Sessional Assignment 2020

Subject: Advance Computer Networks (MS EE)

Submitted to : Sir Naeem Ahmed Jan

Name: Muhammad Fawad Khan

ID: 15605

Iqra national university Peshawar

Q1: Differentiate between a Hub, Switch and Router?

Hub

A hub is to sent out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore, all the computers can receive the message and computers themselves need to decide whether to accept the message.

Switch

A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.

Router

Router is actually a small computer that can be programmed to handle and route the network traffic. It usually connects at least two networks together, such as two LANs, two WANs or a LAN and its ISP network. Routers can calculate the best route for sending data and communicate with each other by protocols.

Hub Vs. Switch

A hub works on the physical layer (Layer 1) of OSI model while Switch works on the data link layer (Layer 2). Switch is more efficient than the hub. A switch can join multiple computers within one LAN, and a hub just connects multiple Ethernet devices together as a single segment. Switch is smarter than hub to determine the target of the forwarding data. Since switch has a higher performance, its cost will also become more expensive.

Switch Vs. Router

In the OSI model, router is working on a higher level of network layer (Layer 3) than switch. Router is very different from the switch because it is for routing packet to other networks. It is also more intelligent and sophisticated to serve as an intermediate destination to connect multiple area networks together. A switch is only used for wired network, yet a router can also link with the wireless network. With much more functions, a router definitely costs higher than a switch.

Hub Vs. Router

As mentioned above, a hub only contains the basic function of a switch. Hence, differences between hub and router are even bigger. For instance, hub is a passive device without software while router is a networking device, and data transmission form in hub is in electrical signal or bits while in router it is in form of packet.

………………………………………………………………………………………………………

Q2: What does a backbone network means?

A backbone or core is a part of computer network that interconnects various pieces of network, providing a path for the exchange of information between different LANs or sub networks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than the networks connected to it .

A large corporation that has many locations may have a backbone network that ties all of the locations together, for example, if a server cluster needs to be accessed by different departments of a company that are located at different geographical locations. The pieces of the network connections (for example: Ethernet, wireless) that bring these departments together is often mentioned as network backbone. Network congestion is often taken into consideration while designing backbones.

One example of a backbone network is the Internet backbone.

………………………………………………………………………………………………………

Q3: Explain the protocols used at different TCP/IP layers?

TCP/IP functionality is divided into four layers, each of which include specific protocols:

The application layer provides applications with standardized data exchange. Its protocols include the HTTP, FTP, Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). At the application layer, the payload is the actual application data.

- HTTP (hypertext transfer protocol) -This is the workhorse of the Web.
- SMTP,POP3,IMap4 – These are email protocols

The transport layer is responsible for maintaining end-to-end communications across the network. TCP handles communications between hosts and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes.

- UDP (used datagram protocol) is connection less protocol and doesn't guarantee delivery.

The network layer also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

- IP (Internet Protocol) – This is the main networking protocol. There are two version of IP (IPv4 and IPV6).

The physical layer, also known as the network interface layer or data link layer, consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this lowest layer include Ethernet for local area networks (LANs) and the Address Resolution Protocol (ARP).

- ARP (address resolution Protocol) -Translates an IP address to a MAC or physical address.(IP4 networks)

…………………………………………………………………………………………………

Q4: What is anonymous FTP?

Anonymous File Transfer Protocol (FTP) allows the public to log into an FTP server with a common login (usually "ftp" or "anonymous") and any password (usually the person's e-mail address) to access the files on the server.

Anonymous FTP is beneficial for the distribution of large files to the public, without having to assign large numbers of login and password combinations for FTP access.

For security purposes, Network Solutions does not support Anonymous FTP.

Anonymous FTP is called anonymous because you don't need to identify yourself before accessing files. In general, you enter the word anonymous or ftp when the host prompts you for a username; you can enter anything for the password, such as your e-mail address or simply the word "guest". In many cases, when you access an anonymous FTP site, you won't even be prompted for your name and password.

You can use the Archie system to obtain a list of anonymous FTP sites and files available on each site.

Many FTP sites are protected. Unlike anonymous FTP sites, these restricted FTP sites can only be accessed by individuals who enter a valid username and password.

……………………………………………………………………………………………………....

Q5: What is subnet mask?

A sub network or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.

Computers that belong to a subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields, the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The IPv6 address specification 2001:db8::/32 is a large address block with 2^{96} addresses, having a 32-bit routing prefix.

For IPv4, a network may also be characterized by its subnet mask or net mask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

Traffic is exchanged between sub networks through routers when the routing prefixes of the source address and the destination address differ. A router serves as a logical or physical boundary between the subnets.

The benefits of subnetting an existing network vary with each deployment scenario. In the address allocation architecture of the Internet using CIDR and in large organizations, it is necessary to allocate address space efficiently. Subnetting may also enhance routing efficiency, or have advantages in network management when sub networks are administratively controlled by different entities in a larger organization. Subnets may be arranged logically in a hierarchical architecture, partitioning an organization's network address space into a tree-like routing structure.

