Hall Ticket Number:

III/IV B.Tech(Regular) DEGREE EXAMINATION

FEBRUARY, 2021 **Electronics & Communication**

Fifth Semester **DATA COMMUNICATION AND COMPUTER NETWORKS**

Time: Three Hours **Maximum:**50 Marks

Answer Question No.1 compulsorily. (10X1 = 10 Marks)

Answer ONE question from each unit. (4X10=40 Marks)

1.	Answer all questions		(10X1=10 Marks)	
	a)	What are the service primitives? There are five types of service primitives: 1. LISTEN : When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection. 2. CONNECT : It connects the server by establishing a connection. Response is awaited. 3. RECIEVE: Then the RECIEVE call blocks the server. 4. SEND : Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message. 5. DISCONNECT : This primitive is used for terminating the connection. After this primitive one can’t send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client. When the server package is received by client then the process is terminated.	CLO-1	1M
	b)	What are the types of guided transmission media? 1. Magnetic Media 2. Twisted Pair Cable 3. Co-axial Cable 4. Power Lines 5. Fibre Optic Cable	CLO-1	1M
	c)	What is a Computer Network? A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data and applications.	CLO-1	1M
	d)	What are different types of Sliding Window Protocols? **Sliding window protocol has two types:** • Go-Back-N ARQ. • Selective Repeat ARQ.	CLO-2	1M
	e)	What is hidden terminal problem? In wireless LANs (wireless local area networks), the hidden terminal problem is a transmission problem that arises when two or more stations who are out of range of each other transmit simultaneously to a common recipient. This is prevalent in decentralised systems where there aren’t any entity for controlling transmissions.	CLO-2	1M

This occurs when a station is visible from a wireless access point (AP), but is hidden from other stations that communicate with the AP.

f) What is Fast Ethernet? — CLO-2 — 1M

Fast Ethernet is popularly named as 100-BASE-X. Here, 100 is the maximum throughput, i.e. 100 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used, which is TX or FX.

g) Compare IPv4 and IPv6. — CLO-3 — 1M

IPv4	IPv6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender

h) Write about Leaky Bucket Mechanism in Traffic Shaping. — CLO-3 — 1M

The **leaky bucket** algorithm is a method of temporarily storing a variable number of requests and organizing them into a set-rate output of packets in an asynchronous transfer mode (ATM) network. The **leaky bucket** is used to implement **traffic policing** and **traffic shaping** in Ethernet and cellular data networks.

i) What is the function of intracoded frame (I-frame) ? — CLO-4 — 1M

Intraframe **coding** is used to represent an individual **frame** independently. The scheme used for intraframe **coding** is essentially identical to JPEG image compression. An intraframe-**coded** picture in the video sequence is referred to as an **intra**-picture (I-picture).

j) What is the function of H.323 — CLO-4 — 1M

H. 323 provides standards for equipment, computers and services for multimedia **communication** across packet based networks and specifies transmission protocols for real-time video, audio and data details. H. 323 is widely used in IP based videoconferencing, Voice over Internet Protocol (VoIP) and Internet telephony.

UNIT I

2. Describe about the TCP/IP reference model. Explain about each layer clearly — CLO-1 — 10M

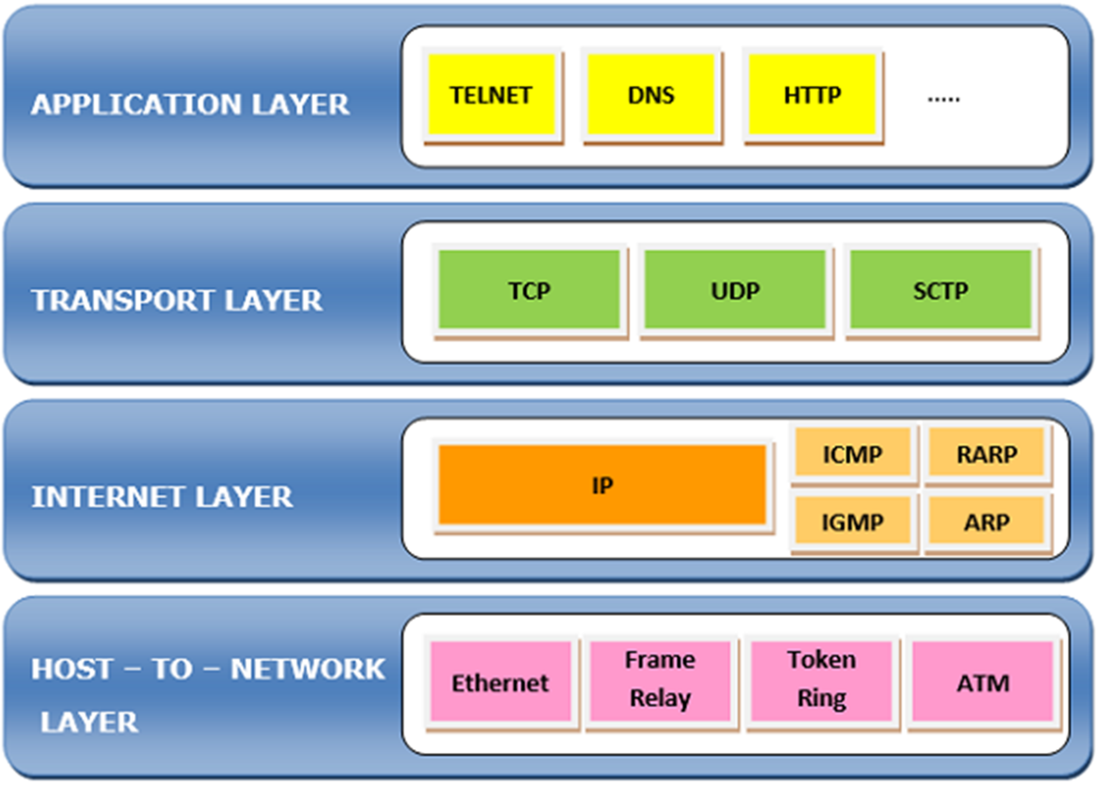
TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are −

- **Host-to- Network Layer −**It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.

