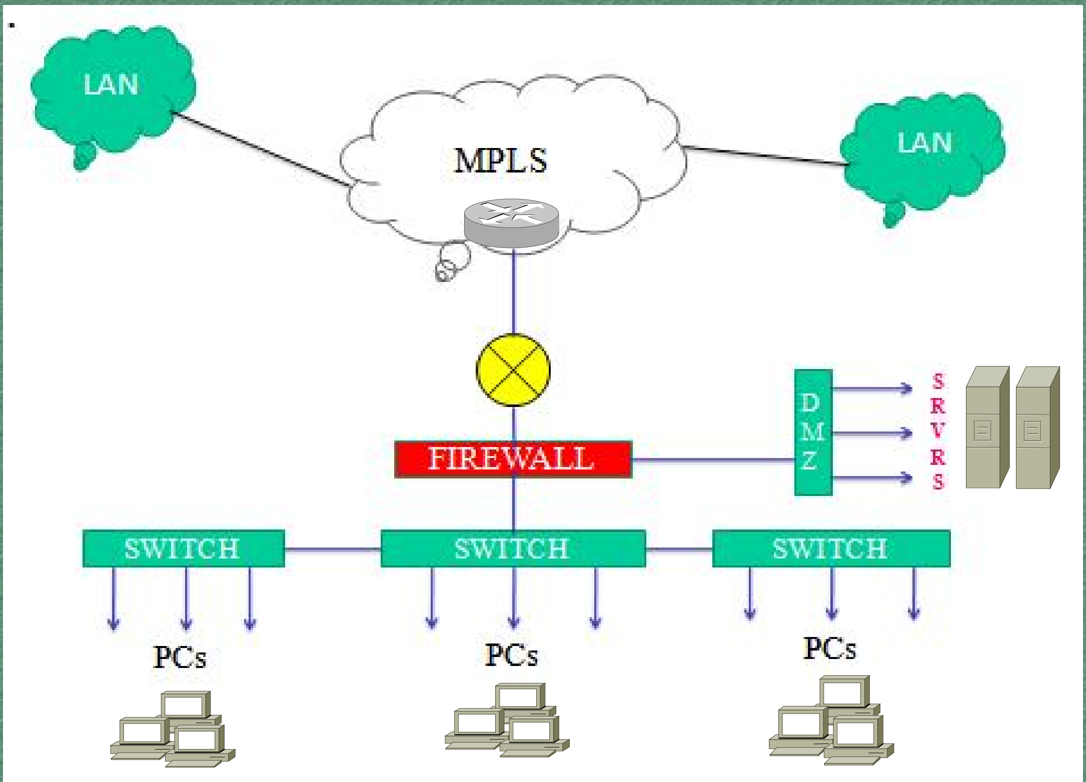
इरिसेट IRISET

TA3

DATA NETWORKS OF IR



Indian Railways Institute of
Signal Engineering and Telecommunications

SECUNDERABAD - 500 017

TA3

DATA NETWORKS OF IR

The Material Presented in this IRISET Notes is for guidance only. It does not over rule or alter any of the Provisions contained in Manuals or Railway Board's directives.

INDIAN RAILWAYS INSTITUTE OF SIGNAL ENGINEERING &
TELECOMMUNICATIONS, SECUNDERABAD - 500 017

Issued in February 2014

TA3

DATA NETWORKS OF IR

CONTENTS

Prepared by	D. Anandam, INW1
Approved by	C.K. Prasad, Professor Tele
DTP	K. Srinivas, JE(D)
Edition no	02
No. of pages	54
No. of sheets	28

http://www.iriset.indianrailways.gov.in

CHAPTER-1

NETWORKING COMPONENTS

1.0 NETWORKS – INTRODUCTION

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer or other device of capable of sending or/and receiving data generated by other nodes on the network, and use of resources between one another. Managing a computer network which are located in different time zones around the world that communicates through teleconferencing, e-mail and multimedia etc. over the network

Most networks use distributed processing, in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of process, separate computers (usually a personal computer or workstation) handle a subset. Advantage of distributed processing is security, distribution of database, faster problem solving etc.

Computer networks achieve these goals in three ways

Sharing information (or data)
Sharing resources (Hardware and Software)
Centralized administration and support

1.1 Network Architecture

A topology is basically a way to organize the network. The physical topology is the way you physically lay out the network, like a map, and the logical topology is the way the information flows on the network (data actually transfers). A logical network describes how the network operates and a physical network describes how networks has been cabled..

1.1.1 Client – Server:

Client/server model is a network in which the role of the client is to issue requests and the role of the server is to service to those requests. Clients connect to the server across the network in order to access the service. A server can be a piece of software running on a computer, or it can be the computer itself.

One of the simplest examples of client-server is a File Transfer Protocol (FTP) session. A computer running FTP software opens a session to an FTP server to download or upload a file. The FTP server is providing file storage services over the network. Because it is providing file storage services, it is said to be a ’file server’. A client software application is required to access the FTP service running on the file server.

Whether a computer is a client, a server, or both, it can serve multiple functions. For example, a single computer can run web server and file server software at the same time to serve different data to clients making different kinds of requests. Client software can also communicate with server software on the same computer. Communication between servers, such as to synchronize data, is sometimes called inter-server or server-to-server communication.

1.1.2 Peer-to-Peer:

A **peer-to-peer** computer network is one in which each computer in the network can act as a client or server for the other computers in the network, allowing shared access to various resources such as files, peripherals etc. without the need for a central server.

Peer-to-peer (P2P) networking eliminates the need for central servers, allowing all computers to communicate and share resources as equals. Music file sharing, instant messaging and other popular network applications rely on P2P technology.

Millions of people use free P2P file sharing programs like BitTorrent software, to swap music, video and other files over the Internet.

1.1.3 VLAN (Virtual Local Area Network):

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical Local Area Network, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

1.1.4 Distributed Services:

The simplest example of a distributed service is Domain Name Service (DNS) which performs the function of turning human-understandable domain names into numerical (dotted quad) computer addresses called IP addresses. Whenever you browse a web page, your computer uses DNS. Your computer sends a DNS request to your local DNS server. Your local DNS server will then contact a remote server on the Internet called a "DNS Root Server" to begin the lookup process. This DNS Root Server will then direct your local DNS server to the owner of the domain name the website is a part of. Thus, there are at least three DNS servers involved in the process of finding and providing the IP address of the website you intended to browse. Your local DNS server provides the query functions and asks other servers for information. The Root DNS server tells your local DNS server where to find an answer. The DNS server that ’owns’ the domain of the website you are trying to browse tells your local DNS server the correct IP address. Your computer stores that IP address in its own local DNS cache. Thus, DNS is a distributed service that runs everywhere, but no one computer can do the job by itself.

