

Configuring ACLs on the WS–X4232–L3 Router Module for the Catalyst 4000 Family

Document ID: 30112

Interactive This document offers customized analysis of your Cisco device.

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions
- Background Theory
- Access Control List Restrictions
- Data–plane Access Control List

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Procedure
- Incorrect Traffic Is Denied
- TCAM Size

Related Information

Introduction

This document describes Access Control List (ACL) support on the WS–X4232–L3 router module for Catalyst 4003 and 4006 switches. Included is a description of the architecture and a sample configuration that employs ACLs in order to restrict data traffic between separate VLANs.

For information on how to configure the router module to route all traffic without the application of ACLs, refer to Configuration and Overview of the Router Module for the Catalyst 4000 Family (WS–X4232–L3).

For additional information on how to install and configure the router module, refer to Installation and Configuration Note for the Catalyst 4000 Layer 3 Services Module.

Prerequisites

Requirements

The router module is supported on the Catalyst 4003 with Supervisor I, and the Catalyst 4006 with Supervisor II. The software requirements for the Catalyst 4003 and 4006 switches in order to support the WS–X4232–L3 module are as follows:

- The Catalyst 4003 Supervisor Engine I (WS–X4012) requires Cisco Catalyst Software Version 5.5(1) or later.

- The Catalyst 4006 Supervisor Engine II (WS-X4013) requires Cisco Catalyst Software Version 5.5(1) or later.
- The Catalyst 4000 Layer 3 Services module requires Cisco IOS® Software Release 12.0(10)W5(18f) or later.

Components Used

The information in this document is based on these software and hardware versions:

- Two Catalyst 4003 switches running Catalyst OS 6.3(10)
- Two WS-X4232-L3 switch routers running Cisco IOS® Software Release 12.0(18)W5(22b)

For an architecture overview of the WS-X4232-L3 router module, refer to the "WS-X4232-L3 Architecture Overview" section of Configuration and Overview of the Router Module for the Catalyst 4500/4000 Family (WS-X4232-L3).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Background Theory

ACLs allow you to restrict network use by certain users or devices. Packet flow can be controlled into or out of the interfaces with the application of ACLs to the WS-X4232-L3 module's gigabit interfaces. ACLs can be configured for all routed network protocols, such as IP or Internetwork Packet Exchange (IPX) in order to filter packets, as packets pass through the CPU or are routed through the WS-X4232-L3 hardware.

Both control-plane and data-plane ACLs are supported. Control-plane ACLs are used to filter data that is processed by the CPU of the router module. Some examples of control-plane traffic are distribution of routing information, Internet Group Management Protocol (IGMP) joins, and IPX Service Advertising Protocols (SAPs) and Get Nearest Server (GNS) packets. Data-plane ACLs are used to filter user data that is routed by hardware in the router module. Examples of these include denying TCP sessions between two hosts, and controlling access to devices in an IPX network. These ACLs are applied to an interface in the input or output direction with the **ip access-group** or **ipx access-group** command.

ACLs are created and applied to an interface for either inbound or outbound traffic. Only one ACL filter can be applied per direction, per protocol, per (sub)interface. When the router receives the data, the router decides whether to forward or block each packet. The router processes each packet based on whether or not the packet matches the criteria in the list. Packets that do not match criteria in your list are automatically blocked by the implicit "deny all traffic" criteria statement at the end of every ACL.

For details on the software features that are supported on the WS-X4232-L3 router module, refer to the Features section of the Installation and Configuration Note for the Catalyst 4000 Layer 3 Services Module.

Access Control List Restrictions

These restrictions apply when you configure ACLs on the Catalyst 4000 Layer 3 Services module:

- ACLs are supported only on Gigabit Ethernet ports and corresponding Gigabit Ethernet subinterfaces.
- ACLs are not supported on Bridge-Group Virtual Interface (BVI), Fast EtherChannel (FEC), Gigabit EtherChannel (GEC), or Fast Ethernet interfaces.
- Reflexive and dynamic ACLs are not supported.
- Access violations accounting is not supported.
- ACL logging is supported only for permitted packets headed to the CPU. Although control-plane ACLs are processed by the CPU, only the permitted packets are sent to the CPU. ACLs program a deny in the hardware before the ACLs reach the CPU and therefore cannot be logged.
- ACL logging is not supported for switched packets.
- Standard, Extended, and Named styles are supported ACLs for IP.

