Lab4

1 Lab4 Part 1 ACL Configuration

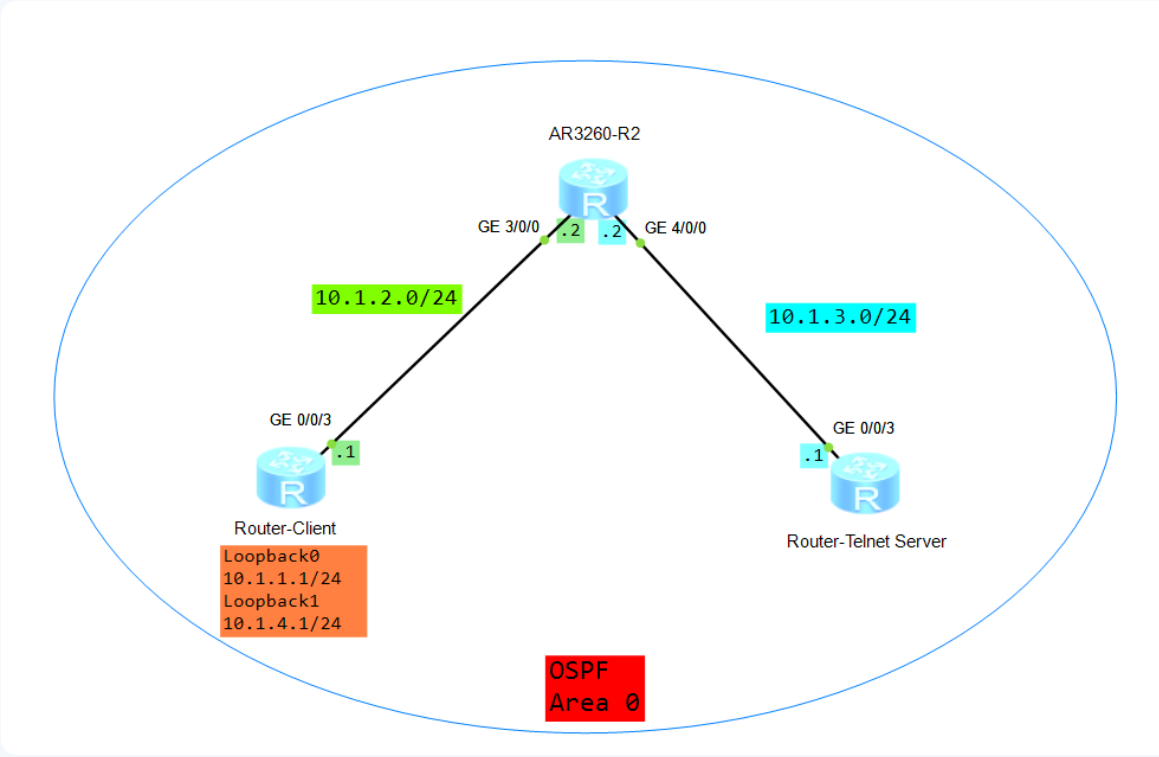
1.1 Overview

Access Control Lists (ACLs) are crucial for network security, allowing control over traffic flow based on specified rules. ACLs can be used to filter packets by source/destination address or port number.

1.2 Objectives

- Understand and configure ACLs.
- Apply ACLs to interfaces.
- Grasp basic traffic filtering methods.

1.3 Networking Topology



R3 is act as telnet server is configured with a Telnet server accessible by LoopBack 1 of R1.

R1 is act as client (end device) to access telnet server using telnet

1.4 Configuration Steps

1.4.1 Step 1: Configure IP Addresses

Assign IP addresses to interfaces on routers R1, R2, and R3.

