Lectures Notes on

"Concept of Networking & IMD Network"

Prepared by

Brajesh Kanajauia Sc-D   & Ashish Kumar Sc-D

India Meteorological Department

Syllabus

1. **Concept of networking**: Protocols, Packet switching and circuit switching, IP Scheme, private and public IP and masking etc. Modems and Communication ports: Modem function, Modem figure of merit, Theory of Modem operation, various modem standard viz V.26, V.29, V.35 etc. and wireless modems, and Multiplexers, Demultiplexers. Serial ports, Ethernet Ports, USB ports, HDMI ports, SAS ports and various port, standard like RS 232, RS 422, RS 485 etc. and connectors viz RJ 45, etc.

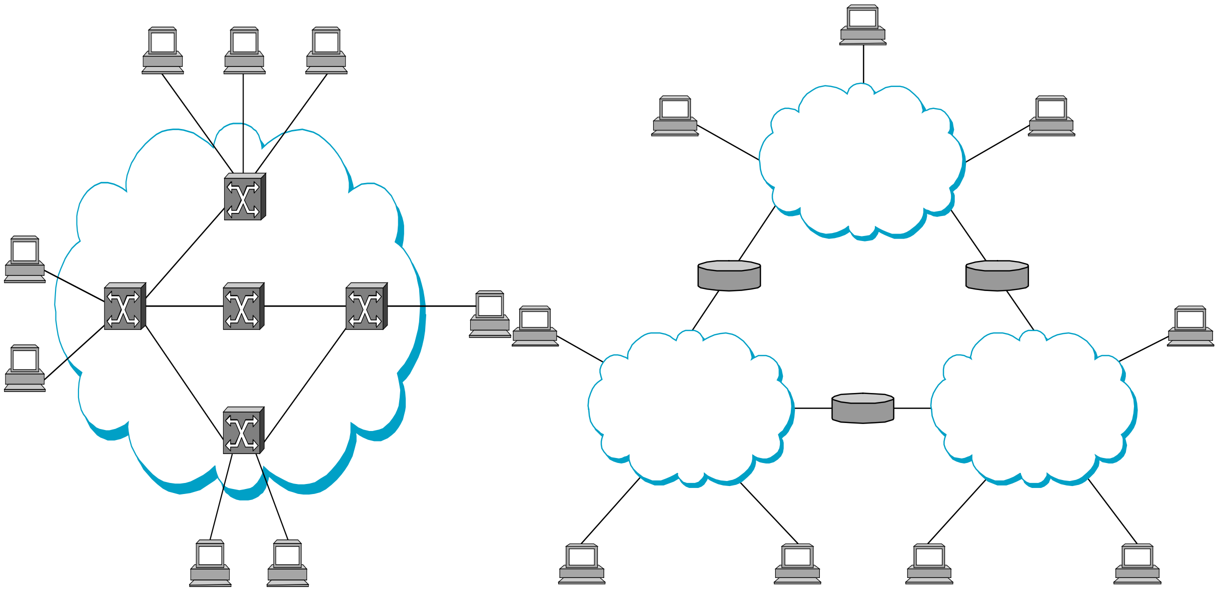
2. **Description of data switching system**: Hardware aspects, Computer architecture in the typical system (RTH Computer/ AMSS), System hardware, Communication, storage and transfer, control and display, and IMD network: MPLS VPN (Virtual Private Network) concept, Leased line, National Knowledge Network (NKN), Internet etc. other sub system (like Modems, LAN switches, SAN switches, Hubs) Message flow and data control in the switching system. SADIS data receiver, LAN, WAN, Wi-Fi, Internet servers (Hardware), MDSS, VSAT communication

3. **IMD network:** MPLS VPN (Virtual Private Network) concept, Leased line, National Knowledge Network (NKN), Internet etc.

Concept of Networking & IMD Networks

What is Network?

A network can be defined recursively as two or more nodes connected by a link, or two or more networks connected by a node.



a. Two or more nodes connected by a link **b. two or more networks connected by a node.**

Nodes: PC, special-purpose hardware hosts switches

Links: coaxial cable, optical fiber wireless etc.

1. Protocols

We now have our computers physically connected to one another and we have a means of uniquely identifying computers within the network or internetwork. What else do we need to do for our network?

We need to define protocols that will be used to carry out tasks**. A Protocol is an agreement between computers that specifies how the computers will work together.**

The Domain Name System (DNS), for example, has a corresponding protocol telling us how, given a hostname, we can convert it to an IP Number. Similarly, the DHCP system specifies how a computer can hook to a network and request an IP Number.

- In general when we define protocol, we need to specify:

- what sort of requests different computers can make of each other,
- what sort of information those requests will contain and what is the exact type and format of that information,
- What to do when something goes wrong.

Let's take a closer look at these using the HTTP, Hypertext Transport Protocol, as an example. HTTP is the protocol that underlies the web. Using HTTP we can send a number of different types of requests to a web server. These include a GET request for a particular resource (e.g., an image or the text of a webpage), a

HEAD request asking for information about a resource (but not asking that the resource itself be sent), and a DELETE request, which as the name suggests asks that a resource be deleted. When sending a request or when replying to a request, we are able to specify additional information in the form of a series of attribute value pairs.

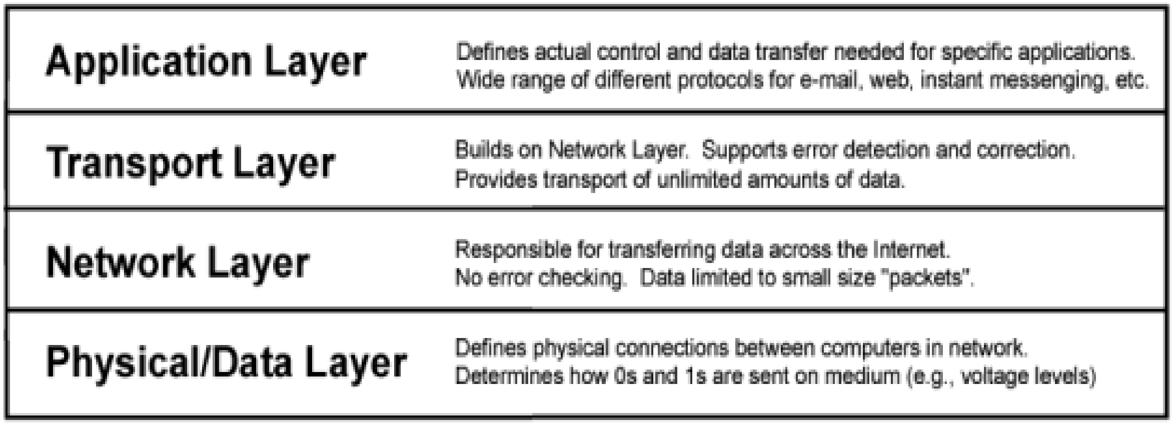
Protocols vs. Programs

What is the relationship between a protocol and a program? A protocol formally specifies the type and form of communication that will take place between computers. It partly dictates how a program using the protocol must work, but it is not a program itself.

Looking again at the HTTP protocol used on the web, Google's Chrome, Apple's Safari, and Microsoft's Edge all follow the rules of HTTP when communicating with a web server. However, they are not the same program; they are three distinct programs and in fact may run on different platforms (e.g., Macintosh vs. PC vs. Android).

The Internet Protocol Stack

The Internet uses four different layers of protocols to form what is referred to as The Internet Protocol Stack or sometimes The Internet Protocol Suite. We'll explore each of these layers, starting at the bottom layer.



Application Layer	Defines actual control and data transfer needed for specific applications. Wide range of different protocols for e-mail, web, instant messenging, etc.
Transport Layer	Builds on Network Layer. Supports error detection and correction. Provides transport of unlimited amounts of data.
Network Layer	Responsible for transferring data across the Internet. No error checking. Data limited to small size "packets".
Physical/Data Layer	Defines physical connections between computers in network. Determines how 0s and 1s are sent on medium (e.g., voltage levels)

Physical Layer

Ultimately, a network must define how computers in the network are connected together and how 0s and 1s are transmitted between them. For example, on old modems that transmitting digital data over voice telephone lines, the protocol specified that the originating modem would send a 0 by making a 1070 Hz tone and a 1 with a 1270 Hz tone whereas the responding modem would send a 0 by making a 2025 Hz tone and a 1 with a 2225 Hz tone.

This layer is necessary for any new network and by its nature will be different for each new type of network. How information is sent in a fiber optic ring network is very different from how it is sent in a WiFi star network.

Network Layer

The Network Layer provides for a uniform model for getting information across the Internet, but it does so with some very severe limitations. On the Internet the network protocol used is the Internet Protocol or IP.

The Internet Protocol specifies that:

- It will make best effort to get information from one point of the network to another point in the network However; best effort does not mean that the information will definitely get there. Information delivery at this level is unreliable. We'll see the next layer up will do a better job of this.

- At the Network Layer, all information is sent in small size chunks called IP Packets.

- ➢ Data in each IP Packet is limited to 64 kbytes.
- ➢ In addition to the actual data the IP Packet contains other information including the sender and recipient's IP Addresses, a checksum for error detection and an indication of how many bytes are actually being sent.
- ➢ If you're sending something larger than 64 kbytes, it will have to be broken down into multiple IP Packets.
- ➢ Packets are not guaranteed to arrive in the order in which they are sent, and as we've previously seen, in fact they are not guaranteed to arrive at all.

Transport Layer

Protocols at the Transport Layer allow us to transfer unlimited information from one device on the Internet to another device on the Internet with error handling taken care of.

- There are several different protocols at this level, but the most well-known is Transmission Control Protocol or TCP. TCP allows us to send data from one IP address to another IP address. It breaks down our data into appropriate IP Packet sized chunks for us. If the packets arrive in the wrong order, it properly reorders them for us. If packets get lost by the underlying IP Protocol, it sends a request to the sender to send a new copy of the lost packet.

- Note that TCP and other Protocols at this level are built on top of the underlying IP Protocol. Their implementation assumes that if they break things down into IP Packet sized chunks, there will be a best-effort attempt to get the data to the destination IP Address.

- TCP is so widely used, that you will often hear that the underlying protocols of the Internet are TCP/IP – meaning that the combination of the network-level Internet Protocol (IP) and the transport-level Transmission Control Protocol (TCP) is what really makes the Internet work.

Application Level

The application level is where all the protocols consumers care about resided. For example: - There are several protocols associated with email. These include: SMTP (Simple Mail Transfer Protocol) is the protocol that sends email through the Internet.Once your mail server receives an email message via SMTP, it sits on the mail server.When you use an email program to read your messages from the server, the email program probably either uses POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to get the messages from the mail server to your device.

As we've previously seen the HTTP Hypertext Transport Protocol is used to request and send webpages.

Transferring files is often done with FTP (File Transfer Protocol) or SFTP (Secure File Transfer Protocol).

In fact, anytime two or more computers carry out a task on the Internet, there needs to be a protocol associated with it.

2. Switching

Switching In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication. It is of two types

a) Circuit Switching –

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

b) Packet Switching –

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order. o If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

3. IP Addressing

Internet Scaling Problems

Over the past few years, the Internet has experienced two major scaling issues as it has struggled to provide continuous and uninterrupted growth:

- The eventual exhaustion of IP version 4 (IPv4) address space
- The need to route traffic between the ever increasing number of net-works that comprise the Internet

The first problem is concerned with the eventual depletion of the IP address space. IPv4 defines a 32-bit address which means that there are only 232 (4,294,967,296) IPv4 addresses available. As the Internet continues to grow, this finite number of IP addresses will eventually be exhausted.

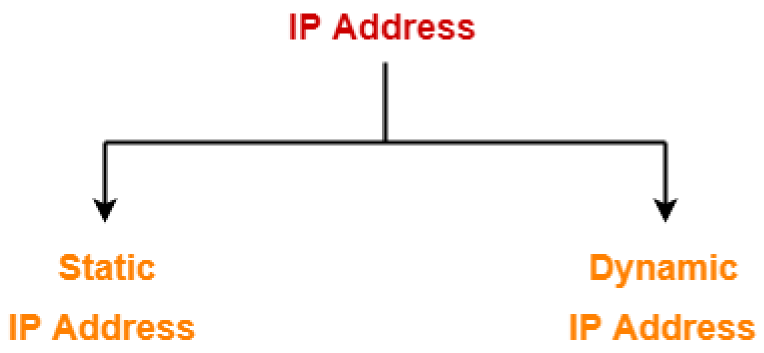
The address shortage problem is aggravated by the fact that portions of the IP address space have not been efficiently allocated. Also, the traditional model of classful addressing does not allow the address space to be used to its maximum potential.

About IP Addressing

- IP Address is short for Internet Protocol Address.
- It is a unique address assigned to each computing device in an IP network.
- ISP assigns IP Address to all the devices present on its network.
- Computing devices use IP Address to identify and communicate with other devices in the IP network.

Types Of IP Address-

IP Addresses may be of the following two types-



1. Static IP Address-

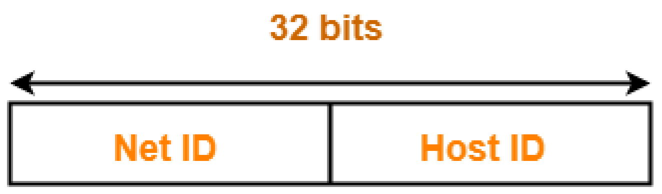
- Static IP Address is an IP Address that once assigned to a network element always remains the same.
- They are configured manually.
- Some ISPs do not provide static IP addresses.
- Static IP Addresses are more costly than dynamic IP Addresses

2. Dynamic IP Address-

- Dynamic IP Address is a temporarily assigned IP Address to a network element.
- It can be assigned to a different device if it is not in use.
- DHCP or PPPoE assigns dynamic IP addresses.

IP Address Format-

- IP Address is a 32 bit binary address written as 4 numbers separated by dots.
- The 4 numbers are called as octets where each octet has 8 bits.
- The octets are divided into 2 components- Net ID and Host ID.



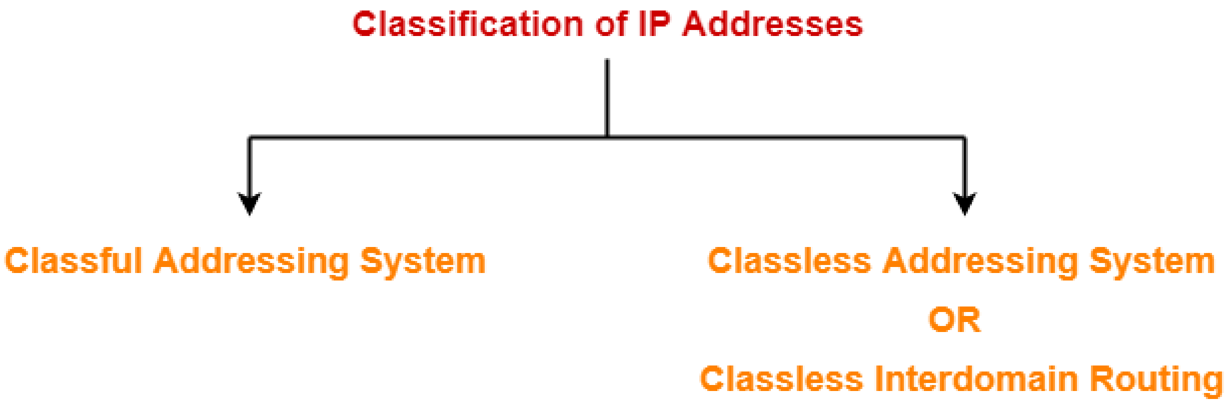
Format of an IP Address

- **Network ID** represents the IP Address of the network and is used to identify the network.
- **Host ID represents** the IP Address of the host and is used to identify the host within the network.

IP Address Example-

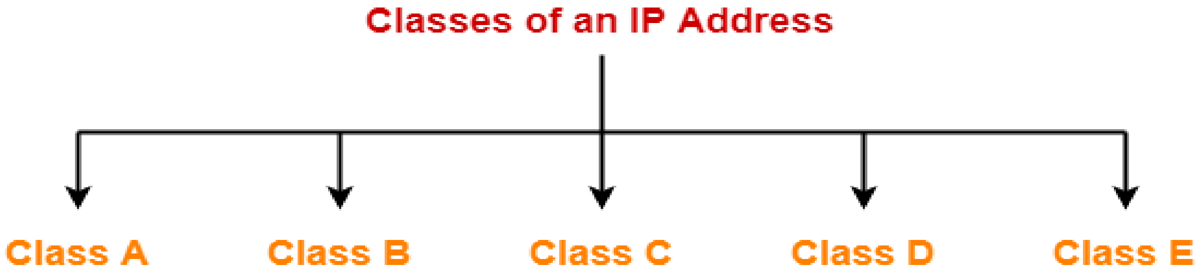
Example of an IP Address is-
00000001.10100000.00001010.11110000
(Binary Representation)
OR
1.160.10.240
(Decimal Representation)

There are two systems in which IP Addresses are classified-

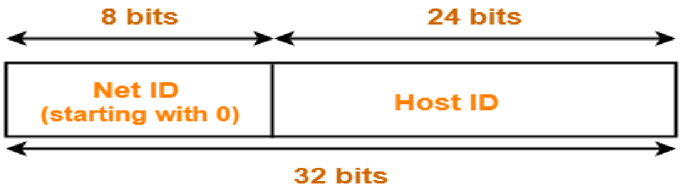

Classification of IP Addresses
Classful Addressing System
Classless Addressing System
OR
Classless Interdomain Routing

Classful Addressing

- In Classful Addressing System, IP Addresses are organized into following 5 classes-



- **Class A-** If the 32 bit binary address starts with a bit 0, then IP Address belongs to class A.
  In class A IP Address,
  - The first 8 bits are used for the Network ID.
  - The remaining 24 bits are used for the Host ID.



Class A IP Address

- **Total Number Of IP Addresses-**

  Total number of IP Addresses available in class A = Numbers possible due to remaining available 31 bits = 231

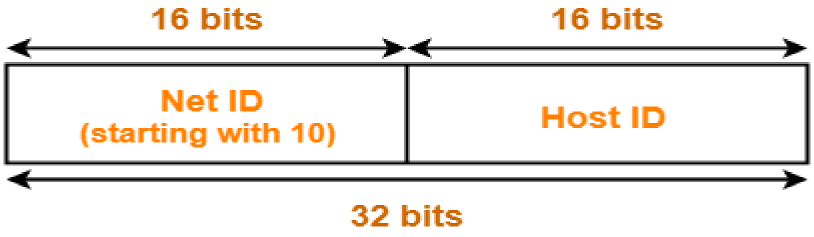
- **Total Number Of Networks-**
  Total number of networks available in class A= Numbers possible due to remaining available 7 bits in the Net ID – 2 = 27 – 2 = 126

- **Total Number Of Hosts-**
  Total number of hosts that can be configured in class A = Numbers possible due to available 24 bits in the Host ID – 2 = 224 – 2 (The reason of subtracting 2 is explained later.)

- **Range Of 1st Octet- We have-**
  Minimum value of 1st octet = 00000000 = 0
  Maximum value of 1st octet = 01111111 = 127 From here,
- **Range of 1st octet = [0, 127]**
  But 2 networks are reserved and unused. So, Range of 1st octet = [1, 126]
- **Use-** Class A is used by organizations requiring very large size networks like NASA, Pentagon etc.

Class B- If the 32 bit binary address starts with bits 10, then IP Address belongs to class B.
In class B IP Address,

- The first 16 bits are used for the Network ID.
- The remaining 16 bits are used for the Host ID.



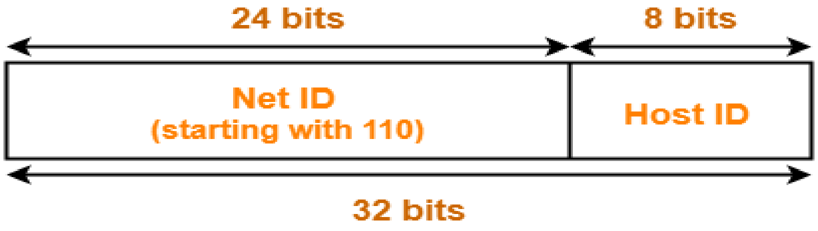
Class B IP Address

- **Total Number Of IP Addresses-**
  Total number of IP Addresses available in class B = Numbers possible due to remaining available 30 bits = 230
- **Total Number Of Networks-**
  Total number of networks available in class B = Numbers possible due to remaining available 14 bits in the Net ID = 214
- **Total Number Of Hosts-**
  Total number of hosts that can be configured in class B = Numbers possible due to available 16 bits in the Host ID – 2 = 216 – 2
- **Range Of 1st Octet- We have-**
  Minimum value of 1st octet = 10000000 = 128
  Maximum value of 1st octet = 10111111 = 191 So, Range of 1st octet = [128, 191]

- **Use-** Class B is used by organizations requiring medium size networks like IRCTC, banks etc

Class C- If the 32 bit binary address starts with bits 110, then IP Address belongs to class C. In class C IP Address,

- The first 24 bits are used for the Network ID.
- The remaining 8 bits are used for the Host ID.



Class C IP Address

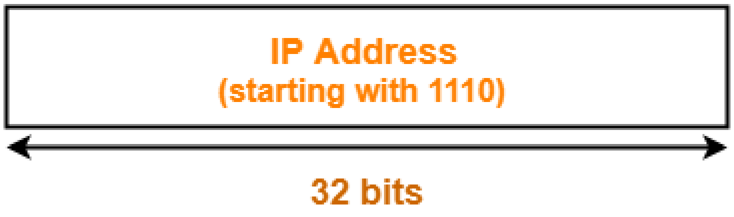
- **Total Number Of IP Addresses-**
Total number of IP Addresses available in class C = Numbers possible due to remaining available 29 bits= 229
- **Total Number Of Networks-**
Total number of networks available in class C = Numbers possible due to remaining available 21 bits in the Net ID = 221
- **Total Number Of Hosts-**
Total number of hosts that can be configured in class C= Numbers possible due to available 8 bits in the Host ID – 2 = 28 – 2

- **Range Of 1st Octet-We have-**
Minimum value of 1st octet = 11000000 = 192
Maximum value of 1st octet = 110111111 = 223 So, Range of 1st octet = [192, 223]

- **Use-**Class C is used by organizations requiring small to medium size networks. For example- engineering colleges, small universities, small offices etc.

Class D- If the 32 bit binary address starts with bits 1110, and then IP Address belongs to class D.

- Class D is not divided into Network ID and Host ID.



Class D IP Address

- **Total Number Of IP Addresses-**

Total number of IP Addresses available in class D = Numbers possible due to remaining available 28 bits = 228

- **Range Of 1st Octet We have-**

Minimum value of 1st octet = 11100000 = 224

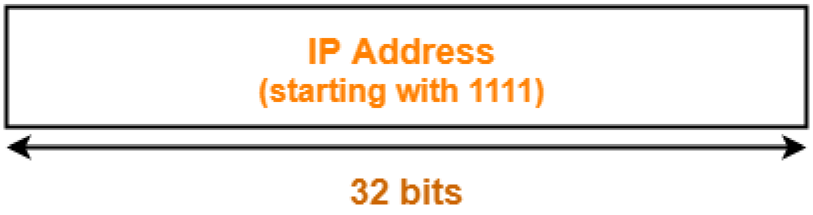
Maximum value of 1st octet = 11101111 = 239 So, Range of 1st octet = [224, 239]

- **Use-**

Class D is reserved for multicasting. In multicasting, there is no need to extract host address from the IP Address. This is because data is not destined for a particular host.

Class E- If the 32 bit binary address starts with bits 1111, then IP Address belongs to class E

Class E is not divided into Network ID and Host ID.



Class E IP Address

- **Total Number Of IP Addresses-**

Total number of IP Addresses available in class E = Numbers possible due to remaining available 28 bits = 2^{28}

- **Range Of 1st Octet-**We have-

Minimum value of 1st octet = **1111**0000 = 240

Maximum value of 1st octet = **1111**1111 = 255 So, Range of 1st octet = [240, 255]

Use- Class E is reserved for future or experimental purposes.

Rules for assigning Host ID:

The Host ID is used to determine the host within any network. The Host ID is assigned based on the following rules:

✓ The Host ID must be unique within any network.

✓ The Host ID in which all the bits are set to 0 cannot be assigned as it is used to represent the network ID of the IP address.

✓ The Host ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Rules for assigning Network ID:

If the hosts are located within the same local network, then they are assigned with the same network ID. The following are the rules for assigning Network ID:

✓ The network ID cannot start with 127 as 127 is used by Class A.

✓ The Network ID in which all the bits are set to 0 cannot be assigned as it is used to specify a particular host on the local network.

