Wireless Data Communications

e-NOTES

B.Sc. Computer Science / B.C.A

Dr.P.Rizwan Ahmed
Vice Principal (Academic) & HOD

Department of Computer Applications &
PG Department of Information Technology

Mazharul Uloom College, Ambur-635802
(Managed by Ambur Muslim Educational Society (AMES),
Affiliated to Thiruvalluvar University, Vellore)
Mail id: deptofbcamuc@gmail.com

Define Wireless LAN

Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the device.

Advantages and Disadvantages of Wireless LAN

Advantages of wireless local area network (WLAN) :

- It's a reliable sort of communication.
- As WLAN reduces physical wires so it's a versatile way of communication.
- WLAN also reduces the value of ownership.
- It's easier to feature or remove workstation.
- It provides high rate thanks to small area coverage.
- For propagation, the sunshine of sight isn't required.
- Easy installation and you would like don't need extra cables for installation.

Disadvantages of wireless local area network (WLAN) :

- WLAN requires license.
- It's a limited area to hide.
- WLAN uses frequency which may interfere with other devices which use frequency.
- The radiation of WLAN are often harmful to the environment
- WLAN is expensive than wires and hubs as it access points.
- Signals can get from nearest signals by access points.
- Chances of errors are high.

Infrared Vs Radio Transmission

Infrared	Radio
▫ uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)	▫ typically using the license free ISM band at 2.4 GHz
Advantages	**Advantages**
▫ simple, cheap, available in many mobile devices ▫ no licenses needed ▫ simple shielding possible	▫ experience from wireless WAN and mobile phones can be used ▫ coverage of larger areas possible (radio can penetrate walls, furniture etc.)
Disadvantages	**Disadvantages**
▫ interference by sunlight, heat sources etc. ▫ many things shield or absorb IR light ▫ low bandwidth	▫ very limited license free frequency bands ▫ shielding more difficult, interference with other electrical devices
Example	**Example**
▫ IrDA (Infrared Data Association) interface available everywhere	▫ WaveLAN, HIPERLAN, Bluetooth

adhoc network

An ad hoc network is one that is spontaneously formed when devices connect and communicate with each other. The term ad hoc is a Latin word that literally means "for this," implying improvised or impromptu.

Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.

Types of Wireless Ad Hoc Networks

Wireless ad hoc networks are categorized into classes. Here are a few examples:

- **Mobile ad hoc network (MANET)**: An ad hoc network of mobile devices.
- **Vehicular ad hoc network (VANET)**: Used for communication between vehicles.

- **Smartphone ad hoc network (SPAN)**: Wireless ad hoc network created on smartphones via existing technologies like Wi-Fi and Bluetooth.
- **Wireless mesh network**: A mesh network is an ad hoc network where the nodes communicate directly with each other to relay information throughout the network.

Radio Access Layer

To support wireless communication, new wireless channel specific physical, medium access and data link layers are need to be added below the ATM network layer. These layers are called Radio Access Layer in the WATM network. The following sections address the design issues of the Radio Access Layer.

Physical Layer (PHY*)*
While a fixed station may own an 25 Mbit/s up to 155 Mbit/s data rate ATM link, a 25 Mbit/s data link in a wireless environment is currently difficult to implement. A several GHz spectrum would be required to provide high speed wireless transmission.

Media Access Control (MAC)
WATM MAC is responsible for providing functionally point to point links for the higher protocol layer to use. To identify each station, both IEEE 48 bit address and local significant address, which is assigned dynamically within a cell, are allowed.

Data Link Control (DLC)
Data Link Control is responsible for providing service to ATM layer. Mitigating the effect of radio channel errors should be done in this layer before cells are sent to the ATM layer.

Radio Resource Control (RRC)
RRC is needed for support of control plane functions related to the radio access layer. It should support radio resource control and management functions for PHY, MAC, and DLC layers.

Handover

A handover is a process in telecommunications and mobile communications in which a connected cellular call or a data session is transferred from one cell site (base station) to another without disconnecting the session. Cellular services are based on mobility and

handover, allowing the user to be moved from one cell site range to another or to be switched to the nearest cell site for better performance.

Handovers are a core element in planning and deploying cellular networks. It allows users to create data sessions or connect phone calls on the move. This process keeps the calls and data sessions connected even if a user moves from one cell site to another.

There are two types of handovers:

1. **Hard Handover:** An instantaneous handover in which the existing connection is terminated and the connection to the destination channel is made.
2. **Soft Handover**: A substantial handover where the connection to the new channel is made before the connection from the source channel is disconnected.

