Hindusthan College of Engineering And Technology
Approved by AICTE, New Delhi, Accredited with 'A' Grade by NAAC
(An Autonomous Institution, Affiliated to Anna University, Chennai)
Coimbatore – 641 032

16CS5301-COMPUTER NETWORKS

INTERNAL TEST II QUESTION BANK ANSWERS

PART A

1. **What are the different signals encoding techniques?**

   Analog data to Analog signals − Amplitude Modulation, Frequency Modulation and Phase Modulation of analog signals.

   Analog data to Digital signals − Pulse Code Modulation (PCM).

   Digital data to Analog signals − Amplitude Shift Keying (ASK), Frequency Shift Keying (FSK), Phase Shift Keying (PSK).

   Digital data to Digital signals: Line Encoding, Block Coding, Scrambling.

2. **What is a digitization? How it can be done?**
   - The process of converting analog signal to digital signal is called digitization.
   - Two techniques to change an analog signal to digital data
     - pulse code modulation
     - delta modulation

3. **Why modulate analog signals?**

   Baseband signals are incompatible for direct transmission. For such a signal, to travel longer distances, its strength has to be increased by modulating with a high frequency carrier wave, which doesn't affect the parameters of the modulating signal.

4. **What are the drawbacks are of code division multiple access?**
   - Each user's transmitted bandwidth is enlarged than the digital data rate of the source. The result is an occupied bandwidth approximately equal to the coded rate.
   - The transmitter and receiver require a complex electronics circuitry.

5. **What is Multiple Access?**

   If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk.

6. What is time division multiple access?

- TDM is a digital multiplexing technique for combining several low-rate digital channels into one high-rate one.
- In TDM the shared channel is divided among its user by means of time slot.
- Each user can transmit data within the provided time slot only.
- Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

7. What is Switching?

A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. A switch is a multi-input, multi-output device that transfers packets from an input to one or more outputs.

8. What is meant by circuit switching?

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels. A connection between two stations is a dedicated path made of one or more links. Each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM.

9. What is meant by packet switching?

If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol In packet switching, there is no resource allocation for a packet.

10. What is Virtual Circuit Switching?

It uses the concept of a virtual circuit (VC) also called a connection-oriented model. It requires that we first set up a virtual connection from the source host to the destination host before any data is sent. A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

11. List the difference between the Circuit switching and packet switching.

Difference between circuit and packet switching

Sno	Circuit switching	Packet switching
1.	Source and destination host are physically connected	No such physical connection exists
2.	Call set up is required.	Call setup is not required.
3.	Switching takes place at the physical layer	Switching takes place at network (datagram) or data link layer (VCN)
4.	Resources such as bandwidth, switch buffer and processing time, are allocated in advance	Resources are allocated on demand
5.	Resources remain allocated for the entire duration of data communication.	Resources can be reallocated when idle
6.	There is no delay during data transfer.	Delay exists at each switch during data transfer
7.	Data transferred between the two stations is a continuous flow of signal	Data is transferred as discrete packets
8.	It is Transparent.	Not transparent.
9.	Charging is time based.	Charging is packet based.
10.	**Example: Telephony**	**Example: Internet**

12. What is routing?

- Routing: Process by which routing table is built.
- Routing table: Built by the routing algorithm as a precursor to build the forwarding table. Generally contains mapping from network numbers to next hops

(a)	
Prefix/Length	**Next Hop**
18/8	171.69.245.10

13. What are the types of routing protocol?

Intra-domain routing

1) Distance vector routing (eg. RIP)
2) Link state routing (eg. OSPF)

Inter domain routing

1) Path vector (eg. BGP)

14. What is link state routing?

Each node knows the state of link to its neighbors and the cost involved. Link-state routing protocols rely on two mechanisms: ¬ Reliable dissemination of link-state information ¬ Route calculation from the accumulated link-state knowledge.

15. What is Reliable Flooding?

Reliable flooding is the process of ensuring all nodes having a copy of the link-state information from all other nodes.

16. Write the features of OSPF.

- **Authentication of routing messages** - Misconfigured hosts are capable of bringing down a network by advertising to reach every host with the lowest cost 0. Such disasters are averted by mandating routing updates to be authenticated.
- **Additional hierarchy** - In OSPF, a domain is partitioned into areas, i.e., a router need not know the complete network, instead only its area.
- **Load balancing** - OSPF allows multiple routes to the same place to be assigned the same cost and will cause traffic to be distributed evenly over those routes.

17. Differentiate between RIP and OSPF.

RIP	OSPF
It is a distance vector protocol	It is a link state protocol
The metrics used in RIP is hop count	The metrics used in OSPF are bandwidth and delay
RIP uses distance vector algorithm to calculate the best path	OSPF uses the SPF algorithm to calculate the best path
In RIP protocol, networks are not divided in areas or tables	In OSPF, routing is carried out in autonomous system, into areas, sub areas as well as backbone areas
Maximum hop count is 15	No hop count

