2.4 Lab 4: Inter-VLAN Communication

2.4.1 Introduction

2.4.1.1 About This Lab

VLANs are separated at Layer 2 to minimize broadcast domains. To enable the communication between VLANs,Huawei provides a variety of technologies. The following two technologies are commonly used:

- Dot1q termination subinterface: Such subinterfaces are Layer 3 logical interfaces. Similar to a VLANIF interface, after a dot1q termination subinterface and its IP address are configured, the device adds the corresponding MAC address entry and sets the Layer 3 forwarding flag to implement Layer 3 communication between VLANs. A Dot1q termination subinterface applies to scenarios where a Layer 3 Ethernet port connects to multiple VLANs.
- VLANIF interface: VLANIF interfaces are Layer 3 logical interfaces. After a VLANIF interface and its IP address are configured, the device adds the MAC address and VID of the VLANIF interface to the MAC address table and sets the Layer 3 forwarding flag of the MAC address entry. When the destination MAC address of a packet matches the entry, the packet is forwarded at Layer 3 to implement Layer 3 communication between VLANs.

  In this lab activity, you will use two methods to implement inter-VLAN communication.

2.4.1.2 Objectives

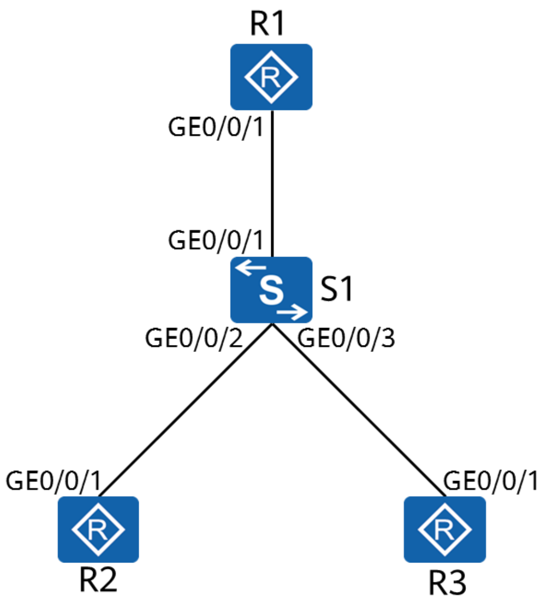
Upon completion of this task, you will be able to:

- Learn how to use Dot1q termination subinterfaces to implement inter-VLAN communication
- Learn how to use VLANIF interfaces to implement inter-VLAN communication
- Understand the forwarding process of inter-VLAN communication

2.4.1.3 Networking Topology

R2 and R3 belong to different VLANs and they need to communicate with each other through VLANIF interfaces and Dot1q termination subinterfaces.

Figure 2-1 Lab topology for inter-VLAN communication



1. Simulate terminal users on R2 and R3 and assign IP addresses 192.168.2.1/24 and 192.168.3.1/24 to the interfaces.
2. The gateway addresses of R2 and R3 are 192.168.2.254 and 192.168.3.254 respectively.
3. On S1, assign GigabitEthernet0/0/2 and GigabitEthernet0/0/3 to VLAN 2 and VLAN 3, respectively.

1.1.2 Lab Configuration

1.1.2.1 Configuration Roadmap

1. Configure Dot1q termination subinterfaces to implement inter-VLAN communication.
2. Configure VLANIF interfaces to implement inter-VLAN communication.

1.1.2.2 Configuration Procedure

Step 1 Complete basic device configuration.

# Name R1, R2, R3, and S1.

The details are not provided here.

# Configure IP addresses and gateways for R2 and R3.

```
<R2> system-view
Enter system view, return user view with Ctrl+Z.
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 192.168.2.1 24
[R2-GigabitEthernet0/0/1]quit
[R2]ip route-static 0.0.0.0 0 192.168.2.254
```

Configure a default route (equivalent to a gateway) for the device.

```
<R3>system-view
Enter system view, return user view with Ctrl+Z.
```

```
[R3]interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1]ip address 192.168.3.1 24
[R3-GigabitEthernet0/0/1]quit
[R3]ip route-static 0.0.0.0 0 192.168.3.254
```

# On S1, assign R2 and R3 to different VLANs.

```
[S1]vlan batch 2 3
Info: This operation may take a few seconds. Please wait for a moment...done.
[S1]interface GigabitEthernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type access
[S1-GigabitEthernet0/0/2]port default vlan 2
[S1-GigabitEthernet0/0/2]quit
[S1]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 3
```

Step 2 Configure Dot1q termination subinterfaces to implement INter-VLAN communication.