✓ The Network ID in which all the bits are set to 1 cannot be assigned as it is reserved for the multicast address.

Classes of IP Address- All the classes of IP Address are summarized in the following table-

Class of IP Address	**Total Number of IP Addresses**	**1st Octet Decimal Range**	**Number of Networks available**	**Hosts per network**	**Default Subnet Mask**
Class A	2^{31}	1 – 126	2^{7} – 2	2^{24} – 2	255.0.0.0
Class B	2^{30}	128 – 191	2^{14}	2^{16} – 2	255.255.0.0
Class C	2^{29}	192 – 223	2^{21}	2^{8} – 2	255.255.255.0
Class D	2^{28}	224 – 239	Not defined	Not defined	Not defined
Class E	2^{28}	240 – 254	Not defined	Not defined	Not defined

Classless Addressing

Classless Addressing is an improved IP Addressing system.

- ✓ It makes the allocation of IP Addresses more efficient.
- ✓ It replaces the older classful addressing system based on classes.
- ✓ It is also known as **Classless Inter Domain Routing (CIDR)**.

CIDR Block-

When a user asks for specific number of IP Addresses,

- ✓ CIDR dynamically assigns a block of IP Addresses based on certain rules.
- ✓ This block contains the required number of IP Addresses as demanded by the user.
- ✓ This block of IP Addresses is called as a **CIDR block**.

Rules for Creating CIDR Block- a CIDR block is created based on the following 3 rules-

Rule-01: All the IP Addresses in the CIDR block must be contiguous.

Rule-02:

- ✓ The size of the block must be presentable as power of 2.
- ✓ Size of the block is the total number of IP Addresses contained in the block.
- ✓ Size of any CIDR block will always be in the form 21, 22, 23, 24, 25 and so on.

Rule-03: First IP Address of the block must be divisible by the size of the block.

REMEMBER

If any binary pattern consisting of (m + n) bits is divided by 2n, then- Remainder is least significant n bits

- ✓ Quotient is most significant m bits
- ✓ So, any binary pattern is divisible by 2n, if and only if its least significant n bits are 0.

Examples-

Consider a binary pattern- 01100100.00000001.00000010.01000000 (represented as 100.1.2.64)

- ✓ It is divisible by 25 since its least significant 5 bits are zero.
- ✓ It is divisible by 26 since its least significant 6 bits are zero.
- ✓ It is not divisible by 27 since its least significant 7 bits are not zero.

CIDR Notation-

CIDR IP Addresses look like- a.b.c.d / n they end with a slash followed by a number called as IP network prefix.

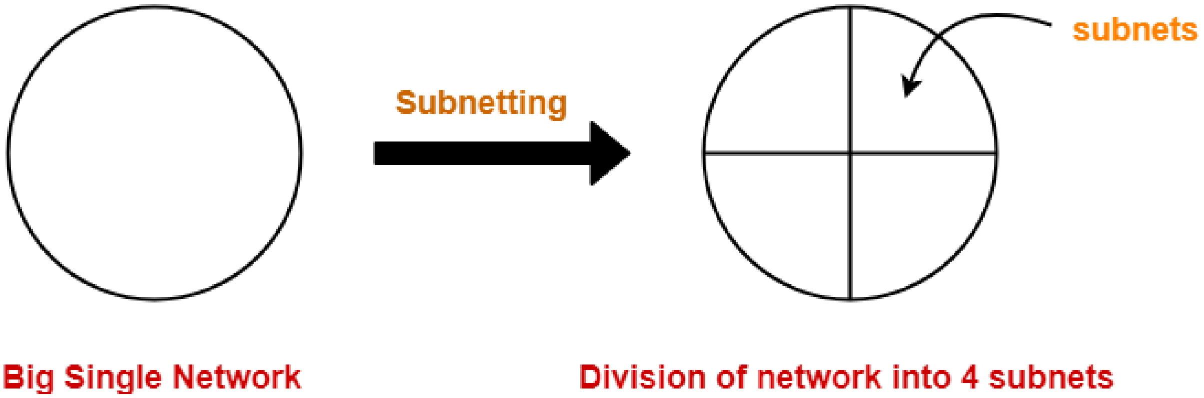
- ✓ IP network prefix tells the number of bits used for the identification of network.
- ✓ Remaining bits are used for the identification of hosts in the network.

Subnetting in Networking-

In networking,

- The process of dividing a single network into multiple sub networks is called as **subnetting**.
- The sub networks so created are called as **subnets.**

Example-Following diagram shows the subnetting of a big single network into 4 smaller subnets-



Advantages- The two main advantages of subnetting a network are-

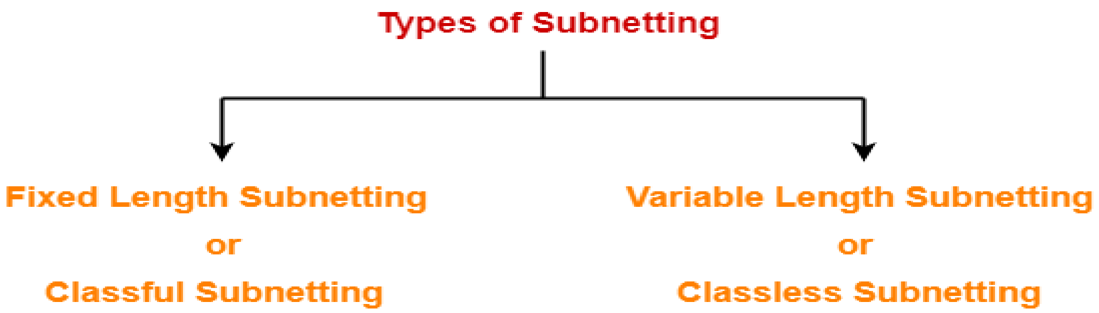
- It improves the security.
- The maintenance and administration of subnets is easy.

Subnet ID-Each subnet has its unique network address known as its **Subnet ID**.

- The subnet ID is created by borrowing some bits from the Host ID part of the IP Address.
- The number of bits borrowed depends on the number of subnets created.

Types of Subnetting-

Subnetting of a network may be carried out in the following two ways-



1. **Fixed Length Subnetting-** Fixed length subnetting also called as **classful subnetting** divides the network into subnets where-
   - ✓ All the subnets are of same size.
   - ✓ All the subnets have equal number of hosts.
   - ✓ All the subnets have same subnet mask.

2. **Variable Length Subnetting-** Variable length subnetting also called as **classless subnetting** divides the network into subnets where-
   - ✓ All the subnets are not of same size.
   - ✓ All the subnets do not have equal number of hosts.
   - ✓ All the subnets do not have same subnet mask.

Disadvantages of Subnetting-

1. Subnetting leads to loss of IP Addresses.

During subnetting,

- We have to face a loss of IP Addresses.
- This is because two IP Addresses are wasted for each subnet.
- One IP address is wasted for its network address.
- Other IP Address is wasted for its direct broadcasting address.

2. Subnetting leads to complicated communication process

After subnetting, the communication process becomes complex involving the following 4 steps-

- ✓ Identifying the network

✓ Identifying the sub network
✓ Identifying the host
✓ Identifying the process
✓

Subnet Mask Use- Subnet mask is used to determine to which network the given IP Address belongs to. Host use its subnet mask to determine whether the other host it wants to communicate with is present within the same network or not.

- If the destination host is present within the same network, then source host sends the packet directly to the destination host.
- If the destination host is present in some other network, then source host routes the packet to the default gateway (router).
- Router then sends the packet to the destination host.

IP Address Terminology

Static means the IP address never changes as long as you stay with the same provider or same server.

Dynamic means the IP address can change from time-to-time.

Public means the IP address can be reached via the Internet from any computer in the world.

Private means the IP address can only be reached by other devices on the same network.

Shared means other people besides you use your IP address for their connection.

Dedicated means no one else uses your IP address for their connection.

Class identifies the range of your IP address and the default subnet mask. Examples of IP classes:

□ A class - 0 to 127 with default mask of 255.0.0.0

□ B class - 128 to 191 with default mask of 255.255.0.0

□ C class - 192 to 223 with default mask of 255.255.255.0

□ D class - 224 to 247 (not currently used)

□ E class - 248 to 255 (not currently used)

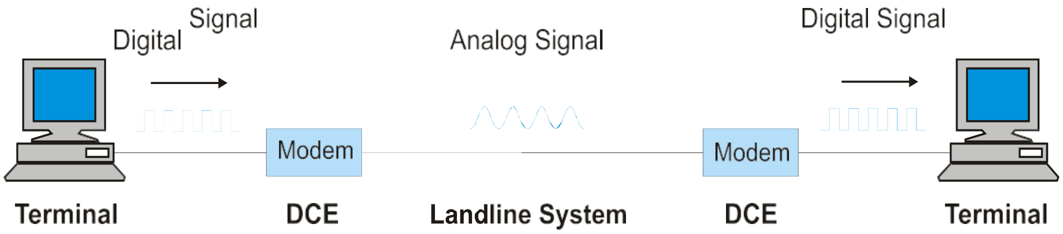
- the incoming and outgoing carriers can be easily implemented.

Modems and multiplexers

Introduction

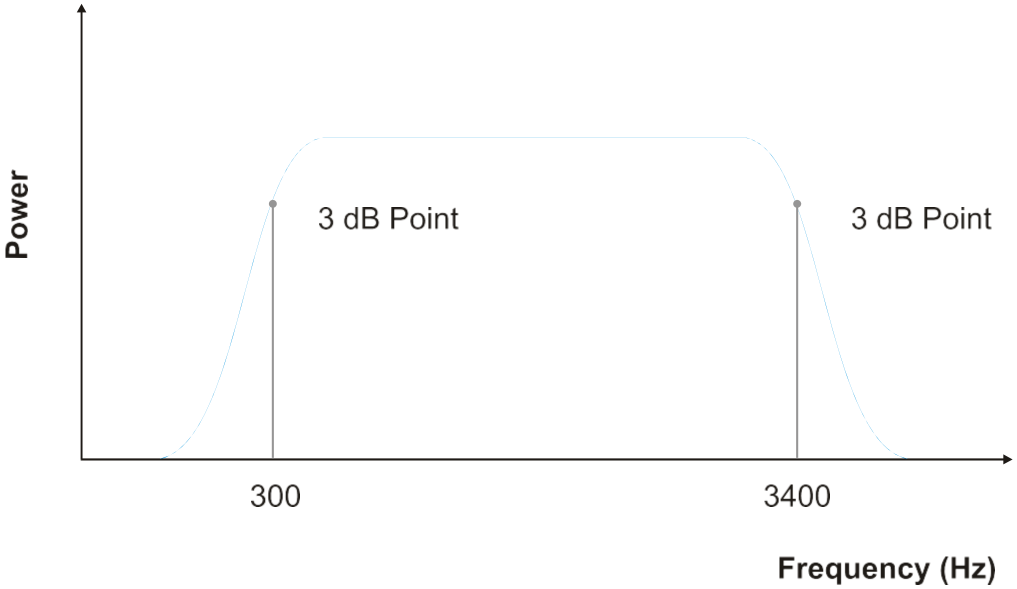
Communications systems, whether they are telephone, landline, or radio, cannot directly transport digital information without some distortion of the signal. This is due to the bandwidth limitation inherent in any of the interconnecting media.

A conversion device, called a modem (modulator/demodulator), is required to convert the digital signals generated by the transmitting device into an analog form suitable for long-distance transmission. The demodulator in the receiving modem receives analogue information and converts it back to the original digital format. Figure 7.1 gives a schematic view of the position of the modem in the communications hierarchy.



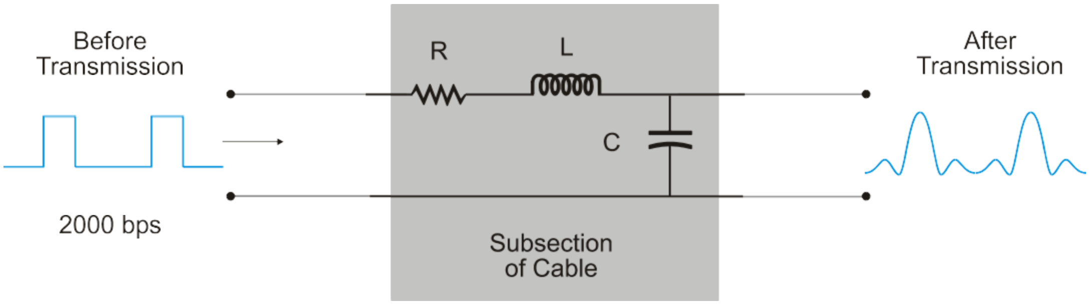
The modem as a component in a typical communication system

The bandwidth in a telephone network is limited by cable resistance, capacitance and inductance. The bandwidth is defined as the difference between the upper and lower allowable frequency and is typically 300 Hz to 3400 Hz for a telephone cable. This is illustrated in below fig. The -3dB points are, by definition, the frequencies at which the output power on the receiving end has fallen to half the input power at the transmitting end.



The bandwidth limitation problem

An example of what a digital signal would look like at the far end of a cable, without conversion to an analog signal



Injection of a digital signal down a cable

Modes of operation

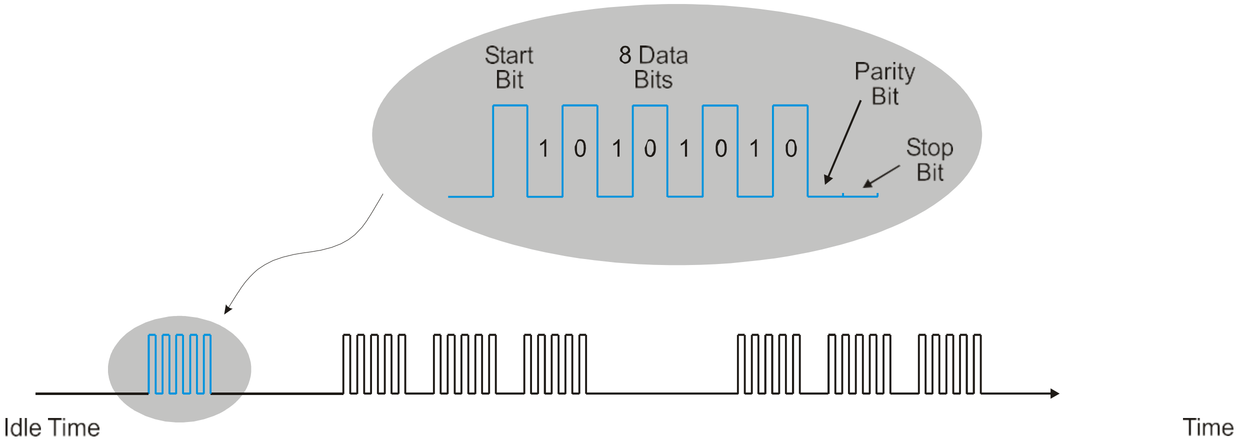
Modems can operate in two modes, namely **half-duplex and full duplex.** A full-duplex system is more efficient than a half-duplex system, as data can flow in both directions simultaneously. A full-duplex system requires a communication capacity of at least twice that of a half-duplex system, where data can flow in both directions, but in only one direction at a time.

Synchronous or asynchronous

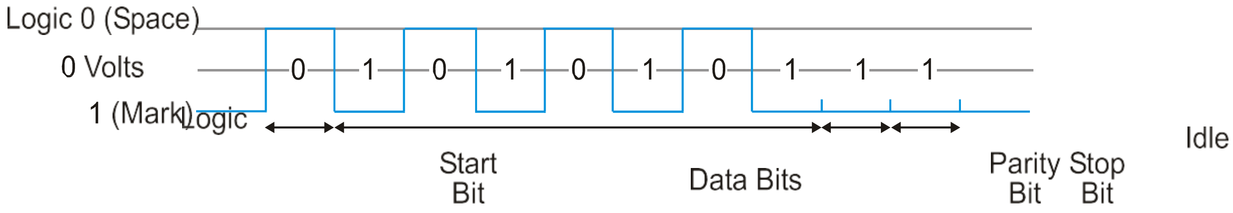
Modems can operate in either of two modes, namely asynchronous and synchronous.

Asynchronous

In asynchronous communication each character is encoded with a start bit at the beginning of the character bit stream and a parity and stop bit at the end of the character bit stream. The start bit allows the receiver to synchronize with the transmitter so that the receiver looks for each character as it is sent. Once the character has been received the communications link returns to the idle state and the receiver waits for the next start bit indicating the arrival of the next character. This is illustrated in below fig.



Asynchronous transmission of a few characters

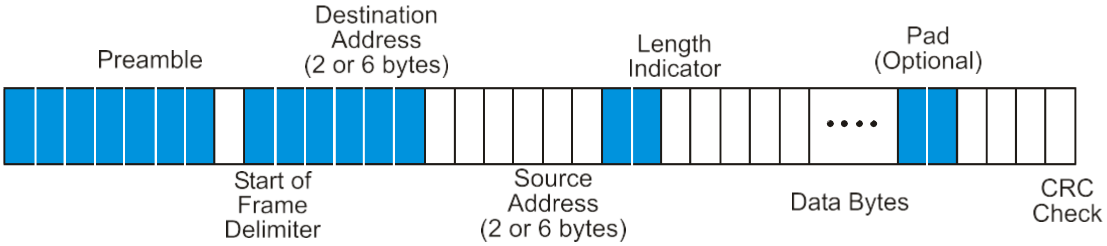


Format of a typical serial asynchronous frame

Synchronous communications

Synchronous communication relies on all characters being sent in a continuous bit stream. The first few bytes in the message contain synchronization data allowing the receiver to synchronize to the incoming bit stream. Synchronization is then maintained by a timing signal or clock. The receiver follows the incoming bit stream and maintains a close

synchronization between the transmitter clock and receiver clock. Synchronous communication provides for far higher speeds of transmission of data, but is avoided in many systems because of the greater technical complexity of the communications' hardware.



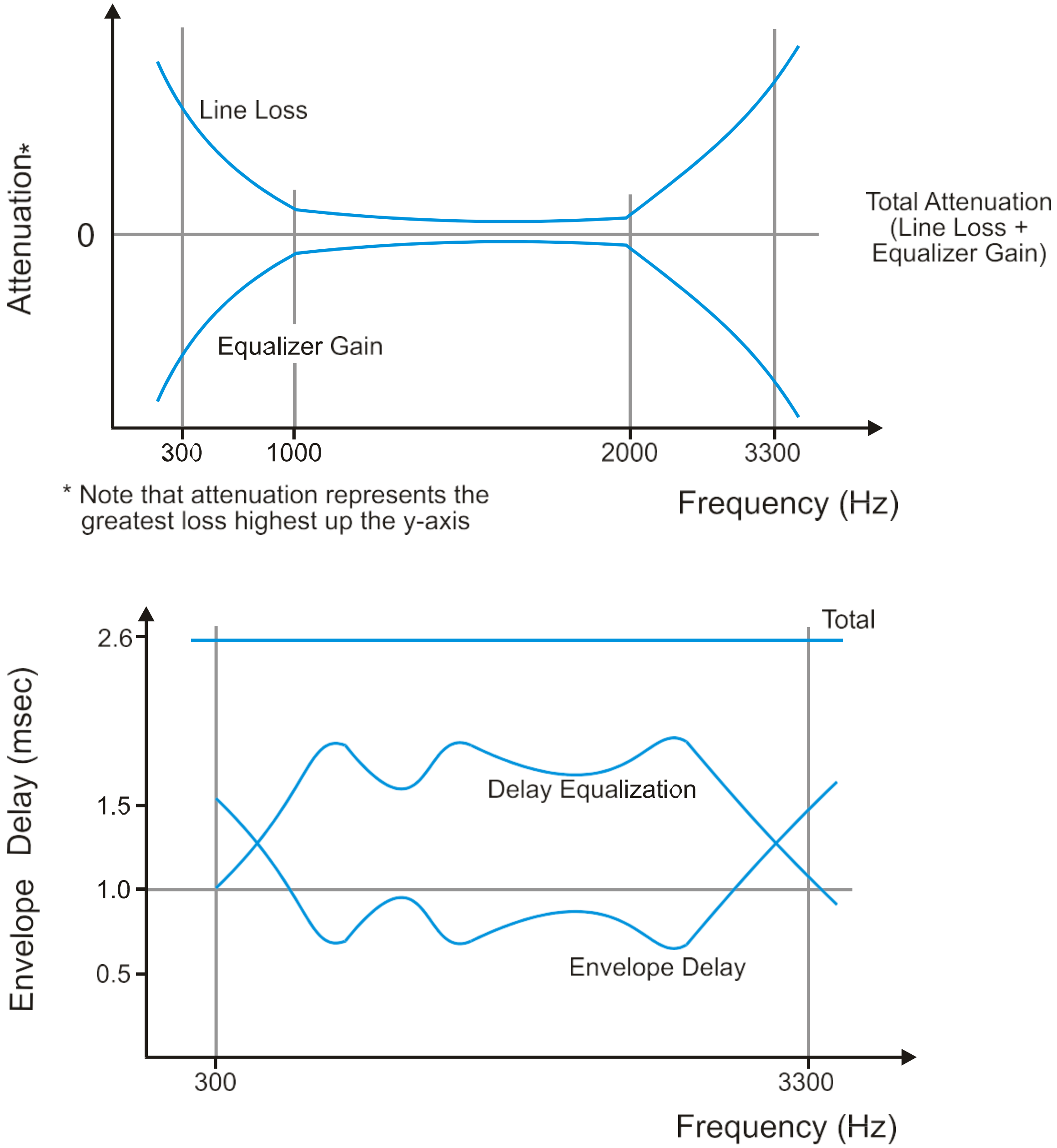
Synchronous communication protocol frame

The major difference between asynchronous and synchronous communications with modems is the need for timing signals.

A synchronous modem outputs a square wave on Pin 15 of the RS-232 DB-25 connector. Pin 15 is called the Transmit Clock pin or, more formally, the DCE Transmitter Signal Element Timing Pin. The square wave is set to the frequency of the modem's bit rate. The attached transmitting device, the DTE, synchronizes its transmission of data from Pin 2 to the modem.

Distortion

There are two significant causes of distortion in the signal during communications . These are attenuation distortion and envelope delay distortion. Both forms of distortion are illustrated in below figure.



Attenuation distortion and envelope delay

Attenuation distortion

Attenuation distortion is the reason why the theoretical smooth, horizontal plot of power transmitted versus frequency is not realized in practice. Higher frequencies tend to attenuate more easily and attenuation becomes more non-linear at the edges of the operating bandwidth, or ‘passband’. Hence, the ‘equalizer’ compensates with an equal and opposite effect, giving a constant total loss throughout the passband.

Envelope delay distortion

Envelope delay distortion reflects the reality of transmission of signals down a line where the phase change to frequency is non-linear, i.e. the phase tends to alter as the signal is transmitted down the communications link. The phase delay is calculated by dividing the phase by the frequency of the signal at any point along the line. The slope of phase versus frequency is called the envelope delay. Delay distortion causes problems in that two different frequencies (respectively indicating ‘1’ and ‘0’) interfere with each other at the receiving modem, thus causing a potential error through what is called inter-symbol interference.

Modulation techniques

The modulation process modifies the characteristics of a sinusoidal carrier signal, which can be represented with the equation:

$$F(t) = A \sin (2\pi\, ft + \square)$$

where:

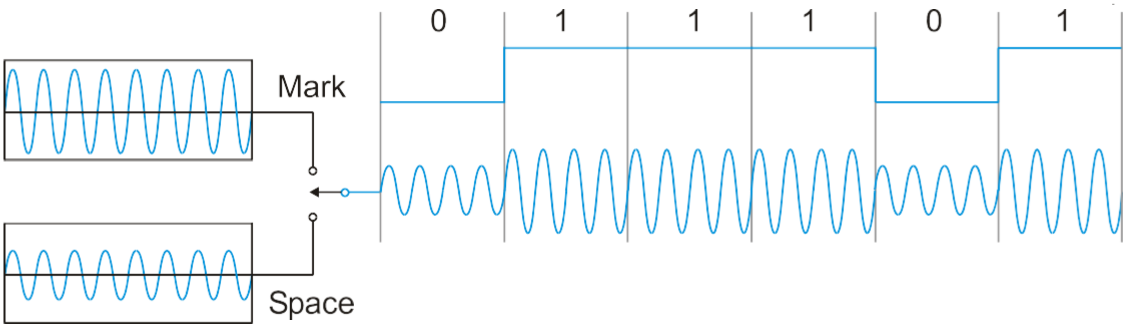
$F(t)$	=	instantaneous value of voltage at time t
A	=	maximum amplitude
f	=	frequency
$\square$	=	phase angle

There are several modulation techniques, including:

- Amplitude Modulation (AM)
- Amplitude Shift Keying (ASK)
- Frequency Modulation (FM)
- Frequency Shift Keying (FSK)
- Phase Modulation (PM)
- Phase Shift Keying (PSK)
- Quadrature Amplitude Modulation (QAM)

Amplitude Shift Keying (ASK)

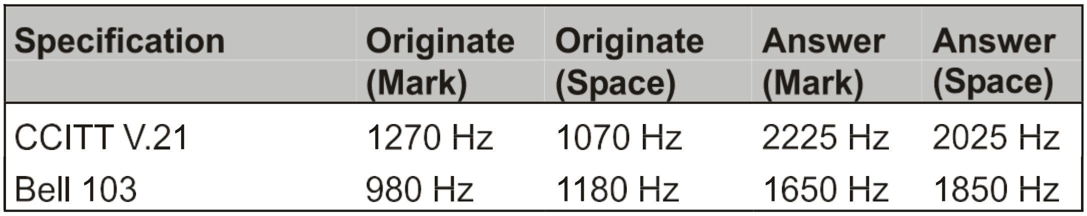
In AM, the amplitude of the carrier signal is varied according to the amplitude of the incoming analog data. A special case of AM is ASK, where the input is a digital stream with only two levels representing ‘1’ and ‘0’. ASK is sometimes still used for low data rates, however, it does have difficulty distinguishing the signal from the noise, as noise in the communications channel is an amplitude-based phenomenon. This form of modulation is indicated in Figure.



