A. Answer the following questions about TCP/IP.

1. **What is NAT? How is it used?**

- NAT, or Network Address Translation, is a method of hiding the IP addresses of devices on a private network from the public internet. This is done by translating the private IP addresses into public IP addresses when data is sent to or from the internet.
- NAT is used for a variety of reasons, including:
    - To conserve public IP addresses: There are a limited number of public IP addresses available, and NAT allows multiple devices to share a single public IP address.
    - To improve security: NAT can help to protect a private network from attack by hiding the IP addresses of the devices on the network.
    - To facilitate communication between different networks: NAT can be used to allow devices on different networks to communicate with each other, even if they have different IP address ranges.
- There are two main types of NAT: static NAT and dynamic NAT. Static NAT is used when a specific device on a private network needs to be accessible from the public internet. Dynamic NAT is used when multiple devices on a private network need to be able to access the public internet.
- NAT is a common feature of home routers and is used by many businesses. It is a valuable tool for conserving public IP addresses, improving security, and facilitating communication between different networks.

2. **What is a socket? What is a port? What is port 21 used for? What about port 53?**

- A socket is an endpoint of a communication link between a computer and another computer or a program. A socket is identified by a combination of an IP address and a port number. The IP address identifies the computer, and the port number identifies the specific service that is running on the computer.
- A port is a number that is used to identify a specific service on a computer.
    - Port 21 is used for File Transfer Protocol (FTP). FTP is a standard network protocol used to transfer files between computers over a TCP/IP network. FTP is a client-server protocol, which means that there are two types of participants in an FTP session: a client and a server. The client initiates the connection and requests a file from the server. The server then transfers the file to the client.
    - Port 53 is used for the Domain Name System (DNS). DNS is a distributed database that maps domain names to IP addresses. When you type a domain name into your web browser, your computer sends a request to a DNS server. The DNS server then returns the IP address of the web server that hosts the website you are trying to visit.

3. **How does DNS work? What would happen if we didn’t have DNS?**

- The Domain Name System (DNS) is a hierarchical distributed database that translates human-readable domain names to IP addresses. When you type a domain name into your web browser, your computer sends a request to a DNS server. The DNS server then returns the IP address of the web server that hosts the website you are trying to visit. The DNS system is made up of a number of different servers, each of which is responsible for a different part of the DNS namespace. The root servers are the top-level servers in the DNS hierarchy. They are responsible for mapping top-level domains (TLDs) to their respective authoritative name servers. The authoritative name servers are responsible for mapping domain names to IP addresses. They are typically managed by the organizations that own the domain names. When you type a domain name into your web browser, your computer sends a request to a DNS resolver. The DNS resolver is typically managed by your Internet service provider (ISP). The DNS resolver then forwards the request to a root server. The root server returns the IP address of the authoritative name server for the TLD that you are trying to reach. The DNS resolver then forwards the request to the authoritative name server. The authoritative name server returns the IP address of the web server that hosts the website you are trying to visit. Your computer then connects to the web server and downloads the website.

- If we didn't have DNS, we would have to remember the IP addresses of every website we wanted to visit. This would be very difficult and inconvenient. DNS makes it possible to access websites by typing in their domain names, which is much easier to remember.

4. **What it BootP used for?**

- The Bootstrap Protocol (BOOTP) is a network protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. While some parts of BOOTP have been effectively superseded by the Dynamic Host Configuration Protocol (DHCP), which adds the feature of leases, parts of BOOTP are used to provide service to the DHCP protocol.
- Here are some of the things that BOOTP is used for:
    - To provide IP addresses to devices that do not have their own IP address configuration, such as diskless workstations.
    - To provide configuration information to devices, such as the name of a boot file to load.
    - To provide name resolution services to devices, such as translating hostnames to IP addresses.
    - To provide authentication services to devices, such as verifying that the device is authorized to connect to the network.

5. **What is DHCP? How does it make the network admins life easier?**

- DHCP stands for Dynamic Host Configuration Protocol. It is a protocol that allows network administrators to automatically assign IP addresses and other configuration information to devices on a network. This can save network administrators a lot of time and effort, as they no longer have to manually configure each device on the network.
- DHCP also makes it easier to manage networks, as network administrators can centrally configure DHCP servers and then let the servers automatically assign IP addresses to devices. This can help to prevent conflicts between IP addresses and can make it easier to track and manage devices on the network. Overall, DHCP is a valuable tool for network administrators. It can save time and effort, make it easier to manage networks, and help to prevent problems.

