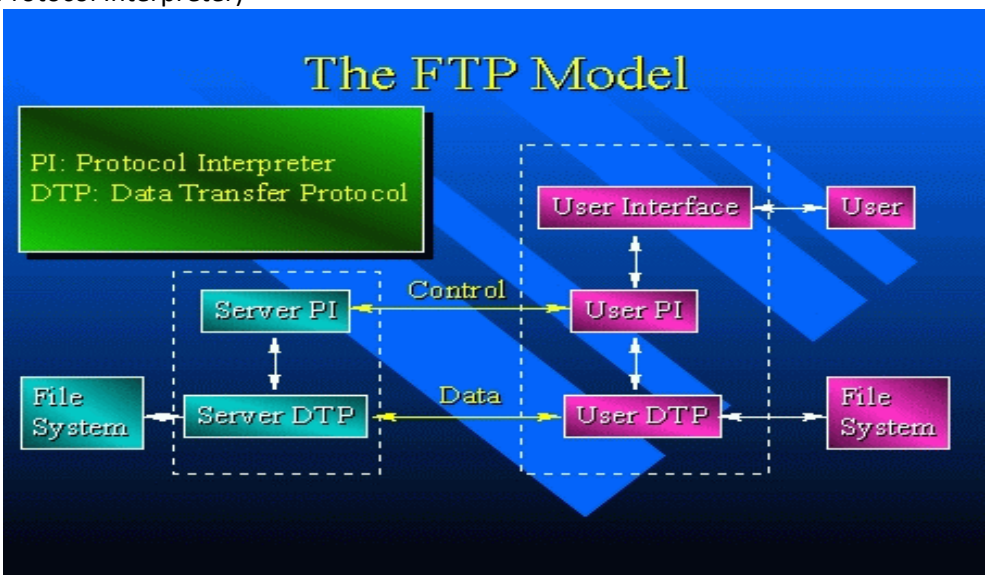
TE Computer -Computer Networks (EndSem Paper Solution-2014-15)

Q1 a) Explain FTP in detail [7]

Ans: Allow file sharing between remote machine, transfer data reliably and efficiently. FTP Protocol falls within client server model, both client & server have 2 process allowing information (Data & command) to be managed , they are

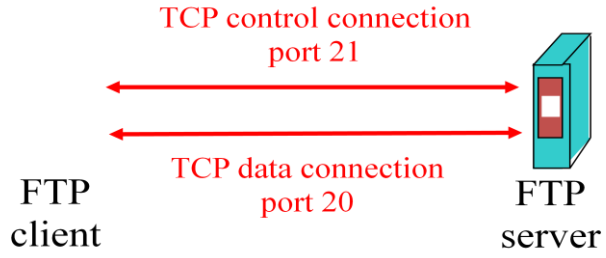
1. DTP(Data transfer Process)
2. PI(Protocol Interpreter)



During FTP Connection 2 transmission channels are open

1. Control Channel (For command)
2. Data Channel (For data)

Control uses port no 21 and Data connection uses Port no 20. FTP client contacts FTP server at port 21, TCP is transport protocol. client authorized over control connection. client browses remote directory by sending commands over control connection. when server receives file transfer command, server opens *2nd* TCP connection (for file) to client . after transferring one file, server closes data connection.



server opens another TCP data connection to transfer another file.control connection: "out of band"
FTP server maintains "state": current directory, earlier authentication

Sample commands:

- sent as ASCII text over control channel
- **USER *username***
- **PASS *password***
- **LIST** return list of file in current directory
- **RETR filename** retrieves (gets) file
- **STOR filename** stores (puts) file onto remote host

TE Computer -Computer Networks (EndSem Paper Solution-2014-15)

Q 1 b) What is QoS. Explain QoS parameters. [8]

Ans: QoS (Quality of Service) is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information. Transmitting this kind of content dependably is difficult in public networks using ordinary "best effort" protocols.

- Reliability- *Reliability* is concerned with the ability of a *network* to carry out a desired operation according to its specifications
- Jitter- **Jitter** is defined as a variation in the delay of received packets.
- Delay- is the amount of time required to transmit packets.
- Bandwidth- amount of information that can be transmitted over a **network** in a given amount of time

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

Techniques to achieve Good QoS:

- Buffering
- Traffic Shaping
- Leaky bucket algorithm
- Token bucket algorithm
- Resource reservation
- Admission control
- Packet scheduling

Q1 c) What is significance of priority and flow label field in IPV6? [5]

Ans: Flow Label/QoS management (20 bits) : The 20-bit flow label field in the IPv6 header can be used by a source to label a set of packets belonging to the same flow. A flow is uniquely identified by the combination of the source address and of a non-zero Flow label. Multiple active flows may exist from a source to a destination as well as traffic that are not associated with any flow (Flow label = 0).

Packet priority/Traffic class (8 bits) : The 8-bit Priority field in the IPv6 header can assume different values to enable the source node to differentiate between the packets generated by it by associating different delivery priorities to them. This field is subsequently used by the originating node and the routers to identify the data packets that belong to the same traffic class and distinguish between packets with different priorities.

TE Computer -Computer Networks (EndSem Paper Solution-2014-15)

Q2a) Explain functionality of DHCP server, Proxy server,File server and Web Server [8]

Ans:

1> DHCP server: The Dynamic Host Configuration Protocol (**DHCP**) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

2> Proxy Server: A **proxy server** is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the **proxy server**, then requests a connection, file, or other resource available on a different **server**.

