NAT 50 Interview Questions

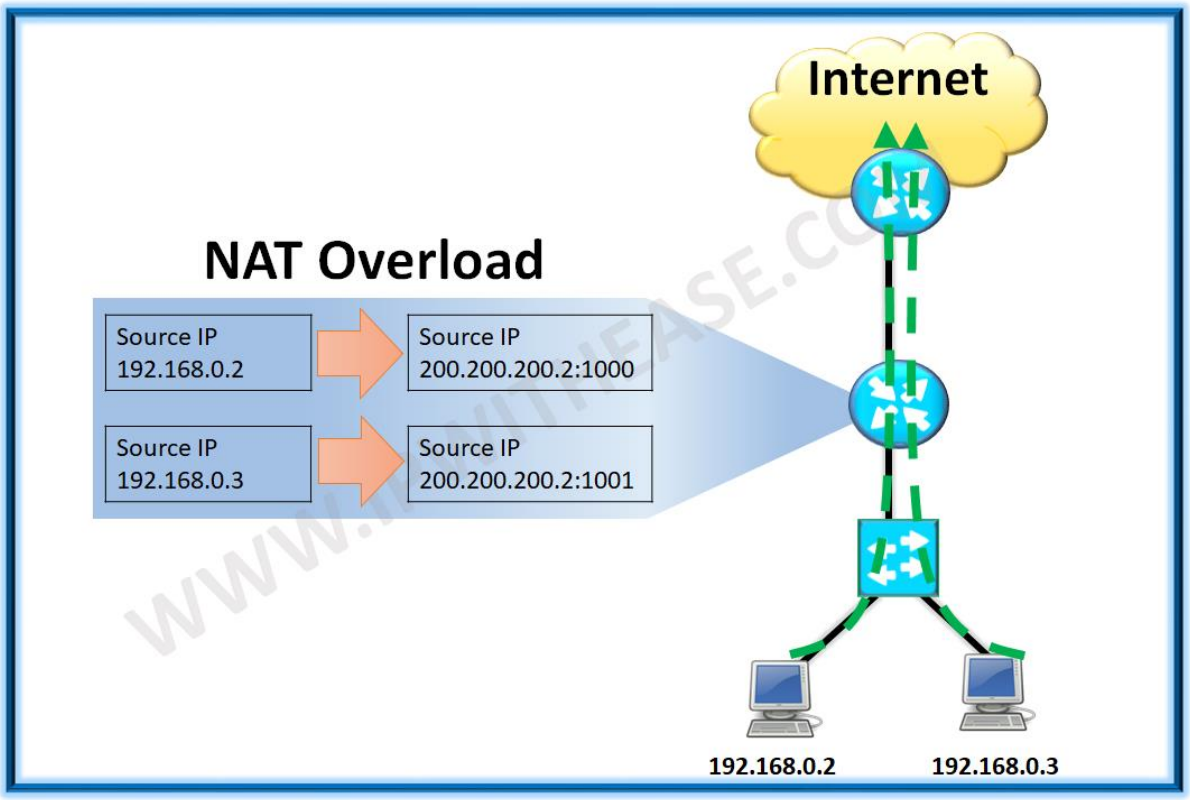
Ques1. What is NAT?

NAT alters IP address in header of an Ip Address packet and allows using Public IP for communication to outside world and private IP for communication to Inside.

Ques2. What is PAT?

Port address translation (PAT) also called **NAT overload** is a flavor of NAT which allows multiple users within a private network to make use of a minimal number of IP addresses. Its basic function is to share a single IP public address between multiple clients who need to use the Internet publicly. It is an extension of network address translation (NAT) and may be called as many-to-one Translation.

Below scenario shows NAT Overload (PAT) configured on Router for giving internet access to multiple inside hosts (Private IP = 192.168.0.2 and 192.168.0.3). The NAT Router translates private source IP of LAN endpoints into same Public IP but with different port number ie 200.200.200.2:1000 and 200.200.200.2:1001 respectively.

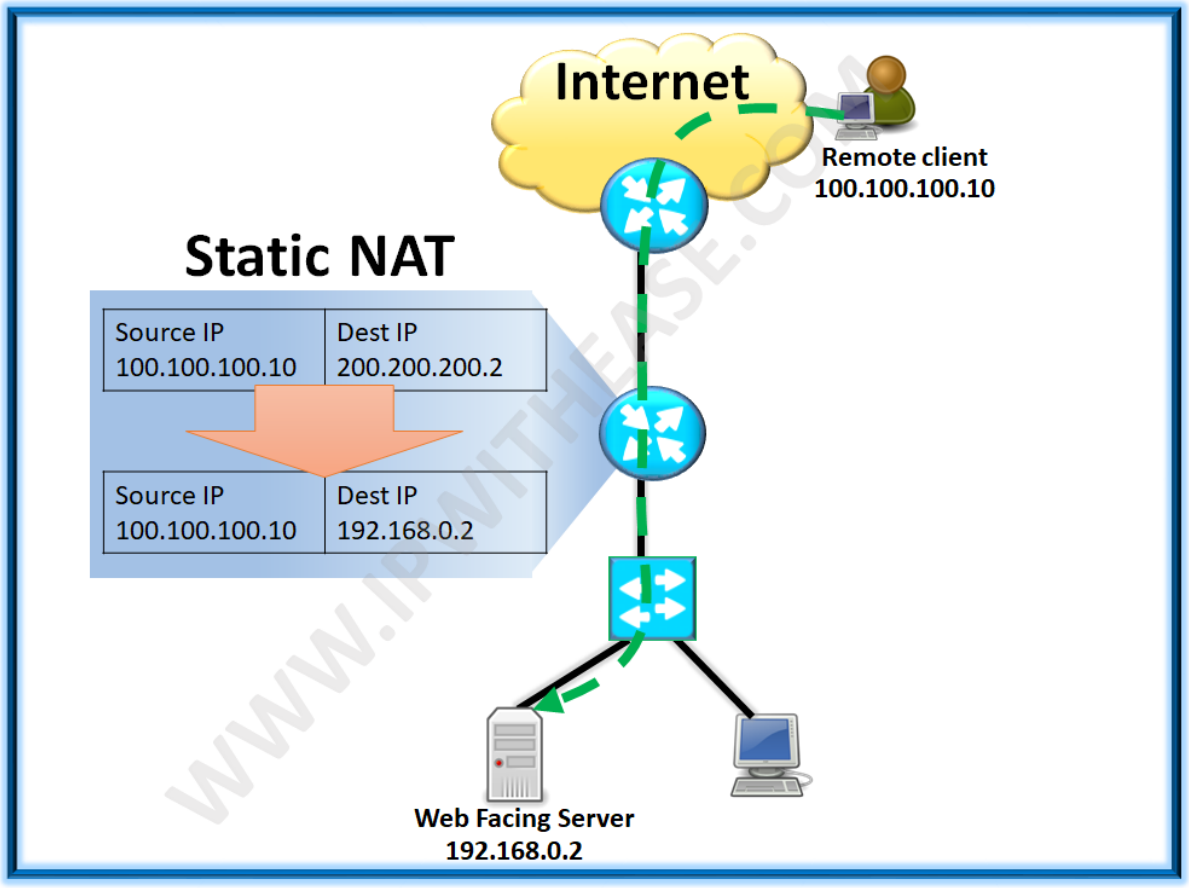


Ques3. What is Static NAT?

