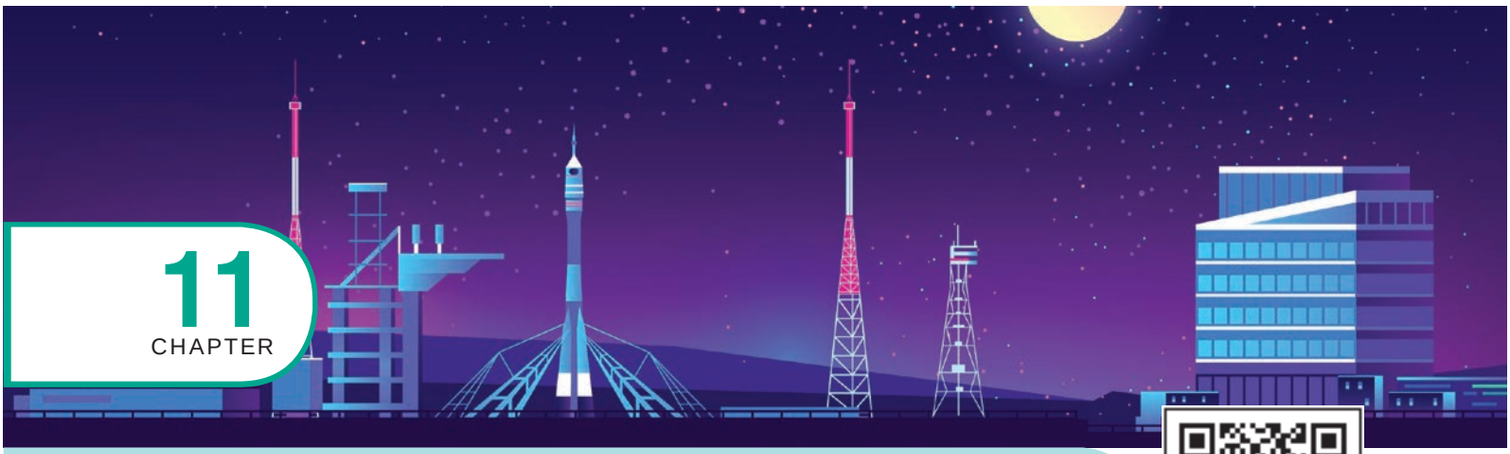

11
CHAPTER

Network Examples and Protocols

8D4TCC

LEARNING OBJECTIVES

- To know network examples like Intranet, Intranet, Extranet
- Different types of mobile networks
- Know about wlans :802.11
- To Know about RFID
- Discuss briefly about the network protocols

11.1 Introduction

Internet Protocol (IP) is the principle of communication protocol amoung the Internet protocols for layering on datagram across boundaries of other networks. Its main function is to allow Internet working and boost up the Internet.

Internet protocol (IP) will discharge packets from the source host and it will deliver to the destination host via IP address in the packet header.

Network protocols is the usual procedures, rules, formal standards and policies comprised of formats which allows communication between more than one device which is connected to the network. Network protocols have to do end-to-end process of secure on time and manage data or network communication.

All requirements which combine process, on network protocols so as to carry out the communication between routers, servers, computers, laptop, and other authorized networked device. Here on network protocols might be installed and rooters in both sender and receiver to ensure data or network communication and apply to software and hardware nodes which communicate on a network.

The broad types of networking protocols, including:

- Network communication protocols is the basic data communication protocol which consist of HTTP and TCP/IP.
- Network security protocol is which implement security over network communication and include HTTP, SFTP and SSL.
- Network management protocol will Provide network governance and

Figure: 11.1 INTERNET

maintenance and include ICMP and SNMP.

11.1.1 Internet / Intranet / Extranet

INTERNET: The **Internet**, "the Net," is a worldwide system of computer networks- A network of networks where the users at any one computer can, if they have permission, get information from any other computer. The Internet is a network of global connections – comprising private, public, business, academic and government networks – linked by guided, wireless and fiber-optic technologies. It was perceived by the Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first recognized as the ARPANet. The unique aim was to generate a network that would permit users of a research computer from one university to "talk to" research computers on other universities. The jargons Internet and World Wide Web are frequently used interchangeably, but they are not precisely the same. The Internet denotes to the global communication system, including infrastructure and hardware, whereas the web is one of the services interconnected over the Internet. See Figure 11.1

INTRANET: It is a private network within an enterprise to share company data and computing resources between the employees. It may consist of many interlinked local area networks. It includes connections through one or more gateway (connects two networks using different protocols together known as protocol convertor) computers to outside Internet. See Figure 11.2

Figure 11.2 Intranet

EXTRANET: It is a private network that uses Internet technology and the public telecommunication system to securely share business's information with suppliers, vendors, partners, customers, or other businesses. See Figure 11.3 and 11.4