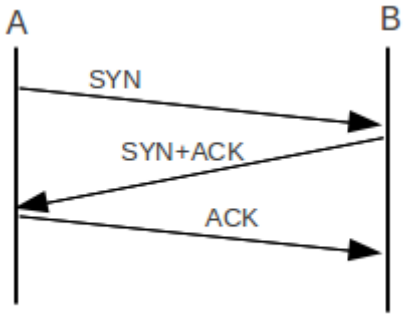
3> File Server: n computing, a **file server** (or **fileserver**) is a computer attached to a network that has the primary purpose of providing a location for shared disk access, i.e. shared storage of computer files (such as documents, sound files, photographs, movies, images, databases, etc.) that can be accessed by the workstations that are attached to the same computer network. The term *server* highlights the role of the machine in the client–server scheme, where the *clients* are the workstations using the storage. A file server is not intended to perform computational tasks, and does not run programs on behalf of its clients. It is designed primarily to enable the storage and retrieval of data while the computation is carried out by the workstations.

4> Web Server: A **Web server** is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form **Web** pages to users, in response to their requests, which are forwarded by their computers' HTTP clients.

Q2 b) Draw and Explain 3 way handshake process of TCP. [4]

Ans: TCP connections are established via an exchange known as the **three-way handshake**. If A is the client and B is the LISTENing server, then the handshake proceeds as follows:

- A sends B a packet with the SYN bit set (a SYN packet)
- B responds with a SYN packet of its own; the ACK bit is now also set
- A responds to B's SYN with its own ACK



TCP three-way handshake

Normally, the three-way handshake is triggered by an application's request to connect; data can be sent only after the handshake completes. This means a one-RTT delay before any data can be sent. The original TCP standard **RFC 793** does allow data to be sent with the first SYN packet, as part of the handshake, but such data cannot be released to the remote-endpoint application until the handshake completes. Most traditional TCP programming interfaces offer no support for this early-data option.

Q2 c) Describe in short working and importance of following commands. [8]

Ans:

1> **Ping: Ping** is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer and back.
Example: Ping IpAddress/Hostname

2> **Netstat:** In computing, **netstat** (network statistics) is a command-line tool that displays network connections for the Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics.

3> **Traceroute:** Traceroute is a command which can **show** you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.

4> **IP Config:** Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, **ipconfig** displays the IP address, subnet mask, and default gateway for all adapters.

Q3 a) Explain WAP protocol stack [8]

Ans: AP is designed in a layered fashion, so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers:

- **Application Layer**

  Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.

- **Session Layer**

  Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

- **Transaction Layer**

  Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

- **Security Layer**

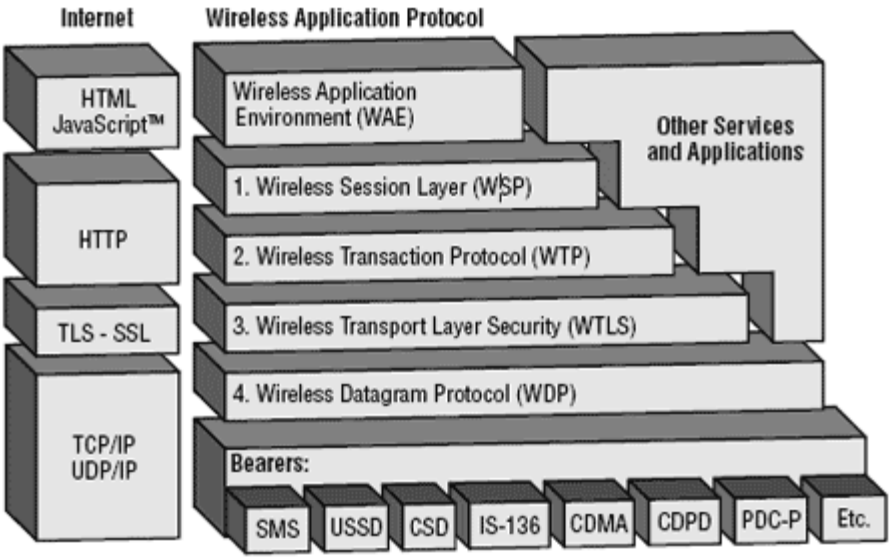
  Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

- **Transport Layer**

  Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.



Note that the mobile network bearers in the lower part of the figure above are not part of the WAP protocol stack.

Q3 b) Write short note on [8]

1> **Wireless LAN:** A **wireless local area network** (**WLAN**) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building. This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name. Types of wireless LANs

The IEEE 802.11 has two basic modes of operation: infrastructure and ad hoc mode. In ad hoc mode, mobile units transmit directly peer-to-peer. In infrastructure mode, mobile units communicate through an access point that serves as a bridge to other networks (such as Internet or LAN).

