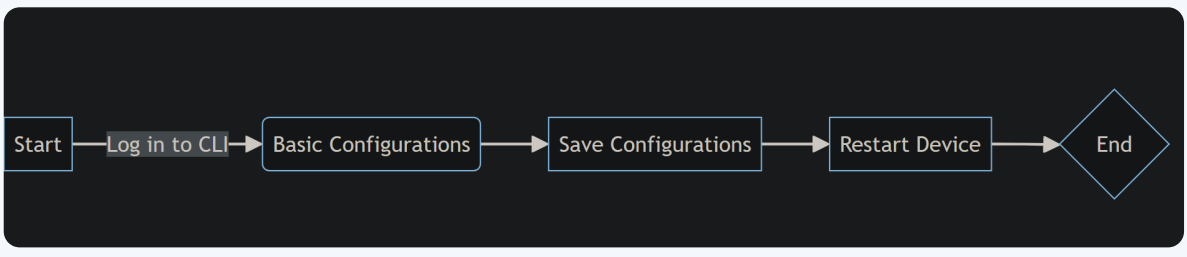
Lab1

1 Lab1 Huawei VRP and Configuration Basics

1.1 Lab Configuration Overview

- **Steps**:
  1. Configure device name and interface IP.
  2. Save configurations.
  3. Restart the device.

1.2 Configuration Roadmap



1.3 Basic Device Configurations

1.3.1 Step-by-Step Guide

1.3.1.1 Step 1: Logging In

- Access the Command Line Interface (CLI) through the console port.

1.3.1.2 Step 2: Displaying Basic Info

```Markdown
<Huawei>display version
```

> Check device version and uptime.

```
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.110 (eNSP V100R001C00)
Copyright (c) 2000-2011 HUAWEI TECH CO., LTD
```

1.3.1.3 Step 3: Setting Up Basic Configurations

```Markdown
<Huawei>system-view
[Huawei]sysname Datacom-Route
```

> Enter system view.

> Change router name.

1.3.1.4 Interface IP Configuration

```Markdown
[Datacom-Router]interface GigabitEthernet0/0/1
[Datacom-Router-GigabitEthernet0/0/1]ip address
192.168.1.1 24
```

> Go to interface view.

> Set IP address for the interface.

1.3.1.5 Undo Configuration

```Markdown
[Datacom-Router-GigabitEthernet0/0/1]undo ip address
```

> Remember to negate incorrect configurations with `undo` command if necessary.

1.3.1.6 Keys

> **`tab`**：When typed into the CLI, pressing the Tab key can autocomplete commands or list available commands if there's more than one option.

> **`?`**：prompts the user for additional information or indicates an error or unknown command in the network simulation environment.

```
[Datacom-Router]inter?
  interface
```

<cr> : Stands for "Carriage Return" and is often shown in command-line help to indicate that you should press the Enter key to execute the command as it is.

1.3.1.7 Display and navigation

---

display this : Displays the configuration of the current module/view you're in. For instance, if you're in a specific interface configuration view, it would display the settings for that interface.

```
[Datacom-Router-GigabitEthernet0/0/1]dis this
#
interface GigabitEthernet0/0/1
 ip address 192.168.100.1 255.255.255.0
#
return
```

quit : Exits from the current mode or goes back one level in the command hierarchy (e.g., from interface configuration mode back to global configuration mode).

display current-configuration : to review settings.

```
#
sysname Datacom-Router
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher OOCM4m($F4ajUn1vMEIBNUw#
 local-user admin service-type http
#
firewall zone Local
 priority 16
#
interface Ethernet0/0/0
```

1.3.1.8 Basic startup

`compare configuration` : This command allows you to compare the current running configuration with another saved configuration file to see what changes have been made.

`dir` : Lists the contents of a directory on a file system, such as flash memory.

```
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time        FileName
    0  drw-             -  Aug 07 2015 13:51:14   src
    1  drw-             -  Apr 09 2024 23:06:50   pmdata
    2  drw-             -  Apr 09 2024 23:06:56   dhcp
    3  -rw-            28  Apr 09 2024 23:06:56   private-dat
    4  drw-             -  Apr 09 2024 23:22:01   mplstpoam

32,004 KB total (31,994 KB free)
```

configuration file The filename extension of a configuration file must be .cfg or .zip

system software The filename extension of system software must be .c

`startup saved-configuration` : This might not be a valid Huawei command as written; however, if referring to viewing startup configurations, it would typically be something like `display startup-config` , which shows you the saved startup configuration that will be used upon next boot.

`display startup` : This is another way to show the system's startup configuration file—what has been saved and will be loaded upon next restart.

```
MainBoard:
  Configured startup system software:        NULL
  Startup system software:                   NULL
  Next startup system software:              NULL
  Startup saved-configuration file:          NULL
  Next startup saved-configuration file:     NULL
  Startup paf file:                          NULL
  Next startup paf file:                     NULL
  Startup license file:                      NULL
  Next startup license file:                 NULL
  Startup patch package:                     NULL
  Next startup patch package:                NULL
```

`reset saved-configuration` : Deletes the current saved configuration so that when you reboot, it will start with default settings (be very careful with this command as it erases your saved setup).

⚠️ **Important**: After `reset saved-configuration` , ensure that you save your desired startup configuration before rebooting.

1.3.1.9 Step 4: Saving Configurations

```Markdown
<Datacom-Router>save
```

> Save current configuration after confirmation.

1.3.2 Restart Procedure

```Markdown
<Datacom-Router>reboot
```

> Command for restarting the device.

1.4 Function Keys Table

Key	Function
Ctrl+A	Moves cursor to beginning of line
Ctrl+B	Moves cursor back one character
Ctrl+C	Stops current functions
Ctrl+D	Deletes character at cursor
Ctrl+E	Moves cursor to end of line
Ctrl+F	Moves the cursor forward one character
Ctrl+H	Deletes the character to the left of the cursor
Ctrl+K	Terminates the connection of an outgoing call during connection establishment.
Ctrl+N or Down Arrow Key	Displays the next command in the command history.
Ctrl+P or Up Arrow Key	Displays the previous command in the command history.
Ctrl+T	Enters a question mark (?).

Key	Function
Ctrl+W	Deletes the character string (word) to the left of the cursor
Ctrl+X	Deletes all characters on the left of the cursor
Ctrl+Y	Deletes the character at the cursor and all characters to the right
Ctrl+Z	Returns to user view
Ctrl+]	Stops or redirects incoming connections
Esc+B	Moves the cursor back one character string (word)
Esc+D	Deletes one character string (word) to the right of the cursor

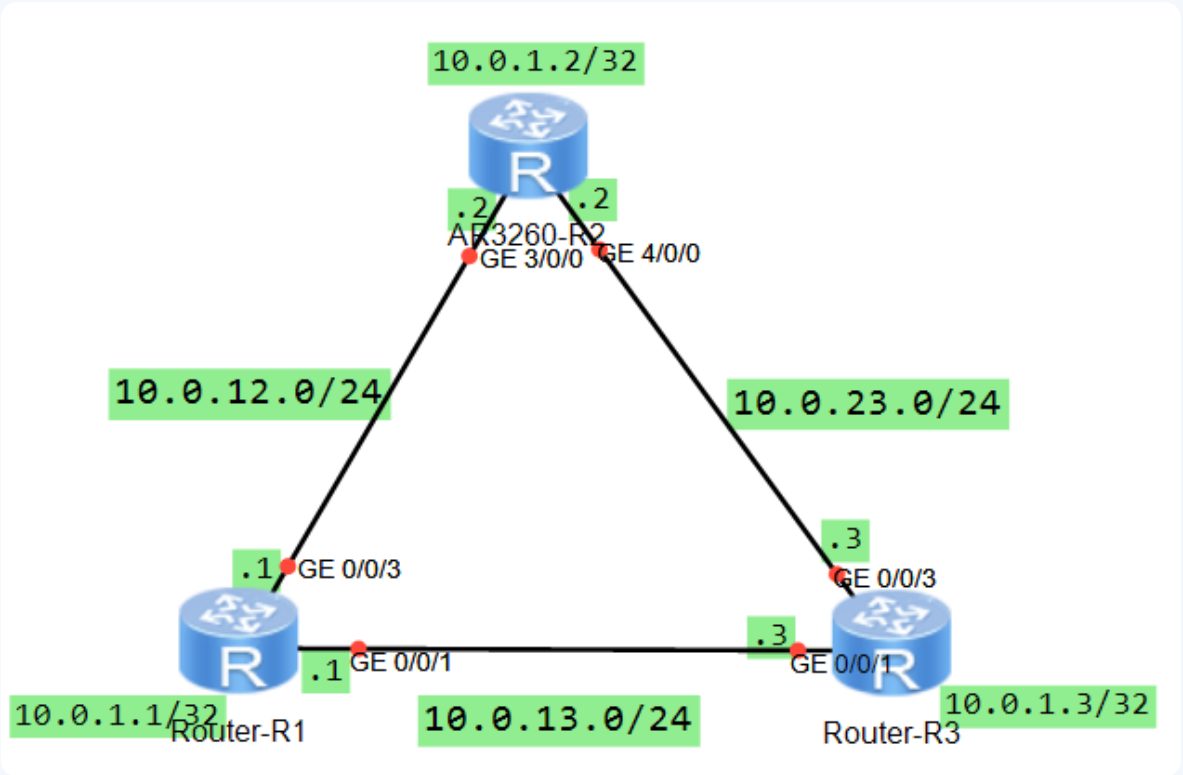
> in my version of Ensp most of the shortcuts don't working

Lab2

1 Lab2 part1 IPv4 Addressing and Routing

1.1 Overview

> This lab focuses on configuring static routes and testing connectivity between loopback interfaces on Huawei routers.



1.2 Equipment Setup

Three routers R1, R2, and R3 are used with loopback interfaces simulating clients.

1.3 Interface Configuration

Device	Interface	IP Address	Subnet Mask
R1	Loopback0	10.0.1.1	/32
R1	Gig0/0/1	10.0.13.1	/24
R1	Gig0/0/3	10.0.12.1	/24
R2	Loopback0	10.0.1.2	/32
R2	Gig3/0/	10.0.12.2	/24
R2	Gig4/0/0	10.0.23.2	/24
R3	Loopback0	10.0.1.3	/32
R3	Gig0/0/1	10.0.13.3	/24
R3	Gig0/0/3	10.0.23.3	/24

1.3.1 R1 Configuration

```markdown
<1>system-view
[1]interface GigabitEthernet0/0/3
[1-GigabitEthernet0/0/3]ip address 10.0.12.1 24
[1-GigabitEthernet0/0/3]interface GigabitEthernet0/0/1
[1-GigabitEthernet0/0/1]ip address 10.0.13.1 24
[1-GigabitEthernet0/0/1]interface LoopBack0
[R1-LoopBack0]ip address 10.0.1.1 32
```

> This sets up the IP addresses for R1's interfaces with subnet masks and configures a loopback interface.

1.3.2 R2 Configuration

```Markdown
<R2>system-view
[R2]interface GigabitEthernet3/0/0
[R2-GigabitEthernet3/0/0]ip address 10.0.12.2 24
[R2-GigabitEthernet3/0/0]interface GigabitEthernet4/0/0
[R2-GigabitEthernet4/0/0]ip address 10.0.23.2 24
[R2-GigabitEthernet4/0/0]interface LoopBack0
[R2-LoopBack0]ip address 10.0.1.2 32
```

> This sets up the IP addresses for R2's interfaces with subnet masks and configures a loopback interface.

1.3.3 R3 Configuration

```Markdown
<R3>system-view
[R3]interface GigabitEthernet0/0/3
[R3-GigabitEthernet0/0/3]ip address 10.0.23.3 24
[R3-GigabitEthernet0/0/3]interface GigabitEthernet0/0/1
[R3-GigabitEthernet0/0/1]ip address 10.0.13.3 24
[R3-GigabitEthernet0/0/1]interface LoopBack0
[R3-LoopBack0]ip address 10.0.1.3 32
```

> This sets up the IP addresses for R3's interfaces with subnet masks and configures a loopback interface.

1.3.4 Connectivity Tests

```
<Huawei>ping 10.0.12.2
  PING 10.0.12.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.12.2: bytes=56 Sequence=1 ttl=255 time=90 ms
    Reply from 10.0.12.2: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 10.0.12.2: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 10.0.12.2: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 10.0.12.2: bytes=56 Sequence=5 ttl=255 time=50 ms

  --- 10.0.12.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/46/90 ms
```

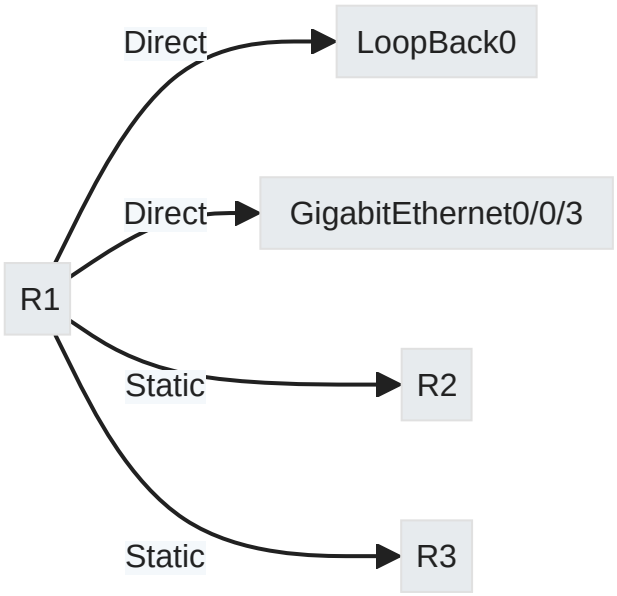
```
<Huawei>ping 10.0.13.3
  PING 10.0.13.3: 56  data bytes, press CTRL_C to break
    Reply from 10.0.13.3: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 10.0.13.3: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 10.0.13.3: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 10.0.13.3: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.13.3: bytes=56 Sequence=5 ttl=255 time=10 ms

  --- 10.0.13.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/30/50 ms
```

1.4 Routing Table Analysis

Destinations : 10 Routes : 10

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.0.12.0/24	Direct	0	0	D	10.0.12.1	GigabitEthernet0/0/3
10.0.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.12.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/3
10.0.13.0/24	Direct	0	0	D	10.0.13.1	GigabitEthernet0/0/1
10.0.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
10.0.13.255/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

Routing table for direct connect



> **Note**
>
> Direct routes are automatically generated for local interfaces.

1.5 Connectivity Tests

Test Connectivity for Loopback

```Markdown
[R1]ping -a 10.0.1.1 10.0.1.2
```

```
ping –a <source-ip-address> <destination-ip-addr>
```

```
PING 10.0.1.2: 56  data bytes, press CTRL_C to break
   Request time out
   Request time out
   Request time out
   Request time out
   Request time out

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

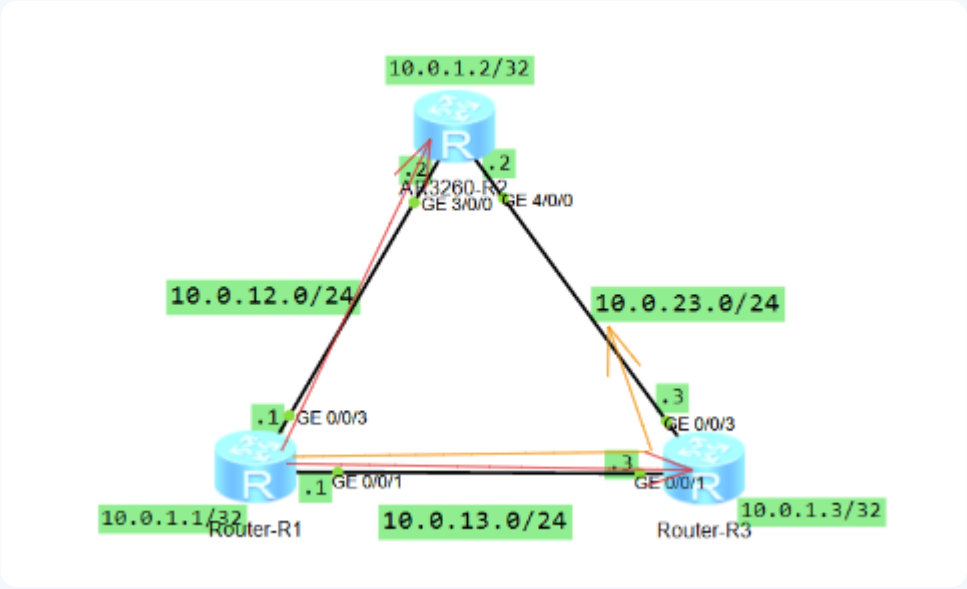
> It fail since router doesn't know the path for loopback you need to configure it either manually of using routing protocol

1.6 Static Routes Configuration

1.6.1 On R1:

Markdown

```
[R1]ip route-static 10.0.23.0 24 10.0.13.3
[R1]ip route-static 10.0.1.3 32 10.0.13.3
[R1]ip route-static 10.0.1.2 32 10.0.12.2
```

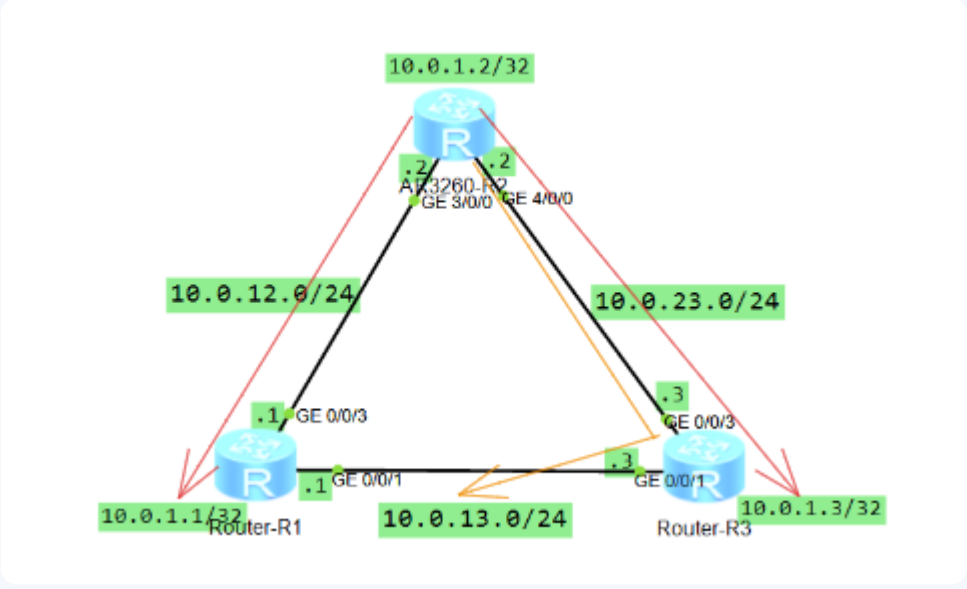


Route to network `10.0.23.0` and loopback `10.0.1.3` and `10.0.1.2`

1.6.2 On R2:

Markdown

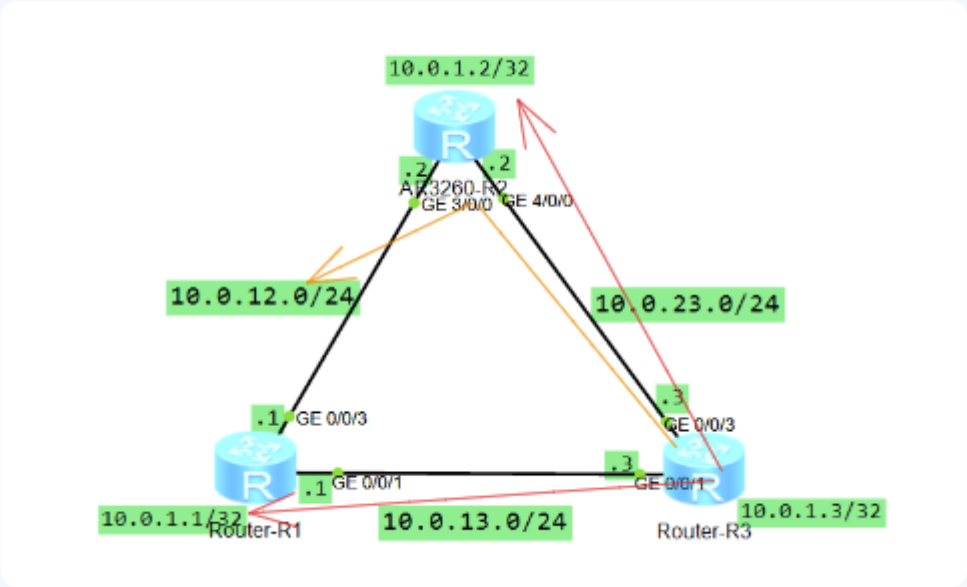
```
[R2]ip route-static 10.0.13.0 24 10.0.23.3
[R2]ip route-static 10.0.1.3 32 10.0.23.3
[R2]ip route-static 10.0.1.1 32 10.0.12.1
```



> Route to network `10.0.13.0` and loopback `10.0.1.3` and `10.0.1.1`

1.6.3 On R3:

```
Markdown
1 [R3]ip route-static 10.0.12.0 24 10.0.23.2
2 [R3]ip route-static 10.0.1.2 32 10.0.23.2
3 [R3]ip route-static 10.0.1.1 32 10.0.13.1
```



> Route to network `10.0.12.0` and loopback `10.0.1.2` and `10.0.1.1`

> After configuration, connectivity between loopback interfaces is successful.

1.6.4 Display connectivity

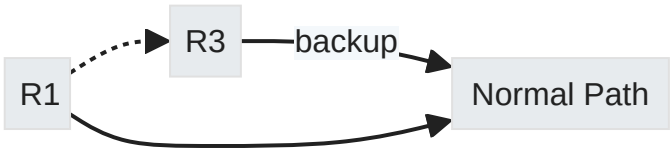
```
<Huawei>ping -a 10.0.1.1 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=255 time=110 ms
    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=255 time=50 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/48/110 ms
```

1.6.5 Display IP routing and Interfaces

```
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.1.2/32  Static  60   0          RD   10.0.12.2       GigabitEthernet
0/0/3
        10.0.1.3/32  Static  60   0          RD   10.0.13.3       GigabitEthernet
0/0/1
       10.0.12.0/24  Direct  0    0           D   10.0.12.1       GigabitEthernet
0/0/3
       10.0.12.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/3
       10.0.13.0/24  Direct  0    0           D   10.0.13.1       GigabitEthernet
0/0/1
       10.0.13.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
       10.0.23.0/24  Static  60   0          RD   10.0.13.3       GigabitEthernet
0/0/1
       127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

```
Interface                         IP Address/Mask      Physical   Protocol
Ethernet0/0/0                     unassigned           down       down
Ethernet0/0/1                     unassigned           down       down
GigabitEthernet0/0/0              unassigned           down       down
GigabitEthernet0/0/1              10.0.13.1/24         up         up
GigabitEthernet0/0/2              unassigned           down       down
GigabitEthernet0/0/3              10.0.12.1/24         up         up
LoopBack0                         10.0.1.1/32          up         up(s)
NULL0                             unassigned           up         up(s)
Serial0/0/0                       unassigned           down       down
Serial0/0/1                       unassigned           down       down
Serial0/0/2                       unassigned           down       down
Serial0/0/3                       unassigned           down       down
```

1.7 Backup Path Configuration

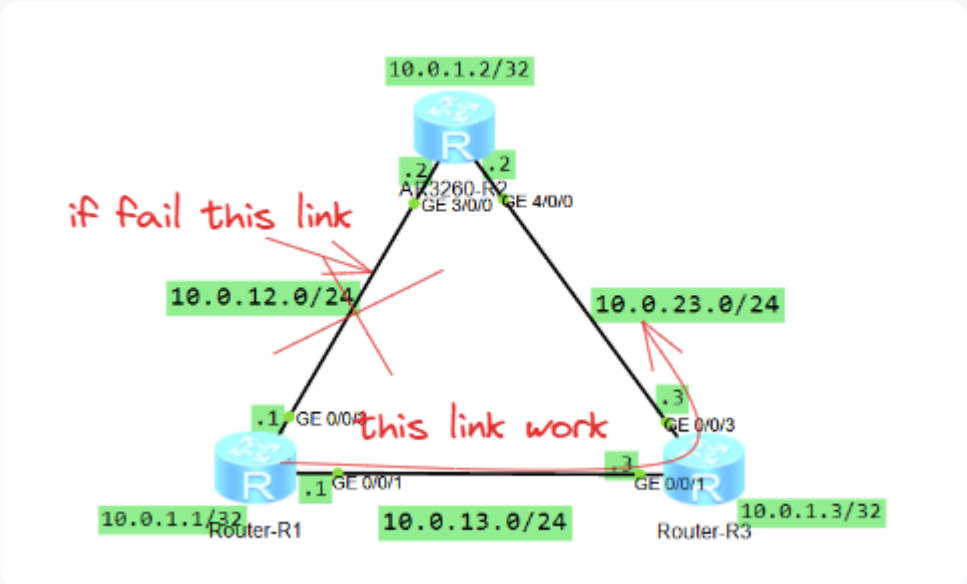


Ensure backup paths have lower priority by setting preference value higher than the normal path routing preference.

1.7.1 R1

Markdown

```
[R1]ip route-static 10.0.23.0 24 10.0.12.2 pre 100
```

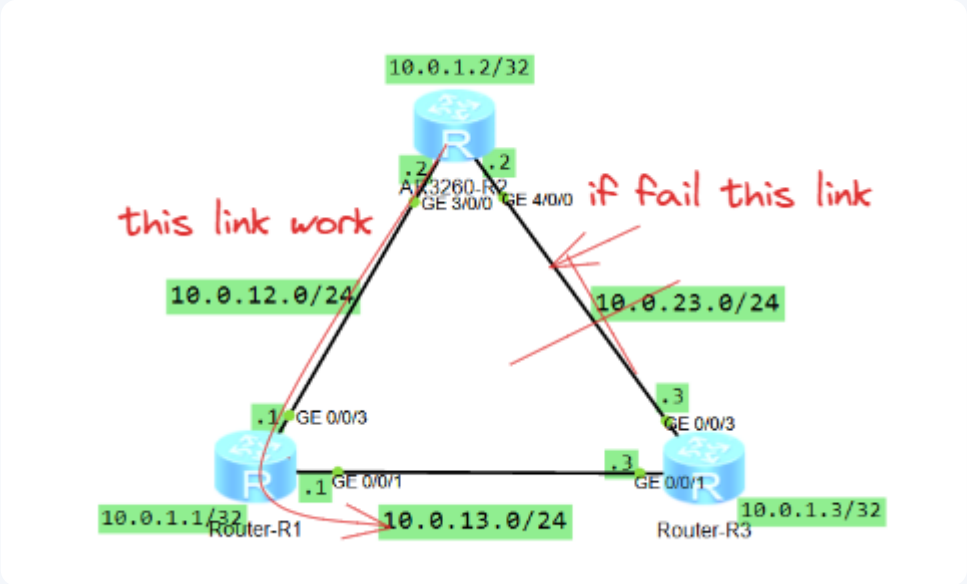


> Backup path to `10.0.23.0` via R3

1.7.2 R2

Markdown

```
[R1]ip route-static 10.0.13.0 24 10.0.12.1 pre 100
```

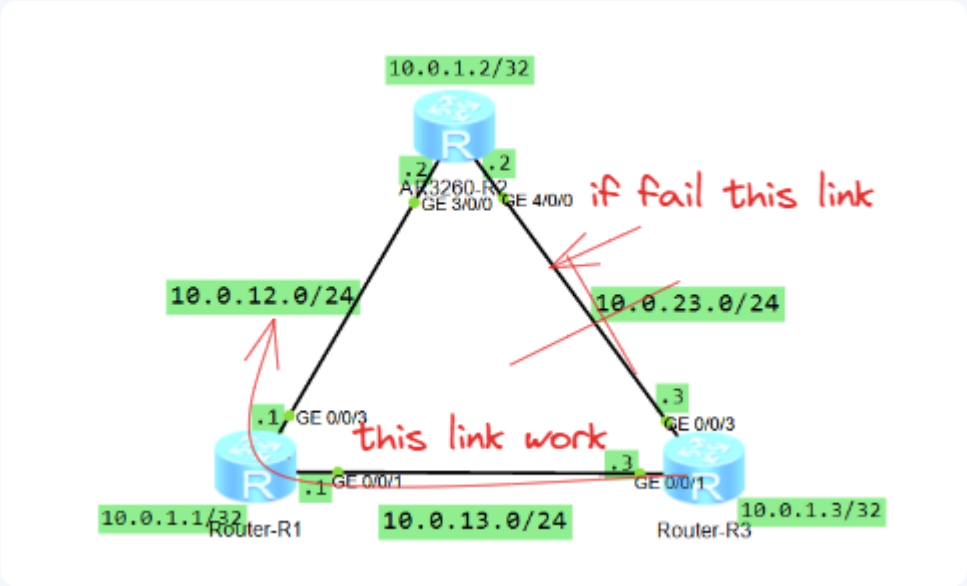


Backup path to `10.0.13.0` via R1

1.7.3 R3

Markdown

```
[R1]ip route-static 10.0.12.0 24 10.0.13.1 pre 100
```



Backup path to `10.0.12.0` via R1

1.7.4 Display routing and connectivity

```
[R1]display IP routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        10.0.1.2/32  Static  100  0           RD  10.0.13.3       GigabitEthernet0/0/1
        10.0.1.3/32  Static  60   0           RD  10.0.13.3       GigabitEthernet0/0/1
       10.0.13.0/24  Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
       10.0.13.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
     10.0.13.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
        127.0.0.0/8  Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

When the primary link is failed the backup link goes up

```
[R1]ping -a 10.0.1.1 10.0.1.2
  PING 10.0.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.0.1.2: bytes=56 Sequence=1 ttl=254 time=80 ms
    Reply from 10.0.1.2: bytes=56 Sequence=2 ttl=254 time=60 ms
    Reply from 10.0.1.2: bytes=56 Sequence=3 ttl=254 time=60 ms
    Reply from 10.0.1.2: bytes=56 Sequence=4 ttl=254 time=110 ms
    Reply from 10.0.1.2: bytes=56 Sequence=5 ttl=254 time=80 ms

  --- 10.0.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 60/78/110 ms
```

Successful connection with backup link

```
[R1]tracert -a 10.0.1.1 10.0.1.2

traceroute to  10.0.1.2(10.0.1.2), max hops: 30 ,packet length: 40,press CTRL_C to break

1 10.0.13.3 40 ms  30 ms  50 ms

2 10.0.23.2 80 ms  80 ms  60 ms
```

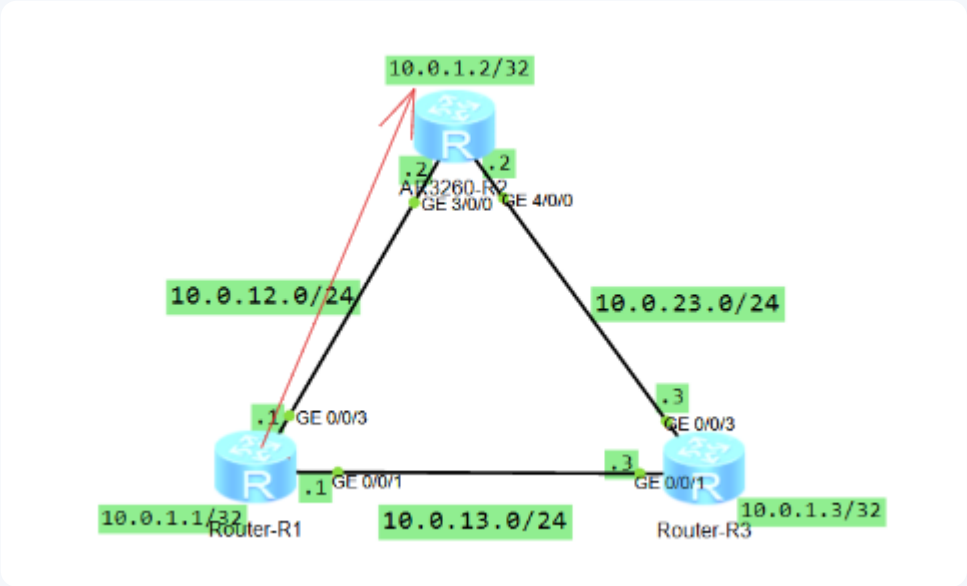
The `tracert` command displays the path of packets from the source to the destination

1.8 Configure a default route on R

Replace static route with default route

Markdown

```
1 [R1]ip route-static 0.0.0.0 0 10.0.12.2
```



Default route to reach loopback `R2`

1.8.1 Display routing

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD  10.0.12.2       GigabitEthernet0/0/3
       10.0.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.1.3/32  Static  60   0           RD  10.0.13.3       GigabitEthernet0/0/1
      10.0.12.0/24  Direct  0    0           D   10.0.12.1       GigabitEthernet0/0/3
      10.0.12.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
    10.0.12.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
      10.0.13.0/24  Direct  0    0           D   10.0.13.1       GigabitEthernet0/0/1
      10.0.13.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
    10.0.13.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

1.9 Quiz Review

Question1

When will static routes be added to the IP routing table?

Answer1

Static routes are added when the next-hop is reachable unless configured otherwise and This route is the optimal route to the destination network or host.

Question2

In step 3, if the -a argument is not specified during the connectivity test between loopback interfaces, what is the source IP address of ICMP packets? Why?

Answer2

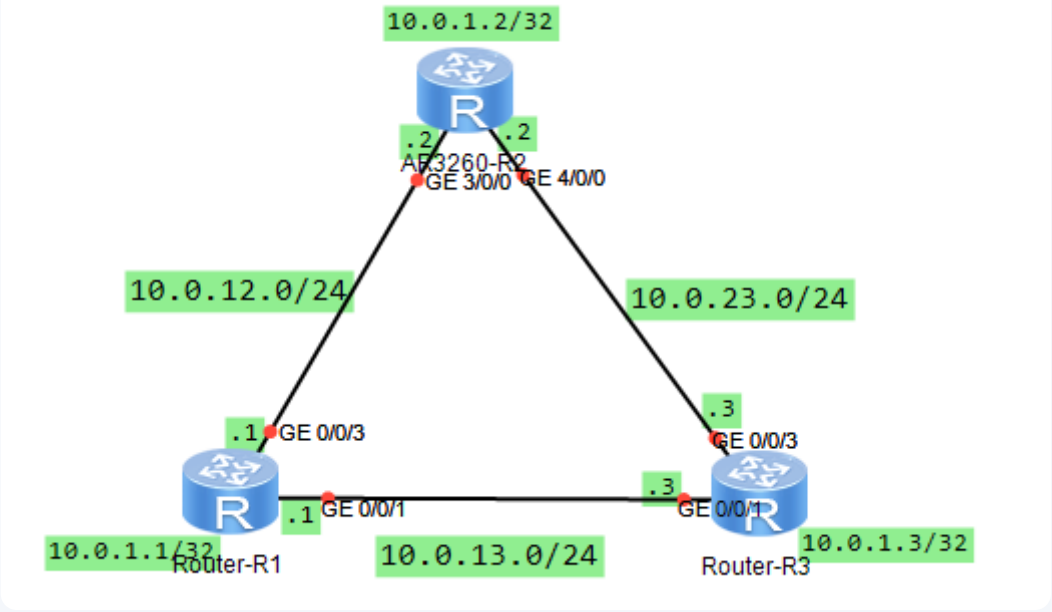
If `-a` argument is omitted in ping command, source IP will be chosen based on routing table entries which best match the destination IP.

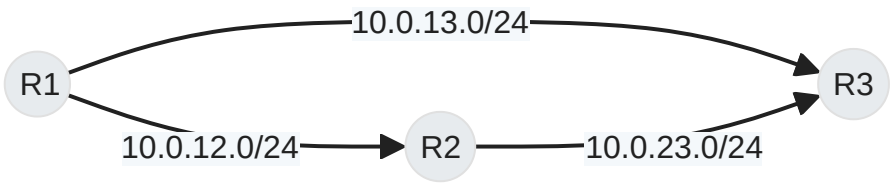
2 Lab2 part2 OSPF Routing

2.1 Overview

This note outlines the steps for configuring OSPF (Open Shortest Path First) on Huawei routers, including basic setup, authentication, default route advertisement, and cost adjustments.

2.2 Basic Device Configuration





- Set up router names.
- Configure IP addresses for physical and loopback interfaces.
- View the routing table using `display ip routing-table`.

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Direct  0    0           D  127.0.0.1       LoopBack0
       10.0.12.0/24  Direct  0    0           D  10.0.12.1       GigabitEthernet0/0/3
       10.0.12.1/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/3
     10.0.12.255/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/3
       10.0.13.0/24  Direct  0    0           D  10.0.13.1       GigabitEthernet0/0/1
       10.0.13.1/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/1
     10.0.13.255/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/1
        127.0.0.0/8  Direct  0    0           D  127.0.0.1       InLoopBack0
        127.0.0.1/32  Direct  0    0           D  127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D  127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D  127.0.0.1       InLoopBack0
```

Note: Initially, only direct routes exist on the device.