1.2 LAN NETWORK ARCHITECTURE – General

Different Local Area Networks follow different protocols and resides data link layer of the OSI model and standardized by IEEE (table1.1). Following characteristics differentiate one LAN from another:

Protocols: The rules and encoding specifications for sending data. A LAN protocol is a set of rules for communicating between computers. Protocols govern format, timing, sequencing and error control. Without these rules the computers can’t make sense of the stream of incoming bits.

Topology: The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.

Media: Devices can be connected by twisted-pair wire, coaxial cables, or fiber optic cables or wireless means.

The following are the some of the different types of popular LANs, with Ethernet over twisted pair cabling, and Wi-Fi are the two most common technologies currently used to build LANs.

- **Ethernet LANs:** It is most widely used LAN technology and specified in a standard called IEEE 802.3. Ethernet uses a bus/star topology in which the individual nodes (devices) are networked with one another via networking equipment such as hubs/switches.

- **Token Ring LANs:** Mostly used in IBM computers and standardized with protocol IEEE 802.5. In a token ring LAN, a number of stations connected by transmission links in a ring topology. It uses a special three-byte frame called a token that travels around the ring. Token-possession grants the possessor permission to transmit on the medium. Token ring frames travel completely around the loop.

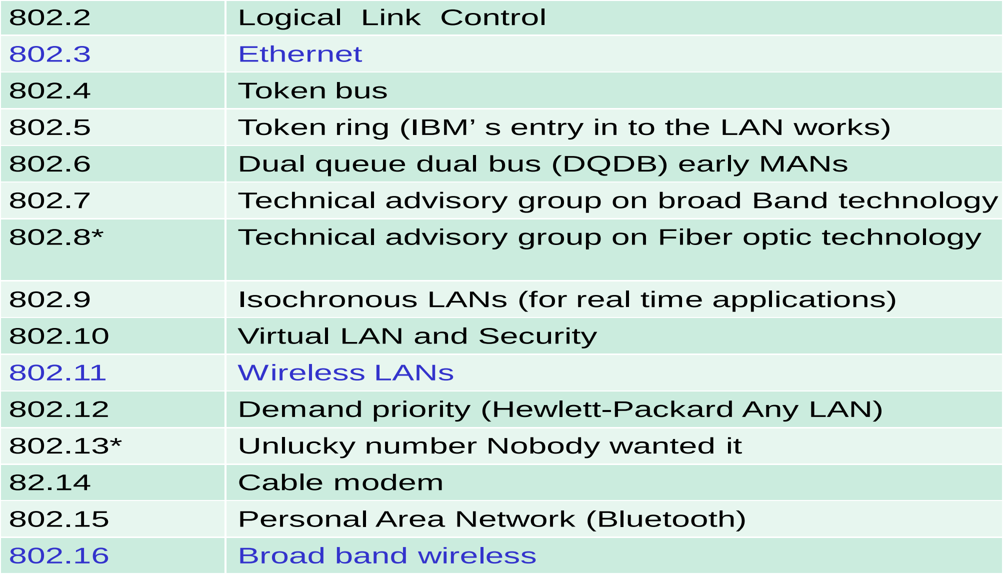
- **Token Bus LANs:** The main difference of token bus from token ring is that the endpoints of the token bus do not meet to form a physical ring. Token bus was standardized by IEEE standard 802.4 and used by General Motors.

- **FDDI LANs:** Fiber Distributed Data Interface is variant of Token Ring A FDDI network contains two optical fiber transmission rings, one as a secondary backup in case the primary ring fails.

1.3 ETHERNET - Introduction

Ethernet is a one of the family of computer networking technologies for local area networks (LANs). Ethernet was commercially introduced in 1980 and standardized in 1985 as IEEE 802.3. The other IEEE LAN standardizations are shown in table 1.3.

Ethernet was so- named by Robert Metcalfe to his LAN invention as once thought “Ether” is a passive substance that exist everywhere in the universe and light is carried by the Ether through out the universe. And he desired that his network invention using shared cabling, also a passive medium could similarly carry data everywhere throughout the network like ether carrying light. Ethernet networks are typically found in a bus or star configuration.



802.2	Logical Link Control
802.3	Ethernet
802.4	Token bus
802.5	Token ring (IBM’ s entry in to the LAN works)
802.6	Dual queue dual bus (DQDB) early MANs
802.7	Technical advisory group on broad Band technology
802.8*	Technical advisory group on Fiber optic technology
802.9	Isochronous LANs (for real time applications)
802.10	Virtual LAN and Security
802.11	Wireless LANs
802.12	Demand priority (Hewlett-Packard Any LAN)
802.13*	Unlucky number Nobody wanted it
82.14	Cable modem
802.15	Personal Area Network (Bluetooth)
802.16	Broad band wireless

Table 1.3 IEEE-LAN standards under 802 working group

1.3.1 Ethernet LAN - BUS Topology

Initial Ethernet LAN technology is a passive, wait-and-listen network architecture. Ethernet provides access to the network using Carrier Sense Multiple Access with Collision Detection (CSMA/CD). This strategy of network access basically means that the devices (such as computers) on the network listen to the network and wait until the line is clear; they "sense" when the line is clear and they can transmit data. The computer then sends its packets out onto the line. If there is more than one computer transmitting, collisions result. Sensing the collisions, the computers stop transmitting and wait until the line is free. One of the computers will then transmit, gaining control of the line and completing the transmission of the data.

To receive data, computers just sit and wait, listening to the line. When they sense that a particular transmission is meant for them, they receive it on their network card.

The main advantage of Ethernet is that it is one of the cheapest and high-speed network architectures to implement. Network interface cards, cabling, and hubs are fairly inexpensive when compared to the hardware required for other architectures such as Token Ring. A major disadvantage of Ethernet relates to collisions and broadcasts on the network. The more collisions and broadcasts, the slower the network will run, and excessive collisions can even bring down the network. Ethernet star technology eliminates the collisions and minimizes the broadcast problems.

1.3.2 Ethernet LAN e – STAR Topology

As technology advanced, the passive media is replaced with an intelligent device called switch and solved the major disadvantages of Ethernet bus i.e. collisions and broadcasts some extent.

Even though switch is advanced and intelligent device, they must flood all broadcast and multicast traffic due to technological requirement. The accumulation of broadcast and multicast traffic from each device in the network is referred to as broadcast radiation and high levels of broadcast and multicast radiation can noticeably degrade network performance and also affects the CPU performance of hosts on the network.

