

CCNA (200-301) Cisco Certified Network Associate

Prepared by Eng. Taghreed Elsayed

Lecture 9

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

مزيد من التفاصيل

Network Address Translation(NAT)

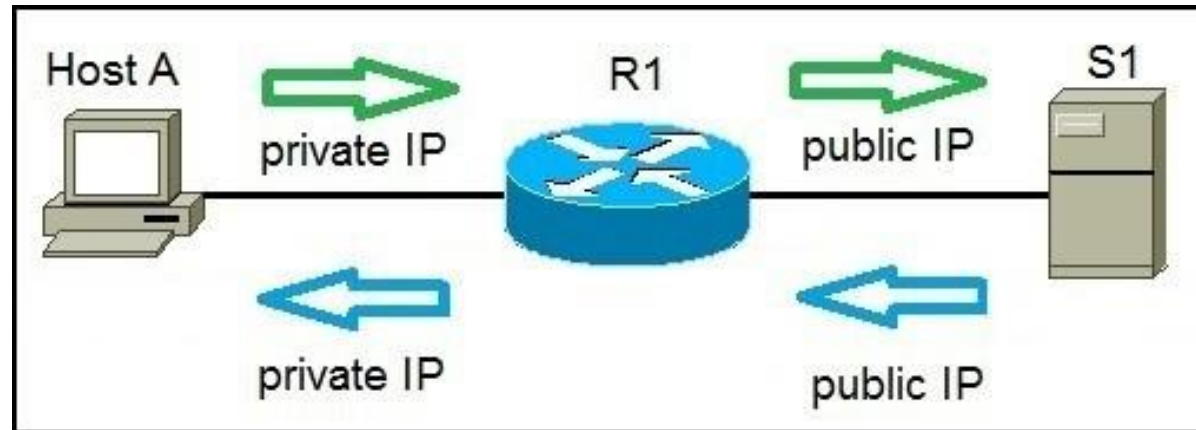


جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

What is NAT?

- ❑ **NAT (Network Address Translation)** is a process of changing the source and destination IP addresses and ports. Address translation reduces the need for IPv4 public addresses and hides private network address ranges. This process is usually done by routers or firewalls.
- ❑ **An example will help you understand the concept:**
 - Host A request a web page from an Internet server. Because Host A uses private IP addressing, the source address of the request has to be changed by the router because private IP addresses are not routable on the Internet.

- ❑ Router R1 receives the request, changes the source IP address to its public IP address and sends the packet to server S1. Server S1 receives the packet and replies to router R1. Router R1 receives the packet, changes the destination IP addresses to the private IP address of Host A and sends the packet to Host A.



❖ **Here are three types of address translation:**

1. Static NAT – : translates one private IP address to a public one. The public IP address is always the same.

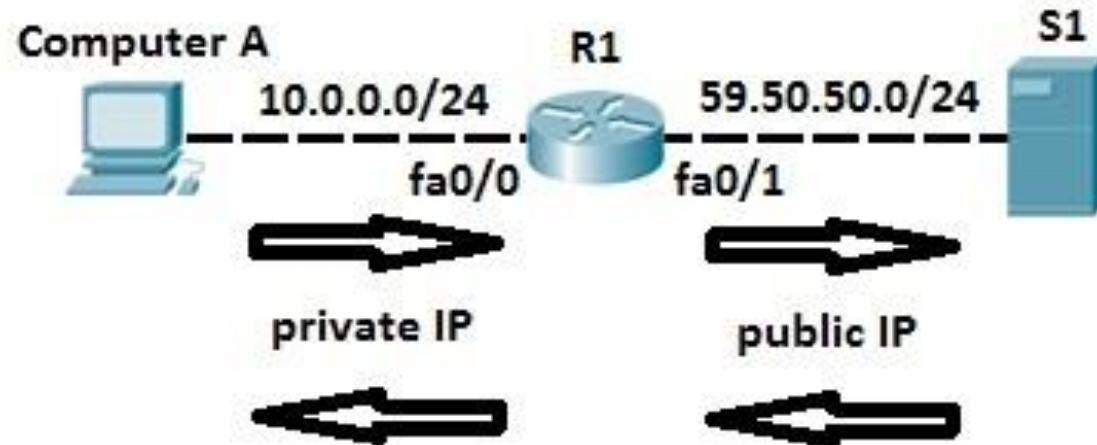
2. Dynamic NAT – : private IP addresses are mapped to the pool of public IP addresses.

3. Port Address Translation (PAT) – : one public IP address is used for all internal devices, but a different port is assigned to each private IP address. Also known as NAT Overload.