2.3 OSPF Process Creation

2.3.1 R1

Markdown

```
[R1]ospf 1 router-id 10.0.1.1
```

Create an OSPF process

default is 1 if not specified

2.3.2 R2

```
[R2]ospf 1
```

> Create an OSPF process

> default is 1 if not specified

2.3.3 R3

```
[R3]ospf 1 router-id 10.0.1.3
```

> Create an OSPF process

> default is 1 if not specified

2.4 Enable OSPF on Interfaces

2.4.1 R1

```
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 10.0.1.1 0.0.0.0
```

> **Define area and enable OSPF on interfaces when the following two conditions are:**

- The mask length of the interface's IP address is not shorter than that specified in the network command.
- The address of the interface must be within the network range specified in the network command.

2.4.2 R2

Markdown

```
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 10.0.1.1 0.0.0.0
```

> **Define area and enable OSPF on interfaces when the following two conditions are:**

- The mask length of the interface's IP address is not shorter than that specified in the network command.
- The address of the interface must be within the network range specified in the network command.

2.4.3 R3

Markdown

```
[R3-ospf-1]area 0
[R3-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R3-ospf-1-area-0.0.0.0]network 10.0.13.0 0.0.0.255
```

```
4 [R3-ospf-1-area-0.0.0.0]network 10.0.1.1 0.0.0.0
```

> **Define area and enable OSPF on interfaces when the following two conditions are:**

- The mask length of the interface's IP address is not shorter than that specified in the network command.
- The address of the interface must be within the network range specified in the network command.

2.4.4 Display the OSPF status

```
[R1]display ospf peer

         OSPF Process 1 with Router ID 10.0.1.1
                   Neighbors

 Area 0.0.0.0 interface 10.0.13.1(GigabitEthernet0/0/1)'s neighbors
 Router ID: 10.0.1.3             Address: 10.0.13.3
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 10.0.13.3  BDR: 10.0.13.1  MTU: 0
   Dead timer due in 36  sec
   Retrans timer interval: 0
   Neighbor is up for 00:00:30
   Authentication Sequence: [ 0 ]

                   Neighbors
Area 0.0.0.0 interface 10.0.12.1(GigabitEthernet0/0/3)'s neighbors
Router ID: 10.0.1.2             Address: 10.0.12.2
  State: Full  Mode:Nbr is  Master  Priority: 1
  DR: 10.0.12.2  BDR: 10.0.12.1  MTU: 0
  Dead timer due in 39  sec
  Retrans timer interval: 4
  Neighbor is up for 00:00:28
  Authentication Sequence: [ 0 ]
```

2.4.5 Display ip routing

```
[R1]display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Public routing table : OSPF
         Destinations : 3        Routes : 4

OSPF routing table status : <Active>
         Destinations : 3        Routes : 4

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.2/32  OSPF    10   1           D   10.0.12.2       GigabitEthernet0/0/3
        10.0.1.3/32  OSPF    10   1           D   10.0.13.3       GigabitEthernet0/0/1
       10.0.23.0/24  OSPF    10   2           D   10.0.13.3       GigabitEthernet0/0/1
                     OSPF    10   2           D   10.0.12.2       GigabitEthernet0/0/3

OSPF routing table status : <Inactive>
         Destinations : 0        Routes : 0
```

2.5 OSPF Authentication Configuration

```
[R1]display ospf peer brief

 OSPF Process 1 with Router ID 10.0.1.1
   Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id          Interface                     Neighbor id      State
 ----------------------------------------------------------------------------
 Total Peer(s):      0
```

> ⚠ **Warning**
>
> Ensure all routers have matching authentication settings to form neighbor relationships.

2.5.1 Interface Authentication Mode:

2.5.2 R1

```
[R1]int gig3/0/0
[R1-GigabitEthernet0/0/1]ospf authentication-mode md5 1 cipher Data
[R1-GigabitEthernet0/0/1]int gig4/0/0
[R1-GigabitEthernet0/0/4]ospf authentication-mode md5 1 cipher Data
```

> For each interface requiring authentication

2.5.3 Area Authentication Mode:

```
[R2-ospf-1-area-0.0.0.0]authentication-mode md5 1 cipher Data
```

> Repeat for every router

> Configure Authentication at the area level

2.5.4 Display Authentication interface

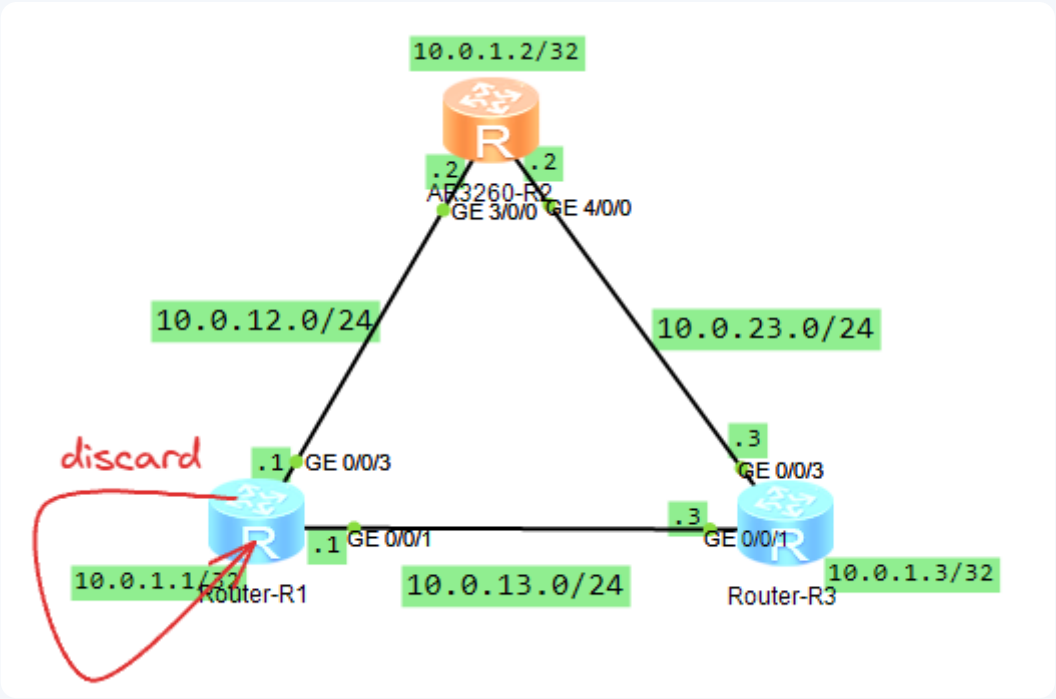
```
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
 ospf authentication-mode md5 1 cipher foCQTYsq-4.A\^38y!DVwQ0#
```

> Since the password is cipher text

2.6 Advertise Default Route in OSPF

Default Route:

```
Markdown
1 [R1]ip route-static 0.0.0.0 0.0.0.0 NULL0
```



> Path for every packet doesn't match the routes table then it will goes into null and it will be discarded

Advertise Default:

```
Markdown
1 [R1-ospf-1]default-route-advertise always
```

> Advertise default route in ospf process

> **Tip:** The 'always' keyword ensures advertisement regardless of active non-OSPF default routes.

2.6.1 Display ip routing table

```
[R2]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 15        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   10.0.12.1       GigabitEthernet0/0/3
       10.0.1.1/32  OSPF    10   1           D   10.0.12.1       GigabitEthernet0/0/3
       10.0.1.2/32  Direct  0    0           D   127.0.0.1       LoopBack0
       10.0.1.3/32  OSPF    10   1           D   10.0.23.3       GigabitEthernet0/0/4
      10.0.12.0/24  Direct  0    0           D   10.0.12.2       GigabitEthernet0/0/3
      10.0.12.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
    10.0.12.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
      10.0.13.0/24  OSPF    10   2           D   10.0.12.1       GigabitEthernet0/0/3
                    OSPF    10   2           D   10.0.23.3       GigabitEthernet0/0/4
      10.0.23.0/24  Direct  0    0           D   10.0.23.2       GigabitEthernet0/0/4
      10.0.23.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/4
    10.0.23.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/4
       127.0.0.0/8  Direct  0    0           D   127.0.0.1       InLoopBack0
       127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

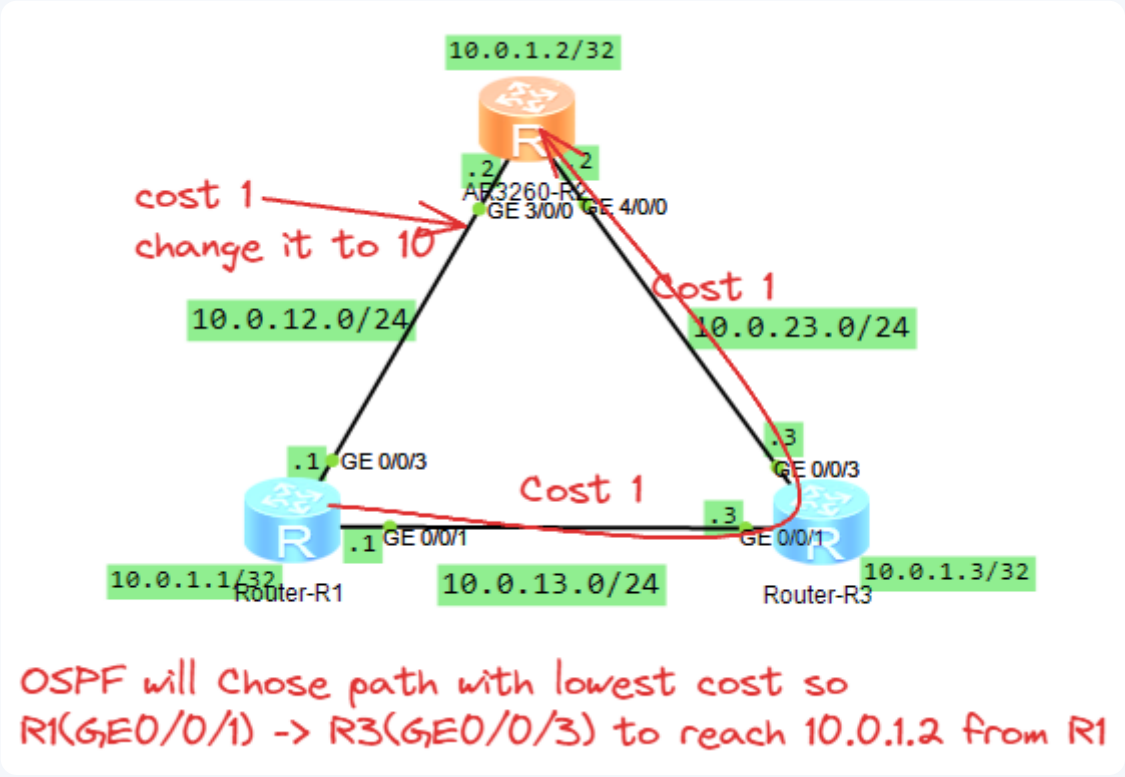
```
[R3]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 15        Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   O_ASE   150  1           D   10.0.13.1       GigabitEthernet0/0/1
       10.0.1.1/32  OSPF    10   1           D   10.0.13.1       GigabitEthernet0/0/1
       10.0.1.2/32  OSPF    10   1           D   10.0.23.2       GigabitEthernet0/0/3
       10.0.1.3/32  Direct  0    0           D   127.0.0.1       LoopBack0
      10.0.12.0/24  OSPF    10   2           D   10.0.23.2       GigabitEthernet0/0/3
                    OSPF    10   2           D   10.0.13.1       GigabitEthernet0/0/1
      10.0.13.0/24  Direct  0    0           D   10.0.13.3       GigabitEthernet0/0/1
      10.0.13.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
    10.0.13.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/1
      10.0.23.0/24  Direct  0    0           D   10.0.23.3       GigabitEthernet0/0/3
      10.0.23.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
    10.0.23.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet0/0/3
```

2.7 Adjusting OSPF Costs

To influence route selection:

Markdown

```
[R1]int gi0/0/3
[R1-GigabitEthernet0/0/3]ospf cost 10
```



Change the cost values of interfaces on R1 so that LoopBack0 on R1 can reach LoopBack0 on R2 via R3.

Check routing table with:

Markdown

```
[R1]display ip routing-table
```

```
[R1]display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14        Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        10.0.1.1/32  Direct  0    0           D  127.0.0.1       LoopBack0
        10.0.1.2/32  OSPF    10   2           D  10.0.13.3       GigabitEthernet0/0/1
        10.0.1.3/32  OSPF    10   1           D  10.0.13.3       GigabitEthernet0/0/1
       10.0.12.0/24  Direct  0    0           D  10.0.12.1       GigabitEthernet0/0/3
       10.0.12.1/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/3
     10.0.12.255/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/3
       10.0.13.0/24  Direct  0    0           D  10.0.13.1       GigabitEthernet0/0/1
       10.0.13.1/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/1
     10.0.13.255/32  Direct  0    0           D  127.0.0.1       GigabitEthernet0/0/1
       10.0.23.0/24  OSPF    10   2           D  10.0.13.3       GigabitEthernet0/0/1
        127.0.0.0/8  Direct  0    0           D  127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0           D  127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D  127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D  127.0.0.1       InLoopBack0
```

And verify path with traceroute:

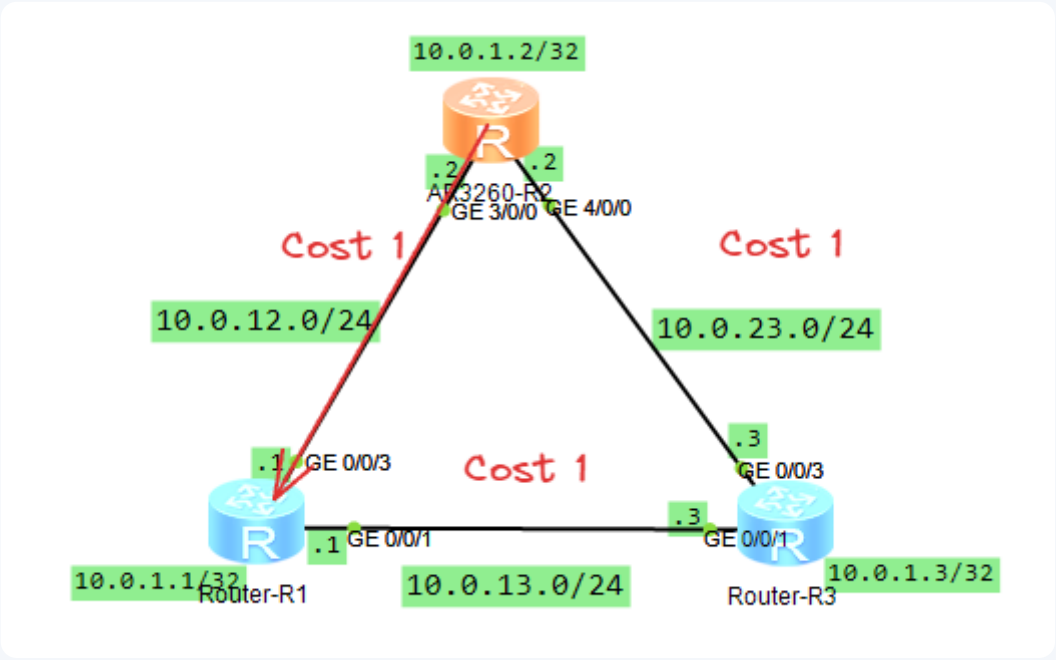
```
Markdown
1 [R1]tracert –a 10.0.1.1 10.0.1.2
```

```
[R1]tracert –a 10.0.1.1 10.0.1.2

traceroute to  10.0.1.2(10.0.1.2), max hops: 30 ,packet length: 40,press CTRL_C to break

1 10.0.13.3 40 ms  50 ms  50 ms

2 10.0.23.2 60 ms  110 ms  70 ms
```

2.8 Quiz Question Review

Question

Question: What is the path for R2 to return ICMP packets to R1?



✓ Success

Answer:

It will be through `GE0/0/3` , ip `10.0.12.2` since the change of cost is only for router 1 and it will not affect router 2 and router 3 so router 2 will choice path `GE0/0/3` with cost = 1 with lowest cost path

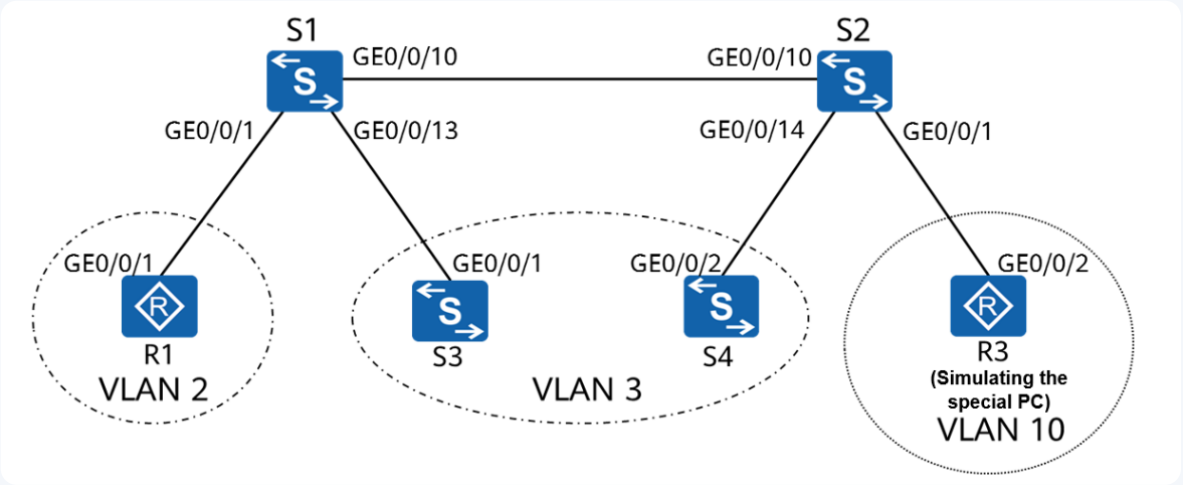
Lab3

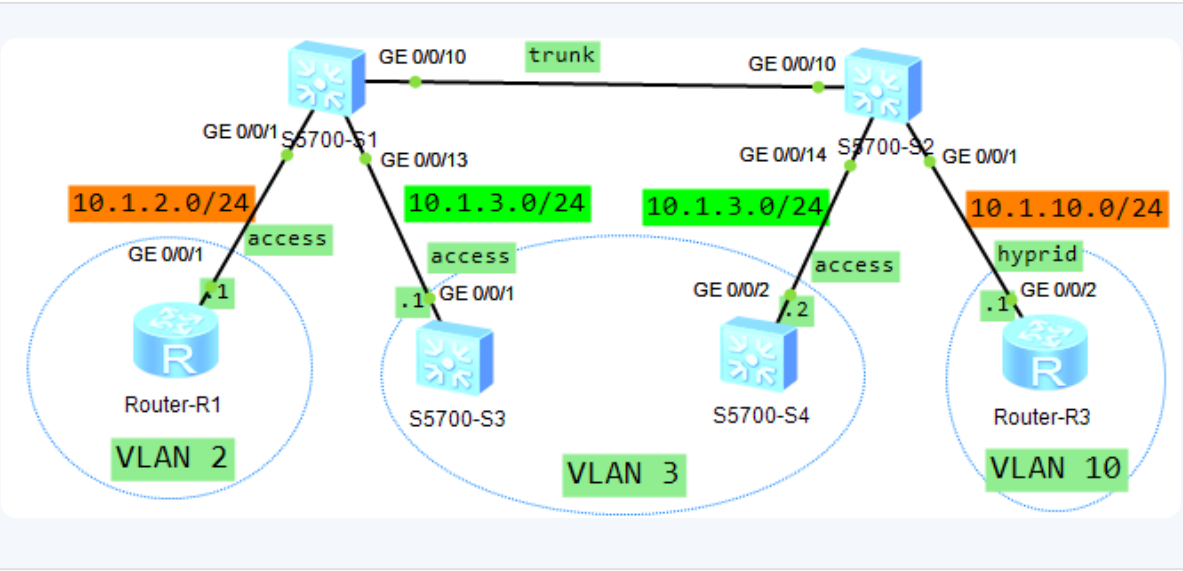
1 Lab3 Part1 Ethernet Basics and VLAN Configuration

1.1 In this lab

- Learn to set up VLANs on Huawei switches.
- Understand how to assign switch ports to VLANs as access, trunk, or hybrid.
- Configure VLAN membership either by port or MAC address.
- Review the MAC address table and VLAN configurations.

1.2 Topology





1.3 Step 1: Interface Shutdown

> Shut down unused interfaces for security purposes(By default all link is shutdown state).

1.4 Step 2: Configure Device IP Addresses

> Assign IP addresses to router and switch interfaces.

Device	Interface	IP Address	Mode
R1	GigabitEthernet0/0/1	10.1.2.1/24	Layer 3

Device	Interface	IP Address	Mode
R3	GigabitEthernet0/0/2	10.1.10.1/24	Layer 3
S3	GigabitEthernet0/0/1	10.1.3.1/24	Layer 3 (if supported)
S4	GigabitEthernet0/0/2	10.1.3.2/24	Layer 3 (if supported)

1.4.1 R1

```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 10.1.2.1 24
```

1.4.2 R3

```
[R3]interface GigabitEthernet0/0/2
[R3-GigabitEthernet0/0/2]ip address 10.1.10.1 24
```

1.4.3 S3 & S4

1.4.3.1 For Scenario 1:

If S3 and S4 support Multi layer switching from Layer 2 interfaces to Layer 3:

```
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]undo portswitch
[S3-GigabitEthernet0/0/1]ip address 10.1.3.1
```

> Convert Switching from layer 2 to Layer 3 mode.

> This step for S3 and S4

1.4.3.2 For Scenario 2:

If S3 and S4 do not support Layer 3 mode:

```Markdown
[S3]vlan batch 3
[S3]interface GigabitEthernet0/0/1
[S3-GigabitEthernet0/0/1]port link-type access
[S3-GigabitEthernet0/0/1]port default vlan 3
[S3]interface Vlanif 3
[S3-Vlanif3]ip address 10.1.3.1 24
```

> Create VLAN and assign ports. Since the switch doesn't support l3 mode so ,you should assign ip with virtual interface `vlanif` since the switches in this topology act like end devices

> This step for S3 and S4

1.5 Step 3: Create VLANs on Switches S1 and S2

```Markdown
[S1]vlan batch 2 3 10
```

> It will be used in trunk port to allow particular vlan tag to be passed

> This step for S1 and S2

1.6 Step 4: Configure Port-Based VLANs

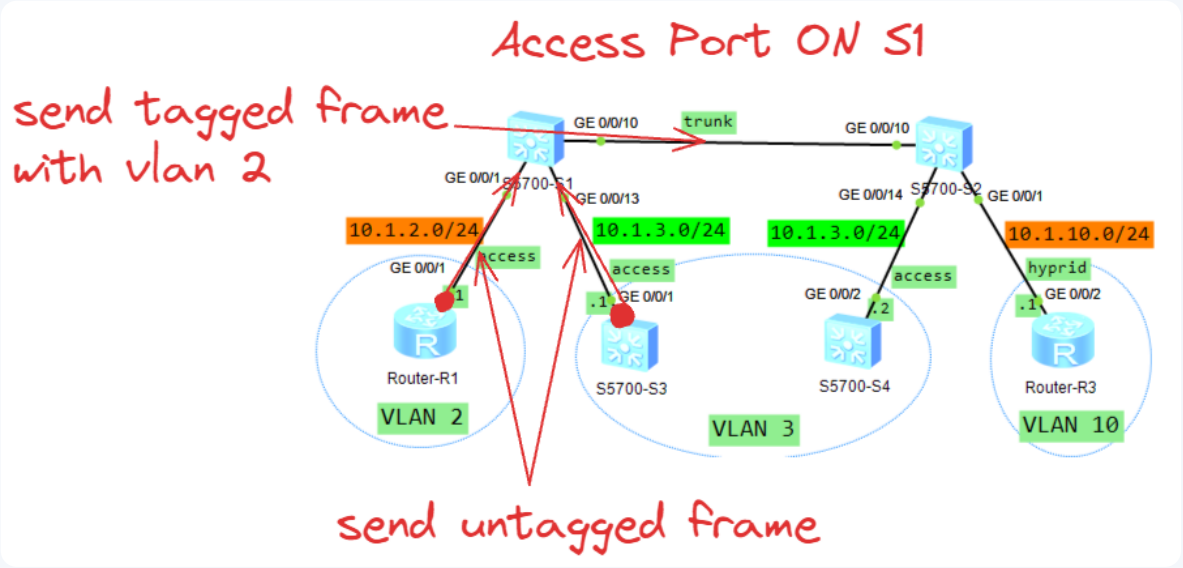
> Access ports are configured for end devices; trunk ports are configured between switches.

1.6.1 Access Ports Configuration:

1.6.1.1 S1

Markdown

```
[S1]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 2
[S1-GigabitEthernet0/0/1]int gig0/0/13
[S1-GigabitEthernet0/0/13]port link-type access
[S1-GigabitEthernet0/0/13]port default vlan 3
```



> Access port for end user since end user doesn't know how to read vlan frame so `port default vlan` is responsible to make it frame without vlan and vice visa

1.6.1.2 S2

Markdown

```
[S2]interface GigabitEthernet0/0/14
[S2-GigabitEthernet0/0/14]port link-type access
[S2-GigabitEthernet0/0/14]port default vlan 3
```

> Access port for end user since end user doesn't know how to read vlan frame so `port default vlan` is responsible to make it frame without vlan and vice visa

1.6.1.3 S3

Markdown

```
[S3]interface GigabitEthernet0/0/1
```

```
[S3-GigabitEthernet0/0/1]port link-type access
[S3-GigabitEthernet0/0/1]port default vlan 3
```

> Access port for end user since end user doesn't know how to read vlan frame so `port default vlan` is responsible to make it frame without vlan and vice visa

1.6.1.4 S4

Markdown

```
[S4]interface GigabitEthernet0/0/2
[S4-GigabitEthernet0/0/2]port link-type access
[S4-GigabitEthernet0/0/2]port default vlan 3
```

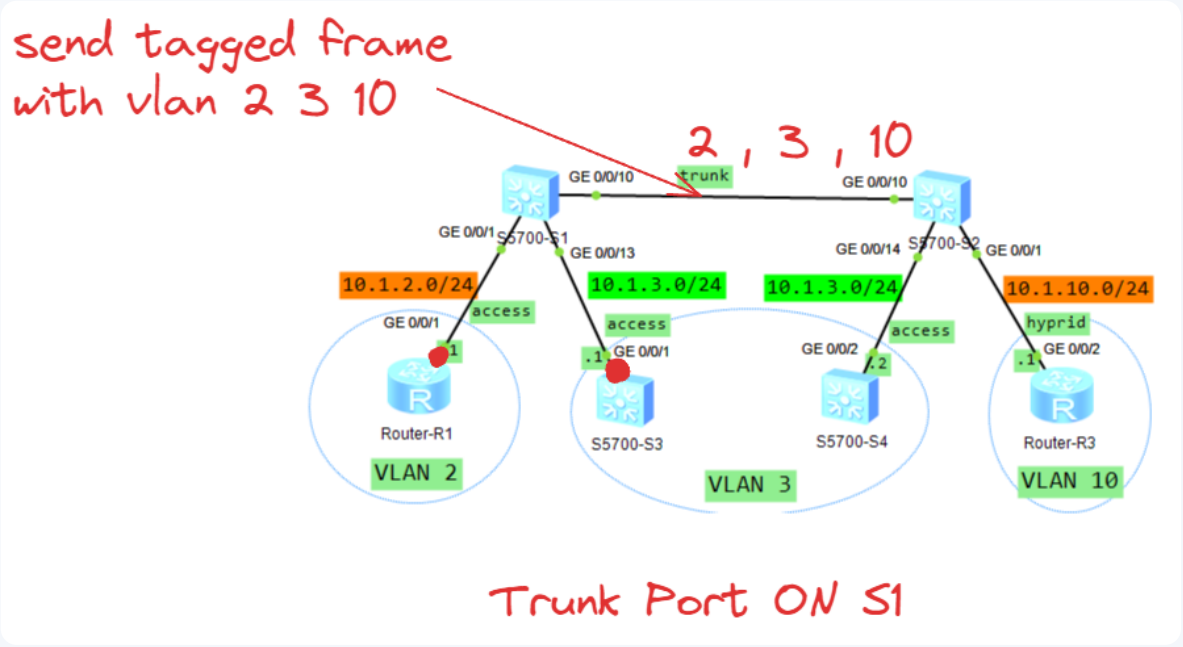
> Access port for end user since end user doesn't know how to read vlan frame so `port default vlan` is responsible to make it frame without vlan and vice visa

1.6.2 Trunk Ports Configuration:

1.6.2.1 S1

Markdown

```
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 2
3 10
[S1-GigabitEthernet0/0/10]undo port trunk allow-pass
vlan 1
```



1.6.2.2 S2

Markdown

```
[S2]interface GigabitEthernet0/0/10
[S2-GigabitEthernet0/0/10]port link-type trunk
[S2-GigabitEthernet0/0/10]port trunk allow-pass vlan 2 3 10
[S2-GigabitEthernet0/0/10]undo port trunk allow-pass vlan 1
```

> On ports connecting switches to carry vlan frame

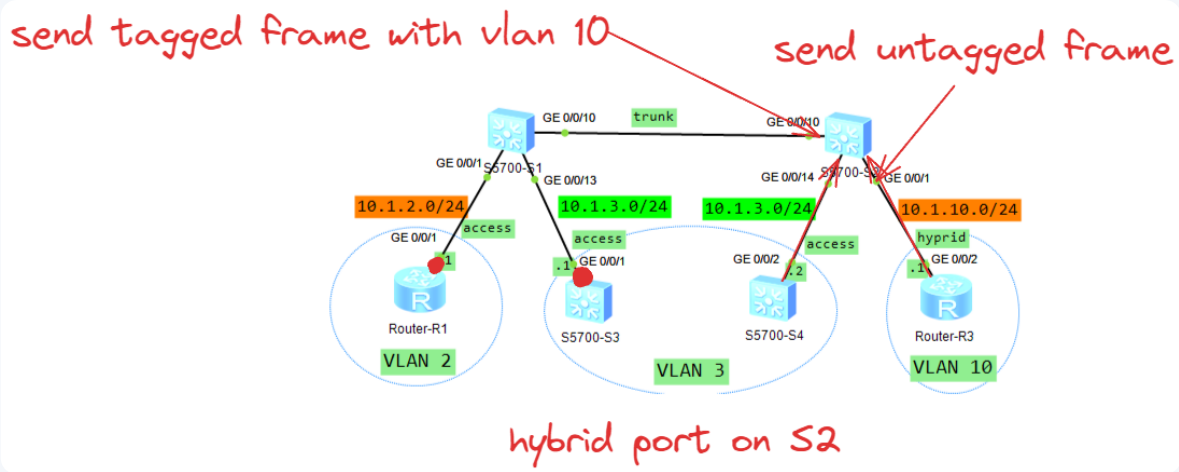
1.7 Step 5: Configure MAC Address-Based VLANs

> Associate specific MAC addresses with a particular VLAN regardless of their access port.