- **Internet Layer** −It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer** − It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer** − This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

The following diagram shows the layers and the protocols in each of the layers −



(OR)

3. Explain in detail about types of wireless transmission. CLO-1 10M

Many users opt for wireless transmission media because it is more convenient than installing cables. In addition, businesses use wireless transmission media in locations where it is impossible to install cables. Types of wireless transmission media used in communications include infrared, broadcast radio, cellular radio, microwaves, and communications satellites.

Infrared

As discussed earlier in the chapter, infrared (IR) is a wireless transmission medium that sends signals using infrared light waves. Mobile computers and devices, such as a mouse, printer, and smart phone, often have an IrDA port that enables the transfer of data from one device to another using infrared light waves.

Broadcast Radio

Broadcast radio is a wireless transmission medium that distributes radio signals through the air over long distances such as between cities, regions, and countries and short distances such as within an office or home. Bluetooth, UWB, Wi-Fi, and WiMAX communications technologies discussed earlier in this chapter use broadcast radio signals.

Cellular Radio

Cellular radio is a form of broadcast radio that is used widely for mobile communications, specifically wireless modems and cell phones. A cell phone is a telephone device that uses high-frequency radio waves to transmit voice and digital data messages.

Some mobile users connect their notebook computer or other mobile computer to a cell phone to access the Web, send and receive e-mail, enter a chat room, or connect to an office or school network while away from a standard telephone line. Read Looking Ahead 8-2 for a look at the next generation of cellular communications.

Personal Communications Services (**PCS**) is the term used by the United States Federal Communications Commission (FCC) to identify all wireless digital communications. Devices that use PCS include cell phones, PDAs, pagers, and fax machines.

Microwaves

Microwaves are radio waves that provide a high-speed signal transmission. Microwave transmission, often called fixed wireless, involves sending signals from one microwave station to another (shown in Figure 8-1 on page 296). Microwaves can transmit data at rates up to 4,500 times faster than a dial-up modem.

A microwave station is an earth-based reflective dish that contains the antenna, transceivers, and other equipment necessary for microwave communications. Microwaves use line-of-sight transmission. To avoid possible obstructions, such as buildings or mountains, microwave stations often sit on the tops of buildings, towers, or mountains.

Microwave transmission is used in environments where installing physical transmission media is difficult or impossible and where line-of-sight transmission is available. For example, microwave transmission is used in wide-open areas such as deserts or lakes; between buildings in a close geo- graphic area; or to communicate with a satellite. Current users of microwave transmission include universities, hospitals, city governments, cable television providers, and telephone companies. Home and small business users who do not have other high-speed Internet connections available in their area also opt for lower-cost fixed wireless plans.

Communications Satellite

A **communications satellite** is a space station that receives microwave signals from an earth-based station, amplifies (strengthens) the signals, and broadcasts the signals back over a wide area to any number of earth-based stations.

These earth-based stations often are microwave stations. Other devices, such as smart phones and GPS receivers, also can function as earth-based stations. Transmission from an earth-based station to a satellite is an uplink. Transmission from a satellite to an earth-based station is a downlink.

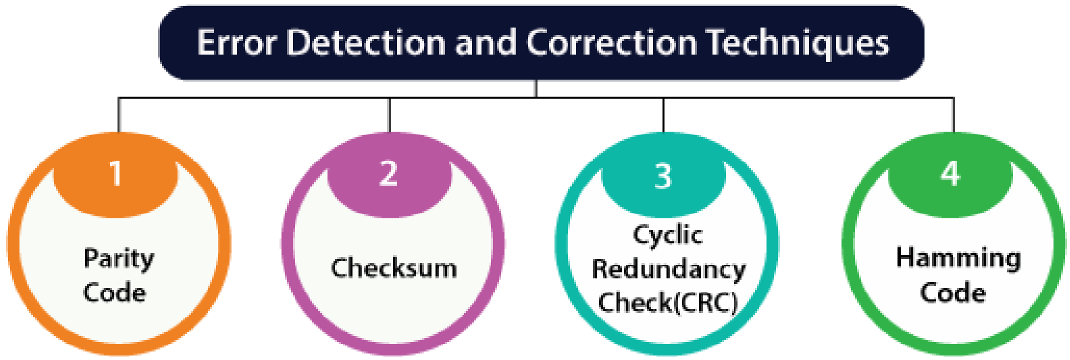
Applications such as air navigation, television and radio broadcasts, weather forecasting, video conferencing, paging, global positioning systems, and Internet connections use communications satellites. With the proper satellite dish and a satellite modem card, consumers access the Internet using satellite technology. With satellite Internet connections, however, uplink transmissions usually are slower than downlink transmissions. This difference in speeds usually is acceptable to most Internet satellite users because they download much more data than they upload. Although a satellite Internet connection is more expensive than cable Internet or DSL connections, sometimes it is the only high-speed Internet option in remote areas.

UNIT II

4.	Explain about different error detecting and correcting codes.	CLO-2	10M

Error detection and correction code plays an important role in the transmission of data from one source to another. The noise also gets added into the data when it transmits from one system to another, which causes errors in the received binary data at other systems. The bits of the data may change(either 0 to 1 or 1 to 0) during transmission.

It is impossible to avoid the interference of noise, but it is possible to get back the original data. For this purpose, we first need to detect either an error **z** is present or not using error detection codes. If the error is present in the code, then we will correct it with the help of error correction codes.



Error detection code

The error detection codes are the code used for detecting the error in the received data **bitstream**. In these codes, some bits are included appended to the original bitstream.

Error detecting codes encode the message before sending it over the noisy channels. The encoding scheme is performed in such a way that the decoder at the receiving can find the errors easily in the receiving data with a higher chance of success.