# Configure a trunk port on S1.

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
The link between S1 and R1 must allow packets from VLAN 2 and VLAN 3 to pass through because R1 needs to terminate
the VLAN tags of packets exchanged between VLANs.
```

# Configure a dot1q termination subinterface on R1.

```
[R1]interface GigabitEthernet 0/0/1.2
```

A subinterface is created and the subinterface view is displayed. In this example, **2** indicates the subinterface number. It is recommended that the subinterface number be the same as the VLAN ID.

```
[R1-GigabitEthernet0/0/1.2]dot1q termination vid 2
```

The **dot1q termination vid** *vlan-id* command configures the VLAN ID for Dot1q termination on a subinterface.

In this example, when GigabitEthernet0/0/1 receives data tagged with VLAN 2, it sends the data to subinterface 2 for VLAN termination and subsequent processing. The data sent from subinterface 2 is also tagged with VLAN 2.

```
[R1-GigabitEthernet0/0/1.2]arp broadcast enable
```

Subinterfaces for VLAN tag termination cannot forward broadcast packets and automatically discard them upon receiving. To allow such subinterfaces to forward broadcast packets, the ARP broadcast function must be enabled using the **arp broadcast enable** command. By default, this function is enabled on some devices.

```
[R1-GigabitEthernet0/0/1.2]ip address 192.168.2.254 24
[R1-GigabitEthernet0/0/1.2]quit
[R1]interface GigabitEthernet 0/0/1.3
[R1-GigabitEthernet0/0/1.3]dot1q termination vid 3
[R1-GigabitEthernet0/0/1.3]arp broadcast enable
[R1-GigabitEthernet0/0/1.3]ip address 192.168.3.254 24
[R1-GigabitEthernet0/0/1.3]quit
```

# Test the connectivity between VLANs.

```
<R2>ping 192.168.3.1
  PING 192.168.3.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=254 time=110 ms
    Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=254 time=70 ms
    Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=254 time=100 ms

  --- 192.168.3.1 ping statistics ---
```

```
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/76/110 ms

<R2>tracert 192.168.3.1
 traceroute to  192.168.3.1(192.168.3.1), max hops: 30 ,packet length: 40,press CTRL_C to break

 1 192.168.2.254 30 ms  50 ms  50 ms

 2 192.168.3.1 70 ms  60 ms  60 ms
VLAN 2 and VLAN 3 can communicate with each other.
```

Step 3 Configure VLANIF interfaces to enable inter-VLAN communication.

# Delete the configuration in the previous step.

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]undo port trunk allow-pass vlan 2 3
[S1-GigabitEthernet0/0/1]undo port link-type
[R1]undo interface GigabitEthernet 0/0/1.2
[R1]undo interface GigabitEthernet 0/0/1.3
```

# Create a VLANIF interface on S1.

```
[S1]interface Vlanif 2
```

The **interface vlanif** *vlan-id* command creates a VLANIF interface and displays the VLANIF interface view. You must create a VLAN before configuring a VLANIF interface.

```
[S1-Vlanif2]ip address 192.168.2.254 24
[S1-Vlanif2]quit
[S1]interface Vlanif 3
[S1-Vlanif3]ip address 192.168.3.254 24
[S1-Vlanif3]quit
```

# Test the connectivity between VLANs.

```
<R2>ping 192.168.3.1
  PING 192.168.3.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.3.1: bytes=56 Sequence=1 ttl=254 time=100 ms
    Reply from 192.168.3.1: bytes=56 Sequence=2 ttl=254 time=50 ms
    Reply from 192.168.3.1: bytes=56 Sequence=3 ttl=254 time=50 ms
    Reply from 192.168.3.1: bytes=56 Sequence=4 ttl=254 time=60 ms
    Reply from 192.168.3.1: bytes=56 Sequence=5 ttl=254 time=70 ms
  --- 192.168.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 50/66/100 ms

<R2>tracert 192.168.3.1

 traceroute to  192.168.3.1(192.168.3.1), max hops: 30 ,packet length: 40,press CTRL_C to break

 1 192.168.2.254 40 ms  30 ms  20 ms

 2 192.168.3.1 40 ms  30 ms  40 ms
VLAN 2 and VLAN 3 can communicate with each other.
```

----End

1.1.3 Verification

The details are not provided here.