This is the one of the main reason for approaching wide area networks (Routers) for limiting the broadcast and multicast radiation with in the local area network

Types of Ethernets:

Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Max.Length
Ethernet	10 Mbps	10BASE-T	802.3	Copper, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	802.3u	Copper, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-T	802.3ab	Copper, 100 m
Gigabit Ethernet	1000 Mbps	1000BASE-SX 1000BASE-LX	802.3z	Fiber,550m(**SX**) 5km (LX)
Gigabit Ethernet	10000 Mbps	10GBASE-T	802.3an	Copper,100m (4pairs)

The original / old Ethernet standards are 10BASE-2 and 10BASE-5

1.4 Ethernet LANs-Devices

- TRANSMISSION MEDIA
- Network Interface Card (NIC)
- HUB
- Bridges
- SWITCH

1.4.1 CABLING OPTIONS

Copper-based network cabling takes two major forms: coaxial cable and twisted-pair cable. Although the prices for fiber-optic cable (which does not experience interference because it uses light energy rather than electrical energy) are dropping and more fiber-optic LANs (particularly LAN backbones) are popping up all the time, copper wire is still the predominant wire type.

1.4.2 COAXIAL CABLE

Two types of coaxial cable are used for networking computers: Thick net (RG-8 and RG-11 coaxial cable) and Thin net (RG-58 coaxial cable). Thick net is a heavy-gauge coaxial cable that is fairly inflexible and requires special equipment (over and above a simple network card) to connect the computer to the network backbone.

Although it is valid for us to discuss coaxial cabling, in reality you are going to find that twisted-pair cable is the network medium of choice for most LANs

1.4.3 TWISTED-PAIR WIRE

Twisted-pair wire comes in two major flavors: unshielded twisted pair (UTP) and shielded twisted pair (STP). The big difference between UTP and STP is that the STP wires are encased in a foil wrap that protects them from interference. UTP is the most commonly used network wiring. It is inexpensive, flexible, and light, thus making it very easy to work with. UTP cable is terminated with an RJ-45 connector. The twisted pair categories are listed in Table 1.3.3

TWISTED PAIR CATEGORIES

Category	Maximum Bandwidth Provided	Additional Information
1	None	Used in old telephone systems; this is not a data-grade cabling.
2	4Mbps	Not really considered a data-grade cable.
3	10Mbps	Considered the minimum cable requirement for data networks running Ethernet.
4	16Mbps	Equivalent to the Type 1 Token-Ring cabling without the shielding.
5	100Mbps	Has become the standard for new LAN installations and has completely overshadowed all the previous categories and called Fast Ethernet
6	1,000Mbps	All 4 pair of CAT6 used for 1Gbps data transmission and called Gigabit Ethernet
7	10,000Mbps	All 4 pairs of CAT 7 used for 10Gbps data transmission and called Gigabit Ethernet

Table 1.3.3 UTP Categories

1.4.4 FIBER-OPTIC CABLE

Fiber-optic cable is a high-speed alternative to copper wire and is often employed as the backbone of larger corporate networks. However, the drop in the price of fiber-optic cable has started to make it a possibility for other LAN uses. Fiber-optic cable uses glass or plastic filaments to move data and provides greater bandwidth as well as longer cable runs.

1.4.5 NETWORK INTERFACE CARDS

The network interface card (NIC) is one of the most important network component (fig.1.3.5) in every computer and performs some of the following important functions. It falls in data link layer (layer-2) of OSI model.

Provides physical connection between computer and network
Provides physical addressing system (MAC) for computer
Enables error checking mechanism (CRC) for the data
Converts parallel data from PC bus in to serial data for transmission

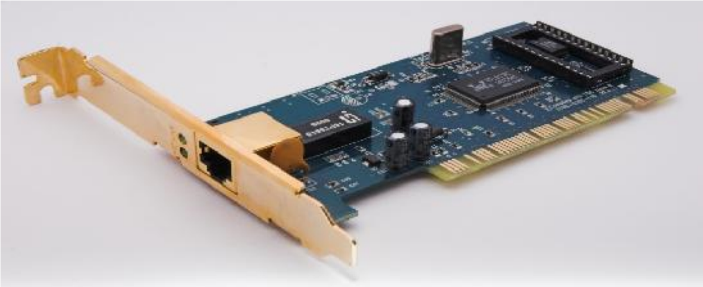
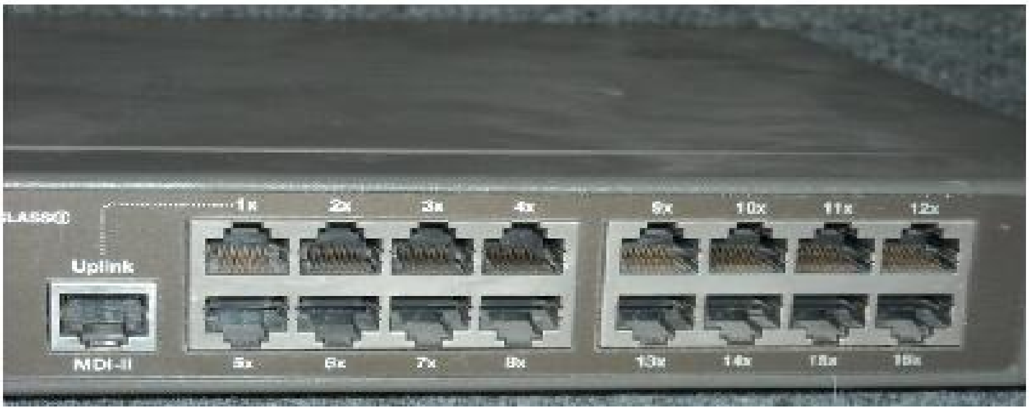


Fig. 1.3.5 Network Interface card – Ethernet

1.4.6 HUBS:

A long central coax cable with workstations connected at regular distances is replaced with hubs to serve as the central connection point for work stations. It provides just centralized bus connection with twisted pair copper cable. If computer 1 talks to computer 3, computer 2 will also hear what computer 1 said. Usually computer 2 just discards traffic not meant for it. Collisions occurs when two systems try to communicate network simultaneously and badly affect the performance of your network. This device works at physical layer (layer-1) of OSI model



Network Hub

1.4.7 BRIDGES:

A bridge connects two segments of the network to conserve the bandwidth available on the network. The bridge works by learning the MAC layer addresses (Ethernet addresses) of the devices on each of its network interfaces. They move frames between ports based on MAC addresses. It works at data link layer (layer-2) of the OSI model. In many respects, a bridge is like an Ethernet switch with very few ports. In practice, a switch can be looked at as a multiport bridge - both have the same basic functionality.

1.4.8 SWITCHES

Modern Ethernet implementations controlled by switches instead of a shared hubs. Perhaps the most striking advancement in contemporary Ethernet networks is the use of **switched Ethernet.** The switch cross connects all clients, servers and network devices, giving each sending-receiving pair the full rated transmission speed. Modern switched Ethernet networks use twisted pair wiring or fiber optics to connect stations in a **radial pattern** and operate at 100 or even 10,000 Mbps where legacy Ethernet networks transmitted data at 10 megabits per second only.
The switch works by learning the MAC layer addresses (Ethernet addresses) of the devices on each of its network interfaces. They move frames between ports based on MAC addresses thus there are no collisions and unnecessary broadcasts.This advancement improves network performance very drastically.