Parity Code

In parity code, we add one parity bit either to the right of the LSB or left to the MSB to the original bitstream. On the basis of the type of parity being chosen, two types of parity codes are possible, i.e., even parity code and odd parity code.

Features of Error detection codes

These are the following features of error detection codes:

- These codes are used when we use message backward error correction

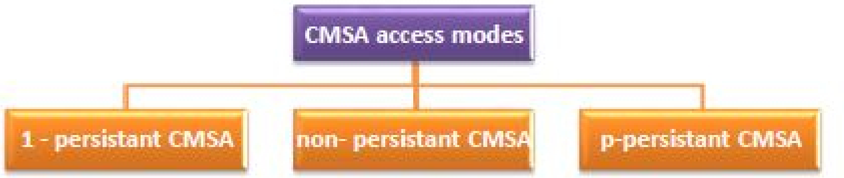
	techniques for reliable data transmission. A feedback message is sent by the receiver to inform the sender whether the message is received without any error or not at the receiver side. If the message contains errors, the sender retransmits the message. o In error detection codes, in fixed-size blocks of bits, the message is contained. In this, the redundant bits are added for correcting and detecting errors. o These codes involve checking of the error. No matter how many error bits are there and the type of error. o Parity check, Checksum, and CRC are the error detection technique. Error correction code Error correction codes are generated by using the specific algorithm used for removing and detecting errors from the message transmitted over the noisy channels. The error-correcting codes find the correct number of corrupted bits and their positions in the message. There are two types of ECCs(Error Correction Codes), which are as follows. Block codes In block codes, in fixed-size blocks of bits, the message is contained. In this, the redundant bits are added for correcting and detecting errors. Convolutional codes The message consists of data streams of random length, and parity symbols are generated by the sliding application of the Boolean function to the data stream. The hamming code technique is used for error correction. **Hamming Code** Hamming code is an example of a block code. The two simultaneous bit errors are detected, and single-bit errors are corrected by this code. In the hamming coding mechanism, the sender encodes the message by adding the unessential bits in the data. These bits are added to the specific position in the message because they are the extra bits for correction.		
	(OR)		
5.	Explain about Carrier Sense Multiple Access Protocols. Carrier Sense Multiple Access (CSMA) is a network protocol for carriertransmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and transmits if the channel is not busy. Using CMSA protocols, more than one users or nodes send and receive data through a shared medium that may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum. **Working Principle** When a station has frames to transmit, it attempts to detect presence of the carrier signal from the other nodes connected to the shared channel. If a carrier signal is detected, it implies that a transmission is in progress. The station waits till the ongoing transmission executes to completion, and then initiates its own transmission. Generally,	CLO-2	10M

transmissions by the node are received by all other nodes connected to the channel.

Since, the nodes detect for a transmission before sending their own frames,collision of frames is reduced. However, if two nodes detect an idle channel at the same time, they may simultaneously initiate transmission. This would cause the frames to garble resulting in a collision.

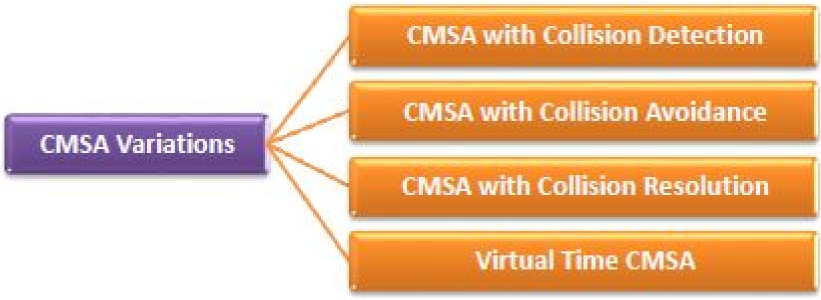
CMSA Access Modes

The versions of CMSA access modes are−



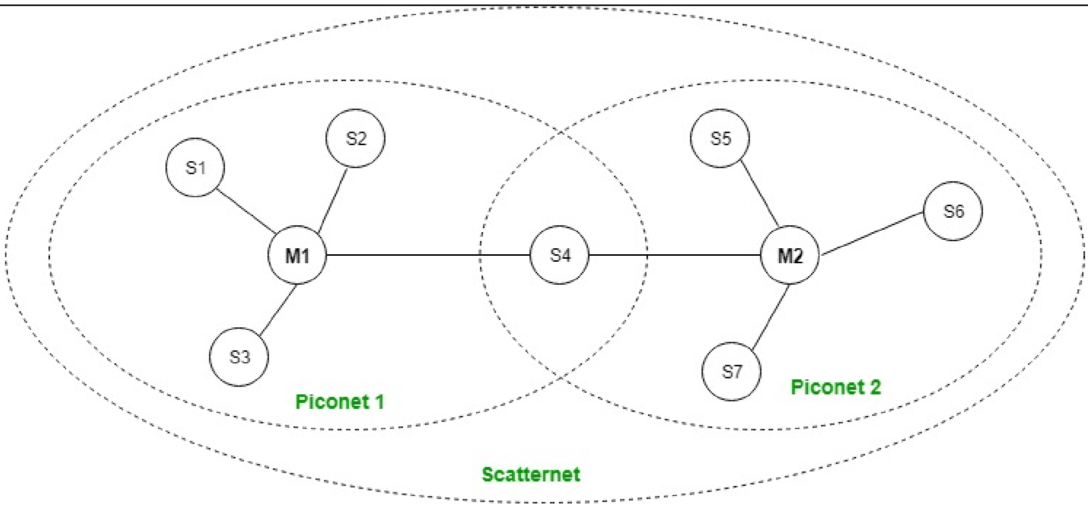
Variations of CMSA protocol

There may be further additions to the basic CMSA protocols. This results is the various protocols as follows−



UNIT III

6.	Explain in detail about Bluetooth. It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum). A bluetooth network is called **piconet** and a collection of interconnected piconets is called **scatternet**. **Bluetooth Architecture:** The architecture of bluetooth defines two types of networks: 1. Piconet 2. Scatternet	CLO-3	10M