Bluetooth

Bluetooth technology is a high speed and low powered wireless technology designed to connect phones or other portable equipment for communication or file transmissions. This is based on mobile computing technology. Following is a list of some prominent features of Bluetooth technology:

- Bluetooth is also known as IEEE 802.15 standard or specification that uses low power radio communications to link phones, computers and other network devices over a short distance without using any type of connecting wires.
- As Bluetooth is an open wireless technology standard so, it is used to send or receive data to connected devices present across a certain distance using a band of 2.4 to 2.485 GHz.
- In Bluetooth technology, the wireless signals transmit data and files over a short distance, typically up to 30 feet or 10 meters.
- Bluetooth technology was developed by a group of 5 companies known as Special Interest Group formed in 1998. The companies are Ericsson, Intel, Nokia, IBM, and Toshiba.
- The range of Bluetooth technology for data exchange was up to 10 meters in older versions of devices, but the latest version of Bluetooth technology i.e., Bluetooth 5.0, can exchange data in the range of about 40-400 meters.

- The average speed of data transmission in Bluetooth technology was around 1 Mbps in the very first version. The second version was 2.0+ EDR, which provided the data rate speed of 3Mbps. The third was 3.0+HS, which provided the speed of 24 Mbps. The latest version of this technology is 5.0.

UNIT V WIRELESS DATA COMMUNICATION

Domain Name System (DNS)

- Domain Name System is an Internet service that translates domain names into IP addresses.
- The DNS has a distributed database that resides on multiple machines on the Internet.
- DNS has some protocols that allow the client and servers to communicate with each other.
- When the Internet was small, mapping was done by using hosts.txt file.
- The host file was located at host's disk and updated periodically from a master host file.
- When any program or any user wanted to map domain name to an address, the host consulted the host file and found the mapping.
- Now Internet is not small, it is impossible to have only one host file to relate every address with a name and vice versa.
- The solution used today is to divide the host file into smaller parts and store each part on a different computer.
- In this method, the host that needs mapping can call the closest computer holding the needed information.

Name space

- The names assigned to the machines must be carefully selected from a name space with complete control over the binding between the names and IP addresses.
- There are two types of name spaces: Flat name spaces and Hierarchical names.

Flat name spaces

- In a flat name space, a name is a sequence of characters without structure.
- A name in this space is assigned to an address.
- The names were convenient and short.

Hierarchical Name Space

- In hierarchical name space, each name consists of several parts.

- First part defines the nature of the organization, second part defines the name of an organization, third part defines department of the organization, and so on

Generic Domains

The generic domains define registered hosts according to their generic behavior.

Generic domain labels are as stated below:

Country Domains

- Country domain uses two character country abbreviations.
- Second labels can be more specific, national designation.
- **For example,** for Australia the country domain is "au", Inida is .in, UK is .uk etc.

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is the standard protocol for email services on a TCP/IP network. SMTP provides the ability to send and receive email messages.

SMTP is an application-layer protocol that enables the transmission and delivery of email over the Internet. SMTP is created and maintained by the Internet Engineering Task Force (IETF).

Simple Mail Transfer Protocol is also known as RFC 821 and RFC 2821.

SMTP is one of the most common and popular protocols for email communication over the Internet and it provides intermediary network services between the remote email provider or organizational email server and the local user accessing it.

SMTP is generally integrated within an email client application and is composed of four key components:

1. Local user or client-end utility known as the mail user agent (MUA)
2. Server known as mail submission agent (MSA)
3. Mail transfer agent (MTA)
4. Mail delivery agent (MDA)

SMTP works by initiating a session between the user and server, whereas MTA and MDA provide domain searching and local delivery services.

SNMP Protocol

SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.

SNMP components –
There are 3 components of SNMP:

1. **SNMP Manager –**
   It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

2. **SNMP agent –**
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

3. **Management Information Base –**
   MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

SNMP messages
Different variables are:

1. **GetRequest**
   SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents.

2. **GetNextRequest**
   This message can be sent to discover what data is available on an SNMP agent.

3. **GetBulkRequest**
   This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.

4. **SetRequest**
   It is used by the SNMP manager to set the value of an object instance on the SNMP agent.

5. **Response**
   It is a message sent from the agent upon a request from the manager.

6. **Trap**
   These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.

File Transmission Protocol (FTP)

FTP means "File Transfer Protocol" and refers to a group of rules that govern how computers transfer files from one system to another over the internet. Businesses use FTP to send files between computers, while websites use FTP for the uploading and downloading of files from their website's servers.

