and 2 destination operations exist, access list 106 below will be processed in hardware:

```
access-list 106 permit tcp any range 100 120 any range 120 140
access-list 106 permit tcp any range 140 160 any range 180 200
access-list 106 permit tcp any range 200 220
access-list 106 deny tcp any range 220 240
```

In the following code, the first two access lists in access list 102 will be processed in hardware. The third access list will be processed in software, because three source and three destination operations exist.

```
access-list 102 permit tcp any lt 80 any gt 100
access-list 102 permit tcp any range 100 120 any range 120 1024
access-list 102 permit tcp any gt 1024 any lt 1023
```

Similarly, for access list 103 below, the third ACE will be processed in software. (Although the operations for source and destination ports look similar, they are considered different Layer 4 operations.)

```
access-list 103 permit tcp any lt 80 any lt 80
access-list 103 permit tcp any range 100 120 any range 100 120
access-list 103 permit tcp any gt 1024 any gt 1023
```



Note *source port lt 80 and destination port lt 80* are considered different operations.

2. Some packets must be sent to the CPU for accounting purposes, but the action is still performed by the hardware. For example, if a packet must be logged, a copy is sent to the CPU for logging, but the forwarding (or dropping) is performed in the hardware. Although logging slows the CPU, it does not affect the forwarding rate. This scenario would happen when:
 - a log keyword is used
 - an output acl denies a packet
 - an input acl denies a packet, and on the interface where the acl is applied, *ip unreachable* is enabled. (*ip unreachable* is enabled by default on all the interfaces.)

