**17IT3503 – Computer Networks**

**Unit-4 Important Questions**

**One Mark Questions**

What are the elements of wireless networks(CO4)

Mention the differences between wired link and wireless link (CO4)

What are the characteristics if 802.11 architecture (CO4)

Define Association (CO4)

Explain the process of Registration with the Home Agent (CO4)

Explain the Types of multimedia Network Applications(CO4)

Describe the Principles of Cryptography (CO4)

Explain different types of Firewalls (CO4)

**Essay Questions**

Explain the process of communication over the shared channel using CDMA with an example(CO4)

Explain wireless links and network charecteristics(CO4)

Explain 802.11 architecture.(CO4)

What is Passive and Active Scanning. Explain with diagram(CO4)

Define the components of Mobile IP (CO4)

Give the names of key fields in the agent advertisement message and their purpose (CO4)

Define spatial redundancy (CO4)

What are properties of Audio (CO4)

What are the properties of secure communication (CO4)

What are the goals of a Firewall (CO4)

**Placement Questions from Unit-4**

**Topic 1: Introduction: Wireless Links and Network Characteristics**

1. What is Hidden terminals problem?

Suppose that there are three mobile A, B, and C. The transmission range of A reaches B, but not C. The transmission range of C reaches B, but not A. Finally the transmission range of B reaches A and C.

A starts sending signal to B, C does not receive this transmission. C also wants to send data to B and senses the medium. The medium appears to be free, the carrier sense fails. C also starts sending data. It will create a collision at B. But A cannot detect this collision at B and continues with its transmission. A is hidden for C and vice versa.

2. What are the components of wireless network?

•User Devices. Users of wireless LANs operate a multitude of devices, such as PCs, laptops, and PDAs.

•Radio NICs. A major part of a wireless LAN includes a radio NIC that operates within the computer device and provides wireless connectivity. ...

•Access Points. ...

•Routers. ...

•Repeaters. ...

•Antenna

3. Why do we use wireless networks?

Wireless networks enable multiple devices to use the same internet connection remotely, as well as share files and other resources. They also allow mobile devices, such as laptops, tablets and mobile phones to move around within the network area freely and still maintain a connection to the internet and the network

4. What are the advantages of wireless network?

Increased Mobility: Wireless networks allow mobile users to access real-time information so they can roam around your company's space without getting disconnected from the network. This increases teamwork and productivity company-wide that is not possible with traditional networks

5. Which is more secure wireless or wired networks?

In the past, wired networks were considered to be far more secure than wireless networks. Today, however, wireless networks are as secure as wired networks, so long as they are properly configured.

**Topic 2: Wifi:80211 Wireless Lans**

1. How many address fields does an 802.11 header have?

4 address fields

Address fields are present in the MAC header of 802.11 frames. A frame may contain 4 address fields. Address fields are 6 octets in length. Address fields are used to indicate Source, Transmitter, Destination, Receiver and BSSID

2. Which technique is used in wireless LAN?

Spread Spectrum. Spread spectrum is currently the most widely used transmission technique for wireless LANs. It was initially developed by the military to avoid jamming and eavesdropping of the signals

3. Is WLAN and WIFI same?

Answer: Both Wi-Fi (wireless fidelity) and WLAN (wireless local area network) mean the same — they both refer to a wireless network that can transfer data at high speeds.

4. What is WLAN and how it works?

WLANs use radio, infrared and microwave transmission to transmit data from one point to another without cables. Therefore WLAN offers way to build a Local Area Network without cables. This WLAN can then be attached to an already existing larger network, the internet for example

5. What are the disadvantages of WLAN?

Disadvantages of wireless local area network (WLAN)

WLAN requires license.

It has a limited area to cover.

Government agencies can limit the signals of WLAN if required. ...

If the number of connected devices increases then data transfer rate decreases.

WLAN uses radio frequency which can interfere with other devices which use radio frequency.

6. What are the features of WLAN?

• High Capacity Load Balancing. ...

• Scalability. ...

• Network Management System. ...

• Role Based Access Control. ...

• Indoor as well as Outdoor coverage options. ...

• The Ability to Measure Performance. ...

• Network Access Control. ...

• Ability to communicate with both 2.4 GHz devices and 5 GHz devices

7. Explain the difference between WLAN and WiMAX.

WLAN stands for wireless local area network, and it provides connectivity between devices that are WLAN compliant. WLAN follows 802.11 standards set by the Institute of Electrical and Electronics Engineers (IEEE) including 11a, 11b, 11g, 11n, 11ac and 11ad.

WiMAX, on the other hand, is used as a wide area network for providing access between various wireless devices. WiMAX follows IEEE standards 16d and 16e.

**Topic 3: Mobile IP**

1. What is Home Agent and Foreign Agent in case of Mobile IP?

In Mobile Internet Protocol (Mobile IP), a home agent is a router on a mobile node's home network that maintains information about the device's current location, as identified in its care-of address. ... A home agent may work in conjunction with a foreign agent, which is a router on the visited network.

2. How Mobile IP is useful in mobile communication?

Mobile IP solves this problem by allowing the mobile node to use two IP addresses: a fixed home address and a care-of address that changes at each new point of attachment. Mobile IP enables a computer to roam freely on the Internet or an organization's network while still maintaining the same home address.

3. What are the requirements for Mobile IP?

The mobile IP has following three components as follows:

• Mobile Node (MN) ...

• Home Agent (HA) ...

• Foreign Agent (FA) ...

