

Contents

Introduction	1
Prerequisites	1
Example: Filtering packets by MAC address	1
Network configuration	1
Analysis	1
Applicable hardware and software versions.....	2
Procedures	4
Verifying the configuration	4
Configuration files	5
Example: Controlling FTP access	5
Network configuration	5
Analysis	5
Applicable hardware and software versions.....	6
Procedures	8
Verifying the configuration	8
Configuration files	9
Example: Filtering packets by IP address	10
Network configuration	10
Analysis	10
Applicable hardware and software versions.....	11
Restrictions and guidelines	13
Procedures	13
Denying the Administration department to access the R&D department	13
Configuring access control for the R&D department	13
Verifying the configuration	14
Configuration files	15
Example: Filtering TCP packets.....	15
Network configuration	15
Analysis	16
Applicable hardware and software versions.....	16
Procedures	19
Configuring access control for the Administration department	19
Configuring access control for the R&D department	19
Verifying the configuration	19
Configuration files	20
Example: Filtering HTTP packets by using a user-defined ACL	21
Network configuration	21
Applicable hardware and software versions.....	21
Procedures	23
Verifying the configuration	23
Configuration files	24

Introduction

This document provides ACL configuration examples.

Prerequisites

This document is not restricted to specific software or hardware versions.

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

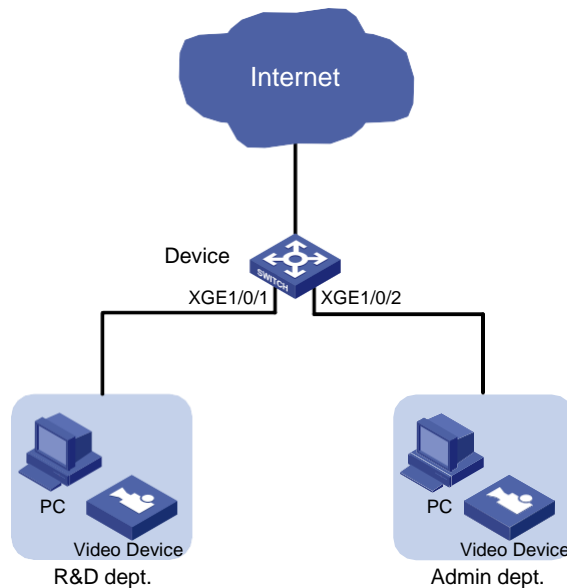
This document assumes that you have basic knowledge of ACL.

Example: Filtering packets by MAC address

Network configuration

As shown in [Figure 1](#), the R&D department and the Administration department have video devices deployed. The video devices use MAC addresses prefixed with 000f-e2. Configure packet filtering on the device to allow outgoing video data to pass through only from 8:30 to 18:00 every day.

Figure 1 Network diagram



Analysis

Because the MAC addresses of the video devices are fixed, you can use an Ethernet frame header ACL to filter packets by MAC address. In the ACL, specify a MAC address and a mask to match the MAC addresses that have the same prefix.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- SC 3130 series.

Procedures

Create a time range **time1** for the time range from 8:30 to 18:00 every day.

```
<Device> system-view
[Device] time-range time1 8:30 to 18:00 daily
```

Configure Ethernet frame header ACL 4000 to allow packets with source MAC addresses prefixed with 000f-e2 to pass through only during **time1**.

```
[Device] acl mac 4000
[Device-acl-mac-4000] rule permit source-mac 000f-e200-0000 ffff-ff00-0000 time-range time1
[Device-acl-mac-4000] rule deny source-mac 000f-e200-0000 ffff-ff00-0000
[Device-acl-mac-4000] quit
```

Apply ACL 4000 to filter incoming packets on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] packet-filter mac 4000 inbound
[Device-GigabitEthernet1/0/1] quit
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] packet-filter mac 4000 inbound
[Device-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify that the ACL is successfully applied for packet filtering.

```
[Device] display packet-filter interface inbound
Interface: GigabitEthernet1/0/1
Inbound policy:
MAC ACL 4000
Interface: GigabitEthernet1/0/2
Inbound policy:
MAC ACL 4000
```

Verify that the video devices can communicate with the external network during the time range **time1**. (Details not shown.)

Verify that the video devices cannot communicate with the external network beyond the time range **time1**. (Details not shown.)