Operation of ASK

Frequency Shift Keying (FSK)

In FM the frequency of the carrier is varied in accordance with the analog input signal. A special case of FM is FSK, which allocates different frequencies to logic ‘1’ and logic ‘0’ of the binary data message. FSK is primarily used by modems operating at data rates of up to 300 bps in full-duplex mode and 1200 bps in half- duplex mode.
The frequencies for the Bell 103/113 and the compatible ITU V.21 standards are shown in Table



Specification	Originate (Mark)	Originate (Space)	Answer (Mark)	Answer (Space)
CCITT V.21	1270 Hz	1070 Hz	2225 Hz	2025 Hz
Bell 103	980 Hz	1180 Hz	1650 Hz	1850 Hz

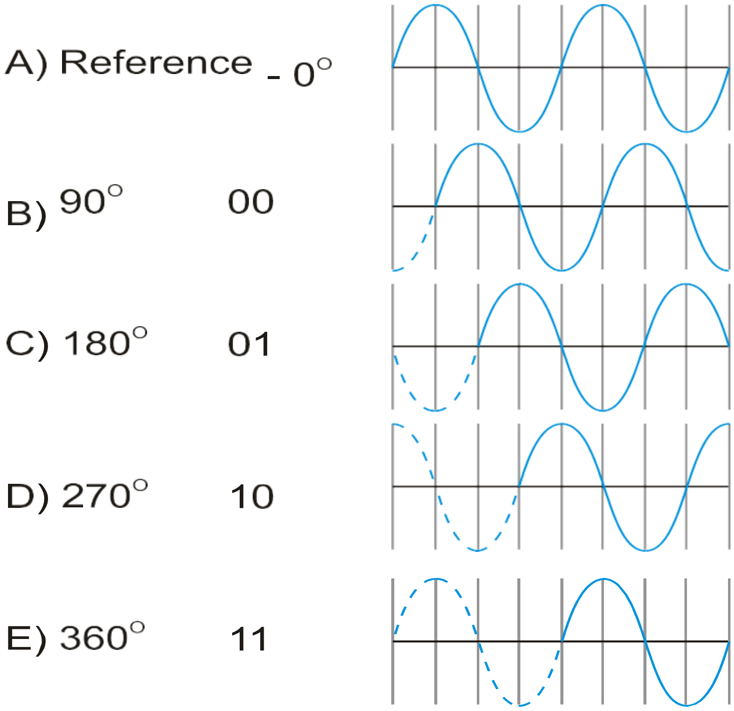
CCITT V.21 and Bell System 103/113 modems frequency allocation

Phase Shift Keying (PSK)

PM is the process of varying the carrier signal by phase in accordance with the input signal. PSK is a special case where the input signal is of a binary nature. There are two forms of PSK, viz. Quadrature Phase Shift Keying (QPSK) and Differential PSK

QPSK

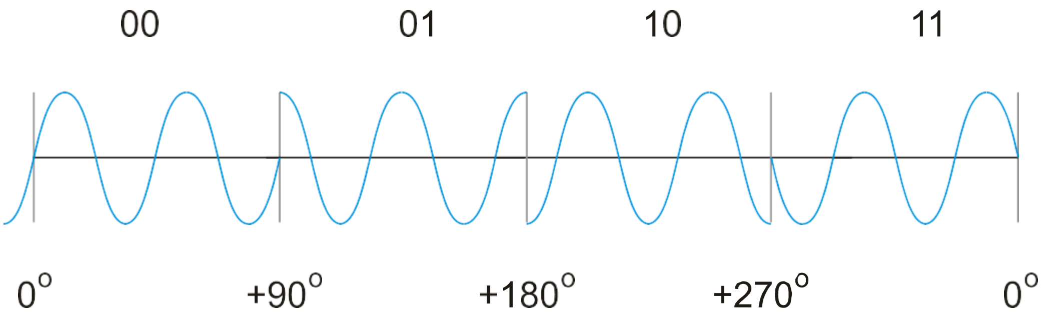
In QPSK four phase angles are used for encoding, viz. 0°, 90°, 180° and 270°. There are four phase angles possible at any one time, allowing the basic unit of data to be a 2-bit pair, or 'dibit'. The four ‘constellation points (B through E) are measured in terms of a reference signal (A) as indicated in below Figure.



Quadrature Phase Shift Keying

Differential PSK

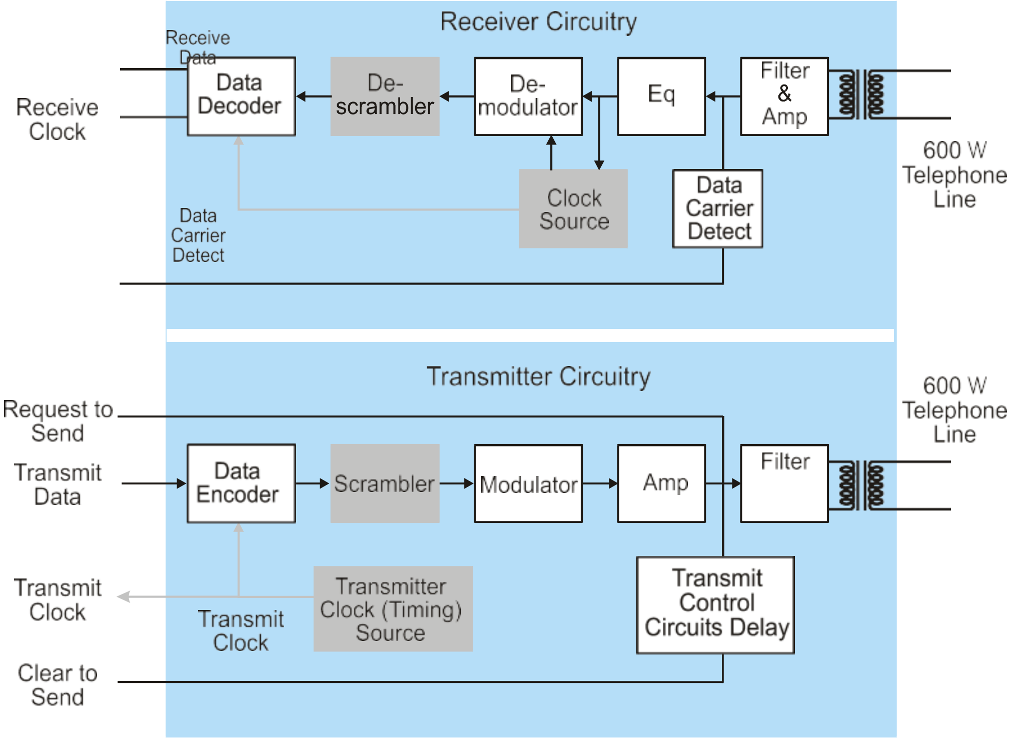
In Differential PSK the phase angle for each cycle is calculated relative to the previous cycle as shown in below Figure



Differential PS

Components of a modem

The components of a modem are indicated in Figure.



Basic components of a modem

The components of a modem can be divided into two areas, viz. the modem transmitter and the modem receiver.

Modem transmitter

The modem transmitter contains a data encoder, scrambler, modulator and amplifier.

Data encoder

The data encoder takes the serial bit stream and uses multi-level encoding, where each signal change represents more than one bit of data, to encode the data. Depending on the modulation technique used the bit rate can be two, four, or more times the baud rate.

Scrambler

The scrambler is used for synchronous operation only. It modifies the bit stream so that long sequences of 1s and 0s do not occur. Long sequences of 1s and 0s are difficult to use in synchronous circuits because of the difficulties they cause in extracting clocking information.

Modulator

The bit stream is converted into the appropriate analogue form using the selected modulation technique. Where initial contact is established with the receiving modem, a carrier is put on the line.

Amplifier

The amplifier increases the level of the signal to the appropriate level for the telephone line and matches the impedance of the line.

Modem receiver

The modem receiver contains a filter and amplifier, equalizer, demodulator, descrambler and data decoder

Filter and amplifier

Noise is removed from the signal and the resultant signal is amplified.

Equalizer

The equalizer minimizes the effect of attenuation and delay on the various components of the transmitted signal. A predefined modulated signal, called a training signal, is sent down the line by the transmitting modem. The receiving modem knows the ideal characteristics of the training signal and the equalizer will adjust its parameters to correct for the attenuation and delay characteristics of the signal.

Demodulator

The demodulator retrieves the bit stream from the analogue signal.

Descrambler

The descrambler is used in synchronous operation only. The descrambler restores the data to its original serial form after it has been encoded in the scrambler circuit, ensuring that long sequences of 1s and 0s do not occur.

Data decoder

The final bit stream is produced in the data decoder in true RS-232 format.

Types of modem

There are two types of wire modems available today, namely **dumb, or non-intelligent** modems, and **smart modems** (Hayes compatible).

Dumb modems

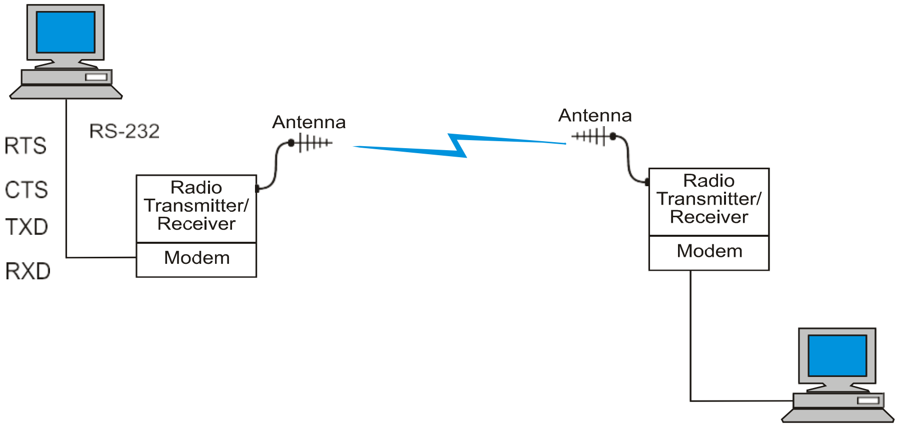
Dumb, or non-intelligent, modems depend on the computer to which they are connected to instruct the modem when to perform most of its tasks such as answering the telephone.

Smart modems

Smart modems have an on-board microprocessor enabling them to perform such functions as automatic dialing and selection of the appropriate method of modulation.
As defined by RS-232, any interaction between a traditional dumb modem and the computer equipment occurs by exchanging signal voltages across wires.

Radio modems

Radio modems are suitable for replacing landlines to remote sites or as a backup to wire or fiber-optic circuits, and are designed to ensure that computers and PLCs, for example, can communicate transparently over a radio link without any specific modifications.



Radio modem configuration

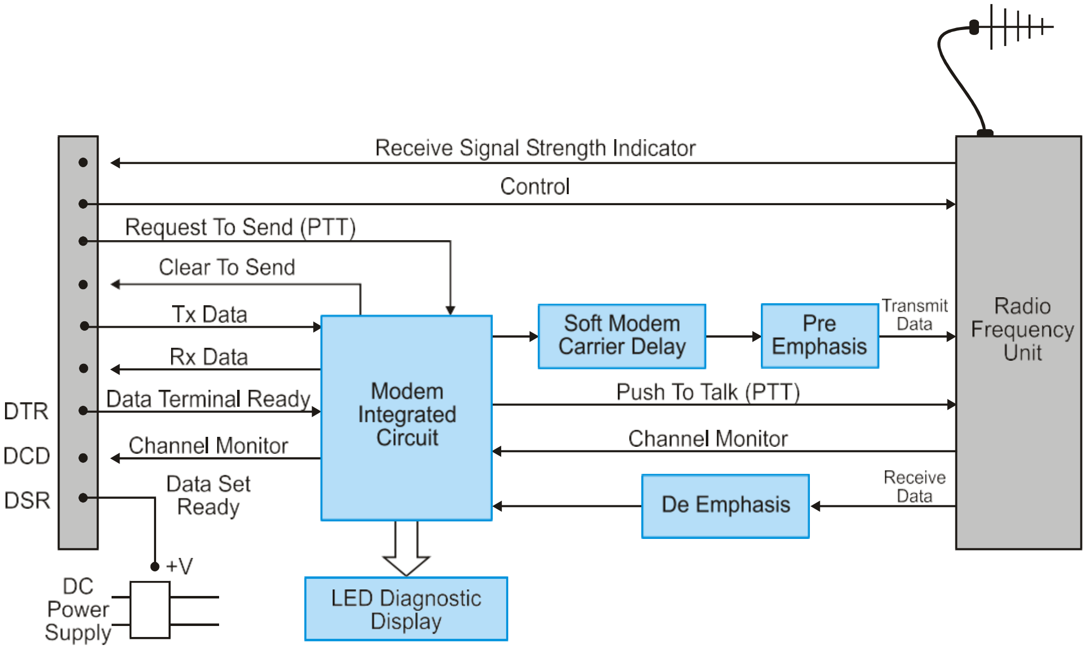
Modern radio modems operate in the 400 to 900 MHz band. Propagation in this band requires a free line-of-sight between transmitting and receiving antennae for reliable communications. Radio modems can be operated in a network, but require a network management software system (protocols) to manage network access and error detection. Often, a master station with hot change-over communicates with multiple radio field stations. The protocol for these applications can use a simple poll/response technique.

.

The interface to the radio modem is typically RS-232, but RS-422, RS-485, and fiber optics are also options. Typical speeds of operation are up to 9600 bps. A buffer is required in the modem and is typically a minimum of 32 kilobytes. Hardware and software flow control techniques are normally provided in the radio modem firmware, ensuring that there is no loss of data between the radio modem and the connecting terminal.

Typical modulation techniques are two level direct FM (1200 to 4800 bps) to three level direct FM (9600 bps).

A typical schematic of a radio modem is given in below Figure.



Typical block diagram of a radio modem

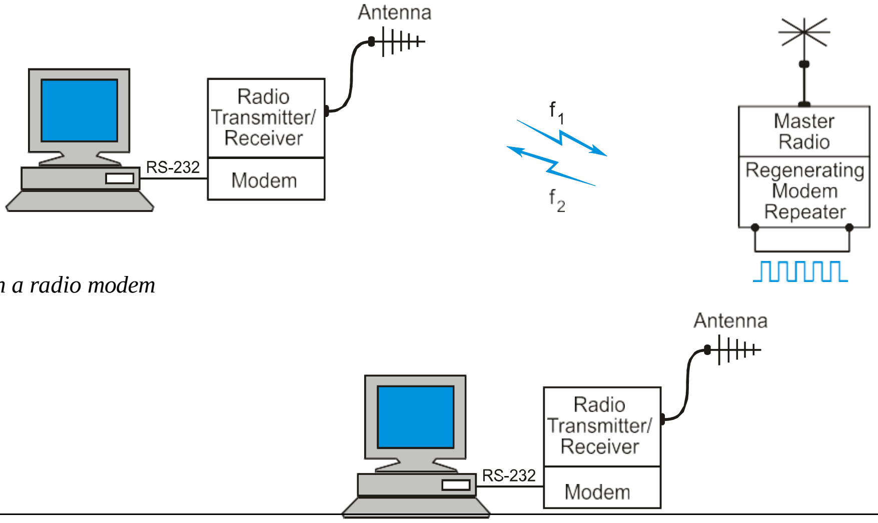
Modes of radio modems

Radio modems can be used in either point-to-point or point-to-multi-point. A point-to-point system can operate in continuous RF mode, which has a minimal turn-on delay in transmission of data, and non-continuous mode where there is a considerable energy saving. The RTS to CTS delay for continuous and switched carriers is of the order of 10 ms and 20 ms respectively.

A point-to-multi-point system generally operates with only the master and one radio modem at a time.

In a multi-point system, if the data link includes a repeater, data regeneration must be performed to eliminate signal distortion and jitter. Regeneration is not necessary for voice systems where some error is tolerable.

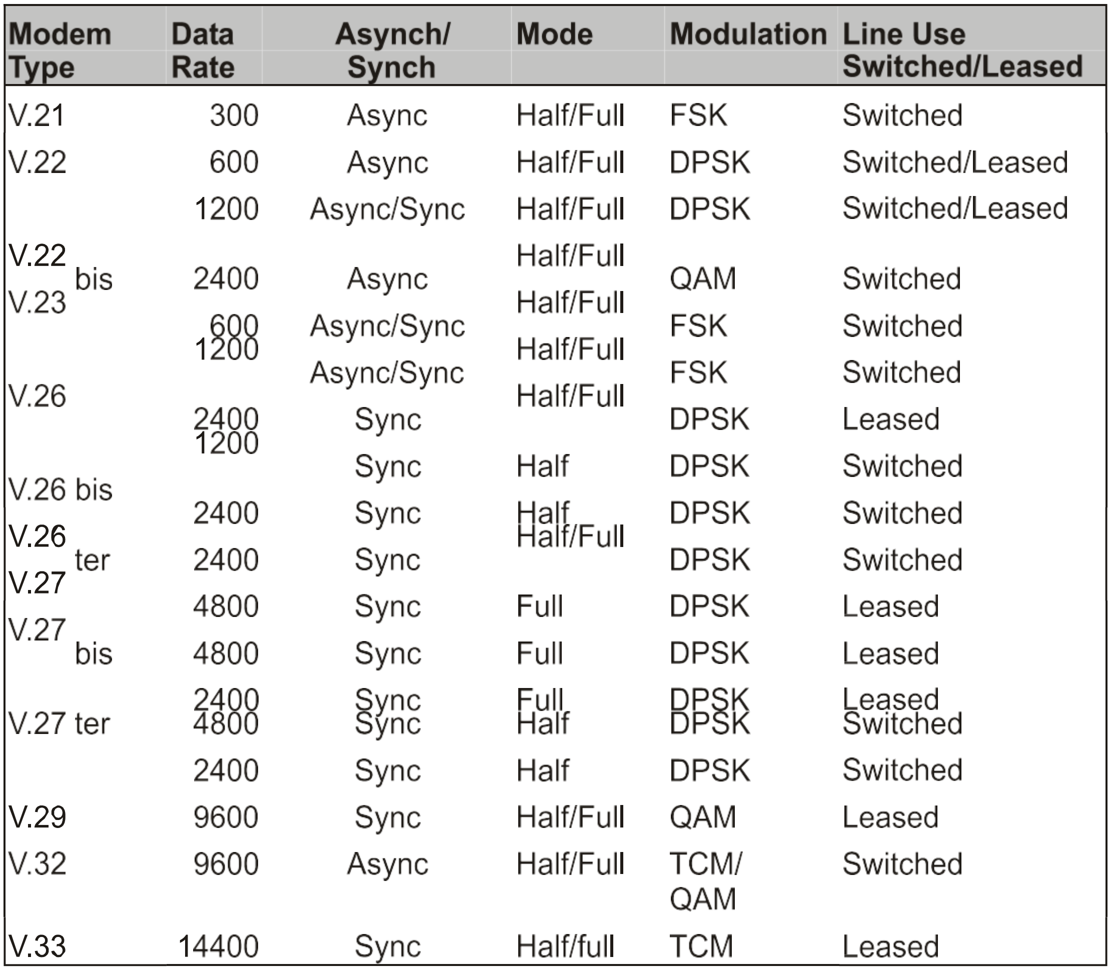
Regeneration is performed by passing the radio signal through the modem, which converts the RF analogue signal back to a digital signal and then applies this output binary data stream to the other transmitting modem, which repeats the RF analogue signal to the next location.


Antenna
Radio Transmitter/ Receiver
Modem
RS-232
f1
f2
Master Radio
Regenerating Modem Repeater
Antenna
Radio Transmitter/ Receiver
Modem
RS-232

Regeneration of a signal with a radio modem

Modem standards

Table below summarizes the ITU-T modem standards.



Modem Type	Data Rate	Asynch/ Synch	Mode	Modulation	Line Use Switched/Leased
V.21	300	Async	Half/Full	FSK	Switched
V.22	600	Async	Half/Full	DPSK	Switched/Leased
	1200	Async/Sync	Half/Full	DPSK	Switched/Leased
V.22			Half/Full		
bis	2400	Async		QAM	Switched
V.23			Half/Full		
	600	Async/Sync		FSK	Switched
	1200		Half/Full		
		Async/Sync		FSK	Switched
V.26			Half/Full		
	2400	Sync		DPSK	Leased
	1200				
		Sync	Half	DPSK	Switched
V.26 bis					
	2400	Sync	Half	DPSK	Switched
V.26			Half/Full		
ter	2400	Sync		DPSK	Switched
V.27					
	4800	Sync	Full	DPSK	Leased
V.27					
bis	4800	Sync	Full	DPSK	Leased
	2400	Sync	Full	DPSK	Leased
V.27 ter	4800	Sync	Half	DPSK	Switched
	2400	Sync	Half	DPSK	Switched
V.29	9600	Sync	Half/Full	QAM	Leased
V.32	9600	Async	Half/Full	TCM/ QAM	Switched
V.33	14400	Sync	Half/full	TCM	Leased

ITU-T Modem standards

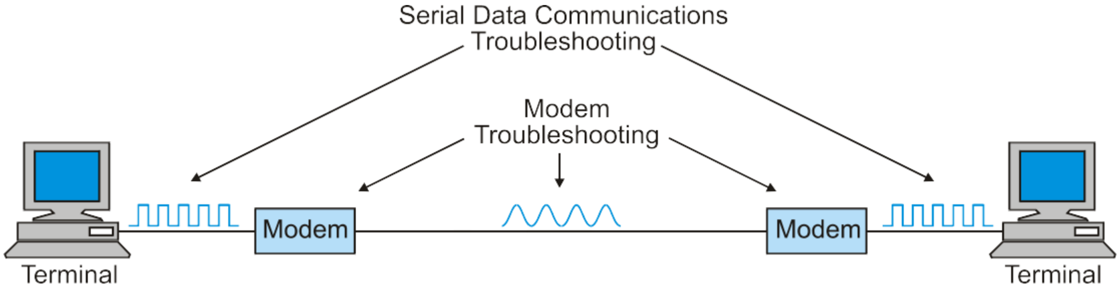
ITU V.34 and V.90 are high-speed dialup modem standards that are commonly used to connect to the Internet. The V.34 and V.90 standards use a modulation scheme very similar to V.22bis. It has a symbol (baud) rate of 3429 symbols per second and can transmit up to 10 bits per symbol. With overheads, this averages out to approximately 33.6 kbps.

V.34 and V.90 use a modified QAM system called ‘super constellation’ that has 1664 possible symbol combinations, though not all symbols are used in every conversation. At the beginning of the conversation the modems transmit special test strings that are used to formulate the best possible connection. The V.34 and V.90 modems will accept asynchronous data from the modem, and then change this to synchronous before sending it down the telephone line. Both standards also use a scrambler and Trellis coding to increase the quality of the signal.

V.90 modems, like the V.34 modems, check the telephone line when they first connect and can modify their parameters for optimal data communications. They also can change parameters midstream if either modem sees the need.

Troubleshooting a system using modems

There are two aspects to troubleshooting a system that uses modems. These relate to satisfactory operation of the RS-232 system, as well as to specifics of the modem



Troubleshooting a system using modems

Troubleshooting the modem

There are various tests available for troubleshooting operational problems associated with a modem, which fall into two categories viz. self-tests and loop-back tests.