6. **What is a “lease” of a DHCP derived address?**

- A lease of a Dynamic Host Configuration Protocol (DHCP) derived address refers to the period of time that a device is allowed to use a specific IP address assigned by a DHCP server. The lease time for the assigned IP address is also provided by the DHCP server. The device is allowed to use the assigned IP address for the duration of the lease, after which it must renew the lease if it wishes to continue using the same IP address. If the lease expires and the device does not renew it, the DHCP server can reassign the IP address to another device. The lease time for DHCP addresses can vary depending on the network configuration and the DHCP server settings. Typical lease times range from a few hours to several days or even weeks. DHCP leases help ensure efficient use of available IP addresses on a network and also provide a mechanism for automatically reconfiguring devices when changes are made to the network settings.

7. **What is WINS? How does it differ from DNS?**

- WINS (Windows Internet Name Service) and DNS (Domain Name System) are both network services that provide name resolution for computers on a network. However, they differ in the way they map names to network addresses. WINS is a legacy name resolution service used by Microsoft Windows computers to resolve NetBIOS names to IP addresses. NetBIOS (Network Basic Input/Output System) is an early network protocol used by Windows computers to share resources, such as files and printers, over a network. WINS servers maintain a database of NetBIOS name-to-IP address mappings, which can be used by Windows computers to find and communicate with other computers on the network.
- One of the key differences between WINS and DNS is the way they handle name resolution. WINS uses a flat namespace, which means that NetBIOS names must be unique within a network. DNS uses a hierarchical namespace, which allows for the same domain name to be used by multiple organizations, as long as they use different subdomains. Another difference is the protocol used for name resolution. WINS uses the NetBIOS protocol, which is a broadcast-based protocol that can be less efficient than DNS. DNS uses the more efficient and widely used TCP/IP protocol. Overall, WINS is a legacy service that is still used by some older Windows networks, while DNS is the more modern and widely used service for name resolution on both the internet and private networks.

8. **What tools/commands can be used to troubleshoot TCP/IP?**

- There are several tools and commands that can be used to troubleshoot TCP/IP issues. Here are some commonly used ones:
    - Ping: Ping is a command-line tool that sends ICMP (Internet Control Message Protocol) packets to a specified IP address or hostname and measures the response time. It can be used to test basic network connectivity between two devices and to verify that an IP address is valid and reachable.
    - Traceroute/Tracert: Traceroute (Unix/Linux) or Tracert (Windows) is a tool that shows the path that packets take from the local computer to a remote destination. It can be used to diagnose network routing problems, identify network congestion points, and troubleshoot slow network performance.
    - Netstat: Netstat is a command-line tool that displays information about active network connections, open ports, and routing tables. It can be used to check whether a connection is established, identify the source and destination IP addresses and ports, and identify potential network issues.
    - Ipconfig/Ifconfig: Ipconfig (Windows) or Ifconfig (Unix/Linux) is a command-line tool that displays network configuration information, such as the IP address, subnet mask, default gateway, and DNS servers. It can be used to verify that the network configuration is correct and to troubleshoot connectivity issues.
    - Wireshark: Wireshark is a network protocol analyzer that captures and analyzes network traffic in real-time. It can be used to diagnose network issues, identify network bottlenecks, and troubleshoot application-level issues.

- These are just a few of the many tools and commands that can be used to troubleshoot TCP/IP issues. The choice of tool will depend on the specific problem being investigated and the operating system and network environment in use.

9. **How does FTP differ from TFTP?**

- FTP (File Transfer Protocol) and TFTP (Trivial File Transfer Protocol) are both file transfer protocols used to transfer files between computers on a network. However, they differ in several ways:
    - Functionality: FTP is a full-featured protocol that supports file transfers, directory listings, and other operations, while TFTP is a simpler protocol that supports only file transfers.
    - Port numbers: FTP uses port 21 for control connections and port 20 for data connections, while TFTP uses port 69 for both control and data connections.
    - Connection type: FTP uses a connection-oriented approach, which means that a connection is established between the client and server before data is transferred. TFTP uses a connectionless approach, which means that each data packet is sent independently without establishing a connection first.
    - Error handling: FTP has built-in error handling and recovery mechanisms, such as checksums and retransmission of lost packets, while TFTP has limited error handling and no built-in recovery mechanisms.
    - Security: FTP supports authentication and encryption mechanisms, such as SSL/TLS, while TFTP has no built-in security mechanisms.
- Overall, FTP is a more advanced and feature-rich protocol than TFTP, and is generally used for transferring large files or directories. TFTP is a simpler protocol that is often used for booting diskless workstations or transferring firmware updates to network devices.