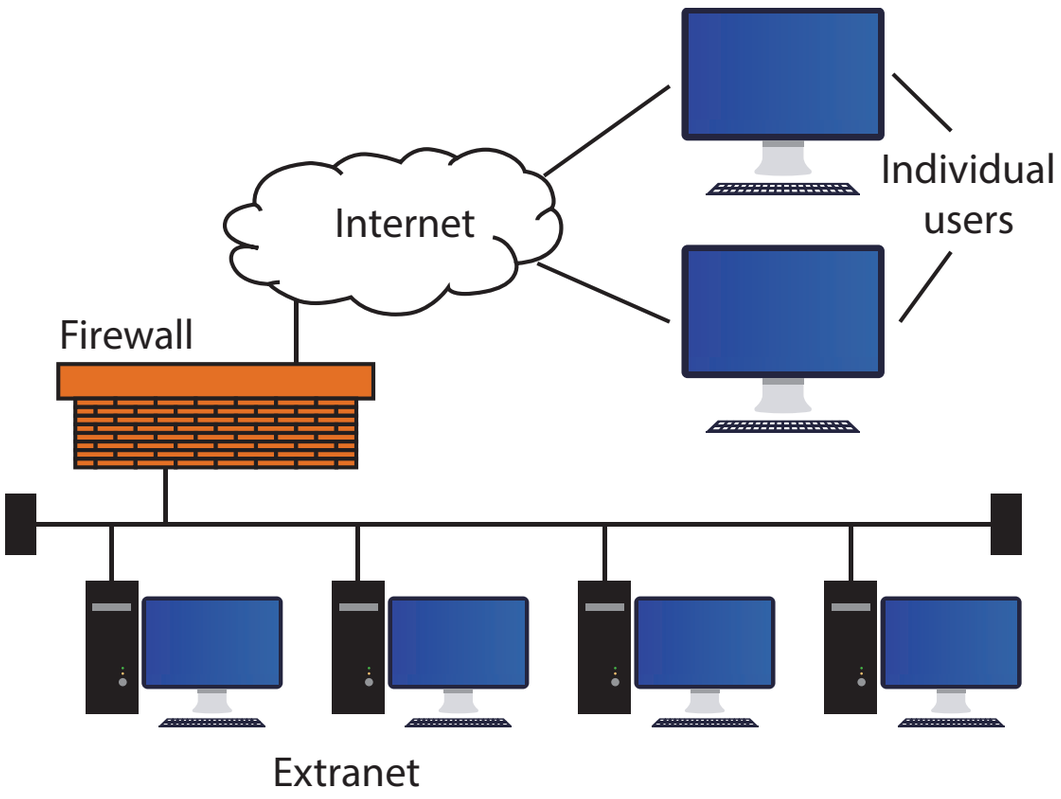

Figure 11.3 Extranet

Internet of Things refers to the digital interconnection of everyday objects (home applicances, wearable devices or automobiles) with the Internet. The 'thing' in IoT refers to objects that have been assigned an IP address and have the ability to collect and transfer data over a network without manual assistance or intervention.

Comparison

Table 11.1 Comparison between Internet, Intranet and Extranet

Type	Definition	Example
Internet	A global network, public TCP/IP network used by over a billion people all over the world	Sending email to a friend
Intranet	A TCP/IP network with access restricted to members of an organization	Accessing your record in the employee personnel file
Extranet	A TCP/IP network with restricted access to members	Checking availability of inventory from an outside supplier