Self-test

For a self-test the modem connects its transmitter to its receiver. The connection with the communications line is interrupted and a specified sequence of bits is transmitted to the receiving parts of the modem where this is then compared with a defined pattern. An error will be indicated on the modem front panel if there is a mismatch.

Loop-back tests

The second set of tests is the loop-back tests. There are four forms of loop back tests viz:

- Local digital loop to test the terminal or computer and connecting RS-232 line
- Local analog loop to test the modem’s modulator and demodulator circuitry
- Remote analog loop to test the connecting cable and local modem
- Remote digital loop to test the local and remote modem and connecting cable

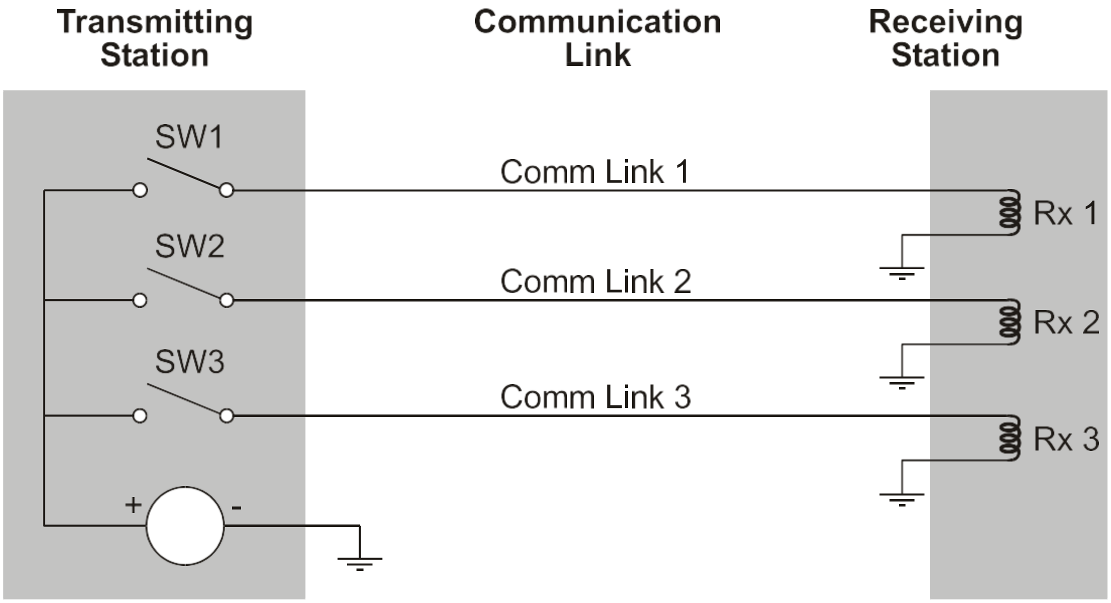
Multiplexing concepts

Multiplexing allows an existing channel to be used for more than one message at a time and has the potential to dramatically expand line utilization. It should be noted that multiple stages of multiplexing are possible. De-multiplexing is the process of extracting the individual channel messages from the multiplexed data.
There are three possible multiplexing techniques viz.

- Space Division Multiplexing (SDM),
- Frequency Division Multiplexing (FDM)
- Time Division Multiplexing (TDM).

SDM

SDM is where multiple paths are created by running new physical channels next to the existing ones to connect a receiver and transmitter as shown in Figure 7.24. Some authorities feel that SDM is not a true multiplexing method. The technique is generally considered unattractive because additional cables, transmitters, and receivers are required



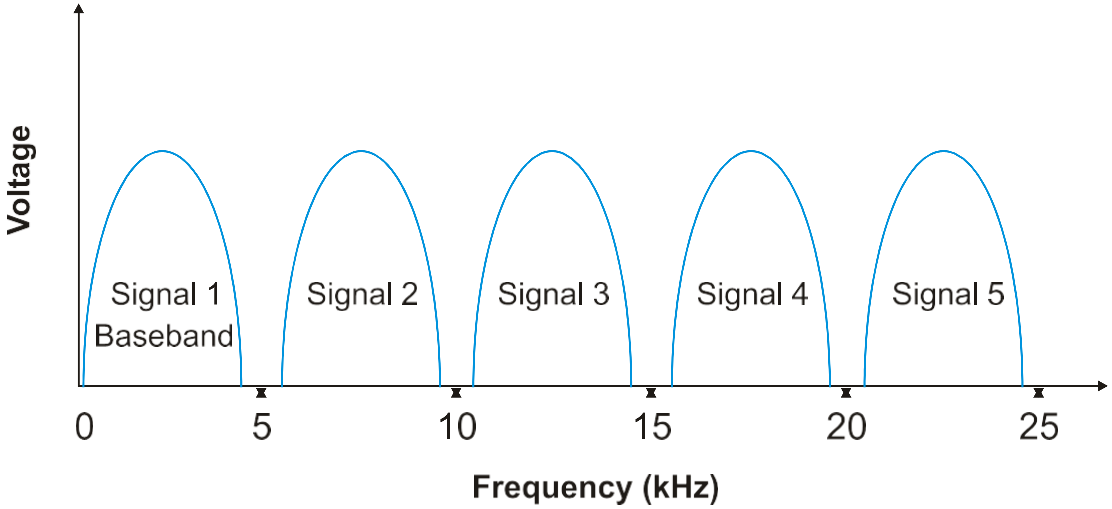
Space division multiplexing

The best example of SDM is the local telephone system. Each telephone is connected to the central office by a local loop not shared by other sub-scribers. Demultiplexing SDM systems is virtually unnecessary as each signal has its own independent link and receiver/transmitter equipment.

FDM

FDM is where different, unique carrier frequencies are used by each channel, allowing several channels to use the same medium e.g. electrical cable. FDM therefore requires that the bandwidth of the link is greater than the aggregate of the bandwidths of the individual channels.

FDM is used extensively in telemetry and radio/TV broadcast applications where each signal representing, for example, temperature, pressure or speed, is within a 0–1 V range, and each signal has an overall bandwidth of no more than 4000 Hz. A basic signal of 0– 4 kHz is called the 'baseband' signal. All of these baseband signals are multiplexed with various sub-carriers spaced 5 kHz apart with a bandwidth extending from 0 Hz to 4 kHz times the number of telemetry channels. Figure 7.26 gives an example of the division of the frequency spectrum.

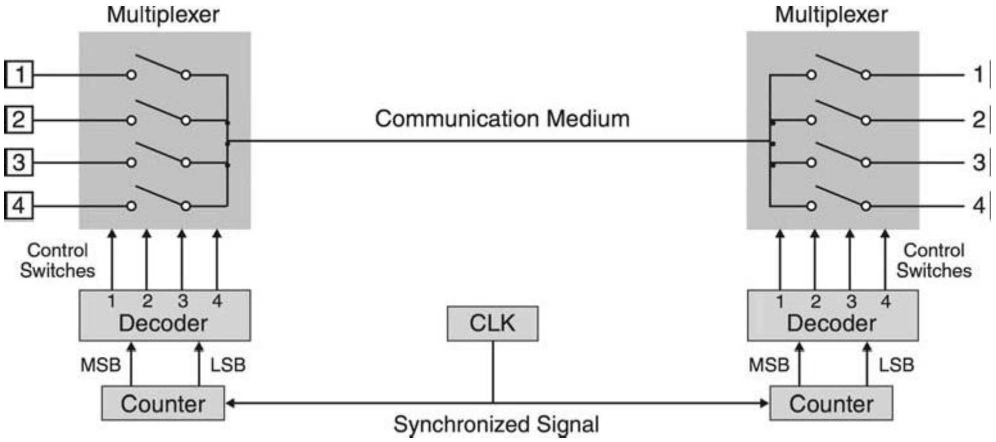


FDM spectrum containing five signals

TDM

In a communications system it is possible for many users to time-share the physical links by switching each signal for a short period of time, as in Figure 7.28. As the scanning rate rises, the system will eventually become ineffective because of an increase in propagation delays, noise, errors and re-transmissions.

Unlike analog signals, digital TDM has greater latitude in sampling each bit of each channel. As long as samples occur within the bit period, even though it may be late or early in the specific bit period, no data will be lost. The greatest limitation of TDM lies in the bandwidth of the communications medium. As the bit rate increases, the frequency requirement of that medium also increases.



Computer Ports

The computer ports are physical docking points of a computer that facilitate users to connect required external devices to the computer or computer network. A connection point that acts as an interface between the computer and external devices like a mouse, printer, modem, etc. is called a port. Ports are of two types −

- **Internal port** − It connects the motherboard to internal devices like hard disk drives, CD drives, internal modems, etc.
- **External port** − It connects the motherboard to external devices like modem, mouse, printer, flash drives, etc.

Expansion of a computer network or interconnection between multiple peripheral devices was possible through computer ports where network connections start and end. Generally, Ports are computer hardware which are software-based means they are operated by a software program like an operating system.

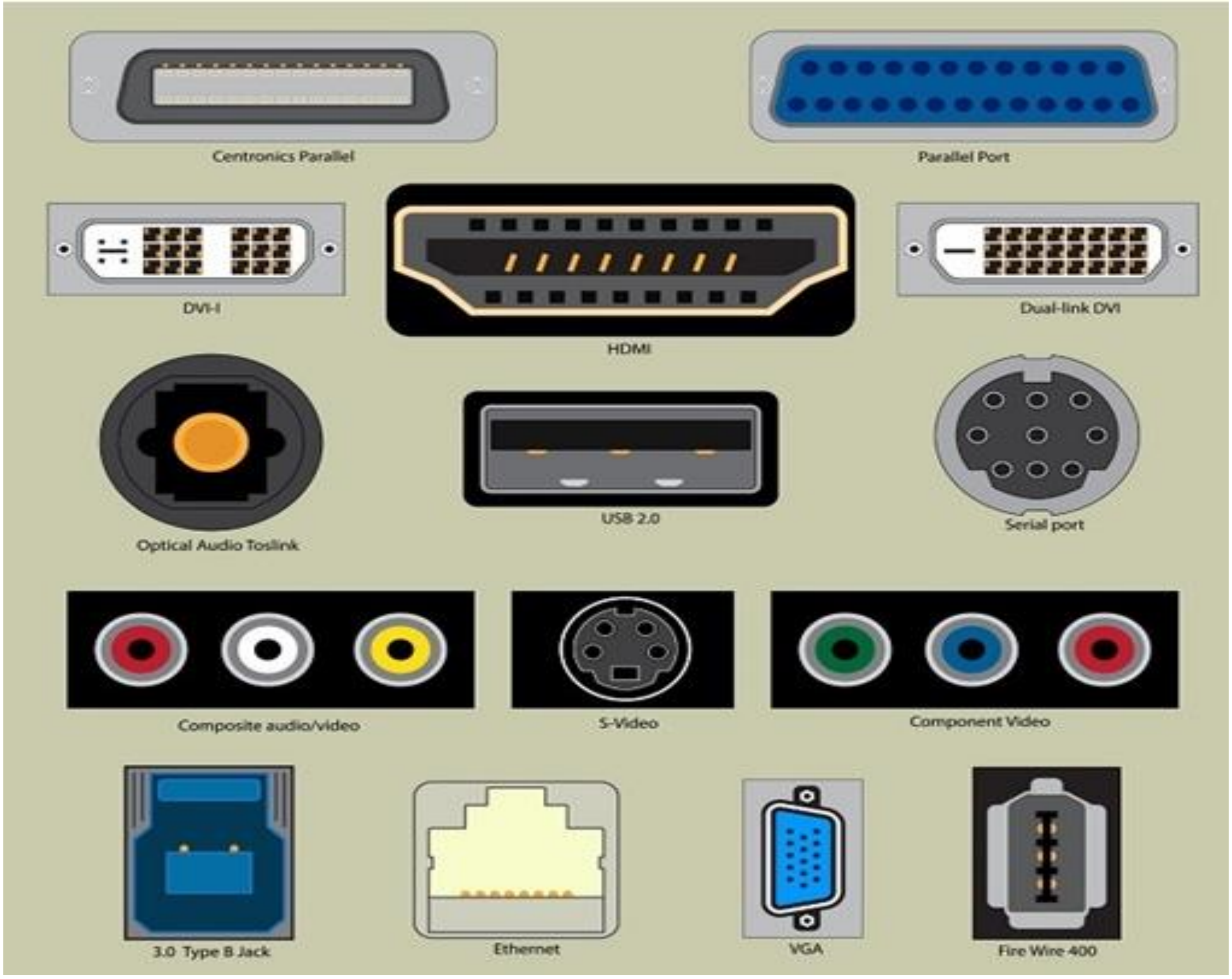


Fig: Some most commonly used computer/ networking ports

Serial Port

In the past, it was used to connect different devices which includes modems, mice, and printers; however, due to the prominence of USB, it has become completely obsolete in modern computers. Serial ports transmit data sequentially means one bit at a time. To do the same, these ports require one cable to transmit 8 bits. However, this makes slower communication. Serial ports are usually having 9-pin or 25-pin male connectors. They are also known as COM (communication) ports or RS323C ports.

Parallel Ports

This is primarily used for connecting printers and other devices that are used for external storage; like serial ports, parallel ports are rarely found on modern computers. Parallel ports can send or receive 8 bits or 1 byte at a time. Parallel ports come in the form of 25-pin female pins and are used to connect printers, scanners, external hard disk drives, etc.

PS/2 Port

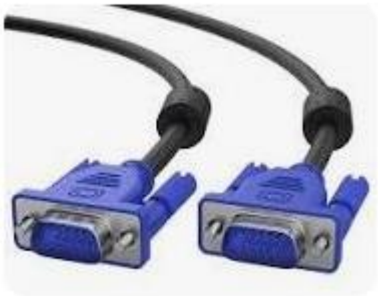
PS/2 stands for Personal System/2. It is a female 6-pin port standard that connects to the male mini-DIN cable. PS/2 was introduced by IBM to connect Input/output peripherals to personal computers. Used to create a connection between keyboards and mice on computers that is of an earlier generation. PS/2 ports have a circular shape, and they are coloured purple for keyboards and green for mice.

Universal Serial Bus (or USB) Port

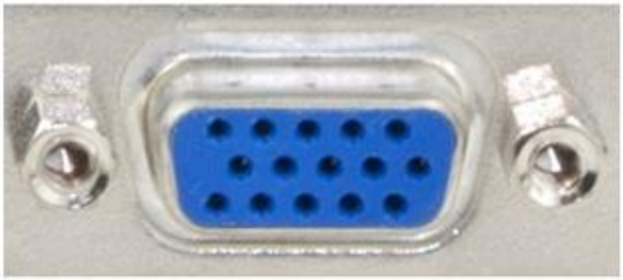
USB stands for Universal Serial Bus. It is the industry standard for short-distance digital data connection. It is one of the most popular ports for connecting accessories, including external hard drives, printers, mice, keyboards, and more. There are different types and sizes of USB ports, such as micro-USB, USB-A, USB-B, and USB-C.USB port is a standardized port to connect a variety of devices like printers, cameras, keyboards, speakers, etc.

VGA (Video Graphics Array) Port

Before the development of DVI, HDMI and DisplayPort, VGA was in use; it's an analogue interface between a computer and the monitor. It's a display standard developed by IBM in 1987; VGA replaced the existing digital CGA and EGA interfaces with a smaller resolution and fewer colours. A standard VGA works on 16-color displays with a refresh rate of 60 Hz and a resolution of 640 × 480. There are 256 colours shown if the resolution is lowered to 320 x 200. Nowadays, it's not in use, older PCs and displays have this video port. Digital connections like HDMI and DisplayPort are replacing it.



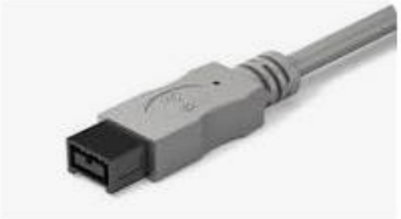
VGA Cable



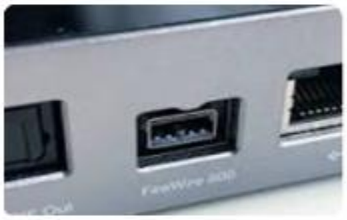
VGA Connector

Firewire Port

An interface with a high data transfer rate is generally utilized for connecting digital camcorders, external hard drives, and other multimedia equipment. USB and Thunderbolt have mostly superseded it. Hence, a FireWire is a high-speed computer data transfer interface that is used to connect personal computers, audio and video devices, as well as other professional and consumer electronic products.



FireWire Connector



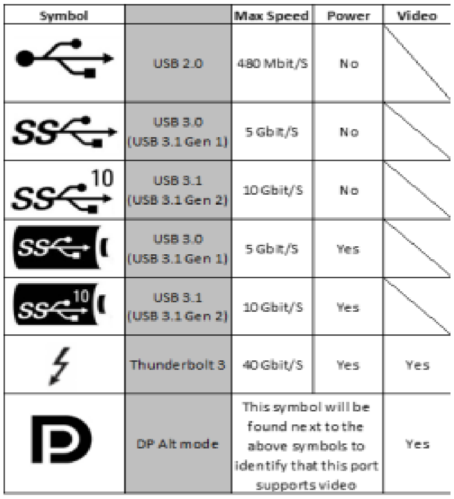
FireWire Port

Ethernet Port

An Ethernet port also known as a jack or socket is a port used to access the internet on commuter. Enables wired network connections, which are normally used for connecting computers to routers, switches and modems that allow Internet access. It's like computer network equipment that Ethernet cables plug into. The main goal of this port is to connect wired network hardware in an Ethernet LAN, MAN, or wide WAN.

USB Port

A USB port is a standard cable connection interface for personal computers and consumer electronics devices. USB stands for Universal Serial Bus, an industry standard for short-distance digital data communications. USB ports allow USB devices to be connected to each other with and transfer digital data over USB cables



Symbol		Max Speed	Power	Video
	USB 2.0	480 Mbit/S	No	
SS	USB 3.0 (USB 3.1 Gen 1)	5 Gbit/S	No	
SS 10	USB 3.1 (USB 3.1 Gen 2)	10 Gbit/S	No	
SS	USB 3.0 (USB 3.1 Gen 1)	5 Gbit/S	Yes	
SS 10	USB 3.1 (USB 3.1 Gen 2)	10 Gbit/S	Yes	
⚡	Thunderbolt 3	40 Gbit/S	Yes	Yes
D	DP Alt mode	This symbol will be found next to the above symbols to identify that this port supports video		Yes

HDMI (High-Definition Multimedia Interface)

It is proprietary audio/video interface for transmitting uncompressed video data and compressed or uncompressed digital audio data from an HDMI-compliant source device, such as a display controller, to a compatible computer monitor, video projector, digital television, or digital audio device.

SAS

In computing, Serial Attached SCSI (S A Small Computer System Interface) is a point to-point serial protocol that moves data to and from computer-storage devices such as hard disk drives and tape drives. ... SAS, like its predecessor, uses the standard SCSI command set.

SAN switch

A storage area network (SAN) switch is a device that connects servers and shared pools of storage devices and is dedicated to moving storage traffic. SAN switches are often Fibre Channel switches, although Ethernet-based SAN switches are also common. SAN switch is designed for a high-performance network with low latency and lossless data transmission. ... Ideally, SAN switch is dedicated to storage traffic only, whether based on Ethernet or Fibre Channel technologies, and the switch is optimized for that specific purpose. SAN, or storage area network, is a computer network which provides access to consolidated and block level data storage.

RS-232

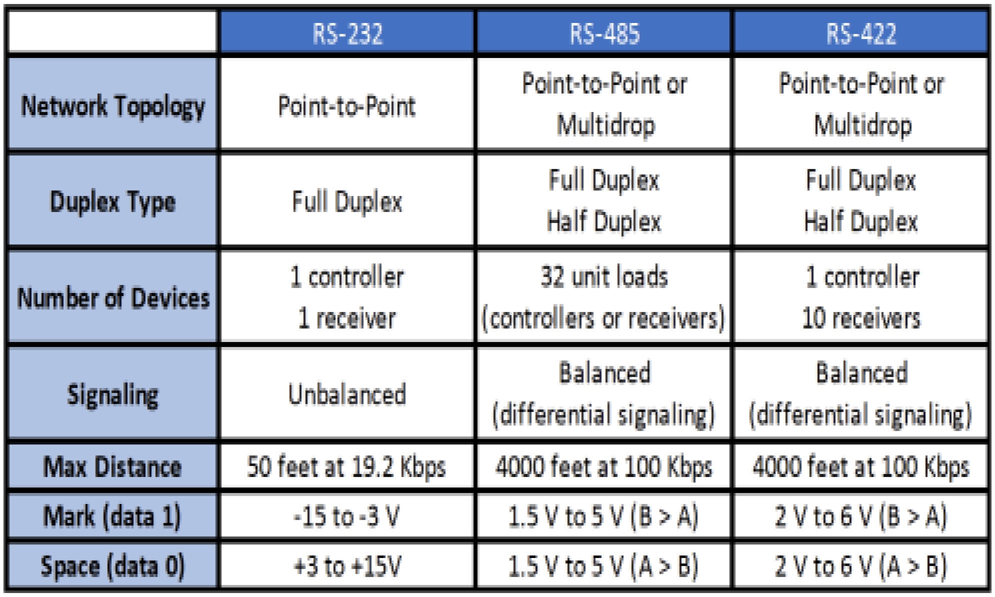
In telecommunications, RS-232, Recommended Standard 232 is a standard originally introduced in 1960 for serial communication transmission of data. It formally defines signals connecting between a DTE (data terminal equipment) such as a computer terminal, and a DCE (data circuit-terminating equipment or data communication equipment), such as a modem.

RS-422

It also known as TIA/EIA-422, is a technical standard originated by the Electronic Industries Alliance that specifies electrical characteristics of a digital signaling circuit. It was intended to replace the older RS-232C standard with a standard that offered much higher speed, better immunity from noise, and longer cable lengths. RS-422 systems can transmit data at rates as high as 10 Mbit/s, or may be sent on cables as long as 1,200 meters at lower rates. It is closely related to RS-423.

RS-485

It is also known as TIA-485(-A) or EIA-485, is a standard defining the electrical characteristics of drivers and receivers for use in serial communications systems. Electrical signaling is balanced, and multipoint systems are supported. The standard is jointly published by the Telecommunications Industry Association and Electronic Industries Alliance (TIA/EIA). Digital communications networks implementing the standard can be used effectively over long distances and in electrically noisy environments. Multiple receivers may be connected to such a network in a linear, multidrop bus. These characteristics make RS-485 useful in industrial control systems and similar applications, used the same signalling systems but on a different wiring arrangement.



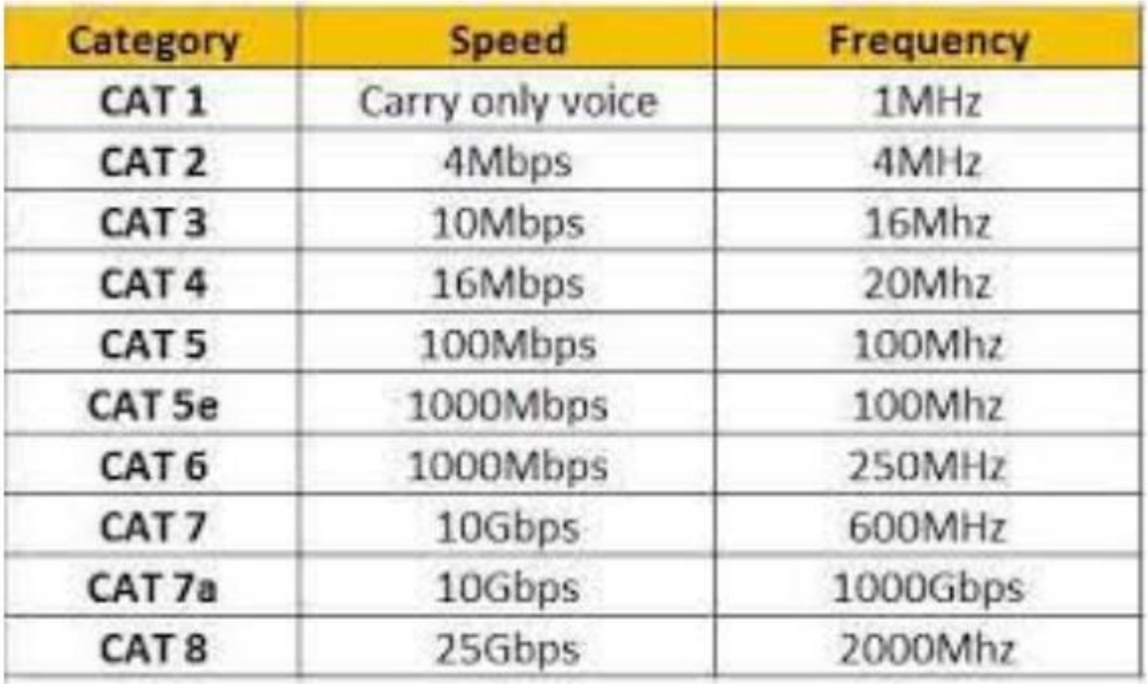
	RS-232	RS-485	RS-422
Network Topology	Point-to-Point	Point-to-Point or Multidrop	Point-to-Point or Multidrop
Duplex Type	Full Duplex	Full Duplex Half Duplex	Full Duplex Half Duplex
Number of Devices	1 controller 1 receiver	32 unit loads (controllers or receivers)	1 controller 10 receivers
Signaling	Unbalanced	Balanced (differential signaling)	Balanced (differential signaling)
Max Distance	50 feet at 19.2 Kbps	4000 feet at 100 Kbps	4000 feet at 100 Kbps
Mark (data 1)	-15 to -3 V	1.5 V to 5 V (B > A)	2 V to 6 V (B > A)
Space (data 0)	+3 to +15V	1.5 V to 5 V (A > B)	2 V to 6 V (A > B)

RJ 45

RJ abbreviated for the Registered Jack. RJ45 is a type of cable connector which is mainly used in computer networks. RJ45 is mainly used for ethernet networking which is used to connect different type of devices like a switch, hub, PC, router, firewall to each other.