Data-plane Access Control List

This document focuses on the data-plane ACLs. This list describes how the restrictions apply directly to data-plane ACLs on the WS-X4232-L3:

- Data-plane ACLs are supported only on Gigabit Ethernet ports and corresponding Gigabit Ethernet subinterfaces.
- Data-plane ACLs are **not** supported on GEC interfaces.
- Data-plane ACLs are not supported on GEC subinterfaces.
- ACL logging is not supported on switched packets which are not processed by the CPU.
- ACL logging for permitted packets, ACL hit counters, and access-violations accounting are not supported.

The standard configuration used for the WS-4243-L3 module is to configure a GEC on the gigabit interfaces connected to the backplane. For information on this type of configuration, refer to Configuration and Overview of the Router Module for the Catalyst 4000 Family (WS-X4232-L3). However, as stated previously, ACLs are not supported on GEC interfaces or GEC subinterfaces. Although the parser allows you to configure an ACL on the portchannel, keep in mind this is not a supported configuration and does not filter traffic.

The only supported configuration is to configure the data-plane ACLs on the Gigabit Ethernet port and their corresponding Gigabit Ethernet subinterfaces. Therefore the only option is to configure each internal gigabit interface as a separate 802.1q trunk or as Layer 2 ports.

When you configure each gigabit interface as an 802.1q trunk, subinterfaces are added. This occurs because trunks are configured on the subinterfaces, and the subinterfaces determine which VLANs are allowed on each trunk link. VLAN control is now possible because data-plane ACLs can be applied to the subinterfaces of a the main interface, as the example here shows:

Note: Only 802.1q encapsulation is supported on the Catalyst 4003 and 4006 with Supervisor Engine I and II respectively.

```
interface GigabitEthernet3
  no ip redirects
  no ip directed-broadcast
  no negotiation auto
  !

!--- Subinterface for VLAN 10.

interface GigabitEthernet3.10

!--- Trunk configuration for 802.1q encapsulation for VLAN 10.
```

```

encapsulation dot1q 10

!--- IP address for VLAN 10.

ip address 192.168.10.1 255.255.255.0

!--- ACL applied to filter all inbound traffic based on the criteria in
!--- ACL 101.

ip access-group 101 in
!

!--- Subinterface for VLAN 20.

interface GigabitEthernet3.20

!--- Trunk configuration for 802.1q encapsulation for VLAN 20.

encapsulation dot1q 20

!--- IP address for VLAN 20.

ip address 192.168.20.1 255.255.255.0

!--- ACL applied to filter all inbound traffic based on the criteria in
!--- ACL 101.

ip access-group 101 in
!

```

If your network consists of only two VLANs, you can configure each Gigabit Ethernet interface as a separate VLAN. VLAN control is now possible because data-plane ACLs can be applied to each gigabit interface, as shown in this example.

```

interface GigabitEthernet3

!--- VLAN 1 IP address.

ip address 172.22.53.1 255.255.255.0

!--- ACL applied to the interface blocks inbound traffic destined for VLAN 10.
!--- ACL applied to filter all inbound traffic based on the criteria in ACL 101.

ip access-group 101 in
no ip redirects
no ip directed-broadcast
no negotiation auto
!
interface GigabitEthernet4

!--- VLAN 10 IP address.

ip address 192.168.1.1 255.255.255.0

!--- ACL applied to the interface blocks inbound traffic destined for VLAN 1.
!--- ACL applied to filter all inbound traffic based on the criteria in ACL 101.

ip access-group 102 in
no ip redirects
no ip directed-broadcast
no negotiation auto

```

Configure

In this section, you are presented with the sample configuration of a simple network that uses data-plane ACLs on the WS-X4232-L3 module to restrict traffic between two separate VLANs. The sample configuration applies the ACLs on the backplane gigabit interfaces (Gigabit Ethernet 3 and 4) to restrict data traffic between separate VLANs. The gigabit interfaces (Gigabit Ethernet 1 and 2) on the front panel are Layer 3 interfaces and are configured the same as any router interface. Therefore, ACL configurations on these ports is not covered.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

In this configuration, these factors are applied to the switches:

- 802.1q trunking between two Catalyst switches is connected with Fast Ethernet Links.
- IP addresses are assigned to the switches for management only.
- VLAN Trunk Protocol (VTP) modes are set on the switches.
- Second VLAN (VLAN 10) is added on the switches; ports are added on those VLANs.
- Spanning-tree portfast is enabled on the ports, where workstations are connected. According to the topology, spanning-tree portfast is enabled on ports 2/4 on both switches.
- Default gateway has been configured.