Static NAT (Network Address Translation) is one-to-one mapping of a private IP address to a public IP address. Static NAT is useful when a network device inside a private network needs to be accessible from internet. A common example is Static NAT configured on Router or Firewall for providing access to Web Facing application in LAN for Users who are on Internet.

With static NAT, translations remain in the NAT translation table as soon as you configure static NAT command, and they remain in the translation table until static NAT is deleted.

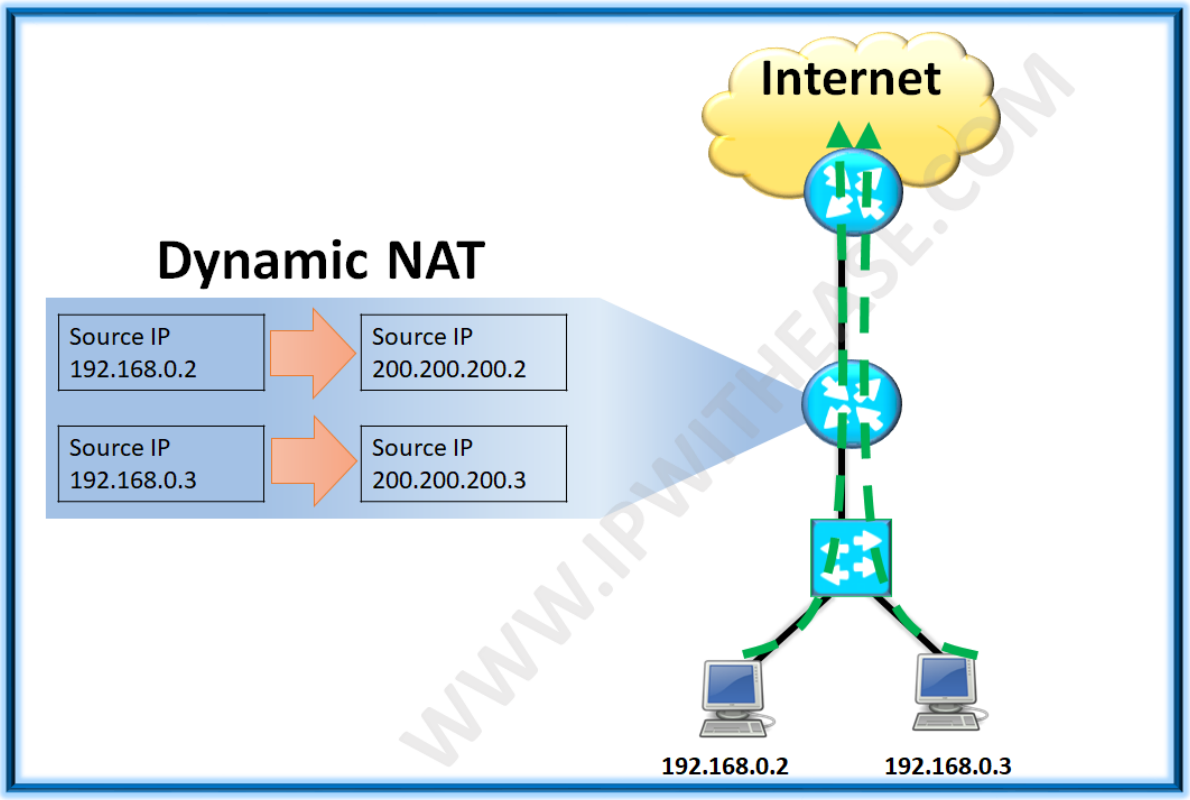
Below scenario shows static NAT configured on Router for giving access to Web Server (Private IP = 192.168.0.2). For outside users, the Web Server IP is 200.200.200.2 which translates to 192.168.0.2 when request from user hits the Router and enters into LAN.



Ques4. What is Dynamic NAT?

Dynamic NAT uses the concept of "POOL" of public IP addresses that can be assigned internal LAN endpoints dynamically. The NAT router creates a one-to-one mapping between an inside local and inside global address and changes the IP addresses in packets as they exit and enter the inside network. Dynamic NAT can't be used to NAT for servers and devices that need to be accessible from the Internet. With dynamic NAT, translations do not exist in the NAT table until the router receives traffic that requires translation. Dynamic translations have a timeout period after which they are purged from the translation table.

Below scenario shows dynamic NAT configured on Router for giving internet access to hosts (Private IP = 192.168.0.2 and 192.168.0.3). The NAT Router translates private source IP of LAN endpoints into Public IPs (200.200.200.2 and 200.200.200.3 respectively) .



Ques5. While configuring NAT on Router, Which command would you place on interface connected to the Internet?

a) ip nat inside
b) ip nat outside
c) ip outside global
d) ip inside local

ip nat outside

Ques6. Which command will show us all the translations active on your router?

Show ip nat translations

Below is an example scenario on output of "show ip nat translations" command -

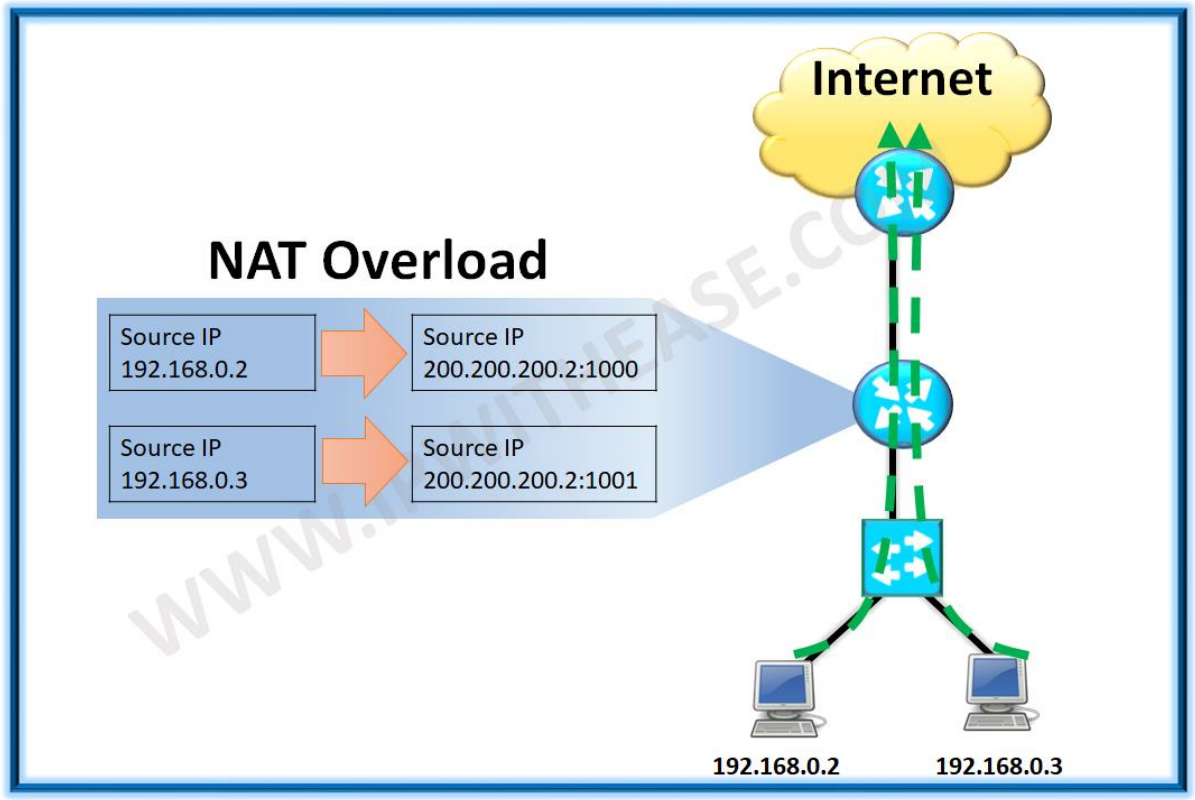
R1# **show ip nat translation**

Pro	Inside global	Inside local	Outside local	Outside global
icmp	10.2.2.2:3	10.1.1.1:3	10.2.2.3:3	10.2.2.3:3
icmp	10.2.2.2:4	10.1.1.1:4	10.2.2.3:4	10.2.2.3:4
icmp	10.2.2.2:5	10.1.1.1:5	10.2.2.3:5	10.2.2.3:5

Ques7. What is NAT Overload?