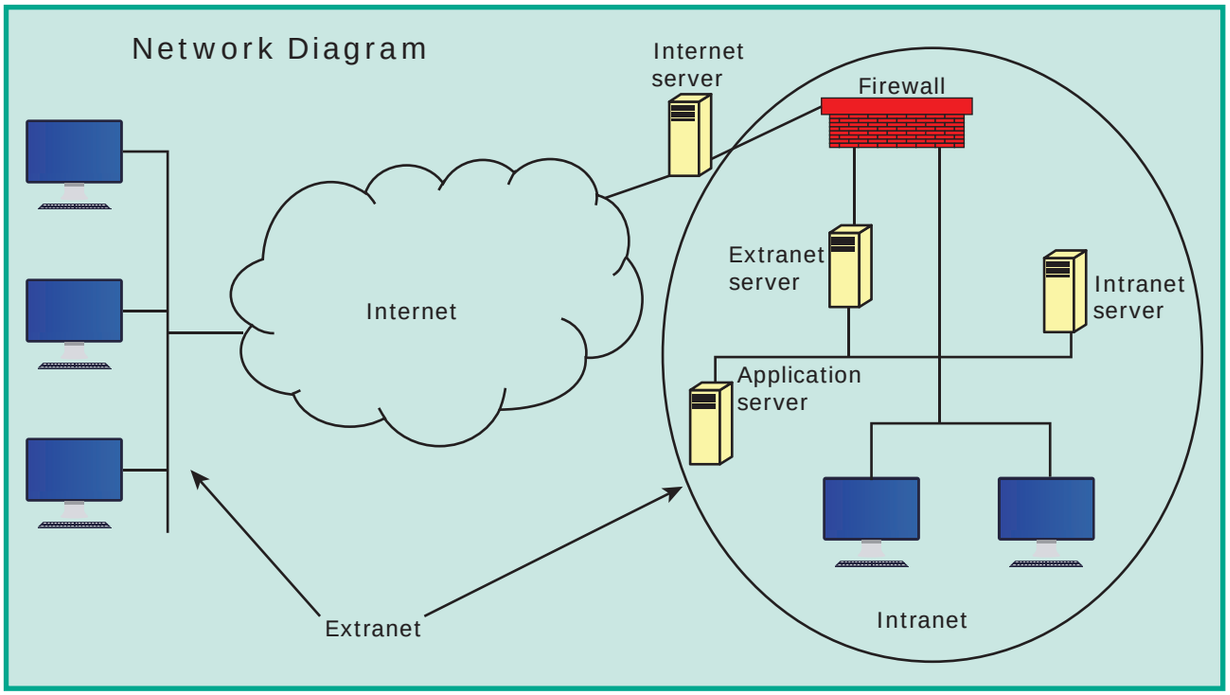

Figure 11.4 Internet, Intranet and Extranet

Table 11.2 Network Applications

Application of Internet.	Application of Intranet	Application of Extranet
• Download programs and files • Social media • E-Mail • E-Banking • Audio and Video Conferencing • E-Commerce • File Sharing • E- Governance • Information browsing • Search the web addresses for access through search engine • Chatting and etc	• Sharing of company policies/rules and regulations • Access employee database • Distribution of circulars/ Office Orders • Access product and customer data • Sharing of information of common interest • Launching of personal/ departmental home pages • Submission of reports • Corporate telephone directories.	• Customer communications • Online education/ training • Account status enquiry • Inventory enquiry • Online discussion • Supply – chain managements • Order status enquiry • Warranty registration • Claims • Distributor promotions

11.1.2 Mobile Networks

A mobile network or cellular network as it is made up of a large number of signal areas called cells. These cells join to form a large coverage area. Users can cross into different cells without losing their connection. Within each cell there is a base station, which sends and receives the mobile signals. A mobile device will connect to the nearest or least base station. The base stations are connected to digital exchange where the communication is sent to other telephone

or data networks. Cells will often be smaller in size in large towns, as the number of users in the area is more. Communication over mobile network is made up of voice, data, images and text messages. See Figure 11.5

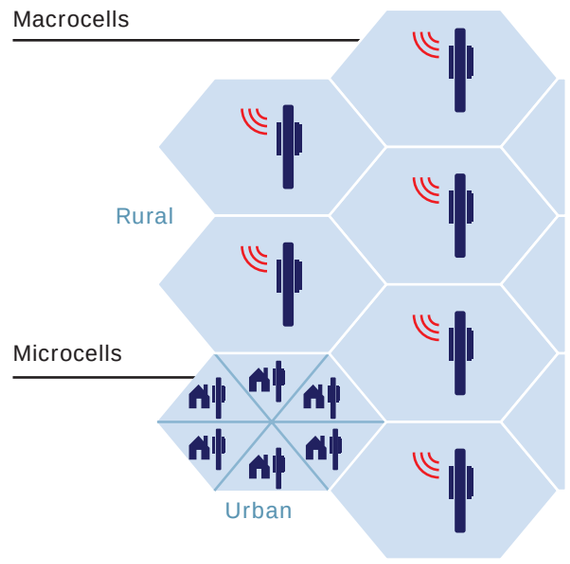

Figure 11.5 Mobile Network

Mobile networking assign to the technology supports voice/data, network connectivity using via radio transmission solution. The common application of mobile networks is mobile phones, tablets, etc.. In the past, wireless communications largely used circuit switching to carry only voice over a network, but now currently both data and voice are being transmitted over both circuit via switched networks and packet-switched networks.

The generation of mobile networks are as follows.

- First Generation(1G) 1981- NMT launch
- Second Generation(2G) 1991-GSM Launch
- Second to Third Generation Bridge (2.5)2000 – GPRS launch
- Third Generation(3G) 2003- UK 3G launch
- Fourth Generation (4 G) 2007
- Fifth Generation (5G) 2019+

First Generation (1G) 1981 – NMT launch

During the initial periods the mobile systems were based on analog transmission. NMT stands for Nordic Mobile Telephone communication. They had a very low traffic density of one call per radio channel, and a very poor voice quality, and they used unsure and unencrypted transmission, which leads to the spoofing of its identities.

Second Generation (2G) 1991 – GSM launch

Later the second generation of mobile systems were placed on digital transmission with GSM. **GSM stands for (Global System for Mobile communication)** was most popular standard which is used in second generation, using 900MHz and 1800MHz for the frequency bands. GSM mobile systems grown digital transmission using SIM. SIM stands for (**Subscriber Identity Module)** technology to authenticate a user for identification and billing purposes, and to encrypt the data to prevent listen without permission (eavesdropping). The transmission used as TDMA. TMDA stands for (**Time Division Multiple Access**) and CDMA stands for **(Code Division Multiple Access)** method to increase the amount of information transported on the network. Mobility is supported at layer 2, which stops seamless roaming across assorted access networks and routing domains. This means that

each operator must cover the entire area or have agreements in place to permit roaming.