CAT Cables

A variety of different cables are available for Ethernet and other telecommunications and networking applications. These network cables that are described by their different categories, e.g. Cat 5 cables, Cat-6 cables, etc., which are often recognized by the TIA (telecommunications Industries Association) and they are summarized below:



Category	Speed	Frequency
CAT 1	Carry only voice	1MHz
CAT 2	4Mbps	4MHz
CAT 3	10Mbps	16Mhz
CAT 4	16Mbps	20Mhz
CAT 5	100Mbps	100Mhz
CAT 5e	1000Mbps	100Mhz
CAT 6	1000Mbps	250MHz
CAT 7	10Gbps	600MHz
CAT 7a	10Gbps	1000Gbps
CAT 8	25Gbps	2000Mhz

ISSD (Information System and Services Division)

- **Telecommunication Division renamed as Information System and Services Division (ISSD) of India Meteorological Department in 2009.**
- **It provides the support function needed for meteorological data and processed weather products to the users, both national and international (including aviation data/ products) round the clock on near real time basis.**
- **It started with administration of IT systems (as delivered by Varsamana Project (mainly CIPS & TRANSMET) and then spread its activities towards management of operational data, workflow, and management /supervision of system integration.**

Main Mission

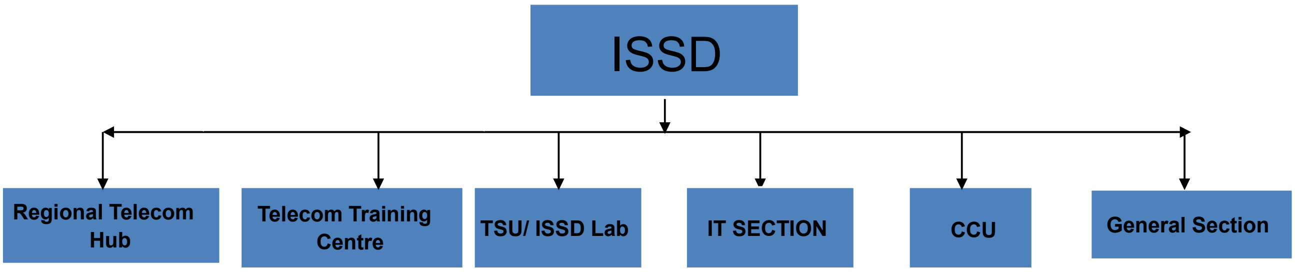
- Management of Information Systems and Telecommunications Support and advice :
- On the use of IT in HPC, data/metadata management and exchange □□In preparation, follow-up of financial management of items related to IT.
- Techno-financial advice in the case of procurement and commissioning of IT oriented systems
- Coordination of procurement of hardware (in relation with CPU) whenever shared by several entities within IMD
- Draft IT master plan and subsequent updates, for approval at higher level.
- Management of IT systems operations whenever shared by several entities within IMD: network, AMSS, HP computing system, data centres and archiving & back-up systems, centralized servers, distributed systems.
- Management and provision of Level 1 support on core systems
- Implementation of Security Policy under authority of DGM
- Implementation of Data Policy under authority of DGM
- Contribution to spreading and training of scientific and technical IT, as well as telecommunications.
- Other missions
- Representation of IMD in international bodies on IT related topics (e.g. WMOCBS meetings)
- Management of IMD WIS role (i.e. GISC
- “South Asia” and DCPC “sat & met data”)
- Management of telecommunication frequency assignment
- Coordination of software developments
- whenever shared between several entities

Milestones

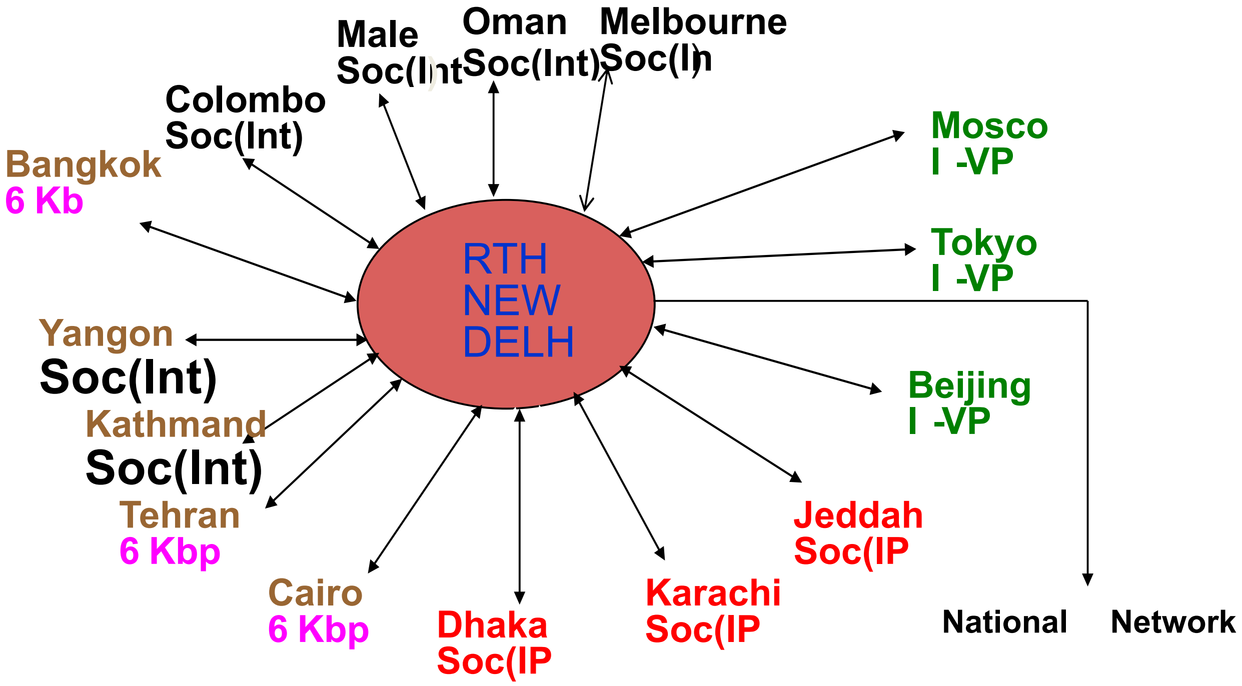
- The Directorate of Telecommunication was set up in IMD at New Delhi in 1969 to cater the need of National Meteorological Service and strengthen the meteorological telecommunication in India.

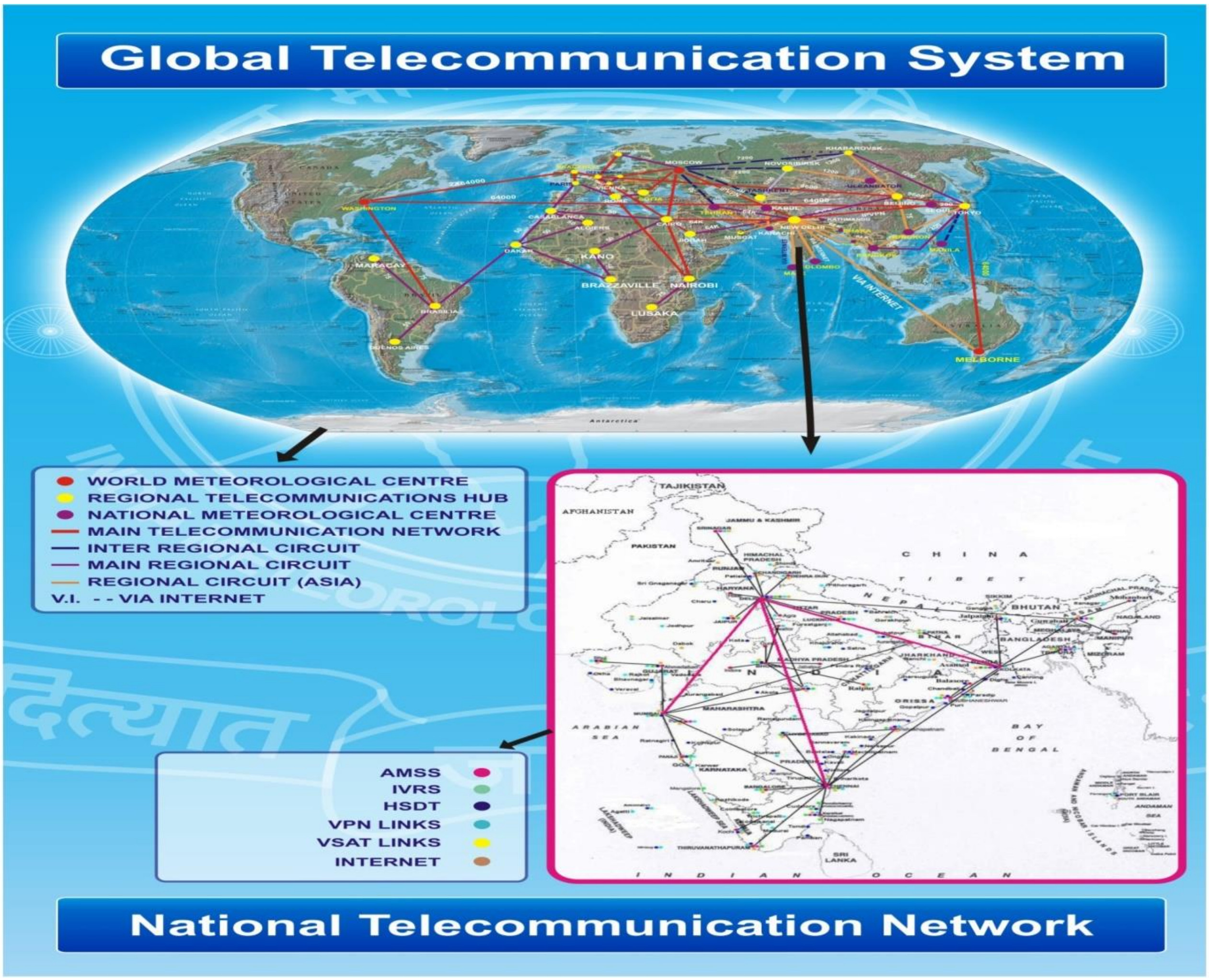
- The data exchange centre was automated in mid-seventies by PHILIPSDS714 computer and became a designated RTH in RA-II connected on GTS. The volume of data exchange was about 2 MB per day and circuit handling up to 2400 bps.
- The system was replaced by VAX 11/750 in 1988 where data handling capability increased manifold and circuit handling (Max.8 nos.) up to 9600bps.

- Above system was replaced with SUN E-250 server based AMSS with 128 circuits handling capability each ranging from 50 baud to 128 kbps and data volume increased to 2.2 Gb per day.
- Now the new RTH system (TRANSMET) with latest state-of the art technology supplied by MFI has been installed and is operational from October 2009. There is no limitation for number of circuit/ circuit speed handling capability. User friendly browser based operation with remote data submission as well as retrieval with data handling capability of the order of Tb.



Links with RTH New Delhi





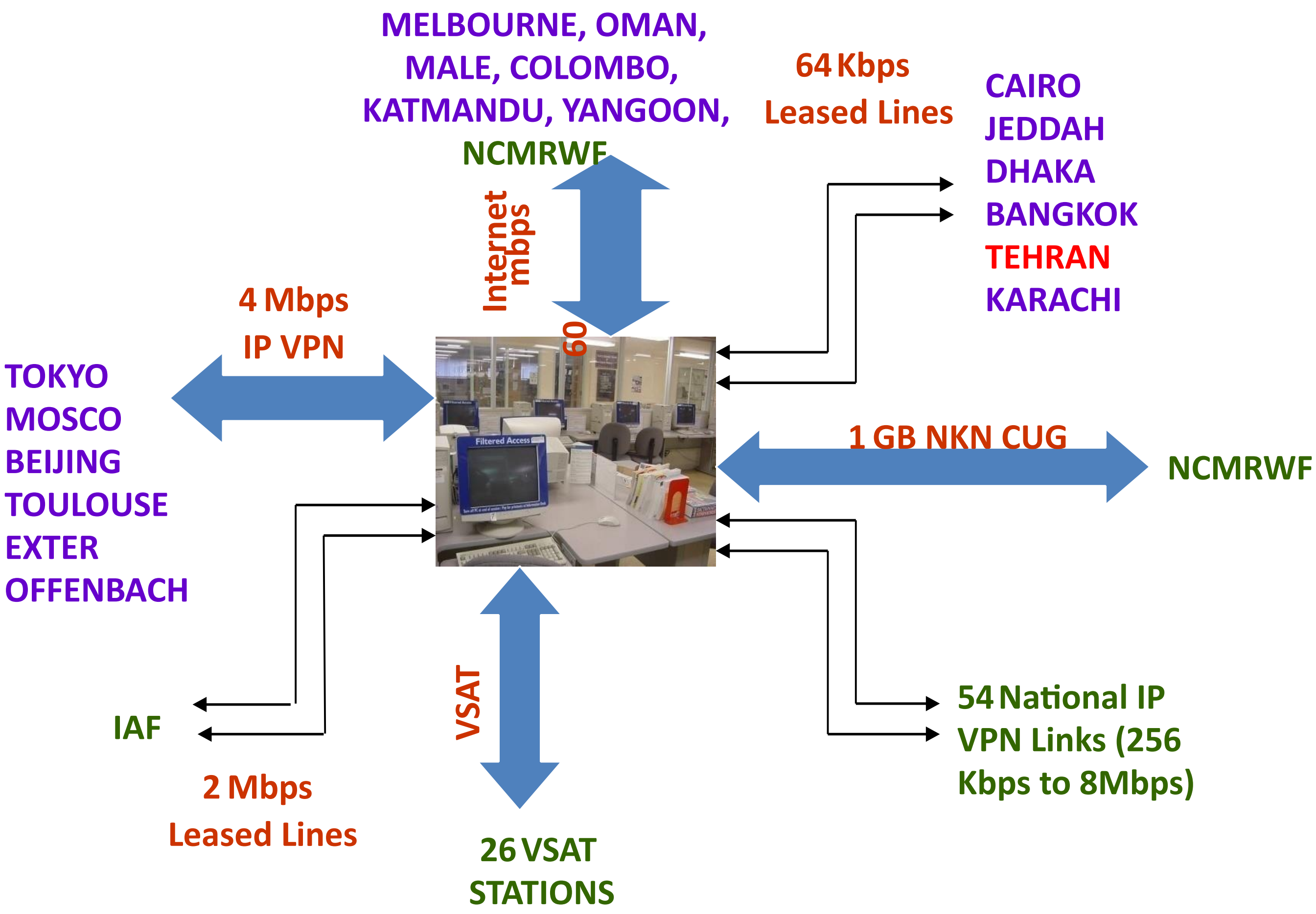
Global Telecommunication System

- ● WORLD METEOROLOGICAL CENTRE
- ● REGIONAL TELECOMMUNICATIONS HUB
- ● NATIONAL METEOROLOGICAL CENTRE
- — MAIN TELECOMMUNICATION NETWORK
- — INTER REGIONAL CIRCUIT
- — MAIN REGIONAL CIRCUIT
- — REGIONAL CIRCUIT (ASIA)
- V.I. - - VIA INTERNET

AMSS	●
IVRS	●
HSDT	●
VPN LINKS	●
VSAT LINKS	●
INTERNET	●

National Telecommunication Network

National and International connectivity at RTH New Delhi



MELBOURNE, OMAN, MALE, COLOMBO, KATMANDU, YANGOON, NCMRWF

Internet 60 mbps

64 Kbps Leased Lines

CAIRO
JEDDAH
DHAKA
BANGKOK
TEHRAN
KARACHI

4 Mbps IP VPN

TOKYO
MOSCO
BEIJING
TOULOUSE
EXTER
OFFENBACH

1 GB NKN CUG

NCMRWF

IAF

2 Mbps Leased Lines

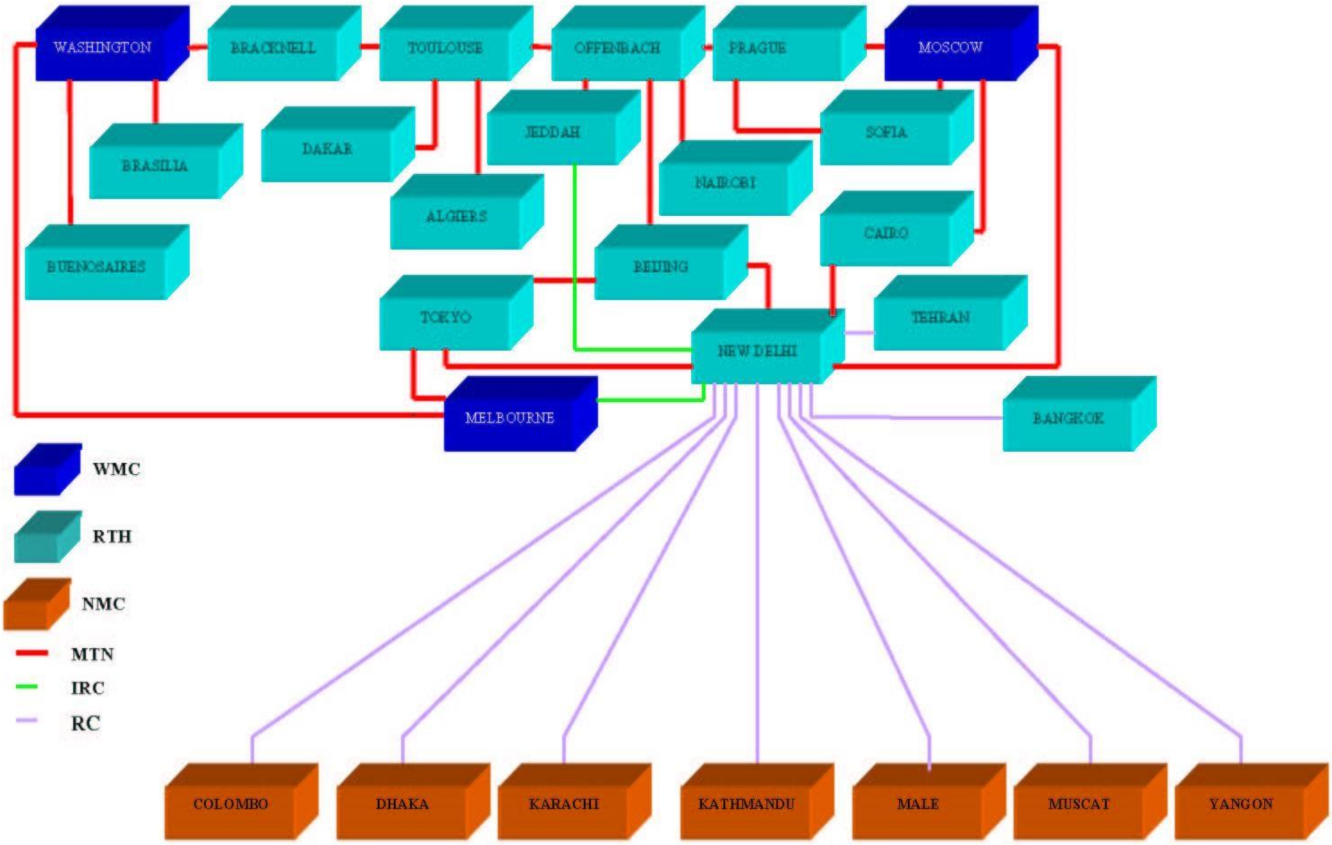
VSAT

26 VSAT STATIONS

54 National IP VPN Links (256 Kbps to 8Mbps)

- ❖ It is one of the 18 major RTHs and three World Meteorological Centers (WMCs) on the Main Telecommunication Network (MTN) of the GTS.
- ❖ Due to strategic location of RTH New Delhi on MTN, it acts as an interface between the eastern and western hemispheres
- ❖ First automated in 1974 with 3rd Generation Computer
- ❖ Replaced in 1988 by VAX11/750, by SUN E250 based server in 2000.
- ❖ Now it is state-of-the-art technology system complying to guidelines/ standards from WMO for data exchange on GTS. The system is operational from Nov 2009.

CONFIGURATION OF THE MAIN TELECOMMUNICATION NETWORK AND REGIONAL/INTER-REGIONAL METEOROLOGICAL TELECOMMUNICATION NETWORKS CONNECTED WITH RTH NEW DELHI



2. Central Information Processing System (CIPS): High end database management system having task centre to develop, test and operationalise meteorological tasks for real time generation of meteorological products.

3. Public Weather System (PWS): To deliver High quality weather products and alerts to end users like print media and Television.

4. Clisys: Climatological data storage system with scalable management tool for effective utilization of these data.

5. Synergie: Decision support system for forecasters to gather, visualize, interact and value add meteorological forecasts and products.

6. Upper Air System – GPS: Ten GPS stations installed have significant impact in the upper air data quality. These data are now accepted by ECMWF in their models.

❖ **During modernization programme of India Meteorological Department, following systems have been installed and are in continuous operation.**

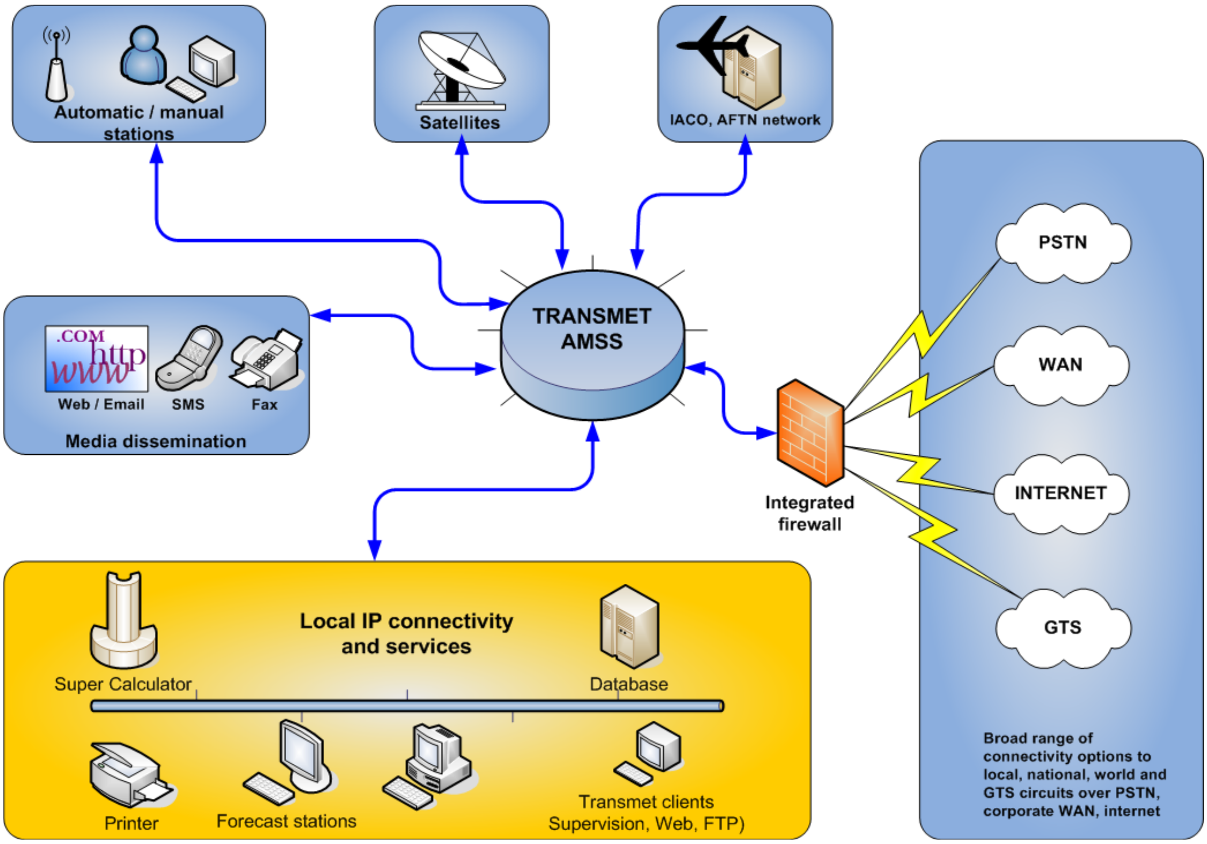
Automatic Message Switching System (AMSS)- Transmet

- A central element in a high technology Meteorological environment.
- TRANSMET AMSS is the heart of meteorological telecommunication.

