Pune Institute of Computer Technology, Pune-43
DEPARTMENT OF INFORMATION TECHNOLOGY
(Academic Year – 2024-25 Sem-II)
UNIT TEST - I

Subject: Computer Networks & Security — Subject Code: 314451
Class: TE — Div.: IX, X, XI — [Max. Marks: 30]
Date: 10/02/2025 — Day: Monday — Duration: 1 Hour

Instructions to the candidate:

1. All questions are compulsory
2. Draw neat diagram wherever necessary.

Que. No.	Questions	Max Marks	CO Mapped	Bloom's Learning Level
1-a	What is FTP? Where and when is it used? Why does it require 02 ports? Explain at least 05 user commands used in FTP?	08	CO-I	L2
1-b	Define DNS. Explain how name resolution happens in DNS. Enlist all the resource records and its functions.	07	CO-I	L2
2-a	State the differences between IEEE 802.11 and IEEE 802.15.	05	CO-II	L1
2-b	Discuss the hidden and exposed station problems in MAC of 802.11.	05	CO-II	L2
2-c	Explain with the help of a neat diagram the architecture of Bluetooth.	05	CO-II	L2

Course Outcomes (CO Mapped):

CO-I	Students will be able to describe, compare and analyze the responsibilities, services offered, and protocol used at application layer of network.
CO-II	Students will be able to discuss the working principle of wireless network and distinguish between different wireless standards.

Bloom's Taxonomy (Bloom's Learning Level):

L1	Remembering	Recall specific facts
L2	Understanding	Grasp meaning of materials
L3	Applying	Use information in a new situation
L4	Analyzing	Identify schemas or relationships
L5	Evaluating	Use information to make judgments
L6	Creating	Create or develop something new

----------******----------

Pune Institute of Computer Technology, Pune-43
DEPARTMENT OF INFORMATION TECHNOLOGY
(Academic Year – 2024-25 Sem-II)
UNIT TEST - I

Subject: **COMPUTER NETWORKS & SECURITY** Subject Code: 314451
Date: 10/02/2025 Day: Monday Duration: 1 Hour

SOLUTION

1-a What is FTP? Where and when is it used? Why does it require two ports? Explain at least five user commands used in FTP.

File Transfer Protocol (FTP) is a standard network protocol used to transfer files between a client and a server over a network (such as the Internet or a local network). It operates using a client-server architecture and relies on TCP (Transmission Control Protocol) for reliable data transmission.

FTP is used in various scenarios, including:

1. Website Management – Web developers use FTP to upload, update, and manage website files on web servers.
2. Remote File Sharing – Organizations use FTP servers to store and share large files among employees.
3. Backup and Storage – FTP is used to back up important data to a remote server.
4. Software Distribution – Companies and developers use FTP to distribute large software updates and patches.
5. Data Exchange – FTP facilitates bulk data transfer between businesses or institutions.

FTP requires two ports:

1. Control Port (Port 21) – Used for sending commands and responses between the client and server.
2. Data Port (Port 20 or a dynamically assigned port) – Used for transferring actual files.

Active vs. Passive Mode:

- **Active Mode**:
  - Client connects from a random high port (1024–65535) to **server port 21** (control).
  - Server connects from **port 20** to the client's specified port for data transfer.
- **Passive Mode**:
  - Client connects from a random high port to **server port 21** (control).
  - Server assigns a random high port (1024–65535) for data transfer, which the client connects to.

The separation of control and data connections allows FTP to manage multiple file transfers efficiently without interfering with the control session.