Second to Third Generations Bridge (2.5G) 2000 – GPRS launch

GPRS was introduced here, this is the excess period of mobile networking development, between 2G and 3G. GPRS stands for(**General Packet Radio Service**).GPRS is a data service which enables mobile devices to send and receive messages, picture messages and e-mails. It allows most popular operating speeds of up to 115kbit/s, latterly maximum of 384kbit/s by usingEDGE. EDGE stands for **EDGE (Enhanced Data rates for Global Evolution)**. GSM data transmission rates typically reached 9.6kbit/s.

Third Generation(3G)2003 – First UK 3G launch

This generation of mobile system merges different mobile technology standards, and uses higher frequency bands for transmission and Code Division Multiple Access to deliver data rates of up to 2Mbit/s supporting multimedia services (MMS: voice, video and data). European standard is UMTS **(Universal Mobile Telecommunication Systems).** Mobile phones systems continue to use digital transmission with SIM authentication for billing systems and for data incorruption. Data transmission used a WCDMA. WCDMA stands for (Wideband Code Division Multiple Access). A technique to obtain data rates between 384kbit/s and 2048kbit/s. Few 3G suppliers use ATM (Asynchronous Transfer Mode) for '**over the air**' network with in MPLS (Multiprotocol Label Switching) or IP for their backbone network.

Mobility still supported at layer 2, and hence like 2G it still prohibits seamless roaming beyond heterogeneous access networks and routing domains. The transmission were band frequencies between 1900 and 2200 MHz. All UMTS license holders at the UK holds a 20 year license with the condition that 80% population coverage is achieved by 31 December 2007. The present third generation licensed operators in the UK can be seen below as at August 2004.

Fourth Generation(4G) 2007

4G is at the research stage. 4G was based on an adhoc networking model where there was no need for a fixed infrastructure operation. Adhoc networking requires global mobility features (e.g. Mobile IP) and connectivity to a global IPv6 network to support an IP address for each mobile device. Logically roaming in assorted IP networks (for example: 802.11 WLAN, GPRS and UMTS) were possible with higher data rates, from 2Mbit/s to 10–100Mbit/s, offering reduced delays and new services. Mobile devices will not expect on a fixed infrastructure, they

Li-Fi is a wireless technology which uses light-emitting diodes (LEDs) for data transmission whereas Wi-Fi uses radio frequencies for data transmission. Li-Fi is the short form of Light Fidelity.

The term Li-Fi was first used by Harald Haas, Professor in Edinburgh University. The computer scientists achieved speeds of 224 gbps in the lab and research is going on. The biggest revolution in the Internet world is going to happen

will require enhanced intelligence to self configure in adhoc networks and having a routing capabilities to route over a packet-switched network.

Fifth Generation (5G) 2019+

5G is the stage succeeds the 4G (LTE/ WiMAx), 3G(umts) and 2G(GSM) syetems. 5G targets to perform the high data rate, reduced latency, energy saving, cost reduction, higher system, capacity, and massive device connectivity. The two phases of 5G, First one will be Release-15 complete by March 2019,Second one Release-16 is expected to complete at March2020, for submission to the ITU(International Telecommunication Union) as a candidate IMT-2020 technology. The ITU IMT – 2020 provides speed up to 20 gigabits per second it has been demonstrated with millimeter waves of 15 gigahertz and higher frequency. 3 GPP standard includes any network using New Radio software. 5G New Radio can access at lower frequencies from 600 MHz to 6 GHz. Speed in the lower frequencies are only modest higher than 4G systems, estimated at 15% to 50% faster.

11.1.3 WLANS 802.11

Wi-Fi stands for Wireless Fidelity. It is a wireless network technology that permits computers and alternative devices to be connected to every alternative into a local area network and to the net without wires and cables. Wi-Fi is additionally stated as wireless local area networkthat stands for wireless local area network, and 802.11, is the technical code for the protocol. See Figure 11.6

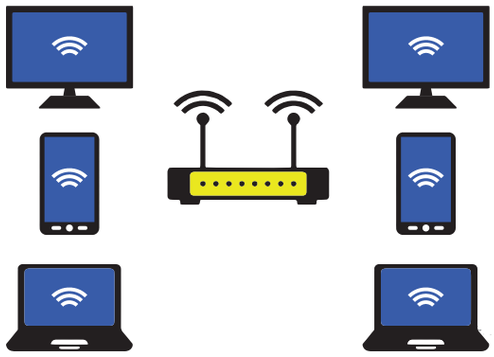

Figure 11.6 Wi-Fi

ADVANTAGES: Benefits of Wi-Fi are

- It provides mobility. Example: I get Internet connection wireless through my laptop computer at home and at work, because of Wi-Fi, hotspots both at home and at work can be used.
- It provides connection to Internet.
- Flexibility of LAN.
- Ensures connectivity.
- It allows remote places to benefit from connectivity.
- Low cost, high benifts.