Configuration files

```
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  packet-filter mac 4000 inbound
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  packet-filter mac 4000 inbound
#
time-range time1 08:30 to 18:00 daily
#
acl mac 4000
  rule 0 permit source-mac 000f-e200-0000 ffff-ff00-0000 time-range time1
  rule 5 deny source-mac 000f-e200-0000 ffff-ff00-0000
```

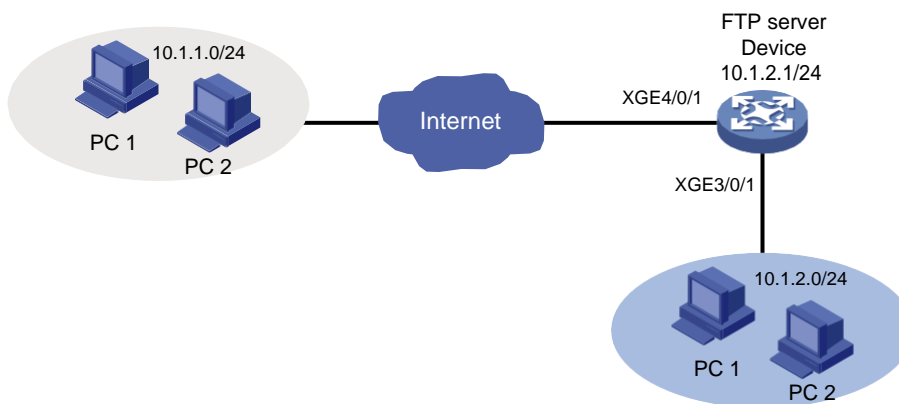
Example: Controlling FTP access

Network configuration

As shown in [Figure 2](#), the device is an FTP server. Configure FTP access control on the device to meet the following requirements:

- Users on subnet 10.1.2.0/24 can access the FTP server at any time.
- Users on subnet 10.1.1.0/24 can access the FTP server during working hours (8:30 to 18:00) on working days (Monday to Friday).
- Qualified users are assigned the level-15 user role.

Figure 2 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- Configure two rules for the ACL. One rule permits packets from subnet 10.1.2.0/24. The other one permits packets from subnet 10.1.1.0/24 and takes effect only during working hours on working days.
- Use the ACL to control access to the FTP server.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

Procedures

```
# Configure the time range ftp for working hours 8:30 to 18:00 from Monday to Friday.
<Device> system-view
[Device] time-range ftp 8:30 to 18:00 working-day

# Create IPv4 basic ACL 2000.
[Device] acl basic 2000

# Configure a rule to permit packets from subnet 10.1.2.0/24.
[Device-acl-ipv4-basic-2000] rule permit source 10.1.2.0 0.0.0.255

# Configure a rule to permit packets from subnet 10.1.1.0/24 during the time range ftp.
[Device-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255 time-range ftp
[Device-acl-ipv4-basic-2000] quit

# Enable FTP server on the device.
[Device] ftp server enable

# Add a local user named ftp and authorize this user to use the FTP service.
[Device] local-user ftp
[Device-luser-manage-ftp] service-type ftp

# Configure a password for the local user.
[Device-luser-manage-ftp] password simple 123456abcd

# Assign the level-15 user role to the local user.
[Device-luser-manage-ftp] authorization-attribute user-role level-15
[Device-luser-manage-ftp] quit

# Use the ACL 2000 to control access to the FTP server.
[Device] ftp server acl 2000
```

Verifying the configuration

Verify that you can use the host at 10.1.2.100 to log in to the FTP server during working hours on working days.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.
```

Verify that you can use the host at 10.1.1.100 to log in to the FTP server during working hours on working days.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\>ftp 10.1.2.1
```

```

Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.

# Verify that you can use the host at 10.1.2.100 to log in to the FTP server outside working hours.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ftp 10.1.2.1
Connected to 10.1.2.1.
220 FTP service ready.
User (10.1.2.1:(none)): ftp
331 Password required for ftp.
Password:
230 User logged in.

# Verify that you cannot use the host at 10.1.1.100 to log in to the FTP server outside working hours.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ftp 10.1.2.1
ftp>
ftp> ls
Not connected.