The main functions:

To receive, check and forward automatically, the meteorological data and products according to the WMO standards. TRANSMET interconnects our Meteorological sub-systems; share in real time our data and product internally and from/to the meteorological world.

The system is in operation from November 2009.


Automatic / manual stations
Satellites
IACO, AFTN network
TRANSMET AMSS
.COM http www
Web / Email
SMS
Fax
Media dissemination
Integrated firewall
PSTN
WAN
INTERNET
GTS
Broad range of connectivity options to local, national, world and GTS circuits over PSTN, corporate WAN, internet
Local IP connectivity and services
Super Calculator
Database
Printer
Forecast stations
Transmet clients Supervision, Web, FTP)

b Fig System Overview

Hardware Configuration

- **Separate AMSS for National and International operations**
- **Each AMSS consists of two servers in hot standby mode**
- **Each Server consists of:**
  - **CPU – Quad core four processor Intel Xeon, 2.4 GHz**
  - **RAM – 8 GB**
  - **HDD – 146.8 GB SAS X 6**
- **Two database server separately for National and International server.**
- **Two E-mail servers in hot standby mode**
- **Two Web servers in hot standby mode**
- **Twelve Operator Terminals for operators as well as administrators.**
- **Cisco firewall for intrusion protection**
- **Latest SADIS 2G receiver to receive SADIS data**
- **Cisco Routers and HP Switches**

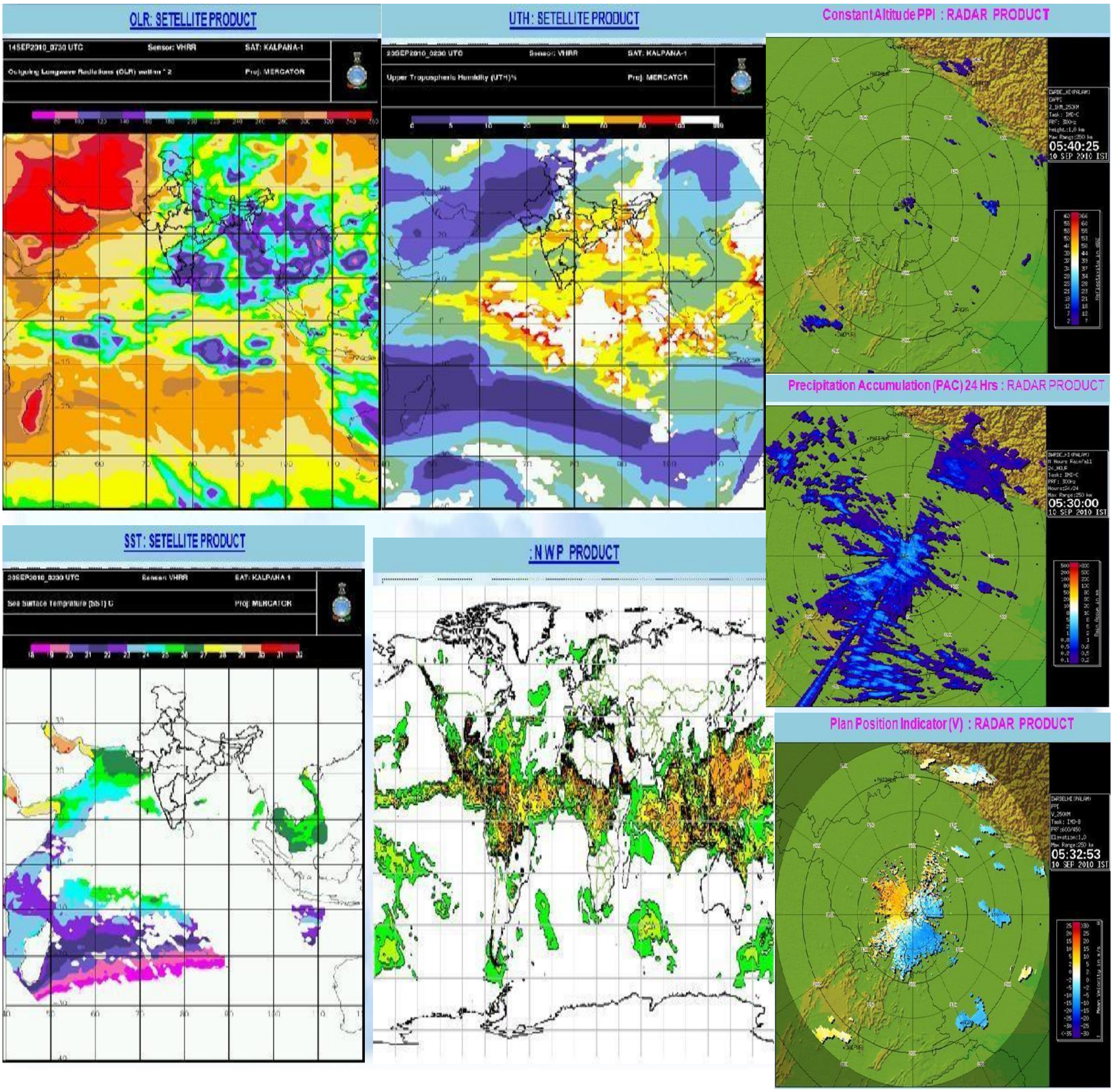
- **GPS Time Server for time synchronization**

Features

- **Web tool for easy deployment and setup:** The system includes a web-based configuration tool for simplified circuit configuration, routing table modification, circuit supervision, database message search and access, redactions of bulletin (SYNOP, TEMP, TAF, METAR …) and system setup etc.
- **Reliability and manageability**: Transmet supports centralized administration and management via Secure Shell (SSH), web interface and local management through the supervision clients. Provision of many debug features allow system administrator to remotely diagnose network problems, operators to diagnose meteorological message syntax, time, format problems and automatic switchover of cluster in case of failover.
- **Fully compliant with all network protocols**: The message switch is fully compliant with all the applicable protocols, procedures, regulations and standards including WMO 386. The system design has taken into consideration the need to accommodate future WMO standards. System can interface to any standard communications device. The system is able to handle all kinds of data required by a National Meteorological Service in WMO format and ICAO standards, switch BUFR and CREX data.
- **Operators, Administrators and Developers WMO tools:** The system provides a set of tools enabling powerful messages database, WMO monitoring, automatic message compilation, messages editing and correction tools, Transmet Software Development Kit, decode encode functionalities and system administration.
- **Single virtual IP address**: One virtual IP address for both LIVE and Standby systems give uninterrupted communication with other centres without any human intervention in case of switchover of the system.
- **Broadcast of GMDSS**: Broadcast of GMDSS bulletins has been integrated with the system. This facility enables broadcast of sea area bulletins over safety net automatically at predefined time for Met Area VIII (N).
- **BUFR**: The system supports data exchange in BUFR format. It can convert automatically the received SYNOP and upper air messages from ASCII to BUFR format and switch to GTS.
- Message submission through web browser URL:http://125.21.185.16: Remote/ part time observatories can submit messages to Transmet directly using web browser.
- **SMS interface**: The system is equipped with dissemination of customized message through SMS to predefined recipients whenever the message with a particular header is received. This facility is quite useful for warning dissemination. Small observational messages can also be submitted to the system through SMS.
- **Dial-up interface: Any authorized remote machine with modem can have access to Transmet data (ASCII and binary), put data and access to the Transmet web to write message using the format functionality.**

- ❖ **SADIS data reception: Latest SADIS 2G receiver has been integrated with the system to receive SADIS data directly, which is fed to the GTS for national and international use. Secure SADIS FTP is also integrated as a backup link to receive SADIS data for use in aviation.**

WIS – A New Concept…



The WMO Information system (WIS) is a coordinated global infrastructure responsible for telecommunications and data management functions and is owned and operated by WMO Members. WIS provides an integrated approach suitable for all WMO Programmes to meet the requirements for routine collection and automated dissemination of observed data and products, as well as data discovery, access, and retrieval services for weather, climate, water, and related data produced by centres and Member countries in the framework of any WMO Programme. It is capable of exchanging large data volumes, such as new ground and satellite-based systems, finer resolutions in numerical weather prediction, and hydrological models and their applications. These data and products must be available to National Hydrological and Meteorological Services (NHMS), but also national disaster authorities for more timely alerts where and when needed. WIS is a vital data communications backbone for integrating the diverse real-time and non-real-time high priority data sets, regardless of location.

WIS is composed of three types of centres and a communications network

- National Centres (NCs)
- Data Collection or Production Centres (DCPCs)
- Global Information System Centres (GISCs)

❖ Detailed specifications/ guidelines regarding WIS functions have been issued by WMO. Data management lies at the heart of the WIS.

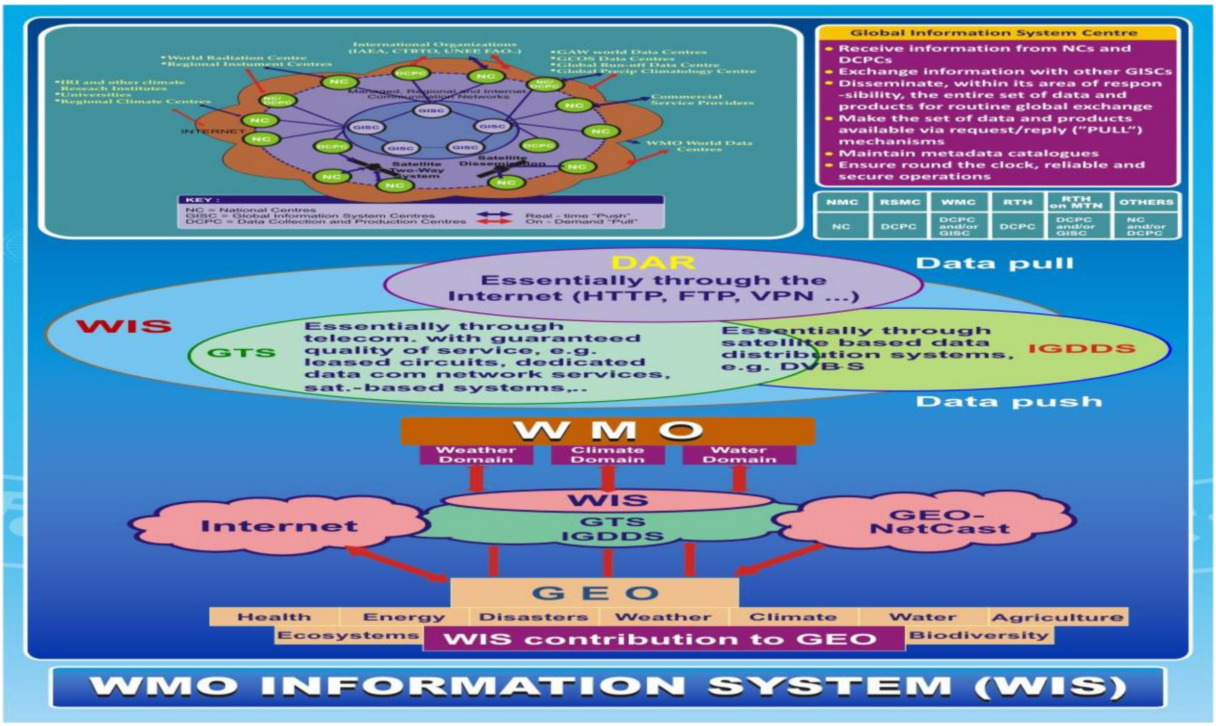
❖ WIS is designed to be a coordinated, distributed, global infrastructure for the collection and sharing of data and information for all WMO and related international programs.

❖ WIS consists of three components viz. GISC, DCPC and NC.

❖ Data Access and Retrieval (DAR) catalogues of WIS are hosted by GISCs .

❖ GISCs can be viewed as forming a central hub of WIS as shown in Fig.

WIS -1



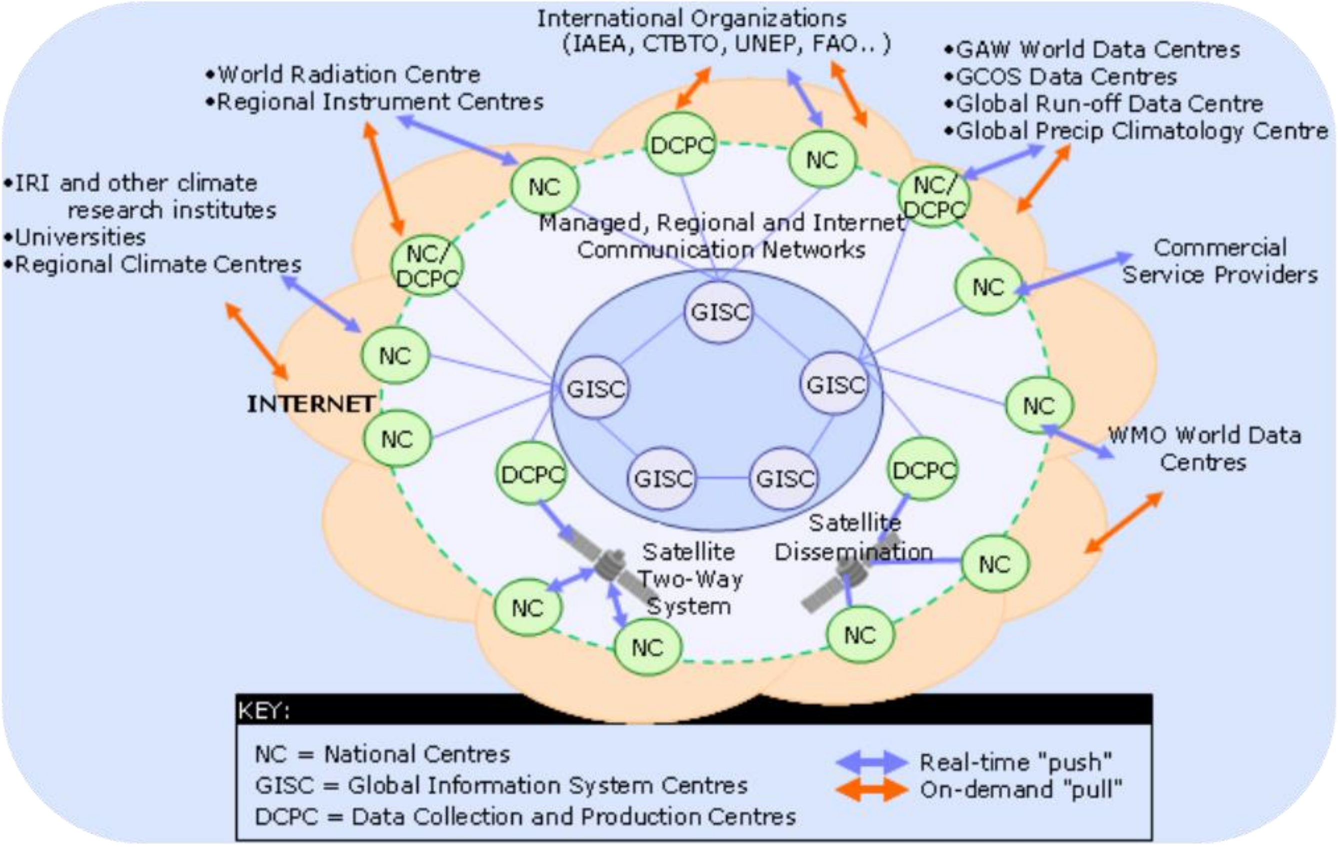
Global Information System Centre

- Receive information from NCs and DCPCs
- Exchange information with other GISCs
- Disseminate, within its area of respon -sibility, the entire set of data and products for routine global exchange
- Make the set of data and products available via request/reply ("PULL") mechanisms
- Maintain metadata catalogues
- Ensure round the clock, reliable and secure operations

NMC	RSMC	WMC	RTH	RTH on MTN	OTHERS
NC	DCPC	DCPC and/or GISC	DCPC	DCPC and/or GISC	NC and/or DCPC

KEY :
NC = National Centres
GISC = Global Information System Centres
DCPC = Data Collection and Production Centres
Real - time "Push"
On - Demand "Pull"

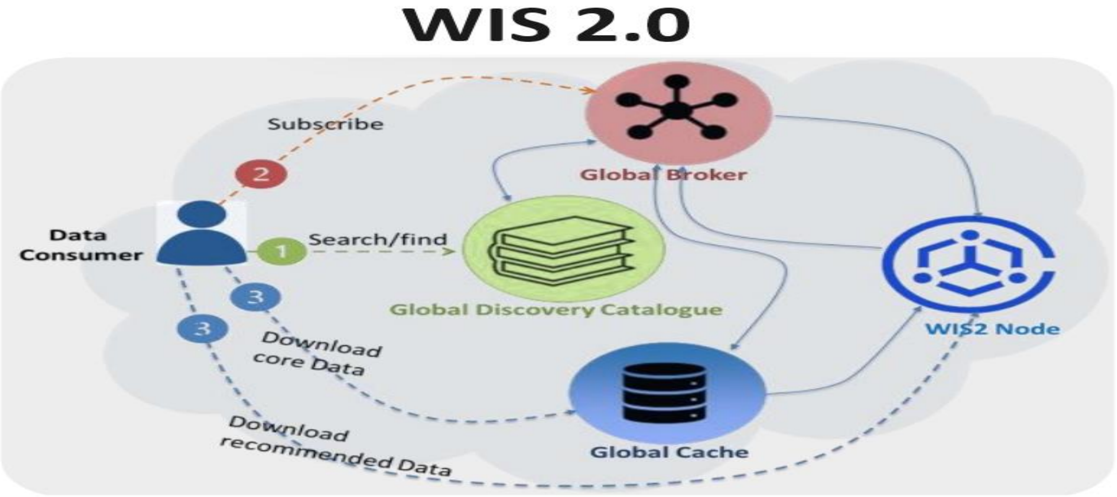
International Organizations (IAEA, CTBTO, UNEP, FAO..)
•World Radiation Centre
•Regional Instument Centres
•IRI and other climate Reseach Institutes
•Universities
•Regional Climate Centres
•GAW world Data Centres
•GCOS Data Centres
•Global Run-off Data Centre
•Global Precip Climatology Centre
Commercial Service Providers
WMO World Data Centres
INTERNET
Managed, Regional and Internet Communication Networks
NC
NC/DCPC
DCPC
GISC
Satellite Two-Way System
Satellite Dissemination
DAR
Essentially through the Internet (HTTP, FTP, VPN ...)
Data pull
WIS
GTS
Essentially through telecom. with guaranteed quality of service, e.g. leased circuits, dedicated data com network services, sat.-based systems,..
Essentially through satellite based data distribution systems, e.g. DVB-S
IGDDS
Data push
W M O
Weather Domain
Climate Domain
Water Domain
Internet
WIS
GTS
IGDDS
GEO-NetCast
G E O
Health
Energy
Disasters
Weather
Climate
Water
Agriculture
Ecosystems
WIS contribution to GEO
Biodiversity
WMO INFORMATION SYSTEM (WIS)

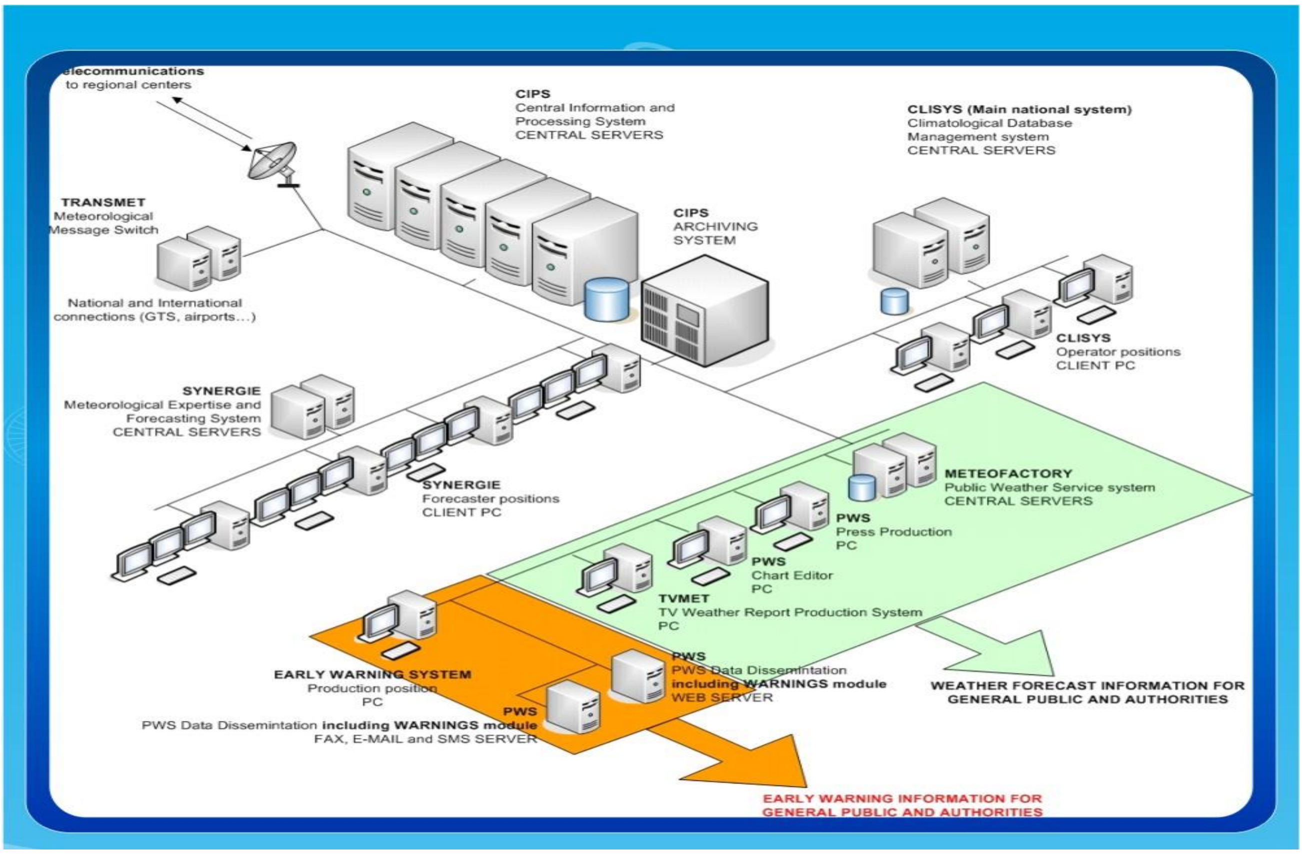

International Organizations (IAEA, CTBTO, UNEP, FAO..)
•World Radiation Centre
•Regional Instrument Centres
•GAW World Data Centres
•GCOS Data Centres
•Global Run-off Data Centre
•Global Precip Climatology Centre
•IRI and other climate research institutes
•Universities
•Regional Climate Centres
Commercial Service Providers
WMO World Data Centres
INTERNET
Managed, Regional and Internet Communication Networks
NC
DCPC
NC/DCPC
GISC
Satellite Two-Way System
Satellite Dissemination
KEY:
NC = National Centres
GISC = Global Information System Centres
DCPC = Data Collection and Production Centres
Real-time "push"
On-demand "pull"

WIS 2.

- WMO Information System 2.0 has been designed to meet the shortfalls of the current WIS and GTS, support the WMO's Unified Data Policy and the Global Basic Observing Network (GBON), and meet the demand for high data volume, variety, velocity, and veracity.
- WIS 2.0 uses the public internet (rather than private dedicated links as for GTS) and uses a "publish-subscribe" pattern where users subscribe to a topic to receive new data in real-time using the MQTT protocol.