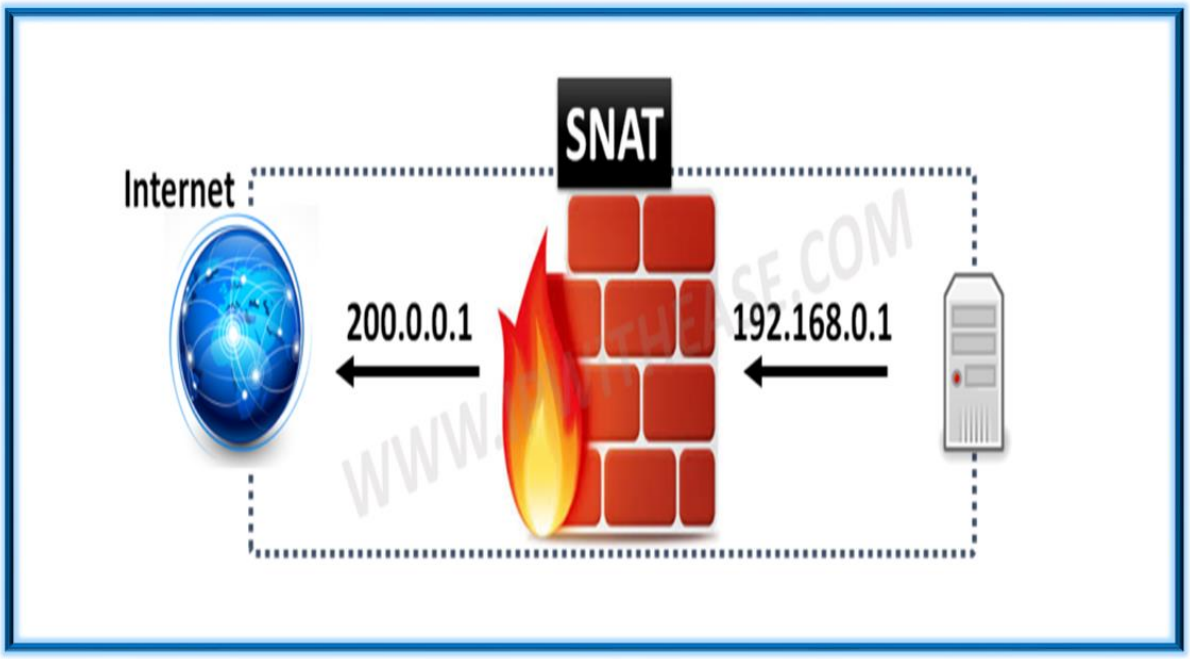
NAT Overload is another type of dynamic NAT which can map multiple private IP addresses to a single public IP address by using a technology known as Port Address Translation. In this case, multiple internal devices are able to share one public address, as mappings are placed into the mappings table based on the source and destination ports that are used. When using PAT, the router maintains unique source port numbers on the inside global IP address to distinguish between translations.

Below scenario shows **NAT Overload (PAT)** configured on Router for giving internet access to multiple inside hosts (Private IP = 192.168.0.2 and 192.168.0.3). The NAT Router translates private source IP of LAN endpoints into same Public IP but with different port number i.e. 200.200.200.2:1000 and 200.200.200.2:1001 respectively.



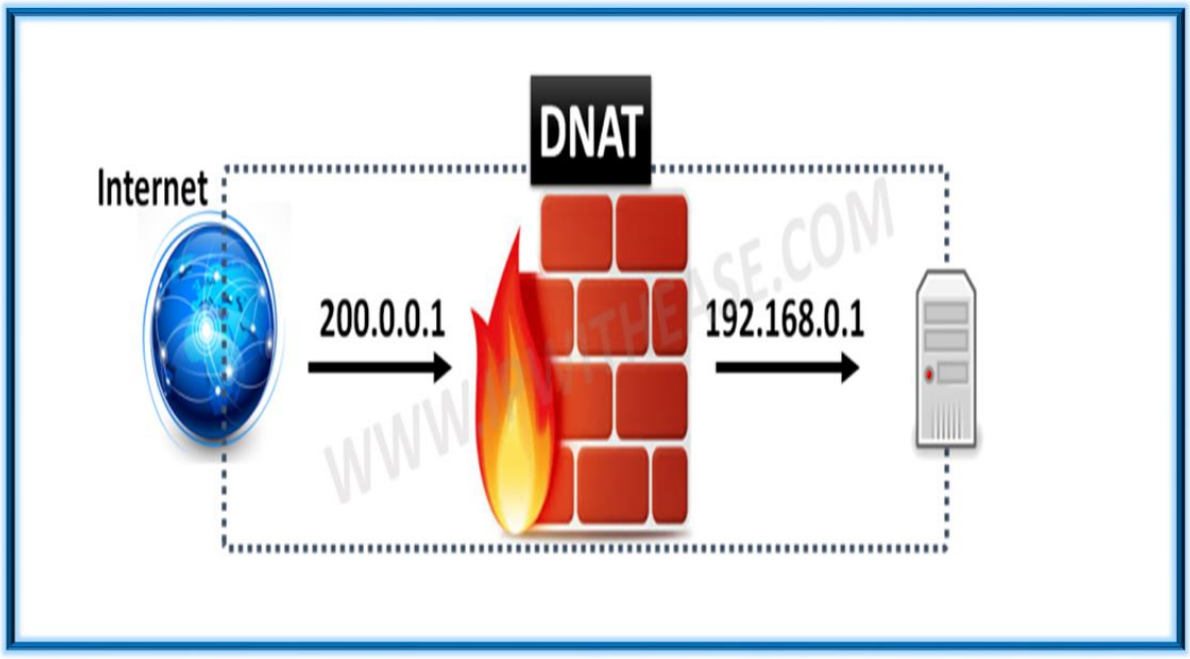
Ques8. What is Source NAT?

SNAT is abbreviation for **Source Network Address Translation**. It is typically used when an internal/private host needs to initiate a connection to an external/public host. The device performing NAT changes the private IP address of the source host to public IP address. It may also change the source port in the TCP/UDP headers.



Ques9. What is Destination NAT?