1.4.1.1 R1

```
1]interface GigabitEthernet0/0/3
1-GigabitEthernet0/0/3]ip address 10.1.2.1 24
1-loopback0]interface loopback0
1-loopback0]ip add 10.1.1.1 24
1-loopback1]interface loopback1
[R1-loopback1]ip add 10.1.4.1 24
```

1.4.1.2 R2

```
[R2]interface GigabitEthernet3/0/0
[R1-GigabitEthernet3/0/0]ip address 10.1.2.2 24
[R1-GigabitEthernet3/0/0]interface GigabitEthernet4/0/0
[R1-GigabitEthernet4/0/0]ip address 10.1.3.2 24
```

1.4.1.3 R3

```
[R3]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.1.3.1 24
```

1.4.2 Step 2: Configure OSPF for Connectivity

1.4.2.1 R1

```
[R1]ospf 1
```

```
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.1.1.1 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.1.4.1 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.1.2.0 0.0.0.255
```

1.4.2.2 R2

Markdown

```
[R2]ospf 1
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.1.3.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.1.2.0 0.0.0.255
```

1.4.2.3 R3

Markdown

```
[R3]ospf 1
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.1.3.0 0.0.0.255
```

> Enable OSPF on all routers to ensure they can communicate with each other.

1.4.2.4 Display 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 ---
```

> Test pining Between R3 & R2 and R3 & R1

1.4.3 Step 3: Set Up Server (R3)

Markdown

```
[R3]telent server enable
[R3]user-interface vty 0 4
[R3-ui-vty0-4]user privilege level 3
[R3-ui-vty0-4]set authentication password cipher huawei
```

> Enable Telnet service on R3 with user level set to 3 and a strong password.

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

1.4.4 Step 4: Create and Apply ACLs

Two methods are described:

1.4.4.1 Method 1

> Apply an ACL directly on the VTY interface of the server (R3) to allow only LoopBack 1 of client (R1) access via Telnet.

> Configure an ACL on R3.

Markdown

```
[R3]acl 3000
[R3-acl-adv-3000]rule 10 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 20 deny tcp source any destination any
```

> Filter traffic on the VTY interface of R3

Markdown

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

```
[R3-ui-vty0-4]acl 3000 inbound
```

Display ACL

Markdown

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

```
Advanced ACL 3000, 2 rules
ACL's step is 5
 rule 10 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq
 telnet (1 times matched)
 rule 20 deny tcp (8 times matched)
```

1.4.4.2 Method 2

Apply an ACL on an intermediate router's (R2) physical interface that filters traffic going towards the server (R3).

Configure an ACL on R2

Markdown

```
[R2]acl 3001
[R2-acl-adv-3001]rule 10 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 20 deny tcp source any
destination any
```

Filter traffic on GE0/0/3 of R3

Markdown

```
[R2]interface GigabitEthernet3/0/0
```

```
[R2-GigabitEthernet3/0/0]traffic-filter inbound acl 3001
```

Display the ACL configuration on R2

Markdown