WLAN Architecture

- **Stations :**All components that can connect into a wireless medium in a network are referred to as stations (STA). All stations are equipped with wireless network interface controllers (WNICs). Wireless stations fall into one of two categories: wireless access points, and clients.
- **Basic service set :** The basic service set (BSS) is a set of all stations that can communicate with each other at PHY layer. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.
- **Extended service set:** An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.
- **Distribution system:** A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

2> **WML Script:** WMLScript is a procedural programming language and dialect of JavaScript used for WML pages and is part of the Wireless Application Protocol (WAP). WMLScript is a client-side scripting language and is similar to JavaScript. Just like JavaScript WMLScript is used for tasks such as user input validation, generation of error message and other Dialog boxes etc. A major difference between JavaScript and WMLScript is that JavaScript code can be embedded in the HTML markup, whereas WMLScript code is always placed in a file separated from the WML markup. URLs are used to refer to the actual WMLScript code in the WML document.

WMLScript has a number of standard libraries. They contain a lot of useful functions that you should get familiar with. We will talk about them in later parts of this WMLScript tutorial.

Example: The following "Hello World" WMLScript example shows you how a WMLScript file typically looks like and demonstrates how to call WMLScript code in a WML document.

```
<?xml version="1.0"?>
<wml>
  <card id="card1" title="WMLScript Tutorial">
    <p>
      <a href="helloWorldEg1.wmls#helloWorld()">Run WMLScript</a><br/>
      $(message)
    </p>
  </card>
</wml>
```

WML Script Functions:

The user-defined functions are declared in a separate file having the extension .wmls. Functions are declared as follows:

```
function name (parameters)
{
   control statements;
   return var;
}
```

The functions used are stored in a separate file with the extension .wmls. The functions are called as the filename followed by a hash, followed by the function name:

Q4 a) Explain all versions of 802.11 standard and compare: [8]
Ans: IEEE developed the first internationally recognized wireless LAN standard – IEEE 802.11 in 1997 .Scope of IEEE 802.11 is limited to Physical and Data Link Layers.
IEEE 802.11 Standards:

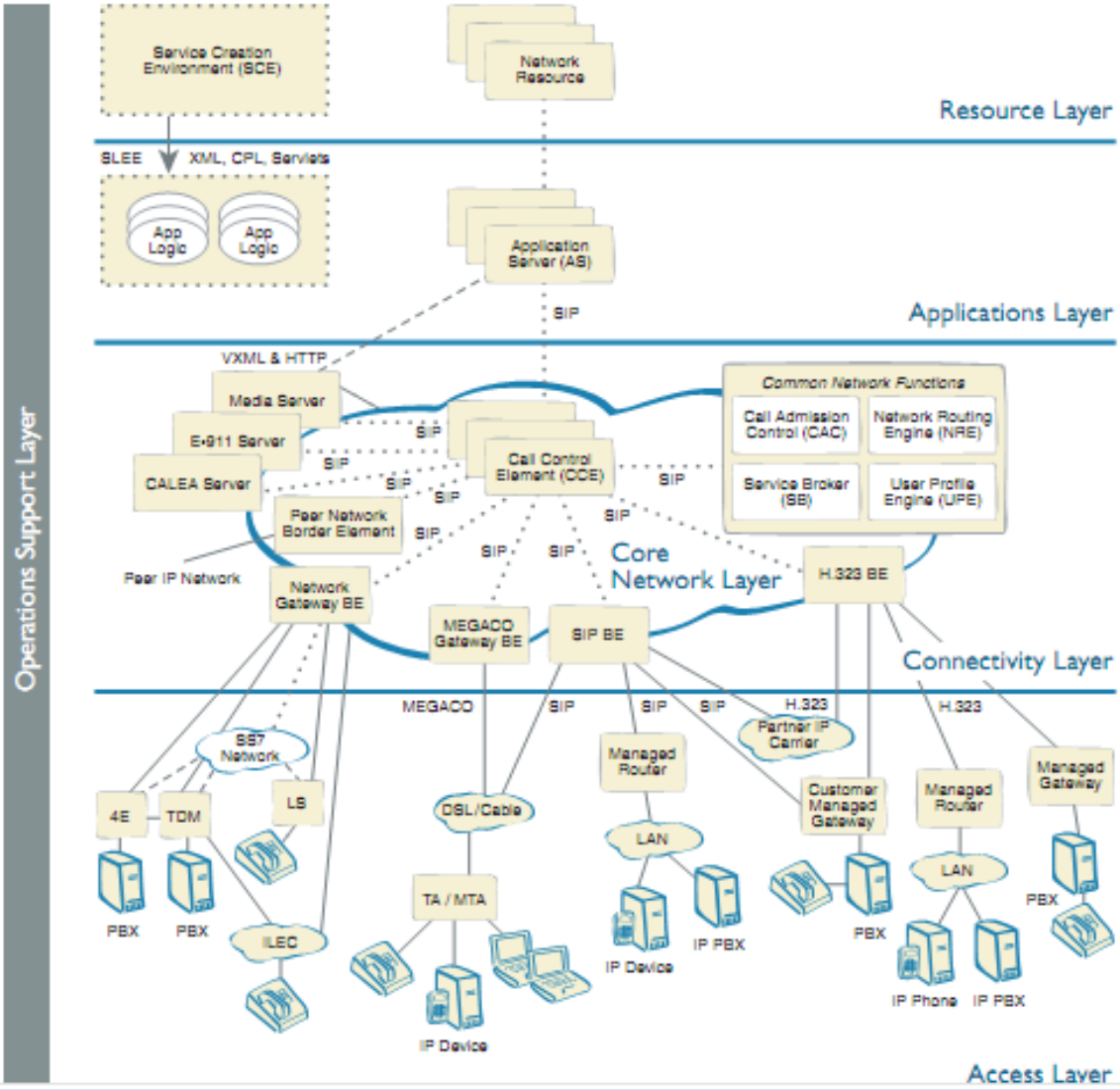
- 802.11a (OFDM Waveform)
- 802.11b
- 802.11g
- 802.11n
- 802.11ac
- 802.11ad
- 802.11af
- 802.11ah
- 802.11ai
- 802.11aj
- 802.11aq
- 802.11ax