Static NAT

- ❑ With static NAT, routers or firewalls translate one private IP address to a single public IP address. Each private IP address is mapped to a single public IP address.
- ❑ Static NAT is not often used because it requires one public IP address for each private IP address.
- ❑ To configure static NAT, three steps are required:
 1. **configure private/public IP address mapping by using the**
➤ ip nat inside source static PRIVATE_IP PUBLIC_IP command

- 2. configure the router's inside interface using the ip nat inside command.
- 3. configure the router's outside interface using the ip nat outside command.
- Here is an example.



- ❑ Computer A requests a web resource from S1. Computer A uses its private IP address when sending the request to router R1. Router R1 receives the request, changes the private IP address to the public one and sends the request to S1. S1 responds to R1. R1 receives the response, looks up in its NAT table and changes the destination IP address to the private IP address of Computer A.
- ❑ In the example above, we need to configure static NAT. To do that, the following commands are required on R1:

NAT (Network Address Translation)

```
R1(config)#ip nat inside source static 10.0.0.2 59.50.50.1
R1(config)#int fa0/0
R1(config-if)#ip nat inside
R1(config-if)#int fa0/1
R1(config-if)#ip nat outside
```

- Using the commands above, we have configured a static mapping between **Computer A's private IP address of 10.0.0.2 and router's R1 public IP address of 59.50.50.1. To check NAT, you can use the show ip nat translations command:**

```
R1#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 59.50.50.1:9        10.0.0.2:9        59.50.50.2:9        59.50.50.2:9
---  59.50.50.1          10.0.0.2          ---                 ---
```

Dynamic NAT

- ❑ Unlike with static NAT, where you had to manually define a static mapping between a private and public address, dynamic NAT does the mapping of a local address to a global address happens dynamically.
- ❑ This means that the router dynamically picks an address from the global address pool that is not currently assigned. The dynamic entry stays in the NAT translations table as long as the traffic is exchanged.

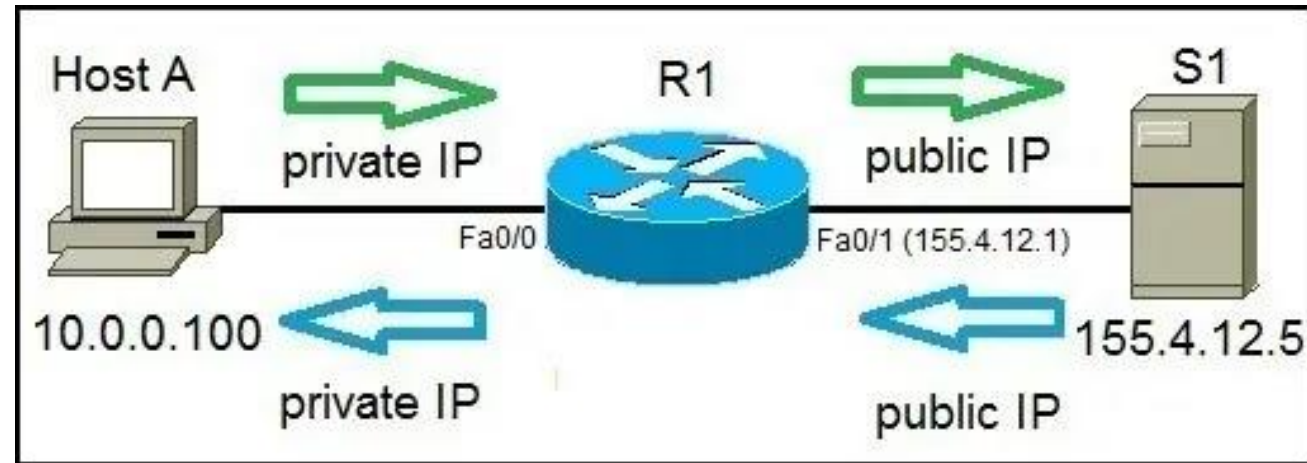
- ❑ The entry times out after a period of inactivity and the global IP address can be used for new translations.
- With dynamic NAT, you need to specify two sets of addresses on your Cisco router:
 - The inside addresses that will be translated
 - A pool of global addresses
- To configure dynamic NAT, the following steps are required:

1. configure the router's inside interface using the *ip nat inside* command.
2. configure the router's outside interface using the *ip nat outside* command.
3. configure an ACL that has a list of the inside source addresses that will be translated.
4. configure a pool of global IP addresses using the *ip nat pool NAME FIRST_IP_ADDRESS LAST_IP_ADDRESS netmask SUBNET_MASK* command
5. enable dynamic NAT with the *ip nat inside source list ACL_NUMBER pool NAME global* configuration command



Consider the following example:

NAT (Network Address Translation)



- ❑ Host A requests a web resource from a internet server S1.
- ❑ Host A uses its private IP address when sending the request to router R1.
- ❑ Router R1 receives the request, changes the private IP address to one of the available global addresses in the pool and sends the request to S1.