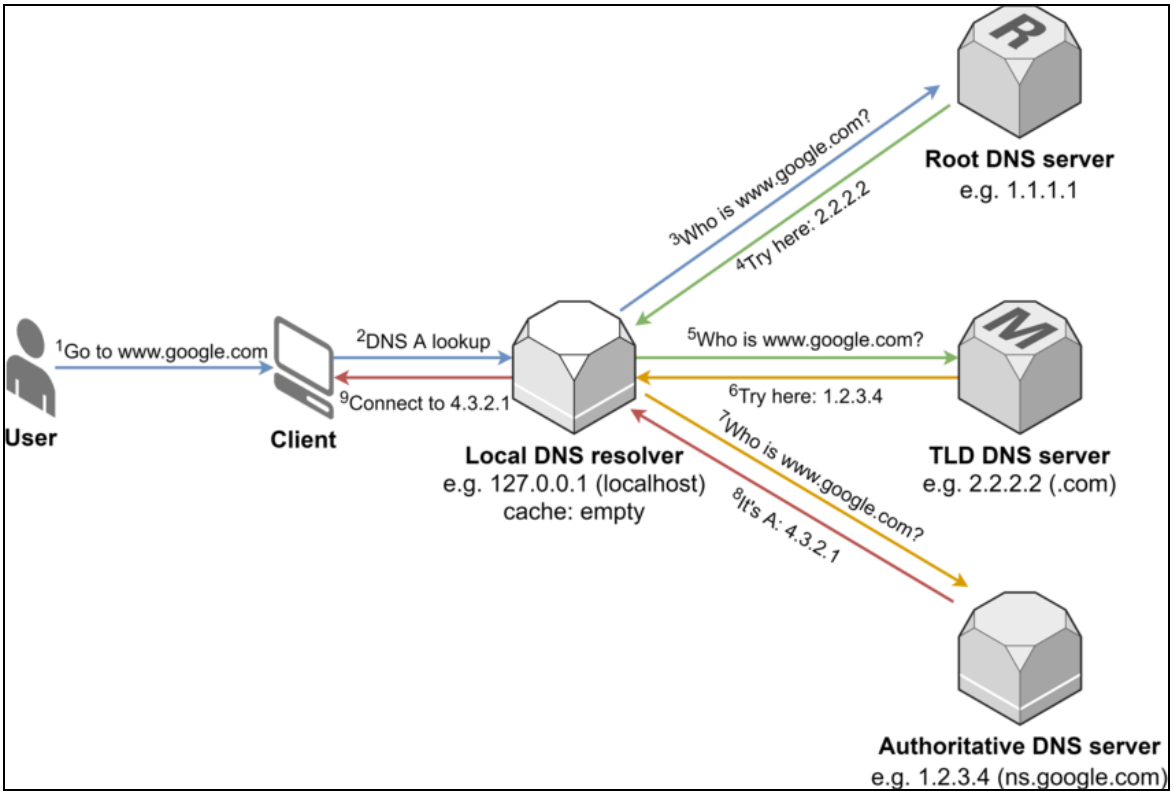
Five Common FTP User Commands:

1. USER – Used to send the username for authentication. Example: USER username
2. PASS – Sends the password for authentication. Example: PASS password
3. LIST – Displays the list of files and directories in the current directory. Example: LIST
4. RETR – Downloads a file from the server to the client. Example: RETR filename.txt
5. STOR – Uploads a file from the client to the server. Example: STOR filename.txt

---

1-b Define DNS. Explain how name resolution happens in DNS. Enlist all the resource records and their functions.

Domain Name System (DNS) is a hierarchical and distributed naming system that translates human-readable domain names (e.g., www.google.com) into IP addresses (e.g., 142.250.190.46), allowing computers to locate and communicate with each other over networks.



DNS Name Resolution

DNS Name Resolution Process

1. **User Request** – The user enters a domain name (e.g., www.example.com) in the web browser.
2. **Local DNS Cache Check** – The system first checks if the requested domain's IP address is stored in its local cache.
3. **Recursive Query to Resolver** – If not found, the request is sent to a recursive DNS resolver (provided by the ISP).
4. **Root Server Query** – If the resolver doesn't have the IP address, it queries the root DNS servers.
5. **TLD Server Query** – The root server directs the query to the Top-Level Domain (TLD) server (.com, .org, etc.).
6. **Authoritative Name Server Query** – The TLD server directs the request to the authoritative DNS server for the domain.
7. **Final Response** – The authoritative DNS server provides the IP address, which is sent back to the client.
8. **Page Load** – The browser uses the retrieved IP to establish a connection and load the website.