11.1.4 RFID

- RFID - Radio Frequency Identification.

RFID is a technology designed to locate objects (Credit cards, Passports or even livestock) using radio signals.

RFID used radio waves to read and capture information stored on a tag attached to an object. Tag can be read from several feet away and does not need to be in direct-line-of-sight of the reader to be tracked. RFID has been made up of two parts a reader and a tag or a label. RFID tags are installed with a transmitter and receiver.

RFID component on the tags has two parts: a microchip which stores and processes the information, and the antenna

to receive and transmit a signal. The Tag replies the information from its memory bank. The reader will transmit to read the result to RFID computer program.

Two types of RFID tags were Active RFID and Passive RFID systems.

1. In a passive RFID tag, the power is supplied by the reader when radio waves from the reader are encountered by a passive RFID tag, the coiled antenna forms a magnetic field.
2. Battery powered RFID tag is installed with small battery that powers the broadcast of information

Main Components of a RFID System

- **A RFID tag:** It has silicon microchip attached to a small antenna and mounted on a substrate. See Figure 11.7

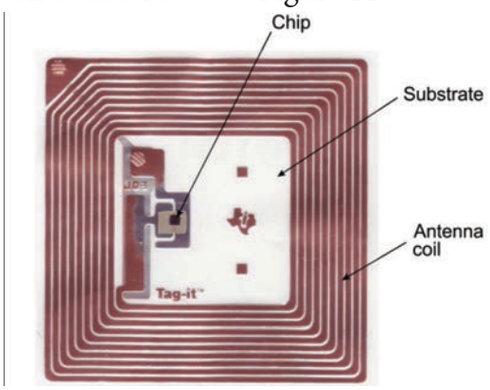

Figure 11.7 RFID Tag

- **A reader:** It has a scanner with antennas to transmit and receive signals, used for communication. See Figure 11.8

Figure 11.8 An RFID Reader

- **A Controller**: It is the host computer with a Microprocessor which receives the reader input and process the data.

Two types of RFID Systems:

1. **Active RFID system:** The tag has its own power source. These systems are used for larger distances and to track high value goods like vehicles.
2. **Passive RFID system:** The tag gets power from a reader antenna to the tag antenna. They are used for shorter range transmission.

11.2 Reference Model

11.2.1 OSI Model

Open System Interconnection (OSI) model was found in the year 1934, general framework that enables network protocols along with software and systems to be developed based on general set of guidelines. It describes the standards for the inter-computer communication. See Figure 11.9

X6CHR4

TIPS

There are many prompts used to remember the OSI layer order:

- Everyone Needs Data Processing.
- Everyone Should Try New Diet Pepsi.

OSI Layers:

1. **Physical Layer:** This is the 1st layer, it defines the electrical and physical specifications for devices.
2. **Data Link Layer:** It is the 2nd layer and it guarantees that the data transmitted

	OSI Layer	TCP/IP	Datagrams are called
Software	Layer 7 Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	Upper Layer Data
	Layer 6 Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	Layer 5 Session	NetBIOS, SAP, Handshaking connection	
	Layer 4 Transport	TCP, UDP	Segment
	Layer 3 Network	IPv4, IPv6, ICMP, IPSec, MPLS, ARP	Packet
Hardware	Layer 2 Data Link	Ethernet, 802.1x, PPP, ATM, Fiber Channel, MPLS, FDDI, MAC Addresses	Frame
	Layer 1 Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	Bits

Figure 11.9 OSI LAYERS

are free of errors. This layer has simple protocols like "802.3 for Ethernet" and "802.11 for Wi-Fi".

3. **Network Layer:** It is the 3rd layer determining the path of the data packets. This layer is responsible for routing of data packets using **IP Addressing**.
4. **Transport Layer:** It is the 4th layer that guarantees the transportation/sending of data successfully. It includes the error checking operation.
5. **Session Layer:** It is the 5th layer, identifies the established system session between different network entities. It controls dialogues between computers .For instance, while accessing a system remotely, session is created between your computer and the remote system.
6. **Presentation Layer:** It is the 6th layer that does the translation of data to the next layer (Prepare the data to the Application Layer). Encryption and decryption protocols occur in this layer such as, Secure Socket Layer (SSL).
7. **Application Layer:** It is the 7th layer, which acts as the user interface platform comprising of software within the system.

11.2.2. TCP / IP

Transmission Control Protocol/Internet Protocol, **TCP/IP** is a set of protocols which governs communications among all computers on the Internet. TCP/IP protocol tells how information should be packaged, sent, and received, as well as how to get to its destination. See Figure 11.10

TCP WORKING: TCP/IP is a combination of two protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). The Internet Protocol typically specifies the logistics of the packets that are sent out over networks; it specifies the packets which have to go, where to go and how to get there. The Transmission Control Protocol is accountable for guaranteeing the trustworthy transmission of data. It checks if any packet is not transmitted and submits it again.