1.1.4 Configuration Reference

Configuration on S1

```
#
sysname S1
#
vlan batch 2 to 3
#
interface Vlanif2
 ip address 192.168.2.254 255.255.255.0
#
interface Vlanif3
 ip address 192.168.3.254 255.255.255.0
#
interface GigabitEthernet0/0/2
 port link-type access
 port default vlan 2
#
interface GigabitEthernet0/0/3
 port link-type access
 port default vlan 3
#
return
```

Configuration on R2

```
#
 sysname R2
#
interface GigabitEthernet0/0/1
 ip address 192.168.2.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.2.254
#
return
```

Configuration on R3

```
#
 sysname R3
#
interface GigabitEthernet0/0/1
 ip address 192.168.3.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.3.254
#
return
```

1.1.5 Quiz

1. If R2 needs to access the network connected to R1, what configuration needs to be performed on S1?
2. As a Layer 3 interface, when will a VLANIF interface go Up?

2 Network Security Basics and Network Access

2.1 Lab 1: ACL Configuration

2.1.1 Introduction

2.1.1.1 About This Lab

An Access Control List (ACL) is a collection of one or more rules. A rule refers to a judgment statement that describes a packet matching condition, which may be a source address, destination address, or port number.

An ACL is a rule-based packet filter. Packets matching an ACL are processed based on the policy defined in the ACL.

2.1.1.2 Objectives

Upon completion of this task, you will be able to:

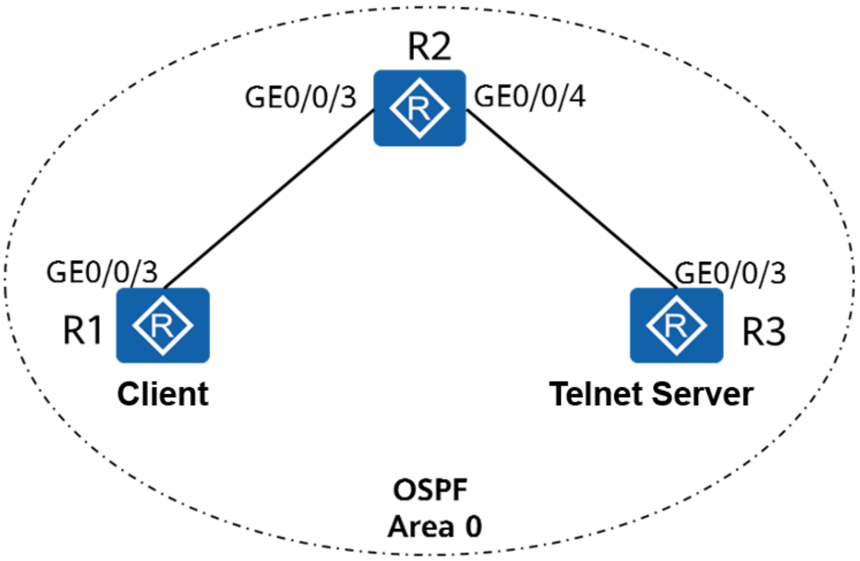
- Learn how to configure ACLs
- Learn how to apply an ACL on an interface
- Understand the basic methods of traffic filtering

2.1.1.3 Networking Topology

As shown in the networking diagram, R3 functions as the server, R1 functions as the client, and they are reachable to reach other. The IP addresses of the physical interfaces connecting R1 and R2 are 10.1.2.1/24 and 10.1.2.2/24 respectively, and the IP addresses of the physical interfaces connecting R2 and R3 are 10.1.3.2/24 and 10.1.3.1/24, respectively. In addition, two logical interfaces LoopBack 0 and LoopBack 1 are created on R1 to simulate two client users. The IP addresses of the two interfaces are 10.1.1.1/24 and 10.1.4.1/24, respectively.