DNAT stands for **Destination Network Address Translation**. Destination NAT changes the destination address in IP header of a packet. It may also change the destination port in the Post to Post Links II error: Unrecognized type:"slug"headers. The typical usage of this is to redirect incoming packets with a destination of a public address/port to a private IP address/port inside your network. Destination NAT is performed on incoming packets, where the DNAT translates a public destination address to a private address. DNAT is a 1-to-1, static translation with the option to perform port forwarding or port translation. Users over Internet Accessing a Web Server hosted in a Data Center is a typical example where DNAT is used to hide the private Address of Web Server and NAT device translates the Public Destination IP reachable to Internet Users to Private IP address of Web Server.



Ques10. Which command would we place on interface on a private/inside/LAN network?

ip nat inside

Ques11. When creating a pool of global addresses, which keyword can be used instead of the "netmask" command?

Alternative to using "netmask" keyword in "prefix-length" while configuring ip nat pool.

Syntax -

ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}

Below is example to show nat pool configuration using prefix-length keyword -

ip nat pool NATPOOL 192.168.10.1 192.168.10.255 prefix-length 24

Ques12. What is ALG?

ALG is abbreviation for "**Application Level Gateway**" and is responsible for translating IP address information inside the payload of an applications packet.

NAT performs translation service on any TCP/UDP traffic that does not carry the source and destination IP addresses in the application data stream. However, application like SIP etc. insert IP the address information within the payload and therefore require support of an Application Level Gateway (ALG).

Ques13. Can I change the amount of time it takes for a NAT translation to time out from the NAT translation table?

Yes, the command to change the NAT Translation timeout setting is –

"Clear ip nat translation <timeout value>"

Ques14. Does NAT occur before or after routing?

Order in which NAT and Routing takes place primarily depends on the direction of traffic flow.

If the packet is from a NAT inside-designated interface, it uses the inside-to-outside list. If the packet is from an outside-to-inside interface, it uses that list.

Direction	Sequence (Order)		
Inside-To-Outside	Policy Routing	Routing	NAT (local to global translation)
Outside-To-Inside	NAT (global to local translation)	Policy Routing	Routing

Ques15. Explain following NAT command – "ip nat inside source list 10 interface FastEthernet 0/0 overload?

The above command establishes dynamic source translation, specifying the access list "**10**". The keyword "**Overloading**" allowed NATting of multiple clients to the **Fast Ethernet 0/0** IP address of the device.

Ques16. What is the maximum number of configurable NAT IP pools?

In practical use, the maximum number of configurable IP pools is limited by the amount of available DRAM in the particular router. (Cisco recommends that you configure a pool size of

255.) Each pool should be no more than 16 bits. In 12.4(11)T and later, IOS introduce CCE (Common Classification Engine). This has limited NAT to only have a maximum of 255 pools. In 12.2S code base, there is no maximum pools restriction.

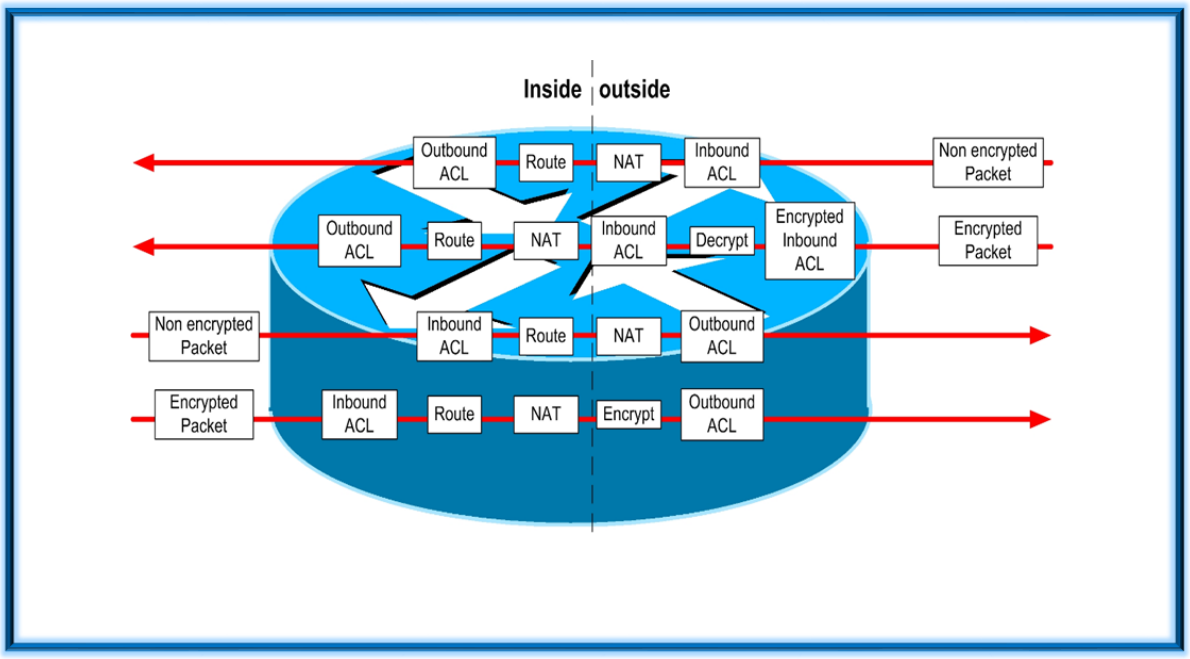
Ques17. Which command will show you the summary of the NAT configuration?

"**Show ip nat statistics**" will provide the requisite out to show summary of NAT configuration.

Ques18. What are two benefits of using NAT?

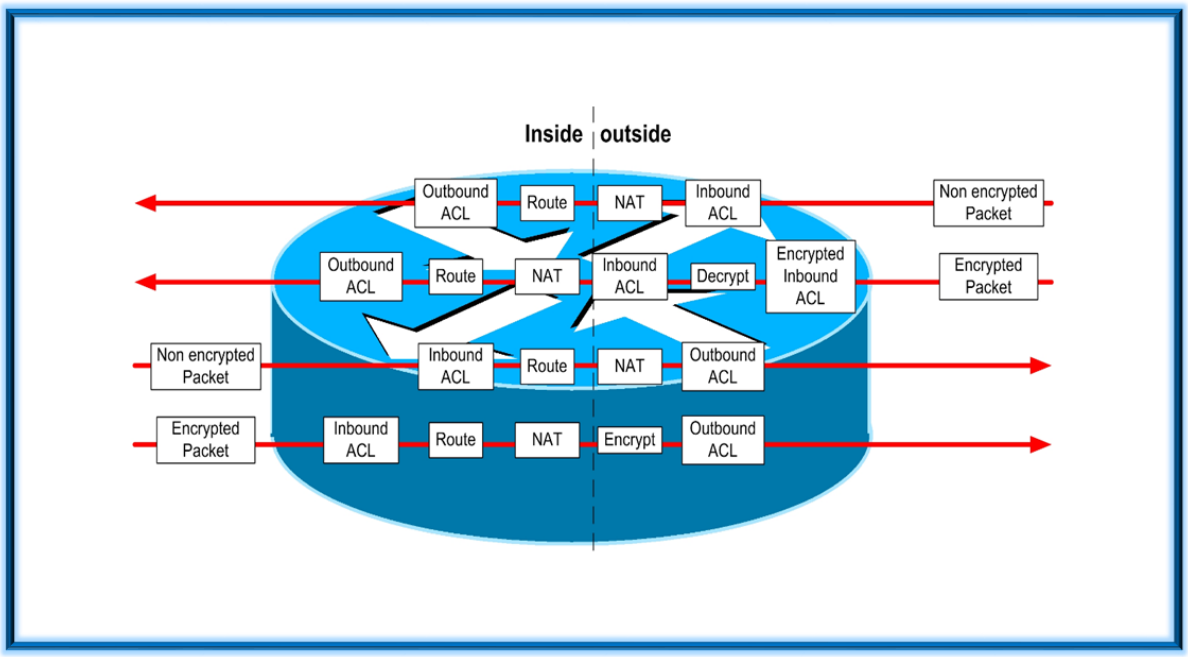
- NAT protects network security because private networks are not advertised.
- NAT eliminates the need to re-address all host that require external access.