Comparison of different IEEE Standards

802.11 protocol	Release date[5]	Frequency (GHz)	Data Rate	Allowable MIMOstreams	Modulation
802.11-1997	Jun 1997	2.4	1 or 2 Mbps	N/A	DSSS, FHSS
a	Sep 1999	5	6 to 54 mbps	N/A	OFDM
b	Sep 1999	2.4	5.5 and 11 Mbps	N/A	DSSS
g	Jun 2003	2.4	6 to 54 Mbps	N/A	OFDM, DSSS
n	Oct 2009	2.4/5	54 Mbit/s to 600 Mbit/s	4	OFDM
ac	Dec 2013	5	1.3 Gbit/s	8	
ad	Dec 2012	60	7 Gbits	N/A	OFDM, single carrier, low-power single carrier

Q5a) Draw and explain VOIP network architecture. [8]
Ans:

In Figure , layers are represented in a high-level AT&T VoIP functional architecture. This is a logical functional architecture and is not intended to represent the physical implementation. The architecture does not specify how functions will be distributed to devices. Instead, it allows the flexibility to package functions into various servers using cost-effective methods, as long as open interfaces to those functions are available for use by other functions. For each access type, a corresponding Border Element (BE) is deployed to manage the access-specific requirements and interfaces. BEs are the demarcation points for the Connectivity Layer, which is a common and shared layer on top of the converged IP/MPLS network, or Core Network Layer. The BEs translate access protocols to SIP, then provide call details to the Call Control Element (CCE). The CCE manages the VoIP infrastructure and creates, removes and joins call legs. To provide a service, the CCE invokes an Application Server (AS), using SIP to communicate. By sharing a common architecture, new access technologies can use all existing and future ASs, and new ASs can support all existing and future access technologies. This architecture supports all real-time communications scenarios, like prepaid card, click-to-chat, and teleconferencing. For a simplified basic call flow, the following steps are performed:



1. The caller's phone connects to the BE using the appropriate access-specific signaling protocol.
2.The BE sends a SIP INVITE to the CCE with Request-URI for the destination's phone number. The CCE
consults with the Service Broker, which indicates that this call has no features.
3.The CCE sends an INVITE to the destination's BE, which communicates with the destination's device using the
appropriate signaling protocol.
4. The call is set up between the two end-points, and the caller and destination talk.
5. The destination hangs up. The BE sends a SIP BYE to the CCE.
6. The CCE sends a BYE to caller's BE, which disconnects the caller.

Q5 b)Explain VANET architecture. What are the challenges in vehicular network. [8]
Ans:
the mobile domain consists of two parts: the vehicle domain and the mobile device domain. The vehicle domain comprises all kinds of vehicles such as cars and buses. The mobile device domain comprises all kinds of portable devices like personal navigation devices and smartphones.

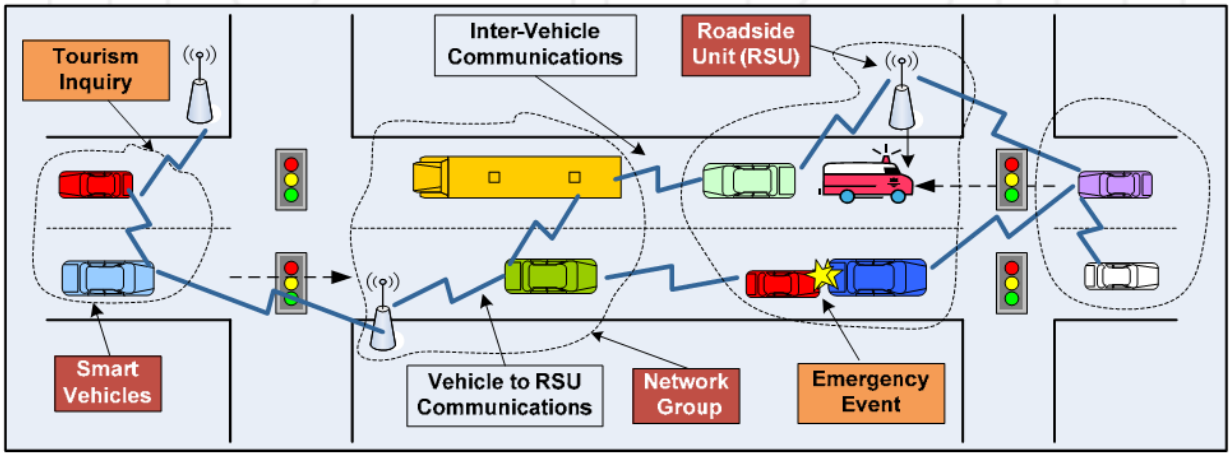


Figure: Basic Architecture of VOIP

Within the infrastructure domain, there are two domains: the roadside infrastructure domain and the central infrastructure domain. The roadside infrastructure domain contains roadside unit entities like traffic lights. The central infrastructure domain contains infrastructure management centers such as traffic management centers (TMCs) and vehicle management centers.