Frequent TCP/IP Protocols

- **HTTP** – It is used between a web client and a web server and it guarantees non-*secure* data transmissions.

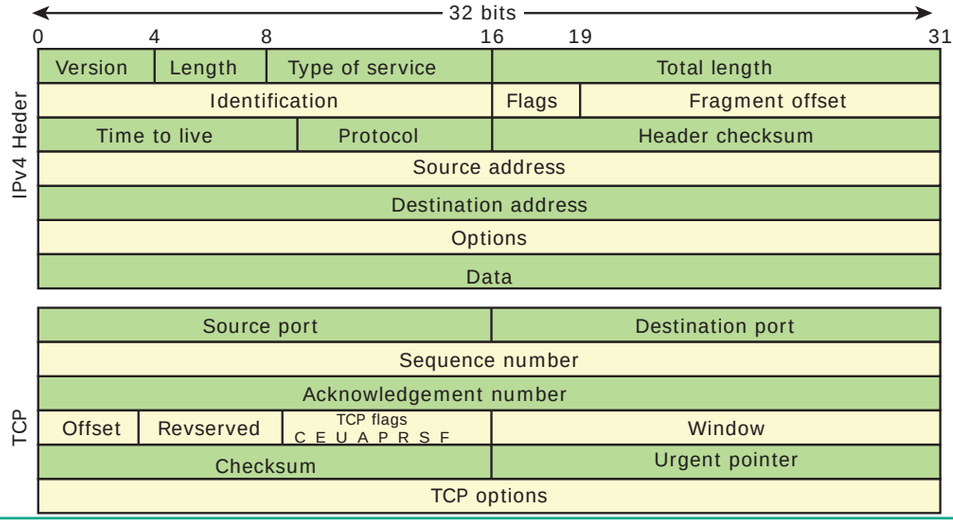

Figure 11.10 TCP/IP Layer

- **HTTPS** – It is used between a web client and a web server ensures *secure* data transmissions.
- **FTP** – It is used between computers for sending and receiving file.

Domain Names and TCP/IP Addresses

The address for any website is not as easy as to remember, domain name are used instead. For example, **216.58.216.164** is one of the IP address for Google and **google.com** is the domain name.

The Different Layers of TCP / IP

There are four total layers of TCP/IP protocol, each of which is listed below with a brief description.

- **Network Access Layer** - concerned with building packets.
- **Internet Layer** - describes how packets are to be delivered.
- **Transport Layer** - ensure the proper transmission of data.
- **Application Layer** - application network processes. These processes include File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).

11.2.3 Other Network Protocols

Network protocols other than OSI and TCP/IP were simply known as other network protocols which implements security over the network communication that include **HTTPs, SSL,** and **SFTP**. Other networks similarly classified in network layer are **IP, ARP, ICMP,IGMP,** at transport layer are **TCP,UDP** at Application Layer are **HTTP, FTP, Telenet, SMTP,** and **DNS.**

HTTPS positions for Hypertext Transfer Protocol Secure. It's a protocol where encoded data transfer on a secure connection. This HTTPS make data more safe and provides data security over the network mainly on public networks like Wi-Fi. See Figure 11.11

For example, let us take a bank website, when we go to login page, we may watch an HTTPS in address bar with some specific design. HTTPS mainly deals with financial transactions or transfer users personal data highly sensitivily. Banking websites are common examples for HTTPS. Data exchanged between the user and the website is not stolen, read or altered by a third party.

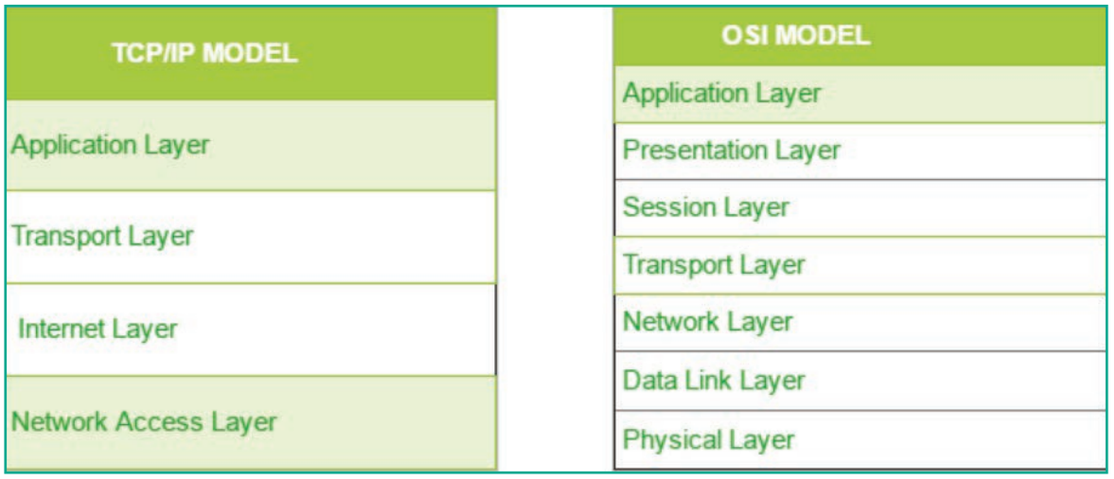

Figure 11.11 Network Layers

In layman's terms, HTTPS gurantees that users watch websites that they want to watch. Data exchanged between the user and the website is not read, stolen or tampered by a third party. But it can't encrypt everything - it has some limitations too. For example, HTTPS can't encrypt host addresses and port numbers.