Ques19. What is NAT Order of Operation – "Inside-to-Outside"?



- If IPsec then check input access list
- Decryption - for CET (Cisco Encryption Technology) or IPSec
- check input access list
- check input rate limits
- input accounting
- Redirect to web cache
- Policy routing
- routing
- NAT inside to outside (local to global translation)
- Crypto (check map and mark for encryption)
- check output access list
- inspect (Context-based Access Control (CBAC))
- TCP intercept
- Encryption
- Queueing

Ques20. What is NAT Order of Operation – “Outside-to-Inside”?



- If IPSec then check input access list
- Decryption - for CET or IPSec
- check input access list
- check input rate limits
- input accounting
- Redirect to web cache
- NAT outside to inside (global to local translation)
- Policy routing
- routing
- Crypto (check map and mark for encryption)
- check output access list
- inspect CBAC
- TCP intercept
- Encryption
- Queueing

Ques21. Can we rate limit the number of NAT translations?

“**Ip nat translation max-entries** “command is used to limit the number of NAT translations.
Syntax –
ip nat translation max-entries {number | all-vrf number | host ip-address number | list listname number | vrf name number}

Device (config)# **ip nat translation max-entries 300**

Ques22. Is there any relation between NAT concurrent sessions and DRAM on device?

As a general understanding, approx. 300 bytes or dynamic memory is used up per NAT translation. Hence, if we have 10000 translations showing in NAT translation table, approx. 3MB of memory will be used.

Ques23. What are NAT IP pools?

Network Address Translation Pool in simple terms is a pool that has been carved out of an allocated address block that assigns inside global addresses on a first come first serve basis to inside local host based on a match found in a specified access control list. The benefit of this type of configuration is that your inside network can use RFC1918 private addressing such as the 10.0.0.0/8 range but still obtain IP connectivity to the outside world using a single public IP address per host.

Ques24. What are static NAT translations?

Static NAT translations have one-to-one mapping between local and global addresses. Users can also configure static address translations to the port level, and use the remainder of the IP address for other translations.
The following example shows NAT translation for static NAT –

"ip nat inside source static 1.1.1.1 2.2.2.2"

Ques25. What is NAT NVI?

Starting with IOS version 12.3(14)T, Cisco introduced the feature of **NAT Virtual Interface**. **NVI** removes the need to configure an interface as either NAT inside or NAT outside. Instead, an interface can be configured to use NAT or not use NAT.
Below configuration examples demonstrates Legacy NAT and NVI commands –

With Legacy Nat Configuration would be like –

```
R1(config)#interface range FastEthernet 0/0
R1(config-if-range)#ip nat inside
R1(config)#interface range FastEthernet 0/1
R1(config-if-range)#ip nat outside
R1(config)#ip nat inside source static 192.168.0.10 172.16.0.10
```

With NVI, NAT Configuration would be like -

```
R1(config)#interface range FastEthernet 0/0
R1(config-if-range)#ip nat enable
R1(config)#interface range FastEthernet 0/1
R1(config-if-range)#ip nat enable
R1(config)#ip nat source static 192.168.0.10 172.16.0.10
```

Ques26. Explain the term –

i. Inside Local
ii. Inside Global
iii. Outside Local
iv. Outside Global

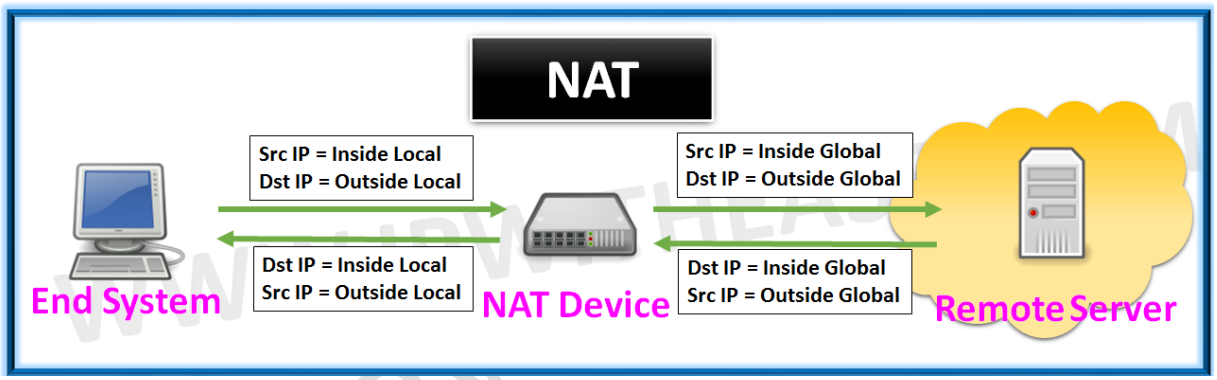
i. **Inside Local** – Refers to actual address assigned to an inside host. In other words, Inside local address is an IP address assigned to an end host inside the LAN network. Inside Local addresses are typically private IP addresses, which stay inside our network.

ii. **Inside Global** - Inside address seen from the outside. Inside Global address are typically public IP addresses which are assigned to our end internet facing router to be used as the IP address for communicating with other devices in the internet. The Inside Local IP addresses are removed at the NAT router and translated with Inside Global address.

iii. **Outside Local** - Actual address assigned to an outside host. The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.

iv. **Outside Global** - Outside address seen from the inside. The IP address assigned to a host on the outside network by the host owner. The address is allocated from a globally routable address or network space.

The above terms can be best illustrated by below diagram -



Ques27. What is Stateful NAT (SNAT)?

Stateful NAT is a high availability configuration where we have redundant pair of NAT Routers. This configuration slows the second router to take over NAT functionality if the first fails.

Ques28. What is NAT-PT?

The **"NAT-PT"** is abbreviation for **"Network Address Translation - Port Translation"** is an IPv6 to IPv4 translation mechanism, which allows IPv6-only devices to communicate with IPv4-only devices and vice versa. NAT-PT is designed to be deployed to allow direct communication between IPv6-only networks and IPv4-only networks transparently that use a single V4 address

Ques29. What conditions necessitate NAT configuration?

Below are 2 key reasons why NAT is used -

- **Usable Public Addresses** - While there are enough private IP addresses to be assigned to all endpoints of a private LAN network, there are only a limited number of public IP addresses that can be given to companies to communicate with the outside network.

- **Security -** As the internal IP addresses are changed for all the computers at the gateway level, the internal IP addresses are never revealed to the external world receiving the packets/ intercepting the packets.