```
[S2] vlan 10
[S2-vlan10] mac-vlan mac-address 5489-9882-6ae2
```

Configure hybrid ports to accept untagged packets from MAC address-based VLANs:

```
[S2]interface GigabitEthernet0/0/1
[S2-GigabitEthernet0/0/1]port link-type hybrid
[S2-GigabitEthernet0/0/1]port hybrid untagged vlan 10
[S2-GigabitEthernet0/0/1]mac-vlan enable
```



1.8 Step 6: Display Configuration Information

1.8.1 Displaying VLAN Information:

```
[S1]display vlan
```

```
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type      Ports
--------------------------------------------------------------------------------
1    common    UT: GE0/0/2(D)     GE0/0/3(D)     GE0/0/4(D)     GE0/0/5(D)
               GE0/0/6(D)         GE0/0/7(D)     GE0/0/8(D)     GE0/0/9(D)
               GE0/0/11(D)        GE0/0/12(D)    GE0/0/14(D)    GE0/0/15(D)
               GE0/0/16(D)        GE0/0/17(D)    GE0/0/18(D)    GE0/0/19(D)
               GE0/0/20(D)        GE0/0/21(D)    GE0/0/22(D)    GE0/0/23(D)
               GE0/0/24(D)
2    common    UT: GE0/0/1(U)
               TG: GE0/0/10(U)
3    common    UT: GE0/0/13(U)
               TG: GE0/0/10(U)
10   common    TG: GE0/0/10(U)

VID  Status  Property      MAC-LRN Statistics  Description
--------------------------------------------------------------------------------
1    enable  default       enable    disable   VLAN 0001
2    enable  default       enable    disable   VLAN 0002
3    enable  default       enable    disable   VLAN 0003
10   enable  default       enable    disable   VLAN 0010
```

```
[S2]display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------

VID  Type      Ports
--------------------------------------------------------------------------------
1    common    UT: GE0/0/1(U)     GE0/0/2(D)     GE0/0/3(D)     GE0/0/4(D)
               GE0/0/5(D)         GE0/0/6(D)     GE0/0/7(D)     GE0/0/8(D)
               GE0/0/9(D)         GE0/0/11(D)    GE0/0/12(D)    GE0/0/13(D)
               GE0/0/15(D)        GE0/0/16(D)    GE0/0/17(D)    GE0/0/18(D)
               GE0/0/19(D)        GE0/0/20(D)    GE0/0/21(D)    GE0/0/22(D)
               GE0/0/23(D)        GE0/0/24(D)
2    common    TG: GE0/0/10(U)
3    common    UT: GE0/0/14(U)
               TG: GE0/0/10(U)
10   common    UT: GE0/0/1(U)     GE0/0/2(D)     GE0/0/3(D)
```

1.8.2 Display the MAC address-based VLAN

```
[S2]display mac-vlan vlan 10
--------------------------------------------------------------------------------
MAC Address       MASK              VLAN       Priority
--------------------------------------------------------------------------------
00e0-fc1c-47a7    ffff-ffff-ffff    10         0

Total MAC VLAN address count: 1
```

1.8.3 Check Connectivity

```
<S3>ping 10.1.3.2
  PING 10.1.3.2: 56  data bytes, press CTRL_C to break
    Reply from 10.1.3.2: bytes=56 Sequence=1 ttl=255 time=80 ms
    Reply from 10.1.3.2: bytes=56 Sequence=2 ttl=255 time=80 ms
    Reply from 10.1.3.2: bytes=56 Sequence=3 ttl=255 time=80 ms
    Reply from 10.1.3.2: bytes=56 Sequence=4 ttl=255 time=70 ms
    Reply from 10.1.3.2: bytes=56 Sequence=5 ttl=255 time=70 ms

  --- 10.1.3.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 70/76/80 ms
```

From S3 to S4 its reachable since they are in same vlans

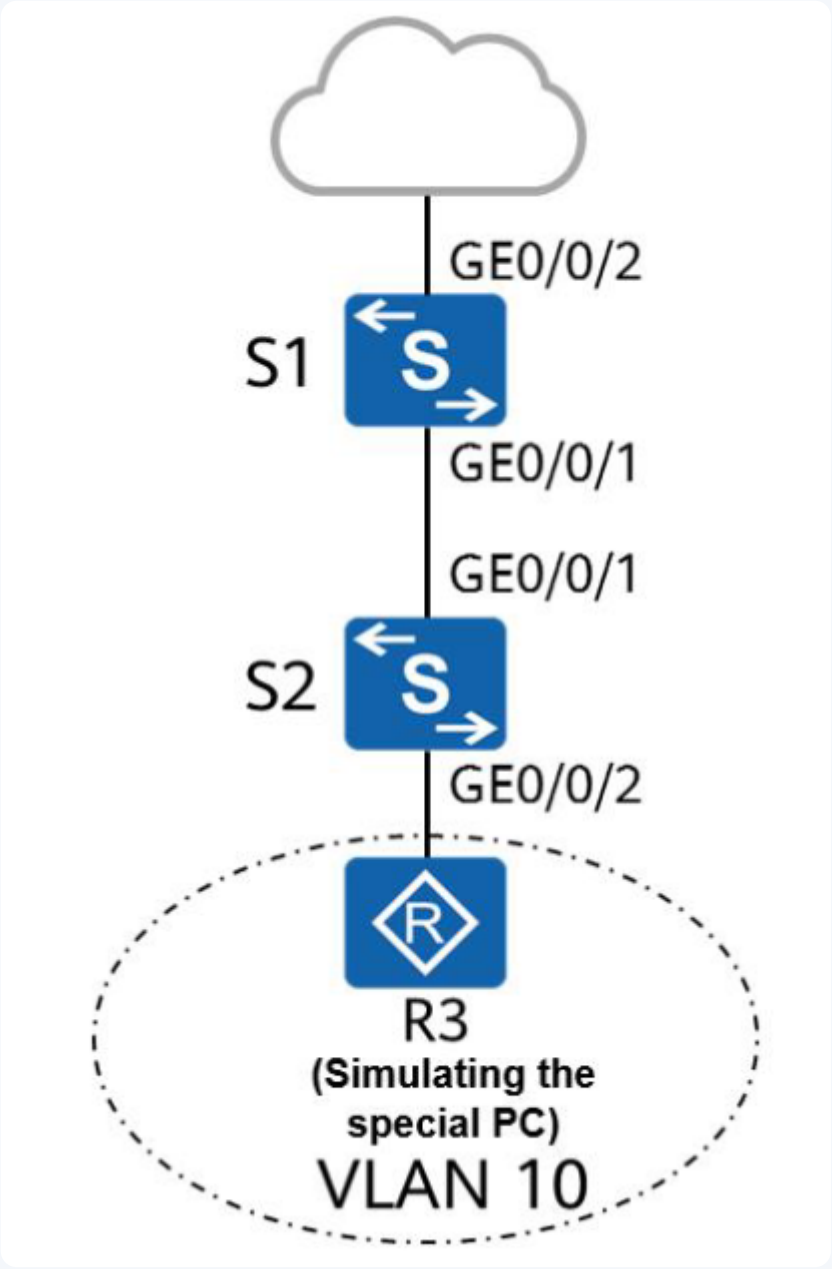
```
<R1>ping 10.1.3.1
  PING 10.1.3.1: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

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

From R1 to R3 its unreachable since they are in different vlans and there is no inter vlan routing

1.9 Quiz

Question1

As shown in the following figure, to ensure the information security of a special service, only some special PCs can access the network through VLAN How can this requirement be implemented on S1



✓ Answer1

- Create a VLAN for PCs with special needs
- Associate the MAC addresses of the PCs with VLAN
- Assign interfaces to VLANs to implement Layer 2 forwardi

Markdown

```
[S1]vlan 10
[S1-vlan10]mac-vlan mac-address 00e0-fc1c-47a7
[S1-vlan10]interface gigabitethernet 0/0/1
[S1-GigabitEthernet0/0/1]mac-vlan enable
```

```
[S1-GigabitEthernet0/0/1]interface gigabitethernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type hybrid
[S1-GigabitEthernet0/0/1]port hybrid untagged vlan 10
[S1-GigabitEthernet0/0/1]interface gigabitethernet 0/0/2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan 10
```

- Create VLANs.
- Associate the MAC address of the PC with VLAN 10
- Enable MAC address-based VLAN assignmen
- Configure GE0/0/1 connected to S2 as a hybrid port to allow data frames of the corresponding VLAN to pass through in untagged mode.
- Configure GE0/0/2 connected to the enterprise network to transparently transmit packets from the VLANs associated with MAC address.

2 Lab3 Part2 Spanning Tree

2.1 Spanning Tree Protocol (STP) Overview

STP is a network protocol that ensures a loop-free topology for Ethernet networks. The protocol allows redundant links in a network to prevent complete network failure if an active link fails, without the danger of bridge loops.

Upon completing this task, you will know how to:

- Toggle STP/RSTP on and off
- Switch between STP modes on a switch

- Set bridge priorities for root bridge selection
- Adjust port priorities to influence root and designated port choices
- Modify port costs affecting root and designated port selection
- Configure ports as edge ports
- Enable or disable RSTP specifically

A company aims to enhance network reliability by adding redundant links in its Layer 2 network while using STP to avoid loops that lead to broadcast storms and MAC address instability.

2.2 Lab Steps

2.2.1 Step 1: enable stp and set it to stp

Markdown

```
[S1]stp enable
[S1]stp mode stp
```

> Enable stp and set the mode to stp. Default is MSTP

> Re-enter same commands for S2 & S3 & S4

2.2.1.1 Display stp

```
[S1]display stp
-------[CIST Global Info][Mode STP]-------
CIST Bridge          :32768.4c1f-cc33-7359                //Bridge ID of the device.
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :32768.4c1f-cc10-5913 / 20000        //ID and path cost of the current root
bridge.
```

[S1]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/10	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/11	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/13	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/14	ROOT	FORWARDING	NONE

[S2]display stp brief

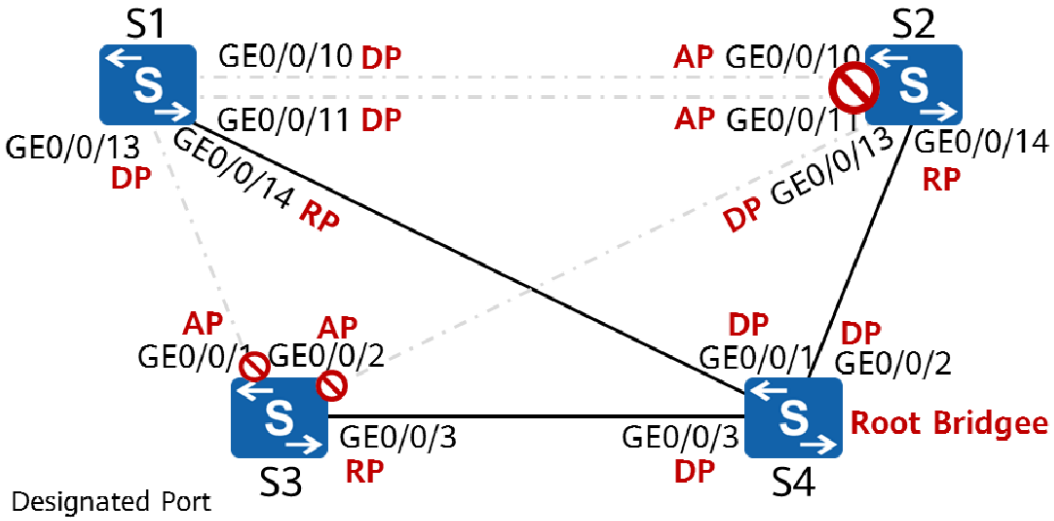
MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/10	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/11	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/13	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/14	ROOT	FORWARDING	NONE

[S3]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/2	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/3	ROOT	FORWARDING	NONE

[S4]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/2	DESI	FORWARDING	NONE
0	GigabitEthernet0/0/3	DESI	FORWARDING	NONE



2.2.2 Step 2: Configuring Root Bridges

Change bridge priorities on S1 and S2 to make S1 the primary root bridge and S2 the secondary root bridge:

```Markdown
[S1] stp root primary
[S2] stp root secondary
```

> Make S1 the primary root bridge with highest priority (0)

> Make S2 secondary with second-highest priority (4096)

2.2.3 Step 3: Modifying Root Ports

To modify a specific interface's cost:

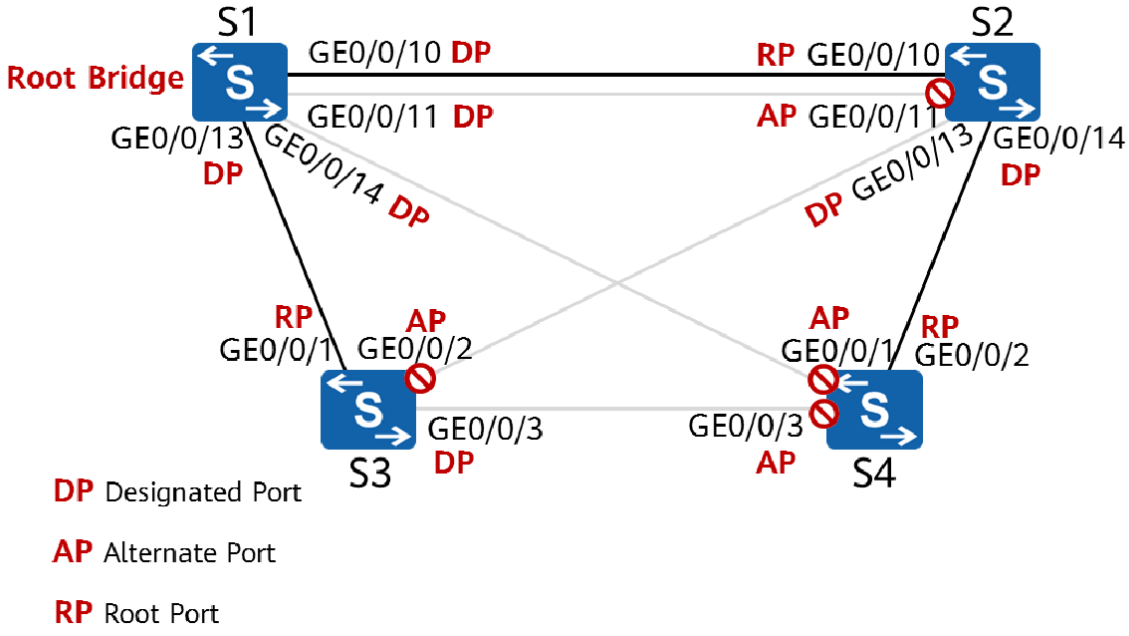
```Markdown
[S4]interface GigabitEthernet0/0/1
[S4-GigabitEthernet0/0/1]stp cost 50000
```

> Modify STP path cost; higher cost will change role to ALTE/DISCARDING state

[S4]display stp brief

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/1	ALTE	DISCARDING	NONE
0	GigabitEthernet0/0/2	ROOT	FORWARDING	NONE
0	GigabitEthernet0/0/3	ALTE	DISCARDING	NONE

Was Previous the Gig0/0/1 Root and the Cost is 20000 and then we change it to 50000 so other port is cost 20000+20000 =40000 so the election for root port is elect gig0/0/2



2.2.4 Step 4: Switching to RSTP Mode

Change all devices from STP to RSTP mode:

Markdown

```
[S1]stp mode rstp
```

Apply it for S2 & S3 S4

```
[S1]display stp
-------[CIST Global Info][Mode RSTP]-------
CIST Bridge             :0      .4c1f-cc33-7359
Config Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times            :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC          :0      .4c1f-cc33-7359 / 0
CIST RegRoot/IRPC       :0      .4c1f-cc33-7359 / 0
CIST RootPortId         :0.0
BPDU-Protection         :Disabled
CIST Root Type          :Primary root
TC or TCN received      :89
TC count per hello      :0
```

2.2.5 Step 5: Configuring Edge Ports

Configure interfaces connected only to terminals as edge ports:

```Markdown
[S3]port-group group-member gigabitethernet 0/0/10 to gigabitethernet 0/0/20
[S3-port-group]stp edged-port enable
```

> Select multiple interfaces in range on S3

2.2.6 Configure loop protection

```Markdown
[S3]interface gigabitethernet0/0/1
[S3]stp loop-protection
```

> prevent Layer 2 forwarding loops and broadcast radiation in a network by blocking redundant paths that could cause a loop if a port incorrectly transitions into forwarding state.

2.2.7 bpdu-protection

Markdown

```
[S3]stp bpdu-protection
```

> BPDU protection enhances network stability by disabling ports that receive unexpected Bridge Protocol Data Units (BPDUs), preventing potential malicious or accidental topology changes.

2.3 Verification Tasks

- Verify which switch is designated as the root bridge and roles of ports after convergence.
- Test redundancy by disabling an active link and checking traffic rerouting through backup links.

```
<S4>dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/1        ALTE  DISCARDING      NONE
   0    GigabitEthernet0/0/3        ROOT  FORWARDING      NONE
```

> After Shutdown interface gig0/0/2 the interface gig0/0/3 goes up

2.4 Quiz Questions

Consider these questions based on lab activities:

Question1

In step 3, if the cost of GigabitEthernet 0/0/14 on S1 is changed to 50000, can the desired result be achieved? Why?

Answer1

it will not change anything since the S1 is bridge and all port is designated

Quesion2

In the current topology, modify the configuration to make GigabitEthernet0/0/11 of S2 the root port.

Markdown

```
[S3]interface gig0/0/10
[S3-GigabitEthernet0/0/10]stp cost 60000
[S3-GigabitEthernet0/0/10]interface gig0/0/13
[S3-GigabitEthernet0/0/13]stp cost 60000
```

Answer2

> Change the cost of other interface and make it bigger to make interface gig0/0/11 more preferer over other interfaces

```
[S2-GigabitEthernet0/0/13]dis stp bri
 MSTID  Port                        Role  STP State     Protection
   0    GigabitEthernet0/0/10       ALTE  DISCARDING      NONE
   0    GigabitEthernet0/0/11       ROOT  FORWARDING      NONE
   0    GigabitEthernet0/0/13       DESI  FORWARDING      NONE
```

Question3

Can the two links between S1 and S2 be in the forwarding state at the same time? Why?

Answer3

Not possible since the broadcast between S1 and S2 if all port is enable it will cause loop storm so at least it should one port is disable

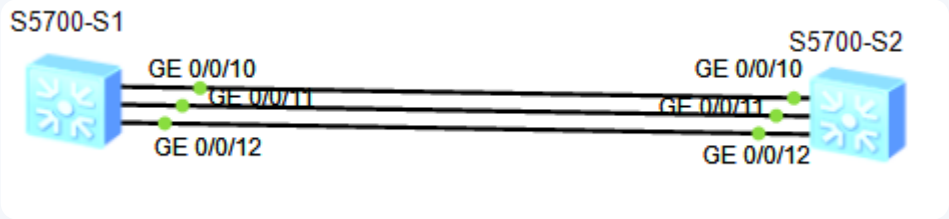
3 Lab3 Part3 Ethernet Link Aggregation

3.1 Overview of Link Aggregation

Link aggregation allows multiple network connections to be combined to increase throughput beyond what a single connection could sustain, or to provide redundancy in case one link fails.

3.2 Configuration Roadmap

1. **Manual Link Aggregation**
2. **LACP Mode Configuration**
3. **Active Link Determination**
4. **Load Balancing Mode Change**



3.3 Manual Link Aggregation

Step 1: Create an Eth-Trunk and set the mode to manual load balancing.

Markdown

```
[S1]interface Eth-Trunk 1
[S1-Eth-Trunk1]mode manual load-balance
[S1-Eth-Trunk1]trunkport gigabitethernet 0/0/10
[S1-Eth-Trunk1]trunkport gigabitethernet 0/0/11
[S1-Eth-Trunk1]trunkport gigabitethernet 0/0/12
```

This configuration for S1 and S2

Create Eth-Trunk 1

Set mode to manual (optional here because it's default)

Add ports to Eth-Trunk

3.3.1 Display Eth-trunk status

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
WorkingMode: NORMAL                   Hash arithmetic: According to SIP-XOR-DIP
Least Active-linknumber: 1            Max Bandwidth-affected-linknumber: 32
Operate status: up                    Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
PortName                      Status      Weight
GigabitEthernet0/0/10         Up          1
GigabitEthernet0/0/11         Up          1
GigabitEthernet0/0/12         Up          1
```

3.3.2 Important Points for Manual Aggregation

- Max of 8 member ports per Eth-Trunk.
- Cannot add an Eth-Trunk into another.
- Each Ethernet port can only belong to one Eth-Trunk.
- Match number of physical ports, port rate, and duplex mode on both ends.

> All links are active and forward data.

3.4 LACP Mode Configuration

> **Step 2:** Configure link aggregation using the LACP protocol.

Markdown

```
[S1]interface eth-trunk 1
[S1-Eth-Trunk1]undo trunkport gigabitethernet 0/0/10
[S1-Eth-Trunk1]undo trunkport gigabitethernet 0/0/11
[S1-Eth-Trunk1]undo trunkport gigabitethernet 0/0/12
[S1-Eth-Trunk1]mode lacp-static
[S1-Eth-Trunk1]trunkport gigabitethernet 0/0/10
```

```
[S1-Eth-Trunk1]trunkport gigabitethernet 0/0/11
[S1-Eth-Trunk1]trunkport gigabitethernet 0/0/12
```

> Remove member ports from the current trunk (if any) since you cant change mode if there is member ports

> Change working mode to LACP

> Re-add the ports under LACP mode

3.4.1 Display Eth-trunk status

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay: Disabled           Hash arithmetic: According to SIP-XOR-DIP
System Priority: 32768            System ID: 4c1f-cc33-7359
Least Active-linknumber: 1        Max Active-linknumber: 8
Operate status: up                Number Of Up Port In Trunk: 3
--------------------------------------------------------------------------------
ActorPortName           Status    PortType  PortPri PortNo PortKey PortState Weight
GigabitEthernet0/0/10   Selected  1GE       32768   11     305     10111100  1
GigabitEthernet0/0/11   Selected  1GE       32768   12     305     10111100  1
GigabitEthernet0/0/12   Selected  1GE       32768   13     305     10111100  1

Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri    SystemID        PortPri PortNo PortKey PortState
GigabitEthernet0/0/10   32768     4c1f-ccc1-4a02  32768   11     305     10111100
GigabitEthernet0/0/11   32768     4c1f-ccc1-4a02  32768   12     305     10111100
GigabitEthernet0/0/12   32768     4c1f-ccc1-4a02  32768   13     305     10111100
```

3.4.2 Actor Selection in LACP

Priority is given based on system priority (lower is better) or by MAC address if there's a tie.

3.5 Active Link Determination

> **Step 3:** Modify parameters such as priority and thresholds for active links.

```Markdown
[S1]lacp priority 100
[S1]interface gigabitethernet0/0/10
[S1-gigabitethernet0/0/10]lacp priority 40000
```

> Set system LACP priority (lower is higher priority) to act like the Actor to initiate the election for LACP

> Port priority lower value mean more preferable so elect for port as active

3.5.1 preemption

```Markdown
[S1-Eth-Trunk1]lacp preempt enable
```

> In LACP mode, the system replaces a failed active link with the highest-priority backup link and, if preemption is enabled a recovered higher-priority link can regain active status; preemption is disabled by default.

3.5.2 Thresholds for Active Ports

Specify lower and upper threshold for active links:

```
[S1-Eth-Trunk1]least active-linknumber 2
[S1-Eth-Trunk1]max active-linknumber 2
```

> The threshold is at least 2 and maximum is 2 if there is 1 port then the eth-trunk will go off and if there is 3 port one of the port will act as backup based of port priority

3.5.2.1 Display Eth-trunk status

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay Time: 30            Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100              System ID: 4c1f-cc33-7359
Least Active-linknumber: 2        Max Active-linknumber: 2
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName           Status     PortType  PortPri  PortNo  PortKey  PortState  Weight
GigabitEthernet0/0/10   Unselect   1GE       40000    11      305      10100000   1
GigabitEthernet0/0/11   Selected   1GE       32768    12      305      10111100   1
GigabitEthernet0/0/12   Selected   1GE       32768    13      305      10111100   1
```

> In this case the GigabitEthernet0/0/10 is unselected since the eth-trunk is set to max active port is 2 and eth-trunk elect them based on their priority port low mean preferable so eth-trunk elect GigabitEthernet0/0/11 & GigabitEthernet0/0/12 since their priority is blow than GigabitEthernet0/0/10

Shut down GigabitEthernet0/0/12 to simulate a link

```
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay Time: 30            Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100              System ID: 4c1f-cc33-7359
Least Active-linknumber: 2        Max Active-linknumber: 2
Operate status: up                Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName           Status     PortType  PortPri PortNo  PortKey   PortState Weight
GigabitEthernet0/0/10   Selected   1GE       40000   11      305       10111100  1
GigabitEthernet0/0/11   Selected   1GE       32768   12      305       10111100  1
GigabitEthernet0/0/12   Unselect   1GE       32768   13      305       10100010  1

Partner:
--------------------------------------------------------------------------------
ActorPortName           SysPri     SystemID        PortPri PortNo  PortKey   PortState
GigabitEthernet0/0/10   32768      4c1f-ccc1-4a02  32768   11      305       10111100
GigabitEthernet0/0/11   32768      4c1f-ccc1-4a02  32768   12      305       10111100
GigabitEthernet0/0/12   0          0000-0000-0000  0       0       0         10100011
GigabitEthernet 0/0/10 has become active.
```

In this case after GigabitEthernet0/0/12 go down the GigabitEthernet0/0/10 will go up since its act as backup

Shut down GigabitEthernet 0/0/11 & 0/0/12 to simulate a link

```
[S1]display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                         WorkingMode: STATIC
Preempt Delay Time: 30            Hash arithmetic: According to SIP-XOR-DIP
System Priority: 100              System ID: 4c1f-cc33-7359
Least Active-linknumber: 2        Max Active-linknumber: 2
Operate status: down              Number Of Up Port In Trunk: 0
--------------------------------------------------------------------------------
ActorPortName           Status     PortType  PortPri PortNo  PortKey   PortState Weight
GigabitEthernet0/0/10   Unselect   1GE       40000   11      305       10100000  1
GigabitEthernet0/0/11   Unselect   1GE       32768   12      305       10100010  1
GigabitEthernet0/0/12   Unselect   1GE       32768   13      305       10100010  1

Partner:
--------------------------------------------------------------------------------
```

Since the least port is set to 2 and in this case is only one port is working so the eth-trunk will go off

3.6 Load Balancing Mode Change

> **Step 4:** Adjust how traffic is distributed across the aggregated links based on criteria like source or destination IP addresses.

Markdown

```
[S1-Eth-Trunk1]load-balance dst-ip
```

> Set load balancing mode based on destination IP

3.6.1 Load Balancing Considerations

Load balancing affects only outgoing traffic; modes can differ between endpoints.

3.7 Quiz Question

Question1

What are the requirements for setting `least active-linknumber` and `max active-linknumber` values?

Answer1

Answer: Both values define thresholds that control the minimum and maximum number of active links allowed before an Eth-Trunks state changes. Setting these helps ensure stability and bandwidth requirements are met according to network design considerations.

4 Lab3 Part4 Inter-VLAN Communication

4.1 Introduction

VLANs are used to segment network traffic at Layer 2, creating separate broadcast domains. To enable communication between VLANs, Huawei routers can employ two primary technologies:

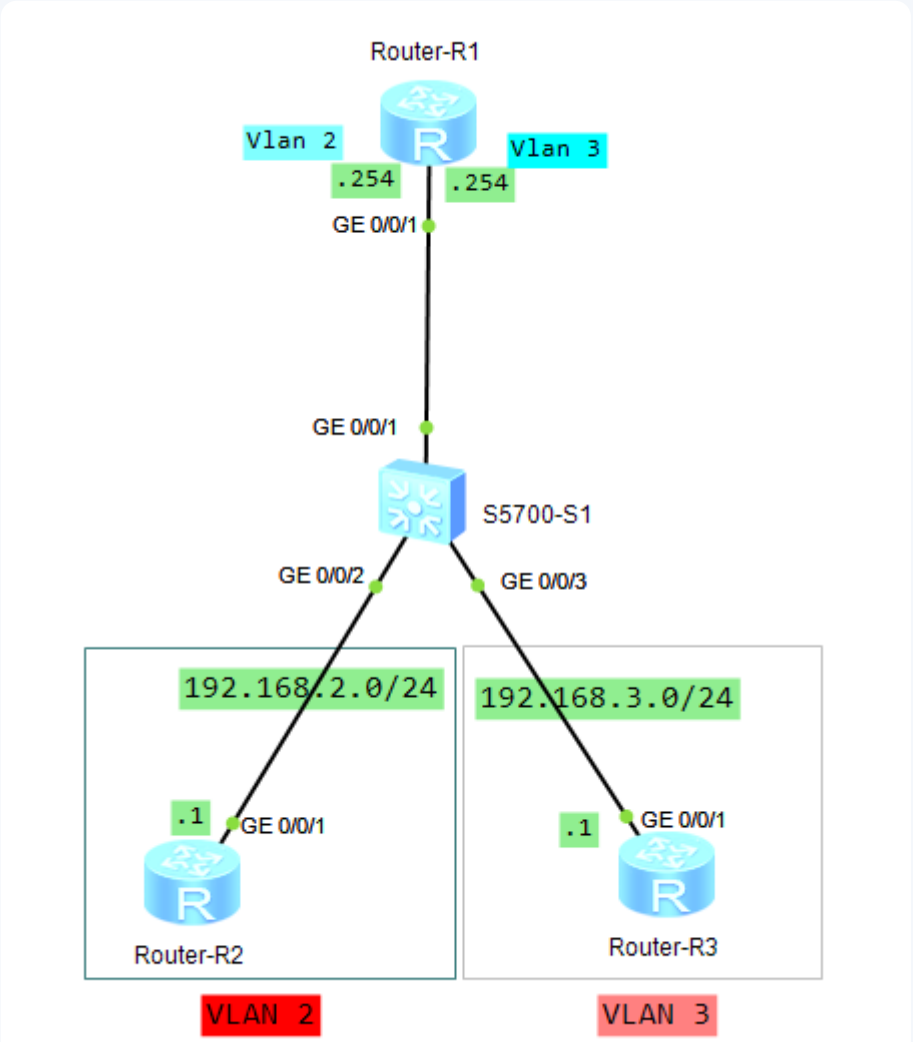
1. **Dot1q Termination Subinterfaces**
    - Layer 3 logical interfaces that allow a single physical interface to route traffic for multiple VLANs.
2. **VLANIF Interfaces**
    - Also Layer 3 logical interfaces, these are associated with specific VLANs and route traffic accordingly.

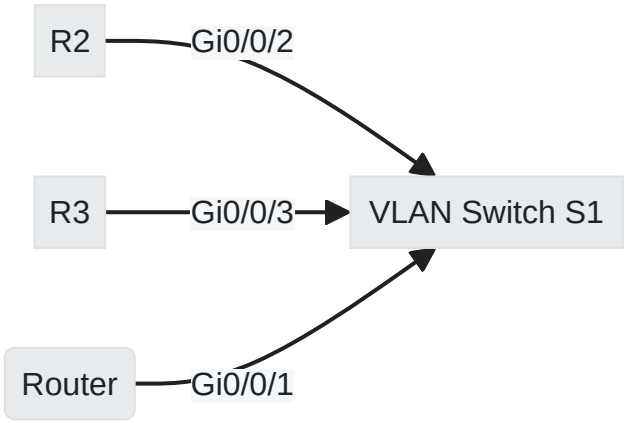
4.2 Objectives

- Understand how to configure both Dot1q termination subinterfaces and VLANIF interfaces for inter-VLAN communication.
- Grasp the forwarding process that enables devices in different VLANs to communicate.

4.3 Networking Topology

- Devices R2 and R3 are in separate VLANs and need to communicate through a router or switch using the aforementioned technologies.





Device	Interface	Description	IP Address
S1	Vlanif2	Gateway for VLAN 2	`192.168.2.254`
S1	Vlanif3	Gateway for VLAN 3	`192.168.3.254`
R2	G0/0/1	Device in VLAN 2	`192.168.2.1`
R3	G0/0/1	Device in VLAN 3	`192.168.3.1`
R1	G0/0/1	Sub interface Gateway for	`192.168.2.254`

Device	Interface	Description	IP Address
		VLAN 2	
R1	G0/0/1	Sub interface Gateway for VLAN 3	`192.168.3.254`

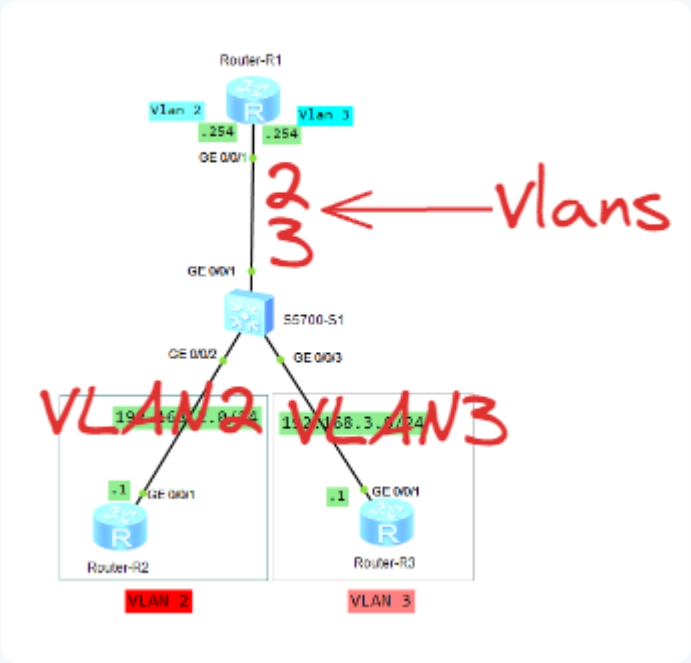
4.4 Configuration Steps

4.4.1 Basic Configuration

> Assign devices to appropriate VLANs on switch S1.

Markdown