TCP/IP procedures are based on a layered framework. TCP/IP has four layers. See Figure 11.12

Network Interface Layer

It is the bottommost level layer. It is comparable to that of the Open System Interconnection Physical and Data Link layers. Different TCP/IP protocols are being used at this layer, Ethernet and Token Ring for local area networks and protocols such as X.25, Frame Relay, and ATM for wide area networks. It is assumed to be an unreliable layer.

Network Layer

It is the layer where data is addressed, packaged, and routed among networks. The important Internet protocols that operate at the Network layer are:

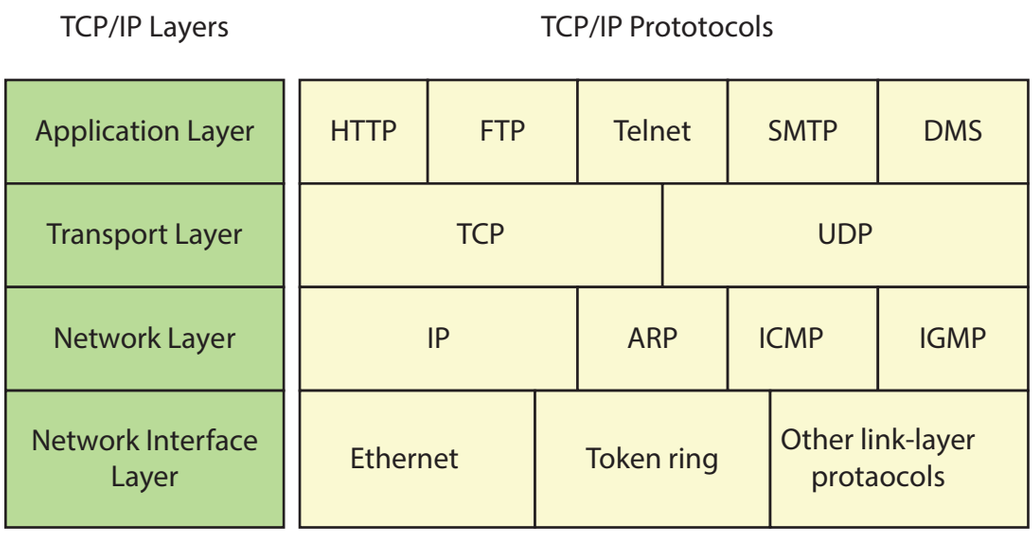

Figure 11.12 TCP/IP Protocols

- **Internet Protocol (IP):** Routable protocol which uses IP addresses to deliver packets. It is an unreliable protocol, does not guarantee delivery of information. **Address Resolution Protocol (ARP):** Resolves IP addresses to MAC (Medium Access Control) addresses. (A MAC address is a hardware identification number that uniquely identifies each device on a network.)i.e., to map IP network addresses to the hardware addresses. **Internet Control Message Protocol (ICMP):** Used by network devices to send error messages and operational information. Example: A host or router might not be reached or a request service is not presented.
- **Internet Group Management Protocol (IGMP):** It is a communication protocol used by hosts and routers to send Multicast (group Communication) messages to multiple IP addresses at once.

Transport Layer

The sessions are recognized and data packets are swapped between hosts in this layer. Two main protocols established at this layer are:

- **Transmission Control Protocol (TCP):** Provides reliable connection oriented transmission between two hosts. It ensures delivery of packets between the hosts. **User Datagram Protocol (UDP):** Provides connectionless, unreliable, one-to-one or one-to-many delivery.

Application Layer

The Application layer of the TCP/IP model is similar to the Session, Presentation, and Application layers of the OSI Reference Model. The most popular Application layer protocols are:

Hypertext Transfer Protocol (HTTP): The core protocol of the World Wide Web. **File Transfer Protocol (FTP):** enables a client to send and receive complete files from a server. **Telnet:** connect to another computer on the Internet. **Simple Mail Transfer Protocol (SMTP):** Provide e-mail services. **Domain Name System (DNS):** Refer to other host computers by using names rather than numbers.

POINTS TO REMEMBER

- The Internet is a network of global connections – comprising private, public, business, academic and government networks – linked by guided, wireless and fiber-optic technologies.
- ARPANET was Advanced Research Projects Agency (ARPA) of the U.S. government in 1969 and was first recognized
- **INTRANET:** It is a private network within an enterprise to share company data and computing resources between the employees.
- **EXTRANET:** It is a private network that uses Internet technology and the public telecommunication system to securely share business's information with suppliers, vendors, partners, customers, or other businesses.