```
[R2]display acl 3001
```

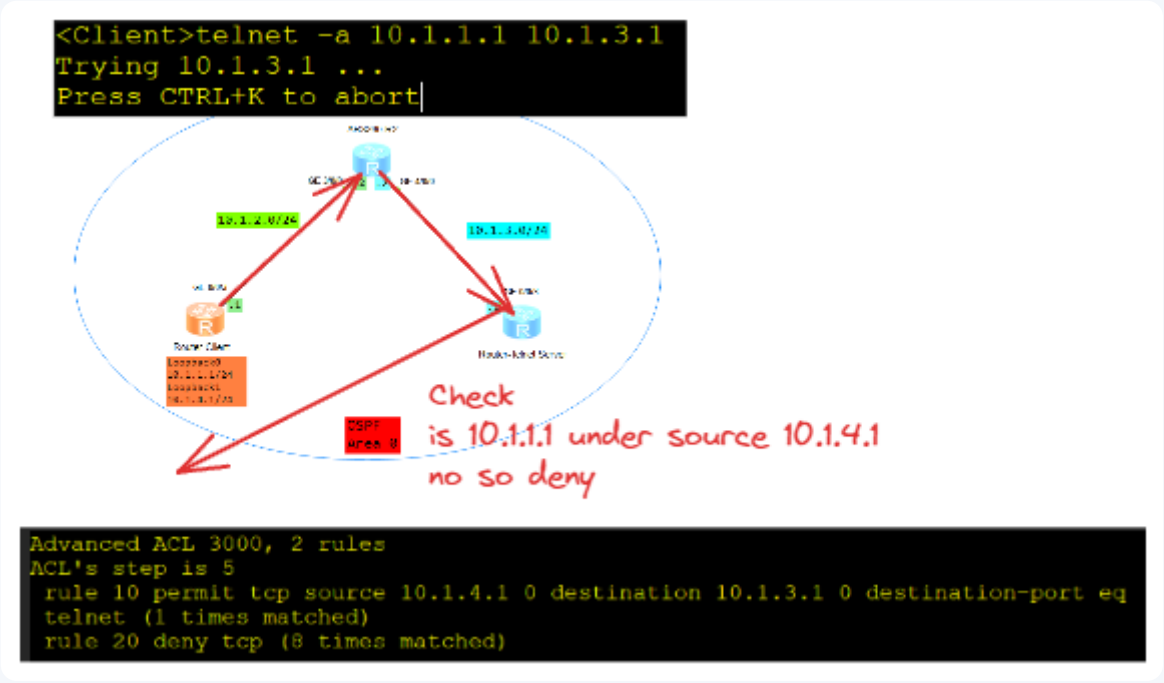
```
Advanced ACL 3001, 2 rules
Acl's step is 5
 rule 10 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet (82 matches)
 rule 20 deny tcp (3 matches)
```

1.5 Verification

Test Telnet access from client (R1) using both LoopBack interfaces and confirm that only LoopBack 1 can successfully establish a connection due to the applied ACL.

1.5.1 Method 1

Apply an ACL directly on the VTY interface of the server (R3) to allow only LoopBack 1 of client (R1) access via Telnet.

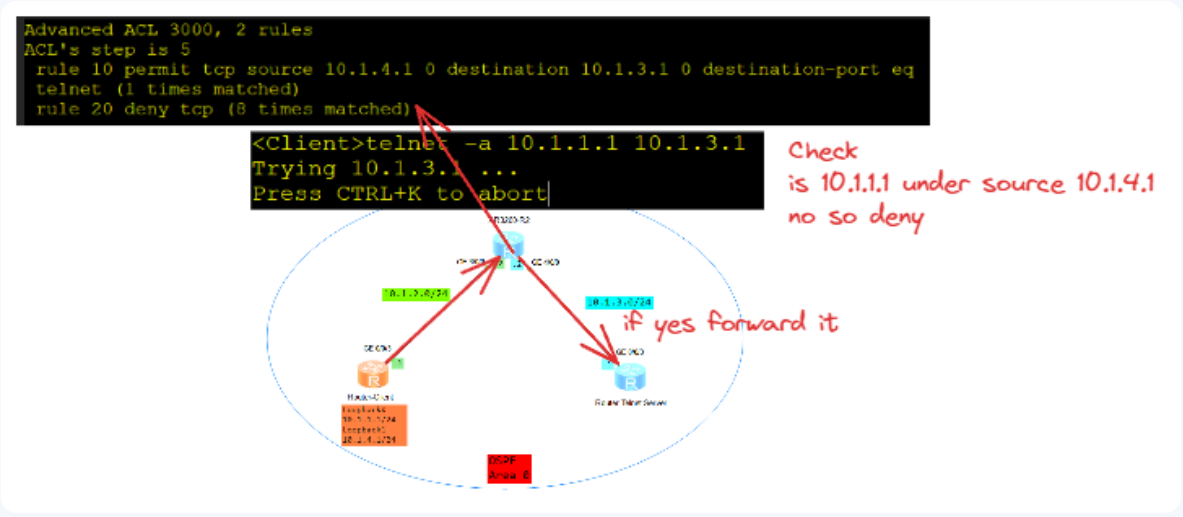



```
<Client>telnet -a 10.1.1.1 10.1.3.1
Trying 10.1.3.1 ...
Press CTRL+K to abort
```

```
<Client>telnet -a 10.1.4.1 10.1.3.1
Trying 10.1.3.1 ...
Press CTRL+K to abort
Connected to 10.1.3.1 ...


Login authentication


Password:
Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
      The current login time is 2024-04-16 05:16:53.
<Telent Server>
```

1.5.2 Method 2

> Apply an ACL on an intermediate router's (R2) physical interface that filters traffic going towards the server (R3).