Communication Architecture: Communication types in VANETs can be categorized into four types.

1> In-vehicle communication, which is more and more necessary and important in VANETs research, refers to the in-vehicle domain. In-vehicle communication system can detect a vehicle's performance and especially driver's fatigue and drowsiness, which is critical for driver and public safety.
2> Vehicle-to-vehicle (V2V) communication can provide a data exchange platform for the drivers to share information and warning messages, so as to expand driver assistance.

3> Vehicle-to-road infrastructure (V2I) communication is another useful research field in VANETs. V2I communication enables real-time traffic/weather updates for drivers and provides environmental sensing and monitoring.

4> Vehicle-to-broadband cloud (V2B) communication means that vehicles may communicate via wireless broadband mechanisms such as 3G/4G. As the broadband cloud may include more traffic information and monitoring data as well as infotainment, this type of communication will be useful for active driver assistance and vehicle tracking.

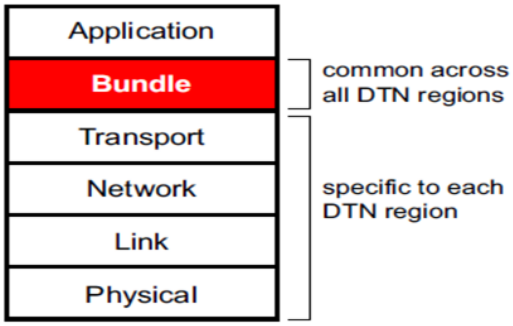
challenges in vehicular network:

- Network Security
- Quality of Service (QoS)
- Broadcast and routing
- Information dissemination
- Data access
- Efficient Routing Algorithms Design
- Co-operative Communications
- Scalability and Robustness:
- Address configuration

Q6 a) what is DTN? Explain different layers of DTN. [8]

Ans:

Disruption Tolerant Networking (DTN) standards, to support **internetworking in space.** The DTN standards support a network service like reliability and security. These are all designed to work in environments **where end-to-end paths may not be available.**such as when an orbiter needs to receive data from Earth and then wait, before it can forward it to a lander on another planet. DTN provides a general-purpose **network- /transport-layer service** that is logically similar to what TCP/IP provides for the terrestrial Internet, but suitable for use in the space environment. DTN also **provides** efficient **reliability,security, in-order delivery, duplicate suppression; class of service (prioritization); remote management; streaming service, rate buffering, and data accounting.** Multiple **applications** including file transfer, messaging (e.g. for mission operations), and streaming audio/video and control its services to reduce risk, cost, and complexity.



DTN Layers

- DTN implements a **store and forward message switching** system by simply overlaying another new protocol layer – called the BUNDLE LAYER on top of the heterogeneous region-specific lower layers.

- This bundle layer brings together the region specific lower layers so that the application programs can communicate across the multiple regions.
- Bundles are just **messages**, make them huge chunk of messages.
- The bundle layer stores and forwards entire bundles between nodes.
- A single bundle layer built into the network is used across the entire network regions that constitute the DTN network.
- The transport layer below the bundle layers are chosen basically based upon their appropriateness to each region in the network.

Q6b) Explain advantages and disadvantages of VOIP over traditional telephone network. [8]
Ans:

VOIP advantages:

- **Cost savings** (uses internet, IP routers...)
- **Rich media service**-People check out friends' presence (such as online, offline, busy), send instant messages, make voice or video calls, transfer images, and so on.
- **Phone portability**
- **Integration and collaboration with other applications**-such as email, web browser, instant messenger, social-networking applications, and so on
- **User control interface**-web GUI, to their customers so that they can change features, options, and services dynamically. For example, speed dial, presence information (online, offline), black/white list, music-on-hold option, anonymous call block …
- **No geographical boundary**
- **Not only voice but also Image,video** is also transmitted.

VOIP Disadvantages:

- **Complicated service and network architecture**
- **Interoperability issues** between different protocols, applications, or products
- **Quality of service (QoS)** issues- ensuring QoS is very difficult and costs lots of time and resources
- **Power outages-** you cannot use VoIP phones during power outages
- **Emergency calls-** service is almost impossible
- **Security issues**
- **Legal issues (lawful interception)**

Q7a) Explain ATM architecture [8]
Ans:

The *asynchronous transfer mode* (ATM) protocol architecture is designed to support the transfer of data with a range of guarantees for quality of service. The user data is divided into small, fixed-length packets, called cells, and transported over virtual connections. ATM operates over high data rate physical circuits, and the simple structure of ATM cells allows switching to be performed in hardware, which improves the speed and efficiency of ATM switches.

Figure (A) shows the reference model for ATM. The first thing to notice is that, as well as layers, the model has planes. The functions for transferring user data are located in the user plane; the functions associated with the control of connections are located in the control plane; and the co-ordination functions associated with the layers and planes are located in the management planes.