10. **How many "nodes/hosts" would the following IP v4 addresses support?**

    a. 207.30.155.0
    b.123.56.0.0
    c. 56.0.0.0

- The number of nodes/hosts that an IP address can support depends on the subnet mask used.

    a. 207.30.155.0:

    - The number of nodes that this IP address can support depends on the subnet mask. If the subnet mask is 255.255.255.0 (/24), then the network address is 207.30.155.0 and the host address space is 0-255, which gives a total of 256 possible nodes. However, if a different subnet mask is used, the number of nodes can be different.

    b. 123.56.0.0:

    - Similarly, the number of nodes that this IP address can support depends on the subnet mask used. If the subnet mask is 255.255.0.0 (/16), then the network address is 123.56.0.0 and the host address space is 0-65535, which gives a total of 65,536 possible nodes. However, if a different subnet mask is used, the number of nodes can be different.

    c. 56.0.0.0:

    - Like the previous examples, the number of nodes that this IP address can support depends on the subnet mask. If the subnet mask is 255.0.0.0 (/8), then the network address is 56.0.0.0 and the host address space is 0-16,777,215, which gives a total of over 16 million possible nodes. However, if a different subnet mask is used, the number of nodes can be different.

11. **Based on the following IPv4 addresses list the default subnet mask for each address and the network address and node/host address:**

    a. 201.210.59.87

    - 201.210.59.87 is a Class C address, so the default subnet mask is 255.255.255.0. The network address is 201.210.59.0, and the node/host address space is 0-255.

    b. 56.112.87.191

    - 56.112.87.191 is a Class B address, so the default subnet mask is 255.255.0.0. The network address is 56.112.0.0, and the node/host address space is 0-65535.

    c. 112.158.2.104

    - 112.158.2.104 is a Class A address, so the default subnet mask is 255.0.0.0. The network address is 112.0.0.0, and the node/host address space is 0-16777215.

    d. 192.158.75.89

    - 192.158.75.89 is a Class C address, so the default subnet mask is 255.255.255.0. The network address is 192.158.75.0, and the node/host address space is 0-255.

    e. 228.195.128.241

    - 228.195.128.241 is a Class D address, which is reserved for multicasting, so it doesn't have a subnet mask or a network or node address space.

12. **What are the following IPv4 addresses used for?**

    a. 127.0.0.1

    - 127.0.0.1 is a special IPv4 address that is reserved for the loopback interface of a device. When this address is used as a destination address, the packet is looped back to the device without being sent over the network. This address is commonly used for testing network applications and for troubleshooting connectivity issues.

    b. 255.255.255.255

    - 255.255.255.255 is a special IPv4 address that is used as the broadcast address for a network. When a packet is sent to this address, it is broadcast to all devices on the network. This address is commonly used by DHCP servers to provide IP addresses to devices on a network.

    c. 244.122.89.3

    - 244.122.89.3 is an invalid IPv4 address. The first octet of an IPv4 address can range from 0 to 255, so an address with a value of 244 in the first octet is not valid.

    d. 127.255.255.255

    - 127.255.255.255 is also an invalid IPv4 address. The loopback address range is from 127.0.0.0 to 127.255.255.255, but 127.255.255.255 is not a valid address within this range.

13. **Convert the following IPv4 addresses to Binary.**

    a. 89.112.45.3

    89 = 01011001
    112 = 01110000

45 = 00101101

3 = 00000011

- The binary representation of 89.112.45.3 is: 01011001.01110000.00101101.00000011

b.158.89.112.101

158 = 10011110

89 = 01011001

112 = 01110000

101 = 01100101

- The binary representation of 158.89.112.101 is: 10011110.01011001.01110000.01100101

c. 189.56.147.125

189 = 10111101

56 = 00111000

147 = 10010011

125 = 01111101

- The binary representation of 189.56.147.125 is: 10111101.00111000.10010011.01111101

