Revision questions

1.Which of the following is a public IP address?

a.126.56.23.0

b.172.16.0.1

c.10.4.2.89

d.172.30.45.23

2.What is the decimal representation of the binary number 1101010?

a.101

b.206

c.106

d.201

3.The last IP address in a network range is known as a what?

a.APIPA

b.Network address

c.Broadcast address

d.Private address

4.If you need a network with at least 256 hosts on it, how many bits would you need for the host element?

a.8

b.9

c.10

d.11

5.What protocol is used to issue an IP address automatically?

a.APIPA

b.DHCP

c.ARP

d.DNS

6.Which of these is a Class B private IP address?

a.10.0.0.1

b.192.168.34.2

c.10.234.56.1

d.172.16.9.90

7.Which of these is not a valid subnet mask?

a.255.124.0.0

b.255.255.128.0

c.255.255.255.192

d.255.255.255.249

8.You wish to add a new host to a network. One of the hosts that's currently on the network has an IP address of 187.34.23.6 and a subnet mask of 255.255.255.240. Which of the following IP addresses can I allocate to the new host?

a.187.34.23.0

b.187.34.23.6

c.187.34.23.14

d.187.34.23.15

Practical:

7.**Explain the following topics:**

What is an IP address?

An **IP address** (Internet Protocol address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main functions:

1. **Identifying a host or network interface**: Every device on the internet has a unique IP address that allows it to be identified and located.
2. **Providing a location**: It specifies where a device is located in the network so that data can be routed correctly.

Explain the difference between an ipv4 and ipv6

Address Format:

- **IPv4**: Uses a 32-bit address scheme, allowing for around 4.3 billion unique addresses. It is usually represented as four decimal numbers separated by periods (e.g., 192.168.1.1).
- **IPv6**: Uses a 128-bit address scheme, allowing for a vastly larger number of addresses (approximately 3.4×10383.4 \times 10^{38}3.4×1038). It is written as eight groups of four hexadecimal digits, separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Address Space:

- **IPv4**: Limited address space, leading to the use of technologies like NAT (Network Address Translation) to mitigate exhaustion.
- **IPv6**: Expands the address space significantly, making exhaustion much less of a concern.

Header Complexity:

- **IPv4**: Has a simpler header format but needs additional features (like NAT) to support modern internet needs.
- **IPv6**: The header is more complex but designed to improve routing and eliminate the need for NAT.

Security:

- **IPv4**: Security features like IPsec are optional.
- **IPv6**: Has built-in security protocols, like mandatory support for IPsec, improving end-to-end encryption.

Transition:

- **IPv4**: Widely used, but addresses are running out.
- **IPv6**: Created to replace IPv4 and address scalability issues, though adoption is still ongoing.

What is a MAC address?

•How does a Mac address get stored?

•How do you keep this info secure?

A **MAC (Media Access Control) address** is a unique identifier assigned to a network interface card (NIC) for communication on the physical network segment. It operates at the **data link layer** of the OSI model and is typically represented as six groups of two hexadecimal digits, separated by colons or hyphens (e.g., 00:1A:2B:3C:4D:5E).

How is a MAC Address Stored?

A MAC address is **burned into the hardware** of a network device, such as a network interface card (NIC), during manufacturing. It is stored in the device's **firmware**, specifically in the NIC's read-only memory (ROM) or another non-volatile storage medium.

How Do You Keep MAC Address Info Secure?

MAC addresses themselves are not inherently secure, as they can be:

- **Spoofed**: An attacker can alter their device's MAC address to impersonate another device.
- **Tracked**: Since a MAC address is unique, it can be used to track a device across different networks.

To enhance security, consider these measures:

1. **MAC Filtering**: Networks can be configured to allow or deny devices based on their MAC addresses, although this can be bypassed through spoofing.
2. **Encryption**: Secure wireless networks with encryption (e.g., WPA3) to prevent unauthorized access.

8.Setup the following using packet tracer:

2 servers

4 switches

8pcs per switch

You must connect bot servers to a router so ping is possible

You must link the router with the cloud

Network Design Overview

1. **Servers**: There are two servers that need to be connected to the network and communicate with each other. They will also need access to the router for internet/cloud connectivity.
2. **Switches**: Each of the 4 switches will connect to 8 PCs (for a total of 32 PCs). The switches will need to be interconnected or connected to a central point for communication across all network devices.
3. **Router**: The router will be the central point to connect all network devices and the servers. The router will also connect to the cloud (typically represented as the Internet).
4. **Cloud**: The cloud will represent the external network or Internet that the router connects to for external communication.

Step-by-Step Design

1. **Connect the PCs to the switches**:
    - Each switch has 8 PCs, so for each switch, connect the 8 PCs directly using Ethernet cables.
2. **Connect the switches to each other**:
    - To enable communication between the PCs on different switches, interconnect the switches. You can do this in several ways:
        - **Star topology**: Connect each switch to the router directly.
        - **Daisy chain**: Connect switch 1 to switch 2, switch 2 to switch 3, and so on. However, this introduces bottlenecks and is not as efficient as a star or hierarchical design.
3. **Connect the servers to the router**:
    - Both servers should be connected directly to the router to allow them to communicate with each other and also access the cloud.

- You can also connect the servers to a switch first, which then connects to the router, but direct connection to the router is preferred for minimizing latency and ensuring reliable communication.

4. **Connect the switches to the router**:
    - To ensure the switches (and the PCs connected to them) can communicate with the servers and the cloud, each switch must be connected to the router.
    - This can be done by connecting the uplink port of each switch to available ports on the router.
5. **Connect the router to the cloud**:
    - The router will have a WAN port that can be connected to the cloud (which represents the Internet or external network).