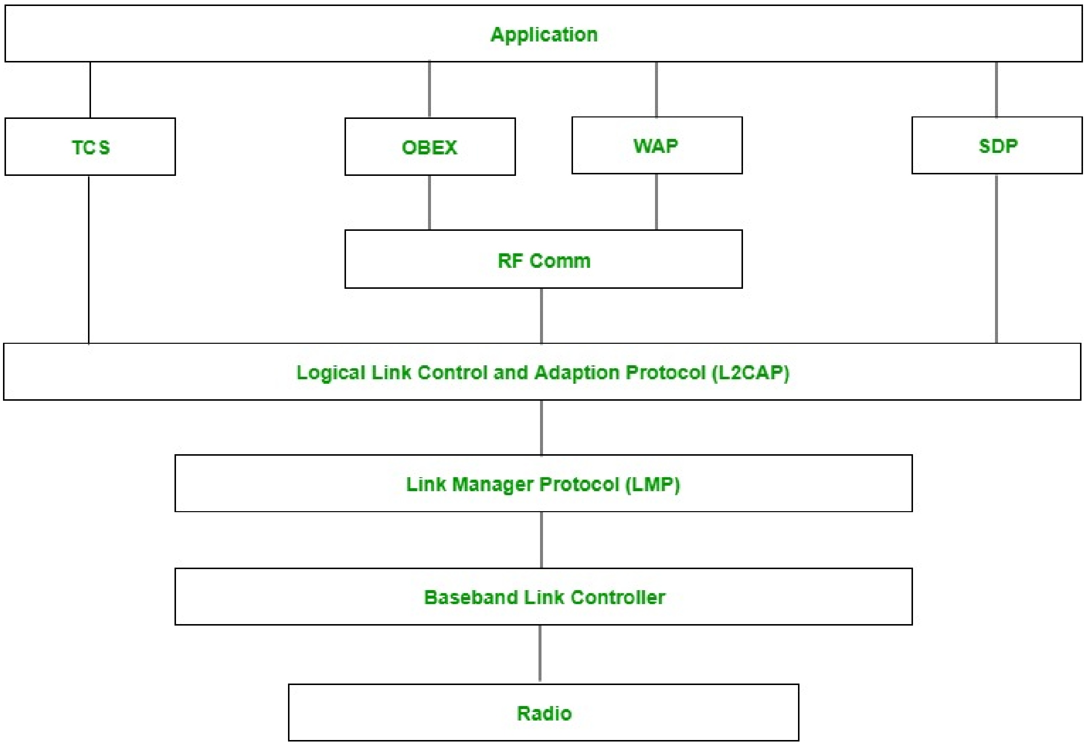
Piconet:

Piconet is a type of bluetooth network that contains **one primary node** called master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there are total of 8 active nodes which are present at a distance of 10 metres. The communication between the primary and secondary node can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also have **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

Scatternet:

It is formed by using **various piconets**. A slave that is present in one piconet can be act as master or we can say primary in other piconet. This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.

Bluetooth protocol stack:

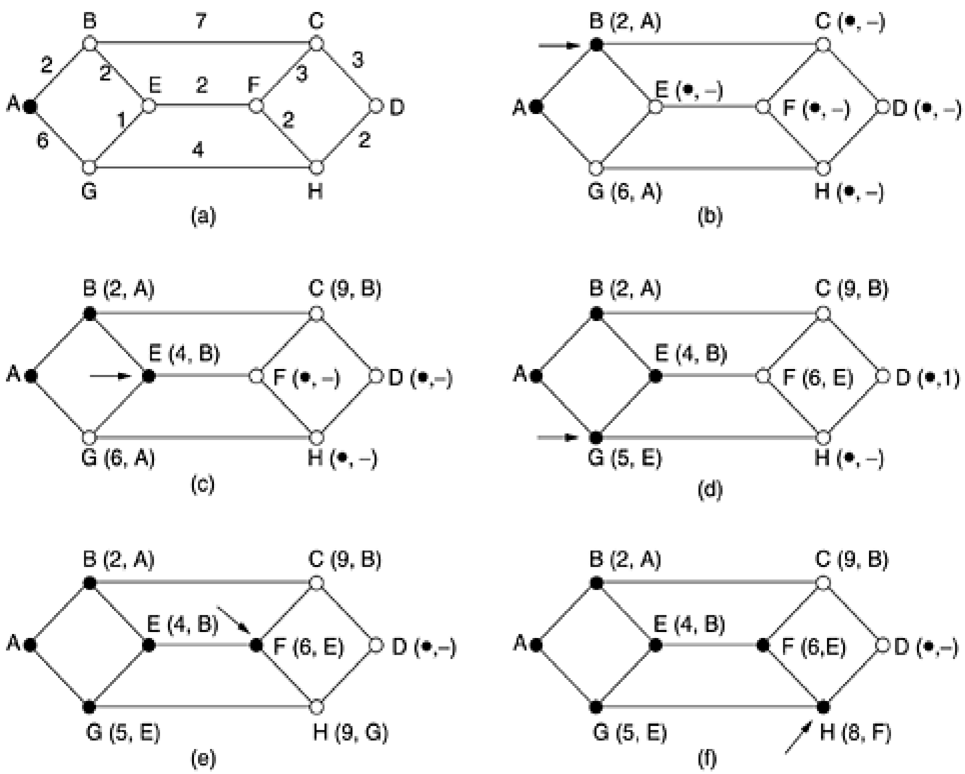


1. **Radio (RF) layer:**

	It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of bluetooth transceiver. It defines two types of physical link: connection-less and connection-oriented. 2. **Baseband Link layer:** It performs the connection establishment within a piconet. 3. **Link Manager protocol layer:** It performs the management of the already established links. It also includes authentication and encryption processes. 4. **Logical Link Control and Adaption protocol layer:** It is also known as the heart of the bluetooth protocol stack. It allows the communication between upper and lower layers of the bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs the segmentation and multiplexing. 5. **SDP layer:** It is short for Service Discovery Protocol. It allows to discover the services available on another bluetooth enabled device. 6. **RF comm layer:** It is short for Radio Frontend Component. It provides serial interface with WAP and OBEX. 7. **OBEX:** It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices. 8. **WAP:** It is short for Wireless Access Protocol. It is used for internet access. 9. **TCS:** It is short for Telephony Control Protocol. It provides telephony service. 10. **Application layer:** It enables the user to interact with the application. **Advantages:** • Low cost. • Easy to use. • It can also penetrate through walls. • It creates an adhoc connection immediately without any wires. • It is used for voice and data transfer. **Disadvantages:** • It can be hacked and hence, less secure. • It has slow data transfer rate: 3 Mbps. • It has small range: 10 meters.		
	(OR)		
7	Explain in detail about Shortest Path Routing Algorithm. **Shortest Path Routing** ➢ It is simple and easy to understand.	CLO-3	10M

- The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line (often called a link).
- To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.
- One way of measuring path length is the **number of hops**.
- Using this metric, the paths *ABC* and *ABE* in Fig. 5-7 are equally long.
- Another metric is the **geographic distance** in kilometers, in which case *ABC* is clearly much longer than *ABE*.

Figure 5-7. The first five steps used in computing the shortest path from* A *to* D. *The arrows indicate the working node.



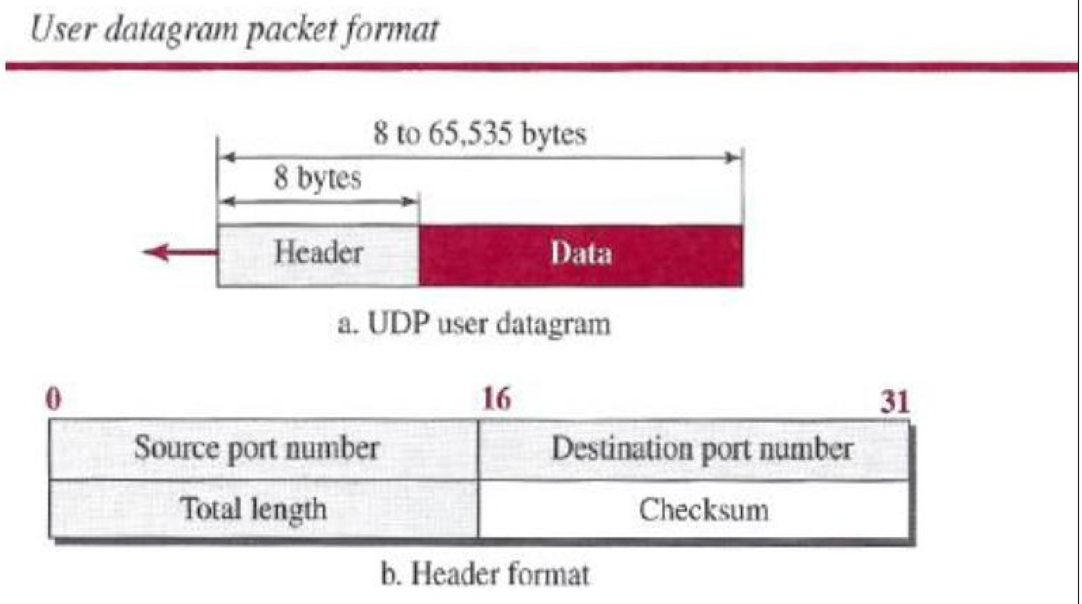
- In the general case, the labels on the arcs could be computed as a function of the **distance**, **bandwidth**, **average traffic**, **communication cost**, **mean queue length**, **measured delay**, and other factors.
- By changing the weighting function, the algorithm would then compute the "shortest" path measured according to any one of a number of criteria or to a combination of criteria.
- Each node is labeled (in parentheses) with its distance from the source node along the best known path. Initially, no paths are known, so all nodes are labeled with infinity.
- As the algorithm proceeds and paths are found, the labels may change, reflecting better paths. A label may be either tentative or permanent. Initially, all labels are tentative.

	➢ When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent and never changed thereafter. ➢ We want to find the shortest path from *A* to *D*. We start out by marking node *A* as permanent, indicated by a filled-in circle. ➢ Then we examine, in turn, each of the nodes adjacent to *A* (the working node), relabeling each one with the distance to *A*. ➢ Whenever a node is relabeled, we also label it with the node from which the probe was made so that we can reconstruct the final path later. ➢ Having examined each of the nodes adjacent to *A*, we examine all the tentatively labeled nodes in the whole graph and make the one with the smallest label permanent, as shown in Fig. 5-7(b). This one becomes the new working node. ➢ We now start at *B* and examine all nodes adjacent to it. If the sum of the label on *B* and the distance from *B* to the node being considered is less than the label on that node, we have a shorter path, so the node is relabeled. After all the nodes adjacent to the working node have been inspected and the tentative labels changed if possible, the entire graph is searched for the tentatively-labeled node with the smallest value. This node is made permanent and becomes the working node for the next round. Figure 5-7 shows the first five steps of the algorithm. ➢ The only difference between the program and the algorithm described above is that in Fig. 5-8, we compute the shortest path starting at the terminal node, *t*, rather than at the source node, *s*. ➢ Since the shortest path from *t* to *s* in an undirected graph is the same as the shortest path from *s* to *t*, it does not matter at which end we begin (unless there are several shortest paths, in which case reversing the search might discover a different one). ➢ The reason for searching backward is that each node is labeled with its predecessor rather than its successor. When the final path is copied into the output variable, *path*, the path is thus reversed. By reversing the search, the two effects cancel, and the answer is produced in the correct order.		
	UNIT IV		
8.	Write in detail about UDP with neat diagrams. ***UDP Protocol*** ✓ UDP provides connectionless, unreliable, datagram service. ✓ Connectionless service means that there is no logical connection between the two ends exchanging messages. ✓ Each message is an independent entity encapsulated in a datagram.	CLO-4	10M

- ✓ UDP does not see any relation (connection) between consequent datagram coming from the same source and going to the same destination.
- ✓ UDP has an advantage: it is message-oriented.
- ✓ It gives boundaries to the messages exchanged.
- ✓ An application program may be designed to use UDP if it is sending small messages and the simplicity and speed is more important for the application than reliability.