DNS Resource Records and Their Functions

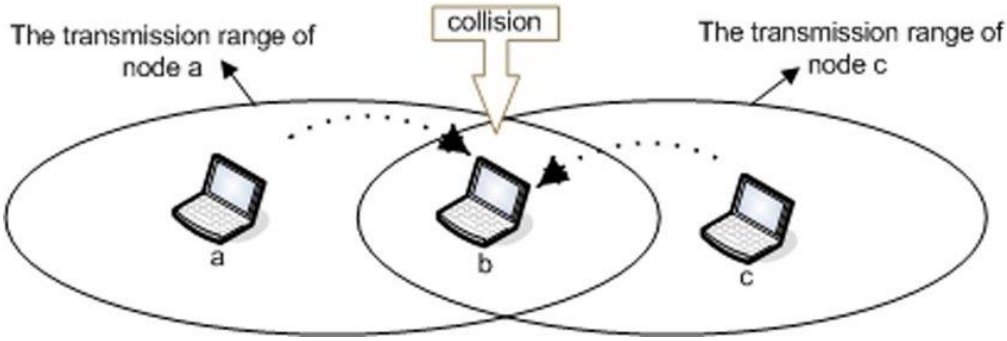
1. A (Address Record) – Maps a domain name to an IPv4 address.
2. AAAA (IPv6 Address Record) – Maps a domain name to an IPv6 address.
3. CNAME (Canonical Name Record) – Maps an alias domain name to a canonical domain name.
4. MX (Mail Exchange Record) – Specifies mail servers for handling email for a domain.
5. NS (Name Server Record) – Specifies the authoritative name servers for a domain.
6. PTR (Pointer Record) – Maps an IP address to a domain name (used in reverse DNS lookup).
7. TXT (Text Record) – Stores arbitrary text data, often used for verification and security purposes.
8. SRV (Service Record) – Specifies a host and port for specific services like SIP or XMPP.

2-a State the differences between IEEE 802.11 and IEEE 802.15.

Feature	802.11 (WiFi)	802.15 (Bluetooth)
Standard	IEEE 802.11	IEEE 802.15.1 (Classic Bluetooth) & 802.15.4 (Zigbee)
Primary Use	Wireless LAN (Internet, networking)	Short-range device communication
Frequency	2.4 GHz, 5 GHz, 6 GHz (WiFi 6E)	2.4 GHz
Range	30-100 meters (depending on version)	1-10 meters (Class-dependent)
Speed	Up to 9.6 Gbps (WiFi 6)	Up to 3 Mbps (Classic Bluetooth), 2 Mbps (BLE)
Power Consumption	Higher (for continuous connectivity)	Lower (optimized for battery efficiency)
Number of Devices	Supports many devices on a network	Limited device pairing (typically 7 active)
Network Type	Infrastructure or ad-hoc mode	Piconet (1 master, 7 active slaves)
Latency	Low (~1–10 ms)	Higher (~100 ms for Classic, ~5 ms for BLE)
Typical Applications	Internet browsing, streaming, gaming, IoT	Wireless headsets, file transfer, IoT, wearables
Connectivity	Supports multiple devices via routers	Peer-to-peer or small networks (piconet)
Use Case	Internet access, large file transfer, streaming	Short-range communication, peripherals, IoT
Security	WPA2, WPA3 encryption	AES encryption, pairing security
Topology	Infrastructure (Access Point) & Ad-hoc	Point-to-point, Piconet (1 master, up to 7 slaves)

2-b Discuss the hidden and exposed station problems in MAC of 802.11.