……………………………………………………………………………………………………

Q6: What is NAT?

Network address translation (**NAT**) is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device. The technique was originally used to avoid the need to assign a new address to every host when a network was moved, or when the upstream Internet service provider was replaced, but could not route the networks address space. It has become a popular and essential tool in conserving global address space in the face of IPv4 address exhaustion. One Internet-routable IP address of a NAT gateway can be used for an entire private network.

……………………………………………………………………………………………………

Q7: Differentiate between TCP and UDP?

TRANSMISSION CONTROL PROTOCOL	**USER DATAGRAM PROTOCOL**
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).

TCP has a (20-80) bytes variable length header.	UDP has a 8 bytes fixed length header.
TCP is heavy-weight.	UDP is lightweight.
TCP doesn’t supports Broadcasting.	UDP supports Broadcasting.
TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

…………………………………………………………………………………………………

Q8: What is RIP and its key features?

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

Features of RIP :

- Updates of the network are exchanged periodically.
- Updates (routing information) are always broadcast.
- Full routing tables are sent in updates.
- Routers always trust on routing information received from neighbor routers. This is also known as routing on rumours.

…………………………………………………………………………………………………

Q9: Explain what is a firewall?

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

How does a firewall work?

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer’s entry point, called ports, which is where information is exchanged with external devices. For example, “Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it’s further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

Types of firewalls

Firewalls can either be software or hardware, though it’s best to have both. A software firewall is a program installed on each computer and regulates traffic through port numbers and applications, while a physical firewall is a piece of equipment installed between your network and gateway.

…………………………………………………………………………………………………

Q10: What is NOS?

A network operating system is a specialized operating system for a network device such as a router, switch or firewall.

A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal computers and, in some instances, older terminals that are connected on a local area network (LAN). The software behind a NOS allows multiple devices within a network to communicate and share resources with each other.

Historically operating systems with networking capabilities were described as network operating system, because they allowed personal computers (PCs) to participate in computer networks and shared file and printer access within a local area network (LAN). This description of operating systems is now largely historical, as common operating systems include a network stack to support a client server model.

…………………………………………………………………………………………………

Q11: What is Denial of Service (DoS)?

A **Denial-of-Service (DoS)** attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.

Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- **Buffer overflow attacks** – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks

- **ICMP flood** – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.

- **SYN flood** – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system, so that it can’t be accessed or used.

An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once. The distribution of hosts that defines a DDoS provide the attacker multiple advantages:

- He can leverage the greater volume of machine to execute a seriously disruptive attack
- The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)
- It is more difficult to shut down multiple machines than one
- The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems

Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

…………………………………………………………………………………………………

Q12: What is piggybacking?

In two-way communication, wherever a frame is received, the receiver waits and does not send the control frame (acknowledgement or ACK) back to the sender immediately.

The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.

This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.

Working Principle

Piggybacking data is a bit different from Sliding Protocol used in the OSI model. In the data frame itself, we incorporate one additional field for acknowledgment (called ACK).

Whenever party A wants to send data to party B, it will carry additional ACK information in the PUSH as well.

For example, if A has received 5 bytes from B, which sequence number starts from 12340 (through 12344), A will place "ACK 12345" as well in the current PUSH packet to inform B it has received the bytes up to sequence number 12344 and expects to see 12345 next time. (ACK number is the next sequence number of the data to be pushed by the other party.)

Three rules govern the piggybacking data transfer.

- If station A wants to send both data and an acknowledgment, it keeps both fields there.
- If station A wants to send just the acknowledgment, then a separate ACK frame is sent.
- If station A wants to send just the data, then the previous acknowledgment field is sent along with the data. Station B simply ignores this duplicate ACK frame upon receiving .

……………………………………………………………………………………………………

Q13: What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).

How does DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it’s important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs “behind the scenes” and requires no interaction from the user’s computer apart from the initial request.

……

Q14: What is OSPF?

Open Shortest Path First (**OSPF**) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). OSPF supports the Classless Inter-Domain Routing (CIDR) addressing model.

OSPF is a widely used IGP in large enterprise networks. IS-IS, another LSR-based protocol, is more common in large service provider networks.

OSPF was designed as an interior gateway protocol (IGP), for use in an autonomous system such as a local area network (LAN). It implements Dijkstra's algorithm, also known as the shortest path first (SPF) algorithm. As a link-state routing protocol it was based on the link-state algorithm developed for the ARPANET in 1980 and the IS-IS routing protocol. OSPF was first standardized in 1989 as RFC 1131, which is now known as OSPF version 1. The development work for OSPF prior to its codification as open standard was undertaken largely by the Digital Equipment Corporation, which developed its own proprietary DECnet protocols.