```
[R1]vlan batch 2 3
[R1]interface GigabitEthernet0/0/2
[R1-GigabitEthernet0/0/2]port link-type access
[R1-GigabitEthernet0/0/2]port default vlan 2
[R1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/3
[R1-GigabitEthernet0/0/3]port link-type access
[R1-GigabitEthernet0/0/3]port default vlan 3
[R1-GigabitEthernet0/0/3]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]port link-type trunk
[R1-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
[R1-GigabitEthernet0/0/1]undo port trunk allow-pass
vlan 1
```



Create Vlan

Assign port for interfaces (Acess and Trunk) access for end device and trunk for carry vlan frames

4.4.1.1 Assign Ip address

4.4.1.1.1 R2

Markdown

```
[R2]interface GigabitEthernet0/0/1
[R2-GigabitEthernet0/0/1]ip address 192.168.2.1 24
```

In this topology R2 is act as end deive

4.4.1.1.2 R3

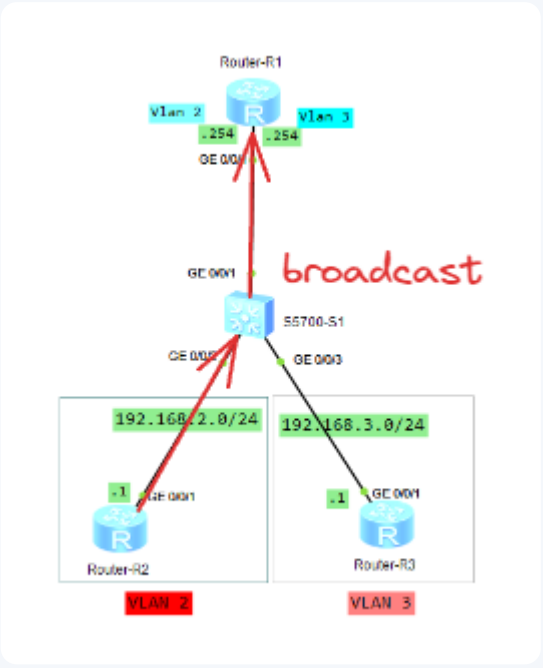
```
[R3]interface GigabitEthernet0/0/1
[R3-GigabitEthernet0/0/1]ip address 192.168.3.1 24
```

In this topology R3 is act as end deive

4.4.1.2 Configure Default Static Route

4.4.1.2.1 R2

```
[R2]ip route-static 0.0.0.0 0 192.168.2.254
```



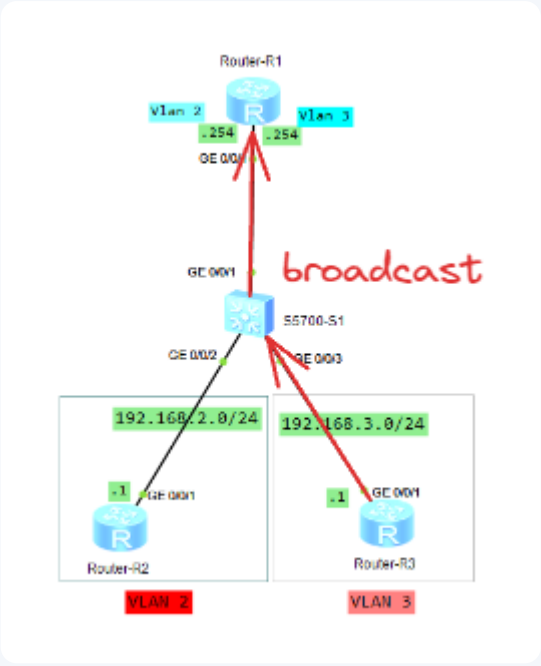
Configure a default route (equivalent to a gateway) for the device since the router is acted as end device

This default static route used for connectivity between different range of ip if like R2 ping R3 (pinging `192.168.2.1` to `192.168.3.1`) so its required router to know the route for `192.168.3.1` so the default router will forward it to its gateway and if its in same broadcast domain like pinging `192.168.2.1` to `192.168.2.254` it will not required for routing since its in same ip domain so the router have routing table with direct route

4.4.1.2.2 R3

Markdown

```
[R3]ip route-static 0.0.0.0 0 192.168.3.254
```



Configure a default route (equivalent to a gateway) for the device since the router is acted as end device

This default static route used for connectivity between different range of ip if like R2 ping R3 (pinging `192.168.2.1` to `192.168.3.1`) so its required router to know the route for `192.168.3.1` so the default router

> will forward it to its gateway and if its in same broadcast domain like pinging `192.168.2.1` to `192.168.2.254` it will not required for routing since its in same ip domain so the router have routing table with direct route

4.4.2 Dot1q Termination Subinterfaces

> Configure subinterfaces on the router for each VLAN.

Markdown

```
[R1]interface GigabitEthernet0/0/1.2
[R1-GigabitEthernet0/0/1.2]dot1q termination vid 2
[R1-GigabitEthernet0/0/1.2]ip add 192.168.2.254 24
[R1-GigabitEthernet0/0/1.2]arp broadcast enable
[R1-GigabitEthernet0/0/1.2]int gig0/0/1.3
[R1-GigabitEthernet0/0/1.3]dot1q termination vid 3
[R1-GigabitEthernet0/0/1.3]ip add 192.168.3.254 24
[R1-GigabitEthernet0/0/1.3]arp broadcast enable
```

> Create subinterface for vlans

> It is recommended that the subinterface number be the same as the VLAN for simplicity for configuration and management

> The idea of `dot1q termination vid` is for receive tagged frame and remove the tag header to process it for routing process then before forward it to next destination re tagged with same `vid` to receive it and forward it for end device

> Subinterfaces for VLAN tag termination cannot forward broadcast packets

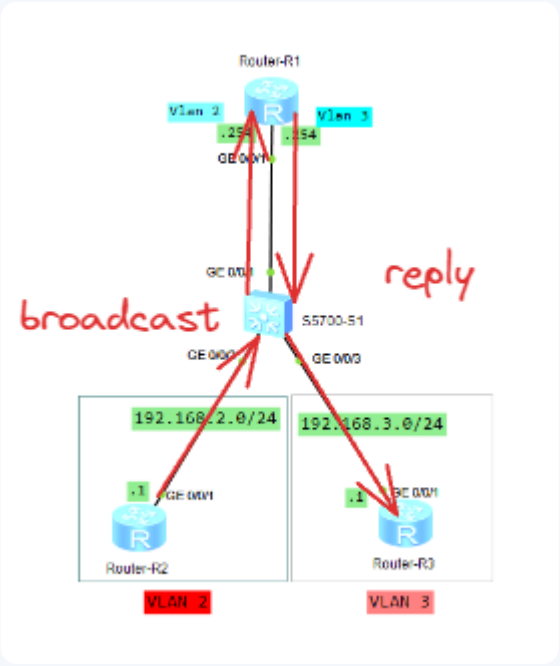
and automatically discard them upon receiving

By default, this function is enabled on some devices

4.4.2.1 Display 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.
```

Tracert:



Test the connectivity between VLANS (2,3)

4.4.3 VLANIF Interface Configuration

For undo the configuration for port links undo `trunk` and `access`

4.4.3.1 Access

Markdown

```
[S]interface gigabitethernet0/0/1
[S1-GigabitEthernet0/0/1]undo port default vlan
```

4.4.3.2 Trunk

```
[S1]interface gigabitethernet0/0/1
[S1-GigabitEthernet0/0/1]undo port trunk pvid vlan
[S1-GigabitEthernet0/0/1]undo port trunk allow-pass vlan all
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 1
```

4.4.3.3 Hybrid

```
[S1]interface gigabitethernet0/0/1
[S1-GigabitEthernet0/0/1]undo port hybrid pvid vlan
[S1-GigabitEthernet0/0/1]undo port hybrid vlan all
[S1-GigabitEthernet0/0/1]port hybrid untagged vlan 1
```

> Instead of subinterfaces, configure a single interface on the switch for each VLAN.

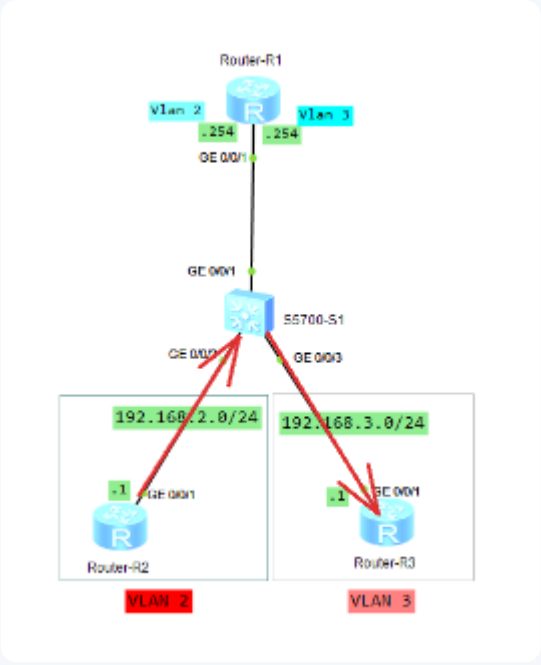
```
[S1]interface vlanif 2
[S1-Vlanif2]ip address 192.168.2.254 24
[S1-Vlanif2]int vlanif 3
[S1-Vlanif3]ip address 192.168.3.254 24
```

4.4.3.4 Display 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.

Tracert:



Test the connectivity between VLANS (2,3)

4.5 Quiz Questions

Question1

If R2 needs to access the network connected to R1, what configuration needs to be performed on S1?

Answer1

Configure the appropriate inter-VLAN routing method (either Dot1Q termination or a VLANIF interface) with correct addressing and routing rules so that packets from R2 can be forwarded to the correct destination through R1.

Question2

As a Layer 3 interface, when will a VLANIF interface go up?

Answer2

A VLANIF interface will go up when it has been assigned an IP address and is associated with an existing active (up/up) physical port that is a member of the corresponding VLAN.

Lab4

1 Lab4 Part 1 ACL Configuration

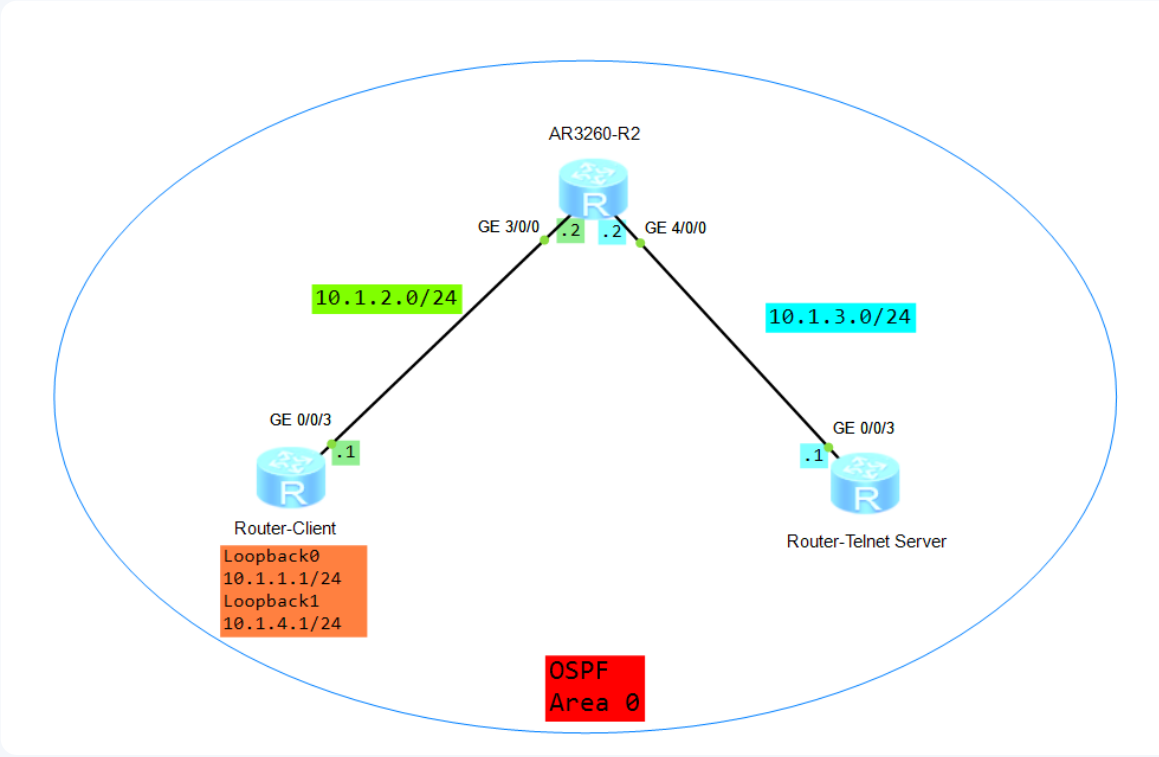
1.1 Overview

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
```

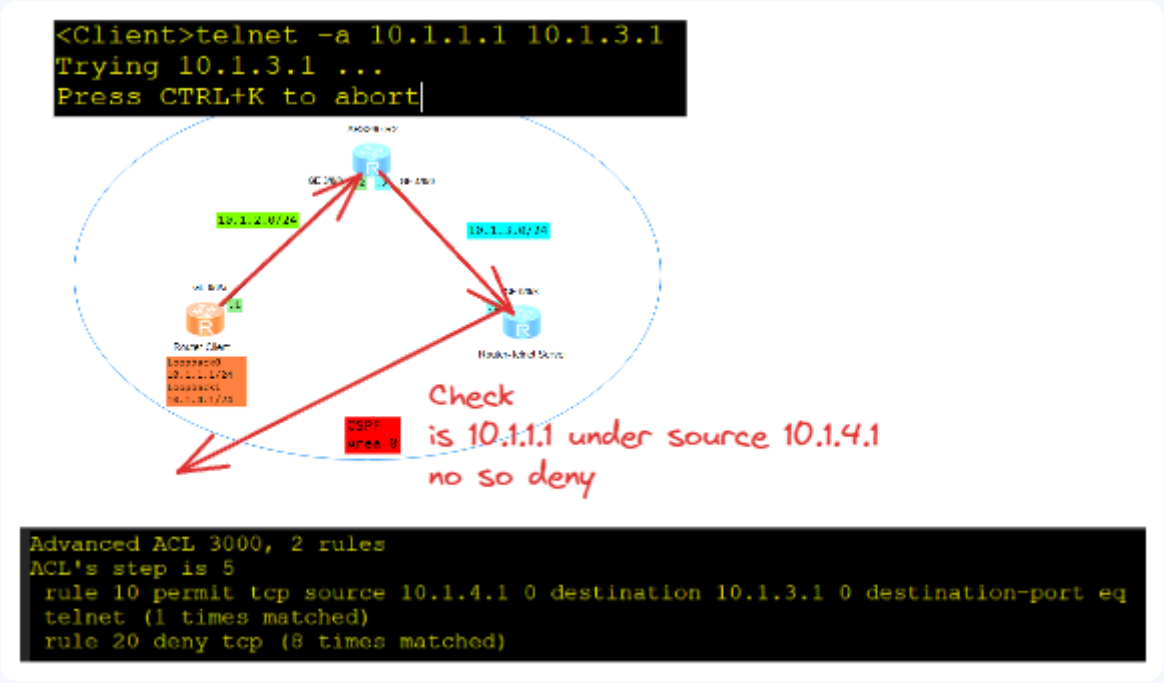
```
Advanced ACL 3001, 2 rules
Acl's step is 5
 rule 10 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-port eq telnet (82 matches)
 rule 20 deny tcp (3 matches)
```

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.

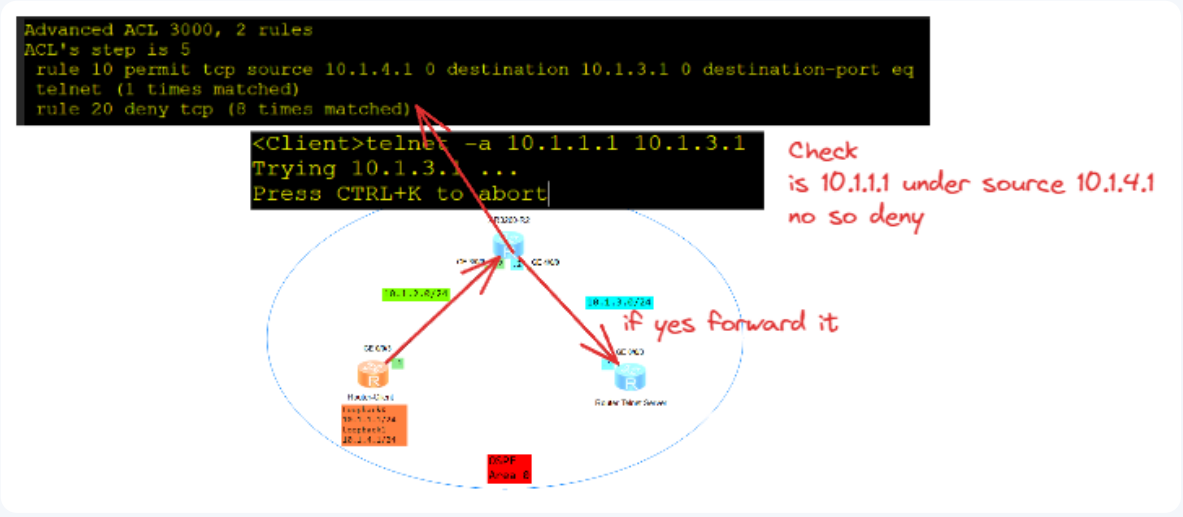



```
<Client>telnet -a 10.1.1.1 10.1.3.1
Trying 10.1.3.1 ...
Press CTRL+K to abort
```

```
<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.

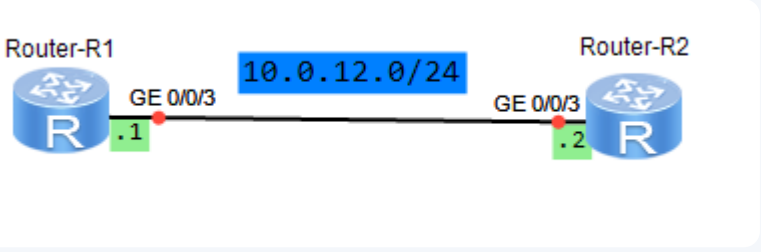
This lab focuses on configuring local AAA for remote Telnet users.

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:

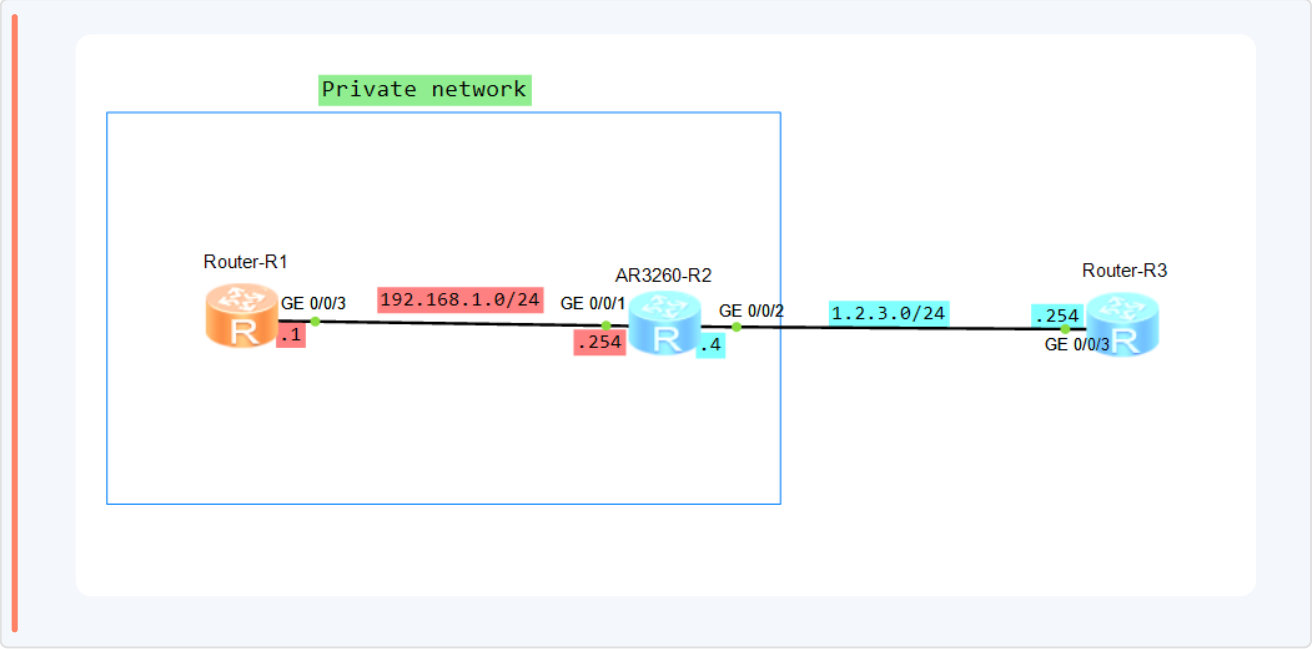
- Protects private networks against external attacks.
- Controls communication between private and public networks.

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

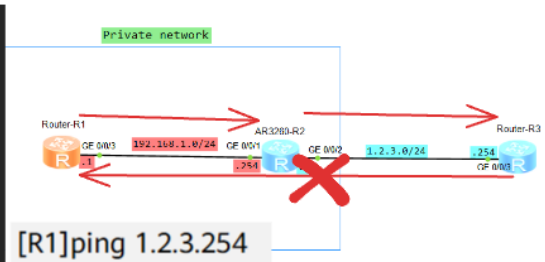
```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 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:

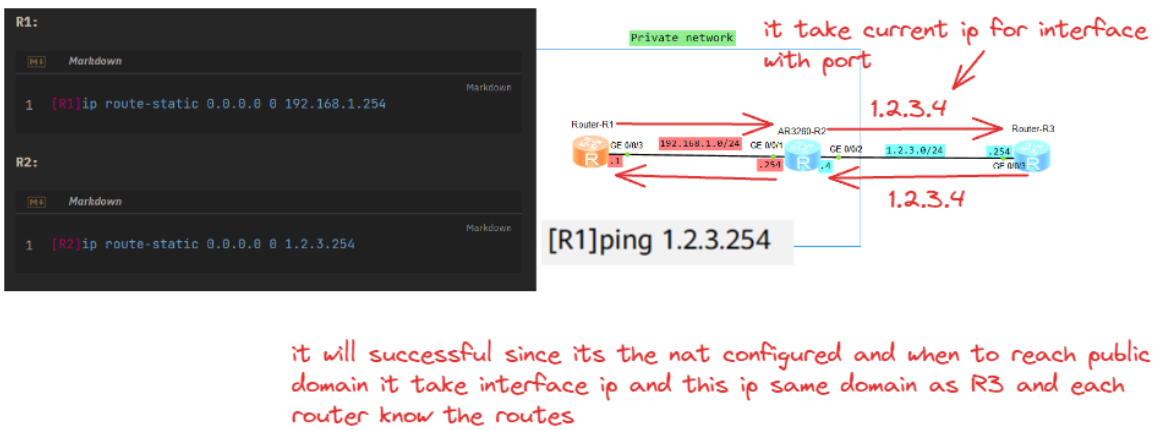
Markdown

```
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.

Lab5

1 Lab5 Part1 FTP Configuration

1.1 Introduction to FTP

FTP (File Transfer Protocol) is a standard network protocol used for transferring files between a client and server on a computer network. It is built on a client-server model architecture using separate control and data connections between the client and server.

- **TFTP** (Trivial File Transfer Protocol) - A simpler version without authentication.
- **SFTP** (Secure File Transfer Protocol) - Uses SSH for secure transfers.

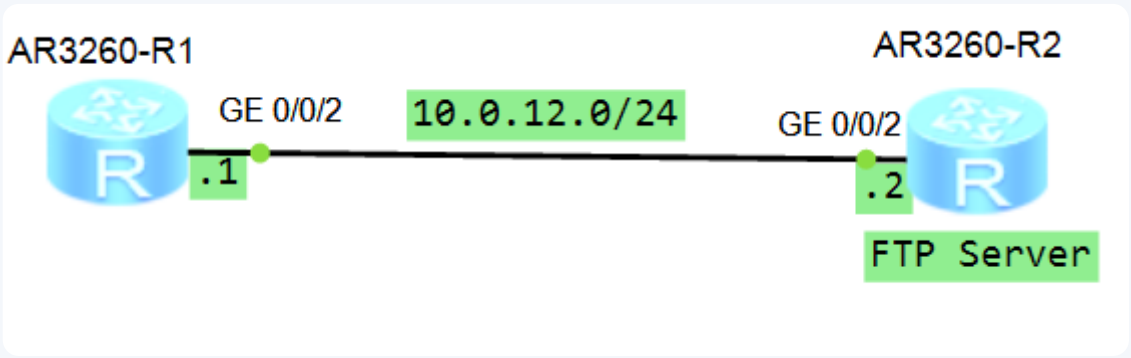
A device can operate as either:

- **Server**: Allows clients to manage and transfer files.
- **Client**: Connects to a server to manage and transfer files.

1.2 Lab Objectives

- Establish an FTP connection.
- Configure FTP server settings.
- Transfer files using FTP.

1.3 Networking Topology



1.4 Lab Configuration Steps

1.4.1 Step 1: Basic Device Setup

> Set device names, configure IP addresses, and save initial configurations.

R1:

```Markdown
[R1]interface GigabitEthernet0/0/2
[R1-GigabitEthernet0/0/2]ip address 10.0.12.1 24
```

R2:

```Markdown
[R1]interface GigabitEthernet0/0/2
```

```
2 [R1-GigabitEthernet0/0/2]ip address 10.0.12.2 24
```

1.4.1.1 Display directory

```
<R1>dir
Directory of flash:/

  Idx  Attr     Size(Byte)      Date   Time(LMT)      FileName
    0  -rw-    126,538,240   Jul 04 2016 17:57:22   ar651c- v300r019c00Sspc100.cc
    1  -rw-         23,963   Feb 21 2020 09:22:53   mon_file.txt
    2  -rw-            721   Feb 21 2020 10:14:33   vrpcfg.zip
    3  drw-              -   Jul 04 2016 18:51:04   CPM_ENCRYPTED_FOLDER
    4  -rw-            783   Jul 10 2018 14:46:16   default_local.cer
    5  -rw-              0   Sep 11 2017 00:00:54   brdxpon_snmp_cfg.efs
    6  drw-              -   Sep 11 2017 00:01:22   update
    7  drw-              -   Sep 11 2017 00:01:48   shelldir
    8  drw-              -   Feb 20 2020 21:33:16   localuser
    9  drw-              -   Sep 15 2017 04:35:52   dhcp
   10  -rw-            509   Feb 21 2020 10:18:31   private-data.txt
   11  -rw-          2,686   Dec 19 2019 15:05:18   mon_lpu_file.txt
   12  -rw-          3,072   Dec 18 2019 18:15:54   Boot_LogFile
   13  -rw-          1,390   Feb 21 2020 10:18:30   test1.cfg

510,484 KB total available (386,448 KB free)
```

```
<R2>dir
Directory of flash:/

 Idx  Attr     Size(Byte)      Date   Time(LMT)      FileName
   0  -rw-    126,538,240     Jul 04 2016 17:57:22  ar651c- v300r019c00Sspc100.cc
   1  -rw-         11,405     Feb 21 2020 09:21:53  mon_file.txt
   2  -rw-            809     Feb 21 2020 10:14:10  vrpcfg.zip
   3  drw-              -     Jul 04 2016 18:51:04  CPM_ENCRYPTED_FOLDER
   4  -rw-            782     Jul 10 2018 14:48:14  default_local.cer
   5  -rw-              0     Oct 13 2017 15:36:32  brdxpon_snmp_cfg.efs
   6  drw-              -     Oct 13 2017 15:37:00  update
   7  drw-              -     Oct 13 2017 15:37:24  shelldir
   8  drw-              -     Feb 20 2020 20:51:34  localuser
   9  drw-              -     Oct 14 2017 11:27:04  dhcp
  10  -rw-          1,586     Feb 21 2020 10:16:51  test2.cfg
  11  -rw-            445     Feb 21 2020 10:16:52  private-data.txt
  12  -rw-          4,096     Aug 06 2019 11:19:08  Boot_LogFile

510,484 KB total available (386,464 KB free)
The configuration files of the two devices are saved successfully.
```

1.4.2 Step 2: Enable FTP Server on R2

> Use the `ftp server enable` command to start the FTP service.

Markdown

```
[R2]ftp server enable
```

1.4.3 Step 3: Configure Local FTP Users on R2

> Create user with password, set service type to FTP, assign privilege level, specify directory access.

> The authorized directory of the FTP user is specified. This directory must

be specified. Otherwise, the FTP user cannot log in to the syst

```Markdown
[R2]aaa
[R2-aaa]local-user ftp password cipher ftp
[R2-aaa]local-user ftp privilege level 15
[R2-aaa]local-user ftp service-type ftp
[R2-aaa]local-user ftp ftp-directory flash:/
```

1.4.4 Step 4: Login from R1 (FTP Client)

Connect to R2 using the `ftp` command followed by the IP address of the server (R2).

```
<R1>ftp 10.0.12.2
Trying 10.0.12.2 ...

Press CTRL+K to abort
Connected to 10.0.12.2.
220 FTP service ready.
User(10.0.12.2:(none)):ftp-client
331 Password required for ftp-client.
Enter password:
230 User logged in.

[R1-ftp]
You have logged in to the file system of R2.
```

1.4.5 Step 5: File Operations from Client Side (R1)

Transfer files using commands like `get` , `put` , or `delete` . Set transfer mode (`ascii` or `binary`) as needed.

```
[R1-ftp]get test2.cfg
200 Port command okay.
```

Download the configuration file

```
[R1-ftp]delete test2.cfg
Warning: The contents of file test2.cfg cannot be recycled. Continue? (y/n)[n]:y
250 DELE command successful.
```

Delete the configuration file

```
[R1-ftp]put test1.cfg
200 Port command okay.
150 Opening ASCII mode data connection for test1.cfg.
226 Transfer complete.
FTP: 875 byte(s) sent in 0.240 second(s) 3.64Kbyte(s)/sec.
```

Upload the configuration file

```
[R1-ftp]bye
221 Server closing.

<R1>
```

> Close the FTP connection

1.5 Quiz

Question1

Does FTP work in active or passive mode by defaul

Answer1

By default, FTP works in **active** mode where the client initiates both command and data connections to the server.

2 Lab5 Part2 DHCP Configuration

2.1 Introduction

Dynamic Host Configuration Protocol (DHCP) is a protocol for automatic IP address assignment, simplifying network administration. It's defined in RFC 2131 and supports both dynamic and static IP allocation.

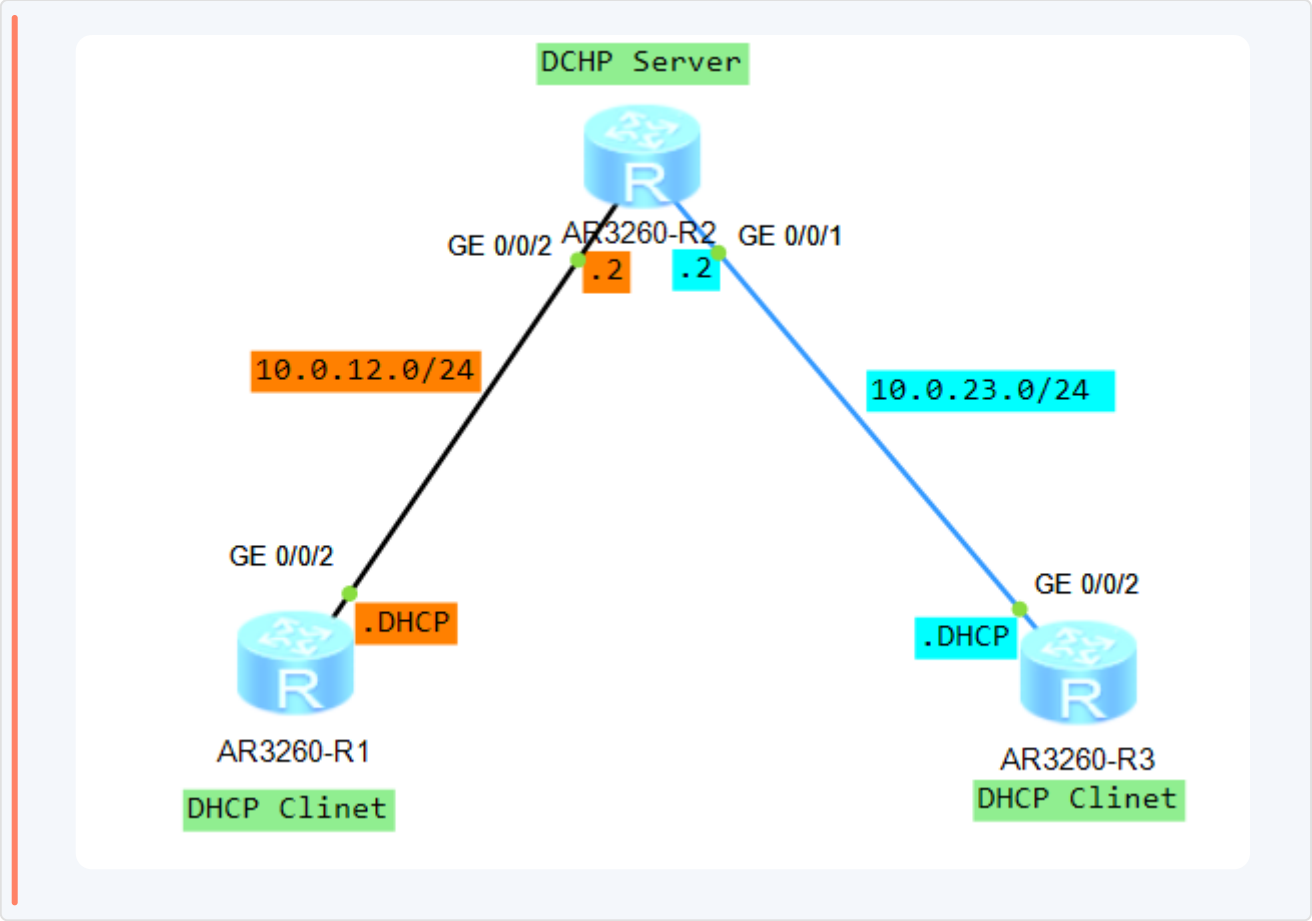
- **Dynamic allocation:** Grants an IP with a lease time, useful when the number of idle IPs is less than the total hosts.
- **Static allocation:** Grants a fixed IP to a client, preventing manual errors and facilitating management.