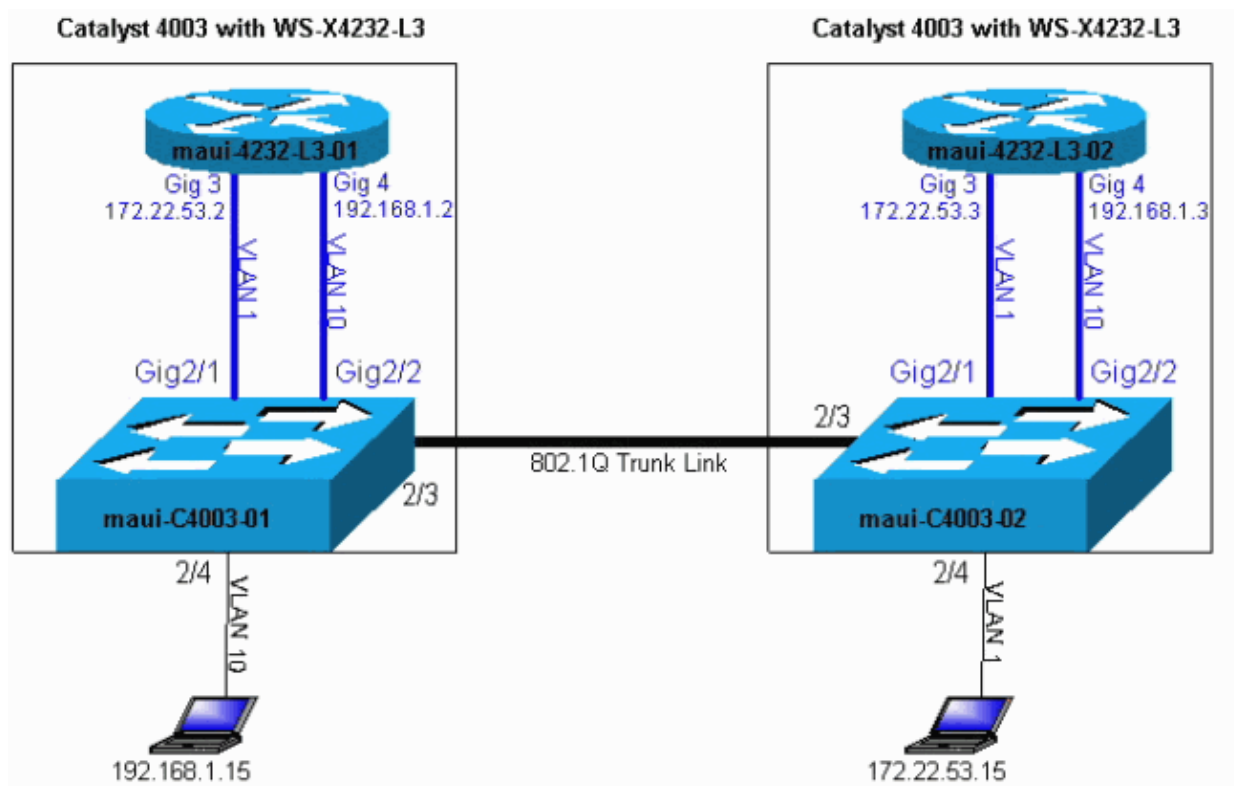
In this configuration, these factors are applied to the WS-X4232-L3 router:

- IP addresses have been assigned to the internal Gigabit Ethernet interfaces.
- Extended ACLs have been configured to restrict data traffic between the default VLAN 1 and the second VLAN 10.
- ACLs have been assigned to the internal Gigabit Ethernet interfaces.

Network Diagram

This document uses the network setup shown in this diagram:

ACLs have been assigned to the internal Gigabit Ethernet interfaces.