```

Configuration files

```

#
time-range ftp 08:30 to 18:00 working-day
#
acl basic 2000
rule 0 permit source 10.1.2.0 0.0.0.255
rule 5 permit source 10.1.1.0 0.0.0.255 time-range ftp
#
local-user ftp class manage
password hash
$h$6$SaX+pDwj5p/w/Yhq$zfUVjlVTrgIntelbrasIRdMAZh6pXJRKcXslOXekUcSsviU7J
CP2Kiv50lSL/1BU2BjnOQ2HRy7P3do7EwvxPeR/0+SA==
service-type ftp
authorization-attribute user-role level-15
authorization-attribute user-role network-operator
#
ftp server enable
ftp server acl 2000

```


Example: Filtering packets by IP address

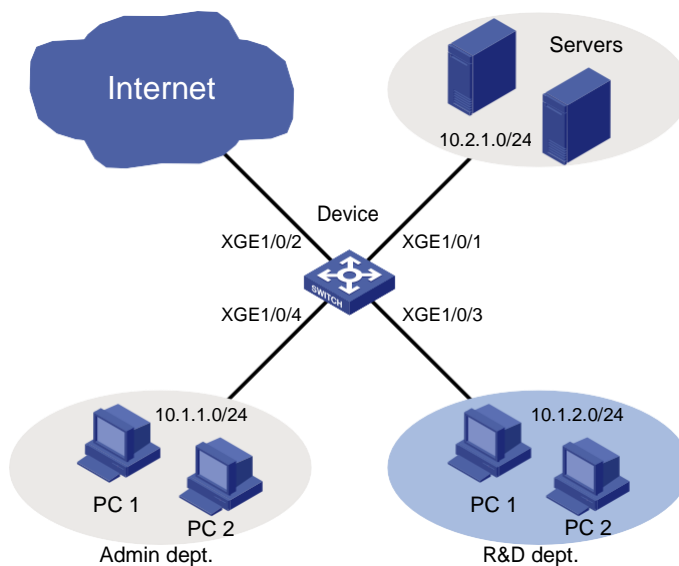
Network configuration

As shown in [Figure 3](#), a company's internal network connects to the Internet through the device. The R&D department, Administration department, and servers are on different subnets.

Configure packet filtering to meet the following requirements:

- The Administration department can access the Internet and servers at any time, but cannot access the R&D department at any time.
- The R&D department can access only the servers during working hours (8:30 to 18:00) on working days (Monday to Friday). It can access the Internet and servers, but cannot access the Administration department outside working hours.

Figure 3 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To deny the Administration department to access the R&D department, perform the following tasks:
 - Configure an advanced ACL to deny packets destined for subnet 10.1.2.0/24.
 - Apply the ACL to filter incoming packets on GigabitEthernet 1/0/4.
- To implement access control for the R&D department, perform the following tasks:
 - Create a time range for the working hours (8:30 to 18:00) on working days (Monday to Friday).
 - Create an advanced ACL and configure the following rules:
 - Configure rules to allow only packets destined for subnet 10.2.1.0/24 to pass through. Set the rules to be active during the time range.
 - To deny the R&D department to access the Administration department, configure a rule to deny packets destined for subnet 10.1.1.0/24.

- Apply the ACL to filter incoming packets on GigabitEthernet 1/0/3.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- SC 3130 series.

Restrictions and guidelines

When you configure ACL rules to allow the R&D department to access only the servers during working hours on working days, configure the permit rule before the deny rule. Otherwise, the interface denies all packets during working hours on working days.

Procedures

Denying the Administration department to access the R&D department

Create IPv4 advanced ACL 3000.

```
<Device> system-view
```

```
[Device] acl advanced 3000
```

Configure a rule to deny packets destined for subnet 10.1.2.0/24 to pass through.

```
[Device-acl-ipv4-adv-3000] rule deny ip destination 10.1.2.0 0.0.0.255
```

```
[Device-acl-ipv4-adv-3000] quit
```

Apply ACL 3000 to filter incoming packets on GigabitEthernet 1/0/4.

```
[Device] interface gigabitethernet 1/0/4
```

```
[Device-GigabitEthernet1/0/4] packet-filter 3000 inbound
```

```
[Device-GigabitEthernet1/0/4] quit
```

Configuring access control for the R&D department

Configure a time range **worktime** for the time range of 8:30 to 18:00 from Monday to Friday.

```
[Device] time-range worktime 8:30 to 18:00 working-day
```

Create IPv4 advanced ACL 3001.

```
[Device] acl advanced 3001
```

Configure a rule to allow packets destined for subnet 10.2.1.0/24 to pass through during **worktime**.

```
[Device-acl-ipv4-adv-3001] rule permit ip destination 10.2.1.0 0.0.0.255 time-range worktime
```

Configure a rule to deny all IP packets to pass through during **worktime**.

```
[Device-acl-ipv4-adv-3001] rule deny ip time-range worktime
# Configure a rule to deny packets destined for subnet 10.1.1.0/24 to pass through.
[Device-acl-ipv4-adv-3001] rule deny ip destination 10.1.1.0 0.0.0.255
[Device-acl-ipv4-adv-3001] quit
# Apply ACL 3001 to filter incoming packets on GigabitEthernet 1/0/3.
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] packet-filter 3001 inbound
[Device-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Verify that the ACLs are successfully applied for packet filtering.

