American International University-Bangladesh (AIUB)

Course: Computer Networks

Faculty Name: Md. Hasibul Islam

Student Name: Shanto Kumar Basak

ID: 20-42945-1

Submitted Date: 23th March 2023

1.

Interconnecting devices are hardware components that allow different devices and networks to communicate and exchange data with each other. These devices are used to link different segments of a network and ensure that information flows smoothly between them.

Some examples of interconnecting devices include:

1. Hubs: A hub is a basic interconnecting device that connects multiple devices to form a single network segment. All data received on one port of a hub is transmitted to all other ports.
2. Switches: A switch is a more advanced interconnecting device that connects multiple devices and segments of a network. Unlike hubs, switches transmit data only to the intended recipient, making communication more efficient.
3. Routers: A router is an interconnecting device that connects multiple networks together. Routers analyze incoming data packets and determine the best path for the data to travel to reach its destination.
4. Bridges: A bridge is an interconnecting device that connects two different network segments together. Bridges work at the data link layer of the OSI model and can filter traffic to improve network performance.

These interconnecting devices are critical components of modern computer networks, enabling communication and data exchange between devices and networks that would otherwise be isolated from each other.

2.

Switches are network devices that operate at the data link layer (Layer 2) of the OSI model. They are designed to connect multiple devices within a network and facilitate the communication between these devices.

Switches work by using the Media Access Control (MAC) addresses of devices to determine where to send data packets. When a switch receives a data packet, it reads the MAC address of the source device and the destination device. It then looks up the MAC address table to determine the port that the destination device is connected to. If the switch already has the MAC address of the destination device in its table, it forwards the data packet only to the port that the destination device is connected to. If the MAC address of the destination device is not in the table, the switch broadcasts the data packet to all ports except the one it received the packet from, in order to learn the MAC address of the destination device.

Switches use a process called switching, where they create virtual circuits between the source and destination devices. This process allows switches to transmit data packets only to the intended recipient, reducing network traffic and improving performance.

In addition to basic switching, modern switches also support advanced features such as VLANs (Virtual Local Area Networks), QoS (Quality of Service) prioritization, and Link Aggregation Control Protocol (LACP) for combining multiple physical links into a single logical link.

3.

A router is a network device that operates at the network layer (Layer 3) of the OSI model. Routers are designed to connect multiple networks together and facilitate the communication between these networks.

Routers work by using the Internet Protocol (IP) addresses of devices to determine where to send data packets. When a router receives a data packet, it reads the IP address of the source device and the destination device. It then uses a routing table to determine the best path for the data packet to reach its destination.

The routing table contains information about the network topology, including the IP addresses of other routers and the networks they are connected to. The router uses this information to find the next hop on the path to the destination network.

If the router does not have a specific entry in its routing table for the destination IP address, it sends the data packet to its default gateway, which is another router that is responsible for forwarding data packets to destinations outside of the local network.

Routers also perform a process called packet forwarding, where they transmit data packets between networks. This process involves encapsulating the data packet in a new header with information about the next hop router and forwarding the packet to that router. This process continues until the packet reaches its final destination.

In addition to basic routing, modern routers also support advanced features such as Network Address Translation (NAT), Access Control Lists (ACLs), and Virtual Private Network (VPN) capabilities, which allow remote users to securely connect to a network.

4.

There are several types of connections that can be used between different devices in a network. The most common types of connections include:

1. Ethernet: Ethernet is a wired networking technology that uses twisted pair or fiber optic cables to transmit data between devices. Ethernet is a widely used technology for connecting computers, routers, switches, and other networking devices.
2. Wi-Fi: Wi-Fi is a wireless networking technology that uses radio waves to transmit data between devices. Wi-Fi is commonly used for connecting laptops, smartphones, tablets, and other mobile devices to a network.
3. Bluetooth: Bluetooth is a wireless technology that is used to connect devices over short distances. It is commonly used for connecting smartphones to wireless headphones, for example.
4. USB: USB (Universal Serial Bus) is a wired connection that is commonly used for connecting devices such as printers, external hard drives, and smartphones to a computer.
5. HDMI: HDMI (High-Definition Multimedia Interface) is a wired connection that is used to transmit high-definition video and audio between devices such as computers, televisions, and game consoles.
6. FireWire: FireWire is a wired connection that is used for high-speed data transfer between devices such as cameras, external hard drives, and audio interfaces.

The choice of connection type depends on factors such as the devices being connected, the distance between them, the speed and reliability required, and the available infrastructure.

5.

Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to automatically assign IP addresses and other network configuration parameters to devices on a network.

DHCP works as follows:

1. When a device connects to a network, it sends a DHCP request message to the network asking for an IP address.
2. A DHCP server on the network receives the request and checks its pool of available IP addresses. If an address is available, the server assigns it to the device and sends a DHCP offer message back to the device.
3. The device receives the DHCP offer message and sends a DHCP request message back to the server, indicating that it accepts the offered IP address.

4. The DHCP server sends a DHCP acknowledgment message back to the device, confirming that the IP address has been assigned.

In addition to IP addresses, DHCP can also assign other network configuration parameters such as subnet masks, default gateways, and DNS server addresses.

DHCP is a useful protocol for managing IP addresses in large networks, as it automates the process of assigning IP addresses and reduces the risk of IP address conflicts. DHCP also allows network administrators to easily manage and change IP addresses and other network configuration parameters on a large scale.

6.

A broadcast domain and a collision domain are two important concepts in computer networking.

A broadcast domain is a logical division of a computer network where all devices can receive broadcast messages from each other. A broadcast message is a network packet that is sent to all devices on a network, regardless of whether they are the intended recipient or not. A broadcast domain is typically defined by a single network switch or router. Devices that are connected to the same switch or router are part of the same broadcast domain and can communicate with each other using broadcast messages.