Configurations

This document uses the configurations shown here:

- maui-C4003-01 (Cisco Catalyst 4003)
- maui-4232-L3-01 (Cisco WS-X232-L3 Router)
- maui-C4003-02 (Cisco Catalyst 4003)
- maui-4232-L3-02 (Cisco WS-X232-L3 Router)

```

maui-C4003-01 (Cisco Catalyst 4003)
begin
!
#
***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Nov 25 2002, 09:14:34
!
#version 6.3(10)
!
!
#system web interface version(s)set prompt maui-C4003-01
!
#test
!
#frame distribution methodset port channel all distribution mac both
!
#vtp
set vtp domain maui
set vlan 1 name default type ethernet mtu 1500 said 10001 state active
set vlan 10 name VLAN0010 type ethernet mtu 1500 said 100010 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active

```

```

set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state active
  stp ieee
set vlan 1005 name trnet-default type trbrf mtu 1500 said 101005 state active
  stp ibm
set vlan 1003 name token-ring-default type trcrf mtu 1500 said 101003 state active
  mode srb aremaxhop 0 stemaxhop 0 backupcrf off
!
#ip

!--- Assign an IP address to the sc0 interface with the
!--- set interface sc0 <vlan> <ip_addr>/ <netmask><broadcast>
!--- command.

set interface sc0 1 172.22.53.5/255.255.255.0 172.22.53.255
set interface sl0 downset interface me1 down

!--- Assign the default gateway with the set ip route default <gateway>
!--- command.
The default gateway is the Gigabit Ethernet 3 interface (VLAN 1 interface) on the
!--- maui-4232-L3-01.

set ip route 0.0.0.0/0.0.0.0 172.22.53.2
!
#spantree
#vlan <VlanId>
!
#set boot command
set boot config-register 0x2102
set boot system flash bootflash:cat4000.6-3-10.bin
!
#module 1 : 0-port Switching Supervisor
!
#module 2 : 34-port Router Switch Card
!

!--- Ports assigned to VLAN 10.
!--- Port 2/2 is the internal gigabit port that connects to the backplane.
!--- Note that port 2/1 does not appear, this is because it is assigned
!--- to VLAN 1 by default.

set vlan 10 2/2,2/4
set port speed 2/3,2/5 100
set port duplex 2/3,2/5 full

!--- Enabling portfast for PC interface.

set spantree portfast    2/4 enable

!--- 802.1q trunk link which passes VLAN 1 and VLAN 10 traffic between
!--- switches.

set trunk 2/3 desirable dot1q 1-1005
!
#module 3 empty
end

```

maui-4232-L3-01 (Cisco WS-X232-L3 Router)

```

maui-4232-L3-01# show run
Building configuration...
Current configuration:
!
version 12.0

```

```

no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname maui-4232-L3-01
!
!
ip subnet-zero
no ip domain-lookup
!
!
!
interface FastEthernet1
  no ip address
  no ip directed-broadcast
  shutdown
!
interface GigabitEthernet1
  no ip address
  no ip directed-broadcast
  shutdown
!
interface GigabitEthernet2
  no ip address
  no ip directed-broadcast
  shutdown
!
interface GigabitEthernet3

!--- VLAN 1 IP address.

ip address 172.22.53.2 255.255.255.0

!--- ACL applied to the interface blocks inbound traffic destined for VLAN 10.

ip access-group 101 in
  no ip redirects
  no ip directed-broadcast
  no negotiation auto

!--- Hot Standby Router Protocol (HSRP) is not required for this configuration, but
!--- is commonly used in this topology. For additional information on HSRP, refer to
!--- Avoiding HSRP Instability in a Switching Environment with Various Router Platforms.
!--- The standby priority command specifies the priority for the HSRP interface.
!--- Increase the priority of at least one interface in the HSRP group to a value greater
!--- than the default (the default is 100).
!--- The interface with the highest priority becomes active for that HSRP group.

  standby priority 110 preempt

!--- The standby ip command enables HSRP and specifies the
!--- group and the HSRP IP address.
!--- If you do not specify a group-number, group 0 is used.

  standby 1 ip 172.22.53.1
!
interface GigabitEthernet4

!--- VLAN 2 IP address.

ip address 192.168.1.2 255.255.255.0

!--- ACL applied to the interface blocks inbound traffic destined for VLAN 1.