  Each Data Provider is required to host a WIS 2.0 node that sends WIS 2.0 data notifications and WIS 2.0 metadata notifications and enables the download of data over HTTP.




elecommunications to regional centers
CIPS Central Information and Processing System CENTRAL SERVERS
CLISYS (Main national system) Climatological Database Management system CENTRAL SERVERS
TRANSMET Meteorological Message Switch
CIPS ARCHIVING SYSTEM
National and International connections (GTS, airports…)
CLISYS Operator positions CLIENT PC
SYNERGIE Meteorological Expertise and Forecasting System CENTRAL SERVERS
METEOFACTORY Public Weather Service system CENTRAL SERVERS
SYNERGIE Forecaster positions CLIENT PC
PWS Press Production PC
PWS Chart Editor PC
TVMET TV Weather Report Production System PC
EARLY WARNING SYSTEM Production position PC
PWS PWS Data Dissemintation including WARNINGS module WEB SERVER
WEATHER FORECAST INFORMATION FOR GENERAL PUBLIC AND AUTHORITIES
PWS PWS Data Dissemintation including WARNINGS module FAX, E-MAIL and SMS SERVER
EARLY WARNING INFORMATION FOR GENERAL PUBLIC AND AUTHORITIES

Integrated work flow

SIGMET TRANSMISSION

As advice by ICAO, MWO is now issuing a test advisory and SIGMET for TC, in addition to valid advisories SIGMET

RSMC NEW DELHI ISSUNIG A TCAC BULLETIN IN PNG AND TEXT FORMAT OF HEADER FKIN21 DEMS (GTS TEXT), PZXE89 DEMS (GTS PNG) AND FKIN21 VIDP (TEXT) AFTN TRNSMISSION.

- **ALL MWO ISSUING SIGMET OF HEADER WCIN31 CCCC.**

SADIS DATA

The Satellite Distribution System (SADIS) is a worldwide satellite-based broadcast system dedicated to primarily distributing aeronautical meteorological information in line with ICAO standards.

- **OPMET, AIRMETs, GAMETs – Text format**
- **SIGWX Charts – PNG format**
- **BUFR encoded high level SIGWX information – BUFR;**
- **Wind, temperature and humidity information-GRIB1&GRIB2**
- **Volcanic ash trajectory/dispersion charts – T.4 facsimile and PNG format**

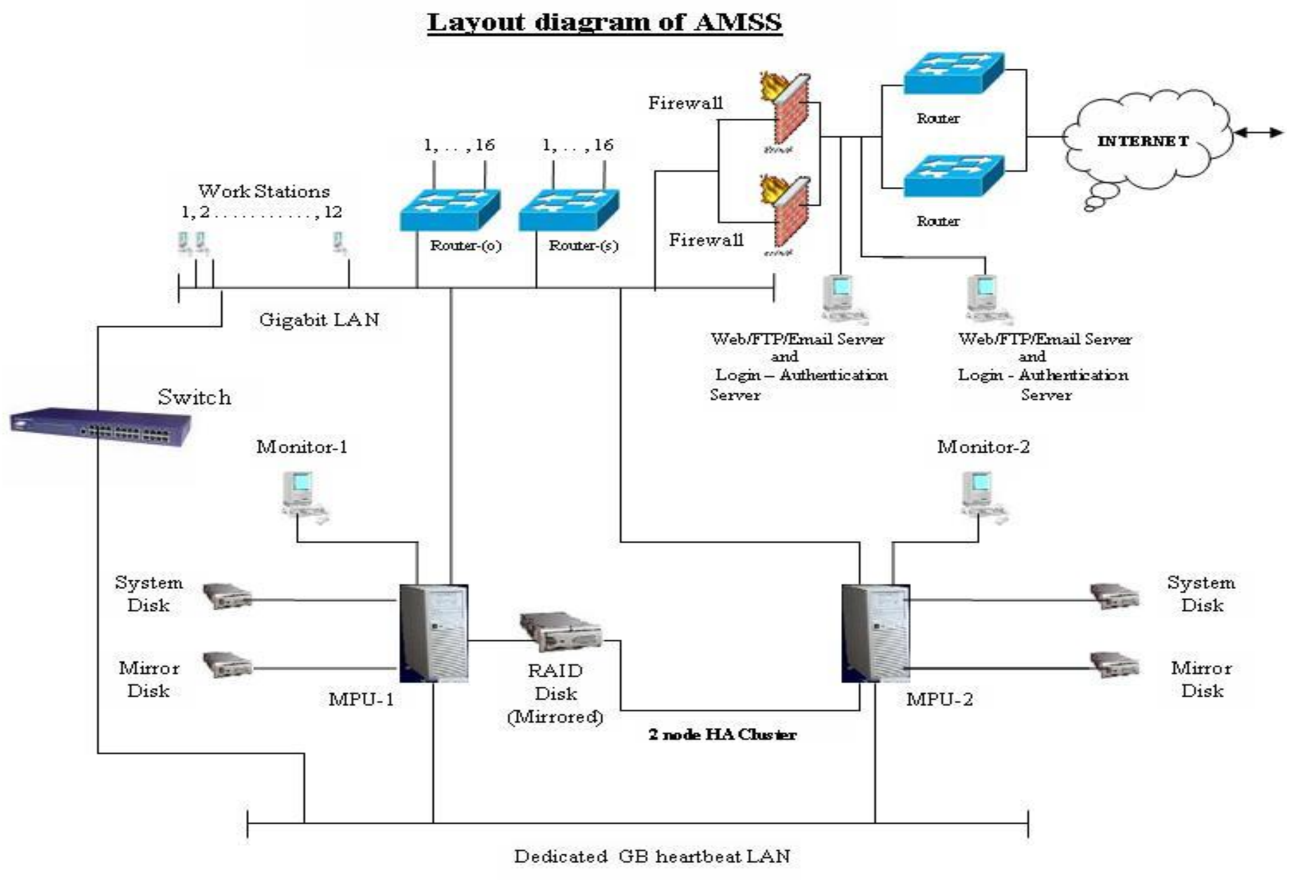
. Volcanic ash and tropical cyclone advisory statements - Text format

SADIS FTP

- This Product is also provided by the Met Office as a high-quality internet source of WAFS and OPMET data to all approved SADIS recipients as a backup to SADIS 2G.
- The Secure SADIS FTP service became operational on 18 November 2010. The Secure SADIS FTP Service builds upon and improves upon the existing SADIS FTP Service by using Digital Certification/Digital Signing techniques to allow downloaded data to be verified in order to guarantee that the data has not been corrupted, changed or otherwise tampered with.
- It also allows for verifying conclusively that the downloaded files originated from the UK Met Office (as SADIS Provider)

AMSS Centre

(Existing 4 at Kolkata, Mumbai, Delhi and Chennai and 2 new at Guwahati and Nagpur, Mirror RTH at Pune)



Features

- High Availability (more than 99.9%)
- Cluster Mode, Duplex Web, E-mail and FTP
- Conversion from CREX, BUFR, GRIB to ASCII and vice versa
- WMO as well as AFTN switch
- Audio visual Alarm for warning messages, Message reception through PSTN/Dial-up and SMS
- Transmission of warnings through SMS to predefined numbers.

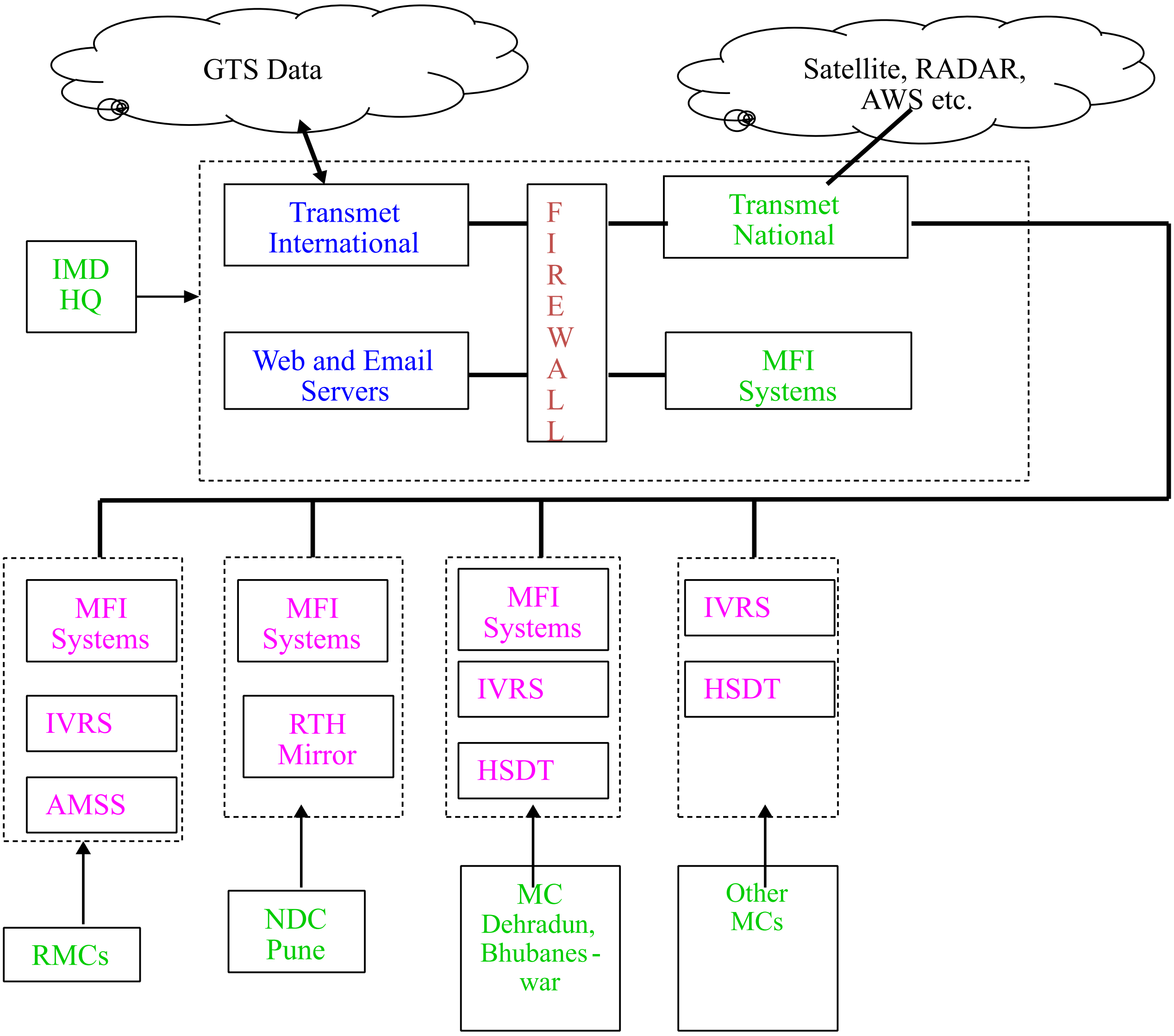
- File switching, OCR base FAX transmission and reception
- Authentication server for Internet users
- Bilingual features (English and Hindi) Daily throughput of data -- 50 GB.
- GUI base interface and web interface

❖ **A central element in a high technology Meteorological environment.**

❖ **TRANSMET AMSS is the heart of meteorological telecommunication**

The main functions:

- **To receive, check and forward automatically, the meteorological data and products according to the WMO standards.**



- **TRANSMET interconnects our Meteorological sub-systems; share in real time our data and product internally and from/to the meteorological world.**

Hardware configuration

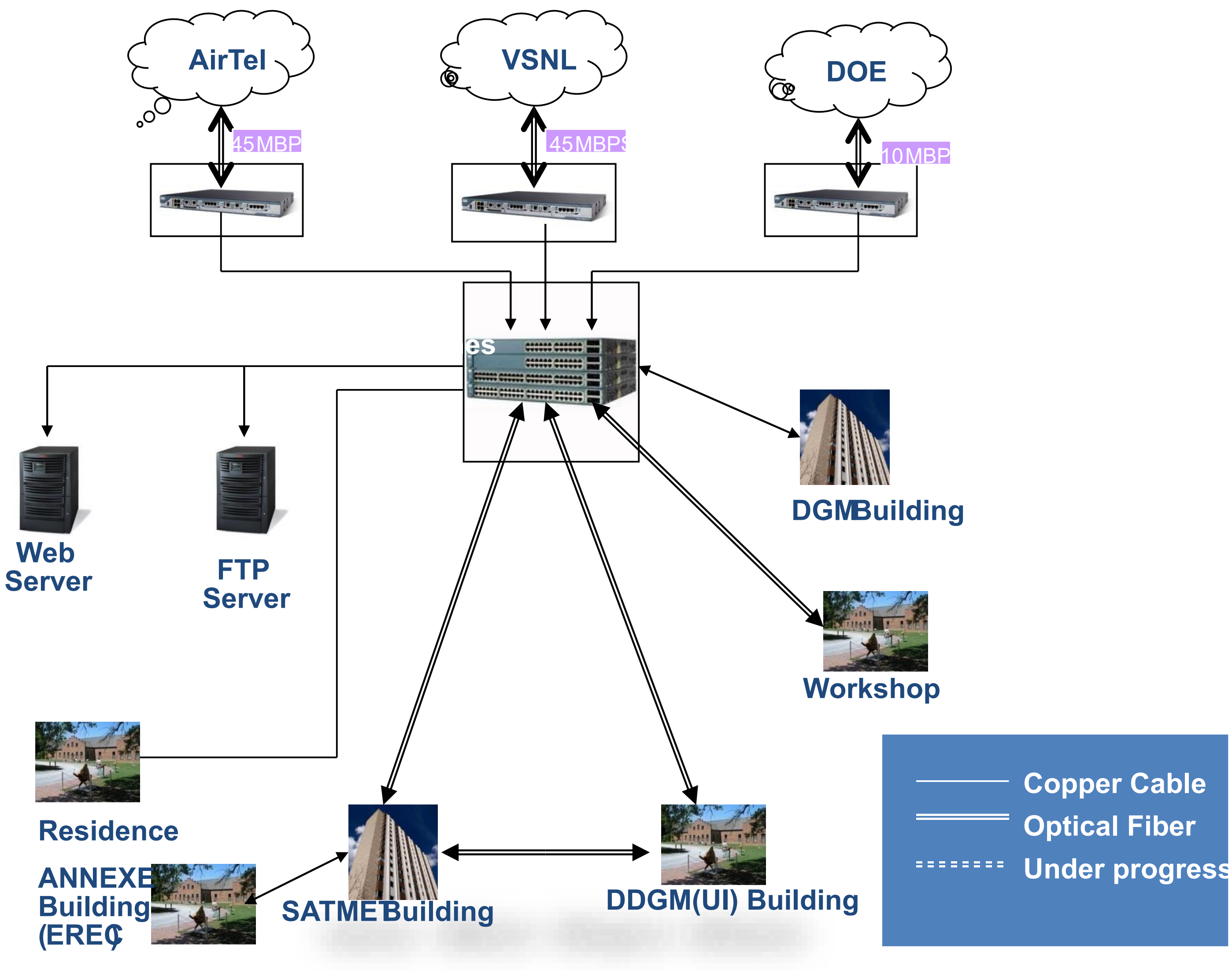
- Separate AMSS for National and International operations
- Each AMSS consists of two servers in hot standby mode
- Each Server consists of:
- CPU – Quad core four processor Intel Xeon, 2.4 GHz
- RAM – 8 GB
- HDD – 146.8 GB SAS X 6

- Two database server separately for National and International server.
- Two E-mail servers in hot standby mode
- Two Web servers in hot standby mode
- Twelve Operator Terminals for operators as well as administrators.
- Cisco firewall for intrusion protection
- Cisco Routers and HP Switches
- GPS Time Server for time synchronization

Features

- Easy browser based Graphical Interface for circuit configuration
- One virtual IP for both LIVE and STANDBY machines.
- Graphical browser-based circuit monitoring tool.
- Audio-visual warning system for circuit failure and special message reception.
- E-mail: Send the whole message to predefined users through e-mail when a message with particular header is received.
- Ability to retrieve message from E-mail and submit that message to GTS
- SMS: Customized message through SMS to predefined recipients whenever a particular header is received. 1. Can be used for warning dissemination 2. Message can be submitted through SMS
- FAX : Warning messages can be diverted to predefined FAX numbers.
- File Switching : Can send satellite, RADAR, model etc. data file to predefined users as soon as those are received through FTP.
- Media file i.e. audio-visual files can also be sent to RMC, MC etc through FTP.
- BUFR : The system can automatically convert the received SYNOP and Upper Air messages to BUFR and send those BUFR messages to GTS.
- GPS Time Server for time synchronization
- Transmet adjust time as per the GPS Time Server.
- Secure Network
- Transmet is protected by Cisco Hardware Firewall.
- AFTN Link
- The system can send GTS data to AFTN Network through its AFTN link and vice-versa

LAN of IMD HQ



Computer Nodes details

Building	Nodes
DGM Building	300
SATMET Building	250
ANNEXE	50
DDGM Building	150
Workshop	50
Residence	50

VIRTUAL PRIVATE NETWORK (VPN)

A technology that creates a network that is physically public, but virtually private. VPNs typically require remote users of the network to be authenticated, and often secure data with encryption technologies to prevent disclosure of private information to unauthorized parties.

Need of VPN?

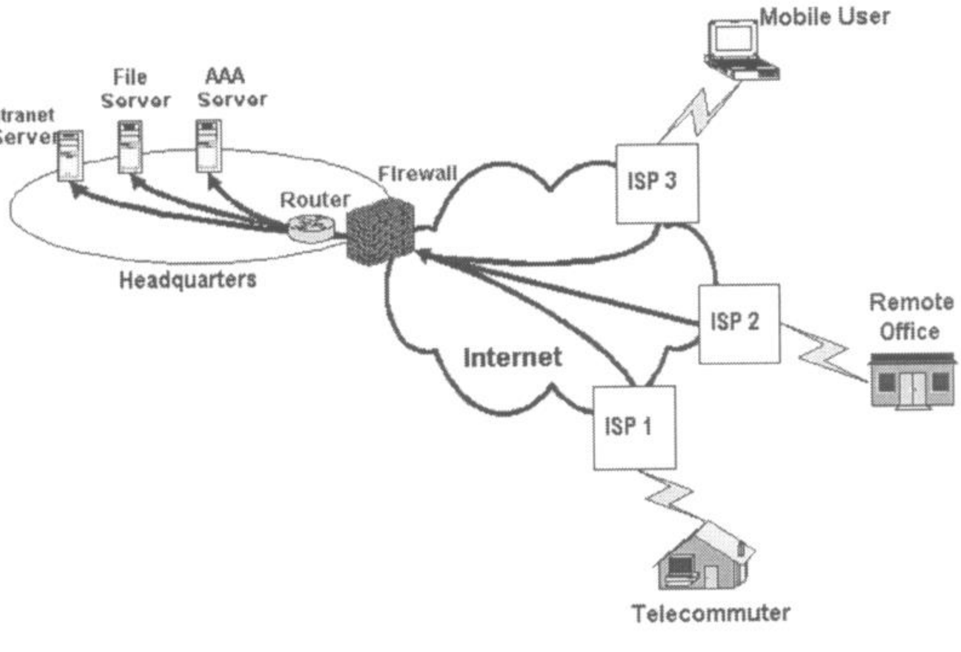
Earlier there was

1. Private Network.

- Completely isolated network is established.
- It creates its own TCP\IP internet.
- Leased lines.
- Isolated from world.
- Costlier

Private Networks vs. Virtual Private Networks

- Employees can access the network (Intranet) from remote locations.
- Secured networks.
- The Internet is used as the backbone for VPNs
- Saves cost tremendously from reduction of equipment and maintenance costs.
- Scalability



Remote access Virtual Private Network

Overview of Working of VPN

- ✓ Two connections – one is made to the Internet and the second is made to the VPN.
- ✓ Datagrams – contains data, destination and source information.
- ✓ Firewalls – VPNs allow authorized users to pass through the firewalls.
- ✓ Protocols – protocols create the VPN tunnels.

Four critical functions

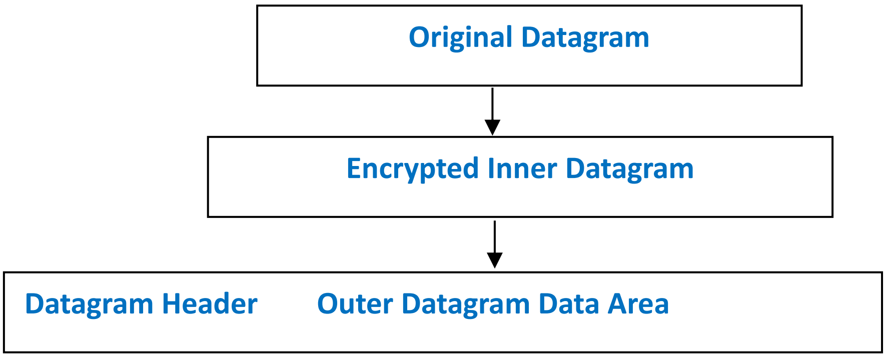
- ✓ Authentication – validates that the data was sent from the sender.
- ✓ Access control – limiting unauthorized users from accessing the network.
- ✓ Confidentiality – preventing the data to be read or copied as the data is being transported.
- ✓ Data Integrity – ensuring that the data has not been altered

ENCRIPTION

- ✓ Encryption -- is a method of “scrambling” data before transmitting it onto the Internet.
- ✓ Public Key Encryption Technique
- ✓ Digital signature – for authentication

TUNNELING

- ✓ A virtual point-to-point connection made through a public network. It transports
- ✓ encapsulated datagrams
- ✓ **A virtual point-to-point connection made through a public network. It transports encapsulated datagrams.**



Data Encapsulation [From Comer]

Two types of end points:

- **Remote Access**
- **Site-to-Site**

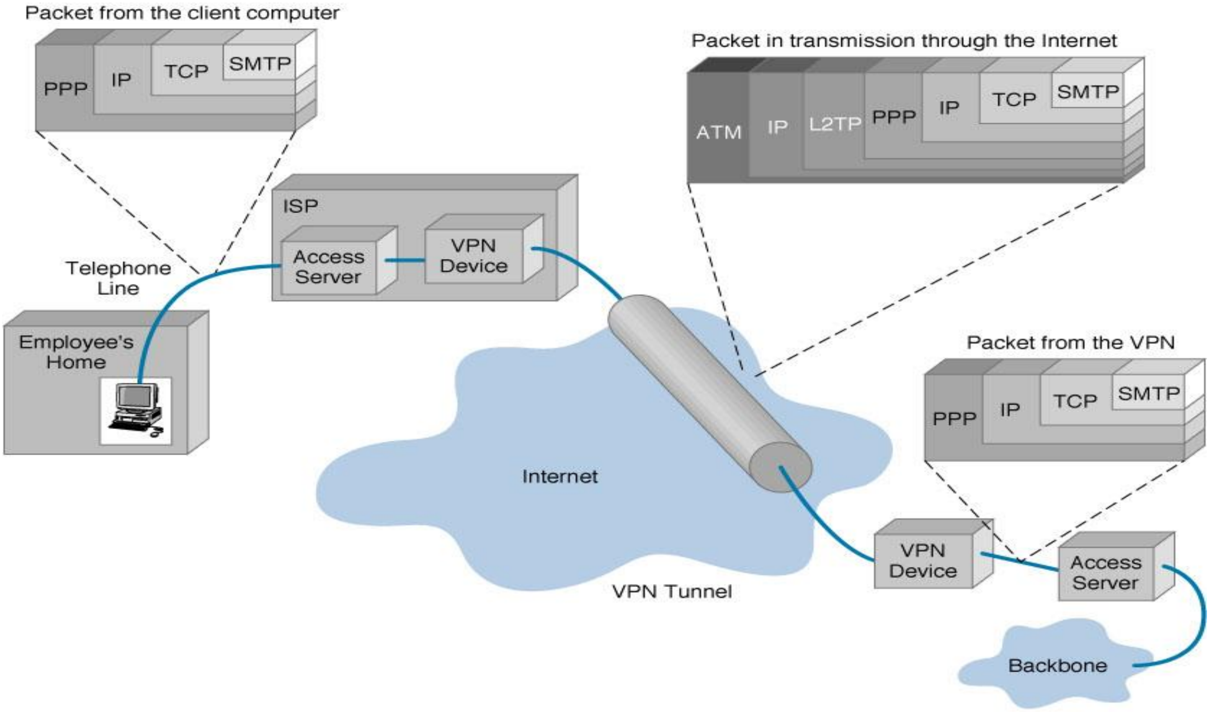
Protocols used in VPN

PPTP -- Point-to-Point Tunneling Protocol

L2TP -- Layer 2 Tunneling Protocol

IPsec -- Internet Protocol Security

VPN Encapsulation of Packets

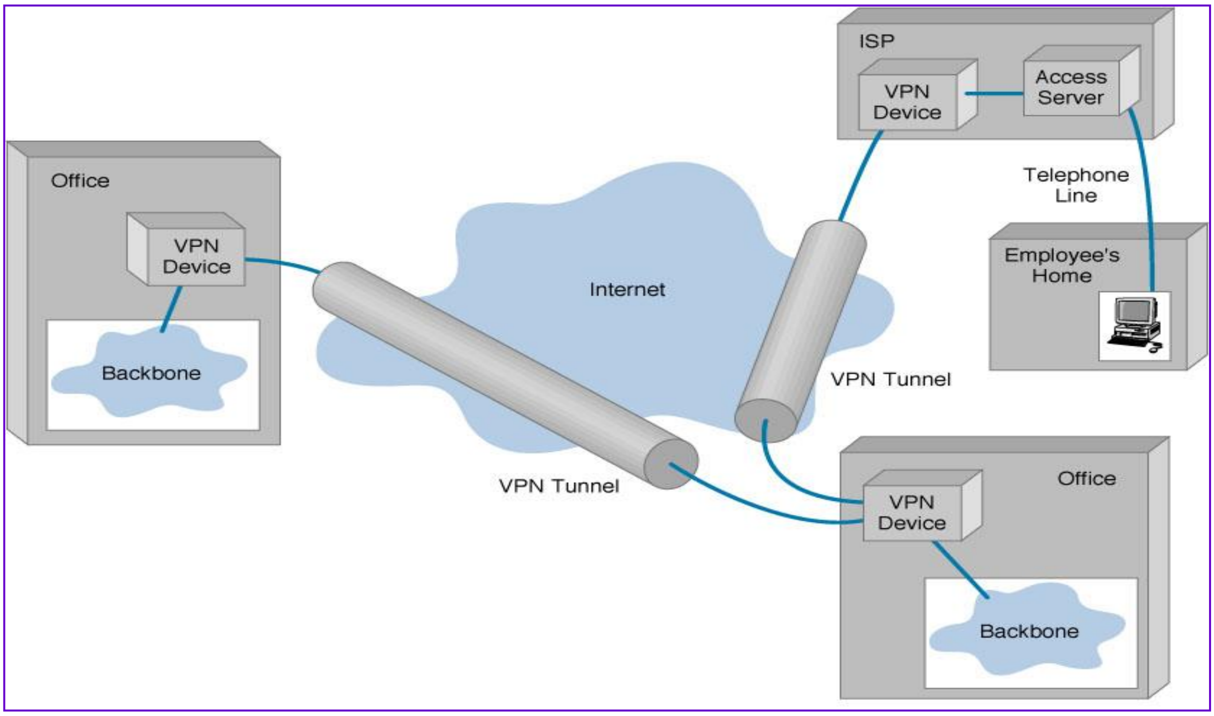


Types of Implementations

There are 3 types of Implementations

- Intranet – Within an organization
- Extranet – Outside an organization
- Remote Access – Employee to Business