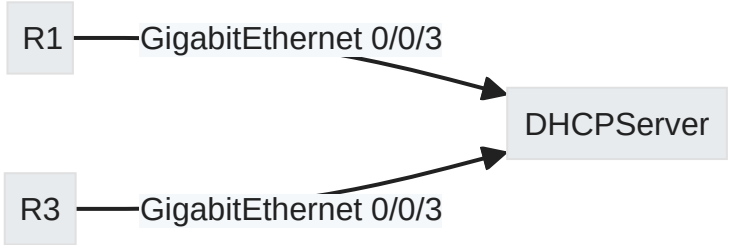
2.2 Objectives

- Configure an interface address pool on the DHCP server.
- Configure a global address pool on the DHCP server.
- Use DHCP to allocate static IP addresses.

2.3 Networking Topology

DHCP reduces the workload of IP address maintenance and improves utilization. The lab setup involves configuring R1 and R3 as DHCP clients and R2 as the DHCP server.





2.4 Lab Configuration Steps

2.4.1 Step 1: Basic Configurations

Configure interface addresses on router R2:

```Markdown
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2] ip address 10.0.12.2 24
[R2-GigabitEthernet0/0/2]quit
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ip address 10.0.23.2 24
```

2.4.2 Step 2: Enable DHCP on all routers

```Markdown
[R2]dhcp enable
```

> The dhcp enable command must be executed before executing any other DHCP-related commands, regardless for DHCP servers or clie

> This configuration applied on R1 ,R2, R3

2.4.3 Step 3: Configure Address Pools

Interface pool for GE 0/0/3 (R1):

```Markdown
```

```
[R2]interface GigabitEthernet 0/0/2
[R2-GigabitEthernet0/0/2]dhcp select interface
[R2-GigabitEthernet0/0/2]dhcp server dns-list 10.0.12.2
```

> This dhcp pool used only on same devices connected on same interface

Global pool configuration:

Markdown

```
[R2]ip pool GlobalPool
[R2-ip-pool-GlobalPool]network 10.0.23.0 mask 24
[R2-ip-pool-GlobalPool]dns-list 10.0.23.2
[R2-ip-pool-GlobalPool]gateway-list 10.0.23.2
[R2-ip-pool-GlobalPool]lease day 2 hour 2
```

> The lease command specifies the lease for IP addresses in a global IP address pool. If the lease is set to unlimited, the lease is unlimited. By default, the lease of IP addresses is one day

Static binding in global pool:

Markdown

```
[R2-ip-pool-GlobalPool]static-bind ip-address 10.0.23.3
mac-address 00e0-fc07-2349
```

> The static-bind command binds an IP address in a global address pool to a MAC address of a client

> You can run the display interface GigabitEthernet0/0/1 to show the mac-address

2.4.4 Step 4: Enable DHCP Server Function on Interfaces

For global pools:

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]dhcp select global
```

2.4.5 Step 5: Configure DHCP Clients (R1 & R3)

Set interfaces to obtain IP via DHCP:

```
[R1]interface GigabitEthernet 0/0/2
[R1-GigabitEthernet0/0/2] ip address dhcp-alloc
```

> On router R1 & R2

2.5 Verification Commands

Check route received by client:

```
[R1]display ip interface brief
Interface                   IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/3        10.0.12.254/24       up         up
```

```
[R1]display dns server
Type:
D:Dynamic        S:Static

No.   Type       IP Address
1       D          10.0.12.2
```

```
[R3]display ip interface brief
Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/3              10.0.23.3/24         up         up
```

```
[R3]display dns server
Type:
D:Dynamic        S:Static
No.   Type       IP Address
1       D          2.23.0.10
```

```
[R2]display ip pool name GlobalPool
  Pool-name             : GlobalPool
  Pool-No               : 1
  Lease                 : 2 Days 2 Hours 0 Minutes
  Domain-name           : -
  DNS-server0           : 10.0.23.2
  NBNS-server0          : -
  Netbios-type          : -
  Position              : Local          Status          : Unlocked
  Gateway-0             : 10.0.23.2
  Mask                  : 255.255.255.0
  VPN instance          : --
 ------------------------------------------------------------------------------
         Start            End        Total   Used   Idle(Expired)   Conflict   Disable
 ------------------------------------------------------------------------------
        10.0.23.1        10.0.23.254   253      1        252(0)          0          0
 ------------------------------------------------------------------------------
```

```
[R2]display ip pool interface GigabitEthernet0/0/4
  Pool-name             : GigabitEthernet0/0/4
  Pool-No               : 0
  Lease                 : 1 Days 0 Hours 0 Minutes
  Domain-name           : -
  DNS-server0           : 10.0.12.2
  NBNS-server0          : -
  Netbios-type          : -
  Position              : Interface         Status              : Unlocked
  Gateway-0             : 10.0.12.2
  Mask                  : 255.255.255.0
  VPN instance          : --
-------------------------------------------------------------------------------
        Start       End             Total   Used    Idle(Expired)   Conflict   Disable
-------------------------------------------------------------------------------
      10.0.12.1   10.0.12.254       253     1         252(0)          0          0
-------------------------------------------------------------------------------
```

2.6 Quiz Questions to Test Understanding

Question1

What are the differences between the application scenarios of a global address pool and those of an interface address pool?

Answer1

1. **Global Address Pool**: Used across multiple networks for centralized IP management; not tied to specific interfaces.
2. **Interface Address Pool**: Linked to a particular interface; allocates IPs to clients on that network segment.

Question2

If there are multiple global address pools, how do you determine the global address pool for a DHCP client

✓ **Answer2**

When determining which global address pool to use for a DHCP client, the DHCP server considers the source of the request, relay information, and administrative policies to allocate an IP from the appropriate pool.

Lab6

1 Lab6 Creating a WLAN

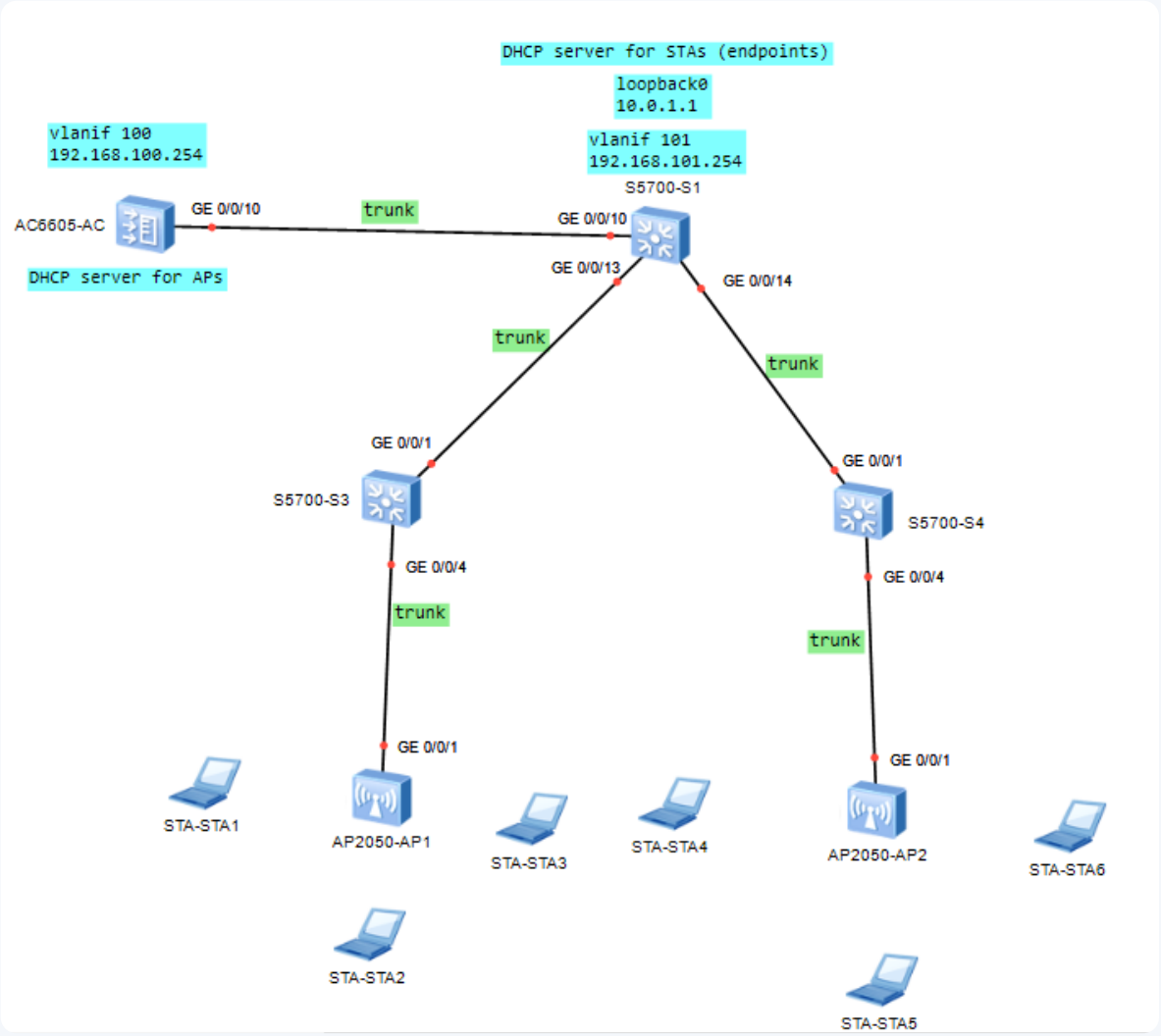
1.1 Overview

These notes summarize the process of configuring a WLAN with Huawei equipment, including setting up VLANs, DHCP services, AP groups, regulatory domain settings, and WLAN service parameters.

1.1.1 Network Components

- Access Controller (AC)
- Access Points (AP)
- Switches (S1, S3, S4)
- Service Terminal (STA)

1.1.2 General Steps



1. Create VLANs and assign IP addresses.
2. Configure IP pools for DHCP.
3. Set up AP groups and regulatory domains.
4. Configure CAPWAP source interface.
5. Bind regulatory domain profile to AP group.
6. Import APs to the AC.
7. Configure WLAN service parameters.

> The S2 switch supports the WLAN-AC function. If the switch does not support the WLAN-AC function, use a common AC to replace the switch. The AC in the following content is an S2 switch.

> The AC functions as a DHCP server to assign IP addresses to APs, S1 functions as a DHCP server to assign IP addresses to stations (STAs)

(end devices)

Topology Service data

- Service data is directly forwarde
  - An Access Control system in out-of-path mode is on the same network as the Access Point but doesn't intercept all traffic; it's part of the local network but not a direct gateway for client data.
  - While the AP communicates directly with clients, the AC can monitor or apply policies to traffic without routing packets through itself, allowing data to travel unimpeded to its destination.

Item	Configuration
AP Management VLAN	VLAN100
Service VLAN	VLAN101
DHCP Server (for APs)	AC as DHCP server
DHCP Server (for STAs)	S1 as DHCP server
STA Default Gateway	192.168.101.254
IP Address Pool for APs	192.168.100.1 - 192.168.100.253/24
IP Address Pool for STAs	192.168.101.1 - 192.168.101.253/24
AC's Source Interface IP	VLANIF100: 192.168.100.254/24
AP Group Name	ap-group1
Referenced Profiles	VAP profile HCIA-wlan, Regulatory domain profile default

Item	Configuration
Regulatory Domain Profile	Name: default
Country Code	CN

Item	Configuration
SSID Profile	Name: HCIA-WLAN
SSID Name	HCIA-WLAN

Item	Configuration
Security Profile	Name: HCIA-WLAN
Security Policy	WPA-WPA2+PSK+AES
Password	HCIA-Datacom

VAP Profile Attribute	Value
Name	HCIA-WLAN
Forwarding Mode	Direct Forwarding
Service VLAN	VLAN 101
Referenced SSID Profile	HCIA-WLAN
Referenced Security Profile	HCIA-WLAN

Explanation

- **AP Management VLAN (VLAN 100):** A dedicated VLAN for network management traffic between Access Points and the wireless controller.
- **Service VLAN (VLAN 101):** A VLAN for user data traffic to segregate it from other network traffic.
- **IP Address of AC's Source Interface (VLANIF100):** 192.168.100.254/24 is the IP address used by the Access Controller to communicate with APs on VLAN 100.
- **AP Group (ap-group1):** A collection of APs sharing common settings like SSID and regulatory domain profiles.
- **Regulatory Domain Profile (default):** Sets power levels and channels per local regulations, here preset for China ("CN").
- **SSID Profile (HCIA-WLAN):** Configures the Wi-Fi network name that users see when connecting to the WLAN.
- **Security Profile (HCIA-WLAN):** Defines WPA-WPA2 PSK authentication with AES encryption for WLAN access using the passphrase "HCIA-Datacom".
- **VAP Profile (HCIA-WLAN):** Details virtual AP settings including direct forwarding mode and associations with Service VLAN, SSID, and

Security profiles.

1.2 Configurations

1.2.1 Configure poe link

```
[S3]interface GigabitEthernet 0/0/4
[S3-GigabitEthernet0/0/4]poe enable
```

These configuration for S3 & S4

The `poe enable` command turns on Power over Ethernet to power devices connected to a port, but it's usually on by default.

1.2.2 VLAN Configuration with IP's

Requirement :

AP Management VLAN	VLAN100
Service VLAN	VLAN101
STA Default Gateway	192.168.101.254

AC:

```
[AC]vlan batch 100 101
[AC]interface GigabitEthernet0/0/10
[AC-GigabitEthernet0/0/10]port link-type trunk
```

```
[AC-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[AC-GigabitEthernet0/0/10]quit
[AC]int vlanif100
[AC-Vlanif100]ip add 192.168.100.254 24
```

> Creating vlans and configure trunk port to carry vlan tag frame and set ip as source ip for AC and gateway for AP's to communicate with AC

S1:

Markdown

```
[S1]vlan batch 100 101
[S1]interface GigabitEthernet0/0/10
[S1-GigabitEthernet0/0/10]port link-type trunk
[S1-GigabitEthernet0/0/10]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/10]interface GigabitEthernet0/0/13
[S1-GigabitEthernet0/0/13]port link-type trunk
[S1-GigabitEthernet0/0/13]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/13]interface GigabitEthernet0/0/14
[S1-GigabitEthernet0/0/14]port link-type trunk
[S1-GigabitEthernet0/0/14]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/14]q
[S1]int vlanif101
[S1-vlanif101]ip address 192.168.101.254 24
[S1-vlanif101]int loopback0
[S1-loopback0]ip address 10.0.1.1 32
```

> Creating vlans and configure trunk port to carry vlan tag frame and set ip as gateway for AP's to communicate with S1 to get ip address and

communicate with external network

Loopback address act as external network for testing purpose

S3:

```
[S3]vlan batch 100 101
[S3]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type trunk
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/4
[S1-GigabitEthernet0/0/4]port link-type trunk
[S1-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/4]port trunk pvid vlan 100
```

Creating vlans and configure trunk port to carry vlan tag frame

The `port trunk pvid vlan 100` command assigns VLAN 100 as the default VLAN for untagged traffic on a trunk port.

S4:

```
[S4]vlan batch 100 101
[S3]interface GigabitEthernet0/0/1
[S1-GigabitEthernet0/0/1]port link-type trunk
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 101
[S1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/4
[S1-GigabitEthernet0/0/4]port link-type trunk
[S1-GigabitEthernet0/0/4]port trunk allow-pass vlan 100 101
```

```
[S1-GigabitEthernet0/0/4]port trunk pvid vlan 100
```

> Creating vlans and configure trunk port to carry vlan tag frame

> The `port trunk pvid vlan 100` command assigns VLAN 100 as the default VLAN for untagged traffic on a trunk port.

1.2.3 DHCP Settings for STAs and APs on AC

Requirement:

AP Management VLAN	VLAN100
Service VLAN	VLAN101

DHCP Server (for APs)	AC as DHCP server
DHCP Server (for STAs)	S1 as DHCP server
STA Default Gateway	192.168.101.254
IP Address Pool for APs	192.168.100.1 - 192.168.100.253/24
IP Address Pool for STAs	192.168.101.1 - 192.168.101.253/24

AC:

Markdown

```
[AC]dhcp enable
[AC]ip pool ap
[AC-ip-pool-ap]network 192.168.100.0 mask 24
[AC-ip-pool-ap]gateway-list 192.168.101.254
[AC-ip-pool-ap]quit
[AC]int vlanif100
[AC-Vlanif100]dhcp select global
```

> Configure dhcp for AC to assign IP's AP's

S1:

```
[S1]dhcp enable
[S1]ip pool sta
[S1-ip-pool-sta]network 192.168.101.0 mask 24
[S1-ip-pool-sta]gateway-list 192.168.101.254
[S1-ip-pool-sta]quit
[S1]int vlanif101
[S1-Vlanif101]dhcp select global
```

> Configure dhcp for S1 to assign IP's STA's

1.2.4 AP Group Configuration on AC

Requirement:

AP Group Name	ap-group1

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
```

> **AP group**
>
> > An AP group aggregates multiple access points as a single entity for easy configuration and management.

1.2.5 Regulatory Domain Profile Binding on AC

Requirement:

Item	Configuration
Regulatory Domain Profile	Name: default
Country Code	CN

```
[AC]wlan
[AC-wlan-view]regulatory-domain-profile name default
[AC-wlan-regulate-domain-default]country-code cn
```

> ⚠ **Regulatory Domain**
>
> > Changing the country code will reset the AP after clearing channel and power configurations.

```
[AC]wlan
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]regulatory-domain-profile default
```

> Bind the regulatory domain profile to an AP group.

1.2.6 CAPWAP Tunnel Source Interface on AC

Requirement:

AP Management VLAN	VLAN100
Service VLAN	VLAN101
STA Default Gateway	192.168.101.254

```
[AC]capwap source interface Vlanif 100
```

> CAPWAP tunnels are used by access points to communicate with the controller.

1.3 Importing APs to AC

Markdown

```
[AC]wlan
[AC-wlan-view]ap auth-mode mac-auth
[AC-wlan-view]ap-id 0 ap-mac 00e0-fc9a-6cc0
[AC-wlan-ap-0]ap-name ap1
[AC-wlan-ap-0]ap-group ap-group1
[AC-wlan-ap-0]ap-id 1 ap-mac 00e0-fcf2-4430
[AC-wlan-ap-1]ap-name ap2
[AC-wlan-ap-1]ap-group ap-group1
```

> Sets authentication mode based on MAC address for AP's

> Adds an AP using its MAC address

> Sets a custom name for an AP

> Binds an AP to a specific group

Display the information about the current:

```
[AC]wlan
[AC-wlan-view]display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal              [2]
------------------------------------------------------------------------------------------------------------------
ID   MAC                   Name Group      IP              Type          State STA Uptime
------------------------------------------------------------------------------------------------------------------
0    00e0-fc25-0ed0 ap1    ap-group1       192.168.100.206 AirEngine5760 nor   0   30M:4S
1    00e0-fc0f-07a0 ap2    ap-group1       192.168.100.170 AirEngine5760 nor   0   31M:31S
------------------------------------------------------------------------------------------------------------------
Total: 2
```

1.4 WLAN Service Parameters

1.4.1 Security Profile Creation on AC

Requirement:

Item	Configuration
Security Profile	Name: HCIA-WLAN
Security Policy	WPA-WPA2+PSK+AES
Password	HCIA-Datacom

Markdown

```
[AC]wlan
[AC-wlan-view]security-profile name HCIA-WLAN
[AC-wlan-sec-prof-HCIA-WLAN]security wpa-wpa2 psk pass-
phrase HCIA-Datacom aes
```

> The security psk command configures WPA/WPA2 pre-shared key (PSK) authentication and encryption

> The PSK is set to HCIA-Datacom. User data is encrypted using the AES encryption algorit

1.4.2 SSID Profile Creation on AC

Requirement:

Item	Configuration
SSID Profile	Name: HCIA-WLAN
SSID Name	HCIA-WLAN

Markdown

```
[AC]wlan
[AC-wlan-view]ssid-profile name HCIA-WLAN
[AC-wlan-ssid-prof-HCIA-WLAN]ssid HCIA-WLAN
```

> Create SSID profile HCIA-WLAN and set the SSID name to HCIA-WLAN

1.4.3 VAP Profile Binding to AP Group on AC

Requirement:

VAP Profile Attribute	Value
Name	HCIA-WLAN
Forwarding Mode	Direct Forwarding
Service VLAN	VLAN 101
Referenced SSID Profile	HCIA-WLAN
Referenced Security Profile	HCIA-WLAN

Markdown

```
[AC-wlan-view] vap-profile name HCIA-WLAN
...
[AC-wlan-ap-group-ap-group1] vap-profile HCIA-WLAN wlan
1 radio all
[AC]wlan
```

```
[AC-wlan-view]vap-profile name HCIA-WLAN
[AC-wlan-vap-prof-HCIA-WLAN]forward-mode direct-forward
[AC-wlan-vap-prof-HCIA-WLAN]service-vlan vlan-id 101
[AC-wlan-vap-prof-HCIA-WLAN]security-profile HCIA-WLAN
[AC-wlan-vap-prof-HCIA-WLAN]ssid-profile HCIA-WLAN
[AC-wlan-vap-prof-HCIA-WLAN]quit
[AC-wlan-view]ap-group name ap-group1
[AC-wlan-ap-group-ap-group1]vap-profile HCIA-WLAN wlan 1 radio all
```

Explanation

1. Create a VAP profile named HCIA-WLAN and configure data forwarding mode using `vap-profile` and `forward-mode` commands, respectively.
2. Set the service VLAN for the VAP with the `service-vlan` command, and bind the SSID and security profiles to the VAP.
3. Apply the VAP profile to both radio 0 and radio 1 in the AP group to ensure configurations are consistent across radios.
4. Use the `vap-profile` command to bind VAP profile HCIA-WLAN to the AP group, delivering all related configurations.

1.5 Verification Commands

1.5.1 Check connectivity from STA to S1 loopback

```
STA>ping 10.0.1.1

Ping 10.0.1.1: 32 data bytes, Press Ctrl_C to break
From 10.0.1.1: bytes=32 seq=1 ttl=255 time=125 ms
From 10.0.1.1: bytes=32 seq=2 ttl=255 time=141 ms
From 10.0.1.1: bytes=32 seq=3 ttl=255 time=125 ms
From 10.0.1.1: bytes=32 seq=4 ttl=255 time=125 ms
From 10.0.1.1: bytes=32 seq=5 ttl=255 time=125 ms

--- 10.0.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 125/128/141 ms
```

1.5.2 display station all

```
<AC>display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
--------------------------------------------------------------------------------
----------------------
STA MAC          AP ID Ap name  Rf/WLAN  Band  Type  Rx/Tx      RSSI  VLAN  IP a
ddress      SSID
--------------------------------------------------------------------------------
----------------------
5489-9892-33de   0     ap1      0/1      2.4G  -     -/-        -     101   192.
168.101.253 HCIA-WLAN
--------------------------------------------------------------------------------
----------------------
Total: 1 2.4G: 1 5G: 0
```

1.6 Quiz

Question1

Use an STA to access the WLAN with the SSID of HCIA-WLAN. Check the IP address obtained by the STA and ping the IP address (10.0.1.1) of LoopBack0 on S1.

Answer1

1. If VLAN 101 is blocked on the network controller's port, devices won't be able to reach services on that VLAN, like S1.
2. If all traffic is sent through a tunnel to the network controller and VLAN 101 isn't blocked there, devices can access S1 even if local network ports block VLAN 101.

- Here's what happens with your data traffic:
  - If direct forwarding is used, your data is sent directly through the network without going through a specific port (GigabitEthernet0/0/10) on the Access Controller (AC).
  - If tunnel forwarding is used and you need to go through GigabitEthernet0/0/10 on the AC, make sure that this port is configured to allow traffic from VLAN 101; otherwise, your device will not be able to communicate with S1.

- > Direct Forwarding: Sending data packets directly to the destination within the same network without intermediaries.

- > Tunnel Forwarding: Encapsulating data packets within another packet to securely traverse different networks or boundaries via a tunnel.

Question2

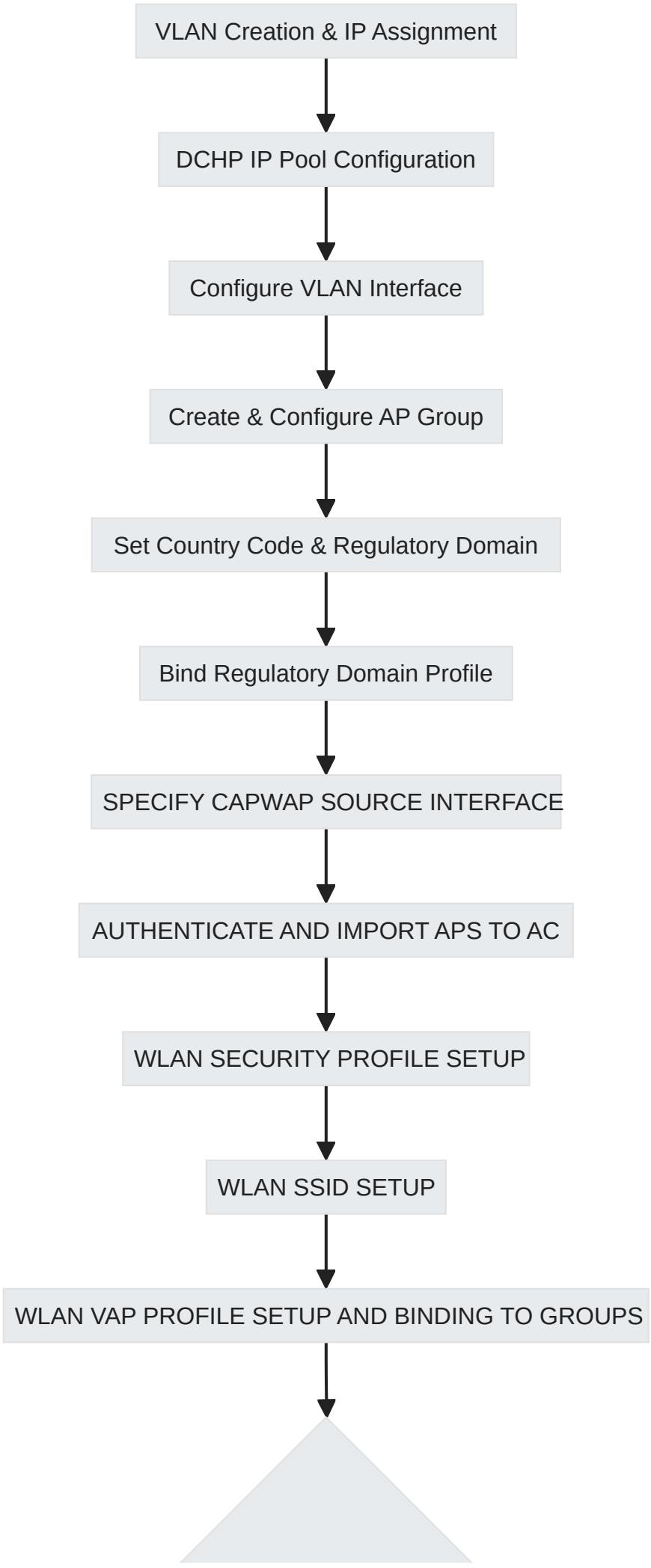
When the STA is connected to the AC, run the display station all command on the AC to check the STA information

Answer2

AP1 and AP2 use different VAP profiles, and different service-VLAN parameters are configured in the VAP profile

1.7 Simplified Process Flow

Below is a simplified process flow chart illustrating the steps from VLAN creation through verification using the Mermaid syntax suitable for Markdown rendering:


VLAN Creation & IP Assignment
DCHP IP Pool Configuration
Configure VLAN Interface
Create & Configure AP Group
Set Country Code & Regulatory Domain
Bind Regulatory Domain Profile
SPECIFY CAPWAP SOURCE INTERFACE
AUTHENTICATE AND IMPORT APS TO AC
WLAN SECURITY PROFILE SETUP
WLAN SSID SETUP
WLAN VAP PROFILE SETUP AND BINDING TO GROUPS

VERIFICATION STEPS

Lab7

1 Lab7 Creating an IPv6 Network

1.1 About This Lab

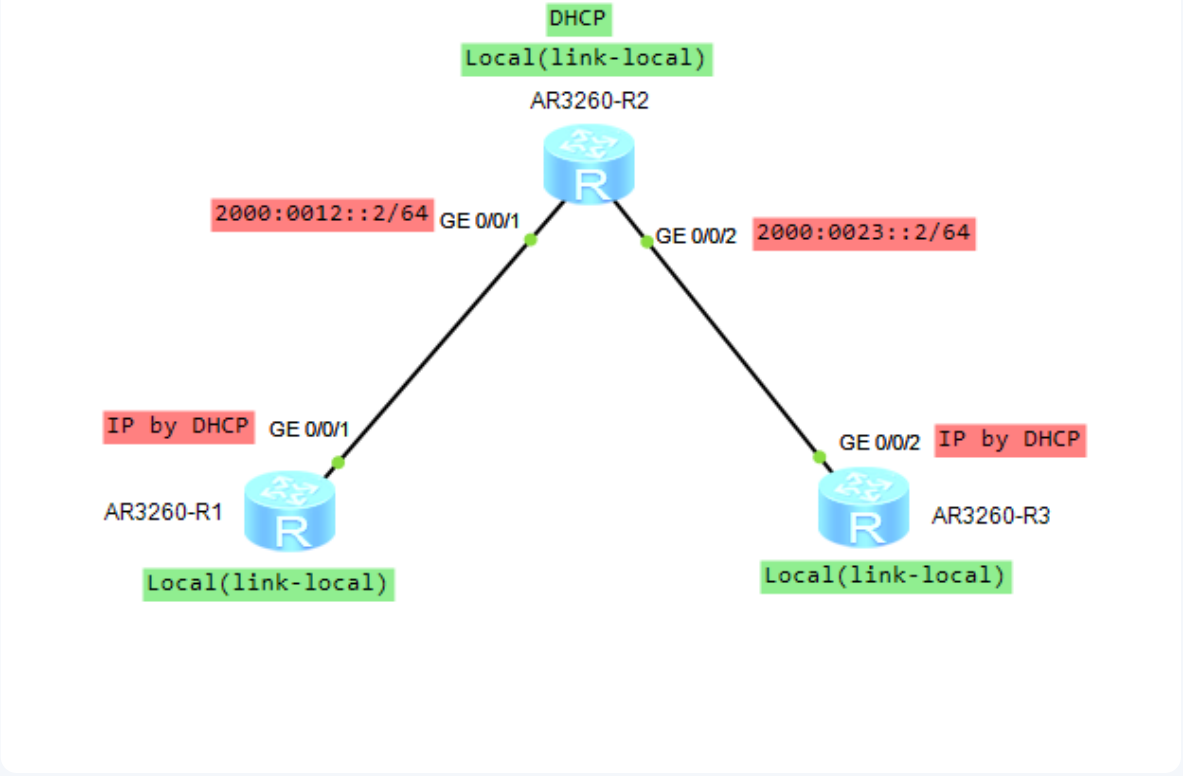
Understanding the configuration of IPv6 addresses, DHCPv6 server setup, stateless address configuration, static routes, and viewing IPv6 information in a lab environment.

1.2 Objectives

- Configure static IPv6 addresses and DHCPv6 server
- learn stateless address configuration
- set up static routes
- view IPv6 info upon task completion.

1.3 Networking Topology

Deploying IPv6 in an enterprise network requires configuring static addresses for R2 interfaces and stateless autoconfiguration for R1's GigabitEthernet0/0/1; use DHCPv6 for R3’s GigabitEthernet0/0/2.



1.4 Basic IPv6 Interface Configuration

R1:

```
[R2-GigabitEthernet0/0/1]ipv6
[R2-GigabitEthernet0/0/1]interface GigabitEthern0/0/1
[R2-GigabitEthernet0/0/1]ipv6 enable
[R2-GigabitEthernet0/0/1]ipv6 address auto link-local
```

> Activates IPv6 on a specified interface.

> Generates a unique link-local address.

> Link-local addresses are used for communication within the same network

> segment or broadcast domain.

R2:

```Markdown
[R2]ipv6
[R2]interface GigabitEthern0/0/1
[R2-GigabitEthernet0/0/1]ipv6 enable
[R2-GigabitEthernet0/0/1]ipv6 address auto link-local
[R2-GigabitEthernet0/0/1]interface GigabitEthern0/0/2
[R2-GigabitEthernet0/0/2]ipv6 enable
[R2-GigabitEthernet0/0/2]ipv6 address auto link-local
[R2-GigabitEthernet0/0/2]interface GigabitEthern0/0/1
[R2-GigabitEthernet0/0/1]ipv6 address 2000:0012::2 64
[R2-GigabitEthernet0/0/1]interface GigabitEthern0/0/2
[R2-GigabitEthernet0/0/2]ipv6 address 2000:0023::2 64
```

> Activates IPv6 on a specified interface.