```
[Device] display packet-filter interface inbound
Interface: GigabitEthernet1/0/3
Inbound policy:
IPv4 ACL 3001
Interface: GigabitEthernet1/0/4
Inbound policy:
IPv4 ACL 3000
```

Verify that you cannot ping through a website on the Internet from the R&D department at 9:30 on Monday.

```
C:\>ping www.google.com
```

```
Pinging www.google.com [173.194.127.242] with 32 bytes of data:
```

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

```
Ping statistics for 173.194.127.242:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>
```

Verify that you can ping through a website on the Internet from the Administration department at 9:30 on Monday.

```
C:\>ping www.google.com
```

```
Pinging www.google.com [173.194.127.242] with 32 bytes of data:
```

```
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
```

```
Ping statistics for 173.194.127.242:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```

    Minimum = 30ms, Maximum = 30ms, Average = 30ms
C:\>

# Verify that you can ping through a website on the Internet from the R&D department at 19:30 on Monday.
C:\>ping www.google.com

Pinging www.google.com [173.194.127.242] with 32 bytes of data:

Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50
Reply from 173.194.127.242: bytes=32 time=30ms TTL=50

Ping statistics for 173.194.127.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 30ms, Maximum = 30ms, Average = 30ms
C:\>

```

Configuration files

```

#
interface GigabitEthernet1/0/3
    port link-mode bridge
    packet-filter 3001 inbound
#
interface GigabitEthernet1/0/4
    port link-mode bridge
    packet-filter 3000 inbound
#
    time-range worktime 08:30 to 18:00 working-day
#
acl advanced 3000
    rule 0 deny ip destination 10.1.2.0 0.0.0.255
#
acl advanced 3001
    rule 0 permit ip destination 10.2.1.0 0.0.0.255 time-range worktime
    rule 5 deny ip time-range worktime
    rule 10 deny ip destination 10.1.1.0 0.0.0.255

```

Example: Filtering TCP packets

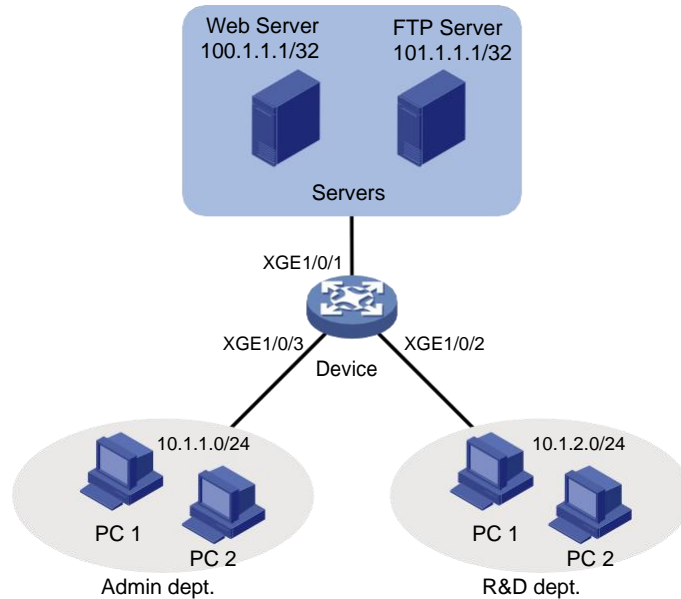
Network configuration

As shown in [Figure 4](#), the R&D department, Administration department, and servers are on different networks, and they are connected through the device.

Configure packet filtering to meet the following requirements:

- The Web server provides HTTP services to only the Administration department.
- The FTP server provides FTP services to only the R&D department.
- The TCP connections between hosts and the Web server can only be initiated by the hosts. The TCP connections between hosts and the FTP server can be initiated by either the hosts or the FTP server.

Figure 4 Network diagram



Analysis

To meet the network requirements, you must perform the following tasks:

- To allow TCP connections initiated by the hosts to the Web server, perform the following tasks:
 - Configure an advanced ACL rule as follows to allow packets sent by the Web server through established TCP connections to pass through:
 - Specify the **established** keyword (the ACK or RST flag bit set) in the rule to match established TCP connections.
 - Because a TCP initiator typically uses a TCP port number higher than 1023, specify a port number range higher than 1023 to match established TCP connections.
 - Configure an advanced ACL rule to deny packets sent from the subnet where the Web server resides to the subnet where the hosts reside.
- FTP uses TCP port 20 for data transfer and port 21 for FTP control. To identify FTP traffic, you must specify TCP ports 20 and 21 in ACL rules.
- To identify HTTP packets, specify TCP port 80 in ACL rules.

Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 6320 and later

The **port link-mode** command is not supported on the following switches and the **port link-mode bridge** command does not appear in their configuration files.

- SC 3130 series.

Procedures

Configuring access control for the Administration department

Create IPv4 advanced ACL 3000.