```

```

ip access-group 102 in
  no ip redirects
  no ip directed-broadcast
  no negotiation auto

!--- The standby priority command specifies the priority for the HSRP interface.

standby priority 100 preempt

!--- The standby ip command enables HSRP and specifies the group and the HSRP
!--- IP address.

standby 1 ip 192.168.1.1
!
ip classless
!

!--- The access-list 101 command does not allow any device on 172.22.53.0 network (VLAN 1)
!--- to send any IP traffic to any device on the 192.168.1.0 network (VLAN 10).

access-list 101 deny ip 172.22.53.0 0.0.0.255 192.168.1.0 0.0.0.255

!--- Allows all other IP traffic to pass.

access-list 101 permit ip any any

!--- The access-list 102 command does not allow any device on 192.168.1.0 network (VLAN 10)
!--- to send IP traffic to any device on the 172.22.53.0 network (VLAN 1).

access-list 102 deny ip 192.168.1.0 0.0.0.255 172.22.53.0 0.0.0.255

!--- Allows all other IP traffic to pass.

access-list 102 permit ip any any
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

```

maui-C4003-02 (Cisco Catalyst 4003)

```

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#time: Mon Nov 25 2002, 09:39:47
!
#version 6.3(10)
!
!
#system web interface version(s)
set prompt maui-C4003-02
!
#test
!
#frame distribution method
set port channel all distribution mac both

```

```

!
#vtp
set vtp domain maui
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 10 name VLAN0010 type ethernet mtu 1500 said 100010 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state active
  stp ieee
set vlan 1005 name trnet-default type trbrf mtu 1500 said 101005 state active
  stp ibm
set vlan 1003 name token-ring-default type trcrf mtu 1500 said 101003 state active
  mode srb aremaxhop 0 stemaxhop 0 backupcrf off
!
#ip

!--- Assign an IP address to the sc0 interface with the
!--- set interface sc0 <vlan> <ip_addr>/<netmask> <broadcast> !--- command.

set interface sc0 1 172.22.53.6/255.255.255.0 172.22.53.255

set interface sl0 down
set interface me1 down

!--- Assign the default gateway with the set ip route default <gateway>
!--- command.
The default gateway is Gigabit Ethernet 3 interface (VLAN 1 interface) on the
!--- maui-4232-L3-02.

set ip route 0.0.0.0/0.0.0.0 172.22.53.3
!
#spantree
#vlan <VlanId>
!
#syslog
set logging level cops 2 default
!
#set boot command
set boot config-register 0x2102
set boot system flash bootflash:cat4000.6-3-10.bin
!
#module 1 : 0-port Switching Supervisor
!
#module 2 : 34-port Router Switch Card

!--- Port assigned to VLAN 10.
!--- Port 2/2 is the internal gigabit port that connects to the backplane.

!--- Note that port 2/1 does not appear here. This is because this port is assigned to VLAN 1 by

set vlan 10 2/2
set port speed 2/3-4 100
set port duplex 2/3-4 full

!--- Enabling portfast for PC interface.

set spantree portfast      2/4 enable

!--- 802.1q trunk link, which passes VLAN 1 and VLAN 10 traffic between switches.

set trunk 2/3 desirable dot1q 1-1005
!
#module 3 empty
end

```

```
maui-4232-L3-02# show run
Building configuration...
Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname maui-4232-L3-02
!
!
ip subnet-zero
no ip domain-lookup
!
!
!
interface FastEthernet1
  no ip address
  no ip directed-broadcast
  shutdown
!
interface GigabitEthernet1
  no ip address
  no ip directed-broadcast
  shutdown
!
interface GigabitEthernet2
  no ip address
  no ip directed-broadcast
  shutdown
!
interface GigabitEthernet3

!--- VLAN 1 IP address.

ip address 172.22.53.3 255.255.255.0

!--- ACL applied to the interface blocks inbound traffic destined for VLAN 10.

ip access-group 101 in
  no ip redirects
  no ip directed-broadcast
  no negotiation auto

!--- The standby priority command specifies the priority for the HSRP interface.

  standby priority 100 preempt

!--- The standby ip command enables HSRP and specifies the group and the HSRP IP address.

  standby 1 ip 172.22.53.1
!
interface GigabitEthernet4

!--- VLAN 10 IP address.

ip address 192.168.1.2 255.255.255.0

!--- ACL applied to the interface blocks inbound traffic destined for VLAN 1.
```

```

ip access-group 102 in
  no ip redirects
  no ip directed-broadcast
  no negotiation auto

!--- The standby priority command specifies the priority for the HSRP interface.

  standby priority 110 preempt

!--- The standby ip command enables HSRP and specifies the group and the HSRP
!--- IP address.

  standby 1 ip 192.168.1.1
!
ip classless
!

!--- The access-list 101 command does not allow any device on the 172.22.53.0 network (VLAN 1)
!--- to send IP traffic to any device on the 192.168.1.0 network (VLAN 10).

access-list 101 deny ip 172.22.53.0 0.0.0.255 192.168.1.0 0.0.0.255

!--- Allows all other IP traffic to pass.

access-list 101 permit ip any any

!--- The access-list 102 command does not allow any device on the 192.168.1.0 network (VLAN 10)
!--- to send traffic to any device on the 172.22.53.0 network (VLAN 1).

access-list 102 deny ip 192.168.1.0 0.0.0.255 172.22.53.0 0.0.0.255

!--- Allows all other IP traffic to pass.

access-list 102 permit ip any any
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end