User Datagram

- ✓ UDP packets, called *user datagram*, have a fixed-size header of 8 bytes made of four fields, each of 2 bytes (16 bits).
- ✓ The 16 bits can define a total length of 0 to 65,535 bytes.
- ✓ However, the total length needs to be less because a UDP user datagram is stored in an IP datagram with the total length of 65,535 bytes.
- ✓ The last field can carry the optional checksum



UDP Services

Process-to-Process Communication

- ✓ UDP provides process-to-process communication using **socket addresses,** a combination of **IP** addresses and port numbers.

Connectionless Services

- ✓ As mentioned previously, UDP provides a *connection less service.*
- ✓ This means that each user datagram sent by UDP is an independent datagram.
- ✓ There is no relationship between the different user data grams even if they are coming from the same source process and going to the same destination program.

Flow Control

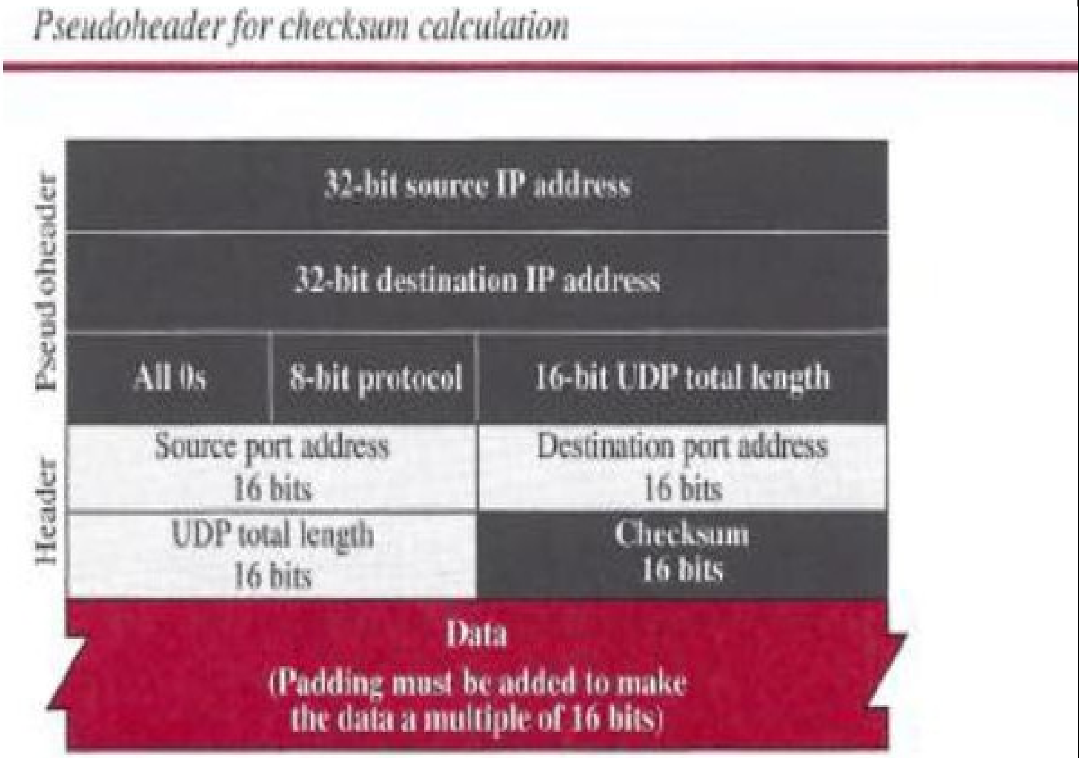
- ✓ UDP is a very simple protocol. There is no *flow control*, and hence no window mechanism. The receiver may overflow with incoming messages.

Error Control

- ✓ There is no *error control* mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated.

Checksum

- ✓ UDP checksum calculation includes three sections: a pseudo header, the UDP header, and the data coming from the application layer.
- ✓ The *pseudo header* is the part of the header of the IP packet in which the user datagram is to be encapsulated with some fields filled with 0s



UDP Applications

UDP Features

Connectionless Service

As we mentioned previously,

- ✓ UDP is a connectionless protocol. Each UDP packet is independent from other packets sent by the same application program.
- ✓ This feature can be considered as an advantage or disadvanta8e depending on the application requirements.
- ✓ UDP does not provide error control; it provides an unreliable service.
- ✓ Most applications expect reliable service from a transport-layer protocol.
- ✓ Although a reliable service is desirable.

Typical Applications

The following shows some typical applications that can benefit more from the services of UDP

- ✓ UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control
- ✓ UDP is suitable for a process with internal flow- and error-control mechanisms.
- ✓ For example, the Trivial File Transfer Protocol (TFIP)
- ✓ UDP is a suitable transport protocol for multicasting.
- ✓ Multicasting capability is embedded in the UDP software
- ✓ UDP is used for management processes such as SNMP
- ✓ UDP is used for some route updating protocols such as Routing Information Protocol (RIP)
- ✓ UDP is normally used for interactive real-time applications that cannot tolerate uneven delay between sections of a received message

(OR)

9.	Write in detail about Streaming Stored Audio/Video with neat diagrams.	CLO-4	10M

streaming stored audio and video. Downloading these types of files from a Web server can be different from downloading other types of files.

First Approach: Using a Web Server A compressed audio/video file can be downloaded as a text file. The client (browser) can use the services of HTTP and send a GET message to download the file. The Web server can send the compressed file to the browser. The browser can then use a help application, normally called a media player, to play the file. Fig.4.10 shows this approach.