> Generates a unique link-local address.

> Link-local addresses are used for communication within the same network segment or broadcast domain.

> Assign global ip as gateway to used as dhcp for our scenario

> In ipv6 each interface can have more than one type ip like `global` , `unicast`

R3:

```Markdown
[R3]ipv6
```

```
[R3]interface GigabitEthern0/0/2
[R3-GigabitEthernet0/0/1]ipv6 enable
[R3-GigabitEthernet0/0/1]ipv6 address auto link-local
```

Activates IPv6 on a specified interface.

Generates a unique link-local address.

Link-local addresses are used for communication within the same network segment or broadcast domain.

1.5 Testing Connectivity with IPv6

Markdown

```
[R1]display ipv6 interface gig0/0/1
```

```
GigabitEthernet0/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:FCFF:FE29:7399
  Global unicast address(es):
    2000:12::2E0:FCFF:FE29:7399,
    subnet is 2000:12::/64 [SLAAC 1970-01-01 02:51:56 2592000S]
  Joined group address(es):
    FF02::1:FF29:7399
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Check IPv6 status and link-local address.

> Ping using link-local addresses requires specifying the source interface with `-i` .

```
<R1>ping ipv6 FE80::2E0:FCFF:FE12:6486 -i GigabitEthernet 0/0/3
  PING FE80::2E0:FCFF:FE12:6486 : 56  data bytes, press CTRL_C to break
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=1 hop limit=64  time = 90 ms
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=2 hop limit=64  time = 10 ms
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=3 hop limit=64  time = 20 ms
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=4 hop limit=64  time = 10 ms
    Reply from FE80::2E0:FCFF:FE12:6486
    bytes=56 Sequence=5 hop limit=64  time = 30 ms

  --- FE80::2E0:FCFF:FE12:6486 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 10/32/90 ms
```

1.6 DHCPv6 Server and Client Configuration

1.6.1 Server Setup

`dhcpv6 server <pool_name>`

Markdown

```
[R2]dhcp enable
[R2]dhcpv6 pool poolv6
[R2-dhcpv6-pool-poolv6]address prefix 2000:0023::/64
[R2-dhcpv6-pool-poolv6]dns-server 2000:0023::2
```

```
[R2-dhcpv6-pool-poolv6]q
[R2]interface GigabitEthernet0/0/2
[R2-GigabitEthernet0/0/2]dhcpv6 server poolv6
```

Enable DHCP service

Create an address pool

Define address prefix

Set DNS server within pool

Associate pool with an interface for also gateway

1.6.2 Client Setup

```Markdown
[R3]dhcp enable
[R3]interface GigabitEthern0/0/2
[R3-GigabitEthernet0/0/2]ipv6 address auto dhcp
```

Enable DHCP client function

The DHCPv6 server does not allocate gateway information; clients learn default routes through RA messages or stateful configuration.

Display the client address:

```
*down: administratively down
(l): loopback
(s): spoofing
Interface                         Physical
GigabitEthernet0/0/2              up
[IPv6 Address] 2000:23::1
```

1.7 Router Advertisement (RA) Flags Configuration

Markdown

```
[R2]interface GigabitEthern0/0/2
[R2-GigabitEthernet0/0/2]ipv6 nd autoconfig managed-address-flag
[R2-GigabitEthernet0/0/2]ipv6 nd autoconfig other-flag
```

- Managed Address Flag (M flag): Informs whether hosts should use stateful configuration for IP addresses.
- Other Configuration Flag (O flag): Indicates if other configurations should be obtained through stateful configuration.

1.8 Stateless Address Autoconfiguration on R1

Markdown

```
1. : `undo ipv6 nd ra halt`
2. : `ipv6 address auto global`
```

R2:

Markdown

```
[R2]interface GigabitEthern0/0/2
```

```
[R2-GigabitEthernet0/0/2]undo ipv6 nd ra halt
[R2-GigabitEthernet0/0/2]interface GigabitEthern0/0/1
[R2-GigabitEthernet0/0/1]undo ipv6 nd ra halt
```

> Enable RA reception

R1:

```Markdown
[R1]interface GigabitEthern0/0/1
[R1-GigabitEthernet0/0/1]ipv6 address auto global
```

> Activate stateless autoconfiguration

R3:

```Markdown
[R3]interface GigabitEthern0/0/2
[R3-GigabitEthernet0/0/2]ipv6 address auto global
```

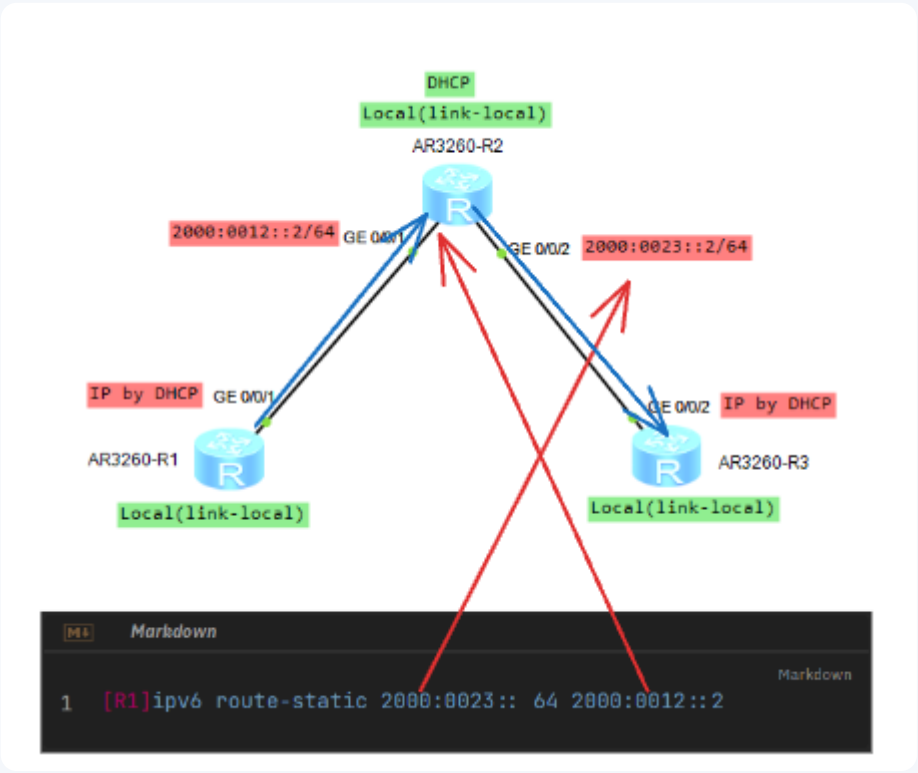
> Activate stateless autoconfiguration

> Stateless mode allows devices to automatically generate their own IP addresses based on received prefixes.

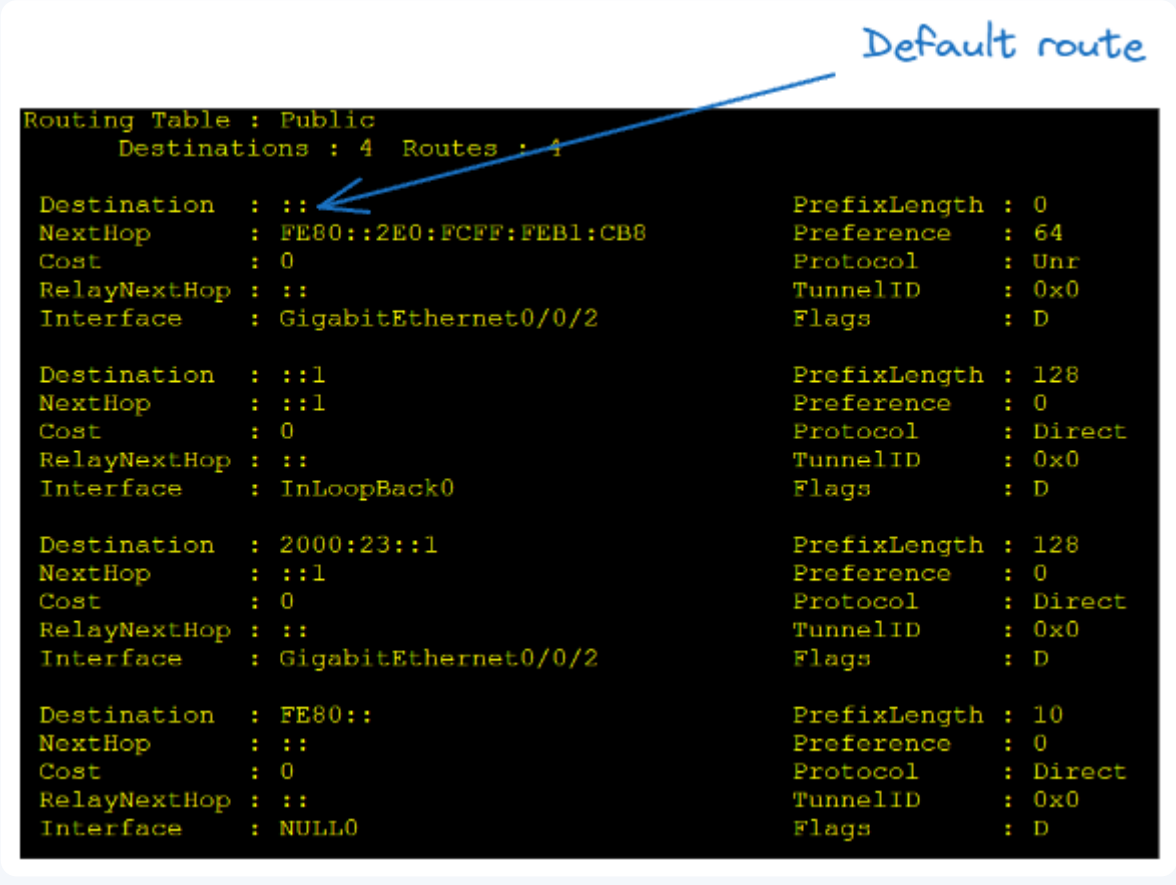
1.9 Static Route Configuration for Connectivity Between R1 and R3

```Markdown
[R1]ipv6 route-static 2000:0023:: 64 2000:0012::2
```

> Add static route on R1 towards network of R3



R3:



> **Note**
>
> R1 has a static route to the network 2000:23::/64. R3 obtains the default route through DHCPv6. Therefore, GigabitEthernet0/0/3 on R1 and GigabitEthernet0/0/3 on R3 can communicate with each other

Test connectivity:

```
[R1]ping ipv6 2000:23::1
  PING 2000:23::1 : 56  data bytes, press CTRL_C to break
    Reply from 2000:23::1
    bytes=56 Sequence=1 hop limit=63   time = 20 ms
    Reply from 2000:23::1
    bytes=56 Sequence=2 hop limit=63   time = 20 ms
    Reply from 2000:23::1
    bytes=56 Sequence=3 hop limit=63   time = 30 ms
    Reply from 2000:23::1
    bytes=56 Sequence=4 hop limit=63   time = 20 ms
    Reply from 2000:23::1
    bytes=56 Sequence=5 hop limit=63   time = 30 ms

  --- 2000:23::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 20/24/30 ms
```

1.10 Verification Commands

Display current IP configuration:

R2:

```
*down: administratively down
(l): loopback
(s): spoofing
Interface                         Physical
GigabitEthernet0/0/1              up
[IPv6 Address] 2000:12::2
GigabitEthernet0/0/2              up
[IPv6 Address] 2000:23::2
```

Check routing table entries:

R2:

```
Routing Table : Public
      Destinations : 6  Routes : 6

 Destination  : ::1                              PrefixLength : 128
 NextHop      : ::1                              Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : InLoopBack0                      Flags        : D

 Destination  : 2000:12::                        PrefixLength : 64
 NextHop      : 2000:12::2                       Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1             Flags        : D

 Destination  : 2000:12::2                       PrefixLength : 128
 NextHop      : ::1                              Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/1             Flags        : D

 Destination  : 2000:23::                        PrefixLength : 64
 NextHop      : 2000:23::2                       Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/2             Flags        : D

 Destination  : 2000:23::2                       PrefixLength : 128
 NextHop      : ::1                              Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : GigabitEthernet0/0/2             Flags        : D

 Destination  : FE80::                           PrefixLength : 10
 NextHop      : ::                               Preference   : 0
 Cost         : 0                                Protocol     : Direct
 RelayNextHop : ::                               TunnelID     : 0x0
 Interface    : NULL0                            Flags        : D
```

Validate neighbor discovery cache entries:

R2:

```
--------------------------------------------------------------------------------
IPv6 Address : 2000:12::2E0:FCFF:FE29:7399
Link-layer   : 00e0-fc29-7399                    State : STALE
Interface    : GE0/0/1                           Age   : 21
VLAN         : -                                 CEVLAN: -
VPN name     :                                   Is Router: TRUE
Secure FLAG  : UN-SECURE

IPv6 Address : FE80::2E0:FCFF:FE29:7399
Link-layer   : 00e0-fc29-7399                    State : STALE
Interface    : GE0/0/1                           Age   : 21
VLAN         : -                                 CEVLAN: -
VPN name     :                                   Is Router: TRUE
Secure FLAG  : UN-SECURE

IPv6 Address : 2000:23::1
Link-layer   : 00e0-fccf-7091                    State : DELAY
Interface    : GE0/0/2                           Age   : 53
VLAN         : -                                 CEVLAN: -
VPN name     :                                   Is Router: TRUE
Secure FLAG  : UN-SECURE

IPv6 Address : FE80::2E0:FCFF:FECF:7091
Link-layer   : 00e0-fccf-7091                    State : STALE
Interface    : GE0/0/2                           Age   : 21
VLAN         : -                                 CEVLAN: -
VPN name     :                                   Is Router: TRUE
Secure FLAG  : UN-SECURE

--------------------------------------------------------------------------------
Total: 4        Dynamic: 4        Static: 0
```

1.11 Quiz

Question1

Why the source interface must be specified in Step 3 (testing the connectivity between link-local addresses) but not in Step 7 (testing the connectivity between GUA addresses)?

Answer1

- The source interface must be specified when testing link-local addresses because these addresses are only valid on their specific interface and are not routable, so the system needs to know which interface to use. For Global Unicast Addresses (GUAs), the system can determine the

appropriate source address/interface based on routing tables, hence it's not necessary to specify.

- The router has multiple interfaces on the FE80::/10 network. When the destination IPv6 address is a link-local address, the outgoing interface cannot be determined by querying the routing table. Therefore, the source interface must be specified

Question2

Describe the difference between stateful address configuration and stateless address configuration and explain why.

Answer2

- Stateful configuration involves a server (like DHCP) assigning IP addresses and other network settings to clients, while stateless configuration (SLAAC) allows devices to self-configure their own IP addresses without a centralized server.
- In stateful mode, all the 128 bits in an IPv6 interface address are specified by the DHCPv6 server. In stateless mode, a 64-bit interface ID is generated based on the EUI-64 specification

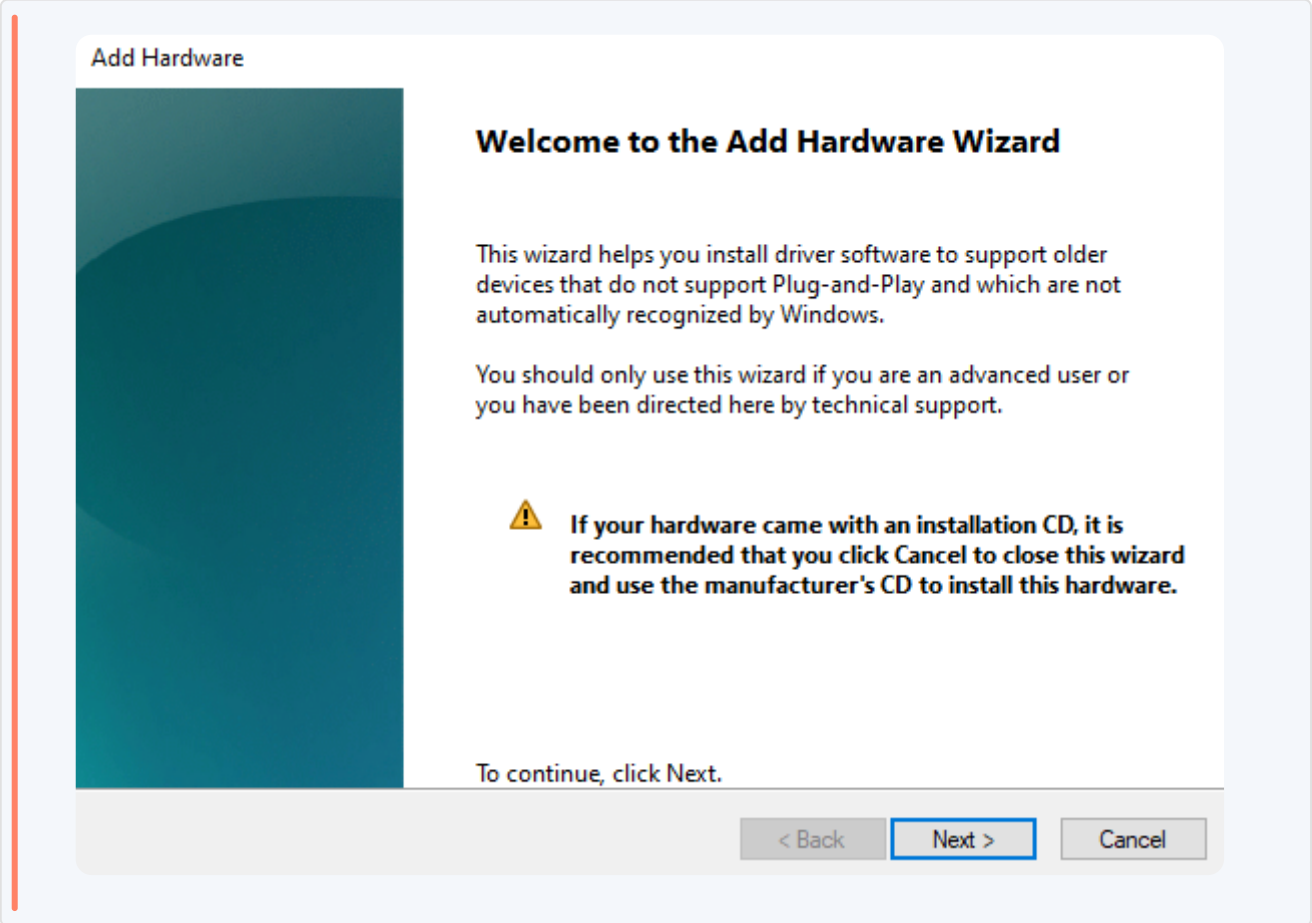
Lab8

1 Lab8 Network Programming and Automation Bas

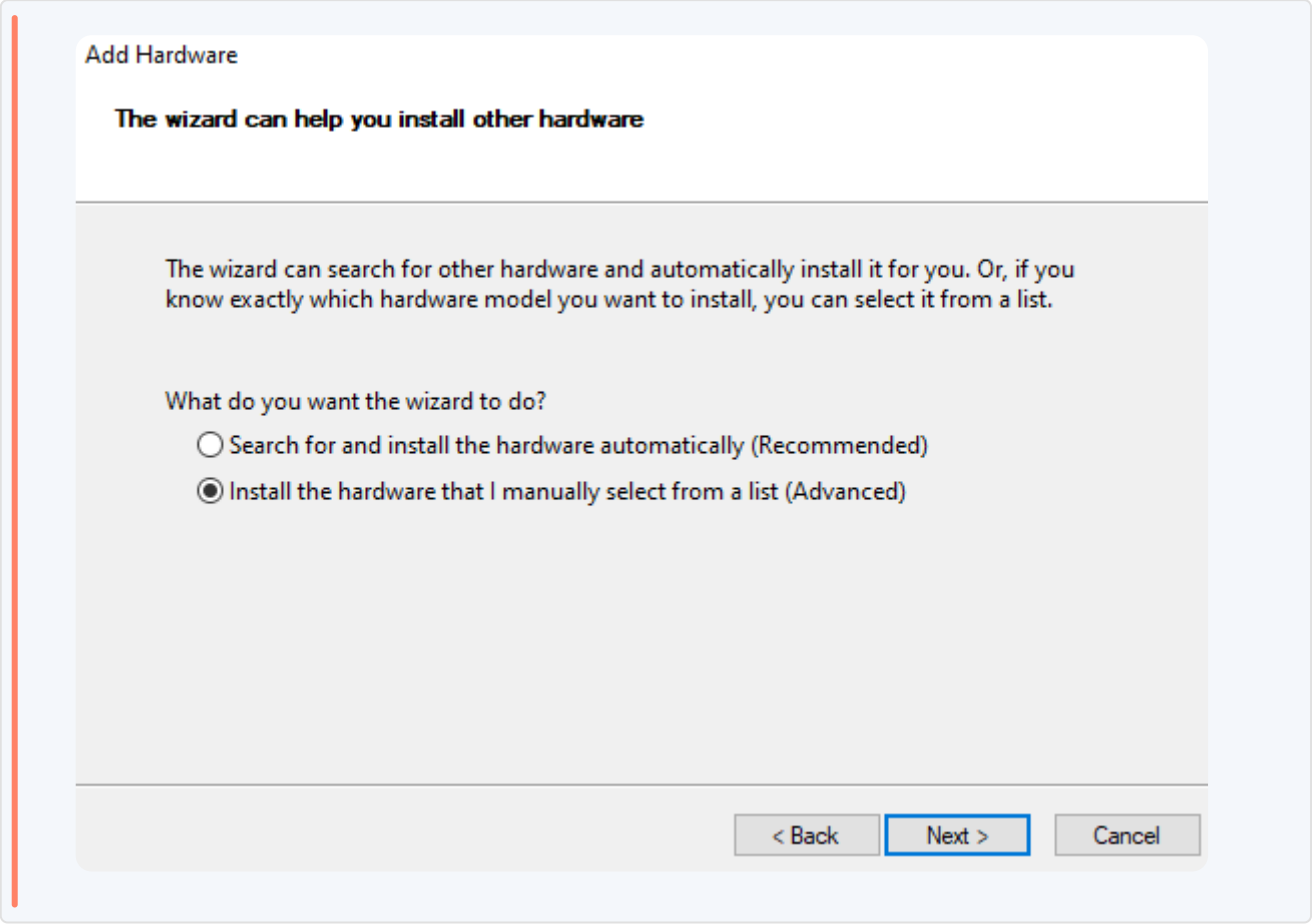
1.1 Connecting PC to eNSP

> This section is about establishing a connection between your physical computer and the eNSP simulation environment.

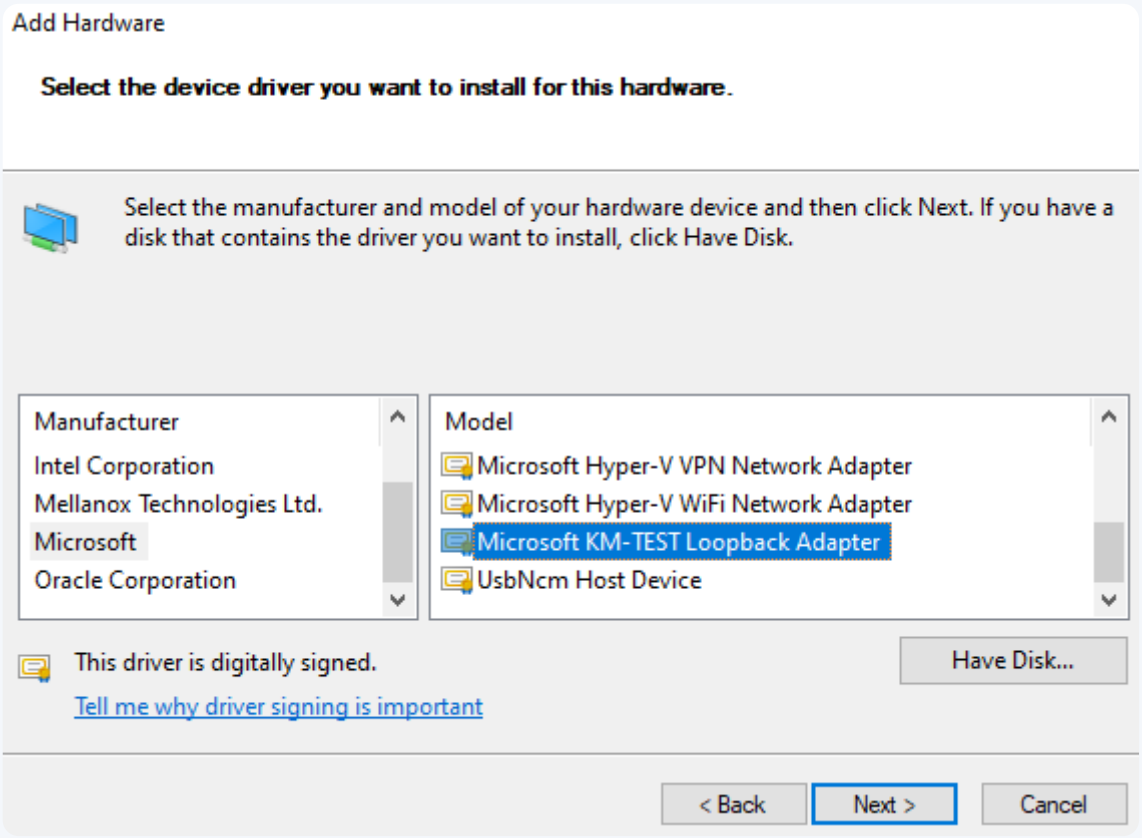
1.1.1 Add a microsoft loobpack interface



From device manger then select your device then action then add legacy hardware

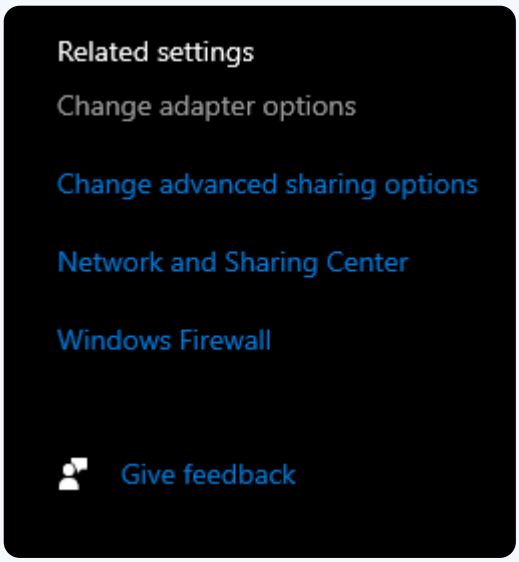


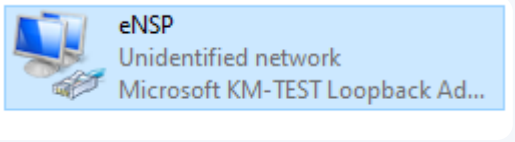
Then choice Network adapter



After initiating the addition of legacy hardware, you would select "Network adapter" from the list of hardware types. This will allow you to manually install a network adapter that can be used within the eNSP simulation.

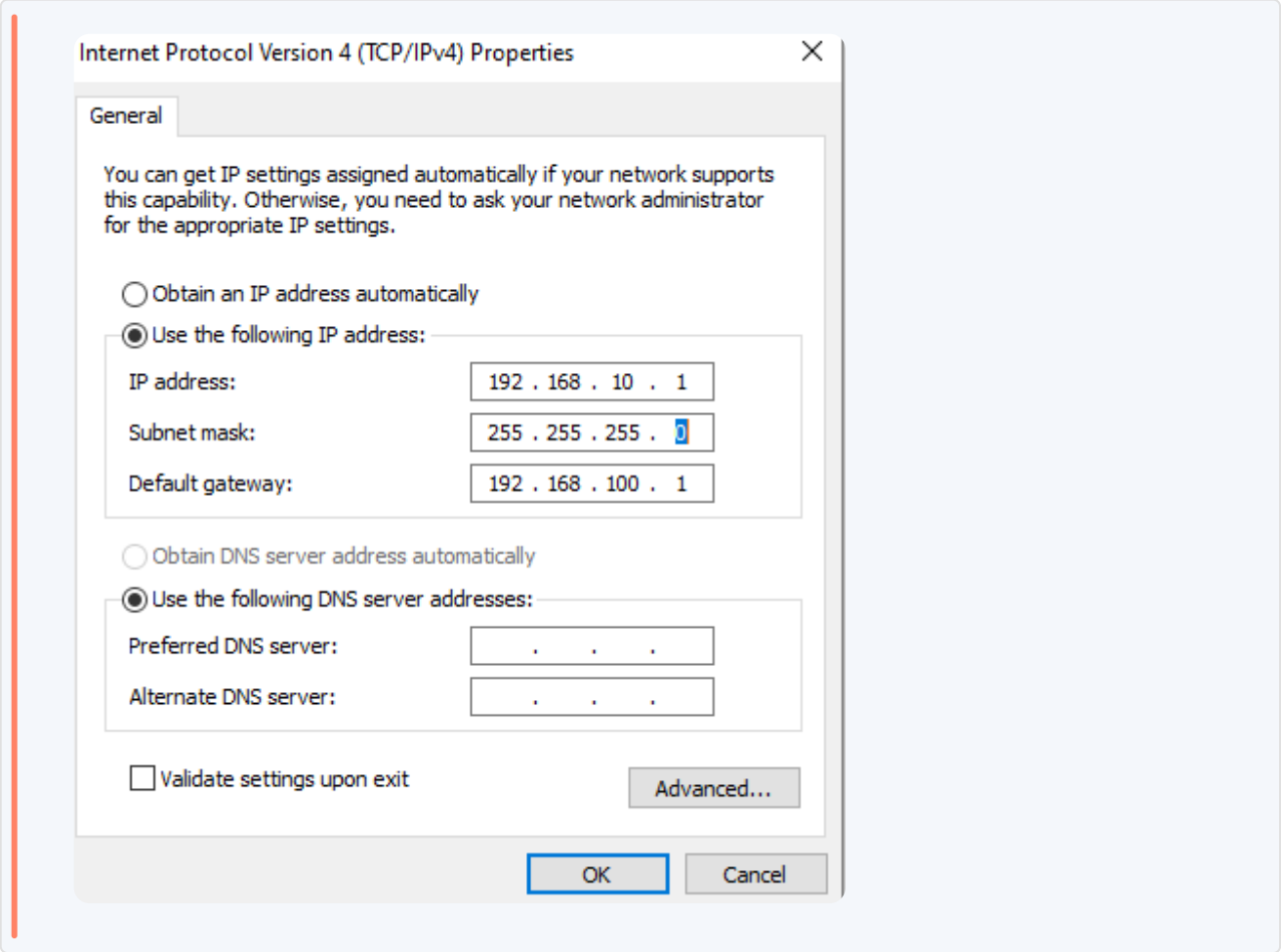
1.1.2 Rename the network adapter to eNSP



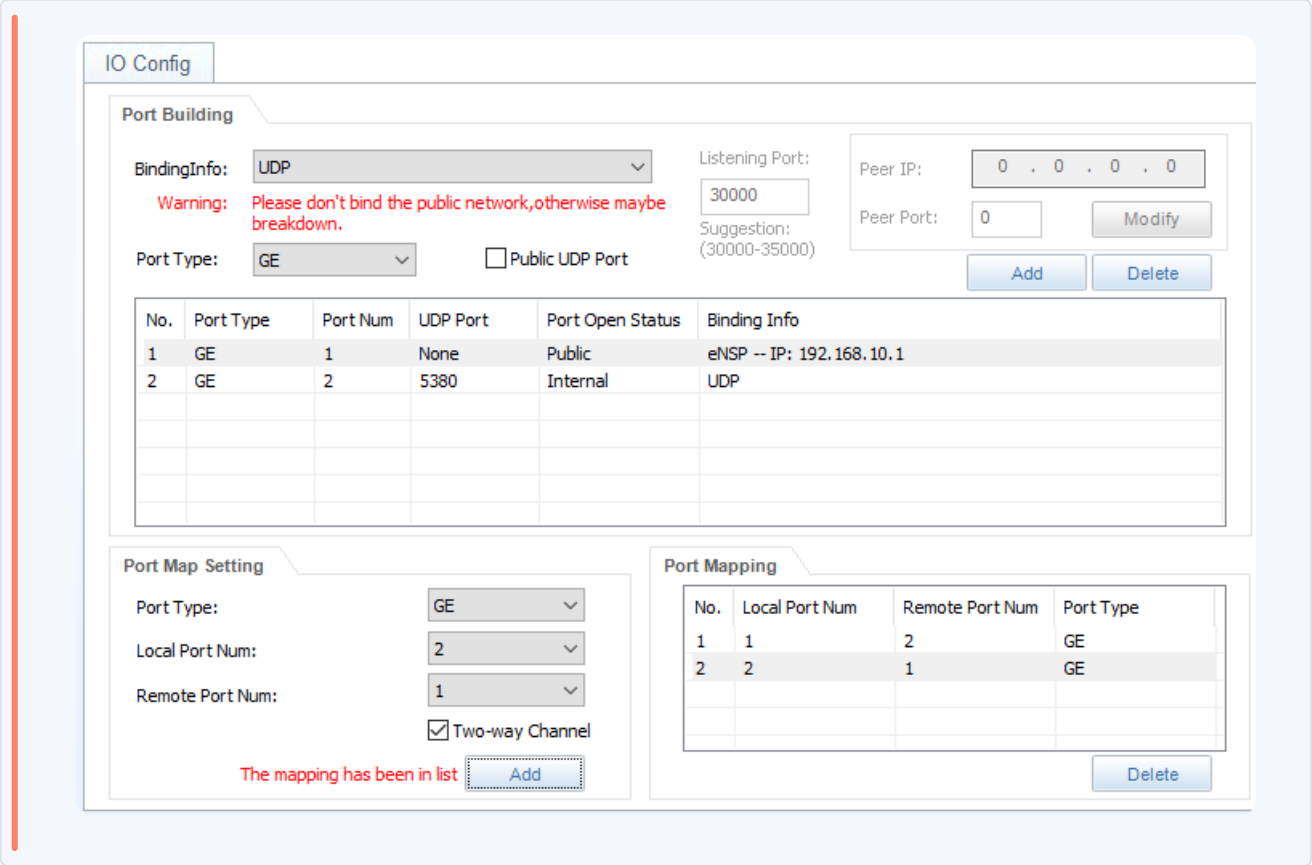


Once the network adapter is installed, you are instructed to rename it to "eNSP." This step is probably done for easier identification when configuring network simulations in eNSP.

1.1.3 Put at IP address 192.168.10.2/24



1.1.4 Open eNSP and connect the cloud to the router



1.1.5 Put an IP address on the router 192.168.10.2/24

> Make sure loopback for physical device in same domain as in ensp environment

1.1.6 ping from your pc to router