Routing protocols like OSPF calculate the shortest route to a destination through the network based on an algorithm. The first routing protocol that was widely implemented, the Routing Information Protocol (RIP), calculated the shortest route based on hops, that is the number of routers that an IP packet had to traverse to reach the destination host. RIP successfully implemented dynamic routing, where routing tables change if the network topology changes. But RIP did not adapt its routing according to changing network conditions, such as data-transfer rate. Demand grew for a dynamic routing protocol that could calculate the fastest route to a destination. OSPF was developed so that the shortest path through a network was calculated based on the cost of the route, taking into account bandwidth, delay and load. Therefore OSPF undertakes route cost calculation on the basis of link-cost parameters, which can be weighted by the administrator. OSPF was quickly adopted because it became known for reliably calculating routes through large and complex local area networks.

……

Q15: What is a ping?

A ping is a signal sent to a host that requests a response. It serves two primary purposes: 1) to check if the host is available and 2) to measure how long the response takes.

A ping request can be performed using a ping command, which is a standard command in most command line interfaces. Several network utilities provide a ping feature, which allows you to ping a server by simply entering the IP address or domain name. Most ping programs send multiple pings and provide and average of the pings at the end.

The ping itself consists of a single packet (often 32 or 56 bytes) that contains an "echo" request. The host, if available, responds with a single packet as a reply. The ping time, measured in milliseconds, is the round trip time for the packet to reach the host and for the response to return to the sender.

Ping response times are important because they add overhead to any requests made over the Internet. For example, when you visit a webpage the ping time is added to the time it takes a server to transmit the HTML and related resources to your computer. Pings are especially important in online gaming, where events happen in real-time.

While Internet connection speeds can affect pings, ping response time is often directly related to the physical distance between the source and destination systems. Therefore, a fast connection between New York and Tokyo will likely have a longer ping than a slow connection between New York and Philadelphia. Network congestion may slow down pings, which is why pings are often used for troubleshooting.

…………………………………………………………………………………………………

Q16: In a network that contains two servers and twenty workstations, where is the best place to install an Anti-Virus program?

Antivirus should be on each computer, if you implement server and node base antivirus that will be best for controlling.

There are no special problems just because you are two server and 20 computer. Every general issue will come along with critical. It will be same as any other computer setup issue.

…………………………………………………………………………………………………

Q17: What is the difference between CSMA/CD and CSMA/CA?

S.NO	CSMA/CD	CSMA/CA
1.	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
2.	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3.	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4.	CSMA / CD resend the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5.	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.
6.	It is more efficient than simple CSMA (Carrier Sense Multiple Access).	While it is similar to simple CSMA (Carrier Sense Multiple Access).

…………………………………………………………………………………………………

Q18: What is RSA Algorithm?

RSA (**Rivest–Shamir–Adleman**) is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". The acronym RSA is the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, which was not declassified until 1997.

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of the prime numbers can decode the message.[2] Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.

RSA is a relatively slow algorithm, and because of this, it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

……………………………………………………………………………………………………

Q19: What are the components of Protocol?

There are mainly three key elements of a protocol, they are as follows:

1. **Syntax**
2. **Semantics**
3. **Timing**

Let's learn these elements in detail.

- **Syntax**

Syntax refers to the structure or format of data and signal levels. It indicates how to read the data in the form of bits or fields. It also decides the order in which the data is presented to the receiver.

Example:

A protocol might expect that the size of a data packet will be 16 bits. In which, the first 4 bits are the sender's address, the next 4 bits are the receiver's address, the next 4 bits are the check-sum bits, and the last 4 bits will contain the message. So, every communication that is following that protocol should send 16-bit data.

- **Semantics**

Semantics refers to the interpretation or meaning of each section of bits or fields. It specifies which field defines what action. It defines how a particular section of bits or pattern can be interpreted, and what action needs to be taken. It includes control information for coordination and error handling.

Example:

It interprets whether the bits of address identify the route to be taken or the final destination of the message or something else.

- **Timing**

Timing refers to two characteristics:

1. When the data should be sent?
2. What will be the speed of sending and receiving the data?

It performs speed matching, sequencing and flow control of the data items.

Example:

A sender can send the data at a speed of 100 Mbps, but the receiver can consume it only at a speed of 20 Mbps, then there may be data losses or the packets might get dropped. So, proper synchronization must be there between a sender and a receiver

……………………………………………………………………………………………………....

Q20: What is Tunnel mode?

Tunnel mode:

- Tunnel mode protects the internal routing information by encrypting the IP header of the original packet. The original packet is encapsulated by a another set of IP headers.
- It is widely implemented in site-to-site VPN scenarios.
- NAT traversal is supported with the tunnel mode.
- Additional headers are added to the packet; so the payload MSS is less.

- More compatible with existing VPN gateways
- Don’t have to implement IPsec on the IPS entity
- Easier to traverse NATs
- More overhead
- Smaller MTU
- Secure operation within IPS scenarios would require negotiation of connection-specific selectors – not current practice
- For hosts with dynamically assigned addresses (iSCSI), interoperability is poor
- Existing implementations typically utilize proprietary extensions for configuration (mode config) or authentication (XAUTH)
- To avoid normative references to proprietary protocols, iSCSI and IPS security drafts would need to cite draft-ietf-ipsec-dhcp-13.txt for config and possibly draft-ietf-ipsra-pic-04.txt – which adds significantly complexity

…………………………………………………………………………………………………......

END