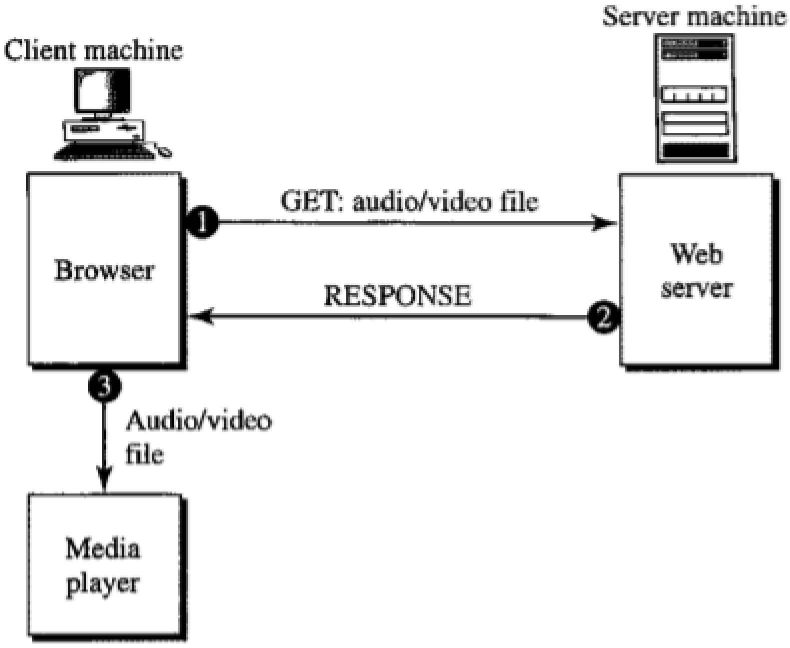
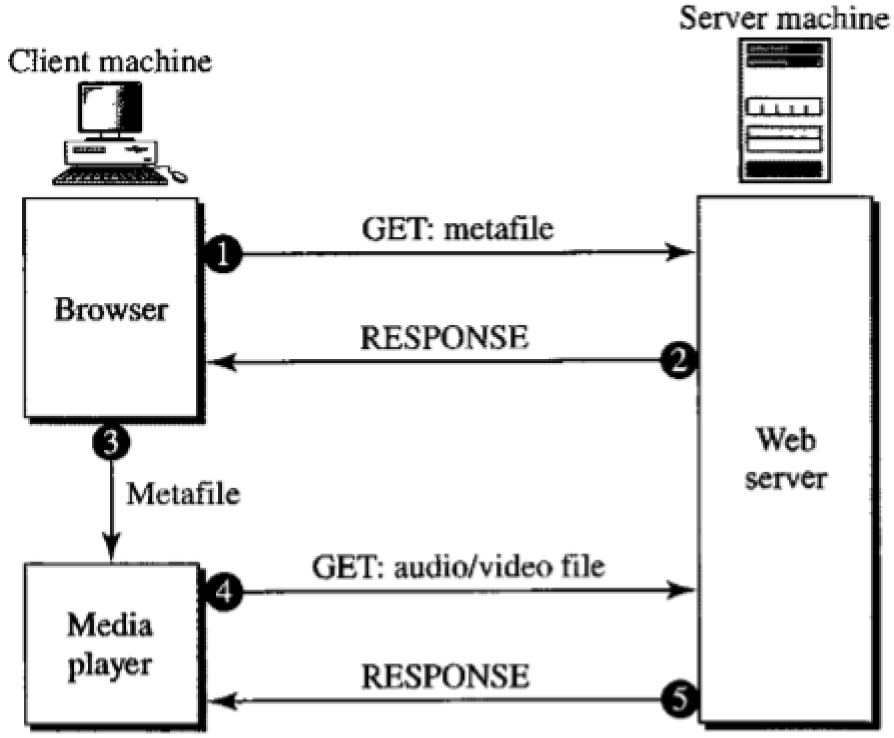


Fig. 4.10 Using a Web Server

This approach is very simple and does not involve streaming. However, it has a drawback. An audio/video file is usually large even after compression. An audio file may contain tens of megabits, and a video file may contain hundreds of megabits. In this approach, the file needs to download completely before it can be played. Using contemporary data rates, the user needs some seconds or tens of seconds before the file can be played.

Second Approach: Using a Web Server with Metafile In another approach, the media player is directly connected to the Web server for downloading the audio/video file. The Web server stores two files: the actual audio/video file and a metafile that holds information about the audio/video file. Fig. 4.11 shows the steps in this approach. 1. The HTTP client accesses the Web server by using the GET message. 2. The information about the metafile comes in the response. 3. The metafile is passed to the

	media player. 4. The media player uses the URL in the metafile to access the audio/video file. 5. The Web server responds.  Fig. 4.11 Using a Web Server with Metafile Third Approach: Using a Media Server The problem with the second approach is that the browser and the media player both use the services of HTTP. HTTP is designed to run over TCP. This is appropriate for retrieving the metafile, but not for retrieving the audio/video file. The reason is that TCP retransmits a lost or damaged segment, which is counter to the philosophy of streaming. We need to dismiss TCP and its error control; we need to use UDP. However, HTTP, which accesses the Web server, and the Web server itself are designed for TCP; we need another server, a media server. Fig.4.12 shows the concept. 1. The HTTP client accesses the Web server by using a GET message. 2. The information about the metafile comes in the response.		