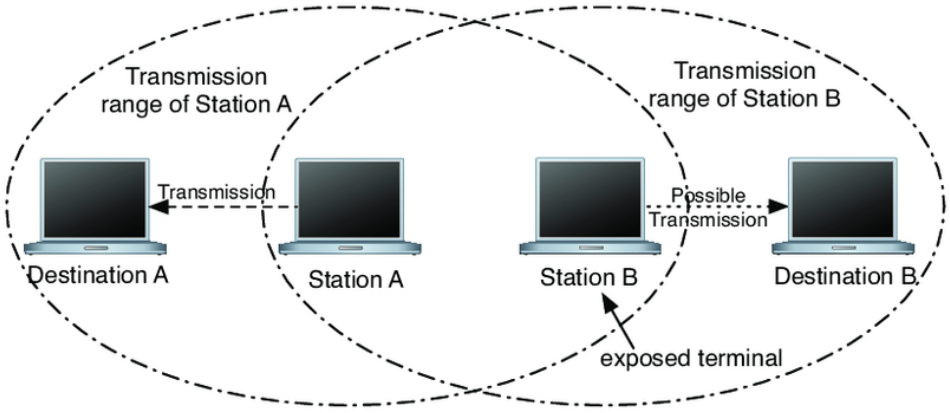
Hidden Station Problem



station B and C both covers station A in their own range. Each station B and C can send data to station A separately. Both stations B and C are outside of range of each other. Suppose station B is sending data to station A and in middle of transmission station C also has to send data to station A. Since station B and station C are out of each other range therefore station C thinks that station A is free. Station C send data to station A and collision occurs at station A.

Solution: The RTS/CTS (Request to Send / Clear to Send) mechanism helps by ensuring only one station transmits at a time.

Exposed Station Problem



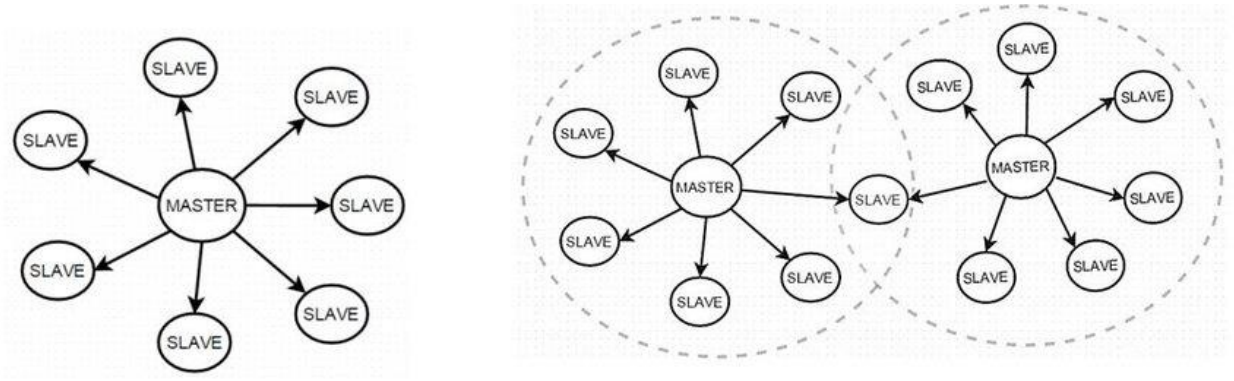
assume there are four stations with the names A, B, C, and D, where B and C are transmitters and A and D are receivers. The stations are set up so that the two emitters B and C can hear each other but the two receivers A and D cannot hear each other over radio waves. Transmission from B to A is happening. As a result, C ceases attempting to transmit to D after mistakenly assuming that the above transmission will cause interference. However, since the communication from C to D is outside of B's range, interference would not have happened. Known as the exposed terminal issue.