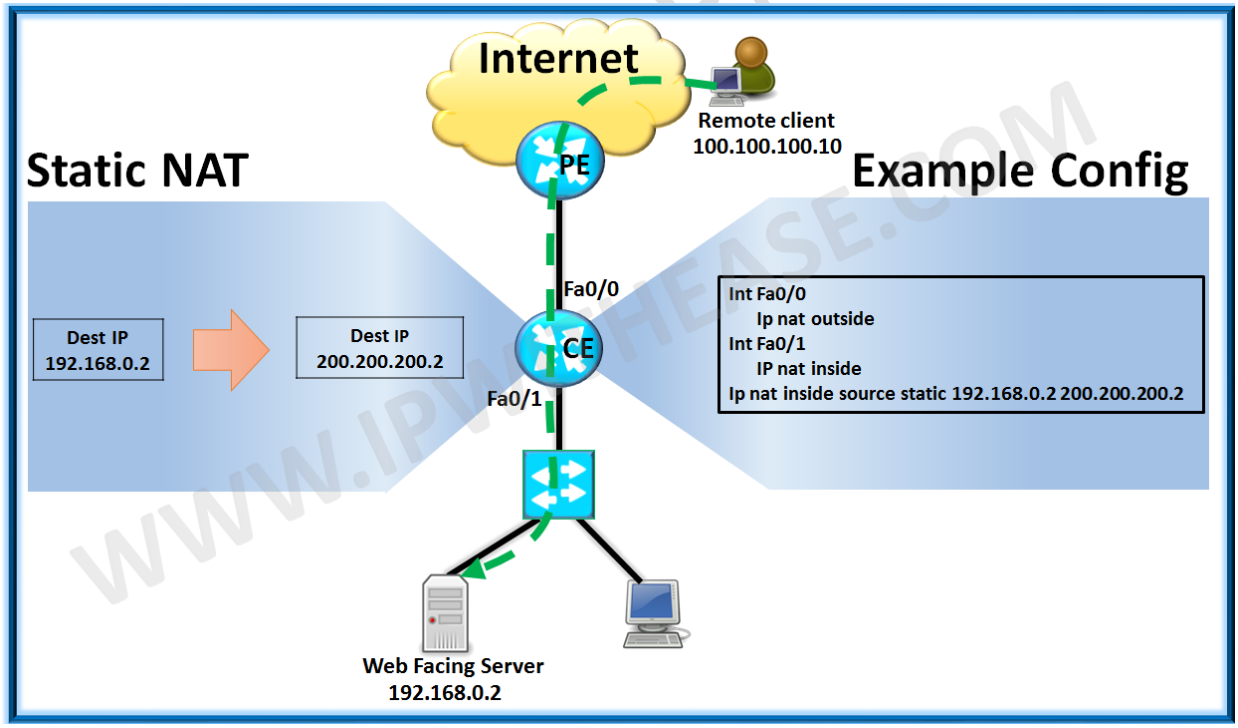
Ques30. What are different types of NAT?

NAT can be divided into below 3 types –

- **Static NAT**
- **Dynamic NAT**
- **NAT Overload (PAT)**

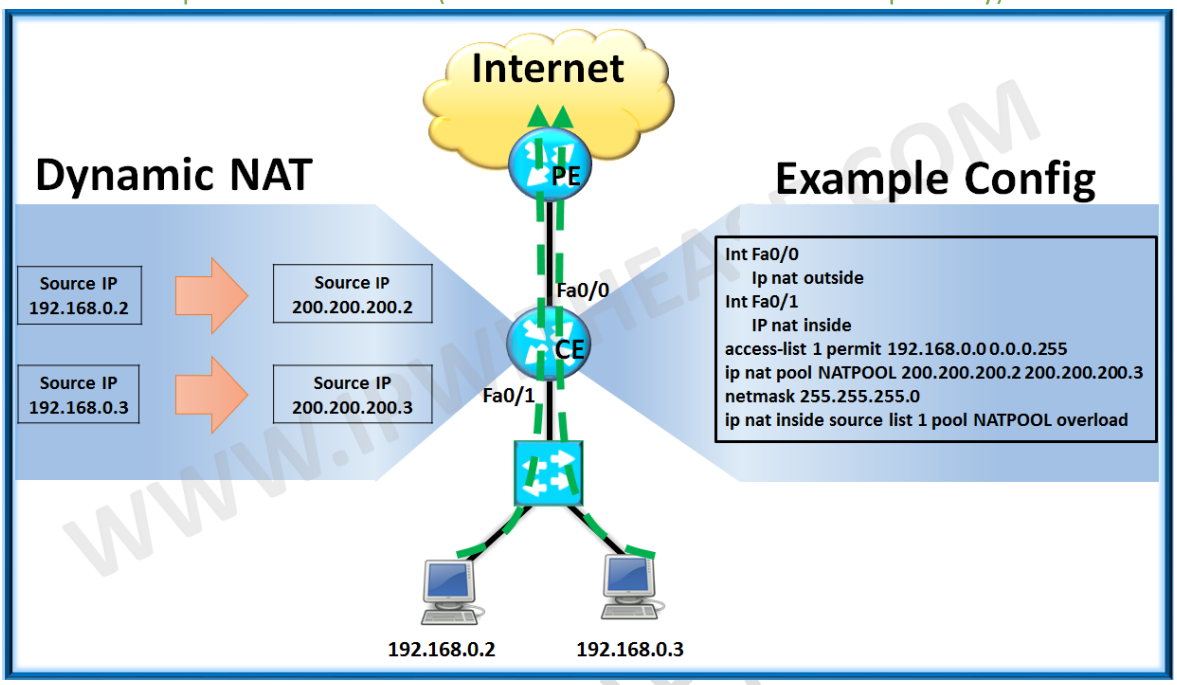
Static NAT (Network Address Translation) is one-to-one mapping of a private IP address to a public IP address. Static NAT is useful when a network device inside a private network needs to be accessible from internet. A common example is Static NAT configured on Router or Firewall for providing access to Web Facing application in LAN for Users who are on Internet. With static NAT, translations remain in the NAT translation table as soon as you configure static NAT command, and they remain in the translation table until static NAT is deleted.

Below scenario shows static NAT configured on Router for giving access to Web Server (Private IP = 192.168.0.2). For outside users, the Web Server IP is 200.200.200.2 which translates to 192.168.0.2 when request from user hits the Router and enters into LAN.