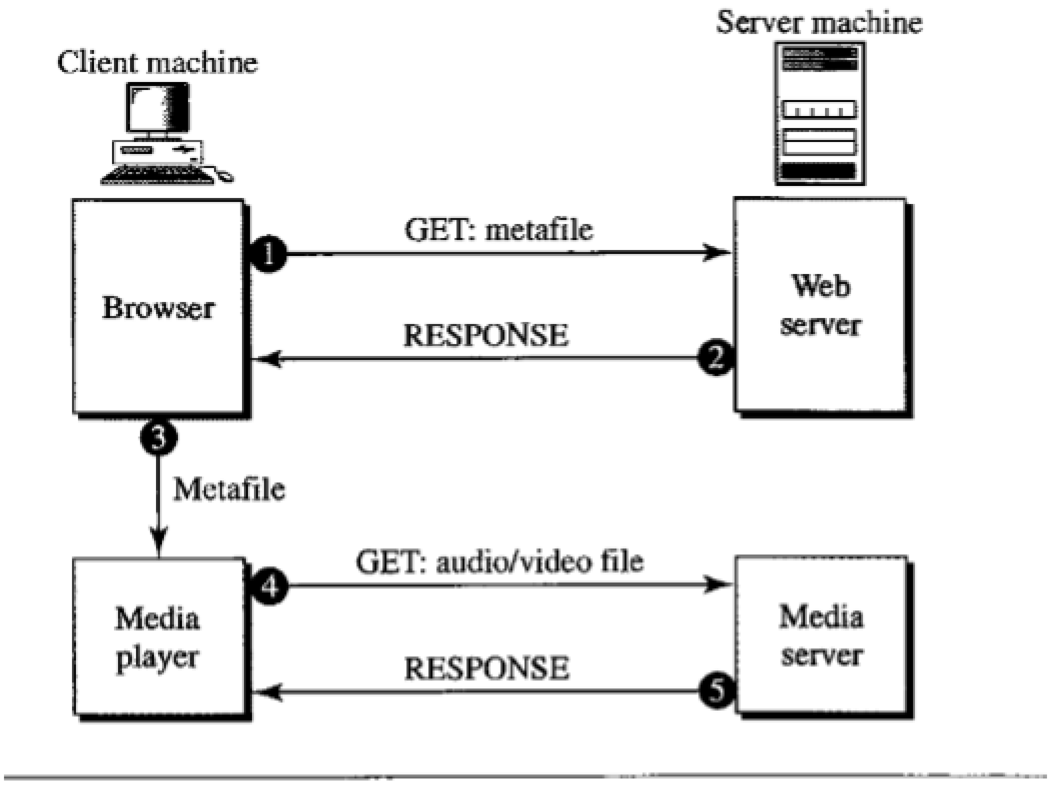
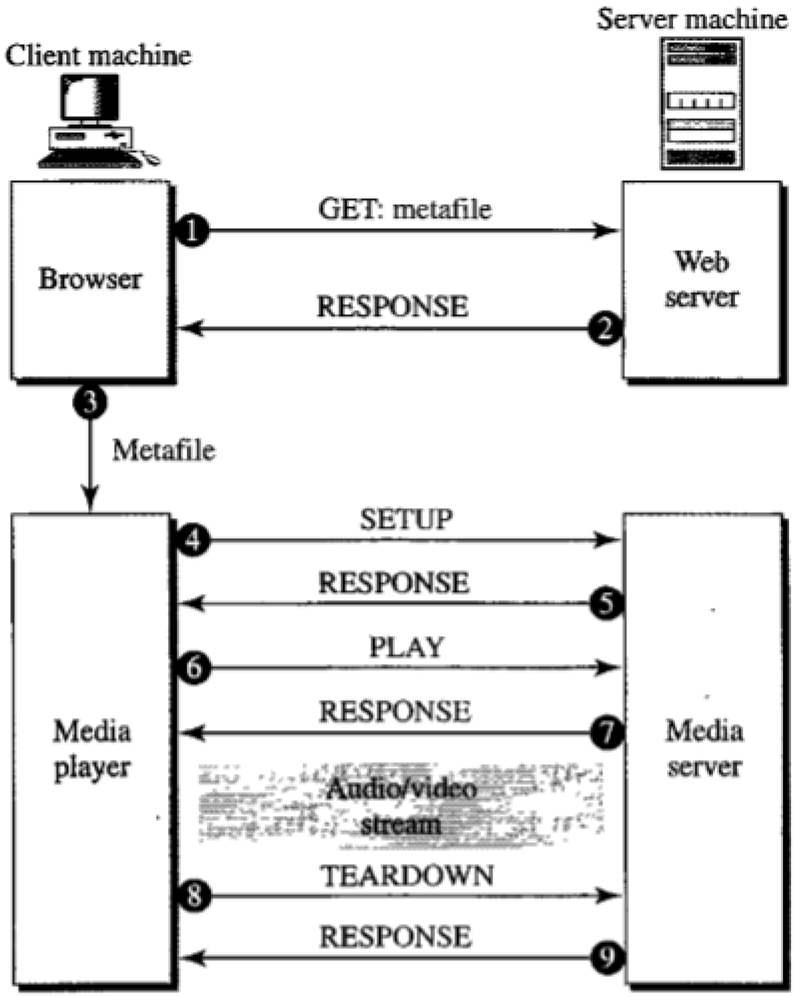


Fig.4.12 Using a Media Server

3. The metafile is passed to the media player. 4. The media player uses the URL in the metafile to access the media server to download the file. Downloading can take place by any protocol that uses UDP 5. The media server responds.

Fourth Approach: Using a Media Server and RTSP The Real-Time Streaming Protocol (RTSP) is a control protocol designed to add more functionalities to the streaming process. Using RTSP, we can control the playing of audio/video. RTSP is an out-of-band control protocol that is similar to the second connection in FTP. Fig.4.13 shows a media server and RTSP.



1. The HTTP client accesses the Web server by using a GET message. 2. The information about the metafile comes in the response. 3. The metafile is passed to the media player. 4. The media player sends a SETUP message to create a connection with the media server. 5. The media server responds. 6. The media player sends a PLAY message to start playing (downloading). 7. The audio/video file is downloaded by using another protocol that runs over UDP. 8. The connection is broken by using the TEARDOWN message. 9. The media server responds. The media player can send other types of messages. For example, a PAUSE message temporarily stops the downloading; downloading can be resumed with a PLAY message.