Solution: Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) allows stations to intelligently decide whether they can transmit.

2-c Explain with the help of a neat diagram the architecture of Bluetooth.

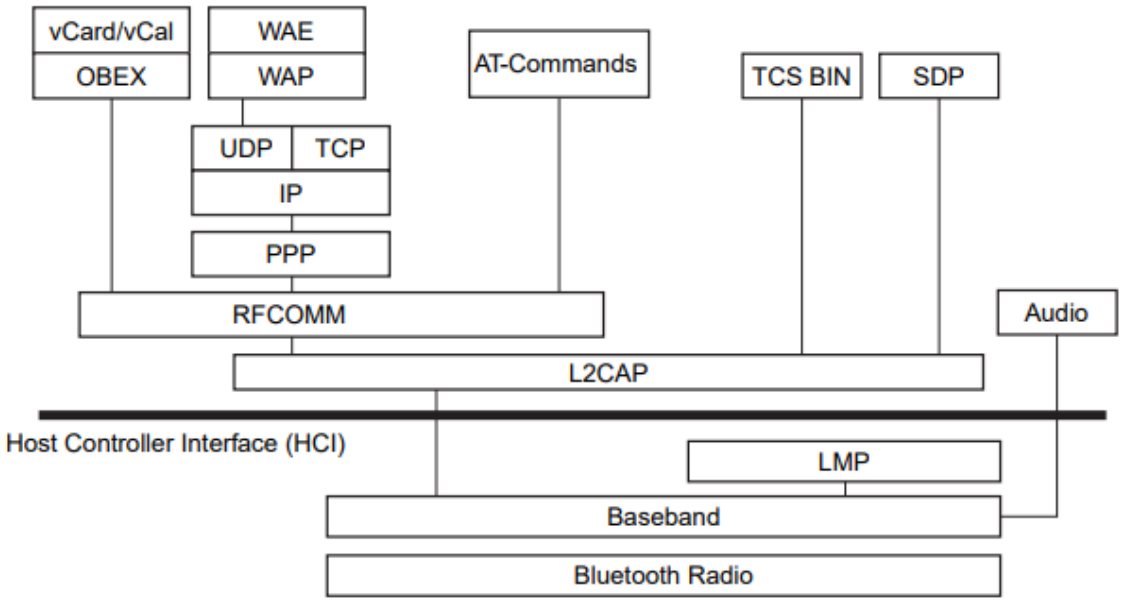
Bluetooth Architecture Components:

1. Piconet: A small network with one master device and up to seven active slave devices.
2. Scatternet: A group of multiple piconets connected through shared devices.



a) Piconet b) Scatternet with 2 piconets

3. Master-Slave Communication: The master controls communication, while slaves follow its commands.



Bluetooth Protocol Stack

Protocols in the Bluetooth Protocol Stack

1. **Core protocols** − This includes Bluetooth radio, Baseband, Link Manager Protocol (LMP), Logical Link Control and Adaptation Protocol (L2CAP), and Service Discovery Protocol (SDP).
2. **Cable Replacement Protocol** − This includes Radio Frequency Communications (RFComm) protocol. It is short for Radio Frontend Component. It provides a serial interface with WAP.
3. **Adopted Protocols** − These are the protocols that are adopted from standard models. The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).
4. **AT Commands** − ATtention command set.

Functions of the Core Protocols

- **Radio** − This is a physical layer equivalent protocol that lays down the physical structure and specifications for transmission of radio waves. It defines air interface, frequency bands, frequency hopping specifications and modulation techniques.
- **Baseband** − This protocol takes the services of radio protocol. It defines the addressing scheme, packet frame format, timing, and power control algorithms.
- **Link Manager Protocol (LMP)** − LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.
- **Logical Link Control and Adaptation Protocol (L2CAP)** − L2CAP provides adaption between upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.
- **Service Discovery Protocol (SDP)**− SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.