Types of Ethernet switches:

- Unmanageable switch
- Manageable switch
- Layer-3 switch

All switches are plug and play devices. Manageable and layer-3 switches are configurable with extra features if required.

Unmanageable switch: these switches operate at Layer 2 of the OSI model. These switches have no configuration interface or options, hence no configuration can be done. These are cheap and plug and play devices. But they cannot support any additional functionality and manageability.

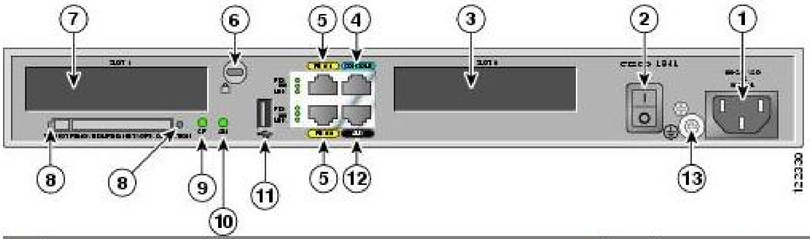
Manageable switch: these switches also operate at Layer 2 of the OSI model like unmanageable switch but support additional functionality and manageability like STP, VLANS, SNMP etc. High-end or "enterprise" switches, provide a serial console and command-line access via telnet and SSH, as well as management via SNMP. More recent devices also provide a web interface. A Web-managed switch is configured through a browser.

Layer 3 switch: Operates at Layer 3 of the OSI model. It has the functionality of switch and router hence works either a switch or a router based on configuration. Layer 3 switches actually differ very little from routers. A Layer 3 switch can support the same routing protocols as network routers do. The Only difference is, a Layer 3 switch will typically posses only Ethernet interfaces and will not possess any WAN ports.

Network Switch

1.4.9 ROUTERS:

Routers are used to connect remote LANs together using different WAN technologies. A router uses a combination of hardware and software to actually "route" data from its source to its destination. Routers have a very sophisticated OS that allows you to configure their various connection ports. It works at network layer (layer 3) of the OSI model, moving packets from one port to another based on L3 addresses – i.e. IP addresses, IPX addresses, etc.



1	Input power connection	8	CompactFlash memory card slot
2	On/Off switch	9	CompactFlash (CF) LED
3	Slot 0 (WIC, VWIC—data only, or HWIC)	10	AIM LED
4	Console port	11	USB port
5	Fast Ethernet ports and LEDs	12	Aux port
6	KensingtonTM security slot	13	Chassis ground connection
7	Slot 1 (WIC, VWIC—data only, or HWIC)		

Router

1.5 Different Router/switch ports, interfaces & connectors are shown in table 1.2

Interface port name	medium	specified distance	Connector
10BASE-T 100BASE-T 1000BASE-T	Shielded/unshielded twisted pair	100 meters	RJ45
1000BASE-CX	balanced copper cabling	25 meters	
1000BASE-SX	multi-mode fiber	500 meters	FX port - SC connectors
1000BASE-LX	single-mode fiber	5 km	
1000BASE-LX10	single-mode fiber	10 km	
1000BASE-BX10	single-mode fiber, over single-strand fiber: 1490 nm downstream 1310 nm upstream	10 km	

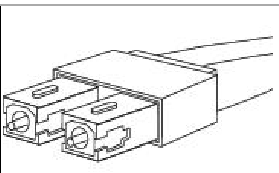
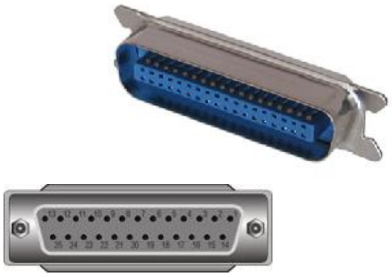
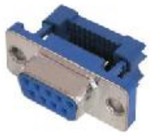
1000BASE-LH	single-mode fiber	10km	
1000BASE-ZX	single-mode fiber at 1550 nm wavelength	~ 70 km	
Serial Port (WAN port)	Copper	15meters	DB-25 Serial Interface RS232 
Auxiliary port (Configuration port)	copper	15meters	DB-9 Serial interface RS232 

Table 1.2 Router/Switch ports, interfaces & connectors

1.5.1 Modular port interfaces

Various optional modules can be installed in the router with modular interface slots, to provide specific capabilities. These modules can be installed inserting them into slots on the chassis

i. Gigabit interface converter (GBIC)

A **gigabit interface** converter (GBIC) is a standard for transceivers as shown in fig 1.5 commonly used with Gigabit Ethernet and fibre channel. By offering a standard, hot swappable electrical interface, one gigabit Ethernet port can support a wide range of physical media, from copper to long-wave single-mode optical fiber, at lengths of hundreds of kilometers.

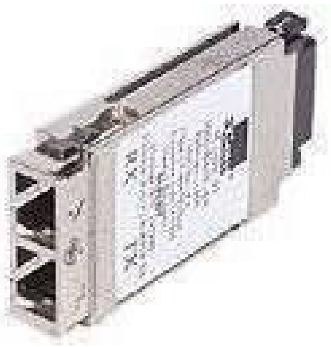


Fig 1.5 GBIC interface module

The appeal of the GBIC standard in networking equipment, as opposed to fixed physical interface configurations, is its flexibility. Where multiple different optical technologies are in use, an administrator can purchase GBICs as needed, not in advance, and they can be the specific type needed for each link. This lowers the cost of the base system and gives the administrator far more flexibility.

ii. SFP MODULES

The **small form-factor pluggable** (**SFP**) is a compact, hot-pluggable optical transceiver as shown in fig 1.6, used in optical communications for both telecommunication and data communications applications. It interfaces a network device mother board (for a switch, router or similar device) to a fiber optic or unshielded twisted pair networking cable. It is a popular industry format supported by several fiber optic component vendors.

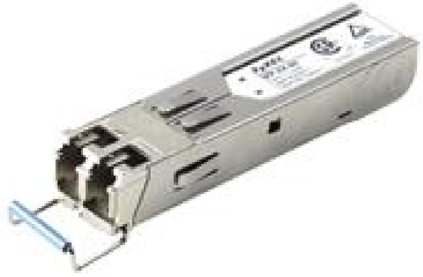


Fig. 1.6 SFP optical trans-receivers (mini GBIC port)

SFP transceivers are available with a variety of different transmitter and receiver types, allowing users to select the appropriate transceiver for each link to provide the required *optical reach* over the available optical fiber type (e.g. multi-mode fiber or single-mode fiber). Optical SFP modules are commonly available in several different categories: 850 nm 550m MMF (SX), 1310 nm 10km SMF (LX), 1550 nm [40 km (XD), 80 km (ZX), 120 km (EX or EZX)], and DWDM.