d. 10.251.178.238

10 = 00001010

251 = 11111011

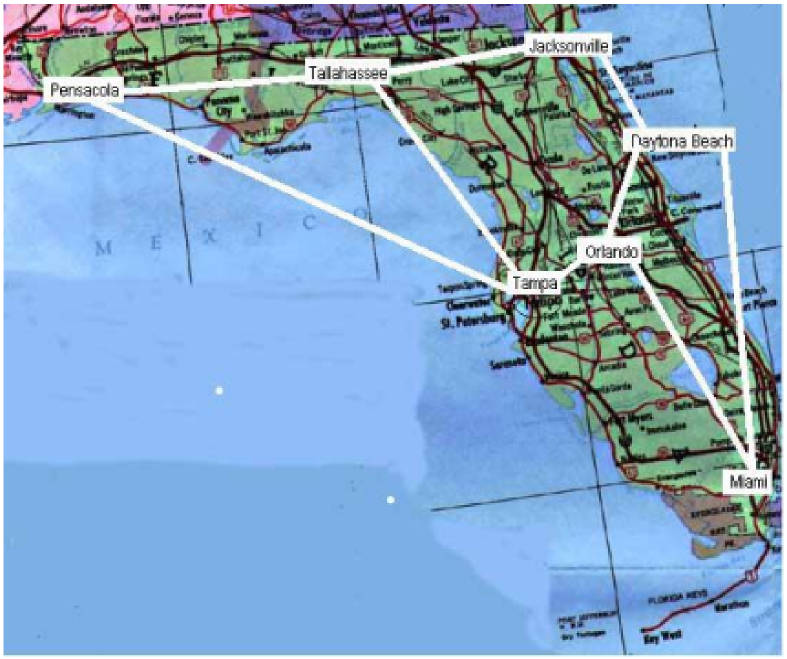
178 = 10110010

238 = 11101110

- The binary representation of 10.251.178.238 is: 00001010.11111011.10110010.11101110

B. Network Design using IPv4 Addressing

1. If you were tasked with setting up a geographic network and you needed at least 7 network addresses and had an IP network address of 190.152.0.0 what would you do? Assign valid IP addresses to the following sub-networks for each city, with the appropriate subnet mask:



a. Pensacola
Network address = 190.152.0.0
Host range = 190.152.0.1 -- 190.152.31.254
Subnet mask = 255.255.224.0

b. Tallahassee
Network address = 190.152.32.0
Host range = 190.152.32.1 -- 190.152.63.254
Subnet mask = 255.255.224.0

c. Jacksonville
Network address = 190.152.64.0
Host range = 190.152.64.1 -- 190.152.95.254
Subnet mask = 255.255.224.0

d. Daytona Beach
Network address = 190.152.96.0
Host range = 190.152.96.1 -- 190.152.127.254
Subnet mask = 255.255.224.0

e. Orlando
Network address = 190.152.128.0
Host range = 190.152.128.1 -- 190.152.159.254
Subnet mask = 255.255.224.0

f. Tampa
Network address = 190.152.160.0
Host range = 190.152.160.1 -- 190.152.191.254
Subnet mask = 255.255.224.0

g. Miami
Network address = 190.152.192.0
Host range = 190.152.192.1 -- 190.152.223.254
Subnet mask = 255.255.224.0

Problems:

1. Convert the following IPv6 addresses into their full length:

a. 1522:8765:21::/48

- 1522:8765:0021:0000:0000:0000:0000:0000/48

b. 1789:1011:0::/64

- 1789:1011:0000:0000:0000:0000:0000:0000/64

c. FE80::0202:B3FF:FE1E:8329/56

- FE80:0000:0000:0000:0202:B3FF:FE1E:8329/56

d. ::/128

- 0000:0000:0000:0000:0000:0000:0000:0000/128

e. 2002:64C8:64C8::/64

- 2002:64C8:64C8:0000:0000:0000:0000:0000/64

f. 2001:cdba::3257:9652

- 2001:CDBA:0000:0000:0000:0000:3257:9652

2. Convert the following IPv6 addresses into their compressed format:

a. FE80:0000:0000:0000:0202:B3FF:FE1E:8329

- FE80::202:B3FF:FE1E:8329

b. 2001:0db8:85a3:0000:0000:8a2e:0370:7334

- 2001:db8:85a3::8a2e:370:7334

c. 2041:0000:130F:0000:0000:07CO:853A:140B

- 2041:0:130F::7C0:853A:140B

d. 2001:cdba:0000:0000:0000:0000:3257:9652

- 2001:cdba::3257:9652

e. Fe80:0:0:0:200:f8ff:fe21:67cf

- FE80::200:F8FF:FE21:67CF

f. 2001:0000:3238:DFE1:0063:0000:0000:FEFB

- 2001:0:3238:DFE1:63::FEFB