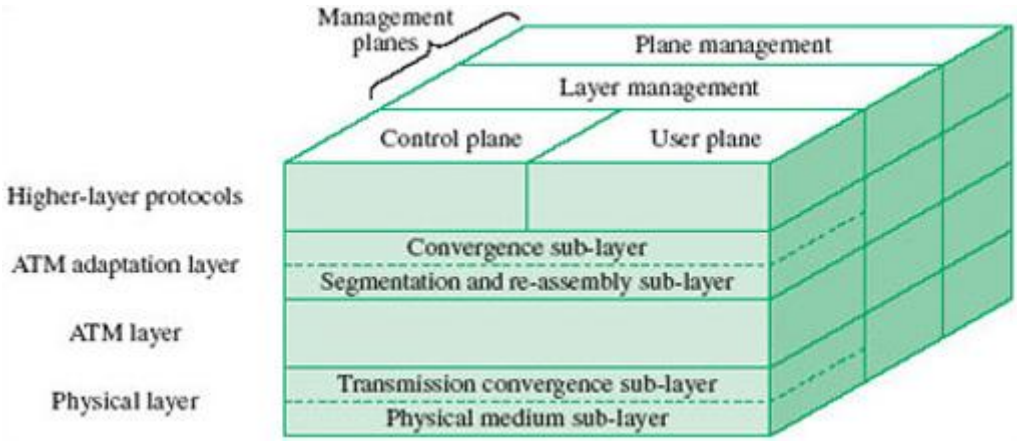


Figure (A): ATM Refence Model

The three-dimensional representation of the ATM protocol architecture is intended to portray the relationship between the different types of protocol. The horizontal layers indicate the encapsulation of protocols through levels of abstraction as one layer is built on top of another, whereas the vertical planes indicate the functions that require co-ordination of the actions taken by different layers. An advantage of dividing the functions into control and user planes is that it introduces a degree of independence in the definition of the functions: the protocols for transferring user data (user plane) are separated from the protocols for controlling connections (control plane).

The protocols in the ATM layer provide communication between ATM switches while the protocols in the ATM adaptation layer (AAL) operate end-to-end between users. This is illustrated in the example ATM network in Figure (B).

Two types of interface are identified in Figure (A): one between the users and the network (user-network interface), and the other between the nodes (switches) within the network (network-node interface).

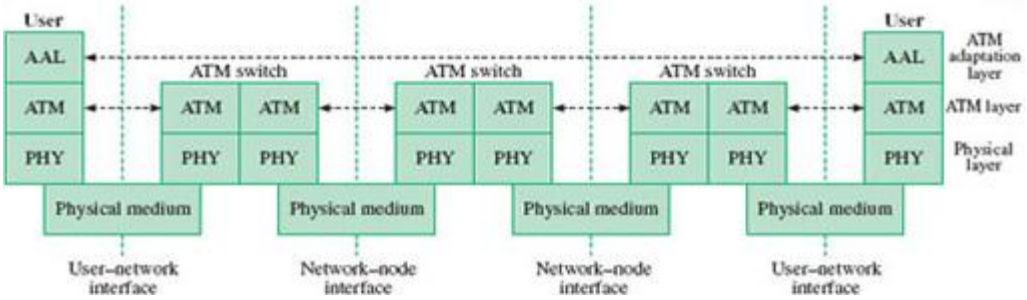


Figure (B) ATM network

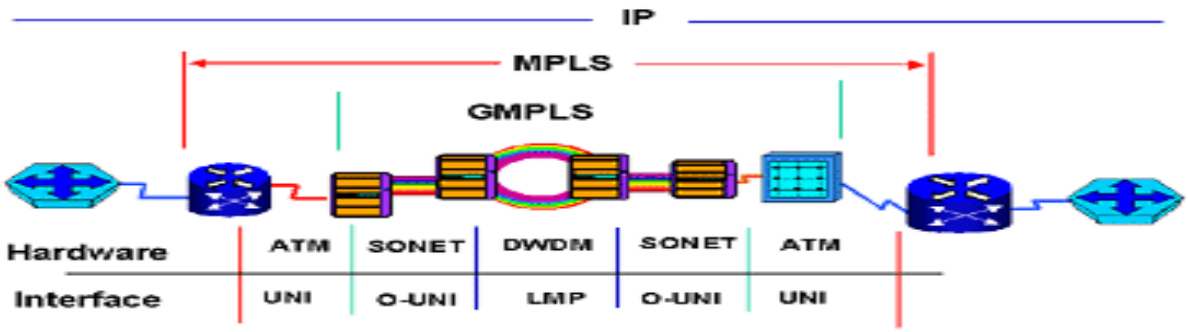
Q7b) Write Short note on(Any Two): [10]
Ans:

1> **GMPLS:**

GMPLS (Generalized Multiprotocol Label Switching), also known as Multiprotocol Lambda Switching, is a technology that provides enhancements to Multiprotocol Label

Switching (MPLS) . Generalized Multiprotocol Label Switching (GMPLS) enhances MPLS architecture by *the complete separation of the control and data planes*.
GMPLS enables a seamless interconnection and convergence of new and legacy networks.
GMPLS is based on the IP routing and addressing models.
support network switching for time, wavelength, and space switching as well as for packet switching.