1.6 COMPUTER TERMINALS AND SERVERS

Client: A client is a program running on a local machine, requests service from server. A client program is started by the user and terminates when the service is completed. Web browser (e.g. Internet Explorer) is client requests the web pages of web server.

Server: A server is a program running on the remote machine providing service to the client program. A server program runs infinitely and waits for requests from clients but it never it initiates a service until it is requested by the client. Web server (e.g. IIS / APACHE) is server serves the web pages as requested by client (e.g. Internet explorer)

Finally, the web server sends the result to the web browser, which interprets the data. The server machine often has a faster CPU, more memory, and more disk space and loaded with NOS (e.g. Windows 2008 server) than a typical client machine.

1.6.1 Computer terminal

A **computer terminal** is an electronic or electromechanical hardware device that is used for entering data into, and displaying data from, a computer or a computing system. A computer terminal is an instance of a human-machine interface (HMI).

The function of a terminal is confined to display and input of data; a device with significant local programmable data processing capability may be called a "smart terminal" or thin client. A personal computer can run software that emulates the function of a terminal, sometimes allowing concurrent use of local programs and access to a distant *terminal host* system.

1.6.2 Proxy Server

In computer networks, a proxy server is a server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client. A proxy server may optionally alter the client’s request or the server’s response, and sometimes it may serve the request without contacting the specified server. In this case, it ’caches’ responses from the remote server, and returns subsequent requests for the same content directly.

A proxy server has many potential purposes, including:

- To keep machines behind it anonymous (mainly for security).
- To speed up access to resources (using caching). Web proxies are commonly used to cache web pages from a web server.
- To apply access policy to network services or content, e.g. to block undesired sites.
- To log / audit usage, i.e. to provide company employee Internet usage reporting.
- To scan transmitted content before delivery for malware.
- To scan outbound content, e.g. for data leak protection.

A proxy server that passes requests and replies unmodified is usually called a gateway or sometimes tunneling proxy.

A proxy server can be placed in the user’s local computer or at various points between the user and the destination servers on the Internet.

A reverse proxy is a (usually) Internet-facing proxy used as a front-end to control and protect access to a server on a private network, commonly also performing tasks such as load-balancing, authentication, decryption or caching.

1.6.3 Fire Wall

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications as shown in fig 1.7. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

Packet filter: Packet filtering inspects each packet passing through the network and accepts or rejects it, based on user-defined rules. Although difficult to configure, it is fairly effective and mostly transparent to its users. In addition, it is susceptible to IP spoofing.

Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.

Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

Unified Threat Management (UTM): The best approach is to have a simple and converged network security appliance – a UTM device. The administrator needs to manage only a single device or two, if it's a failover cluster. A UTM device is a combo device that includes stateful firewall, deep application inspection, Intrusion prevention, content security, VPN, anti spam and anti virus. The most important feature of a UTM security appliance is its ability to stop hacker attacks through its intrusion prevention mechanism. Intrusion prevention examines traffic patterns to determine if an attack is ongoing and proactively stops it.

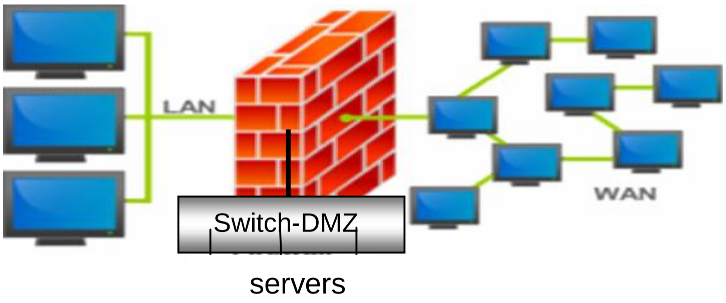


Fig: 1.7 Firewall

1.6.4 Database Server

A database server is a computer program that provides database services to other computer programs or computers, as defined by the client-server model. The term may also refer to a computer dedicated to running such a program. Database management systems frequently provide database server functionality, and some DBMSs (e.g., MySQL) rely exclusively on the client-server model for database access.

In a master-slave model, database master servers are central and primary locations of data while database slave servers are synchronized backups of the master acting as proxies.

1.6.5 NMS (Network Management System)

A Network Management System (NMS) is a combination of hardware and software used to monitor and administer a network.

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
- Maintenance is concerned with performing repairs and upgrades—for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.
- Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

A common way of characterizing network management functions is FCAPS—Fault, Configuration, Accounting, Performance and Security.

Data for network management is collected through several mechanisms, including agents installed on infrastructure, synthetic monitoring that simulates transactions, logs of activity, sniffers and real user monitoring. In the past network management mainly consisted of monitoring whether devices were up or down; today performance management has become a crucial part of the IT team's role which brings about challenges - especially for global organizations.

A large number of access methods exist to support network and network device management. Access methods include the SNMP, command-line interface (CLIs), custom XML, CMIP, Windows Management Instrumentation (WMI), Transaction Language 1, CORBA, NETCONF, and the Java Management Extensions (JMX).

1.6.6 Mail Server

Mail Server is a computer process or software that transfers electronic mail messages from one computer to another, in single hop application-level transactions. It implements both the client (sending) and server (receiving) portion of the simple mail transfer protocol (SMTP)

The term mail server is also loosely used to mean a computer acting as an MTA (Mail transfer agent) by running the appropriate software. The term mail exchanger (MX), in the context of the Domain Name System formally refers to an IP address assigned to a device hosting a mail server, and by extension also indicates the server itself.

An MTA receives mail from another MTA or MSA (Mail submission agent) or from a mail user agent (MUA). The transmission details are specified by the Simple Mail Transfer Protocol (SMTP). In case any recipients of a given message are not hosted locally, the message is relayed, that is, forwarded to another MTA. Every time an MTA receives an email message, it adds a Received trace header field to the top of the headers of the message, thereby building a sequential record of MTAs handling the message. How to choose a target MTA for the next hop is also described in SMTP, but can usually be overridden by configuring the MTA software with specific routes. The MTA works behind the scenes, while the user usually interacts with the MUA. One may distinguish initial submission as first passing through a mail submission agent (MSA) – formally, port 25 is used for communication between MTAs, or from an MSA to an MTA, while port 587 is used for communication between an MUA and an MSA.

For recipients hosted locally, the final delivery of email to a recipient mailbox is the task of a message delivery agent (MDA). For this purpose the MTA transfers the message to the message handling service component of the message delivery agent. Upon final delivery, the Return-Path field is added to the envelope to record the return path.

