

# CS 305 Lab Tutorial

## Lecture 12 NAT, RIP, OSPF

Dept. Computer Science and Engineering  
Southern University of Science and Technology

# Topic

- IPv4 Addressing
- NAT
  - Static conversion
  - Dynamic conversion
  - NAPT
- Routing Protocol
  - RIP
  - OSPF
- Practice
  - Build network on simulator
  - Configure
  - Test

# Part A. IPv4 Addressing (1)

- Class A/B/C network address assignment
  - class A, class B, class C
  - parts of this were eventually defined (MSB '1110') for use with IPv4 multicast and parts are still reserved

<div>class A</div> <div>0.0.0.0 - 127.0.0.0</div>	0	NetworkID (7bits)		HostID(24bits)		
<div>class B</div> <div>128.0.0.0 - 191.255.255.255</div>	1	0	NetworkID (14bits)		HostID(16 bits)	
<div>class C</div> <div>192.0.0.0 - 223.255.255.255</div>	1	1	0	NetworkID (21bits)		HostID(8 bits)
<div>class D</div> <div>224.0.0.0 - 239.255.255.255</div>	1	1	1	0	MulticastGroupID(28bits)	
<div>class E</div> <div>240.0.0.0 - 247.255.255.255</div>	1	1	1	1	0	Reserved(27bits)

# IPv4 Addressing (2)

- Major problems of class A/B/C network numbers:
  - Exhaustion of the Class B network address space.
  - Growth of routing tables in Internet routers beyond the ability of current software, hardware, and people to effectively manage.
  - Eventual exhaustion of the 32-bit IPv4 address space.
- CDIR: Classless Inter-domain Routing
  - "classless"
  - hierarchical blocks of IP addresses (referred to as prefixes)
  - /16, /24, .....

# IPv4 Addressing(3)

- Public: require IP addresses that are globally unambiguous
  - hosts that need network layer access outside the enterprise
- Private: may be ambiguous between enterprises
  - hosts that do not require access to hosts in other enterprises or the Internet at large
  - hosts that need access to a limited set of outside services which can be handled by mediating gateways
  - Private address space
    - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
    - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
    - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

# Part B.

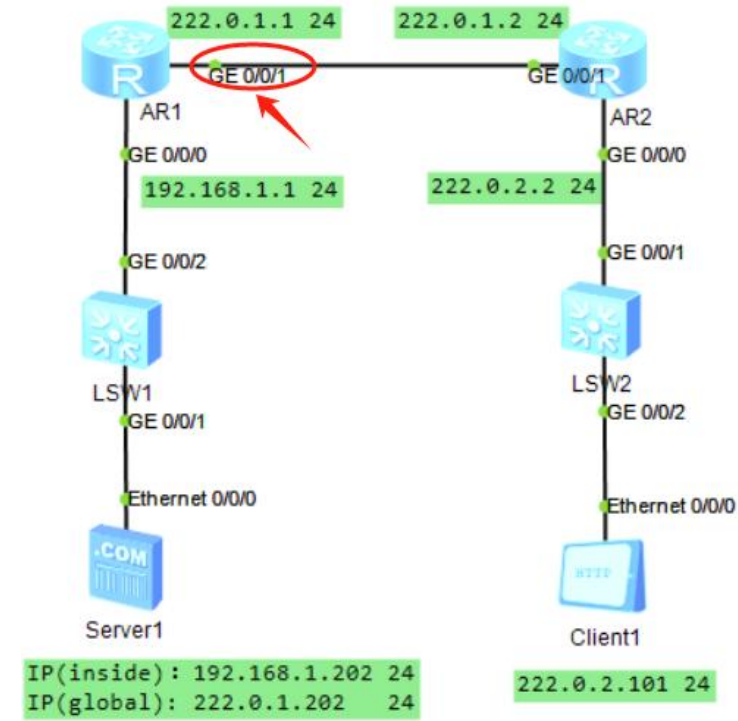
## NAT - Network Address Translator

- The need for IP Address translation arises when a network's internal IP addresses cannot be used outside the network either for privacy reasons or because they are invalid for use outside the network.
- Traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.
  - Basic **Network Address Translation** or Basic **NAT**: IP addresses are mapped from one group to another.
  - **Network Address Port Translation**, or **NAPT**: many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports.

# NAT(Static conversion)

The mapping relationship of IP addresses is one-to-one and remains unchanged.

- With the help of static conversion, the access of external network to some special servers in internal network can be realized.
- **Demo1 : NAT(Static conversion) -1**
  - The current server has a private address (192.168.1.202/24) and a global address (222.0.1.202/24). In order to hide the private address of the server, it is necessary to perform static address mapping on the router of the network where the server is located.
  - Configuration steps on eNSP:
    - step0. Complete the basic configuration of the network, including the basic configuration of Client1 and Server1, interface configuration on AR1 and AR2, and static routing configuration(route information about how to network 222.0.2.0/24) on AR1.
    - step1. **Determine the interface to be used for NAT:** GE 0/0/1 of AR1(The address of this interface is in the same network as the global address converted by NAT)
    - step2. **Apply the NAT static conversion configuration on the interface :**
      - **nat static global <global address> inside <private address> [netmask <netmask of private address 255.255.255.255>]**



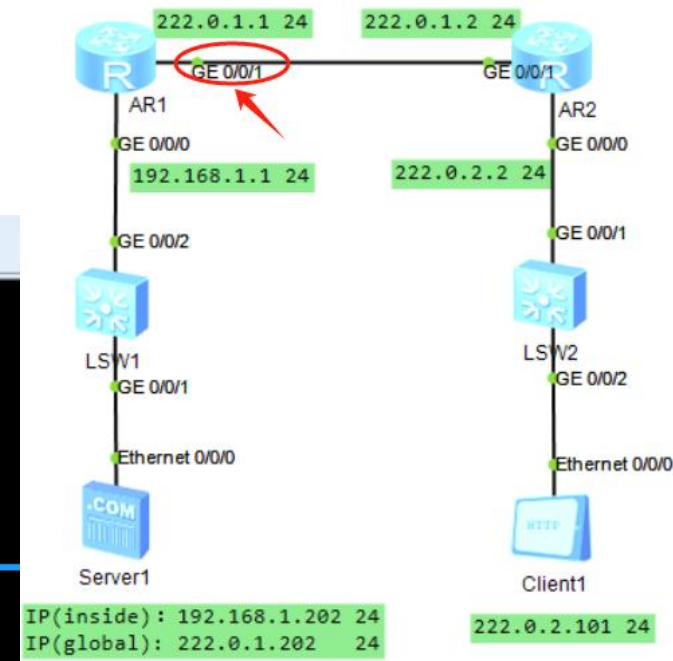
e.g.  
nat static global 222.0.1.202 inside  
192.168.1.202 netmask 255.255.255.255

# Demo1-NAT(Static conversion)-2

The following figure shows the configuration on the two interfaces of AR1 on the network where the server is located.

Note that for the convenience of testing NAT, the routing to the network(192.168.1.0 / 24) is not configured on AR2, and only direct routing items are available on AR2.

```
AR1
[Huawei]int gi0/0/0
[Huawei-GigabitEthernet0/0/0]dis this
[V200R003C00]
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
return
[Huawei-GigabitEthernet0/0/0]int gi0/0/1
[Huawei-GigabitEthernet0/0/1]dis this
[V200R003C00]
#
interface GigabitEthernet0/0/1
 ip address 222.0.1.1 255.255.255.0
 nat static global 222.0.1.202 inside 192.168.1.202 netmask 255.255.255.255
#
return
```



Server1 is configured with private address: 192.168.1.202 24

Server1 Configuration Window:

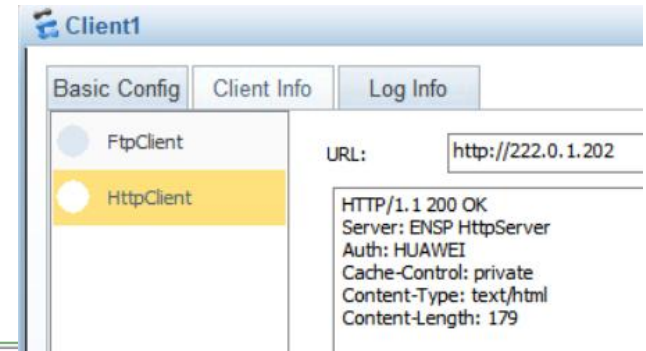
- Basic Config | Server Info | Log Info
- MAC Address: 54-89-98-AC-08-8D (Format: 00-01-02-03-04-05)
- IPv4 Config:
  - Local Address: 192 . 168 . 1 . 202
  - Subnet Mask: 255 . 255 . 255 . 0
  - Gateway: 192 . 168 . 1 . 1
  - DNS: 0 . 0 . 0 . 0