```
C:\Users\Bakaito>ping 192.168.10.101

Pinging 192.168.10.101 with 32 bytes of data:
Reply from 192.168.10.101: bytes=32 time=2ms TTL=255
Reply from 192.168.10.101: bytes=32 time=9ms TTL=255
Reply from 192.168.10.101: bytes=32 time=5ms TTL=255
```

1.2 Introduction

1.2.1 About This Lab

After completing this lab activity, you will learn how to use Python `telnetlib` for network automation.

1.2.2 Objectives

- Understand basic Python syntax.
- Learn to use `telnetlib` for network tasks.

1.2.3 Networking Topology

A company's switch has a management IP address of `192.168.56.101/24`. The task is to automate viewing the current configuration file of the device.

1.3 Lab Configuration

1.3.1 Configuration Roadmap

1. **Configure Telnet**: Set up Telnet access with a password.

2. **Compile a Python script**: Use `telnetlib` to log into the device and retrieve its configuration.

1.3.2 Configuration Procedure

1.3.2.1 Step 1: Configure ip address on interface

```
[S1]interface vlanif1
[S1-vlanif1]ip address 192.168.10.101 24
```

1.3.2.2 Step 2: Configure Telnet on the Switch

```
[S1]user-interface vty 0 4
[S1-ui-vty0-4]authentication-mode password
[S1-ui-vty0-4]set authentication password simple Huawei@123
[S1-ui-vty0-4]protocol inbound telnet
[S1-ui-vty0-4]user privilege level 15
[S1]q
[S1]telnet server enable
```

> Set up a Telnet login password.

> Enable Telnet service for access.

1.3.2.3 Step 3: Write the Python Code

Python

```python
import telnetlib
import time

# Define the host and password for your device
host = '192.168.56.101'
password = 'Huawei@123'

# Establish a connection to the host using Telnet on default port 23
tn = telnetlib.Telnet(host)

# Read until the password prompt appears
tn.read_until(b"Password:")

# Send the password followed by a newline character to simulate pressing Enter
tn.write(password.encode('ascii') + b"\n")

# Send command to display current configuration on the device
tn.write(b'display cu \n')

# Wait for one second to ensure command execution is complete before proceeding
time.sleep(1)

# Read any data available from output buffer, decode it from ASCII, and print it out
print(tn.read_very_eager().decode('ascii'))

# Close Telnet session after completing tasks
tn.close()
```

Code Interpretation

`telnetlib` for Telnet communication and `time` for pausing the script execution when necessary.

define the IP address of the host (network device) and the corresponding password. We then create a Telnet object (`tn`) that connects to this host. The script waits until it encounters the "Password:" prompt before sending over the encoded password with an appended newline character (`\n`) to log in.

After successfully logging into the network device, we use `write()` method of our Telnet object (`tn`) to issue commands to it. In this case, we send over `"display cu \n"` which is a shorthand command for displaying current configuration settings on Huawei devices. A brief pause is introduced with `time.sleep(1)` to allow time for command execution and output generation. Finally, we read eagerly any available data from output buffer, decode it from ASCII encoding, and print it on console.

The last step involves closing our Telnet session by calling `close()` method on our Telnet object (`tn`). This is important because network devices typically have limited VTY (Virtual Teletype) connections available; closing sessions ensures these resources are freed up for other users or processes.

1.3.2.4 Step 4: Execute the Compiler

Use Jupyter Notebook or any other preferred compiler to run the script.

1.3.2.5 Step 5: Output Example

```
D:\Shared\Huawei\HCIA\Labs\Lab13>py Script.py
D:\Shared\Huawei\HCIA\Labs\Lab13\Script.py:1: DeprecationWarning: 'telnetlib' is deprecated and slated for removal in Python 3.13
  import telnetlib

Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 2.
      The current login time is 2024-04-22 00:02:23.
<S1>display cu
#
sysname S1
#
cluster enable
ntdp enable
ndp enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password simple admin
 local-user admin service-type http
#
interface Vlanif1
 ip address 192.168.56.101 255.255.0.0
  ---- More ----

D:\Shared\Huawei\HCIA\Labs\Lab13>
D:\Shared\Huawei\HCIA\Labs\Lab13>
```

1.4 Quiz Questions for Revision

Question1&2

Q1: How do you use `telnetlib` to configure a device, such as setting the IP address of its management interface?

Q2: How do you save the configuration file to a local directory?

Python

```python
import telnetlib
import time

#  Set variables for the host IP address and host
host = '192.168.56.101'
password = 'huawei'

# Create a Telnet session to the host.
tn = telnetlib.Telnet(host)
tn.read_until(b"Password:")
```

```
11
12  # Send the password followed by a newline character to
    log in.
13  tn.write(password.encode('ascii') + b"\n")
14
15  # Enter system view mode on the device by sending
    "system-view".
16  tn.write(b'system-view \n')
17
18  #  Select interface `gig0/0/1` by sending "interface
    gig0/0/1".
19  tn.write(b'interface gig0/0/1 \n')
20
21  # Assign IP address `192.168.56.101` to that interface
    with "ip address 192.168.56.101".
22  tn.write(b'ip address 192.168.56.101 \n')
23
24  # Exit from interface configuration mode with "q"
    (quit).
25  tn.write(b'quit \n')
26
27  # Save the configuration changes with "save".
28  tn.write(b'save \n')
29  time.sleep(1)
30
31  # Close the Telnet connection.
32  tn.close()
```

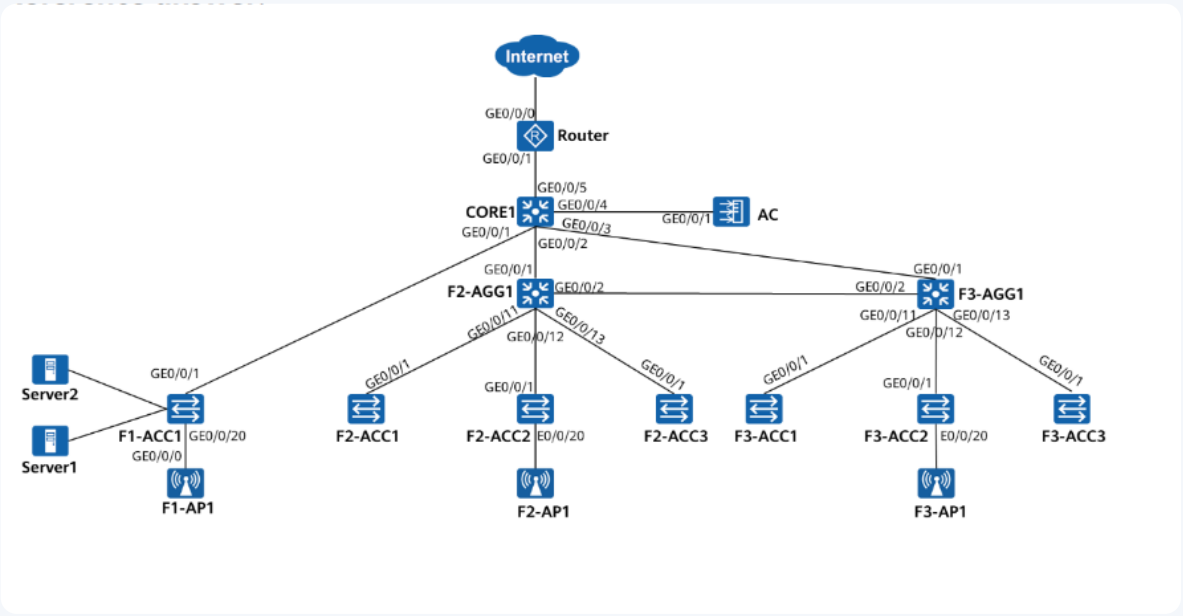
Lab9

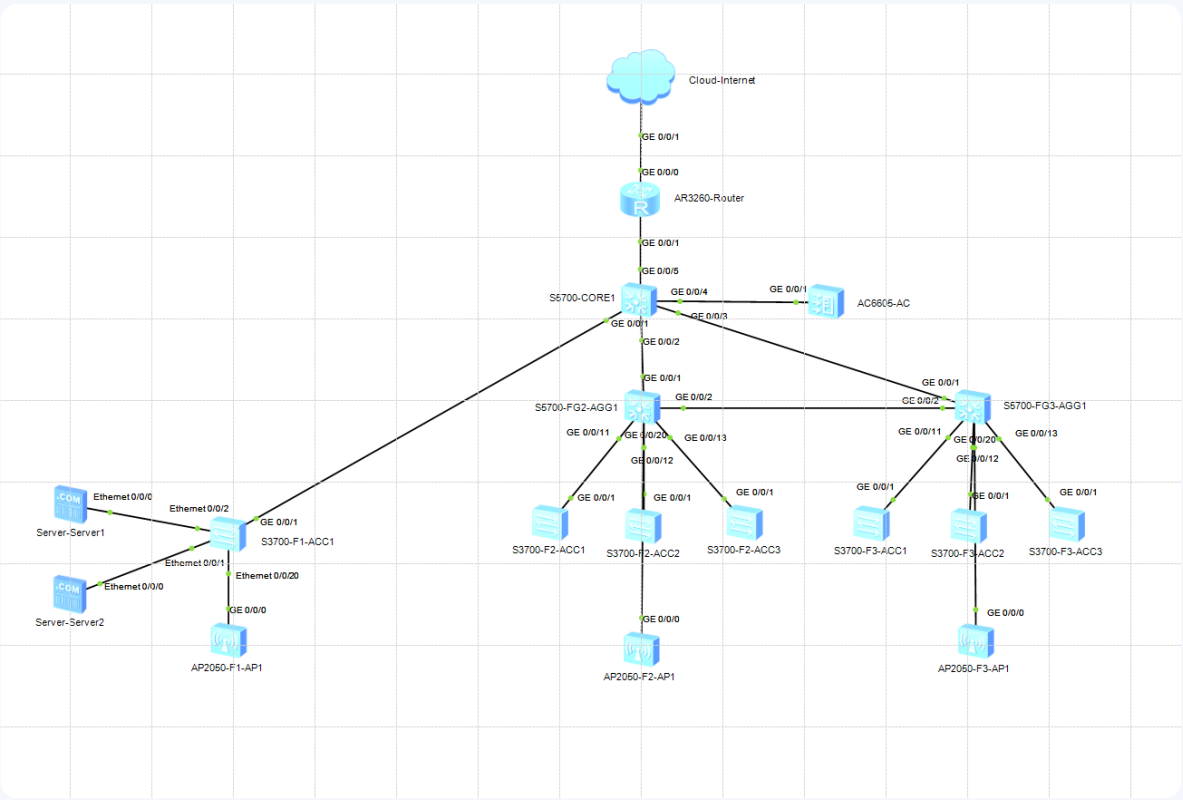
1 Lab9 Configuring a Campus Network

1.1 Introduction

- Campus networks are crucial for digital connectivity in various settings such as factories, government buildings, shopping malls, etc.
- They support daily work, R&D, production, and management activities.
- The lab activity involves creating a campus network to understand common technologies and their practical applications.

1.2 Networking Topology





- Network construction is needed for a six-floor office building with three floors currently in use.
- Core equipment is on the first floor; networking devices are on each floor.

1.2.1 Requirement Collection and Analysis

Collect information such as:

1. Number of wired/wireless terminals
2. Project budget
3. Terminal types
4. Network management mode (e.g., SNMP)
5. Traffic volume and patterns
6. Redundancy and failover requirements
7. Security needs
8. Internet access method
9. Future expansion plans

1.2.2 Planning and Design Task

Design a physical topology for the network considering:

- Device selection based on terminal counts (wired: 10+200+200+500; wireless: 100+50+50+200)
- Ensure bandwidth requirements (100 Mbit/s for computers, 2 Mbit/s per wireless client)
- Deploy at least three dual-band APs per floor for quality wireless access

1.3 Layer 2 Network Design

Requirements:

1. **Wired Network VLANs:**
    - Assign ports GE0/0/1 to GE0/0/10 on the core equipment room's access switch to a single VLAN for server connectivity.
    - In the general manager's office on the second floor (connected via F2-ACC2), create a unique VLAN separate from the administrative department's VLAN.

- On the third floor, allocate ports E0/0/1 to E0/0/10 on switches F3-ACC1 and F3-ACC3 to the marketing department's VLAN; assign ports E0/0/11 to E0/0/20 for R&D department use.
- Designate all ports from E0/0/1 to E0/0/19 on F3-ACC2 for marketing department VLAN access.

2. **Wireless Network VLANs:**
    - Ensure wireless terminals across different floors are assigned distinct VLANs.
    - Implement individual wireless network management VLANs specific to each floor.
      Proposed VLAN Structure:

- **Servers:** VLAN 100
- **General Manager's Office (second floor):** VLAN 101
- **Administrative Department (second floor):** VLAN 102
- **Marketing Department (third floor):** VLAN 103
- **R&D Department (third floor):** VLAN 104
- **Wireless Terminals:**
    - **First Floor:** VLAN 105
    - **Second Floor:** VLAN 106
    - **Third Floor:** VLAN 107
- **Layer 2 Management:**
    - **First Floor:** VLAN 1
    - **Second Floor:** VLAN 2
    - **Third Floor:** VLAN 3
- **Additional Interconnection and Management:**
    - **F2-AGG1 to CORE1 Link:** VL201
        - **F3-AGG1 to CORE1 Link**: VL202
        - **F2-AGG1 to F3-AGG1 Link:** VL203
        - **CORE1to Router Link :** VL204
- **Wireless Network Management VLANS :**

- **First Floor :** VL205
- **Second Floor :** VL206
- **ThirdFloor :** VL207

VLAN ID	Description
1	Management VLAN - 1st Floor Layer 2 Devices
2	Management VLAN - 2nd Floor Layer 2 Devices
3	Management VLAN - 3rd Floor Layer 2 Devices
100	Servers VLAN
101	General Manager's Office VLAN
102	Administrative Department VLAN
103	Marketing Department VLAN
104	R&D Department VLAN
105	Wireless Terminals VLAN - 1st Floor
106	Wireless Terminals VLAN - 2nd Floor
107	Wireless Terminals VLAN - 3rd Floor
201	Interconnect F2-AGG1 to CORE1
202	Interconnect F3-AGG1 to CORE1
203	Interconnect F2-AGG1 to F3-AGG1
204	Interconnect CORE1 to Router
205	Wireless Network Management VLAN - 1st Floor
206	Wireless Network Management VLAN - 2nd Floor
207	Wireless Network Management VLAN - Third Floor

1.3.1 CORE1 Switch Configuration

Markdown

```
[CORE1]interface GigabitEthernet0/0/1
[CORE1-GigabitEthernet0/0/1]port link-type trunk
[CORE1-GigabitEthernet0/0/1]port trunk allow-pass vlan
100 105 205
```

```
ORE1-GigabitEthernet0/0/1]interface
gabitEthernet0/0/2
ORE1-GigabitEthernet0/0/2]port link-type access
ORE1-GigabitEthernet0/0/2]port default vlan 201
ORE1-GigabitEthernet0/0/2]interface
gabitEthernet0/0/3
ORE1-GigabitEthernet0/0/3]port link-type access
ORE1-GigabitEthernet0/0/3]port default vlan 202
ORE1-GigabitEthernet0/0/3]interface
GigabitEthernet0/0/4
[CORE1-GigabitEthernet0/0/4]port link-type access
[CORE1-GigabitEthernet0/0/4]port default vlan 205
[CORE1-GigabitEthernet0/0/4]interface
GigabitEthernet0/0/5
[CORE1-GigabitEthernet0/0/5]port link-type access
[CORE1-GigabitEthernet0/0/5]port default vlan 204
```

Code Explanation

- Sets the port to trunk mode.
- Allows VLANs 100, 105, and 205 to pass through, which are server VLAN, wireless terminals on the first floor, and wireless network management on the first floor respectively.
- Configures the port as an access port with a specified default VLAN for interconnections between switches and routers.
- Each interface is assigned to a different VLAN for segregating traffic.

1.3.2 F2-AGG1 Switch Configuration

Markdown

```
[F2-AGG1]interface GigabitEthernet0/0/1
[F2-AGG1-GigabitEthernet0/0/1]port link-type access
[F2-AGG1-GigabitEthernet0/0/1]port default vlan 201
```

```
[F2-AGG1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2
[F2-AGG1-GigabitEthernet0/0/2]port link-type access
[F2-AGG1-GigabitEthernet0/0/2]port default vlan 203
[F2-AGG1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/11
[F2-AGG1-GigabitEthernet0/0/11]port link-type trunk
[F2-AGG1-GigabitEthernet0/0/11]port trunk pvid vlan 2
[F2-AGG1-GigabitEthernet0/0/11]port trunk allow-pass vlan 2 102
[F2-AGG1-GigabitEthernet0/0/11]interface GigabitEthernet0/0/12
[F2-AGG1-GigabitEthernet0/0/12]port link-type trunk
[F2-AGG1-GigabitEthernet0/0/12]port trunk pvid vlan 2
[F2-AGG1-GigabitEthernet0/0/12]port trunk allow-pass vlan 2 101 106 206
[F2-AGG1-GigabitEthernet0/0/12]interface GigabitEthernet0/0/13
[F2-AGG1-GigabitEthernet0/0/13]port link-type trunk
[F2-AGG1-GigabitEthernet0/0/13]port trunk pvid vlan 2
[F2-AGG1-GigabitEthernet0/0/13]port trunk allow-pass vlan 2 102
```

Code Explanation

- Configures the port as an access port for interconnection with CORE1 (vlan 201).
- Configured as trunk ports to manage traffic from multiple VLANs - General Manager's Office (vlan 101), Administrative Department (vlan 102), and Wireless Networks (vlans 106 & 206).
- Sets up links to other switches for aggregation purposes.
- Assigns appropriate VLANs for these inter-switch connections.
- Configures ports in trunk mode with allowed VLANs for different departments.
- PVID (Primary VLAN ID) is used where untagged frames are assigned this VLAN.

1.3.3 F3-AGG1 Switch Configuration

```
[F3-AGG1]interface GigabitEthernet0/0/1
[F3-AGG1-GigabitEthernet0/0/1]port link-type access
[F3-AGG1-GigabitEthernet0/0/1]port default vlan 202
[F3-AGG1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2
[F3-AGG1-GigabitEthernet0/0/2]port link-type access
[F3-AGG1-GigabitEthernet0/0/2]port default vlan 203
[F3-AGG1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/11
[F3-AGG1-GigabitEthernet0/0/11]port link-type trunk
[F3-AGG1-GigabitEthernet0/0/11]port trunk pvid vlan 3
[F3-AGG1-GigabitEthernet0/0/11]port trunk allow-pass vlan 3 103 to 104
[F3-AGG1-GigabitEthernet0/0/11]interface GigabitEthernet0/0/12
[F3-AGG1-GigabitEthernet0/0/12]port link-type trunk
[F3-AGG1-GigabitEthernet0/0/12]port trunk pvid vlan 3
[F3-AGG1-GigabitEthernet0/0/12]port trunk allow-pass vlan 3 103 107 207
[F3-AGG1-GigabitEthernet0/0/12]interface GigabitEthernet0/0/13
[F3-AGG1-GigabitEthernet0/0/13]port link-type trunk
[F3-AGG1-GigabitEthernet0/0/13]port trunk pvid vlan 3
[F3-AGG1-GigabitEthernet0/0/13]port trunk allow-pass vlan 3 103 to 104
```

Code Explanation

- Similar configuration logic applies here as with F2-AGG1 but this time for third-floor departments like Marketing (vlan 103) and R&D (vlan 104), along with Wireless Networks (vlans 107 & 207).

- Specifies ports in trunk mode with permitted VLANs for different departments on the third floor.

1.3.4 Access Switches Configuration

1.3.4.1 Specific Floor Configurations

Each floor has its specific configuration based on departmental requirements:

1.3.4.1.1 First Floor Access Switches (F1-ACC1-2)

Markdown

```
[F1-ACC1]interface GigabitEthernet0/0/1
[F1-ACC1-GigabitEthernet0/0/1]port link-type trunk
[F1-ACC1-GigabitEthernet0/0/1]port trunk allow-pass vlan 100 105 205
[F1-ACC1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2
[F1-ACC1-GigabitEthernet0/0/2]port link-type access
[F1-ACC1-GigabitEthernet0/0/2]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/3
[F1-ACC1-GigabitEthernet0/0/3]port link-type access
[F1-ACC1-GigabitEthernet0/0/3]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/3]interface GigabitEthernet0/0/4
[F1-ACC1-GigabitEthernet0/0/4]port link-type access
[F1-ACC1-GigabitEthernet0/0/4]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/4]interface GigabitEthernet0/0/5
```

```
[F1-ACC1-GigabitEthernet0/0/5]port link-type access
[F1-ACC1-GigabitEthernet0/0/5]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/5]interface
GigabitEthernet0/0/6
[F1-ACC1-GigabitEthernet0/0/6]port link-type access
[F1-ACC1-GigabitEthernet0/0/6]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/6]interface
GigabitEthernet0/0/7
[F1-ACC1-GigabitEthernet0/0/7]port link-type access
[F1-ACC1-GigabitEthernet0/0/7]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/7]interface
GigabitEthernet0/0/8
[F1-ACC1-GigabitEthernet0/0/8]port link-type access
[F1-ACC1-GigabitEthernet0/0/8]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/8]interface
GigabitEthernet0/0/9
[F1-ACC1-GigabitEthernet0/0/9]port link-type access
[F1-ACC1-GigabitEthernet0/0/9]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/9]interface
GigabitEthernet0/0/10
[F1-ACC1-GigabitEthernet0/0/10]port link-type access
[F1-ACC1-GigabitEthernet0/0/10]port default vlan 100
[F1-ACC1-GigabitEthernet0/0/10]interface
GigabitEthernet0/0/20
[F1-ACC1-GigabitEthernet0/0/20]port link-type trunk
[F1-ACC1-GigabitEthernet0/0/20]port trunk pvid vlan 205
[F1-ACC1-GigabitEthernet0/0/20]port trunk allow-pass
vlan 105 205
```

Code Explanation

- Configured primarily for server connections (`vlan 100`) and wireless terminals (`vlan 105`).
- Configuration same idea for F1-ACC2

1.3.4.1.2 Second Floor Access Switches (F2-ACC1-3)

Markdown

```
[F2-ACC1]interface Ethernet0/0/1
[F2-ACC1-Ethernet0/0/1]port link-type access
[F2-ACC1-Ethernet0/0/1]port default vlan 102
[F2-ACC1-Ethernet0/0/1]interface Ethernet0/0/2
[F2-ACC1-Ethernet0/0/2]port link-type access
[F2-ACC1-Ethernet0/0/2]port default vlan 102
[F2-ACC1-Ethernet0/0/2]interface Ethernet0/0/3
[F2-ACC1-Ethernet0/0/3]port link-type access
[F2-ACC1-Ethernet0/0/3]port default vlan 102
[F2-ACC1-Ethernet0/0/3]interface Ethernet0/0/4
[F2-ACC1-Ethernet0/0/4]port link-type access
[F2-ACC1-Ethernet0/0/4]port default vlan 102
[F2-ACC1-Ethernet0/0/4]interface Ethernet0/0/5
[F2-ACC1-Ethernet0/0/5]port link-type access
[F2-ACC1-Ethernet0/0/5]port default vlan 102
[F2-ACC1-Ethernet0/0/5]interface Ethernet0/0/6
[F2-ACC1-Ethernet0/0/6]port link-type access
[F2-ACC1-Ethernet0/0/6]port default vlan 102
[F2-ACC1-Ethernet0/0/6]interface Ethernet0/0/7
[F2-ACC1-Ethernet0/0/7]port link-type access
[F2-ACC1-Ethernet0/0/7]port default vlan 102
[F2-ACC1-Ethernet0/0/7]interface Ethernet0/0/8
[F2-ACC1-Ethernet0/0/8]port link-type access
[F2-ACC1-Ethernet0/0/8]port default vlan 102
[F2-ACC1-Ethernet0/0/8]interface Ethernet0/0/9
[F2-ACC1-Ethernet0/0/9]port link-type access
[F2-ACC1-Ethernet0/0/9]port default vlan 102
[F2-ACC1-Ethernet0/0/9]interface Ethernet0/0/10
[F2-ACC1-Ethernet0/0/10]port link-type access
[F2-ACC1-Ethernet0/0/10]port default vlan 102
[F2-ACC1-Ethernet0/0/10]interface Ethernet0/0/11
[F2-ACC1-Ethernet0/0/11]port link-type access
[F2-ACC1-Ethernet0/0/11]port default vlan 102
```

```
[F2-ACC1-Ethernet0/0/11]interface Ethernet0/0/12
[F2-ACC1-Ethernet0/0/12]port link-type access
[F2-ACC1-Ethernet0/0/12]port default vlan 102
[F2-ACC1-Ethernet0/0/12]interface Ethernet0/0/13
[F2-ACC1-Ethernet0/0/13]port link-type access
[F2-ACC1-Ethernet0/0/13]port default vlan 102
[F2-ACC1-Ethernet0/0/13]interface Ethernet0/0/14
[F2-ACC1-Ethernet0/0/14]port link-type access
[F2-ACC1-Ethernet0/0/14]port default vlan 102
[F2-ACC1-Ethernet0/0/14]interface Ethernet0/0/15
[F2-ACC1-Ethernet0/0/15]port link-type access
[F2-ACC1-Ethernet0/0/15]port default vlan 102
[F2-ACC1-Ethernet0/0/15]interface Ethernet0/0/16
[F2-ACC1-Ethernet0/0/16]port link-type access
[F2-ACC1-Ethernet0/0/16]port default vlan 102
[F2-ACC1-Ethernet0/0/16]interface Ethernet0/0/17
[F2-ACC1-Ethernet0/0/17]port link-type access
[F2-ACC1-Ethernet0/0/17]port default vlan 102
[F2-ACC1-Ethernet0/0/17]interface Ethernet0/0/18
[F2-ACC1-Ethernet0/0/18]port link-type access
[F2-ACC1-Ethernet0/0/18]port default vlan 102
[F2-ACC1-Ethernet0/0/18]interface Ethernet0/0/19
[F2-ACC1-Ethernet0/0/19]port link-type access
[F2-ACC1-Ethernet0/0/19]port default vlan 102
[F2-ACC1-Ethernet0/0/19]interface Ethernet0/0/20
[F2-ACC1-Ethernet0/0/20]port link-type access
[F2-ACC1-Ethernet0/0/20]port default vlan 102
[F2-ACC1-Ethernet0/0/20]interface Ethernet0/0/21
[F2-ACC1-Ethernet0/0/21]port link-type access
[F2-ACC1-Ethernet0/0/21]port default vlan 102
[F2-ACC1-Ethernet0/0/21]interface Ethernet0/0/22
[F2-ACC1-Ethernet0/0/22]port link-type access
[F2-ACC1-Ethernet0/0/22]port default vlan 102
[F2-ACC1-GigabitEthernet0/0/1]interface
GigabitEthernet0/0/1
[F2-ACC1-GigabitEthernet0/0/1]port link-type trunk
```

```
[F2-ACC1-GigabitEthernet0/0/1]port trunk pvid vlan 2
[F2-ACC1-GigabitEthernet0/0/1]port trunk allow-pass
vlan 2 102
```

Code Explanation

- Configured for General Manager's Office (`vlan 101`) and Administrative Department (`vlan 102`). Separate wireless network configurations are also included (`vlans 106 & 206`).
- Configuration same idea for F2-ACC2 and F2-ACC3

1.3.4.1.3 Third Floor Access Switches (F3-ACCX)

Markdown

```
[F3-ACC1]interface Ethernet0/0/1
[F3-ACC1-Ethernet0/0/1]port link-type access
[F3-ACC1-Ethernet0/0/1]port default vlan 103
[F3-ACC1-Ethernet0/0/1]interface Ethernet0/0/2
[F3-ACC1-Ethernet0/0/2]port link-type access
[F3-ACC1-Ethernet0/0/2]port default vlan 103
[F3-ACC1-Ethernet0/0/2]interface Ethernet0/0/3
[F3-ACC1-Ethernet0/0/3]port link-type access
[F3-ACC1-Ethernet0/0/3]port default vlan 103
[F3-ACC1-Ethernet0/0/3]interface Ethernet0/0/4
[F3-ACC1-Ethernet0/0/4]port link-type access
[F3-ACC1-Ethernet0/0/4]port default vlan 103
[F3-ACC1-Ethernet0/0/4]interface Ethernet0/0/5
[F3-ACC1-Ethernet0/0/5]port link-type access
[F3-ACC1-Ethernet0/0/5]port default vlan 103
[F3-ACC1-Ethernet0/0/5]interface Ethernet0/0/6
[F3-ACC1-Ethernet0/0/6]port link-type access
[F3-ACC1-Ethernet0/0/6]port default vlan 103
[F3-ACC1-Ethernet0/0/6]interface Ethernet0/0/7
[F3-ACC1-Ethernet0/0/7]port link-type access
```

```
[F3-ACC1-Ethernet0/0/7]port default vlan 103
[F3-ACC1-Ethernet0/0/7]interface Ethernet0/0/8
[F3-ACC1-Ethernet0/0/8]port link-type access
[F3-ACC1-Ethernet0/0/8]port default vlan 103
[F3-ACC1-Ethernet0/0/8]interface Ethernet0/0/9
[F3-ACC1-Ethernet0/0/9]port link-type access
[F3-ACC1-Ethernet0/0/9]port default vlan 103
[F3-ACC1-Ethernet0/0/9]interface Ethernet0/0/10
[F3-ACC1-Ethernet0/0/10]port link-type access
[F3-ACC1-Ethernet0/0/10]port default vlan 103
[F3-ACC1-Ethernet0/0/10]interface Ethernet0/0/11
[F3-ACC1-Ethernet0/0/11]port link-type access
[F3-ACC1-Ethernet0/0/11]port default vlan 104
[F3-ACC1-Ethernet0/0/11]interface Ethernet0/0/12
[F3-ACC1-Ethernet0/0/12]port link-type access
[F3-ACC1-Ethernet0/0/12]port default vlan 104
[F3-ACC1-Ethernet0/0/12]interface Ethernet0/0/13
[F3-ACC1-Ethernet0/0/13]port link-type access
[F3-ACC1-Ethernet0/0/13]port default vlan 104
[F3-ACC1-Ethernet0/0/13]interface Ethernet0/0/14
[F3-ACC1-Ethernet0/0/14]port link-type access
[F3-ACC1-Ethernet0/0/14]port default vlan 104
[F3-ACC1-Ethernet0/0/14]interface Ethernet0/0/15
[F3-ACC1-Ethernet0/0/15]port link-type access
[F3-ACC1-Ethernet0/0/15]port default vlan 104
[F3-ACC1-Ethernet0/0/15]interface Ethernet0/0/16
[F3-ACC1-Ethernet0/0/16]port link-type access
[F3-ACC1-Ethernet0/0/16]port default vlan 104
[F3-ACC1-Ethernet0/0/16]interface Ethernet0/0/17
[F3-ACC1-Ethernet0/0/17]port link-type access
[F3-ACC1-Ethernet0/0/17]port default vlan 104
[F3-ACC1-Ethernet0/0/17]interface Ethernet0/0/18
[F3-ACC1-Ethernet0/0/18]port link-type access
[F3-ACC1-Ethernet0/0/18]port default vlan 104
[F3-ACC1-Ethernet0/0/18]interface Ethernet0/0/19
[F3-ACC1-Ethernet0/0/19]port link-type access
```