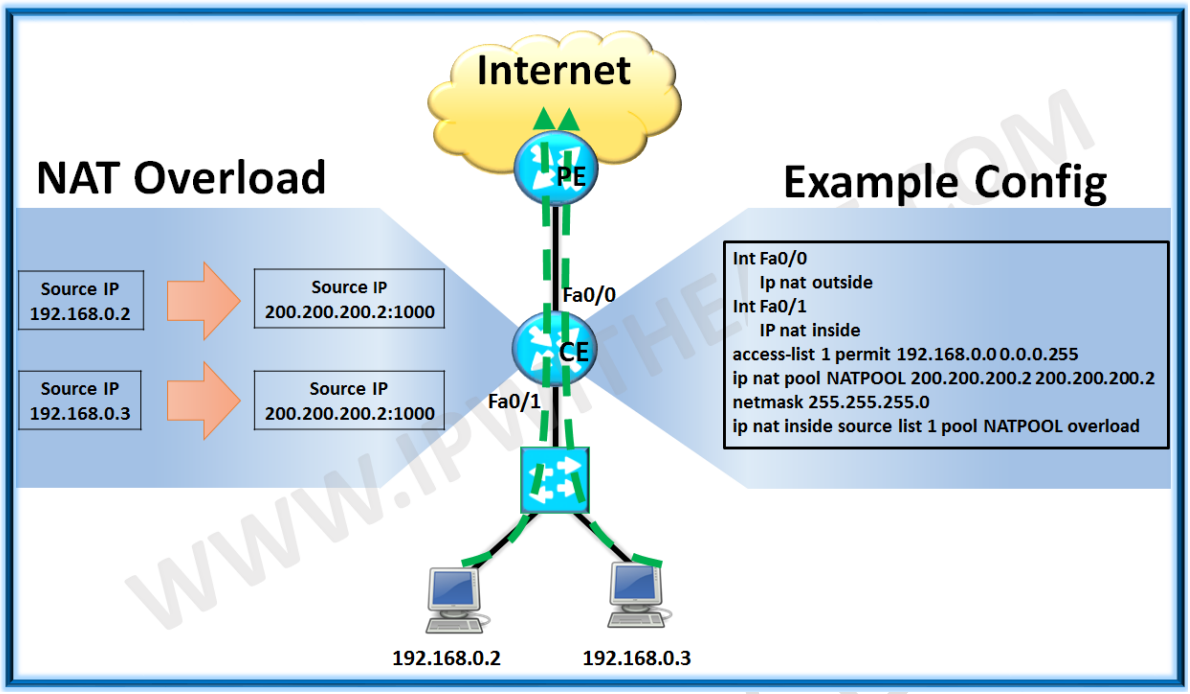
Dynamic NAT is uses the concept of **"POOL"** of public IP addresses that can be assigned internal LAN endpoints dynamically. The NAT router creates a one-to-one mapping between an inside local and inside global address and changes the IP addresses in packets as they exit and enter the inside network. Dynamic NAT can't be used to NAT for servers and devices that need to be accessible from the Internet. With dynamic NAT, translations do not exist in the NAT table until the router receives traffic that requires translation. Dynamic translations have a timeout period after which they are purged from the translation table.

Below scenario shows dynamic NAT configured on Router for giving internet access to hosts (Private IP = 192.168.0.2 and 192.168.0.3). The NAT Router translates private source IP of LAN endpoints into Public IPs (200.200.200.2 and 200.200.200.3 respectively).



NAT Overload is another type of **dynamic NAT** which can map multiple private IP addresses to a single public IP address by using a technology known as Port Address Translation. In this case, multiple internal devices are able to share one public address, as mappings are placed into the mappings table based on the source and destination ports that are used. When using PAT, the router maintains unique source port numbers on the inside global IP address to distinguish between translations.

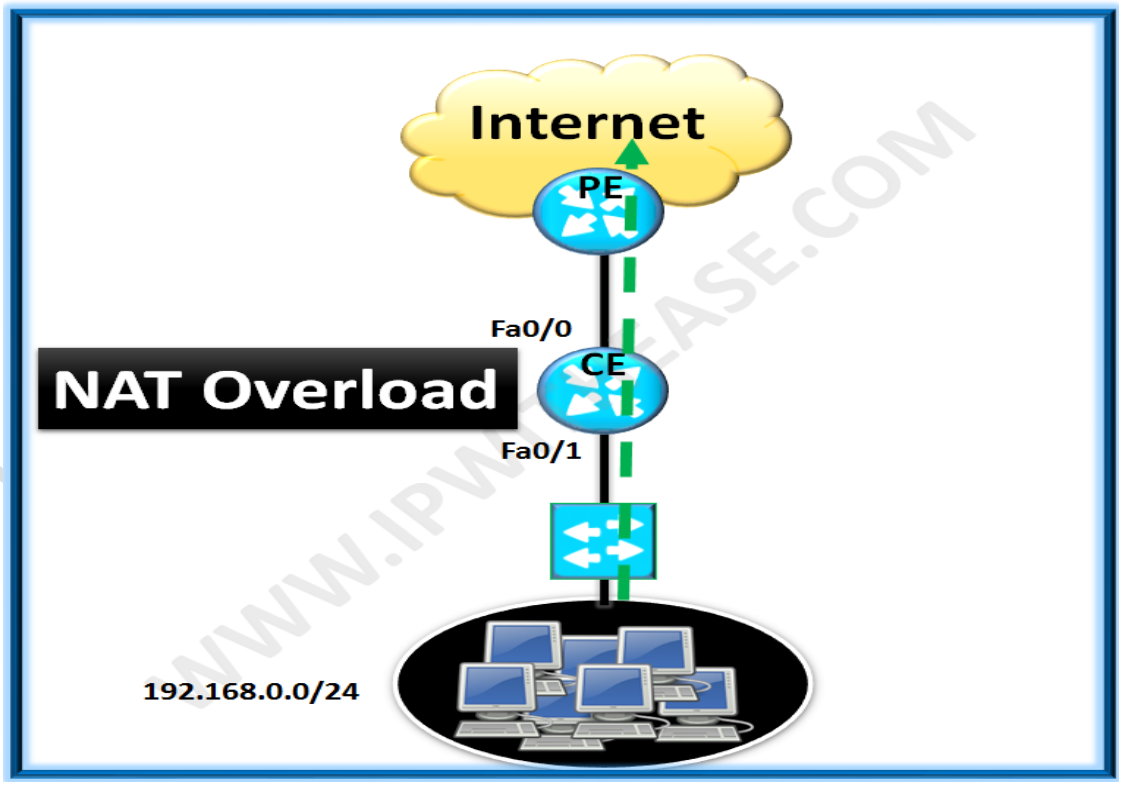
Below scenario shows **NAT Overload (PAT)** configured on Router for giving internet access to multiple inside hosts (Private IP = 192.168.0.2 and 192.168.0.3). The NAT Router translates private source IP of LAN endpoints into same Public IP but with different port number ie 200.200.200.2:1000 and 200.200.200.2:1001 respectively.



Ques31. A Branch Office has 30 LAN users who want to access Internet for browsing. What type of NAT would be required here?

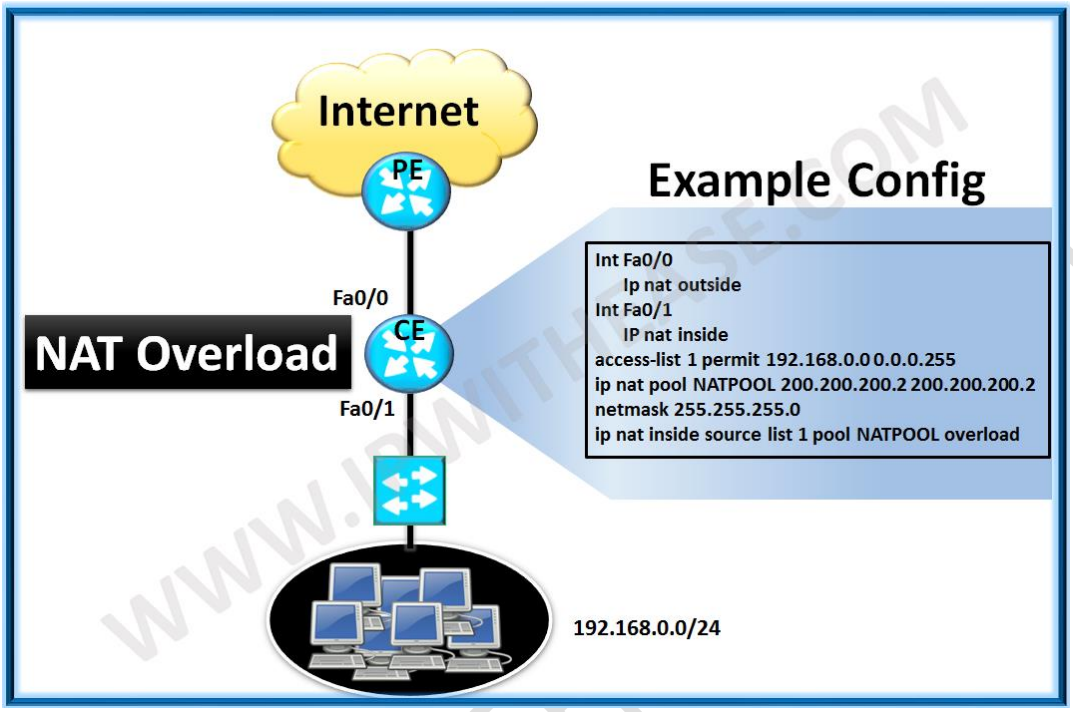
The NAT type suitable for requirement where multiple (30) LAN users need to access Internet for Browsing is **NAT Overload.**