18. What are the salient features of IPV6?

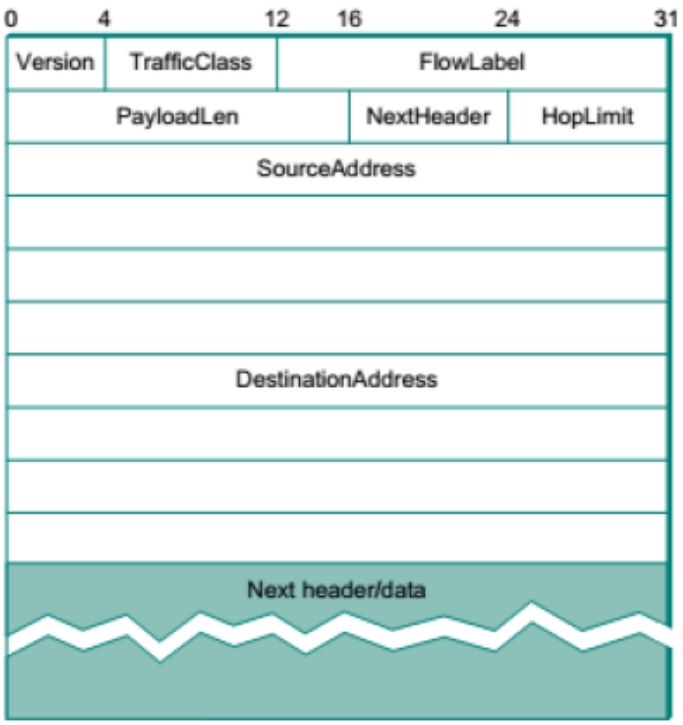
The striking features of IPv6 are:

1) Support for real-time services
2) Security support
3) Auto configuration
4) Enhanced routing functionality, including support for mobile hosts.

19. Differentiate between IPv4 and IPv6.

IPv4	IPv6
IPv4 addresses are 32 bit length.	**IPv6 addresses** are 128 bit length.
IPv4 addresses are **binary numbers** represented in decimals.	**IPv6 addresses** are **binary numbers** represented in **hexadecimals**.
IPSec support is only optional.	Inbuilt **IPSec** support.
Fragmentation is done by sender and forwarding routers.	**Fragmentation** is done only by sender.
No packet flow identification.	Packet flow identification is available within the **IPv6 header** using the **Flow Label** field.
Checksum field is available in **IPv4 header**	No checksum field in **IPv6 header**.
Options fields are available in **IPv4 header**.	No option fields, but **IPv6 Extension headers** are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	**Address Resolution Protocol (ARP)** is replaced with a function of **Neighbor Discovery Protocol (NDP)**.
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	**Broadcast messages** are not available. Instead a link-local scope "All nodes" **multicast IPv6 address** (FF02::1) is used for broadcast similar functionality.
Manual configuration (Static) of **IPv4 addresses** or DHCP (Dynamic configuration) is required to configure **IPv4 addresses**.	Auto-configuration of addresses is available.

20. Draw the sketch of IPv6 Packet Header.



1) **Version**—specifies the IP version, i.e., 6.
2) **TrafficClass**—defines the priority of the packet with respect to traffic congestion. It is either congestion-controlled or non-congestion controlled.
3) **FlowLabel**—is designed to provide special handling for a particular flow of data. The router handles flow with the help of a flow table.
4) **PayloadLen**—gives the length of the packet, excluding the IPv6 header
5) **NextHeader**—If options are required, then it is specified in one or more special headers following the IP header, its value is contained in NextHeader field. Otherwise, it identifies the higher-level protocol (TCP/UDP).
6) **HopLimit**—This field serves the same purpose as TTL field in IPv4.
7) **SourceAddress and DestinationAddress**—contains 16-byte address of the source and destination host respectively.

21. What is IP addressing?

Internet Protocol address (IP address) is a logical numeric address that is assigned to every single computer. An IP address is a logical address that is used to uniquely identify every node in the network. IP addresses are hierarchical, i.e., it corresponds to hierarchy in the internetwork. IP addresses consist of two parts, network id and host id. The network id identifies the network to which the host is attached. o Hosts attached to the same network have the same network id in their IP address. The host id is used to uniquely identify a host on a network.

22. What is subnetting?

With the rapid growth of the internet & the ever-increasing demand for new addresses, the standard address class structure has been expanded by borrowing bits from the Host portion to allow for more Networks. Under this addressing scheme, called Subnetting, separating the Network & Host requires a special process called Subnet Masking Subnetting is done by borrowing host bits and using them as network bits.

23. What is the need for subnetting?

- Improve network performance and speed
- Reduce network congestion
- Boost network security
- Control network growth
- Ease administration

24. What is CIDR?

Classless Interdomain Routing (CIDR) tries to balance between minimize the number of routing table entries and handling addresses space efficiently. CIDR aggregates routes, by which an entry in the forwarding table is used to reach multiple networks. CIDR aims to collapse the multiple addresses that would be assigned to a single AS onto one address, i.e., supernetting.

25. What is ARP?

The Address Resolution Protocol (ARP) enables a source host to know the physical address of another node when the logical address is known. ARP relies on broadcast support provided by physical networks such as Ethernet, Token ring, etc. ARP enables each host on a network to build up a table of mapping between IP address and physical address.

26. What is DHCP?

Dynamic Host Configuration Protocol (DHCP) enables auto configuration of IP address to hosts using DHCP. DHCP relies on the existence of a DHCP server that is responsible for providing configuration information to hosts. There is at least one DHCP server for an administrative domain.