```

Verify

This section provides information you can use to confirm your configuration works properly.

Since the focus of this document is on the ACL configuration, this document does not cover the verification of the ethernet trunk between the switches. For more information on trunking, refer to [Trunking Between Catalyst 4000, 5000, and 6000 Family Switches Using 802.1q Encapsulation](#)

If you have the output of a **show trunk** command from your Cisco device, you can use to display potential issues and fixes. To use, you must be a registered customer, be logged in, and have JavaScript enabled.

You can use Output Interpreter to display potential issues and fixes. To use Output Interpreter, you must be a registered customer, be logged in, and have JavaScript enabled.

To verify that the ACLs are configured correctly, first view the ACL configuration with the **show ip**

access-list command.

```
maui-4232-L3-01#show ip access-lists
Extended IP access list 101
  deny ip 172.22.53.0 0.0.0.255 192.168.1.0 0.0.0.255
  permit ip any any
Extended IP access list 102
  deny ip 192.168.1.0 0.0.0.255 172.22.53.0 0.0.0.255
  permit ip any any
maui-4232-L3-01#
```

Since the ACL configuration on both of the switches is identical, maui-c4003-01 and maui-4232-L3-01 are used to verify if the ACL currently permits or denies traffic correctly.

To do this, perform a simple ping test from the PC (connected to port 2/4) to the maui-4232-L3-01 internal gigabit interfaces. Since this PC is in VLAN 10, the default gateway should be 192.168.1.1. According to the ACLs that have been defined, traffic that comes from this PC must be blocked when you try to ping any device on VLAN 1 (172.22.53.0), but you must be able to ping any device on VLAN 10 (192.168.1.0).

This output shows the ping test from PC (192.168.1.15) to Gigabit Ethernet 4 (192.168.1.1):

```
O:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
O:\>
```

The **show ip access-lists** command provides a packet count that shows which ACL entry is being hit. Issue another **show ip access-list** command in order to see that the ACL counters have incremented, and thus see that the ACL permits the traffic, as shown in the output here:

```
maui-4232-L3-01#show ip access-lists
Extended IP access list 101
  deny ip 172.22.53.0 0.0.0.255 192.168.1.0 0.0.0.255
  permit ip any any
Extended IP access list 102
  deny ip 192.168.1.0 0.0.0.255 172.22.53.0 0.0.0.255
  permit ip any any (5 matches)
maui-4232-L3-01#
```

This output shows the ping test from PC (192.168.1.15) to Gigabit Ethernet 3 (172.22.53.1):

```
O:\>ping 172.22.53.1
Pinging 172.22.53.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.22.53.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
O:\>
```

Issue another **show ip access-list** command to see that the counter has incremented for the traffic that was denied by the ACL, as seen in the output here:

```
maui-4232-L3-01#show ip access-lists
Extended IP access list 101
  deny ip 172.22.53.0 0.0.0.255 192.168.1.0 0.0.0.255
  permit ip any any
Extended IP access list 102
  deny ip 192.168.1.0 0.0.0.255 172.22.53.0 0.0.0.255 (5 matches)
  permit ip any any (5 matches)
maui-4232-L3-01#
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Procedure

These steps explain the debug process. First verify that there are no ACLs currently applied.

Note: Use extreme caution when you debug a system with heavy traffic. ACLs can be used to debug specific traffic, but you must understand the processes and the traffic flow to do so. It is always recommended to turn off logging and to issue the **syslog** or the **show logging** command in a live production network.

1. Configure the ACL to apply to your network. The example provided uses the ACLs from the configuration in this document.
2. Begin the debug process with the **debug ip packet 101 detail** command.

This is the **debug** output of a ping that was issued from the PC (192.168.1.15) to the Gigabit Ethernet 3 interface (172.22.53.1) on the router. You can see from output that the traffic destined for 172.22.53.0 network from the 192.168.1.0 network is denied, and the traffic from the 192.168.1.0 to the 192.168.1.0 network is sent.