- While the technology used by the GMPLS control plane remains IP-based, the data plane (traffic plane) can now diversify to include more varieties of traffic like:
    - Support multiple types of traffic (ATM, IP, SONET and *etc.)*
    - Support both peer and overlay models
    - Support multi-vendors
    - Perform fast provisioning



- GMPLS is conceptually similar to MPLS, but instead of using an explicit label to distinguish an LSP at each LSR, some physical property of the received data stream is used
- The most commonly used schemes are:
    - using the timeslot to identify the LSP, on a Time Division Multiplexed (TDM) link
    - using the wavelength to identify the LSP, on a Wavelength Division Multiplexed (WDM) link
    - using the fiber or port on which a packet is received.

2> **SDN:**

Software-defined networking (SDN) is an approach to computer networking that allows network administrators to manage network services through abstraction of higher-level functionality. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane). SDN requires some method for the control plane to communicate with the data plane. One such mechanism is OpenFlow.

- Separate Control plane and Data plane entities
    - Network intelligence and state are logically centralized
    - The underlying network infrastructure is abstracted from the applications
- Execute or run Control plane software on general purpose hardware
    - Decouple from specific networking hardware
    - Use commodity servers
- Have programmable data planes
    - Maintain, control and program data plane state from a central entity

- An architecture to control not just a networking device but an entire network

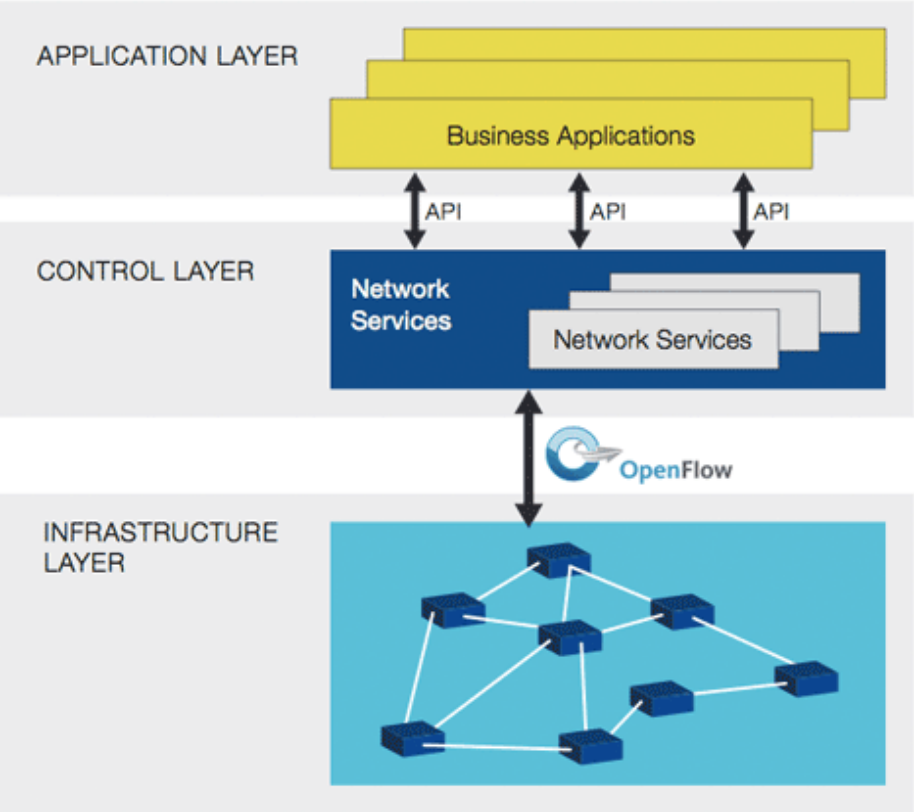


Figure: SDN Architecture

SDN Benefits:

- **Dynamic , Manageable ,cost-effective, adaptable**
- **Directly programmable**
- **Agile**: administrators dynamically adjust network-wide traffic flow to meet changing needs.
- **Centrally managed**
- **Programmatically configured**: SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs
- **Open standards-based and vendor-neutral**

Q8 a) what is Virtualization. Explain its Types. [8]

Ans:

In computing, virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments.

There are 5 types of Virtualization

1> **Hardware Virtualization :** This is most common type of virtualization used today, hardware virtualization is common because of the advantages it offers concerning hardware utilization and application uptime. It typically refers to virtualizing a server.

Normally, a server devotes complete control of it's hardware resources (cpu, RAM, and storage) to the actions of a single operating system. When you virtualize your hardware, it means that a program called a hypervisor manages the hardware's resources and divides them among different isolated operating systems, referred to as "virtual machines."

2> Desktop Virtualization:

Desktop Virtualization separates the desktop environment from the physical device that is used to access it. This is most often configured as a "virtual desktop infrastructure" (VDI) where many personal desktops (say Windows 10) are run as virtual machines on a server, but employees access those desktops from client devices (generally PCs).The advantage to Desktop Virtualization is in work convenience and information security.

3> Application virtualization

Similar to VDI mentioned above, application virtualization differs in that it delivers only a specific application from a server to the user's device. Instead of logging into an entire desktop, the user will interact with the application as though it were a native application on the client device. This makes application virtualization preferable for work on tablets or smartphones because the native presentation makes working easier.The big advantage to application virtualization is efficiency.

4> Storage Virtualization

Storage virtualization improves storage flexibility by creating a unified virtual pool of storage from physical storage devices in a network. What this does is present all physical storage in a cluster as a single shared group - visible to all servers. Storage virtualization is important because it allows for virtual machine portability without necessitating a shared storage array (generally a NAS or SAN).