# Demo1-NAT(Static conversion)-3

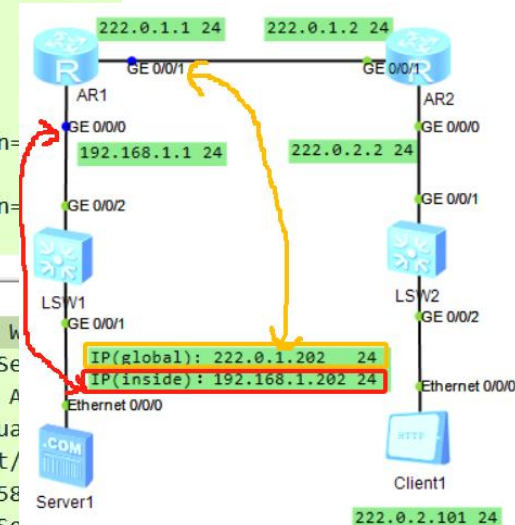
Capture packets on the GE0/0/0 and GE0/0/1 of AR1:

- Initiate HTTP access to Server1 on Client1
- The packets sent and received on the **GE0/0/1** are the packets exchanged between the global addresses of Server1 (222.0.1.202) and Client1.
- The packets sent and received on the **GE0/0/0** are the packets exchanged between the private addresses of Server1 (192.168.1.202) and Client1.



Source	Protocol	Destination	Length	Info
222.0.2.101	TCP	222.0.1.202	58	2050 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
222.0.1.202	TCP	222.0.2.101	58	80 → 2050 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
222.0.2.101	TCP	222.0.1.202	54	2050 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
222.0.2.101	HTTP	222.0.1.202	211	GET / HTTP/1.1 Continuation
222.0.1.202	HTTP	222.0.2.101	361	HTTP/1.1 200 OK (text/html)
222.0.2.101	TCP	222.0.1.202	54	2050 → 80 [ACK] Seq=158 Ack=308 Win=7885 Len=0
222.0.2.101	TCP	222.0.1.202	54	2050 → 80 [FIN, ACK] Seq=158 Ack=308 Win=7885 Len=0
222.0.1.202	TCP	222.0.2.101	54	80 → 2050 [ACK] Seq=308 Ack=159 Win=8034 Len=0
222.0.1.202	TCP	222.0.2.101	54	80 → 2050 [FIN, ACK] Seq=308 Ack=159 Win=8034 Len=0
222.0.2.101	TCP	222.0.1.202	54	2050 → 80 [ACK] Seq=159 Ack=309 Win=7884 Len=0

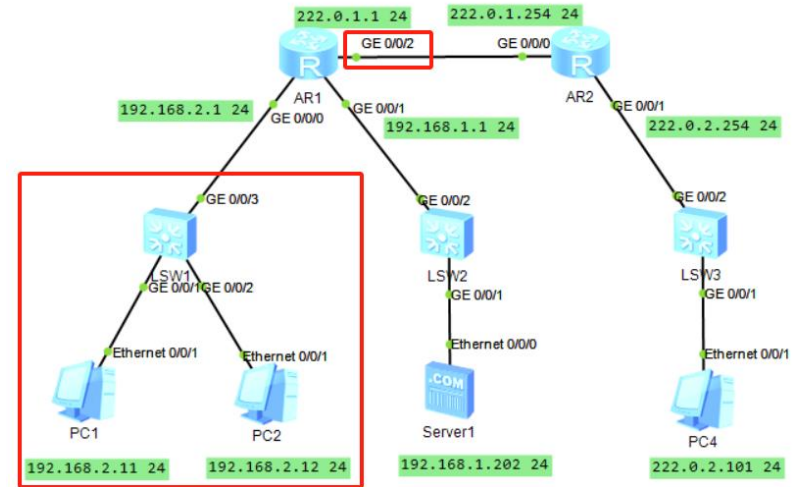
Source	Protocol	Destination	Length	Info
222.0.2.101	TCP	192.168.1.202	58	2050 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
192.168.1.202	TCP	222.0.2.101	58	80 → 2050 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
222.0.2.101	TCP	192.168.1.202	54	2050 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=0
222.0.2.101	HTTP	192.168.1.202	211	GET / HTTP/1.1 Continuation
192.168.1.202	HTTP	222.0.2.101	361	HTTP/1.1 200 OK (text/html)
222.0.2.101	TCP	192.168.1.202	54	2050 → 80 [ACK] Seq=158 Ack=308 Win=7885 Len=0
222.0.2.101	TCP	192.168.1.202	54	2050 → 80 [FIN, ACK] Seq=158 Ack=308 Win=7885 Len=0
192.168.1.202	TCP	222.0.2.101	54	80 → 2050 [ACK] Seq=308 Ack=159 Win=8034 Len=0
192.168.1.202	TCP	222.0.2.101	54	80 → 2050 [FIN, ACK] Seq=308 Ack=159 Win=8034 Len=0
222.0.2.101	TCP	192.168.1.202	54	2050 → 80 [ACK] Seq=159 Ack=309 Win=7884 Len=0



# NAT(Dynamic conversion)

**NAT(Dynamic conversion): The mapping relationship of IP addresses is uncertain and random.**

- It is suitable for scenarios where the number of hosts accessing the Internet at the same time in an internal network is less than the number of IP addresses in the configured legitimate address.
- **Demo2. NAT(Dynamic conversion) -1**
  - Requirement:  
a group of private address(192.168.2.1 - 192.168.2.254)  
share a group of global address(222.0.1.110-222.0.1.120)
  - Configuration steps about NAT(Dynamic conversion) on eNSP:
    - step0. **Determin the router and the interface which applies the NAT(dynamic conversion)**
    - step1. **Create a “nat address-group” to specify the range of the global address group**
      - command: **nat address-group** <group-number> <x.x.x.x start-address> <x.x.x.x end-address>
    - step2. **Create an “acl” and specify the range of the private address group**
      - command: **acl** <acl-number>
      - command: **rule** <rule-number> **permit source**<private address-start address> <wildcast mask>
    - step3. **Switch to Interface(which NAT dynamic conversion would be applied) Configuration View , applies the NAT configuration**
      - command: **interface** <interface type and number>
      - command: **nat outbound** <acl -number> **address-group** <group-number> **no-pat**



# Demo2-NAT(Dynamic conversion)-2

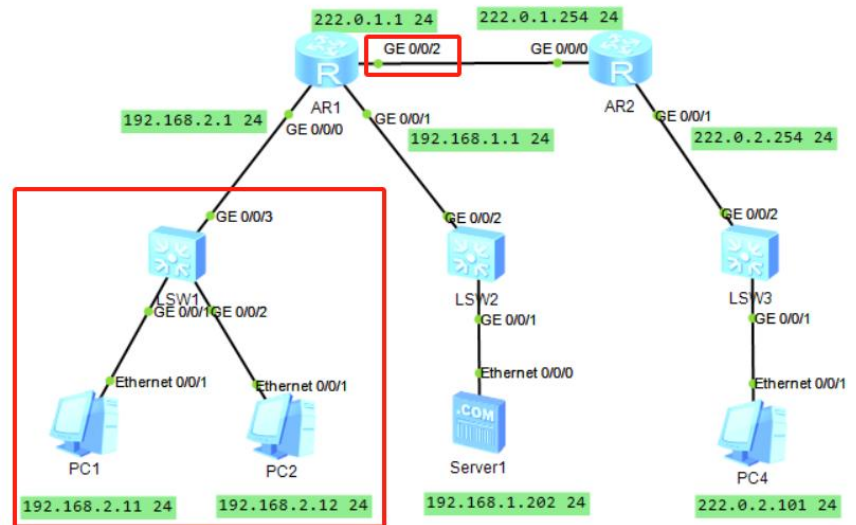
The details about the configurations related to NAT(Dynamic conversion) are as follows:

```
[AR1]dis nat address-group
```