```
<Client>telnet -a 10.1.1.1 10.1.3.1
Trying 10.1.3.1 ...
Press CTRL+K to abort
```

```
<Client>telnet -a 10.1.4.1 10.1.3.1
Trying 10.1.3.1 ...
Press CTRL+K to abort
Connected to 10.1.3.1 ...


Login authentication


Password:
Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 1.
      The current login time is 2024-04-16 05:16:53.
<Telent Server>
```

1.6 Quiz Challenge

Question1

Configure an ACL that allows only FTP service access via loopback0 on client (R1), while permitting remote Telnet management via

loopback1.

Answer1

Sample Rule for FTP Service via loopback0

Markdown

```
[R2]acl number 3002
[R2-acl-adv-3002]rule 5 permit tcp source 10.1.2.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3002]rule 10 permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.3.1 0.0.0.0 destination-port range
[R2-acl-adv-3001]rule 15 deny tcp source any 20 21
[R2-acl-adv-3001]quit
[R2]interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3] traffic-filter inbound acl 300
```

2 Lab4 Part 2 Local AAA Configuration

2.1 Introduction

Authentication, Authorization, and Accounting (AAA) provides a management mechanism for network security with three main functions:

- **Authentication:** Verifies user access to the network.
- **Authorization:** Authorizes services for users.

- **Accounting:** Records network resources used by users.

AAA can be implemented using various protocols, with RADIUS being the most common in practice.

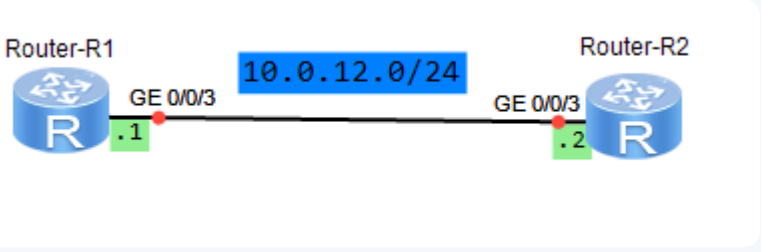
This lab focuses on configuring local AAA for remote Telnet users.

2.2 Objectives

Upon completing this lab, you should be able to:

1. Configure local AAA.
2. Create a domain for user management.
3. Create a local user.
4. Understand domain-based user management.

2.3 Networking Topology



Client R1 —Telnet→ Network Device R2

Configure local AAA on both `R1` (client) and `R2` (network device), controlling access to resources on `R2` .

2.4 Lab Configuration Steps

2.4.1 Step 1: Basic Device Configuration

Configure IP addresses:

R1:

```Markdown
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 10.0.12.1 2
```

R2:

```Markdown
[R2]interface GigabitEthernet0/0/3
[R2-GigabitEthernet0/0/3]ip address 10.0.12.2 24
```

2.4.2 Step 2: Configure an AAA Scheme on R2

```Markdown
[R2]aaa
[R2-aaa]authentication-scheme huawei
[R2-aaa-authen-huawei]authentication-mode local
[R2-aaa-authen-huawei]q
[R2-aaa]authorization-scheme huawei
[R2-aaa-author-huawei]authorization-mode local
```

Create authentication and authorization schemes named `huawei` with local modes.

> A device functioning as an AAA server is called a local AAA server, which can perform authentication and authorization, but not accounting

2.4.3 Step 3: Create a Domain and Apply the AAA Scheme

```Markdown
[R2-aaa]domain huawei
[R2-aaa-domain-huawei]authentication-scheme huawei
[R2-aaa-domain-huawei]authorization-scheme huawei
```

> Create a domain named `huawei` and apply previously created schemes for authentication and authorization.

2.4.4 Step 4: Configure Local Users

```Markdown
[R2-aaa]local-user lab@huawei password cipher huawei
[R2-aaa]local-user lab@huawei service-type telnet
[R2-aaa]local-user lab@huawei privilege level 3
```

> Create a local user `hcia@huawei` with password `huawei`, service type as Telnet, and privilege level of 3.

> Username and domain are parsed from a string with "@" as the delimiter; before "@" is the username, after is the domain. Without "@", the entire string is the username with a default domain.

> The `local-user service-type` command defines a user's access type, restricting login to that type only; if set to telnet, web access is not possible, but multiple types can be set for one user.

> A local user's privilege level determines command access; users can execute only those within or below their assigned level.

2.4.5 Step 5: Enable Telnet Function on R2

Markdown

```
[R2]telnet server enable
[R2]user-interface vty 0 4
[R2-ui-vty0-4]authentication-mode aaa
```

> Enable Telnet server function and configure VTY lines (0-4) authentication mode as AAA.

> By default, the user authentication mode of the VTY user interface is not configured.

2.5 Verification of Configuration

Use `telnet` command from `R1` to login into `R2`.