- Communication over mobile network is be made up of voice, data, images and text messages.
- RFID –(**R**adio **F**requency **Id**entification) uses **RF** wireless technology to **identify**.
- Open System Interconnection (OSI) model was found in the year 1934, over all basis that permits network protocols along with software and schemes to be developed based on Universal guidelines.
- **Transmission Control Protocol/Internet Protocol**, **TCP/IP** is a set of protocols permitting communications among all computers on the Internet.
- **HTTP** – A protocol used between a web client and a web server protects non-*secure* data transmissions. The core protocol of the World Wide Web.
- **HTTPS** - A protocol used between a web client and a web server permits *secure* data transmissions.
- **FTP** - Used between computers for sending and receiving data. Enables a client to send and receive complete files from a server.
- **Internet Protocol (IP):** routable protocol which uses IP addresses to deliver packets. It is an unreliable protocol, does not guarantee delivery of information.
- **Address Resolution Protocol (ARP):** Resolves IP addresses to MAC (Medium Access Control) addresses.(A MAC address is a hardware identification number that uniquely identifies each device on a network.)
- **Internet Control Message Protocol (ICMP):** Used by network devices to send error messages and operational information.
- **Transmission Control Protocol (TCP):** Provides reliable connection oriented transmission between two hosts. It guarantees delivery of packets between the hosts.
- **Simple Mail Transfer Protocol (SMTP):** Provides e-mail services.
- **Domain Name System (DNS):** A method of refering to other host computers by using names rather than numbers.

A-Z GLOSSARY

Internet	Several networks, small and big all over the world, are connected together to form a Global network called the Internet.
Intranet	It is a website used by organizations to provide a place where employees can access company related information.
Extranet	It is a private network using Internet technology to share part of business information with supplier's partners and customers.
APRANet	Advanced Research Projects Agency Network
TCP/IP	Transmission Control Protocol / Internet Protocol

Wi-Fi	Wireless Fidelity.
RFID	Radio Frequency Identification.
OSI	Open System Interconnection
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
FTP	File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
UDP	User Datagram Protocol
SMTP	Simple Mail Transfer Protocol
DNS	Domain Name System

EVALUATION

LYK75V

Part - I

Choose the correct answer

1. Which one of the following will be easy way to use Internet technology and the public telecommunication system to securely share business's information with suppliers, vendors, partners and customers.

   a) Extranet b) Intranet

   c) arpanet d) arcnet

2. Match the following and choose the correct answer

   i. HTTP -The core protocol of the World Wide Web.

   ii. FTP- enables a client to send and receive complete files from a server.

   iii. SMTP - Provide e-mail services.

   iv. DNS- Refer to other host computers by using names rather than numbers.

   a) i, ii, iii, iv b) ii, iii, iv, i

   c) iii, iv, i, ii d) iv, iii, ii, i

3. Communication over ----------
   ------is be made up of voice, data, images and text messages.

   a) Social media

   b) mobile network

   c) whatsapp

   d) software

4. Wi-Fi stands for----------

   a) Wireless Fidelity

   b) wired fidelity

   c) wired optic fibre

   d) wireless optic fibre

5. A TCP/IP network with access restricted to members of an organization

   a) LAN b) MAN

   c) WAN d) Intranet

6. RFID stands for ----------
   a) Radio Free identification
   b) real Frequency identity
   c) Radio Frequency indicators
   d) Radio Frequency Identification.
7. It guarantees the sending of data is successful and which checks error on operation at OSI layer is----------
   a) Application layer
   b) Network layer
   c) Transport Layer
   d) Physical layer
8. Which one of the following will secure data on transmissions
   a) HTTPS b) HTTP
   c) FTP d) SMTP
9. ---------- provides e-mail service
   a) DNS b) TCP
   c) FTP d) SMTP
10. ---------- refer to other host computers by using names rather than numbers.
    a) DNS b) TCP
    c) FTP d) SMTP

Part - II

Short Answers

1. Define Intranet
2. What is the uses of mobile networks?
3. List out the benefits of WiFi
4. How many types of RFID system available and what are they?
5. Expand HTTP, HTTPS, FTP.

Part - III

Explain in Brief Answer

1. Compare Internet, Intranet and Extranet
2. List out the components of a RFID enabled system.
3. Write short notes on HTTP, HTTPS, FTP.
4. What are the layers available in TCP/IP Reference Model?
5. Expand ARP, ICMP, SMTP and DNS.

Part - IV

Explain in detail

1. Explain about Internet, Intranet and Extranet.
2. Discuss about OSI model with its layers.
3. Difference between TCP/IP and OSI Reference Model.
4. Explain about the development, merits and demerits in Mobile networks.

STUDENT ACTIVITIES

List out some web address with http and https

1. Find some of the http web addresses
2. Give some example for https
3. Can you know difference between http and https.