NAT Address-Group Information:

Index	Start-address	End-address
2	222.0.1.110	222.0.1.120

Total : 1

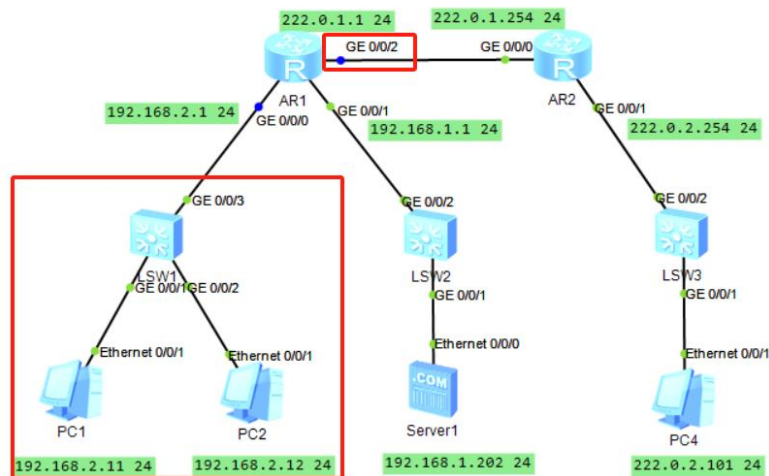


```
[AR1]acl 2000
[AR1-acl-basic-2000]dis this
[V200R003C00]
#
acl number 2000
rule 5 permit source 192.168.2.0 0.0.0.255
#
return
[AR1-acl-basic-2000]
```

```
AR1-GigabitEthernet0/0/2 dis this
[V200R003C00]
#
interface GigabitEthernet0/0/2
ip address 222.0.1.1 255.255.255.0
nat outbound 2000 address-group 2 no-pat
#
return
```



# Demo2-NAT(Dynamic conversion)-3



After the configuration is done, initiate a “ping” test from PC1 to PC4, capturing packets at GE0/0/0 and GE0/0/2 on AR1 respectively

Packets captured on **GE0/0/0** are as follows: **PC1** communicates with PC4 by using the same private address(**192.168.2.11**)

Source	Protocol	Destination	Len	Info
192.168.2.11	ICMP	222.0.2.101	74	Echo (ping) request id=0x988a,
222.0.2.101	ICMP	192.168.2.11	74	Echo (ping) reply id=0x988a,
192.168.2.11	ICMP	222.0.2.101	74	Echo (ping) request id=0x998a,
222.0.2.101	ICMP	192.168.2.11	74	Echo (ping) reply id=0x998a,
192.168.2.11	ICMP	222.0.2.101	74	Echo (ping) request id=0x9a8a,
222.0.2.101	ICMP	192.168.2.11	74	Echo (ping) reply id=0x9a8a,
192.168.2.11	ICMP	222.0.2.101	74	Echo (ping) request id=0x9b8a,
222.0.2.101	ICMP	192.168.2.11	74	Echo (ping) reply id=0x9b8a,
192.168.2.11	ICMP	222.0.2.101	74	Echo (ping) request id=0x9c8a,
222.0.2.101	ICMP	192.168.2.11	74	Echo (ping) reply id=0x9c8a,

Packets captured on **GE0/0/2** are as follows: **PC1** communicates with PC4 by using the different global addressess (**222.0.1.110 - 222.0.1.114**)

Source	Protocol	Destination	Len	Info
222.0.1.110	ICMP	222.0.2.101	74	Echo (ping) request id=0x988a,
222.0.2.101	ICMP	222.0.1.110	74	Echo (ping) reply id=0x988a,
222.0.1.111	ICMP	222.0.2.101	74	Echo (ping) request id=0x998a,
222.0.2.101	ICMP	222.0.1.111	74	Echo (ping) reply id=0x998a,
222.0.1.112	ICMP	222.0.2.101	74	Echo (ping) request id=0x9a8a,
222.0.2.101	ICMP	222.0.1.112	74	Echo (ping) reply id=0x9a8a,
222.0.1.113	ICMP	222.0.2.101	74	Echo (ping) request id=0x9b8a,
222.0.2.101	ICMP	222.0.1.113	74	Echo (ping) reply id=0x9b8a,
222.0.1.114	ICMP	222.0.2.101	74	Echo (ping) request id=0x9c8a,
222.0.2.101	ICMP	222.0.1.114	74	Echo (ping) reply id=0x9c8a,

```

PC1
Basic Config Command MCPacket UDPacket Console
PC>ping 222.0.2.101

Ping 222.0.2.101: 32 data bytes, Press Ctrl_C to break
From 222.0.2.101: bytes=32 seq=1 ttl=126 time=63 ms
From 222.0.2.101: bytes=32 seq=2 ttl=126 time=78 ms
From 222.0.2.101: bytes=32 seq=3 ttl=126 time=94 ms
From 222.0.2.101: bytes=32 seq=4 ttl=126 time=78 ms
From 222.0.2.101: bytes=32 seq=5 ttl=126 time=62 ms
    
```

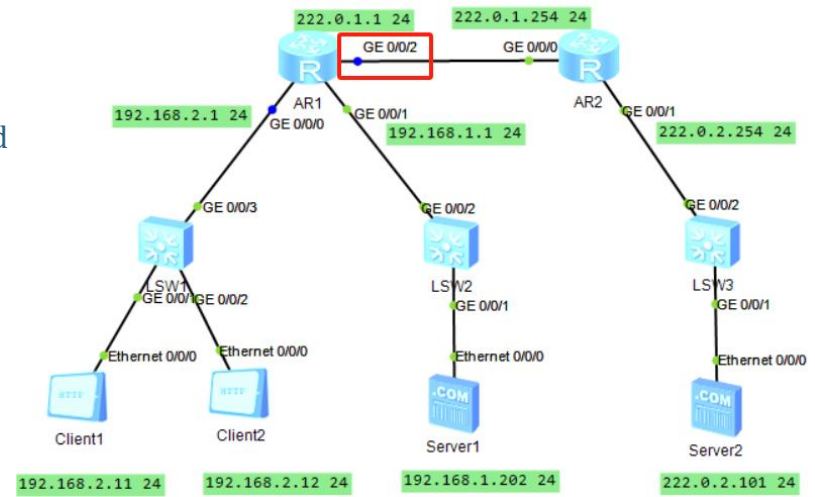
# NAPT(Network Address Port Translation)

NAPT: many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports.

- NAPT allow multiple hosts to share a single public IP address, distinguished by port numbers at the transport layer, commonly used in home or small business networks.

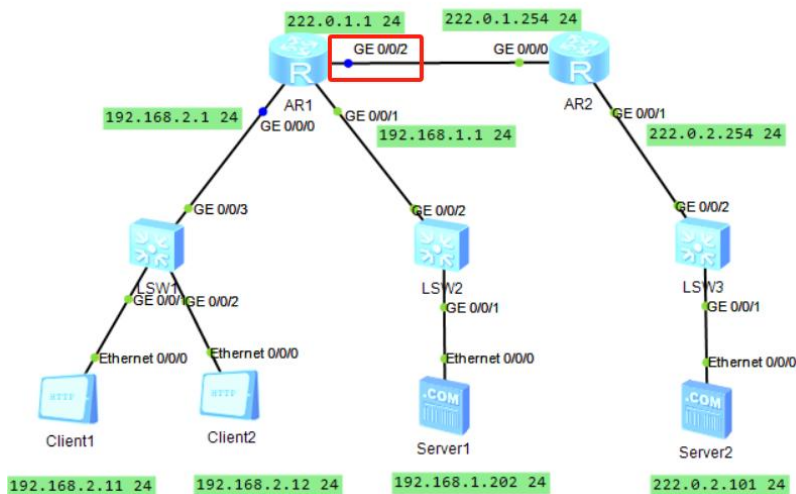
- **Demo3. NAT(Dynamic conversion) -1**

- Requirement:  
a group of private address(192.168.2.11, 192.168.2.12, ...) share a global address(222.0.1. 101)
- Configuration steps about NAPT on eNSP:
  - step0. **Determin the router and the interface which applies the NAPT**
  - step1. **Create a “nat address-group” to specify the global address**
    - command: **nat address-group** <group-number> <x.x.x.x the global address> <x.x.x.x the global address>
  - step2. **Create an “acl” and specify the range of the private address group**
    - command: **acl** <acl-number>
    - command: **rule** <rule-number> **permit source** <private address-start address> <wildcast mask>
  - step3. **Switch to Interface(which NAPT would be applied) Configuration View , applies the NAPT configuration**
    - command: **interface** <interface type and number>
    - command: **nat outbound** <acl -number> **address-group** <group-number>