```
!--- Traffic destined for a device on a different VLAN is denied.
```

```
04:16:23: IP: s=192.168.1.15 (GigabitEthernet4), d=172.22.53.1, len 100, access
denied
04:16:23:      ICMP type=8, code=0
04:16:23:
04:16:23: IP: s=192.168.1.1 (local), d=192.168.1.15 (GigabitEthernet4), len 56,
sending
04:16:23:      ICMP type=3, code=13
04:16:23:
04:16:23: IP: s=192.168.1.15 (GigabitEthernet4), d=172.22.53.1, len 100, access
denied
04:16:23:      ICMP type=8, code=0
04:16:23:04:16:25: IP: s=192.168.1.15 (GigabitEthernet4), d=172.22.53.1, len 100, ac
denied
04:16:25:      ICMP type=8, code=0
```

```
!--- Traffic destined for the same VLAN is sent.
```

```
04:16:25:04:16:25: IP: s=192.168.1.1 (local), d=192.168.1.15 (GigabitEthernet4), len
sending
04:16:25:      ICMP type=3, code=13
04:16:25:
04:16:25: IP: s=192.168.1.15 (GigabitEthernet4), d=172.22.53.1, len 100, access
```

```

denied
04:16:25:      ICMP type=8, code=0
04:16:25:04:16:27: IP: s=192.168.1.15 (GigabitEthernet4), d=172.22.53.1, len 100, ac
denied
04:16:27:      ICMP type=8, code=0
04:16:27:
04:16:27: IP: s=192.168.1.1 (local), d=192.168.1.15 (GigabitEthernet4), len 56,
sending
04:16:27:      ICMP type=3, code=13
04:16:27:

```

3. To stop the debug output, issue the **no debug all** command in enable mode or issue the **un all** shortcut command to disable multiple debugs.

Incorrect Traffic Is Denied

If the desired traffic is denied, the ACL configuration may be too specific. Try to add a broader access-list in addition to the one that is already configured. This helps determine if the specific ACL is blocking traffic that is supposed to be allowed to pass. Issue the **show ip access-lists** command to see which ACL entry is being hit by the traffic. This can be determine this if you look at the individual counter for each entry.

Note: The **log** keywords which can be appended to the ACL entries for ACL logging, ACL hit counters, and access-violations accounting are not supported on the WS-X4232-L3.

For additional information on configuring access-list on the WS-X4232-L3 module refer to Configuring Access Control Lists in the Installation and Configuration Note for the Catalyst 4000 Layer 3 Services Module document.

TCAM Size

Before you configure the access-list region in Ternary Content Addressable Memory (TCAM), make sure that TCAM has enough space to accommodate the access-list region. You can change the ACL TCAM size when you use Switching Database Manager (SDM) commands. If you plan to support bigger ACLs, you must reclaim TCAM space from other areas, such as IPX, IP, or bridging. The enhanced Gigabit Ethernet interface module supports TCAM sizes of 32K (32-bit) entries. The combined size of the protocol regions and access lists must not exceed your TCAM space. The default size of the ACL in a 32K TCAM is 512 (128-bit) entries.

If you receive this error message, you need to increase the TCAM space with the SDM command.

```

Warning:Programming TCAM entries failed
Please remove last ACL command to re-activate ACL operation.
!<ACL number or name> <IP or IPX> <INPUT_ACL or OUTPUT_ACL> from TCAM group for !<interf
Please see the documentation to see how TCAM space can be increased on this platform to

```

For more information on how to configure the TCAM space with the SDM command, refer to Configuring the Switching Database Manager.

Related Information

- [Catalyst 4000 Family Release Notes](#)
- [Release Notes for Catalyst 4000 Family Layer 3 Services Module Cisco IOS Release 12.0W5](#)
- [Installation and Configuration Note for the Catalyst 4000 Layer 3 Services Module](#)
- [Configuration and Overview of the Router Module for the Catalyst 4000 Family \(WS-X4232-L3\)](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 15, 2007

Document ID: 30112