- ❑ S1 responds to R1.
- ❑ R1 receives the response, looks up in its NAT table and changes the destination IP address to the private IP address of Host A.
- To configure dynamic NAT, the following commands are required on R1:
- 1. **First we need to configure the router's inside and outside NAT interfaces:**

```
R1(config)#int f0/0  
R1(config-if)#ip nat inside  
R1(config-if)#int f0/1  
R1(config-if)#ip nat outside
```

- **2. Next, we need to configure an ACL that will include a list of the inside source addresses that will be translated. In this example we want to translate all inside hosts on the 10.0.0.0/24 network:**

```
R1(config)#access-list 1 permit 10.0.0.0 0.0.0.255
```

3. We need to configure the pool of global (public) IP addresses available on the outside interface:

```
R1(config)#ip nat pool STUDY-CCNA_POOL 155.4.12.1 155.4.12.3 netmask 255.255.255.0
```

The pool configured above consists of 3 addresses: 155.4.12.1, 155.4.12.2, and 155.4.12.3.

4. Lastly, we need to enable dynamic NAT:

```
R1(config)#ip nat inside source list 1 pool STUDY-CCNA_POOL
```

- ❑ The command above tells the router to translate all addresses specified in the **access list 1** to the pool of global addresses **named MY POOL.**
- ❑ You can list all NAT translations using the **show ip nat translations** command.
- ❑ Generate some traffic **from the PC to the server** first to test:

```
C:\>ping 155.4.12.5
```

```
Pinging 155.4.12.5 with 32 bytes of data:
```

```
Reply from 155.4.12.5: bytes=32 time<1ms TTL=127
```

```
Reply from 155.4.12.5: bytes=32 time=3ms TTL=127
```

```
Reply from 155.4.12.5: bytes=32 time=1ms TTL=127
```

```
Reply from 155.4.12.5: bytes=32 time<1ms TTL=127
```

```
Ping statistics for 155.4.12.5:
```

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

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

```
    Minimum = 0ms, Maximum = 3ms, Average = 1ms
```



- ❑ Then enter the ***show ip nat translations*** command quickly enough before the translation has timed out.

```
R1#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 155.4.12.1:16      10.0.0.100:16     155.4.12.5:16     155.4.12.5:16
```

- ❑ In the output above you can see that the translation has been made between the Host A's private IP address (***Inside local, 10.0.0.100***)

❑ to the first available public IP address from the **pool (Inside global, 155.4.12.1)** and it is connecting to the server on the **outside** (Outside local and Outside global, 155.4.12.5) .

❑ **NOTE**

You can remove all NAT translations from the table by using the

❑ **clear ip nat translation *** command.

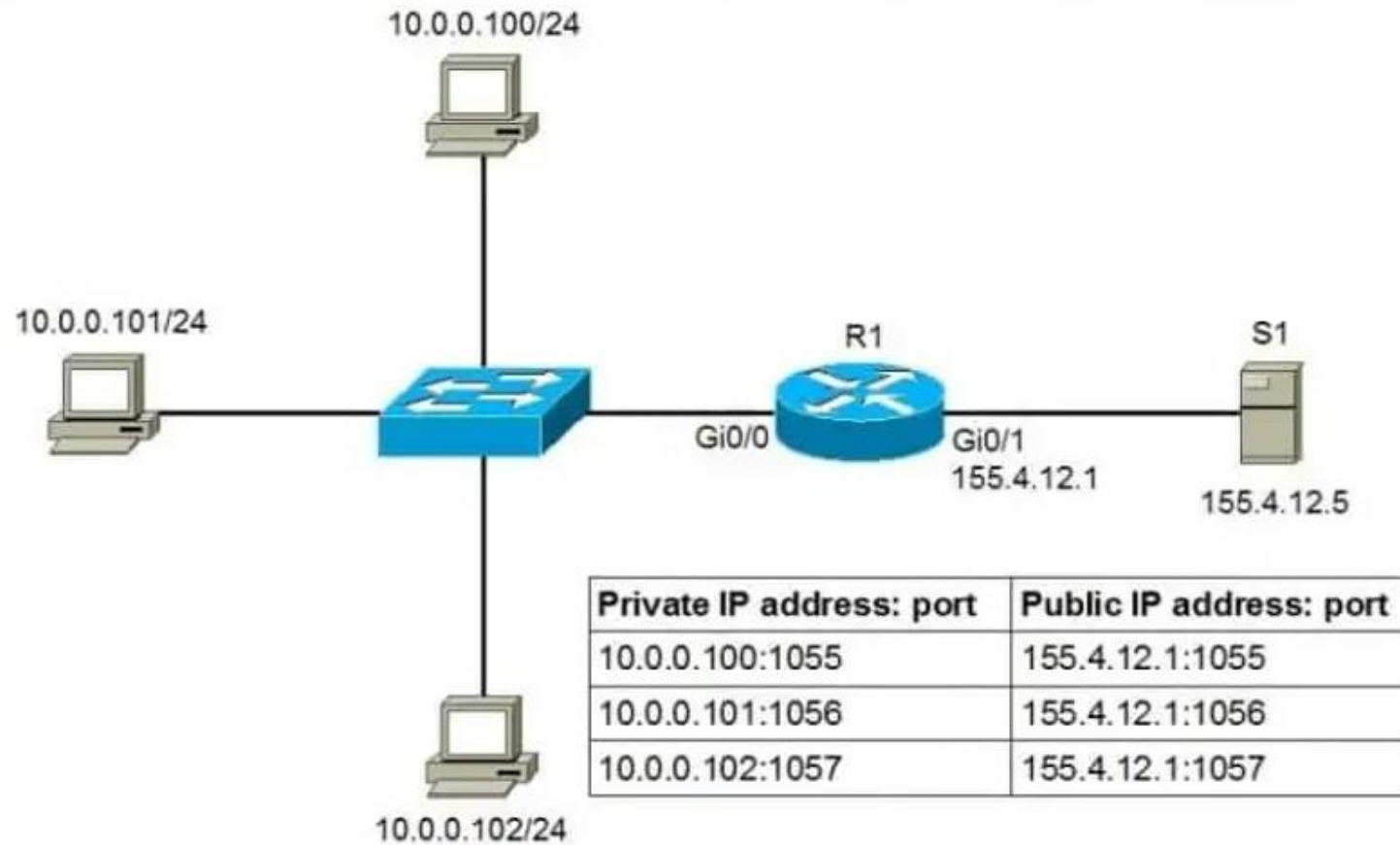
Port Address Translation (PAT) configuration