A collision domain, on the other hand, is a logical division of a network where network packets can potentially collide with each other. A collision occurs when two or more devices on a network transmit data at the same time, resulting in data corruption and transmission errors. In Ethernet networks, collisions occur when multiple devices share the same physical network segment (such as a hub or repeater). A collision domain is typically defined by a single network segment. Devices that are connected to the same network segment are part of the same collision domain and must contend with each other for access to the network.

In modern networks, the use of switches and full-duplex Ethernet has largely eliminated the need for collision domains, as switches can provide dedicated, point-to-point connections between devices. However, broadcast domains remain an important concept in network design and management, as they can affect network performance and security.

7.

The Domain Name System (DNS) is a network protocol that is used to translate domain names into IP addresses (such as 203.0.113.1) that can be used to locate and communicate with network resources.

DNS works as follows:

1. When a user enters a domain name into a web browser or other application, the application sends a DNS query to a DNS resolver (also known as a DNS recursive resolver) that is configured on the user's device or network.
2. The DNS resolver checks its cache to see if it has a record of the IP address associated with the domain name. If it does, it returns the IP address to the application and the query is complete.
3. If the DNS resolver does not have a record of the IP address, it sends a DNS query to a DNS root server, which is the first stop in a chain of DNS servers that can help resolve the query.
4. The DNS root server responds to the DNS resolver with a referral to a top-level domain (TLD) server that is responsible for the TLD associated with the domain name in the query (such as .com or .org).
5. The DNS resolver sends a query to the TLD server, which responds with a referral to a domain name server (DNS) that is authoritative for the domain name in the query.
6. The DNS resolver sends a query to the authoritative DNS server, which responds with the IP address associated with the domain name in the query.
7. The DNS resolver caches the IP address and returns it to the application that made the original DNS query.

The DNS protocol is hierarchical and distributed, which means that there are many DNS servers around the world that work together to translate domain names into IP addresses. DNS plays a critical role in the functioning of the internet, as it enables users to easily locate and communicate with resources on the network without having to remember complex IP addresses.

8.

You have been given a network with the IP address 192.168.10.0/24. You need to divide this network into subnets to accommodate the following requirements:

- Subnet A: 60 hosts
- Subnet B: 40 hosts
- Subnet C: 20 hosts
- Subnet D: 10 hosts

Using VLSM, you need to calculate the appropriate subnet masks and network addresses for each subnet.

To solve this problem using VLSM, you should start by identifying the largest subnet requirement, which is Subnet A with 60 hosts. This requires a subnet mask that can accommodate at least 64 hosts (2^6 - 2 = 62 hosts). A /26 subnet mask (255.255.255.192) would be appropriate for this subnet, as it provides 62 usable IP addresses.

The next largest subnet requirement is Subnet B with 40 hosts. This requires a subnet mask that can accommodate at least 44 hosts (2^6 - 2 = 62 hosts). A /26 subnet mask (255.255.255.192) would be too large for this subnet, as it would provide 62 usable IP addresses. Instead, a /27 subnet mask (255.255.255.224) would be appropriate, as it provides 30 usable IP addresses.

Subnet C requires 20 hosts, which requires a subnet mask that can accommodate at least 22 hosts (2^5 - 2 = 30 hosts). A /27 subnet mask (255.255.255.224) would be too large for this subnet, as it would provide 30 usable IP addresses. Instead, a /28 subnet mask (255.255.255.240) would be appropriate, as it provides 14 usable IP addresses.

Finally, Subnet D requires 10 hosts, which requires a subnet mask that can accommodate at least 14 hosts (2^4 - 2 = 14 hosts). A /28 subnet mask (255.255.255.240) would be too large for this subnet, as it would provide 14 usable IP addresses. Instead, a /29 subnet mask (255.255.255.248) would be appropriate, as it provides 6 usable IP addresses.

Here's a summary of the subnet information:

Subnet A: 192.168.10.0/26 Subnet B: 192.168.10.64/27 Subnet C: 192.168.10.96/28 Subnet D: 192.168.10.112/29

You can now assign IP addresses to devices within each subnet using the appropriate network addresses and subnet masks.

9.

The ARP (Address Resolution Protocol) cache is an important component of network communication. It is used to maintain a mapping of IP addresses to MAC addresses in a local network segment. When a device wants to communicate with another device on the same network, it needs to know the MAC address of the target device in order to send data to it. The ARP cache stores this information, so that the device doesn't have to perform an ARP request every time it wants to communicate with another device.

Here are some reasons why the ARP cache is important:

1. Faster network communication: Without the ARP cache, every time a device wants to communicate with another device on the same network segment, it would have to send out an ARP request to find the MAC address of the target device. This can slow down network

communication, as it adds extra overhead to every communication. The ARP cache stores this information, so that devices can communicate more efficiently without having to perform an ARP request every time.

2. Reduced network traffic: By caching the ARP information, the network traffic is reduced. Without the ARP cache, every device would have to send an ARP request to find the MAC address of the target device, leading to unnecessary traffic on the network.

3. Security: The ARP cache can help protect against ARP spoofing attacks, which involve an attacker sending false ARP messages to associate their MAC address with the IP address of another device on the network. By caching the ARP information, the device can verify the MAC address of the target device before sending data to it, which can help prevent ARP spoofing attacks.

4. Troubleshooting: The ARP cache can also be used for troubleshooting network connectivity issues. If a device is unable to communicate with another device on the same network segment, checking the ARP cache can help determine if the device has the correct MAC address for the target device.

In summary, the ARP cache is an important component of network communication, as it helps to maintain a mapping of IP addresses to MAC addresses in a local network segment, improving network efficiency, security, and troubleshooting capabilities.