1.6.7 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by devices (DHCP clients) which dynamically distributes the IP address to the destination host.

Dynamic Host Configuration Protocol automates network-parameter assignment to network devices from one or more fault-tolerant DHCP servers. Even in small networks, DHCP is useful because it can make it easy to add new machines to the network.

When a DHCP-configured client (a computer or any other network-aware device) connects to a network, the DHCP client sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the DNS servers, other servers such as time servers, and so forth. On receiving a valid request, the server assigns the computer an IP address, a lease (length of time the allocation is valid), and other IP configuration parameters, such as the subnet mask and the default gateway. The query is typically initiated immediately after booting, and must complete before the client can initiate IP-based communication with other hosts.

Depending on implementation, the DHCP server may have three methods of allocating IP-addresses:

- Dynamic allocation: A network administrator assigns a range of IP addresses to DHCP, and each client computer on the LAN has its IP software configured to request an IP address from the DHCP server during network initialization. The request-and-grant process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed (dynamic re-use of IP addresses).
- Automatic allocation: The DHCP server permanently assigns a free IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.

Static allocation: The DHCP server allocates an IP address based on a table with MAC address/IP address pairs, which are manually filled in (perhaps by a network administrator). Only requesting clients with a MAC address listed in this table will be allocated an IP address

1.6.8 DNS Server

The Domain Name System (DNS) is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. An often used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, www.games.com translates to 208.77.188.166.

The Domain Name System makes it possible to assign domain names to groups of Internet users in a meaningful way, independent of each user’s physical location. Because of this, World-Wide Web (WWW) hyperlinks and Internet contact information can remain consistent and constant even if the current Internet routing arrangements change or the participant uses a mobile device. Internet domain names are easier to remember than IP addresses such as 208.77.188.166

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their particular domains, and in turn can assign other authoritative name servers for their sub-domains. This mechanism has made the DNS distributed, fault tolerant, and helped avoid the need for a single central register to be continually consulted and updated.

In general, the Domain Name System also stores other types of information, such as the list of mail servers that accept email for a given Internet domain. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

1.7 SPECIFIC DEVICES USED IN PRS NETWORKS

1.7.1 Dumb Terminals

A dumb terminal is a monitor based input output device that does no independent processing, but relies on the computational resources of a computer to which it is connected over a dedicated circuit (or) through a network. Essentially an input/output (I/O) device with no internal processing power, a dumb terminal is a simple input output device comprising a keyboard, monitor, network interface and buffer memory that has only enough intelligence to respond to simple control codes from a computer. This device comes with no hard drive and low powered processors but can run applications on a central server. Normally such terminals are associated with Main frame computers.

1.7.2 Thin Clients

A thin client (sometimes also called a lean or slim client) as shown in fig 1.8, is a computer or a computer program which depends on some other computer (its server) to fulfill its traditional computational roles. This stands in contrast to the traditional fat client, a computer designed to take on, these roles by itself.

The most common type of modern thin client is a low-end computer terminal which concentrates solely on providing a graphical user interface to the end-user. The remaining functionality, in particular the operating system, is provided by the server.

Fig: 1.8 Thin client

The notion of a thin client extends directly to any client-server architecture: in which case, a thin client application is simply one which relies on its server to process most or all of its business logic.

Thin clients are made from low-cost hardware with few moving parts; they can operate in more hostile environments than conventional computers. However, they inevitably need a network connection to their server, which must be isolated from such hostile environments. Since thin clients are cheap, they offer a low risk of theft in general, and are easy to replace when they are stolen or broken.

On the other hand, to achieve this simplicity, thin clients are generally highly integrated systems. This means that they may lag behind thick clients in terms of extensibility and accessibility.

1.7.3 Terminal Server

Terminal Server as shown in fig 1.9 allows asynchronous RS 232 compatible devices to access host computer systems over a TCP/IP network. It connects to the TCP/IP network via a 10/100 BASE-T compatible Ethernet port.

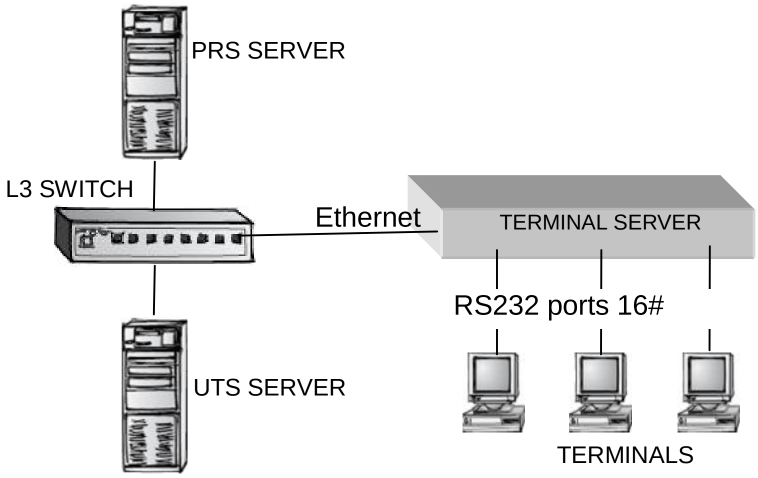


Fig. 1.9: Terminal Server – a typical application

The CYGNUS 1021 incorporates several useful features that simplify operator interaction.

These features include:

- Ability to initiate multiple simultaneous sessions from each terminal port. This allows operators to establish sessions with several different hosts simultaneously, and to switch between these sessions without needing to terminate any of them.
- Ability to program separate answer back codes for each session on a port. This allows host applications to authenticate the port from which a connection is established, thereby reducing the possibility of unauthorized access.