```
[F3-ACC1-Ethernet0/0/19]port default vlan 104
[F3-ACC1-Ethernet0/0/19]interface Ethernet0/0/20
[F3-ACC1-Ethernet0/0/20]port link-type access
[F3-ACC1-Ethernet0/0/20]port default vlan 104
[F3-ACC1-Ethernet0/0/20]interface GigabitEthernet0/0/1
[F3-ACC1-GigabitEthernet0/0/1]port link-type trunk
[F3-ACC1-GigabitEthernet0/0/1]port trunk pvid vlan 3
[F3-ACC1-GigabitEthernet0/0/1]port trunk allow-pass
vlan 3 103 to 104
```

Code Explanation

- Configured similarly with departments separated into Marketing (`vlan 103`) and R&D (`vlan104`). The wireless networks have their respective VLAN IDs (`vlans107 &207`).
- Configuration same idea for F3-ACC2 and F3-ACC3

1.4 Layer 3 Network Design

Layer 3 Network Design

- **Address Range:** 192.168.0.0/16
- **First Floor:**
  - **Servers:** Static IPs, Gateway = CORE1
  - **Wireless devices/APs:** DHCP by CORE1
  - **Access Switches:** Static management IPs, Gateway = CORE1
- **Second & Third Floors:**
  - **All Devices/APs:** DHCP by respective aggregation switch
  - **Access Switches:** Static management IPs, Gateway = respective aggregation switch
- **Routing Protocol:** OSPF for network-wide connectivity
- Internet Access through the router

Network	Address Assignment Method	Gateway	Routing Configuration	Network Description
192.168.1.0/24	Static addresses	CORE1	Default route to CORE1	L2 management network, first floor
192.168.2.0/24	Static addresses	F2-AGG1	Default route to F2-AGG1	L2 management network, second floor
192.168.3.0/24	Static addresses	F3-AGG	Default route to F3-AGG	L2 management network, third floor
192.168.100.0/24	Static addresses	CORE1	OSPF through gateway devices	Server network
192.168.101.0/24	DHCP (F2-AGG1)	F2-AGG1	OSPF through gateway devices	General Manager's Office network
192.168.102.0/24	DHCP (F2-AGG1)	F2-AGG1	OSPF through gateway devices	Administrative Department network
192.168.103.0/24	DHCP (F3-AGG1)	F3-AGG1	OSPF through gateway devices	Marketing Department network
192.168.104.0/24	DHCP (F3-AGG1)	F3-AGG1	OSPF through gateway devices	R&D Department network
192.168.105.0/24	DHCP (CORE1)	CORE1	OSPF through gateway devices	Wireless terminals network, first floor

Network	Address Assignment Method	Gateway	Routing Configuration	Network Description
192.168.106.0/24	DHCP (F2-AGG1)	F2-AGG1	OSPF through gateway devices	Wireless terminals network, second floor
192.168.107.0/24	DHCP (F3-AGG1)	F3-AGG1	Advertised in OSPF through gateway devices	Wireless terminals on the third floor
192.168.201.0/30	Static addresses	None	OSPF, neighbor relationship & default route	Interconnectior between F2-AGG1 and CORE1
192.168.202.0/30	Static addresses	None	OSPF, neighbor relationship & default route	Interconnectior between F3-AGG1 and CORE1
192.168.203.0/30	Static addresses	None	OSPF, neighbor relationship & default route	Interconnectior between F2-AGG1 and F3-AGG1
192.168.204.0/30	Static addresses	None	OSPF, neighbor relationship & default route	Interconnectior between CORE1 and router
192.168.205.0/24	DHCP (CORE1)	CORE1	Advertised in OSPF through gateway devices	Wireless network management network on the first floor
192.168.206.0/24	DHCP (F2-AGG1)	F2-AGG1	Advertised in OSPF through gateway devices	Wireless network management network on the second floor
192.168.207.0/24	DHCP (F3-AGG1)	F3-AGG1	Advertised in OSPF through	Wireless network management

Network	Address Assignment Method	Gateway	Routing Configuration	Network Description
			gateway devices	network on the third floor

1.4.1 Router Configuration

> Configures OSPF for dynamic routing across different network segments defined by their respective VLANs.

Markdown

```
[Router]ospf 1
[Router-ospf-1]area 0.0.0.0
[Router-ospf-1-area-0.0.0.0]network 192.168.204.0
0.0.0.3
```

Code Explanation

- **area 0.0.0.0**: Specifies the OSPF area as area 0, which is typically the backbone area in OSPF.
- **network 192.168.204.0 0.0.0.3**: Includes the interface with an IP address within the specified range (192.168.204.0-2) to OSPF area 0.

1.4.2 CORE1 Configuration

> Acts as a central point of connectivity between different VLANs and performs inter-VLAN routing using SVIs.

Markdown

```
[CORE]interface Vlanif1
```

```
[CORE1-Vlanif1]ip address 192.168.1.254 255.255.255.0
[CORE1-Vlanif1]interface Vlanif100
[CORE1-Vlanif100]ip address 192.168.100.254
255.255.255.0
[CORE1-Vlanif100]interface Vlanif201
[CORE1-Vlanif201]ip address 192.168.201.1
255.255.255.252
[CORE1-Vlanif201]interface Vlanif202
[CORE1-Vlanif202]ip address 192.168.202.1
255.255.255.252
[CORE1-Vlanif202]interface Vlanif204
[CORE1-Vlanif204]ip address 192.168.204.2
255.255.255.252
[CORE1-Vlanif204]ospf 1
[CORE1-ospf-1]area 0.0.0.0
[CORE1-ospf-1-area-0.0.0.0]network 192.168.1.0
0.0.0.255
[CORE1-ospf-1-area-0.0.0.0]network 192.168.100.0
0.0.0.255
[CORE1-ospf-1-area-0.0.0.0]network 192.168.105.0
0.0.0.255
[CORE1-ospf-1-area-0.0.0.0]network 192.168.205.0
0.0.0.255
[CORE1-ospf-1-area-0.0.0.0]network 192.168.201.0
0.0.0.3
[CORE1-ospf-1-area-0.0.0.0]network 192.168.202.0
0.0.0.3
[CORE1-ospf-1-area-0.0.0.0]network 192.168.204.0
0.0.0.3
```

Code Explanation

- **CORE1**: The core switch/router in the network, handling inter-VLAN routing and OSPF for Layer 3 communication.
- **interface VlanifX**: Each `Vlanif` command configures an SVI (Switched Virtual Interface) for a particular VLAN, assigning an IP address and subnet mask to that VLAN interface.

- **Example:**
- **Vlanif1**: This is the VLAN interface for VLAN ID 1, which is for Layer 2 de| IP Network	Address Assignment	Gateway	Routing Configuration	Network Description
  Enables OSPF routing protocol with process ID of `1`.
- Each **network** command adds respective networks to OSPF, allowing routers to share routes within these networks.

1.4.3 F2-AGG1 Configuration

> Aggregate connections from access switches on their respective floors and perform routing functions within their scope of responsibility.

Markdown

```
[FG2-AGG1]ip pool admin
[FG2-AGG1-ip-pool-admin]gateway-list 192.168.102.254
[FG2-AGG1-ip-pool-admin]network 192.168.102.0 mask
255.255.255.0
[FG2-AGG1-ip-pool-admin]ip pool manager
[FG2-AGG1-ip-pool-manager]gateway-list 192.168.101.254
[FG2-AGG1-ip-pool-manager]network 192.168.101.0 mask
255.255.255.0
[FG2-AGG1-ip-pool-manager]interface Vlanif2
[FG2-AGG1-Vlanif2]ip address 192.168.2.254
255.255.255.0
[FG2-AGG1-Vlanif2]interface Vlanif101
[FG2-AGG1-Vlanif101]ip address 192.168.101.254
255.255.255.0
[FG2-AGG1-Vlanif101]dhcp select global
[FG2-AGG1-Vlanif102]interface Vlanif102
[FG2-AGG1-Vlanif102]ip address 192.168.102.254
255.255.255.0
[FG2-AGG1-Vlanif102]dhcp select global
```

```
[FG2-AGG1-Vlanif102]interface Vlanif201
[FG2-AGG1-Vlanif201]ip address 192.168.201.2
255.255.255.252
[FG2-AGG1-Vlanif201]interface Vlanif203
[FG2-AGG1-Vlanif203]ip address 192.168.203.1
255.255.255.252
[FG2-AGG1-Vlanif203]ospf 1
[FG2-AGG1-ospf-1]area 0.0.0.0
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.2.0
0.0.0.255
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.101.0
0.0.0.255
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.102.0
0.0.0.255
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.106.0
0.0.0.255
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.201.0
0.0.0.3
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.203.0
0.0.0.3
[FG2-AGG1-ospf-1-area-0.0.0.0]network 192.168.206.0
0.0.0.255
```

Code Explanation

- Defines DHCP pools for different departments on the second floor with specific gateway-list and network ranges.
- Similar to CORE1, defines interfaces and assigns IP addresses with gateways for different VLANs on F2-AGG1.
- Enables OSPF within specified areas and includes necessary networks into OSPF similar to CORE1's configuration but specific to F2-AGG1's connected networks.

1.4.4 F3-AGG1 Configuration

> Aggregate connections from access switches on their respective floors and perform routing functions within their scope of responsibility.

Markdown

```
[FG3-AGG1]ip pool marketing
[FG3-AGG1-ip-pool-marketing]gateway-list 192.168.103.254
[FG3-AGG1-ip-pool-marketing]network 192.168.103.0 mask 255.255.255.0
[FG3-AGG1-ip-pool-marketing]ip pool rd
[FG3-AGG1-ip-pool-id]gateway-list 192.168.104.254
[FG3-AGG1-ip-pool-id]network 192.168.104.0 mask 255.255.255.0
[FG3-AGG1-ip-pool-id]interface Vlanif3
[FG3-AGG1-Vlanif3]ip address 192.168.3.254 255.255.255.0
[FG3-AGG1-Vlanif3]interface Vlanif103
[FG3-AGG1-Vlanif103]ip address 192.168.103.254 255.255.255.0
[FG3-AGG1-Vlanif103]dhcp select global
[FG3-AGG1-Vlanif103]interface Vlanif104
[FG3-AGG1-Vlanif104]ip address 192.168.104.254 255.255.255.0
[FG3-AGG1-Vlanif104]dhcp select global
[FG3-AGG1-Vlanif104]interface Vlanif202
[FG3-AGG1-Vlanif202]ip address 192.168.202.2 255.255.255.252
[FG3-AGG1-Vlanif202]interface Vlanif203
[FG3-AGG1-Vlanif203]ip address 192.168.203.2 255.255.255.252
[FG3-AGG1-Vlanif203]ospf 1
[FG3-AGG1-ospf-1]area 0.0.0.0
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.103.0 0.0.0.255
```

```
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.104.0 0.0.0.255
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.107.0 0.0.0.255
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.202.0 0.0.0.3
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.203.0 0.0.0.3
[FG3-AGG1-ospf-1-area-0.0.0.0]network 192.168.207.0 0.0.0.255
```

Code Explanation

- This section mirrors F2-AGG1's approach but applies it to third-floor configurations, establishing DHCP pools and defining interfaces with correct IP addressing and gateways aligned with third-floor requirements.
- Defines DHCP pools for different departments on the second floor with specific gateway-list and network ranges.
- Similar to CORE1, defines interfaces and assigns IP addresses with gateways for different VLANs on F3-AGG1.
- Enables OSPF within specified areas and includes necessary networks into OSPF similar to CORE1's configuration but specific to F3-AGG1's connected networks.

1.4.5 Access Switches (ACC) Configuration Example (F1-ACC1)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F1-ACC1]interface Vlanif1
[F1-ACC1-Vlanif1]ip address 192.168.1.1 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 1.

1.4.6 Access Switches (ACC) Configuration Example (F2-ACC1)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F2-ACC1]interface Vlanif2
[F2-ACC1-Vlanif2]ip address 192.168.2.1 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 2.

1.4.7 Access Switches (ACC) Configuration Example (F2-ACC2)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F2-ACC2]interface Vlanif1
```

```
[F2-ACC2-Vlanif1]interface Vlanif2
[F2-ACC2-Vlanif2]ip address 192.168.2.2 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 2.

1.4.8 Access Switches (ACC) Configuration Example (F2-ACC3)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F2-ACC3]interface Vlanif2
[F2-ACC3-Vlanif2]ip address 192.168.2.3 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 2.

1.4.9 Access Switches (ACC) Configuration Example (F3-ACC1)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F3-ACC1]interface Vlanif3
```

```
[F3-ACC1-Vlanif3]ip address 192.168.3.1 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 3.

1.4.10 Access Switches (ACC) Configuration Example (F3-ACC2)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F3-ACC2]interface Vlanif3
[F3-ACC2-Vlanif3]ip address 192.168.3.2 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 3.

1.4.11 Access Switches (ACC) Configuration Example (F3-ACC3)

> Provide direct connectivity to end devices like computers, printers, etc., within their assigned access layer VLANs.

Markdown

```
[F3-ACC3]interface Vlanif3
[F3-ACC3-Vlanif3]ip address 192.168.3.3 255.255.255.0
```

> These configurations are simpler; they define management interfaces for access switches including their static IP addresses which act as gateways for devices directly connected to them for floor 3.

1.5 WLAN Design

Design a WLAN with the following requirements:

- Centralized management of all APs by an Access Controller (AC) with limited forwarding capacity.
- APs on the first floor connect to the AC at Layer 2, while those on the second and third floors connect at Layer 3 via gateway CORE1.
- Implement unique SSIDs for each floor with WPA-WPA2+PSK+AES security, each having a distinct password.

Item	First Floor	Second Floor
WLAN		
AP Management VLAN	VLAN205	VLAN206
Service VLAN	VLAN105	VLAN106
DHCP Server	CORE1	F2-AGG1
AC's Source IP	**VLANIF205:**192.168.205.253/24	**VLANIF205:**192.168.205.253/
AP Group Name	WLAN-F1	WLAN-F2
Profiles		
VAP Profile	**Name:** WLAN-F1	**Name:** WLAN-F2
Regulatory Domain	- **Country code:** CN (default)	- **Country code**: CN (default)
SSID Profile	- **SSID name:** WLAN-F1	- **SSID name:** WLAN-F2

Item	First Floor	Second Floor
Security Profile	- WPA-WPA2+PSK+AES	- WPA-WPA2+PSK+AES
- Password:	--WLAN@Guest123	--WLAN@Employee2
- Forwarding Mode	--direct forwarding	--direct forwarding

1.5.1 CORE1 Configuration

Markdown

```
[CORE1]vlan batch 100 105 201 to 202 204 to 205
[CORE1]dhcp enable
[CORE1]ip pool ap-f1
[CORE1-ip-pool-ap-f1]gateway-list 192.168.205.254
[CORE1-ip-pool-ap-f1]network 192.168.205.0 mask
255.255.255.0
[CORE1-ip-pool-ap-f1]excluded-ip-address
192.168.205.253
[CORE1-ip-pool-sta-f1]ip pool sta-f1
[CORE1-ip-pool-sta-f1]gateway-list 192.168.105.254
[CORE1-ip-pool-sta-f1]network 192.168.105.0 mask
255.255.255.0
[CORE1-ip-pool-sta-f1]interface Vlanif105
[CORE1-Vlanif105]ip address 192.168.105.254
255.255.255.0
[CORE1-Vlanif105]dhcp select global

```

Code Explanation

- Creates a batch of VLANs that are to be used on this device. VLANs are virtual LANs used to segment network traffic.
- Enables DHCP server on CORE1.

- Defines an IP address pool named `ap-f1` for AP management on the first floor.
- Defines the IP address pools for Access Points (APs) and wireless stations (STAs) on the first floor, including gateways and network masks.
- Sets a default gateway for this pool.
- Specifies the network range and subnet mask for DHCP clients in this pool.
- Excludes a specific IP address from being assigned by DHCP.
- Assigns an IP address to the interface associated with VLAN105, which is designated for wireless terminals on the first floor, and configures it to use global DHCP settings.

1.5.2 F2-AGG1 Configuration

Markdown

```
[F2-AGG1]vlan batch 2 101 to 102 106 201 203 206
[F2-AGG1]dhcp enable
[F2-AGG1]ip pool ap-f2
[F2-AGG1-ip-pool-ap-f2]gateway-list 192.168.206.254
[F2-AGG1-ip-pool-ap-f2]network 192.168.206.0 mask
255.255.255.0
[F2-AGG1-ip-pool-ap-f2]option 43 sub-option 3 ascii
192.168.205.253
[F2-AGG1-ip-pool-ap-f2]ip pool sta-f2
[F2-AGG1-ip-pool-sta-f2]gateway-list 192.168.106.254
[F2-AGG1-ip-pool-sta-f2]network 192.168.106.0 mask
255.255.255.0
[F2-AGG1-ip-pool-sta-f2]interface Vlanif106
[F2-AGG1-Vlanif106]ip address 192.168.106.254
255.255.255.0
[F2-AGG1-Vlanif106]dhcp select global
[F2-AGG1-Vlanif206]interface Vlanif206
[F2-AGG1-Vlanif206]ip address 192.168.206.254
255.255.255.0
```

```
15 [F2-AGG1-Vlanif206]dhcp select global
```

Code Explanation

- Creates a batch of VLANs that are to be used on this device. VLANs are virtual LANs used to segment network traffic.
- Enables DHCP server on F2-AGG1.
- Defines an IP address pool named `ap-f2` for AP management on the second floor.AP management (`ap-f2`) and service network (`sta-f2`).
- Defines the IP address pools for Access Points (APs) and wireless stations (STAs) on the second floor, including gateways and network masks.
- Sets a default gateway for this pool.
- Specifies the network range and subnet mask for DHCP clients in this pool.
- Excludes a specific IP address from being assigned by DHCP.
- Assigns an IP address to the interface associated with VLAN106 and VLAN206, which is designated for wireless terminals and management on the second floor, and configures it to use global DHCP settings.

1.5.3 F3-AGG1 Configuration

Markdown

```
1 [F3-AGG1]vlan batch 3 103 to 104 107 202 to 203 207
2 [F3-AGG1]dhcp enable
3 [F3-AGG1]ip pool ap-f3
4 [F3-AGG1-ip-pool-ap-f3]gateway-list 192.168.207.254
5 [F3-AGG1-ip-pool-ap-f3]network 192.168.207.0 mask
  255.255.255.0
6 [F3-AGG1-ip-pool-ap-f3]option 43 sub-option 3 ascii
  192.168.205.253
7 [F3-AGG1-ip-pool-ap-f3]ip pool sta-f3
8 [F3-AGG1-ip-pool-sta-f3]gateway-list 192.168.107.254
```

```
[F3-AGG1-ip-pool-sta-f3]network 192.168.107.0 mask
255.255.255.0
[F3-AGG1-ip-pool-sta-f3]interface Vlanif107
[F3-AGG1-Vlanif107]ip address 192.168.107.254
255.255.255.0
[F3-AGG1-Vlanif107]dhcp select global
[F3-AGG1-Vlanif207]interface Vlanif207
[F3-AGG1-Vlanif207]ip address 192.168.207.254
255.255.255.0
dhcp select global
```

Code Explanation

- Creates a batch of VLANs that are to be used on this device. VLANs are virtual LANs used to segment network traffic.
- Enables DHCP server on F3-AGG1.
- Defines an IP address pool named `ap-f3` for AP management on the second floor.AP management (`ap-f3`) and service network (`sta-f3`).
- Defines the IP address pools for Access Points (APs) and wireless stations (STAs) on the thrid floor, including gateways and network masks.
- Sets a default gateway for this pool.
- Specifies the network range and subnet mask for DHCP clients in this pool.
- Excludes a specific IP address from being assigned by DHCP.
- Assigns an IP address to the interface associated with VLAN107 and VLAN207, which is designated for wireless terminals and management on the thrid floor, and configures it to use global DHCP settings.

1.5.4 Access Controller (AC) Configuration

Markdown

```
[AC]vlan batch 205
[AC]interface Vlanif205
```

```
[AC-Vlanif205]ip address 192.168.205.253 255.255.255.0
[AC]q
[AC]capwap source interface vlanif205
[AC]wlan
[AC-wlan-view]security-profile name WLAN-F1
[AC-wlan-sec-prof-WLAN-F1]security wpa-wpa2 psk pass-phrase WLAN@Guest123 aes
[AC-wlan-sec-prof-WLAN-F1]security-profile name WLAN-F2
[AC-wlan-sec-prof-WLAN-F2]security wpa-wpa2 psk pass-phrase WLAN@Employee2 aes
[AC-wlan-sec-prof-WLAN-F2]security-profile name WLAN-F3
[AC-wlan-sec-prof-WLAN-F3]security wpa-wpa2 psk pass-phrase WLAN@Employee3 aes
[AC-wlan-sec-prof-WLAN-F3]ssid-profile name WLAN-F1
[AC-wlan-ssid-prof-WLAN-F1]ssid WLAN-F1
[AC-wlan-ssid-prof-WLAN-F1]ssid-profile name WLAN-F2
[AC-wlan-ssid-prof-WLAN-F2]ssid WLAN-F2
[AC-wlan-ssid-prof-WLAN-F2]ssid-profile name WLAN-F3
[AC-wlan-ssid-prof-WLAN-F3]ssid WLAN-F3
[AC-wlan-ssid-prof-WLAN-F3]vap-profile name WLAN-F1
[AC-wlan-vap-prof-WLAN-F1]service-vlan vlan-id 105
[AC-wlan-vap-prof-WLAN-F1]ssid-profile WLAN-F1
[AC-wlan-vap-prof-WLAN-F1]security-profile WLAN-F1
[AC-wlan-vap-prof-WLAN-F1]vap-profile name WLAN-F2
[AC-wlan-vap-prof-WLAN-F2]service-vlan vlan-id 106
[AC-wlan-vap-prof-WLAN-F2]ssid-profile WLAN-F2
[AC-wlan-vap-prof-WLAN-F2]security-profile WLAN-F2
[AC-wlan-vap-prof-WLAN-F2]vap-profile name WLAN-F3
[AC-wlan-vap-prof-WLAN-F3]service-vlan vlan-id 107
[AC-wlan-vap-prof-WLAN-F3]ssid-profile WLAN-F3
[AC-wlan-vap-prof-WLAN-F3]security-profile WLAN-F3
[AC-wlan-vap-prof-WLAN-F3]ap-group name WLAN-F1
[AC-wlan-ap-group-WLAN-F1]radio 0
[AC-wlan-group-radio-WLAN-F1/0]vap-profile WLAN-F1 wlan 1
[AC-wlan-group-radio-WLAN-F1/0]radio 1
```

```
[AC-wlan-group-radio-WLAN-F1/1]vap-profile WLAN-F1 wlan 1
[AC-wlan-group-radio-WLAN-F1/1]radio 2
[AC-wlan-group-radio-WLAN-F1/2]vap-profile WLAN-F1 wlan 1
[AC-wlan-group-radio-WLAN-F1/2]ap-group name WLAN-F2
[AC-wlan-ap-group-WLAN-F2]radio 0
[AC-wlan-group-radio-WLAN-F2/0]vap-profile WLAN-F2 wlan 2
[AC-wlan-group-radio-WLAN-F2/0]radio 1
[AC-wlan-group-radio-WLAN-F2/1]vap-profile WLAN-F2 wlan 2
[AC-wlan-group-radio-WLAN-F2/1]radio 2
[AC-wlan-group-radio-WLAN-F2/2]vap-profile WLAN-F2 wlan 2
[AC-wlan-group-radio-WLAN-F2/2]ap-group name WLAN-F3
[AC-wlan-ap-group-WLAN-F3]radio 0
[AC-wlan-group-radio-WLAN-F3/0]vap-profile WLAN-F3 wlan 2
[AC-wlan-group-radio-WLAN-F3/0]radio 1
[AC-wlan-group-radio-WLAN-F3/1]vap-profile WLAN-F3 wlan 2
[AC-wlan-group-radio-WLAN-F3/1]radio 2
[AC-wlan-group-radio-WLAN-F3/2]vap-profile WLAN-F3 wlan 2
[AC-wlan-group-radio-WLAN-F3/2]ap-id 0 type-id 60 ap-mac xxx
[AC-wlan-ap-0]ap-name F1-AP1
[AC-wlan-ap-0]ap-group WLAN-F1
[AC-wlan-ap-0]ap-id 1 type-id 60 ap-mac xxx
[AC-wlan-ap-1]ap-name F2-AP1
[AC-wlan-ap-1]ap-group WLAN-F2
[AC-wlan-ap-1]ap-id 2 type-id 60 ap-mac xxx
[AC-wlan-ap-2]ap-name F3-AP1
[AC-wlan-ap-2]ap-group WLAN-F3
```

Code Explanation

- Sets up the management interface for wireless networks on the first floor with specific security profiles per SSID, including WPA2 Personal encryption and pre-shared keys.
- `capwap source interface vlanif205` : Sets the source interface of CAPWAP control messages sent by AC to APs.
- For each AP group corresponding to a different floor (`WLAN-F1` , `WLAN-F2` , `WLAN-F3`), Virtual AP profiles are assigned along with SSID profiles that define network names and security settings.
- `security-profile` : Defines security settings like WPA/WPA2 PSK and AES encryption keys per floor SSID.
- `ssid-profile` : Associates SSID names with profiles created earlier in the config.
- `vap-profile` : Configures virtual access points with forwarding modes along with their respective service VLAN IDs.
- `ap-id ... type-id ... ap-mac ...` : Registers each AP by specifying its ID, type, MAC address, and associates it with a predefined group according to its location.

1.5.5 F1-ACC1,F2-ACCx,F3-ACCx

> For each ACC device (`F1-ACC1` , `F2-ACCx` , `F3-ACCx`), create relevant VLAN batches that match their respective locations within the building structure:

Example: `F2-ACC1`

Markdown

```
[F2-ACC1]vlan batch 2 102
```

> This assigns specific VLAN IDs required by that access point's location within the building structure.

1.6 Security and Egress Design

Requirements :

1. Guest WiFi access is restricted to the Internet only, no intranet access.
2. Only wireless devices can connect to the Internet.
3. Router has a static IP range of 1.1.1.1 to 1.1.1.10/24 with a gateway of 1.1.1.254.
4. External users must access an internal web server at 192.168.100.1 on port 80, using NAT for security and restricted to web services only.

Requirement Title	Implementation Detail	Applicable Device
Intranet Access Control	Configure a traffic filter or policy on CORE1 for guest access control.	CORE1
Internet Access Control	Enable NAT on the router but disable address translation for specific networks.	Router
Web Server Mapping	Configure NAT server on the router interface to manage web server accessibility.	Router

1.6.1 Router Configuration

Markdown

```
[Router]acl number 2000
[Router-acl-basic-2000]rule 5 permit source 192.168.105.0 0.0.0.255
[Router-acl-basic-2000]rule 10 permit source 192.168.106.0 0.0.0.255
[Router-acl-basic-2000]rule 15 permit source 192.168.107.0 0.0.0.255
[Router-acl-basic-2000]q
[Router]nat address-group 1 1.1.1.2 1.1.1.10
```

```
[Router]interface GigabitEthernet0/0/0
[Router-GigabitEthernet0/0/0]ip address 1.1.1.1 255.255.255.0
[Router-GigabitEthernet0/0/0]nat server protocol tcp global current-interface 8080 inside 192.168.100.1 www
[Router-GigabitEthernet0/0/0]nat outbound 2000 address-group 1
[Router-GigabitEthernet0/0/0]q
[Router]ip route-static 0.0.0.0 0.0.0.0 1.1.1.254
```

IP	Description
192.168.105.0/24	Network of the wireless terminals on the first floor
192.168.106.0/24	Network of the wireless terminals on the second floor
192.168.107.0/24	Network of the wireless terminals on the third floor

Code Explanation

- **ACL (Access Control List)**: Defines a set of rules that filter traffic based on IP addresses.
- `rule` **lines:** Permit traffic from the specified wireless VLANs (for guests).
- **NAT Address Group**: Defines a range of public IP addresses `(1.1.1.2 to 1.1.1.10)` for NAT (Network Address Translation) to use when translating private IP addresses to public ones.
- Configures the IP address for `GigabitEthernet interface 0/0/0` on the router for network subnet for public network.
- Configures static NAT to map the internal web server's private IP (`192.168.100.1`) and port (`80`) to an external IP on port `8080` .
- `nat outbound` : Applies NAT to traffic matched by ACL `2000` , using the defined address group.
- Enables dynamic NAT for outbound traffic, using the defined address group for translation `(1.1.1.2 to 1.1.1.10)` .
- Configures a default static route with next-hop IP address as `1.1.1.254` (ISP Gateway).

1.6.2 CORE Switch Configuration

```Markdown
[CORE]acl number 3000
[CORE-acl-basic-2000]rule 5 deny ip source 192.168.105.0 0.0.0.255 destination 192.168.0.0 0.0.255.255
[CORE-acl-basic-2000]rule 10 permit ip
```

Code Explanation

- Defines an ACL with ID `30000` that denies guest VLAN traffic (`192.168.105.0`).
- Allows all other IP traffic by default, ensuring guests cannot access internal networks but can reach other destinations (typically, this means internet access only).

1.6.3 Aggregation and Access Layer Switches

> For switches `F2-AGG` , `F3-AGG` , and access layer switches (`F-ACC`), static routes are configured:

1.6.4 F1-ACC1 Switch Example

```Markdown
[F1-ACC1]ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
```

> - Sets a default static route pointing to its uplink gateway at `192.168.1.254` . Replace `1` with appropriate floor number and device number based on your topology like `F2` number is `2` .

1.6.5 AC Configuration (Wireless Access Controller)

```Markdown
[AC]ip route-static 0.0.0.0 0.0.0.0 192.168.205.25
```

- Sets a default static route pointing to its uplink gateway at `192.168.205.25` .

1.7 Network Management Design

Requirement:

- Utilize SNMPv3 with authentication and encryption for NMS communication.
- Devices use management VLAN to reach NMS at 192.168.100.2/24, except routers and AC.
- Routers interface with NMS via GE0/0/1.
- AC connects to NMS using VLANIF 205.
- All devices should send SNMP alarms to the NMS.

1.7.1 Router Configuration

```Markdown
[Router]snmp-agent sys-info version v3
[Router]snmp-agent group v3 datacom privacy
[Router]snmp target-host trap-hostname nms address 192.168.100.2 udp-port 162 trap-paramsname datacom
[Router]snmp target-host trap-paramsname datacom v3 securityname test privacy
[Router]snmp usm-user v3 test datacom authentication-mode md5 huaweilab privacy-mode aes128 huaweilab
[Router]snmp-agent trap source GigabitEthernet0/0/1
```

```
[Router]snmp-agent trap enable
[Router]snmp-agent
```

Command explanation

- Initializes the SNMP agent and sets it to use version 3, which is more secure than previous versions.
- Creates a group named `datacom` with privacy enabled, meaning that encryption is used.
- Specifies the NMS host where traps should be sent. `192.168.100.2` is the NMS IP address, and traps are sent using UDP port 162.
- Configures trap parameters with a security name of `test` and privacy (encryption) enabled.
- Sets up a user-based security model (USM) user named `test` in group `datacom`. Authentication uses MD5 with the password `huaweilab`, and encryption uses AES128 with the same password.
- Sets the source interface for sending traps to NMS as GigabitEthernet0/0/1.
- Enables the device to send traps to the NMS server.

1.7.2 CORE1 and Other Switches Configuration (Similar for F2/F3-AGG1, F1/F2/F3-ACC1/ACC2/ACC3)

Markdown

```
[CORE1]snmp-agent sys-info version v3
[CORE1]snmp-agent group v3 datacom privacy
[CORE1]snmp-agent target-host trap address udp-domain
192.168.100.2 params securityname datacom v3
[CORE1]snmp usm-user v3 test datacom authentication-
mode md5 huaweilab privacy-mode aes128 huaweilab
[CORE1]snmp-agent trap source vlanif1
[CORE1]snmp-agent trap enable
[CORE1]snmp-agent
```

Command explanation

- Initializes the SNMP agent and sets it to use version 3, which is more secure than previous versions.
- Creates a group named `datacom` with privacy enabled, meaning that encryption is used.
- Specifies the NMS host where traps should be sent. `192.168.100.2` is the NMS IP address, and traps are sent using UDP port 162. under security under datacom name
- Sets up a user-based security model (USM) user named `test` in group `datacom`. Authentication uses MD5 with the password `huaweilab`, and encryption uses AES128 with the same password.
- Enables the device to send traps to the NMS server.
- Replace `vlanif1` 1 with VLAN interface number specific to each device; sets this as the source for SNMP traps.

1.7.2.1 Device-Specific Configurations

Device	Trap Source Interface	NMS Communication Path
Router	GE0/0/1	Directly through GE0/0/1
CORE1	VLANIF1	Via management VLAN1
F2-AGG1	VLANIF2	Via management VLAN2
F3-AGG1	VLANIF3	Via management VLAN3
AC	VLANIF205	Via specific VLANIF205
F1-ACC1	VLANIF1	Via management VLANIF1
F2-ACC2	VLANIF2	Via management VLANIF2
F2-ACC3	VLANIF2	Via management VLANIF2
F3-ACC1	VLANIF3	Via management VLANIF3
F3-ACC2	VLANIF3	Via management VLANIF3
F3-ACC3	VLANIF3	Via management VLANIF3

1.7.3 AC (Access Controller) Configuration

```
[AC]snmp-agent sys-info version v3
[AC]snmp-agent group v3 datacom privacy
[AC]snmp-agent target-host trap address udp-domain 192.168.100.2 params securityname datacom v3
[AC]snmp usm-user v3 test datacom authentication-mode md5 huaweilab privacy-mode aes128 huaweilab
[AC]snmp-agent trap source vlanif205
[AC]snmp-agent trap enable
[AC]snmp-agent
```

Command explanation

- Initializes the SNMP agent and sets it to use version 3, which is more secure than previous versions.
- Creates a group named `datacom` with privacy enabled, meaning that encryption is used.
- Specifies the NMS host where traps should be sent. `192.168.100.2` is the NMS IP address, and traps are sent using UDP port 162. under security under datacom name
- Sets up a user-based security model (USM) user named `test` in group `datacom` . Authentication uses MD5 with the password `huaweilab` , and encryption uses AES128 with the same password.
- Enables the device to send traps to the NMS server.
- Sets VLAN interface 205 as the source of SNMP traps for communication with NMS.

1.8 Quiz

Question1

In your project, you have three devices (CORE1, F2-AGG1, and F3-AGG1) that are connected in a circle, which is called a physical ring. To avoid any

issues with data loops (where data could go around in circles forever), you've put each connecting link into its own separate VLAN (a virtual network within your physical network).

✓ **Answer1**

- You thought that by doing this, you wouldn't have any loops because each VLAN is like a separate path. However, during testing, you found that two of the devices are not talking to each other properly - they're not becoming neighbors as they should.
- The problem is that even though you've separated the links into different VLANs to stop loops at the network layer, there's still a loop at the physical layer - the actual cables and devices are still forming a ring. Normally, Spanning Tree Protocol (STP) helps prevent these kinds of loops by blocking some paths. But STP doesn't understand VLAN tags - it just sees one big network.
- So what's likely happening here is that STP has blocked one of your links to prevent a loop. But since you've already separated the paths with VLANs (which STP isn't aware of), this block is unnecessary and it's stopping your devices from communicating.
- The solution? Since you've already organized loop prevention with VLANs, you can safely turn off STP on the links between these three devices. This will allow them to talk to each other without STP blocking any of them. Just make sure that your VLAN-based separation really prevents all possible loops before disabling STP to avoid any potential issues.