```
<R1>telnet 10.0.12.1
Trying 10.0.12.1 ...
Press CTRL+K to abort
Connected to 10.0.12.1 ...


Login authentication


Username:lab@huawei
Password:
Info: The max number of VTY users is 10, and the number
      of current VTY users on line is 2.
      The current login time is 2024-04-17 07:15:01.
<R1>
```

Username: lab@huawei
Password: huawei

Check online users on `R2` using the command:

Markdown

```
1 [R2]display users
```

```
<R1>dis users
  User-Intf    Delay    Type   Network Address     AuthenStatus    AuthorcmdFlag
  0    CON 0   00:07:50                                              no
  Username : Unspecified

+ 34   VTY 0   00:00:00  TEL    10.0.12.2                pass          no
  Username : lab@huawei
```

3 Lab4 Part 3 NAT Configuration

3.1 Introduction to NAT

Network Address Translation (NAT) is critical in addressing IPv4 shortages by allowing reuse of IP addresses. It offers two key benefits:

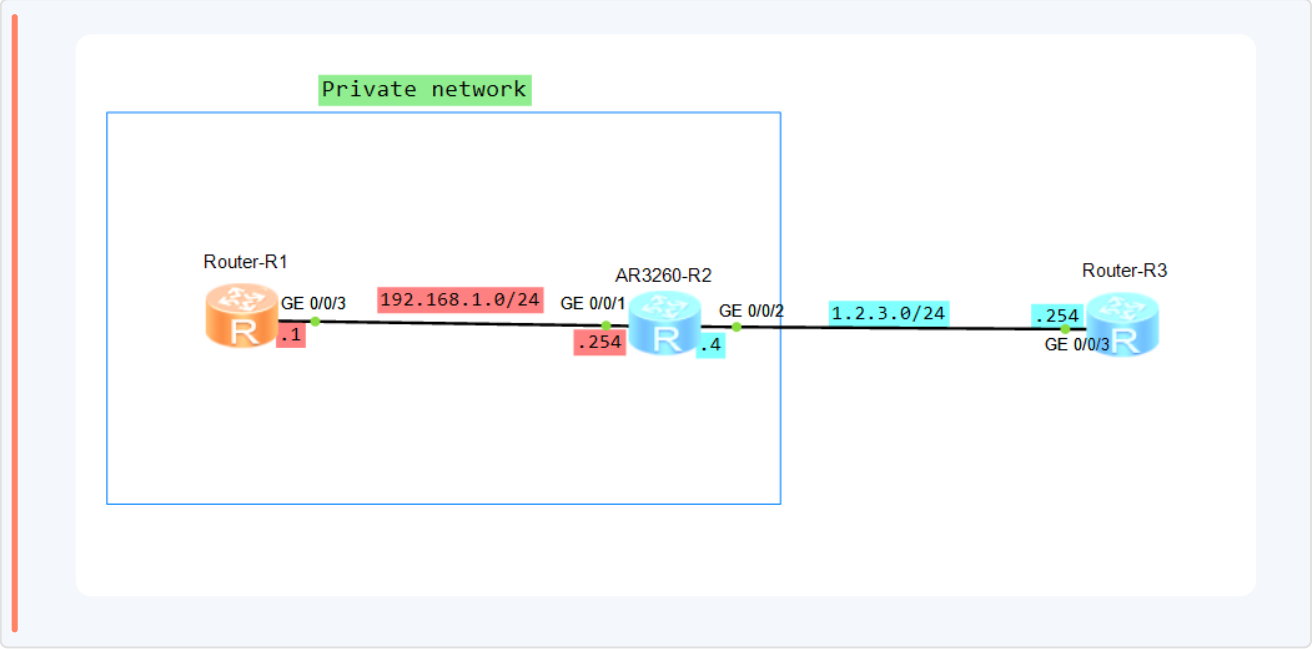
- Protects private networks against external attacks.
- Controls communication between private and public networks.

In this lab, we will configure NAT to understand its principle.

3.2 Objectives

- Configure dynamic NAT.
- Understand Easy IP configuration.
- Set up a NAT server.

3.3 Networking Topology Overview



1. **Intranet Setup**: R1 and R2 are within an intranet using private IPv4 addresses.
2. **Router Roles**:
    - R1: Client

- R2: Gateway for R1 and egress router to the public network

3. **Public Network Simulation**: R3 acts as the public network.

3.4 Configuration Steps

3.4.1 Basic Configurations

3.4.1.1 Assign IP addresses to interfaces on routers R1, R2, and R3.

R1:

```Markdown
[R1]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]ip address 192.168.1.1 24
```

R2:

```Markdown
[R2]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/3]ip address 192.168.1.254 24
[R2]interface GigabitEthernet0/0/2
[R2-GigabitEthernet0/0/3]ip address 1.2.3.4 24
```

R3:

```Markdown
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 1.2.3.254 24
```

3.4.1.2 Configure static routes on routers to ensure connectivity.

R1:

```
[R1]ip route-static 0.0.0.0 0 192.168.1.254
```

R2:

```
[R2]ip route-static 0.0.0.0 0 1.2.3.254
```

3.4.1.3 Set up Telnet on R1 and R3 for verification purposes.

R1:

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
[R1-ui-vty0-4]q
[R1]aaa
[R1-aaa]local-user user1 password cipher huawei
[R1-aaa]local-user user1 service-type telnet
[R1-aaa]local-user user1 privilege level 3
```

R3:

```
[R3]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
[R1-ui-vty0-4]q
[R1]aaa
```

```
[R1-aaa]local-user user1 password cipher huawei
[R1-aaa]local-user user1 service-type telnet
[R1-aaa]local-user user1 privilege level 3
```

3.4.1.4 Test Connectivity

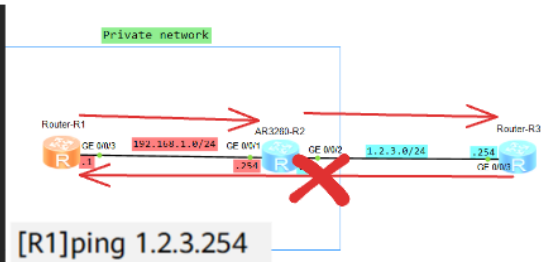
```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
100.00% packet loss
```

R1:

```
Markdown
[R1]ip route-static 0.0.0.0 0 192.168.1.254
```

R2:

```
Markdown
[R2]ip route-static 0.0.0.0 0 1.2.3.254
```



[R1]ping 1.2.3.254

it will not success because when ping reach R3 but R3 doesnt know the path for R1 so the pining message goes unsuccessful

```
[R2]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
```

3.4.2 Dynamic NAT Configuration

> Configure a NAT address pool on R2 with the range 1.2.3.10 to 1.2.3.20. Associate an ACL with the NAT address pool on GigabitEthernet0/0/4 of R2.

R2:

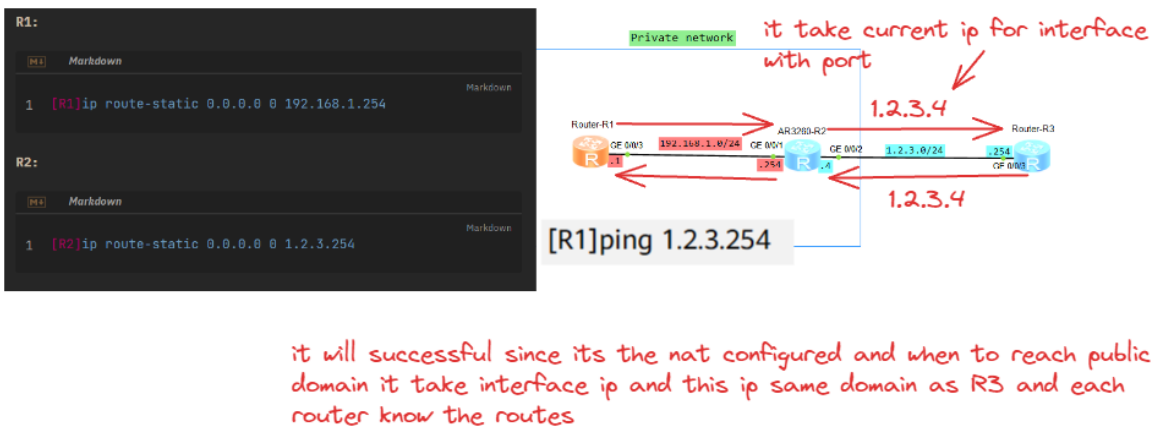
Markdown

```
1 [R2]nat address-group 1 1.2.3.10 1.2.3.20
```

```
[R2]acl 2000
[R2-acl-basic-2000]rule 10 permit source any
[R2-acl-basic-2000]q
[R2]int gig0/0/2
[R2-GigabitEthernet0/0/2]nat outbound 2000 address-group 1
```

3.4.2.1 Test Connectivity

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=20 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 20/32/60 ms
```



```
<R1>telnet 1.2.3.254
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.254 ...
  Connected to 1.2.3.254 ...
Login authentication


Username:test
Password:
<R3>
```

```
[R2]display nat session all
  NAT Session Table Information:
    Protocol               : TCP(6)
    SrcAddr    Port Vpn    : 192.168.1.1     62185      //Source IP address and source port before NAT
    DestAddr   Port Vpn    : 1.2.3.254       23
    NAT-Info
    New SrcAddr            : 1.2.3.11                   //Source IP address after NAT
    New SrcPort            : 49149                      //Source port after NAT
    New DestAddr           : ----
    New DestPort           : ----

  Total : 1
```

NAT table

3.4.3 Easy IP Configuration

If GigabitEthernet0/0/4 on R2 has a dynamically assigned IP (e.g., DHCP), Easy IP is configured instead:

R2:

Markdown

```
[R2-GigabitEthernet0/0/2]nat outbound 2000
```

3.4.3.1 Test Connectivity

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/30/30 ms
```

> Easy IP NAT same as PAT to provide you with map multiple private ip within one public since its use port with public ip

```
[R2]display nat session all
 NAT Session Table Information:
      Protocol               : TCP(6)
      SrcAddr   Port Vpn     : 192.168.1.1      58546          //Source IP address and source port before
NAT
      DestAddr Port Vpn      : 1.2.3.4      23
      NAT-Info
      New SrcAddr            : 1.2.3.4     //Source IP address after NAT, that is, the address of GigabitEthernet
0/0/4 on R2
      New SrcPort            : 49089              //Source port after NAT
      New DestAddr           : ----
      New DestPort           : ----

  Total : 1
```

3.4.4 NAT Server Setup

> This allows access from external users to internal services by configuring a mapping table:

Markdown

```
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2] nat server protocol tcp
global current-interface telnet inside 192.168.1.1
telnet
```

> Establishing a static NAT configuration on the router where the `current-interface` term implies that the NAT will utilize the IP address of the interface it is applied to. The `inside` designation corresponds to the private IP addresses within our network that will be mapped to a global (public) IP address or interface for outbound communication.

3.4.4.1 Test Connectivity

```
<R3>telnet 1.2.3.4 2323
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.4 ...
  Connected to 1.2.3.4 ...

Login authentication


Username:test
Password:
<R1>
```

```
[R2]display nat session all
        Protocol                : TCP(6)
        SrcAddr    Port Vpn     : 1.2.3.254      61359
        DestAddr Port Vpn       : 1.2.3.4        2323          //Destination IP address and port before
NAT
        NAT-Info
        New SrcAddr             : ----
```

3.5 Quiz

Question1

When configuring NAT Server, should the destination ports before translation be the same as those after translation

Answer1

NAT Server configuration doesn't require matching external and internal ports. Different ports can enhance security or support multiple services on

one IP. External users connect using designated ports, which NAT translates to the server's actual internal ports.