FTP works by opening two connections that link the computers trying to communicate with each other. One connection is designated for the commands and replies that get sent between the two clients, and the other channel handles the transfer of data. During an FTP transmission, there are four commands used by the computers, servers, or proxy servers that are communicating. These are "send," "get," "change directory," and "transfer."

While transferring files, FTP uses three different modes: block, stream, and compressed. The stream mode enables FTP to manage information in a string of data without any boundaries between them. The block mode separates the data into blocks, and in the compress mode, FTP uses an algorithm called the Lempel-Ziv to compress the data.

Types of FTP

While FTP can be used to accomplish several kinds of tasks, there are three primary categories of FTPs.

FTP Plain

FTP Plain refers to normal FTP without encryption. By default, it uses port 21, and it is supported by the majority of web browsers.

FTPS

FTPS refers to FTP Secure or FTP secure sockets layer (SSL) because this kind of FTP server uses SSL encryption, which is slightly different than traditional FTP. The primary difference is the security that comes with FTPS, which was the first type of encrypted FTP invented.

FTPES

The "E" in FTPES means "explicit," making the acronym stand for File Transfer Protocol over explicit transport layer security (TLS)/SSL. This type of FTP begins like regular FTP, using port 21, but then special commands upgrade it to a TLS/SSL-encrypted transmission. Because it tends to work well with firewalls, some prefer to use FTPES over FTPS.

Digital Signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

1. **Key Generation Algorithms**: Digital signature is electronic signatures, which assure that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise, the data can be altered or someone can also act as if he was the sender and expect a reply.

2. **Signing Algorithms**: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier.

3. **Signature Verification Algorithms** : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value.

How do Digital Signatures work?

Digital signature solution providers will produce two keys: a public key and a private key, using a mathematical procedure. When a signer digitally signs a document, a cryptographic hash of the document is created.

That cryptographic hash is then encrypted using the sender's private key, which is kept safe in an HSM box. It is then added to the document and delivered together with the sender's public key to the recipients.

With the sender's public key certificate, the recipient may decode the encrypted hash. On the recipient's end, a cryptographic hash is created once again.

To verify its legitimacy, the cryptographic hashes are compared. If they match, the document has not been tampered with and is genuine.

BootStrap Protocol and DHCP

BOOTP stands for **Bootstrap Protocol** and **DHCP** stands for **Dynamic host configuration protocol**. These protocols square measure used for getting the information science address of the host alongside the bootstrap info. The operating of each protocol is totally different in some manner. Dynamic host configuration protocol is also the extended version of the Bootstrap Protocol.

Bootstrap Protocol

The Bootstrap Protocol is a networking protocol that allows a configuration server to provide an IP address to network devices automatically in Internet Protocol networks. RFC 951 was the first to define the BOOTP.

When a network-connected machine wakes up, its IP stack sends out BOOTP network signals asking for an IP address. When a BOOTP configuration server receives a request, it assigns an IP address from a pool of addresses that an administrator has prepared.

BOOTP is implemented with the UDP as the transport protocol, with the (DHCP) server accepting client queries on port 67 and the client receiving (DHCP) server answers on port 68. Only IPv4 networks aresupported by BOOTP.

Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol for Internet Protocol (IP) networks that assigns IP addresses and other communication settings to devices connected to the network using a client-server architecture.

DHCP is a client/server protocol that automatically assigns an IP address and other configuration information to an Internet Protocol (IP) host, such as the subnet mask and default gateway. When using DHCP, the server uses port 67 and the client uses port 68.

When a computer is connected into a different location on the network, DHCP allows a network administrator to oversee and distribute IP addresses from a central location, and it immediately transmits a new Internet Protocol (IP) address.

The technique removes the need to manually configure network devices by combining two network components: a centrally deployed network DHCP server and the client instances of the protocol stack on each computer or device. When a client connects to

the network forthe first time, it utilizes the DHCP protocol to ask the DHCP server for a set of parameters.

Difference between BOOTP and DHCP

BOOTP	DHCP
BOOTP stands for Bootstrap Protocol.	While DHCP stands for Dynamic host configuration protocol.
BOOTP does not provide temporary IP addressing.	While DHCP provides temporary IP addressing for only limited amount of time.
BOOTP does not support DHCP clients.	While it support BOOTP clients.
In BOOTP, manual-configuration takes place.	While in DHCP, auto-configuration takes place.
BOOTP does not support mobile machines.	Whereas DHCP supports mobile machines.
BOOTP can have errors due to manual-configuration.	Whereas in DHCP errors do not occur mostly due to auto-configuration.