```
<Device> system-view
[Device] acl advanced 3000
```

Configure a rule to allow TCP packets from the Web server to the hosts on subnet 10.1.1.0/24, with TCP port number higher than 1023 and the ACK or RST flag set.

```
[Device-acl-ipv4-adv-3000] rule permit tcp established source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255 destination-port gt 1023
```

Configure a rule to deny TCP packets from subnet 100.1.1.1/32 to subnet 10.1.1.0/24 to pass through.

```
[Device-acl-ipv4-adv-3000] rule deny tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255
```

Configure a rule to deny FTP packets sourced from 101.1.1.1/32 to pass through.

```
[Device-acl-ipv4-adv-3000] rule deny tcp source 101.1.1.1 0 source-port range 20 21
[Device-acl-ipv4-adv-3000] quit
```

Apply ACL 3000 to filter outgoing packets on GigabitEthernet 1/0/3.

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] packet-filter 3000 outbound
[Device-GigabitEthernet1/0/3] quit
```

Configuring access control for the R&D department

Create IPv4 advanced ACL 3001.

```
[Device] acl advanced 3001
```

Configure a rule to deny HTTP packets sourced from 100.1.1.1/32 to pass through.

```
[Device-acl-ipv4-adv-3001] rule deny tcp source 100.1.1.1 0 source-port eq 80
[Device-acl-ipv4-adv-3001] quit
```

Apply ACL 3001 to filter outgoing packets on GigabitEthernet 1/0/2.

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] packet-filter 3001 outbound
[Device-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Verify that the ACLs are successfully applied for packet filtering.

```
[Device] display packet-filter interface outbound
Interface: GigabitEthernet1/0/2
Outbound policy:
  IPv4 ACL 3001
Interface: GigabitEthernet1/0/3
Outbound policy:
  IPv4 ACL 3000
```

Verify that you cannot Telnet to the FTP server from the Administration department.

```
C:\>telnet 101.1.1.1 21
Connecting To 101.1.1.1...Could not open connection to the host, on port 21:
Connect failed
```

```
C:\>
```

2. Verify that from the Webserver, you can ping a host in the Administration department, but cannot access a shared folder on the host:

Set a shared folder on a host in the Administration department. (Details not shown.)

Ping the host from the Web server. The ping operation succeeds.

```
C:\>ping 10.1.1.110
```

```
Pinging 10.1.1.110 with 32 bytes of data:
Reply from 10.1.1.110: bytes=32 time=2ms TTL=128
Reply from 10.1.1.110: bytes=32 time=14ms TTL=128
Reply from 10.1.1.110: bytes=32 time=1ms TTL=128
Reply from 10.1.1.110: bytes=32 time=1ms TTL=128
```

```
Ping statistics for 10.1.1.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 4ms
```

```
C:\>
```

Verify that you cannot access the share folder from the Web server. (Details not shown.)

3. Verify that you cannot Telnet to the Web server from the R&D department.

```
C:\>telnet 100.1.1.1 80
Connecting To 100.1.1.1...Could not open connection to the host, on port 80:
Connect failed
```

```
C:\>
```


Configuration files

```
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  packet-filter 3001 outbound
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  packet-filter 3000 outbound

#
acl advanced 3000
  rule 0 permit tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255 destination
-port gt 1023 established
  rule 5 deny tcp source 100.1.1.1 0 destination 10.1.1.0 0.0.0.255
  rule 10 deny tcp source 101.1.1.1 0 source-port range ftp-data ftp
#
acl advanced 3001
  rule 0 deny tcp source 100.1.1.1 0 source-port eq www
```