Below is an example scenario on **NAT Overload -**



Ques32. In above question, LAN users belong to subnet 192.168.0.0/24 while Public IP assigned to Internet Router is 202.200.200.10. What will be the router NAT Configuration?

The **NAT Overload** configuration on Cisco Router is shown in attached diagram. For simplicity, a separate Public IP assigned by ISP has been used to perform NAT Overload (PAT) on Internet Router.



Ques33. An Office has an Internet connection and has 1 Web Server which needs to be accessed from Internet. What type of NAT would meet the requirement?

Static NAT will be configured on the NAT device for allowing Web Server to be accessible from Internet.

Ques34. In the above question what detail is required to configure NAT so that the Server is accessible from Internet?

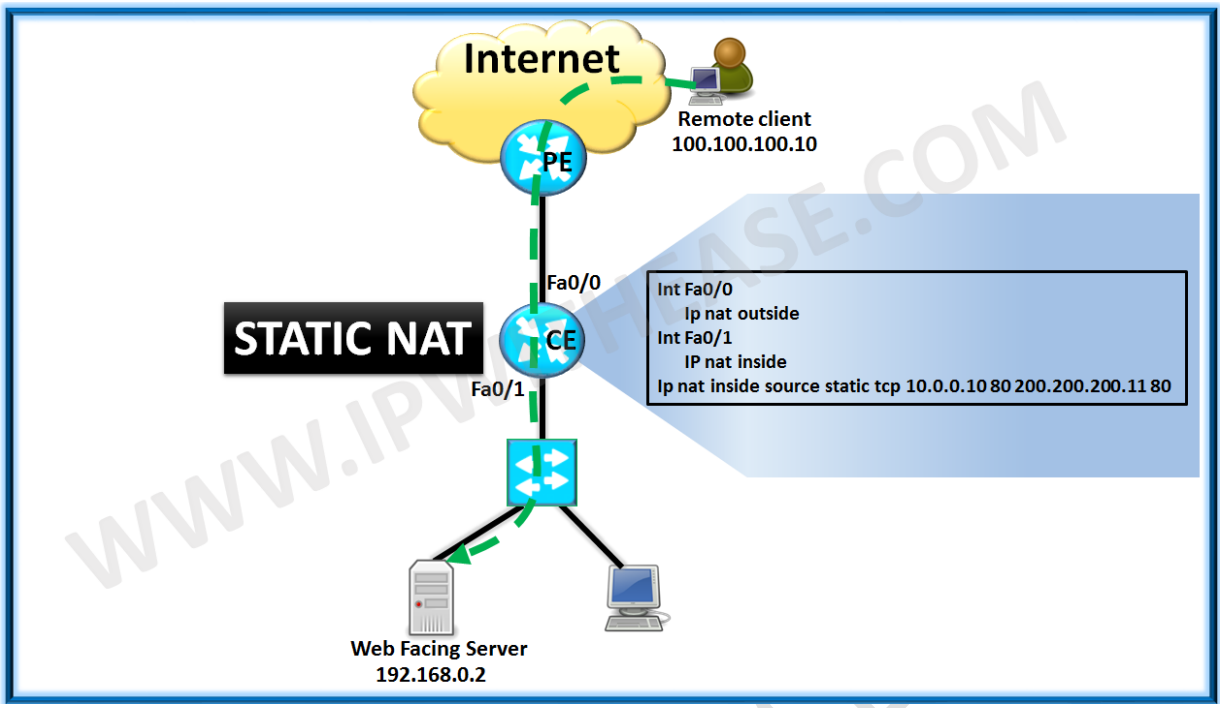
Following detail would be required –

- Inside Local address (Web Server LAN Side address) – This will be the Source address of static NAT
- Inside Global address (Web Server Internet Side address) – This will be Public IP address for accessing Web server from Internet
- TCP/UDP port number of Web Server application.

Ques35. Web Server local IP is 10.0.0.10 and uses TCP port 80. Provider has given Public IP 200.200.200.11. What is the NAT configuration on Internet Router?

Below is the configuration statement –

Interface fa0/0
Ip nat outside
Interface fa0/1
Ip nat inside
ip nat inside source static tcp 10.0.0.10 80 200.200.200.11 80



Ques36. What is difference between NAT and PAT?

Parameter	NAT	PAT
Abbreviation for	Network Address Translation	Port Address Translation
Principle	Public addresses are mapped one-to-one to the private/Inside addresses	Many to One (One real IP to many internal) a single routable address can serve for multiple devices on private network
Change	IP address only changes	IP address and port number changes
Standard	RFC 2766	RFC 2766
Usage	This is commonly used in an organization that wants to give Access to Web Server to the Internet with a single public IP address translating to a single IP address in the private address	This is commonly used on a Device when a corporation/office wants all IP addresses in its internal network to use a single IP address.Eg – Web Browsing

	space. Eg - Web Hosting servers.	

Ques37. Two computers are behind (i.e. Inside LAN) a NAT router. The computers use the router public IP address for sharing internet connection.If a user on the internet pings the public IP address of the router, which device would respond?

In such a scenario the Router will respond considering the fact that NAT Overload (PAT) has been configured with Router Public IP address instead of static NAT with Computer private address.

Ques38. Which NAT command would you place on the interface on a private (Inside LAN) network?

Ip nat inside

Ques39. What is disadvantage of NAT?

- NAT (Network Address Translation) is a processor and memory intensive technology and hence uses key device resources.
- NAT (Network Address Translation) cause loss of end-device to end-device IP traceability
- Some technologies may not function in a NAT (Network Address Translation) configured network.
- Communication over IPsec with NAT enabled may drop packets due to rejection of header changes which are made by NAT.
- Some applications (Like Office 365 and Skype) may use multiple NAT sessions (especially when NAT Overload is configured) and limit the allowed concurrent users. Since NAT Overload (PAT) has limitation of 65535 ports hence maximum sessions cannot go beyond 65535.

Ques40. Where is “ip nat inside” and “ip nat outside” used?

Typically "**ip nat inside**" is configured on the interfaces in our local environment which cannot be routed to the internet (typically private range of IP Addresses) and “**ip nat outside**" we would configure on the interface which is connected to the internet.