# Demo3-NAPT(2)

NAPT: In demo3 here, map 192.168.1.11, 192.168.1.12, and other PCs with the same high 28 bits of the IP address as 192.168.1.11 to the same global address 222.0.1.101 (distinguished by different ports)



Q: If add new Clients to the subnet(192.168.1.0/24), which private IP addresses could be assigned to these Clients to share the global address(222.0.1.101) by using the existing NAPT mapping?

```
[AR1]nat address-group 2 ?
  IP_ADDR<X.X.X.X> Start address
[AR1]nat address-group 2 222.0.1.101 ?
  IP_ADDR<X.X.X.X> End address
[AR1]nat address-group 2 222.0.1.101 222.0.1.101
[AR1]
```

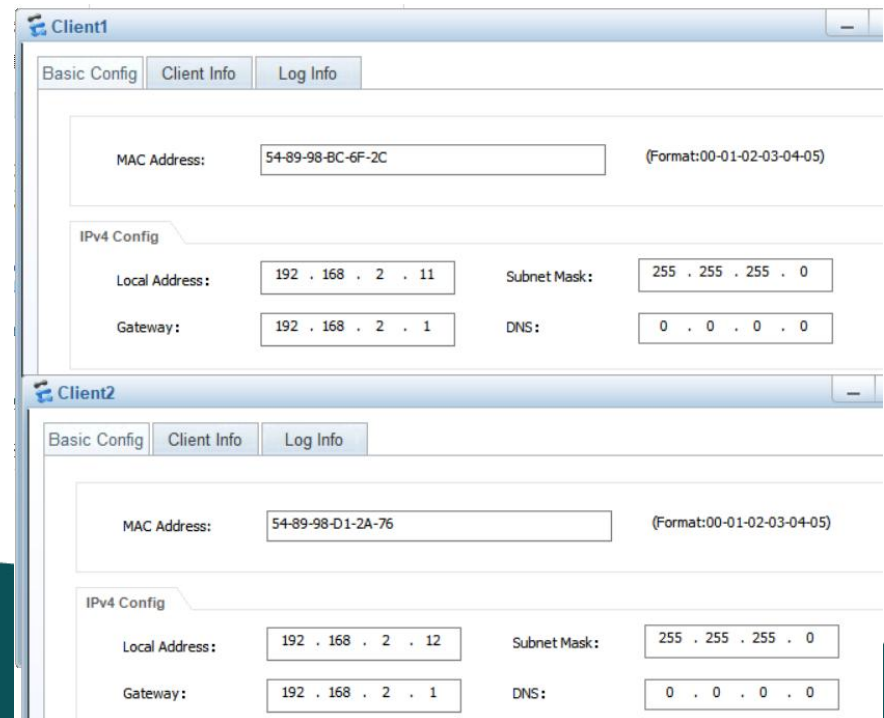
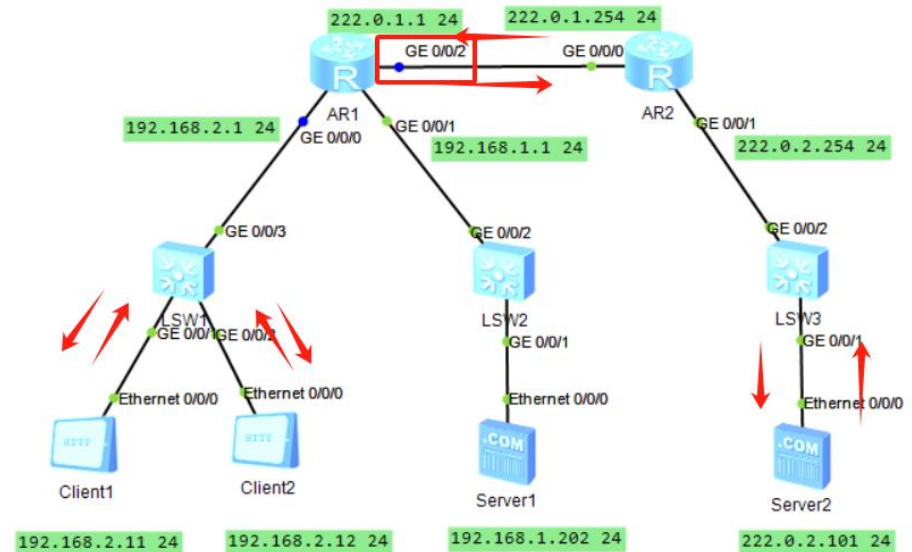
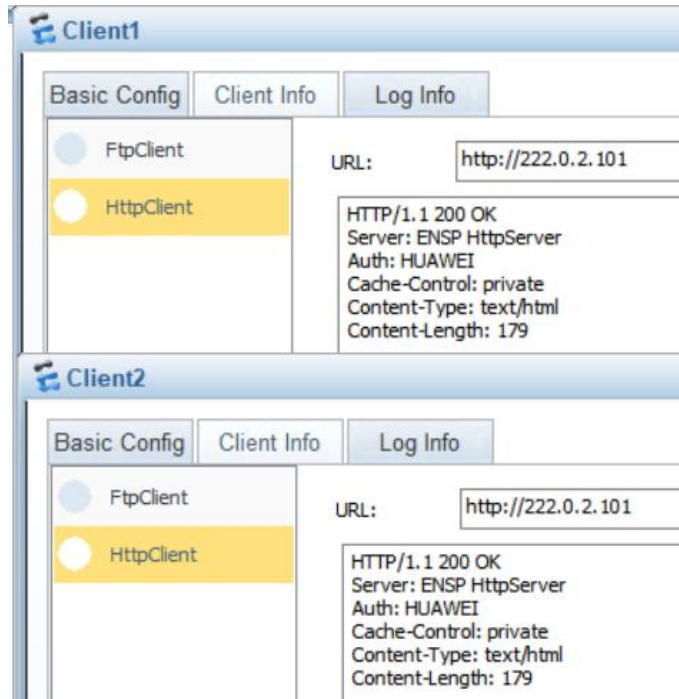
```
[AR1]acl 2000
[AR1-acl-basic-2000]rule 5 permit source 192.168.2.11 ?
  IP_ADDR<X.X.X.X> Wildcard of source
  0 Wildcard bits : 0.0.0.0 ( a host )
[AR1-acl-basic-2000]rule 5 permit source 192.168.2.11 0.0.0.15
```

```
[AR1-GigabitEthernet0/0/2]nat outbound ?
  INTEGER<2000-3999> Apply basic or advanced ACL
[AR1-GigabitEthernet0/0/2]nat outbound 2000 ?
  address-group IP address-group of NAT
  interface Specify the interface
  <cr> Please press ENTER to execute command
[AR1-GigabitEthernet0/0/2]nat outbound 2000 address-group ?
  INTEGER<0-7> Index of address-group
[AR1-GigabitEthernet0/0/2]nat outbound 2000 address-group 2 ?
  no-pat Not use PAT
  <cr> Please press ENTER to execute command
[AR1-GigabitEthernet0/0/2]nat outbound 2000 address-group 2
[AR1-GigabitEthernet0/0/2]
```



# Demo3-NAPT(3)

After the NAPT configuration is done, Client1 and Client2(both Client1 and Client2 are configured with private addresses) initiate HTTP access to Server2.