1.7.4 Network Terminal Server (NeTS)

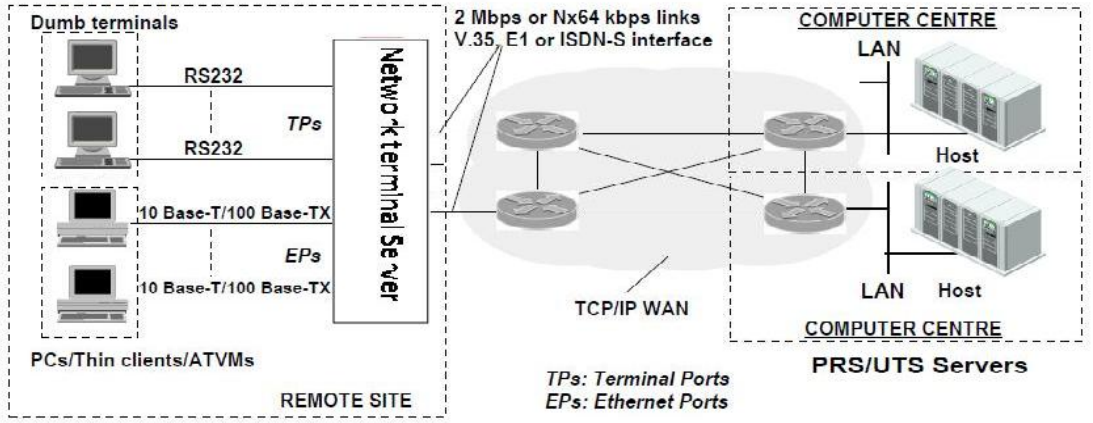


Fig. 1.10: Network Terminal Server – a typical application

Network Terminal Server (NeTS) as shown in fig 1.10, is an ideal solution for connecting terminal equipment such as dumb terminals, PCs, thin clients and serial printers at remote stations in the Indian Railways' PRS and UTS applications to the central servers. It is a standard compliant, cost effective alternative to solutions which require a terminal server, LAN switch and router at the remote site to achieve this purpose, and also has features which facilitate PRS-UTS integration. Dumb terminals and serial printers can be connected to the product's Terminal Ports. PCs and Thin Clients can be connected to its LAN port

1.7.5 STATMUX (Statistical Multiplexer)

Statistical time division multiplexer (Statmux) as shown in fig 1.1, allows traffic from up to sixteen (16) asynchronous RS232 compatible devices, and a telephone voice conversation, to be carried on a single leased circuit between two locations. The typical application of the product is to extend a cluster of terminals from a central mainframe/minicomputer to a remote location.

Traffic from data devices connected to the "terminal ports" of the CYGNUS 517 is combined using "statistical" multiplexing, and sent onto the leased line through the unit's "composite port". Statistical multiplexing allocates the capacity of the leased line based on the need of each user. This is an efficient method to share leased line capacity, especially in transaction processing applications where a human operator at a terminal carries out transactions on a central computer

The composite port of the CYGNUS 517 is meant to be connected to leased lines

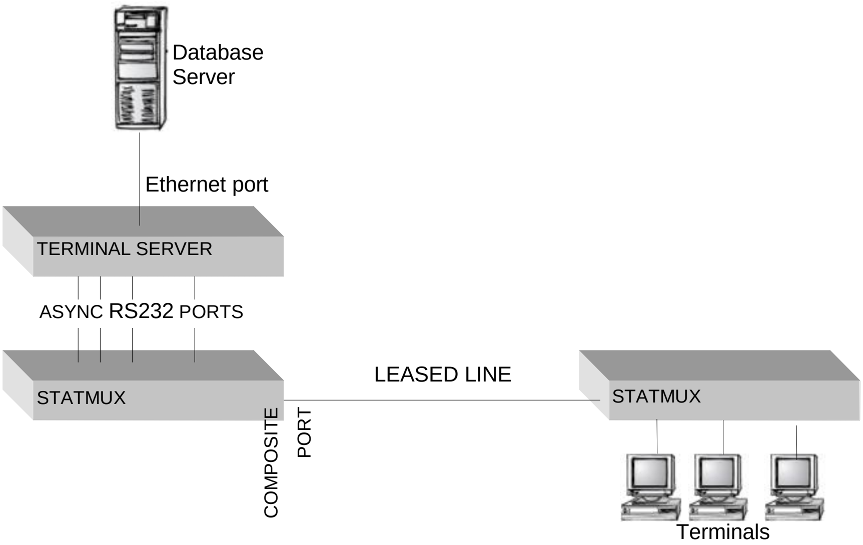


Fig. 1.11 STATMUX - a typical application

1.7.6 LINE DRIVER

A Line driver is an amplifier used to improve the transmission reliability of a usually digital intra facility metallic transmission line, over extended distances, by driving the input to the transmission line with a higher than normal signal level.

1.8 VSAT

VSAT stands for "***Very Small Aperture Terminal***" and refers to receive / transmit terminals installed at dispersed sites connecting to a central hub via satellite using small diameter antenna dishes (0.6 to 3.8 meter).

VSAT technology represents a cost effective solution for users seeking an independent communications network connecting a large number of geographically dispersed sites. VSAT networks offer value-added satellite-based services capable of supporting the Internet, data, LAN, voice/fax communications, and can provide powerful, dependable private and public network communications solutions. It supports traffic capacity of 9.6Kbps to 2Mbps.

1.8.1 VSAT System Architecture

A VSAT system consists of a satellite transponder, central hub or a master earth station, and remote VSATs. The VSAT terminal has the capability to receive as well as transmit signals via the satellite to other VSATs in the network. Depending on the access technology used the signals are either sent via satellite to a central hub, which is also a monitoring centre, or the signals are sent directly to VSATs with the hub being used for monitoring and control.

1.8.2 TYPES OF VSAT

There are two types of VSAT Satellite

a. Bi-Directional Operation - The dish both sends (uplinks) and receives (downlinks) information.
b. Receive-Only Operation - The dish receives (downlinks) information only.

1.8.3 VSAT Topologies

The network of VSATs at different locations adopts different topologies depending on the end applications traffic flow requirements. These topologies could be Star or Mesh.

i. Star topology

The most popular of these is Star topology as shown in **fig 1.12a**, here we have a big central earth station known as the hub. Generally the hub antenna is in the range of 6-11metre in diameter. This hub station controls, monitors and communicates with a large number of dispersed VSATs. Since all VSATs communicate with the central hub station only, this network is more suitable for centralized data applications. Large organizations, like banks, with centralized data processing requirements is a case in point.

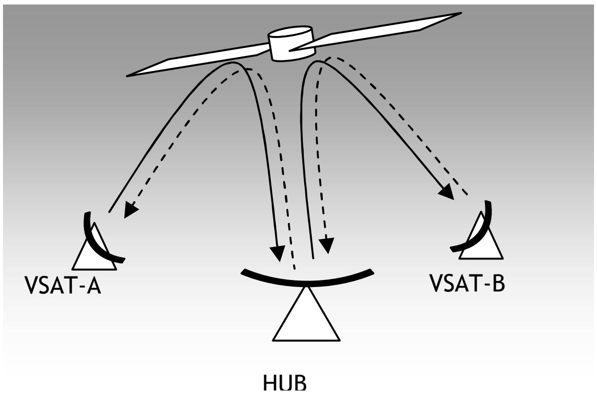


Fig. 1.12a Star topology

ii. Mesh topology

In a mesh topology a group of VSATs communicate directly with any other VSAT in the network without going through a central hub as shown in **Fig. 1.12b.** A hub station in a mesh network performs only the monitoring and control functions. These networks are more suitable for telephony applications. These have also been adopted to deploy point to point high speed links.