One user (Loopback 1 of R1) needs to remotely manage R3. You can configure Telnet on the server, configure password protection, and configure an ACL to ensure that only the user that meets the security policy can log in to R3.

Figure 2-1 Lab topology for ACL configuration



2.1.2 Lab Configuration

2.1.2.1 Configuration Roadmap

1. Configure IP addresses.
2. Configure OSPF to ensure network connectivity.
3. Create an ACL to match desired traffic.
4. Configure traffic filtering.

2.1.2.2 Configuration Procedure

Step 1 Configure IP addresses.

# Configure IP addresses for R1, R2, and R3.

```
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.1.2.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]interface LoopBack 0
[R1-LoopBack0]ip address 10.1.1.1 24
[R1-LoopBack0]quit
[R1]interface LoopBack 1
[R1-LoopBack1]ip address 10.1.4.1 24
[R1-LoopBack0]quit
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.1.2.2 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 10.1.3.2 24
[R2-GigabitEthernet0/0/4]quit
```

```
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 10.1.3.1 24
[R3-GigabitEthernet0/0/3]quit
```

Step 2 Configure OSPF to ensure network connectivity.

# Configure OSPF on R1, R2, and R3 and assign them to area 0 to enable connectivity.

```
[R1]ospf
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.1.2.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]network 10.1.4.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0]return
```

```
[R2]ospf
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.1.2.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]network 10.1.3.2 0.0.0.0
[R2-ospf-1-area-0.0.0.0]return
```

```
[R3]ospf
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.1.3.1 0.0.0.0
[R3-ospf-1-area-0.0.0.0]return
```

# Run the ping command on R3 to test network connectivity.

```
<R3>ping 10.1.1.1
  PING 10.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=254 time=40 ms
    Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=254 time=40 ms
    Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=254 time=20 ms
    Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=254 time=40 ms
    Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=254 time=30 ms
  --- 10.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/34/40 ms

<R3>ping 10.1.2.1
  PING 10.1.2.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.2.1: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 10.1.2.1: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 10.1.2.1: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 10.1.2.1: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.1.2.1: bytes=56 Sequence=5 ttl=254 time=50 ms
  --- 10.1.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 30/34/50 ms

<R3>ping 10.1.4.1
  PING 10.1.4.1: 56  data bytes, press CTRL_C to break
    Reply from 10.1.4.1: bytes=56 Sequence=1 ttl=254 time=50 ms
    Reply from 10.1.4.1: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 10.1.4.1: bytes=56 Sequence=3 ttl=254 time=40 ms
    Reply from 10.1.4.1: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 10.1.4.1: bytes=56 Sequence=5 ttl=254 time=30 ms
  --- 10.1.4.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/36/50 ms
```

Step 3 Configuration R3 as a server.

# Enable the Telnet function on R3, set the user level to 3, and set the login password to Huawei@123.

```
[R3]telnet server enable
```

The **telnet server enable** command enables the Telnet service.

```
[R3]user-interface vty 0 4
```

The **user-interface** command displays one or multiple user interface views.

The Virtual Type Terminal (VTY) user interface manages and monitors users logging in using Telnet or SSH.

```
[R3-ui-vty0-4]user privilege level 3
[R3-ui-vty0-4] set authentication password cipher
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use "aaa" authentication mode.
Enter Password(<8-128>):Huawei@123
Confirm password:Huawei@123
[R3-ui-vty0-4] quit
```

Step 4 Configure an ACL to match desired traffic.

Method 1: Configure an ACL on the VTY interface of R3 to allow R1 to log in to R3 through Telnet using the IP address of loopback 1.

# Configure an ACL on R3.

```
[R3]acl 3000
[R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R3-acl-adv-3000]rule 10 deny tcp source any
[R3-acl-adv-3000]quit
```

# Filter traffic on the VTY interface of R3.

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]acl 3000 inbound
```

# Display the ACL configuration on R3.

```
[R3]display acl 3000
```

The **display acl** command displays the ACL configuration.