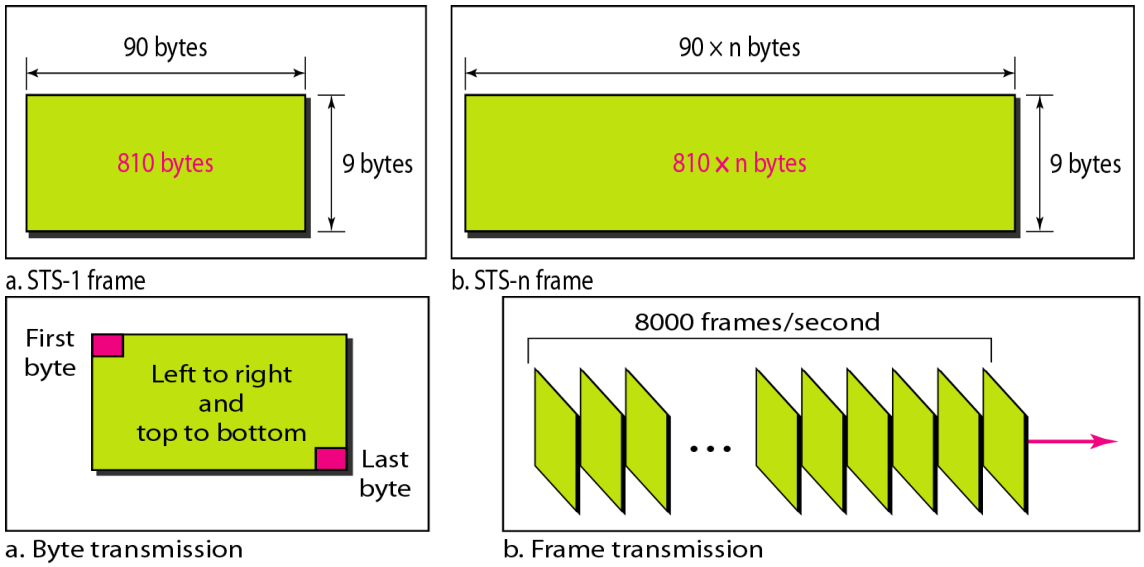
5> Network Virtualization (sometimes referred to as Software-Defined Networking)

Similar to storage virtualization, network virtualization pools resources from all physical networking equipment and presents it to virtual machines and applications as a single virtual network.This increases network agility and drastically reduces provisioning time for new network architectures. What once involved physically connecting devices and then configuring each device to properly communicate is now done virtually in moments (both manually and through automated templates).

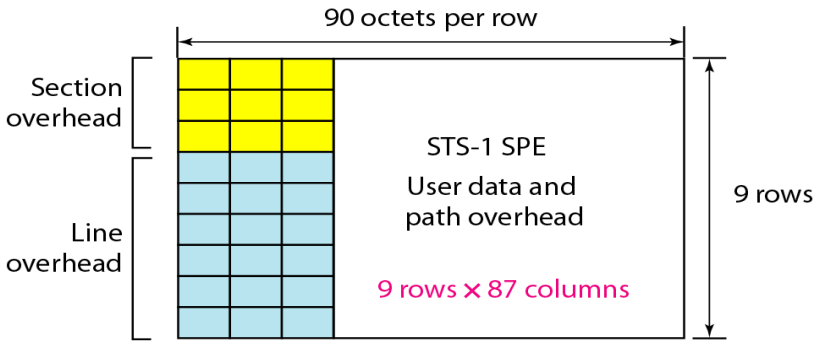
Q8 b) Explain SONET Frame structure. [6]

Ans: This signal is known as Synchronous Transport Signal Level-1 (STS-1). It consists of 9 rows of 90 bytes i.e. a total of 810 bytes. It is transmitted from left to right and top to bottom. The two dimensional figure is just for convenience. Actual transmission takes place serially i.e. the left most byte in the top row is transmitted, then the second byte in the first row and so on. After the 90^{th} byte in the first row the left most byte in the second row is transmitted and it goes on. One more point to be noted is that msb is transmitted first and the numbering of bits in a byte is as shown in figure. The frame length is 125μs (i.e. 8000 frames per

second). The STS-1 has a bit rate of 51.84Mbps. The frame for the lowest SDH rate STM-1 contains 270 columns by 9 rows. We will learn more about it later.



In SONET, the data rate of an STS-n signal is *n* times the data rate of an STS-1 signal
In SONET, the duration of any frame is 125 μs



Q8 c) What are different client layers of optical fiber. [4]

Ans: The network that use optical fiber as their underlying transmission mechanism. These network are called as Client Layers of the Optical Layer. All client layer that we discussed here perform time division multiplexing.

Client N/w are divided into two types

1>Backbone N/W

2>Metro N/W

In the backbone networks

a. Synchronous Optical Network (SONET)/ Synchronous Digital Hierarchy (SDH)

b. Optical Transport Network(OTN)

c. Generic Framing Procedure(GFP)

d. Internet Protocol (IP)

e. Asynchronous Transfer Mode (ATM)

f. Multiprotocol Label Switching (MPLS)

In the metro networks

a. Gigabit Ethernet
b. 10-Gigabit Ethernet
c. Fiber channel
d. Resilient Packet Ring (RPR)