# Demo3-NAPT(4)

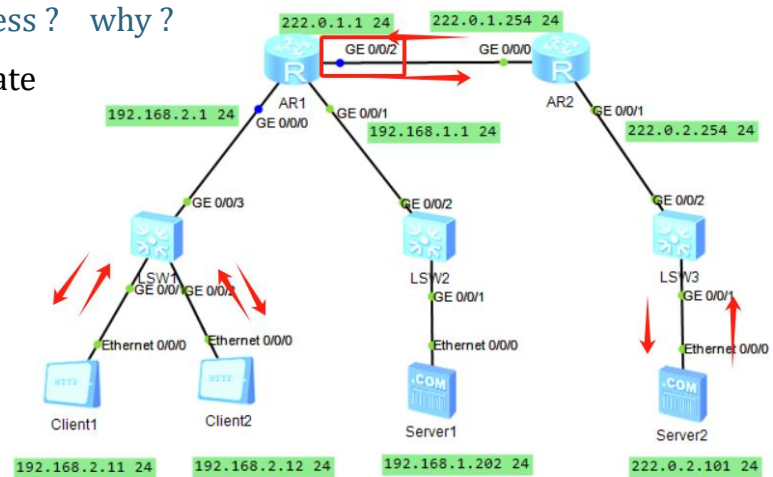
Q: Is NAPT suitable for multiple servers sharing the same global address ? why ?

Client1 and Client2(both Client1 and Client2 are configured with private addresses) initiate HTTP access to Server2.

Source	Protocol	Destination	Length	Info
192.168.2.11	TCP	222.0.2.101	54	2050 → 80 [SYN] Seq=0 Win=8
222.0.2.101	TCP	192.168.2.11	58	80 → 2050 [SYN, ACK] Seq=0
192.168.2.11	TCP	222.0.2.101	54	2050 → 80 [ACK] Seq=1 Ack=1
192.168.2.11	HTTP	222.0.2.101	211	GET / HTTP/1.1 Continuation
222.0.2.101	TCP	192.168.2.11	54	80 → 2050 [ACK] Seq=1 Ack=1
222.0.2.101	HTTP	192.168.2.11	361	HTTP/1.1 200 OK (text/html)
192.168.2.11	TCP	222.0.2.101	54	2050 → 80 [ACK] Seq=158 Ack=1
192.168.2.11	TCP	222.0.2.101	54	2050 → 80 [FIN, ACK] Seq=15
222.0.2.101	TCP	192.168.2.11	54	80 → 2050 [ACK] Seq=308 Ack=1
222.0.2.101	TCP	192.168.2.11	54	80 → 2050 [FIN, ACK] Seq=30
192.168.2.11	TCP	222.0.2.101	54	2050 → 80 [ACK] Seq=159 Ack=1
192.168.2.12	TCP	222.0.2.101	58	2050 → 80 [SYN] Seq=0 Win=8
222.0.2.101	TCP	192.168.2.12	58	80 → 2050 [SYN, ACK] Seq=0
192.168.2.12	TCP	222.0.2.101	54	2050 → 80 [ACK] Seq=1 Ack=1
192.168.2.12	HTTP	222.0.2.101	211	GET / HTTP/1.1 Continuation
222.0.2.101	HTTP	192.168.2.12	361	HTTP/1.1 200 OK (text/html)
192.168.2.12	TCP	222.0.2.101	54	2050 → 80 [ACK] Seq=158 Ack=1
192.168.2.12	TCP	222.0.2.101	54	2050 → 80 [FIN, ACK] Seq=15
222.0.2.101	TCP	192.168.2.12	54	80 → 2050 [ACK] Seq=308 Ack=1
222.0.2.101	TCP	192.168.2.12	54	80 → 2050 [FIN, ACK] Seq=30
192.168.2.12	TCP	222.0.2.101	54	2050 → 80 [ACK] Seq=159 Ack=1

Packets captured on AR1's GE0/0/2----->

- private address **192.168.2.11** with port 2050 is mapped to global address **222.0.1.101** with port **552**
- private address **192.168.2.12** with port 2050 is mapped to global address **222.0.1.101** with port **808**



Packets captured on AR1's GE0/0/0  
←-----

Source	Protocol	Destination	Length	Info
222.0.1.101	TCP	222.0.2.101	58	552 → 80 [SYN] Seq=0 Win=8192
222.0.2.101	TCP	222.0.1.101	58	80 → 552 [SYN, ACK] Seq=0 Ack=1
222.0.1.101	TCP	222.0.2.101	54	552 → 80 [ACK] Seq=1 Ack=1 Win=
222.0.1.101	HTTP	222.0.2.101	211	GET / HTTP/1.1 Continuation
222.0.2.101	TCP	222.0.1.101	54	80 → 552 [ACK] Seq=1 Ack=158 Wi
222.0.2.101	HTTP	222.0.1.101	361	HTTP/1.1 200 OK (text/html)
222.0.1.101	TCP	222.0.2.101	54	552 → 80 [ACK] Seq=158 Ack=308
222.0.1.101	TCP	222.0.2.101	54	552 → 80 [FIN, ACK] Seq=158 Ack=
222.0.2.101	TCP	222.0.1.101	54	80 → 552 [ACK] Seq=308 Ack=159
222.0.2.101	TCP	222.0.1.101	54	80 → 552 [FIN, ACK] Seq=308 Ack=
222.0.1.101	TCP	222.0.2.101	54	552 → 80 [ACK] Seq=159 Ack=309
222.0.1.101	TCP	222.0.2.101	58	808 → 80 [SYN] Seq=0 Win=8192
222.0.2.101	TCP	222.0.1.101	58	80 → 808 [SYN, ACK] Seq=0 Ack=1
222.0.1.101	TCP	222.0.2.101	54	808 → 80 [ACK] Seq=1 Ack=1 Win=
222.0.1.101	HTTP	222.0.2.101	211	GET / HTTP/1.1 Continuation
222.0.2.101	HTTP	222.0.1.101	361	HTTP/1.1 200 OK (text/html)
222.0.1.101	TCP	222.0.2.101	54	808 → 80 [ACK] Seq=158 Ack=308
222.0.1.101	TCP	222.0.2.101	54	808 → 80 [FIN, ACK] Seq=158 Ack=
222.0.2.101	TCP	222.0.1.101	54	80 → 808 [ACK] Seq=308 Ack=159
222.0.2.101	TCP	222.0.1.101	54	80 → 808 [FIN, ACK] Seq=308 Ack=
222.0.1.101	TCP	222.0.2.101	54	808 → 80 [ACK] Seq=159 Ack=309



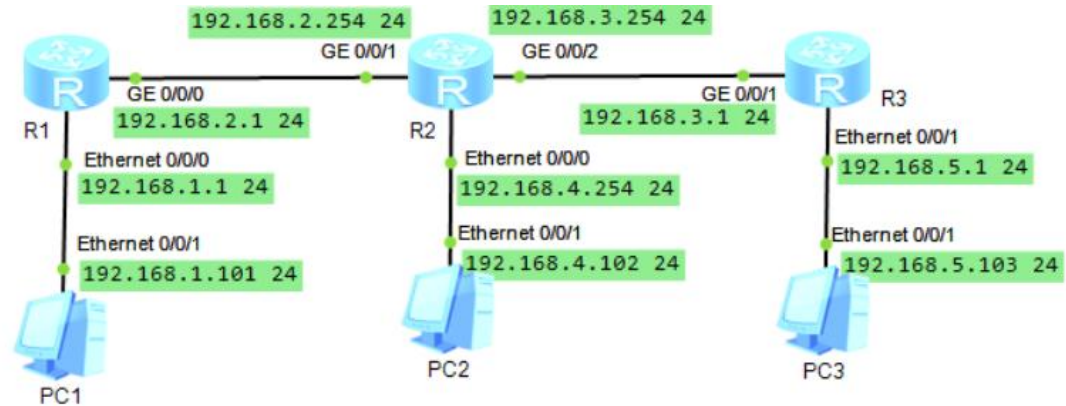
# Part C.

## RIP - Routing Information Protocol

- Distance Vector or Ford-Fulkerson algorithms
- This protocol is most useful as an "interior gateway protocol" (IGP)
- represents the metric as a sum of "costs" for individual hops
- update:
  - every gateway that participates in routing sends an update message to all its neighbors once every **30** seconds
  - wait for **180** seconds before timing out a route
- version:
  - RIP V1 (broadcast, No authentication, ...)
  - RIP V2 (multicast, authentication, ...)