Virtual Private Networks (VPN)   Basic Architecture



Based of Device Used in VPN

There are 3 types

- **Hardware**
- **Firewall**
- **Software**

- ❖ **Device Types: Hardware - Usually a VPN type of router**

<u>Pros</u>

- **Highest network throughput**
- **Plug and Play**
- **Dual-purpose**

<u>Cons</u>

- **Cost**
- **Lack of flexibility**

- ❖ **Device Types: Firewall – More Security**

<u>Pros</u>

- **“Harden” Operating System**
- **Tri-purpose**
- **Cost-effective**

<u>Cons</u>

- **Still relatively costly**

Device Types: Software

- ❖ **Ideal for 2 end points not in same org.**
- ❖ **Great when different firewalls implemented**
- ❖ **Device Types: Software – More Security**

<u>Pros</u>

- **Flexible**
- **Low relative cost**

<u>Cons</u>

- **Lack of efficiency**
- **More labor training required**
- **Lower productivity; higher labor costs**

Advantage and Disadvantage of VPN

Advantage

Cost Saving

- ❖ **Eliminating the need for expensive long-distance leased lines**

- **Reducing the long-distance telephone charges for remote access.**
- **Transferring the support burden to the service providers**
- **Operational costs**

Scalability

- **Flexibility of growth**
- **Efficiency with broadband technology**

Disadvantages

- **VPNs require an in-depth understanding of public network security issues and proper deployment of precautions**
- **Availability and performance depends on factors largely outside of their control**
- **Immature standards**
- **VPNs need to accommodate protocols other than IP and existing internal network technology**

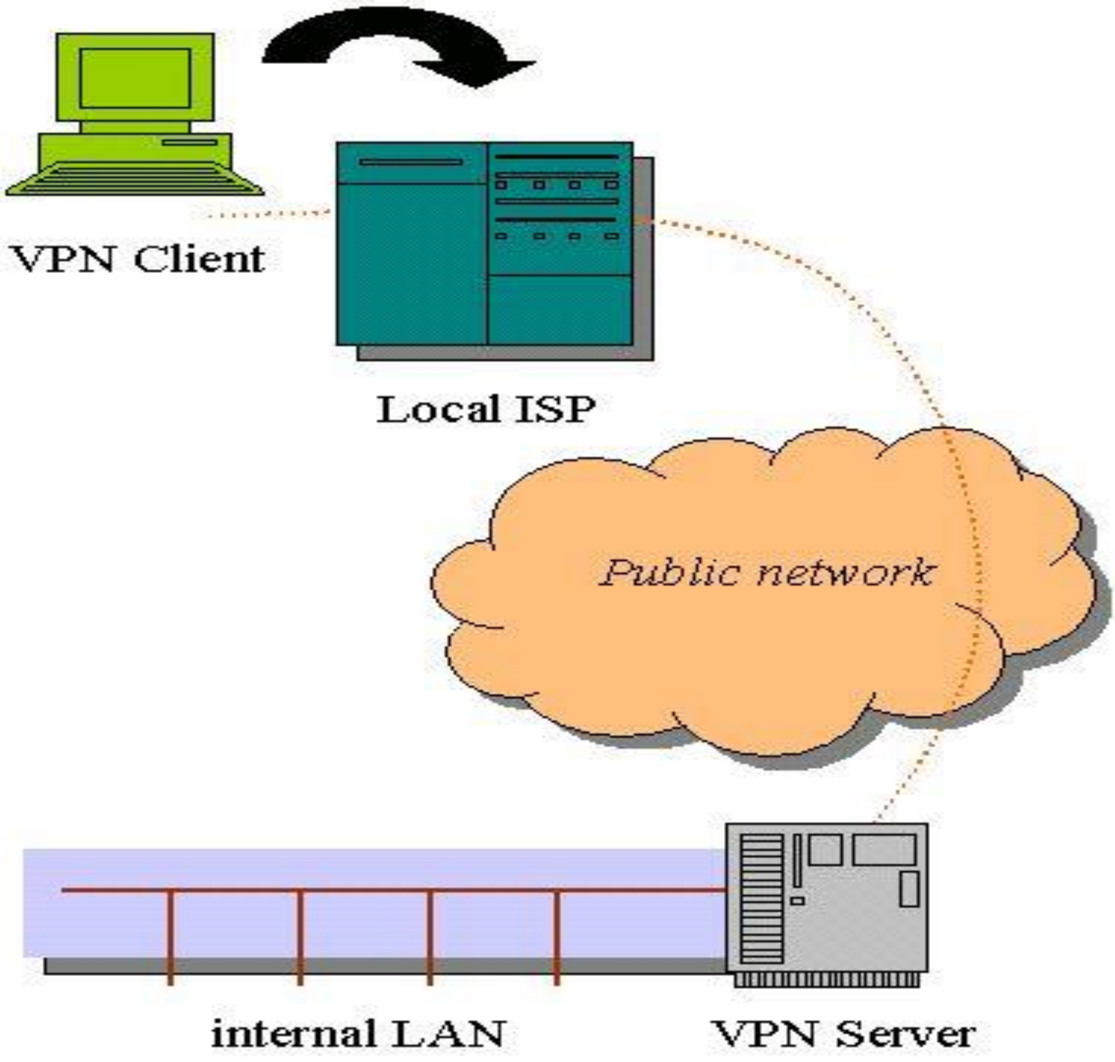
Applications:

Site-to-Site VPNs

Applications:

Site-to-Site VPNs

- **Large-scale encryption between multiple fixed sites such as remote offices and central offices**
- **Network traffic is sent over the branch office Internet connection**
- **This saves the company hardware and management expenses**



Industries That May Use a VPN

- Healthcare: enables the transferring of confidential patient information within the medical facilities & health care provider
- Manufacturing: allow suppliers to view inventory & allow clients to purchase online safely
- Retail: able to securely transfer sales data or customer info between stores & the headquarters
- Banking/Financial: enables account information to be transferred safely within departments & branches
- General Business: communication between remote employees can be securely exchanged

Multiprotocol Label Switching (MPLS) based VPN

Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table. The labels identify virtual links (*paths*) between distant nodes rather than endpoints. MPLS can encapsulate packets of various network protocols. MPLS supports a range of access technologies, including T1/E1, ATM, Frame Relay, and DSL.

- MPLS Based Layer 3 VPNs
– Provider's router participates in customer's layer 3 routing.
– Provider router manages VPN-specific routing tables, distributes routes to remote sites.
– CPE routers advertise their routes to the provider.

- MPLS Based Layer 2 VPNs
– Customer maps their layer 3 routing to the circuit mesh.
– Provider delivers Layer 2 circuits to the customer, one for each remote site.
– Customer routes are transparent to provider.

National knowledge network

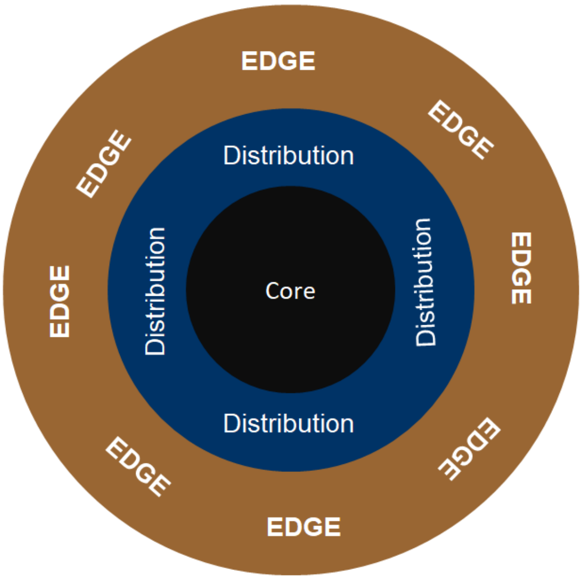
Welcome to 10,000,000,000 bits per second !

National Knowledge Network (NKN) is a multi-gigabit national research and education network, whose purpose is to provide a unified high speed network backbone for educational and research institutions in India. The network is managed by the National Informatics Centre.

The NKN is a hierarchical network divided into three basic layers – ultra-high speed CORE (multiples of 10 Gbit/s; Level 1), Distribution (Level 2), and Edge (speeds of 1 Gbit/s or higher; User Level). Depending on the type of connectivity required by the user organization, geographical presence, and the location of Point of Presence (PoP) of NKN, (belonging to Core and Distribution), connectivity would be provided to the institutes. NKN backbone will typically have 18 Core PoPs and around 25 Distribution PoPs across the country. The NKN backbone will be created by multiple bandwidth providers and the edges can be provided by any service provider.

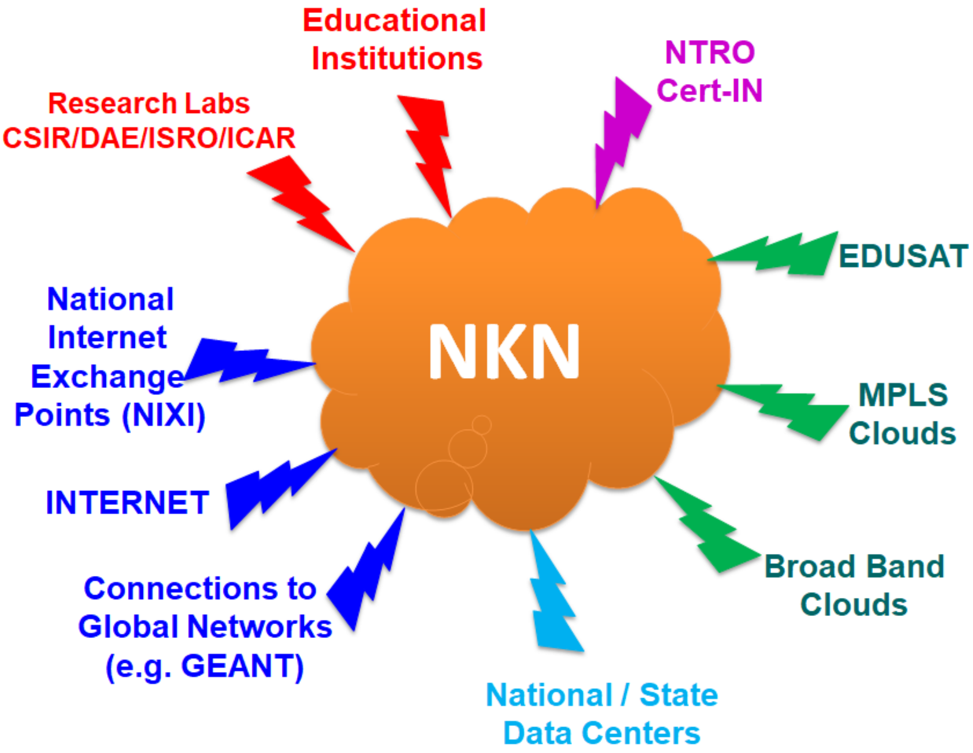
The network is designed to support Overlay Networks, Dedicated Networks, and Virtual Networks. Advanced applications in areas such as Health, Education, Science & Technology, Grid Computing, Bioinformatics, Agriculture, and Governance will be an integral part of NKN. The entire network will seamlessly integrate with the global scientific community at multiple gigabits per second speed.

NKN Topology



Why ?

- **Computational Resource Access**
- **Critical Mass of Scientists in Key Areas**
- **Common Country-wide Classrooms**
- **Increased Peer Group Interaction**
- **Data Bases Sharing Online**

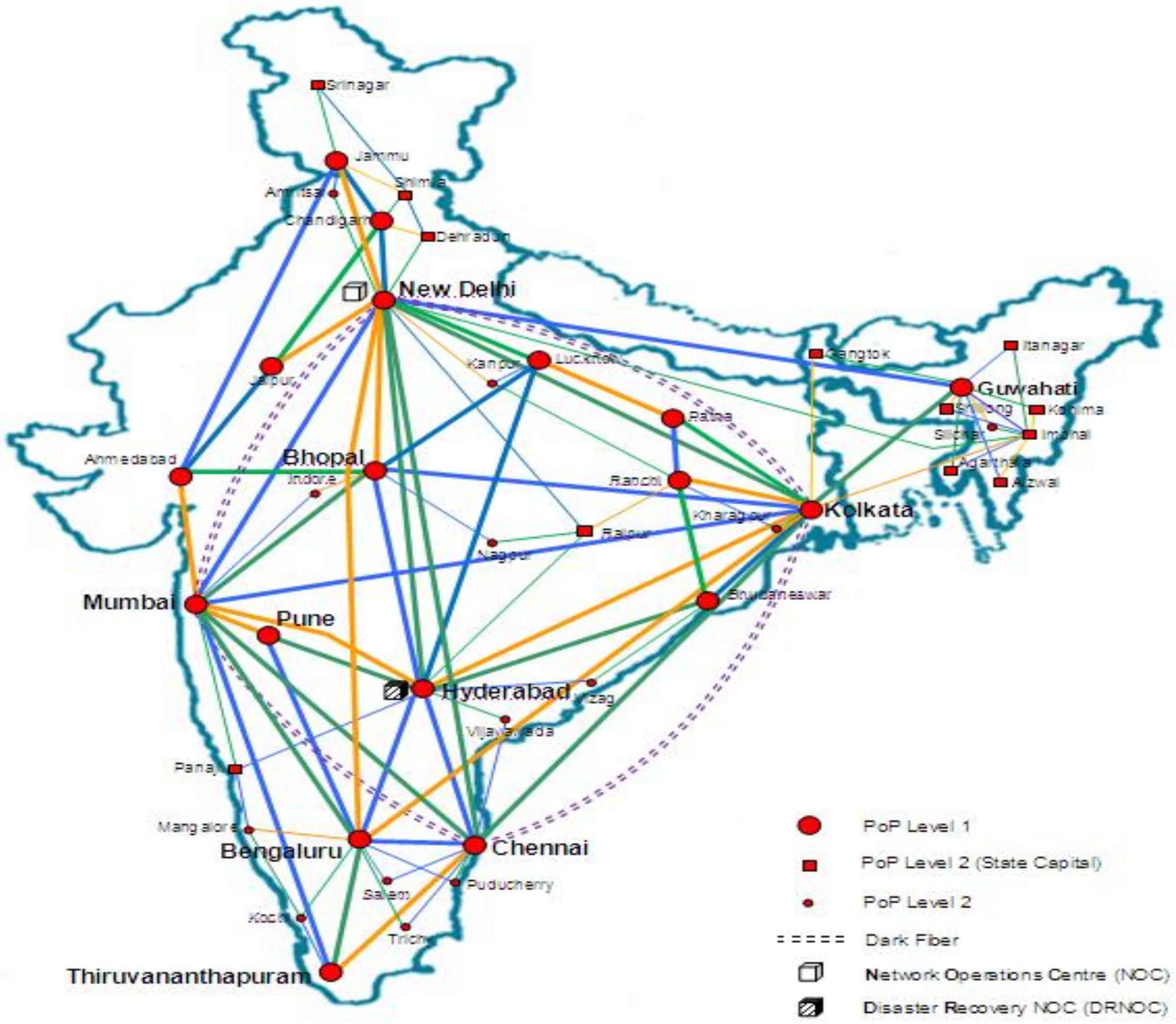

Educational Institutions
NTRO Cert-IN
Research Labs CSIR/DAE/ISRO/ICAR
EDUSAT
National Internet Exchange Points (NIXI)
NKN
MPLS Clouds
INTERNET
Broad Band Clouds
Connections to Global Networks (e.g. GEANT)
National / State Data Centers

Application required high bandwidth.

- Virtual Laboratories
- Collaborative Mega Science Projects
- Innovative Info-Bio-Nano Experiments
- Non-invasive Medicare for Diseases like Cancer
- Diagnostic Domes as Public Health Centers in Rural Areas
- Country-wide Classroom
- University without Walls
- Voice Conferencing among Researchers
- Video Conferencing among Researchers
- On-line access to Electronic Resources

Life @ 10 Gbps

- **Scenario #1: Education**
- **Scenario #2: Research**
- **Scenario #3: HealthCare**
- **Scenario #4: Governance**
- **Scenario #5: FarmCare**
- **Scenario #6: HPC: Weather Modeling**



Features NKN

- High Capacity, Highly Scalable Backbone
- Provide QoS and Security
- Wide Geographical Coverage
- Common Standard Platform
- Bandwidth from Many NLD's
- Highly Reliable & Available by Design
- Test beds (for various implementation)
- Dedicated and Owned**.**

NKN design philosophy is to Encourage, Enable, Enrich and Empower the user community to test and implement innovative ideas without any restriction from the network technology and its administration. Based on that philosophy, as a next generation network, NKN will cater to the following requirements:

Network design –

NKN design follows all the current standards to permit seamless inter-operability amongst technologies and seamless integration amongst different original equipment manufacturers.

Security requirements –

With the growing number of incidences reported by CERT and the increasing challenges posed by innovations in convergence, keeping the network alive can be possible only with very stringent security measures designed, implemented and deployed.

Service requirements –

These requirements are essential for transparent delivery of services based on either heritage (as in telephony) or the general requirements for a particular service.

Network requirements –

These requirements are network-specific and can be tied to specific services, specific delivery mechanism (client could be variety of devices like PC/ PDA/ any other device) and access mechanisms like (intranet / Internet). The design will cater to the overall performance goal of the NKN infrastructure.

Operational requirements –

The NKN is designed to cater to the requirements of tracking, troubleshooting, health monitoring and proactive performance monitoring. With the converged network it becomes more important to proactively monitor the network for impending issues.

NKN Services:

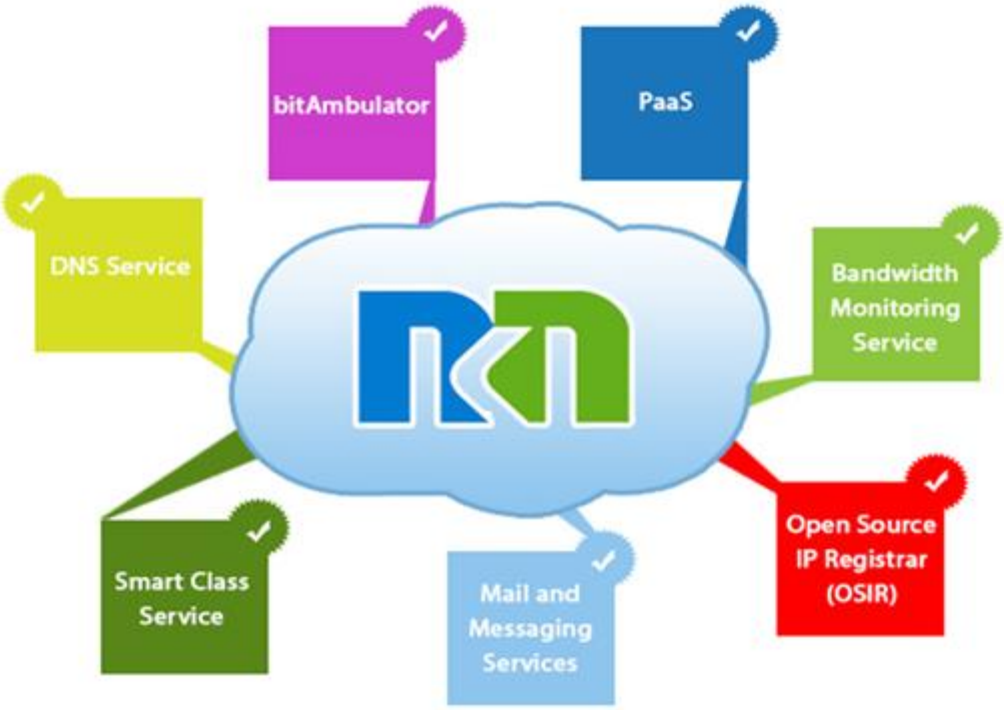
NKN is steadily evolving as the National Education Research Network (NREN) of India. The project has already made significant progress by connecting over 1700+ institutes in the network. NKN is now being looked as the harbinger of change in our knowledge society but this also brings together the responsibility to continuously look forward to providing the much-required impetus to R&D initiatives related to networking technology.

NKN understands the requirement of R&D initiatives without a profit motive and therefore took a step forward in facilitation of this cause. The team comprising of zealous engineers and networking experts have worked over past few months to develop set of NKN products and services.

NKN Services are categorized into three major categories:

Network Oriented Services

Application Services


bitAmbulator
PaaS
DNS Service
nkn
Bandwidth Monitoring Service
Open Source IP Registrar (OSIR)
Smart Class Service
Mail and Messaging Services

Community Services:

The focus area is the common problems faced by a pool of users and provide them an easy access to tools and technologies through a centralized mechanism. The delivery mechanism for these services is primarily cloud-based technology which allows us to disseminate it to a larger audience within short span of time.

Collaborative Research :

NKN enables collaboration among researchers from different educational networks like GLORIAD, TEIN3, GARUDA, CERN etc. NKN also enables sharing of scientific databases and remote access to advanced research facilities.

Grid Computing:

NKN has the capability to handle high bandwidth with low latency with a provision overlay grid computing. Some of the grid-based applications are climate change/global warming, science projects like Large Hadron Collider (LHC) and ITER.

Sharing of Computing Resources:
High-performance computing is critical for national security, industrial productivity, and advances in science and engineering. The network enables many institutions to access high-performance computing to conduct advanced research in areas such as weather monitoring, earthquake engineering and other computationally intensive fields.

Countrywide Virtual Classroom:
NKN is a platform for delivering effective distance education where teachers and students can interact in real time. This is especially significant in a country like India where access to education is limited by factors such as geography, lack of infrastructure facilities etc.

e-Governance:
The NKN will provide high speed backbone connectivity for e-governance infrastructure such as Data Centres at the national and state levels, and networks (SWANs). The NKN will also provide massive data transfer capabilities required for e-governance applications.

The End.