**1. Your environment has 25 computers, and you decide to connect this network to the Internet. You would like for all of the computers to have access to the Internet at the same time, but you only have four (4) usable publicly routable IP addresses. What should be configured on the router so that all computers can connect to the Internet simultaneously? (5 points)**

**Answer:** To let all 25 computers go online at the same time using just four public IP addresses, I would set up PAT (Port Address Translation) on the router also called NAT Overload. PAT lets many devices inside the network share a single public IP by giving each connection a different port number. This way, the router knows which reply goes back to which computer. Even with only one or a few public IPs, PAT can support dozens or even hundreds of devices.

**How PAT Works:**

- **Private IPs (inside network):** Computers might use 192.168.1.1 to 192.168.1.25
- **Public IPs (on the router):** Router uses 203.0.113.1 to 203.0.113.4
- **Translation:**
    - For example:
        - 192.168.1.10:5000 → 203.0.113.1:5000
        - 192.168.1.11:6000 → 203.0.113.1:6000

This lets all 25 computers connect using only one public IP thanks to port separation.

**2. What is considered to be the inside host's address before translation? (5 points)**

**Answer:** Before NAT changes the address, the computer's IP is called an inside local address. This is the private IP assigned to the device inside the network. It can't be used on the internet directly and is only used within the local network.

**3. Complete this sentence by filling the blanks: (10 points)**
PAT allows us to use the **__ transport____** layer to identify the hosts, which in turn allows us to theoretically use up to **___ 65536___** hosts with only one real IP address.

**4. True/False? (3 points)**

The NAT pool names are case in-sensitive.

**Answer:** False — NAT pool names are **case-sensitive**. This means Corp and corp would be treated as different names.

**5. When looking at the IP NAT translations, you may see many translations from the same host to the corresponding host at the destination. Describe if this is typical and what does it mean? (10 points)**

**Answer:** Yes, this is typical behavior in a network using NAT. It usually means that a single internal device is communicating with multiple services or making several simultaneous connections to the same destination host.

For example, if one user opens multiple browser tabs or uses different apps that all connect to the internet, each connection will create a separate NAT translation. This happens because NAT tracks each connection using both the source IP and the port number.

So, seeing many translations from the same internal host is normal and just shows that it's actively using the network for multiple connections.

**6. Complete this sentence, by filling the two blanks: (10 points)**
Any outside device's packet destination address that happens to be responding to any inside device is known at the **___inside global_____** address. This means that the initial mapping has to be in held in the **_NAT table__** table, so that all packets arriving from a specific connection get translated consistently.

**7. Describe how does NAT-T work and why you should be concerned about deploying it and when is it useful? (10 points)**

**Answer:** NAT-T is a technique used to make IPSec VPNs work properly when they pass through devices doing NAT. Normally, IPSec encrypts the IP headers including the source and destination IP which prevents NAT from modifying the packet. Because NAT can't read or change encrypted headers, the packets get dropped, and the VPN fails.

NAT-T fixes this by wrapping the encrypted IPSec packet inside a UDP packet, usually using port 4500. This lets the NAT device treat it like a regular packet and forward it correctly, without interfering with the encrypted data. The IPSec packet stays secure and intact.

It's very useful when someone is working remotely like from home or a hotel and needs to connect to a company VPN through a home router or firewall.

**There are reasons to be cautious:**

- NAT-T adds extra processing, which might increase latency a little.
- Not all routers or firewalls support NAT-T correctly, which can cause connection failures.
- Some firewalls may not inspect encapsulated packets properly, creating a security risk.

So while NAT-T is a great solution for secure VPNs over NAT, it needs to be set up and monitored carefully to avoid connectivity or security issues.

**8. Do you think it is possible to build a configuration with both static and dynamic NAT translations? Provide detailed explanation – a simple "yes" or "no" does not suffice. (10 points)**

**Answer:** Yes, it's definitely possible to use both static and dynamic NAT on the same router. Static NAT is typically used when an internal device, like a web or email server, needs to be consistently reachable from outside the network using a fixed public IP address. This is a one-to-one and permanent mapping.

On the other hand, dynamic NAT is used for devices like employee computers or internal printers that need occasional internet access. These devices are assigned public IPs from a pool, but the mapping is temporary and may change with each session.

Using both together helps networks stay flexible. Static NAT ensures critical servers are always reachable with a known IP, while dynamic NAT and PAT lets many users share a limited number of public IPs. Most routers support this mix and use access lists to decide which traffic gets static vs. dynamic NAT treatment.

**9. Explain how PAT handles incoming and outgoing traffic. (10 points)**

**Answer:** Port Address Translation (PAT), also called NAT Overload, manages traffic by assigning unique port numbers to each session. When a device from the internal network sends traffic out to the internet, PAT changes the private IP address to the router's public IP address and attaches a unique port number to it. This helps the router track which internal device started each session.

When responses come back from the internet, PAT checks the destination port number in the packet and uses its NAT table to match it with the correct internal device. It then forwards the traffic back to the right host inside the network.

This system allows many devices to share one public IP address while keeping their sessions separate making PAT very efficient for environments with limited public IPs.

**10. Which layer of the OSI model does PAT operate at? (2 points)**

**Answer:** PAT works at Layer 4. The Transport Layer, because it depends on TCP/UDP port numbers.

**11. Which of the following is a common use case for PAT? (5 points)**

A) Assigning static IP addresses to servers
B) Allowing multiple devices to access the internet using a single public IP address
C) Directly connecting internal devices to external networks
D) Creating virtual private networks (VPNs)

**Answer:** B) Allowing multiple devices to access the internet using a single public IP address.

PAT (Port Address Translation) enables multiple internal hosts to share a single public IP by assigning a unique port number to each session. This is the most common and efficient use of PAT in home, office, and enterprise networks.

**12. Describe the difference between Outside Global and Outside Local Addresses, as used in NAT. Clearly describe as to which address pertains to (10 points).**

**Answer:** The Outside Global Address is the real, public IP address assigned to an external device like a web server — by its own ISP. This is the address that is visible and routable on the public internet.

The Outside Local Address is how that same external device appears from within your private network. Sometimes, it stays the same as the outside global address. But in special cases, like when NAT is translating or mapping for routing purposes, it may temporarily assign a different internal IP for that outside device.

**In short:**

- **Outside Global =** Real public IP of the external device
- **Outside Local =** How your NAT router sees that external IP from the inside

This translation helps your internal network manage sessions and avoid conflicts when working with overlapping networks or VPN tunnels.

**13. If VLSM and NAT did not exist, describe what would be the consequences? (10 points)**

**Answer:** If VLSM and NAT didn't exist, it would be extremely difficult to build efficient and scalable networks using IPv4.

Without NAT, every device needing internet access would require its own public IP address. Since IPv4 only has about 4.3 billion addresses, we would have run out long ago. NAT solves this by letting many private devices share a few public IPs. Without it, businesses and homes couldn't connect large numbers of devices affordably.

Without VLSM (Variable Length Subnet Masking), network administrators would have to use fixed-size subnets, which would waste many IP addresses. For example, a small subnet needing only 10 IPs might be forced to use a whole /24 block (256 IPs). That would quickly exhaust address space, especially in large organizations.

Together, NAT and VLSM help make IPv4 work efficiently. Without them, we'd have run out of IP addresses much sooner, and the move to IPv6 would've been urgent and unavoidable.