# RIP(1)

- Configuration on eNSP
  - 0. interface configuration on the interface of Router
    - command: **rip 1**
  - 1. start rip configuration
    - command: **version** <version number>
  - 2. specify the rip version
    - command: **network** <network ID>



```
R1
[Huawei] rip 1
[Huawei-rip-1] version 2
[Huawei-rip-1]
Dec 2 2023 10:29:07-08:00 Huawei DS/4/DA
.25.191.3.1 configurations have been chan
e change loop count is 0 and the maximum
[Huawei-rip-1] network 192.168.1.0
[Huawei-rip-1] network 192.168.2.0
```

The configurations about RIP in this demo are as following:

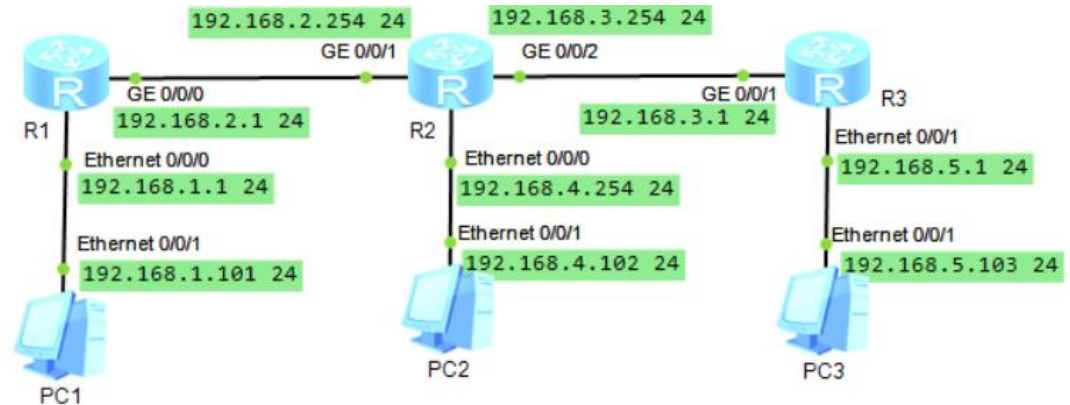
```
R1
[Huawei-rip-1]dis this
#
rip 1
version 2
network 192.168.1.0
network 192.168.2.0
#
return
```

```
R2
[Huawei-rip-1]dis this
#
rip 1
version 2
network 192.168.2.0
network 192.168.4.0
network 192.168.3.0
#
return
```

```
R3
[Huawei-rip-1]dis this
#
rip 1
version 2
network 192.168.3.0
network 192.168.5.0
#
return
[Huawei-rip-1]
```

# RIP(2)

- After the configuration on RIP is done, the routing-table of R1 is as following:
  - the routing to 192.168.3.0/24, 192.168.4.0/24, 192.168.5.0/24 are generated by RIP
  - Cost is determined by the number of routers on the routing path



R1

```
[Huawei]dis ip routing-table
```

Route Flags: R - relay, D - download to fib

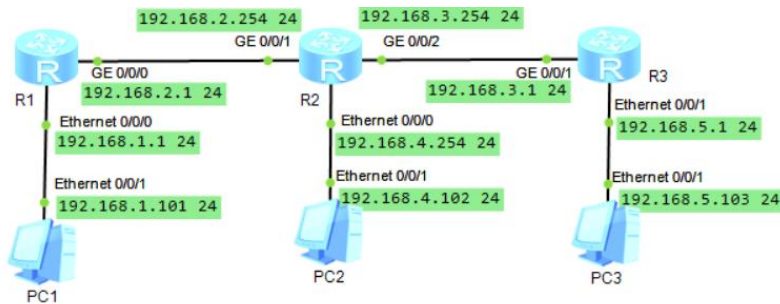
-----

Routing Tables: Public

Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
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
192.168.1.0/24	Direct	0	0	D	192.168.1.1	Ethernet0/0/0
192.168.1.1/32	Direct	0	0	D	127.0.0.1	Ethernet0/0/0
192.168.2.0/24	Direct	0	0	D	192.168.2.1	GigabitEthernet0/0/0
192.168.2.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/0
192.168.3.0/24	RIP	100	1	D	192.168.2.254	GigabitEthernet0/0/0
192.168.4.0/24	RIP	100	1	D	192.168.2.254	GigabitEthernet0/0/0
192.168.5.0/24	RIP	100	2	D	192.168.2.254	GigabitEthernet0/0/0

# RIP(3)



the routing-table of R2:

----->

the routing-table of R3:

----->

R2

```
[Huawei]dis 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
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
192.168.1.0/24	RIP	100	1	D	192.168.2.1	GigabitEthernet
0/0/1						
192.168.2.0/24	Direct	0	0	D	192.168.2.254	GigabitEthernet
0/0/1						
192.168.2.254/32	Direct	0	0	D	127.0.0.1	GigabitEthernet
0/0/1						
192.168.3.0/24	Direct	0	0	D	192.168.3.254	GigabitEthernet
0/0/2						
192.168.3.254/32	Direct	0	0	D	127.0.0.1	GigabitEthernet
0/0/2						
192.168.4.0/24	Direct	0	0	D	192.168.4.254	Ethernet0/0/0
192.168.4.254/32	Direct	0	0	D	127.0.0.1	Ethernet0/0/0
192.168.5.0/24	RIP	100	1	D	192.168.3.1	GigabitEthernet
0/0/2						

R3

```
[Huawei]dis ip routing-table
```

Route Flags: R - relay, D - download to fib

-----

Routing Tables: Public

Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
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
192.168.1.0/24	RIP	100	2	D	192.168.3.254	GigabitEthernet
0/0/1						
192.168.2.0/24	RIP	100	1	D	192.168.3.254	GigabitEthernet
0/0/1						
192.168.3.0/24	Direct	0	0	D	192.168.3.1	GigabitEthernet
0/0/1						
192.168.3.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet
0/0/1						
192.168.4.0/24	RIP	100	1	D	192.168.3.254	GigabitEthernet
0/0/1						
192.168.5.0/24	Direct	0	0	D	192.168.5.1	Ethernet0/0/1
192.168.5.1/32	Direct	0	0	D	127.0.0.1	Ethernet0/0/1

# Part D.

## OSPF – Open Shortest Path First

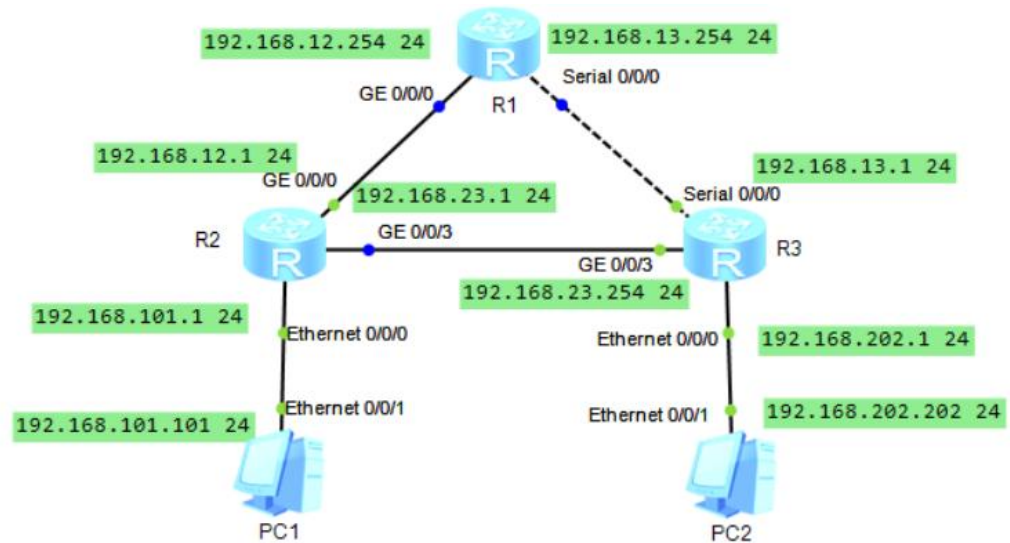
- A link-state routing protocol
- OSPF is classified as an Interior Gateway Protocol (IGP)
- Each router maintains a database describing the Autonomous System's topology



# OSPF(1)

## Configuration on eNSP

- step1 : start OSPF configuration
  - command: **ospf** <process number>
- step2: specify the index of area
  - command: **area** <area index>
- step3: add the network info which is connect directly by the Router
  - command: **network** <network ID> <wildcast mask>
  - wildcast mask: the result of performing bitwise inversion on a 32-bit subnet mask.
    - e.g. the subnet mask is: 255.255.255.0, the the wildcast mask is 0.0.0.255



R1