• Care of Address (COA) ...

• Correspondent Node (CN) ...

• Home Network. ...

• Foreign network

4. What is CoA in Mobile IP?

Used in Internet routing, a care-of address (usually referred to as CoA) is a temporary IP address for a mobile device. This allows a home agent to forward messages to the mobile device.

5. What are the entities of mobile IP?

Mobile IP Functional Entities

Mobile Node (MN)-Host or router that changes its point of attachment from one network to another.

Home Agent (HA)-Router on a mobile node's home network that intercepts datagrams destined for the mobile node, and delivers them through the care-of address.

6. What is agent advertisement in Mobile IP?

An agent advertisement is an Internet Control Message Protocol (ICMP) router advertisement that has been extended to also carry a mobility agent advertisement extension. A foreign agent can be too busy to serve additional mobile nodes.

7. What is Agent solicitation?

Mobility agents transmit agent advertisements to advertise their services on a network. In the absence of agent advertisements, a mobile node can solicit advertisements. This is known as agent solicitation.

**Topic 4: Multimedia Networking Applications**

1. What is meant by streaming stored audio and video?

Sol: Streaming means a user can listen (or watch) the file after the downloading has started. In the first category, streaming stored audio/video, the files are compressed and stored on a server. A client downloads the files through the Internet. This is sometimes referred to as on-demand audio/video

2. What are the 5 types of multimedia?

Sol: The Five Multimedia Elements Edit. Text, image, audio, video, and animation are the five multimedia elements. The first multimedia element is text. Text is the most common multimedia element.

3. What is multimedia and its examples?

Multimedia is a broad term for combining multiple media formats. Whenever text, audio, still images, animation, video and interactivity are combined together, the result is multimedia. Slides, for example, are multimedia as they combine text and images, and sometimes video and other types

4. What is the purpose of streaming?

Sol: Streaming is a means to send and receive data (such as audio or video) in a continuous flow over a network. It allows playback to begin while sending the rest of the data. For example, as soon as your computer or phone receives the beginning of a movie, you're able to start watching it

5. What is the difference between streaming and watching?

“Streaming” a TV show means watching it through a web site — i.e., you have not downloaded it, but you are viewing a “stream” of video. “Watching” a TV show generally means viewing it via cable, satellite, or bunny ears. But the term “watching” is also used when a person watches something over the internet.

6. What are the major components of multimedia?

The following are the different components used in multimedia system:

•Text: It is the primary component of multimedia. ...

•Graphic: A digital representation of non-text information such as drawing, photographs etc are known as graphics. ...

•Audio: Audio is one of the important components of multimedia

**Topic 5: What is Network security & Principles of cryptography**

1. What are the principles of network security?

Network security involves three key principles of confidentiality, integrity, and availability. Depending upon the application and context, one of these principles might be more important than the others

2. Explain the difference between symmetric and asymmetric encryption.

A: Long story short, symmetric encryption uses the same key for both encryption and decryption, whereas asymmetric encryption employs different keys for the two processes. Symmetric is faster for obvious reasons but requires sending the key through an unencrypted channel, which is a risk

3. Name the three means of user authentication.

A: There is biometrics (e.g. a thumbprint, iris scan), a token, or a password. There is also two-level authentication, which employs two of those methods.

4. Define Cryptography in your own way along with its benefits?

Well, it is actually a method of securing communications through some protocols in order to make the information secure or understood able only by the sender as well as the receiver. Earlier this strategy was based on mathematical theories and computer science. However, with improvement in technology, it is presently based on some vast protocols that are difficult to crack. Thus information security, as well as authenticity can always be ensured and it’s the leading benefit of Cryptography.

5. What is decryption? What is its need?

Cryptography has two important modules and they are encryption and second is decryption. Encryption is basically an approach that converts information into secret codes. It is also known as encoding. It is done to make the information secure. On the other side decryption is a process that is opposite to it i.e. converting the coded information back to its actual form. Only the receiver knows the protocols to decode that information.

6. What do you mean by Secret Key Cryptography and Public Key Cryptography? How they are different from one another

Both these are the algorithms of encryption and contribute in data security. Secret Key Cryptography can be used for both encryption as well as decryption. It is also considered as symmetric approach and contains only one key. On the other hand Public Key cryptography is basically an asymmetric approach. There are two keys in this approach and one is basically the public key and any user can access the information. The other key is private and can only be accessed by administrator.

7. Can you tell what the prime objectives of modern cryptography are?

There are four prime objectives and they are:

• Confidentiality

• Non repudiation

• Authenticity

• Integrity

**Topic 6: Operational Security : firewalls**

1. What are the different types of firewall?

The 3 types of firewall are:

• Packet filtering firewall.

• Circuit-level gateway.

• Stateful inspection firewall.

2. Which is the most secure type of firewall?

Proxy firewalls have their own IP address which prevents direct network contact with other systems and is championed as the most secure type of firewall available

3. Why is firewall needed?

Why do I need a Firewall? A firewall is an essential part of your business' security system. Without it, your network is open to threats. A firewall keeps destructive and disruptive forces out, and controls the incoming and outgoing network traffic based on security parameters that you can control and refine

4. How does a firewall work?

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through. ... With a firewall in place, the landscape is much different.

5. How long does a firewall last?

about five to eight years

Firewalls, Switches, & Wireless Access Points: Your typical firewall, access point, and switch last about five to eight years. Like a server, you will definitely want to replace it before waiting on its failure