```
Advanced ACL 3000, 2 rules
```

An advanced ACL is created. It is numbered 3000 and contains two rules.

```
Acl's step is 5
```

The step between ACL rule numbers is 5.

```
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
```

Rule 5 allows matched traffic to pass through. If no packet matches the rule, the **matches** field is not displayed.

```
 rule 10 deny tcp
```

Method 2: Configure an ACL on the physical interface of R2 to allow R1 to log in to R3 through Telnet from the IP address of the physical interface.

# Configure an ACL on R2.

```
[R2]acl 3001
[R2-acl-adv-3001]rule 5 permit tcp source 10.1.4.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3001]rule 10 deny tcp source any
[R2-acl-adv-3001]quit
```

# Filter traffic on GE0/0/3 of R3.

```
[R2]interface GigabitEthernet0/0/3
```

```
[R2-GigabitEthernet0/0/3]traffic-filter inbound acl 3001
```

# Display the ACL configuration on R2.

```
[R2]display acl 3001
Advanced ACL 3001, 2 rules
Acl's step is 5
rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet (21 matches)
```

Rule 5 allows matched traffic to pass through, and 21 packets have matched the rule.

```
rule 10 deny tcp (1 matches)
```

----End

2.1.3 Verification

Test the Telnet access and verify the ACL configuration.

1. On R1, telnet to the server with the source IP address 10.1.1.1 specified.

```
<R1>telnet -a 10.1.1.1 10.1.3.1
```

The **telnet** command enables a user to use the Telnet protocol to log in to another device.

-a *source-ip-address*: specifies the source IP address. Users can communicate with the server from the specified IP address.

```
  Press CTRL_] to quit telnet mode
  Trying 10.1.3.1 ...
  Error: Can't connect to the remote host
```

2. On R1, telnet to the server with the source IP address 10.1.4.1 specified.

```
<R1>telnet -a 10.1.4.1 10.1.3.1
  Press CTRL_] to quit telnet mode
  Trying 10.1.3.1 ...
  Connected to 10.1.3.1 ...

Login authentication

Password:
<R3>quit
```

2.1.4 Configuration Reference (Method 1)

Configuration on R1

```
#
 sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.1.4.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 10.1.2.1 0.0.0.0
network 10.1.4.1 0.0.0.0
#
return
```

Configuration on R2

```
#
 sysname R2
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet0/0/4
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.2 0.0.0.0
  network 10.1.3.2 0.0.0.0
#
return
```

Configuration on R3

```
#
 sysname R3
#
acl number 3000
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.3.1 0.0.0.0
#
 telnet server enable
#
user-interface vty 0 4
 acl 3000 inbound
 authentication-mode password
 user privilege level 3
 set authentication password cipher %^%#Z5)H#8cE(YJ6YZ:='}c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#
#
return
```

2.1.5 Configuration Reference (Method 2)

Configuration on R1

```
#
 sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.1.4.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.1 0.0.0.0
  network 10.1.2.1 0.0.0.0
  network 10.1.4.1 0.0.0.0
#
return
```

Configuration on R2

```
#
 sysname R2
#
```

```
acl number 3001
 rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet
 rule 10 deny tcp
#
interface GigabitEthernet0/0/3
 ip address 10.1.2.2 255.255.255.0
traffic-filter inbound acl 3001
#
interface GigabitEthernet0/0/4
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.2 0.0.0.0
  network 10.1.3.2 0.0.0.0
#
return
```

Configuration on R3

```
#
 sysname R3
#
interface GigabitEthernet0/0/3
 ip address 10.1.3.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.3.1 0.0.0.0
#
 telnet server enable
#
user-interface vty 0 4
authentication-mode password
 user privilege level 3
 set authentication password cipher %^%#Z5)H#8cE(YJ6YZ:='}c-;trp&784i>HtKl~pLnn>2zL16cs<6E}xj.FmK5(8%^%#
#
return
```

2.1.6 Quiz

R3 functions as both a Telnet server and an FTP server, the IP address of loopback 0 on R1 must be used to access only the FTP service, and the IP address of loopback 1 on R1 must be used to remotely manage R3 using Telnet.

Configure an ACL to meet the requirements.