```
[Huawei]ospf 1
[Huawei-ospf-1]area 0
[Huawei-ospf-1-area-0.0.0.0]network 192.168.12.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]network 192.168.13.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]q
[Huawei-ospf-1]q
[Huawei]
```

R2

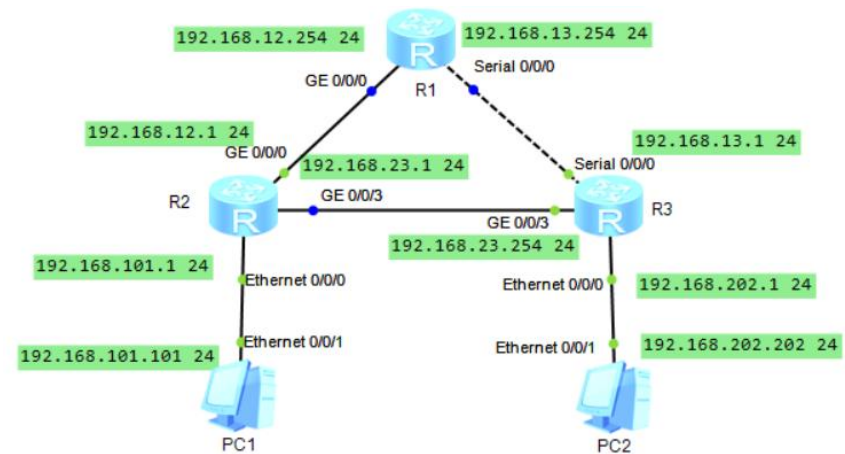
```
[Huawei]ospf 1
[Huawei-ospf-1]area 0
[Huawei-ospf-1-area-0.0.0.0]network 192.168.101.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]network 192.168.12.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]network 192.168.23.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]q
[Huawei-ospf-1]
```

R3

```
[Huawei]ospf 1
[Huawei-ospf-1]area 0
[Huawei-ospf-1-area-0.0.0.0]network 192.168.13.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]network 192.168.23.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]network 192.168.202.0 0.0.0.255
[Huawei-ospf-1-area-0.0.0.0]q
[Huawei-ospf-1]q
[Huawei]
```

# OSPF(2)

After the configuration on OSPF is done, using command “**display ospf peer**” to view information about the router's neighbors



```
R1
[Huawei]dis ospf peer

      OSPF Process 1 with Router ID 192.168.12.254
      Neighbors

Area 0.0.0.0 interface 192.168.12.254(GigabitEthernet0/0/0)'s neighbors
Router ID: 192.168.101.1   Address: 192.168.12.1
  State: Full  Mode:Nbr is Master  Priority: 1
  DR: 192.168.12.1  BDR: 192.168.12.254  MTU: 0
  Dead timer due in 29 sec
  Retrans timer interval: 5
  Neighbor is up for 00:17:48
  Authentication Sequence: [ 0 ]

      Neighbors

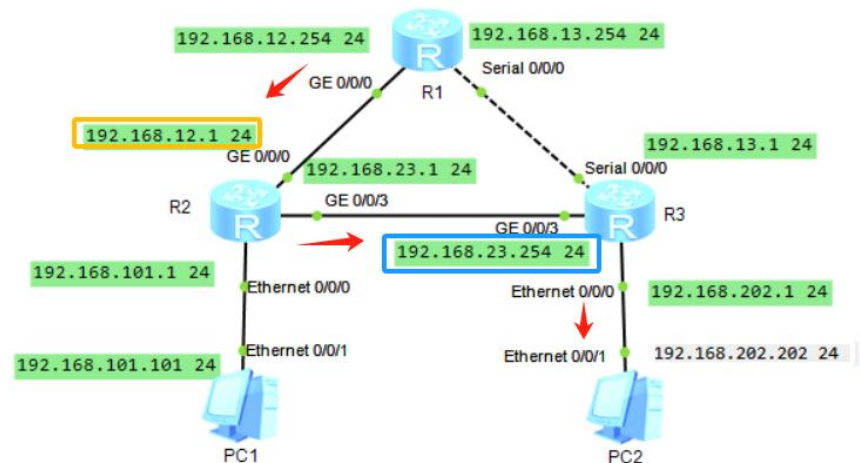
Area 0.0.0.0 interface 192.168.13.254(Serial0/0/0)'s neighbors
Router ID: 192.168.202.1   Address: 192.168.13.1
  State: Full  Mode:Nbr is Master  Priority: 1
  DR: None  BDR: None  MTU: 0
  Dead timer due in 33 sec
  Retrans timer interval: 5
  Neighbor is up for 00:15:21
  Authentication Sequence: [ 0 ]
```

# OSPF(3)

Initiate a “tracert” test from R1 to PC2, tracking the transmission path of the test packets

Q. Why R1 choose R2(192.168.12.1) other than R3(192.168.13.1) as the next hop ?

It seems that from R1 to PC2, passing directly through R3 is the least cost option?



```

R1
[Huawei] tracert 192.168.202.202

tracert to 192.168.202.202 (192.168.202.202), max hops: 30 ,packet length: 40,press CTRL_C to break
 1 192.168.12.1 50 ms 50 ms 40 ms
 2 192.168.23.254 60 ms 70 ms 60 ms
 3 192.168.202.202 90 ms 80 ms 100 ms
[Huawei]
    
```

```

R1
[Huawei]dis 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
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
192.168.12.0/24      Direct   0    0              D    192.168.12.254     GigabitEthernet
0/0/0
192.168.12.254/32    Direct   0    0              D    127.0.0.1          GigabitEthernet
0/0/0
192.168.13.0/24      Direct   0    0              D    192.168.13.254     Serial0/0/0
192.168.13.1/32      Direct   0    0              D    192.168.13.1       Serial0/0/0
192.168.13.254/32    Direct   0    0              D    127.0.0.1          Serial0/0/0
192.168.23.0/24      OSPF     10    2              D    192.168.12.1       GigabitEthernet
0/0/0
192.168.101.0/24     OSPF     10    2              D    192.168.12.1       GigabitEthernet
0/0/0
192.168.202.0/24     OSPF     10    3              D    192.168.12.1       GigabitEthernet
0/0/0
    
```



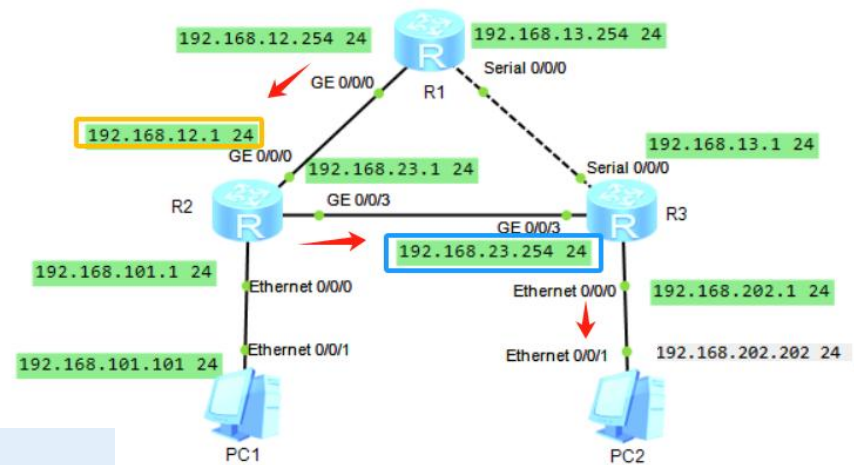
# OSPF(4)

Q. How to calculate the “cost” in OSPF ?

link cost

R1->R3->PC2 : 1562 + 1 = 1563

R1->R2->R3->PC2 : 1+1+1 = 3



```

R1
[Huawei]dis ospf routing

    OSPF Process 1 with Router ID 192.168.12.254
    Routing Tables

Routing for Network
Destination      Cost   Type      NextHop      AdvRouter      Area
192.168.12.0/24  1      Transit   192.168.12.254 192.168.12.254 0.0.0.0
192.168.13.0/24  1562   Stub      192.168.13.254 192.168.12.254 0.0.0.0
192.168.23.0/24  2      Transit   192.168.12.1  192.168.101.1  0.0.0.0
192.168.101.0/24 2      Stub      192.168.12.1  192.168.101.1  0.0.0.0
192.168.202.0/24 3      Stub      192.168.12.1  192.168.202.1  0.0.0.0

Total Nets: 5
Intra Area: 5  Inter Area: 0  ASE: 0  NSSA: 0

[Huawei]
    
```

The route with lowest link cost is the final choice for the Router, so R1->R2->R3->PC2 is the final choice.