- ❑ With **Port Address Translation (PAT)**, a single public IP address is used for all internal private IP addresses, but a different port is assigned to each private IP address.
- ❑ This type of NAT is also known as **NAT Overload** and is the typical form of NAT used in today's networks. It is even supported by most consumer-grade routers.
- ❑ **PAT allows you to support** many hosts with only few public IP addresses. It works by creating dynamic NAT mapping, in which a global (public) IP address and a unique port number are selected.

- ❑ The router keeps a NAT table entry for every unique combination of the private IP address and port, with translation to the global address and a unique port number.
- ❖ We will use the following example network to explain the benefits of using PAT:

Chapter 04

NAT (Network Address Translation)



- ❑ As you can see in the picture above, PAT uses unique source port numbers on the inside global (public) IP address to distinguish between translations.
- ❑ For example, if the host with the IP address of 10.0.0.101 wants to access the server S1 on the Internet, the host's private IP address will be translated by R1 to 155.4.12.1:1056 and the request will be sent to S1. S1 will respond to 155.4.12.1:1056.
- ❑ R1 will receive that response, look up in its NAT translation table, and forward the request to the host.

Port Address Translation (PAT) configuration

- ❑ To configure PAT, the following commands are required:
 - configure the router's inside interface using the *ip nat inside* command.
 - configure the router's outside interface using the *ip nat outside* command.
 - configure **an access list that includes** a list of the inside source addresses that should be translated.
- ❑ enable PAT with the *ip nat inside source list ACL_NUMBER interface TYPE overload* global configuration command.

- ❑ **Here is how we would configure PAT** for the network picture above. First, we will define the outside and inside interfaces on R1:

```
R1(config)#int Gi0/0
R1(config-if)#ip nat inside
R1(config-if)#int Gi0/1
R1(config-if)#ip nat outside
```

- ❑ **Next, we will define an access list that will include all private IP addresses we would like to translate:**

```
R1(config-if)#access-list 1 permit 10.0.0.0 0.0.0.255
```

- **The access list defined above includes all IP addresses from the 10.0.0.0 – 10.0.0.255 range.**
- Now we need to enable NAT and refer to the ACL created in the previous step and to the interface whose IP address will be used for translations:

```
R1(config)#ip nat inside source list 1 interface Gi0/1 overload
```

- ❑ To verify the NAT translations, we can use the show ip nat translations command after hosts request a web resource from S1:

```
R1#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 155.4.12.1:1024 10.0.0.100:1025 155.4.12.5:80 155.4.12.5:80
tcp 155.4.12.1:1025 10.0.0.101:1025 155.4.12.5:80 155.4.12.5:80
tcp 155.4.12.1:1026 10.0.0.102:1025 155.4.12.5:80 155.4.12.5:80
```

- ❑ **Notice that** the same IP address (155.4.12.1) has been used to translate three private IP addresses (10.0.0.100, 10.0.0.101, and 10.0.0.102).
- ❑ The port number of the public IP address is unique for each connection. So when S1 responds to 155.4.12.1:1026, R1 look into its NAT translations table and forward the response to 10.0.0.102:1025



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