```

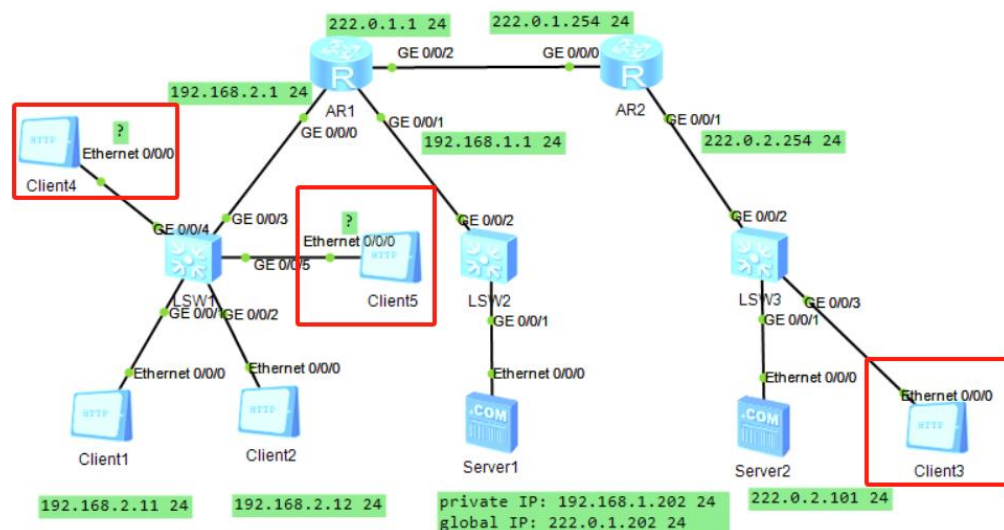
R1
[Huawei]dis ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
Destinations : 10      Routes : 10

Destination/Mask    Proto    Pre  Cost    Flags NextHop      Interface
-----
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
192.168.12.0/24      Direct   0    0        D  192.168.12.254 GigabitEthernet
0/0/0
192.168.12.254/32    Direct   0    0        D  127.0.0.1      GigabitEthernet
0/0/0
192.168.13.0/24      Direct   0    0        D  192.168.13.254 Serial0/0/0
192.168.13.1/32      Direct   0    0        D  192.168.13.1   Serial0/0/0
192.168.13.254/32    Direct   0    0        D  127.0.0.1      Serial0/0/0
192.168.23.0/24      OSPF     10    2        D  192.168.12.1   GigabitEthernet
0/0/0
192.168.101.0/24     OSPF     10    2        D  192.168.12.1   GigabitEthernet
0/0/0
192.168.202.0/24     OSPF     10    3        D  192.168.12.1   GigabitEthernet
0/0/0
    
```

# Practice 12.1

Build the following network topology, complete the configuration, achieve the following functions

- ① Client 1, Client2, Client4 and Client5 are configured with private address while share the same global address 222.0.1.101, clients could access the http server Server2.
  - NOTE: The ACL rules related to the NAT/NAPT MUST be : rule 5 permit source 192.168.2.11 0.0.0.15
- ② Server1 is configured with private address 192.168.1.202 /24 , the external clients access the server through the server's global address 222.0.1.202/24.



tips:

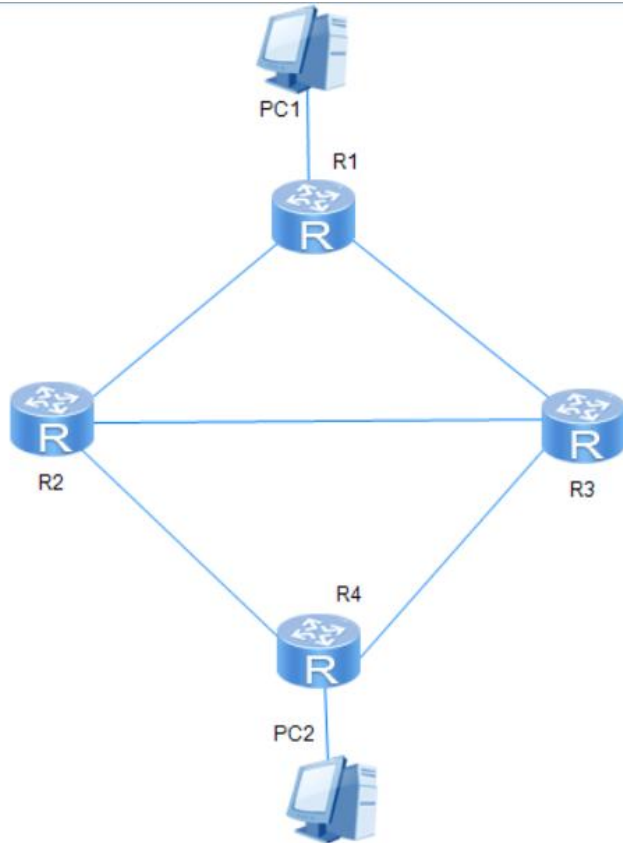
nat address-group <group id> <x.x.x.x> <x.x.x.x>

acl <acl id>

rule <rule id> permit source <x.x.x.x> <x.x.x.x>

nat outbound <acl id> address-group <group id> [no-pat]

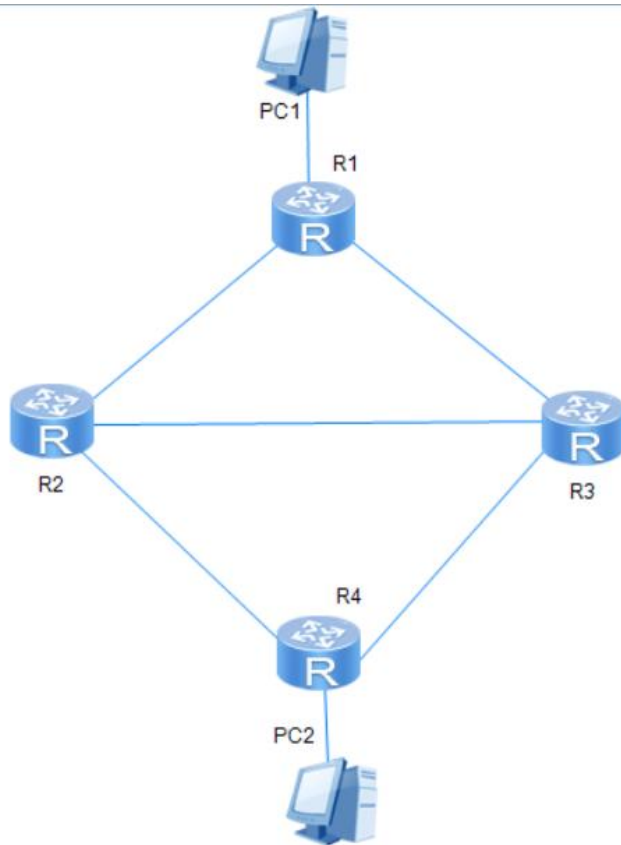
# Practice 12.2(1)



## Build the network

- Do the configuration on PCs and the interfaces of Routers
  - place notes near the interfaces to display its IPv4 address.
- Enable and configure RIP protocol on routers
  - make all the nodes(including PCs and Routers) reachable in the network.
  - list the route-table on each router in the network
  - using “ping” on PC1 to check if PC2 is reachable, while ICMP request packet leave from PC1, what's its routing path? is it the shortest path (here shortest path means minimum hops) between two nodes?
- **Tips:** use “undo rip id” on router to disable RIP protocol

# Practice 12.2(2)



Build the network

- Do the configuration on PCs and the interfaces of Routers
  - place notes near the interfaces to display its IPv4 address.
- Enable and configure OSPF protocol on routers
  - make all the nodes(including PCs and Routers) reachable in the network.
  - list the route-table on each router.
  - using “ping” on PC1 to check if PC2 is reachable, while ICMP request packet leave from PC1, what's its routing path? if the routing path is not “R1->R2->R3->R4”, try to make it.
- List the differences between RIP and OSPF protocol(at least 3 aspects) , using this practice to improve it.
- Tips, while using the serial interface of the router, “Serial” of “Connections” is suggested to connect the serial interface.