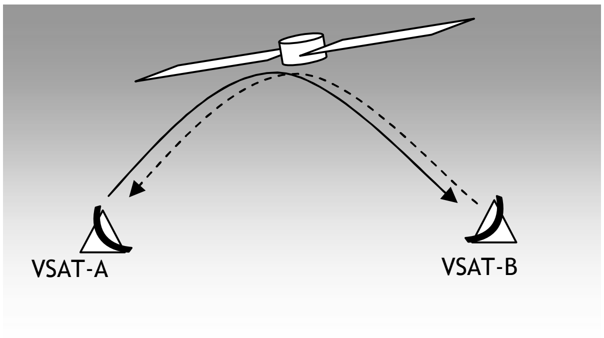


Fig. 1.12b Mesh topology

However, in actual practice a number of requirements are catered to by a hybrid network topology. Under hybrid networks a part of the network operates on a star topology while some sites operate on a mesh topology.

1.8.4 VSAT SPECTRUM

Three ranges of spectrum make up VSAT are shown in table 1.3

Frequency Band	Uplink (GHz)	Downlink (GHz)
C - Band	5.925 - 6.425	3.700 - 4.200
KU - Band	14.000 - 14.500	10.950 - 11.700
Extended C - Band	6.725 - 7.025	4.500- 4.800

Table 1.3 VSAT frequency spectrum

1.8.5 Multiple Accessing Schemes

The primary objective of the VSAT networks is to maximize the use of common satellite and other resources amongst all VSAT sites. The methods by which these networks optimize the use of satellite capacity, and spectrum utilization in a flexible and cost-effective manner are referred to as satellite access schemes. Each of the above topologies is associated with an appropriate satellite access scheme. Good network efficiency depends very much on the multiple accessing schemes. There are many different access techniques tailored to match customer applications. Access techniques including stream, transaction reservation, slotted Aloha and hybrid mechanisms are used and are configurable on a per-port basis, enabling customers to run multiple applications simultaneously. Voice of 5.6 Kbit/s Hughes-proprietary CELP compression as well as voice of 8/16 Kbit/s ADPCM compression schemes, synchronous data of 1.2 to 64 Kbit/s, asynchronous data of up to 19.2 Kbit/s and G3 fax relay are some of the applications.

1.8.6 Components of VSAT Terminal and Hub station

In contrast to the hub station, the remote terminals are much simpler. To minimize total system costs, most of VSAT networks are designed to have a single expensive hub and a large number of much smaller remote terminals.

i. VSAT terminal

Remote terminal consists of several main subsystems which include:

a. **A dish antenna**: generally 0.55 to 2.4 m in diameter (though larger dishes are sometimes required), which can be wall, roof or ground mounted.

b. **An outdoor unit (ODU):** which contains the microwave electronics for the terminal?

This is usually the size of a shoe box, but it may be much smaller. If the ODU is large it is normally supported on the antenna mount behind the dish. Smaller ODUs can be attached directly to the rear of the feed assembly in front of the dish.

In case of Reception the ODU consists of:-

- Band path Filter which passes the wanted signal.
- Low Noise Receiver (LNA) inserts between the antenna and the earth station receiver which pre-amplify the received weak signal.
- Down converter which changes receive frequency before feeding the demodulator into IF signal (70 or 140 MHz) and if a combination of LNA and down converter built into one device attached to the feed this is called Low Noise Block(LNB).

But in case of Transmission the ODU consists of:

- Up converter which changes the 70 or 140 MHz IF to the required transmit frequency before feeding it to the High Power Amplifier (HPA).
- Solid State Power Amplifier (SSPA) is a VLSI solid state device that is gradually replacing Traveling Wave Tubes in satellite communications systems because they are lighter weight and is more reliable, amplifies the up-converted signal before feeding the antenna. Output powers of HPA are usually in the range 0.1–6W (Ku band) and are usually from 2-16W (C-band).

c. **An indoor unit (IDU):** which provides the

- modulation, encoder & multiplexing (in case of transmission),
- demodulation, decoder & demultiplexing (in case of reception)
- Synchronization with the rest of the network and supports the user interfaces.

This box is usually about the size of a domestic video recorder. Remote terminals usually support a wide range of common electrical interfaces such as RS-232, RS-422, V.35, as well as voice and TV. Several common protocols are also generally supported including SDLC, 3270 bisync, X.25, async and Ethernet. **Fig. 1.13** shows VSAT Remote Terminal Block Diagram. Link availability is also usually designed to be high, with an end to end availability of better than 99.7% being quite common.

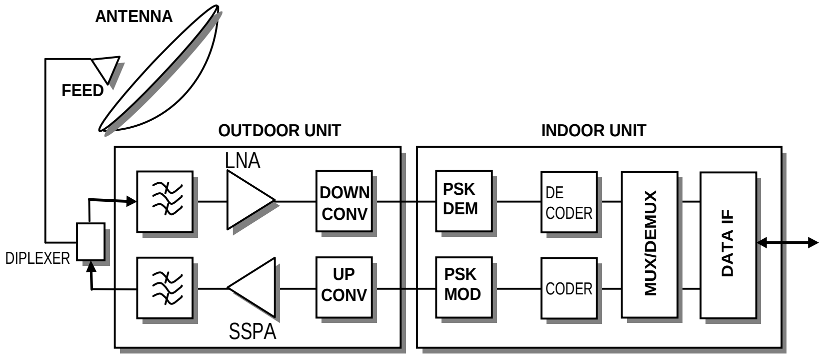


Fig. 1.13 VSAT Remote Terminal Block Diagram

ii. VSAT Hub Station

The hub station consists of several main subsystems as shown in **Fig 1.14**; except for the antenna these are usually fully redundant with automatic switchover in the event of failure:

- A switch (generally a packet switch) which controls routing between host ports and the modulator and demodulator ports, as well as adding and reading header address information which controls routing to and from individual IDUs.
- One or more modulators which modulate the outbound carriers with the stream generated by the switch (each outbound carrier has a dedicated modulator).
- A bank of demodulators which receive the inbound carriers and extract the data packets and feed them to the switch.
- An NCC (network control centre) which controls and monitors the operation of the hub and the IDUs in the network.
- An RFT (radio frequency terminal), which contains:

- The transmit subsystem containing up converters which change the 70 or 140 MHz IF to the required transmit frequency before feeding it to the HPA.
- Uplink power control is often provided so that the power transmitted by the hub can be increased to compensate for high link attenuation due to precipitation in bad weather and can also control the interference.
- The receive subsystem consisting of a LNA and a down converter to change the received frequency to the IF frequency (70 or 140 MHz).
- The antenna subsystem consisting of a large antenna (6 to 9 m in diameter) on a mount with a tracking system which allows the antenna to follow the satellite as it moves very slightly in the sky.

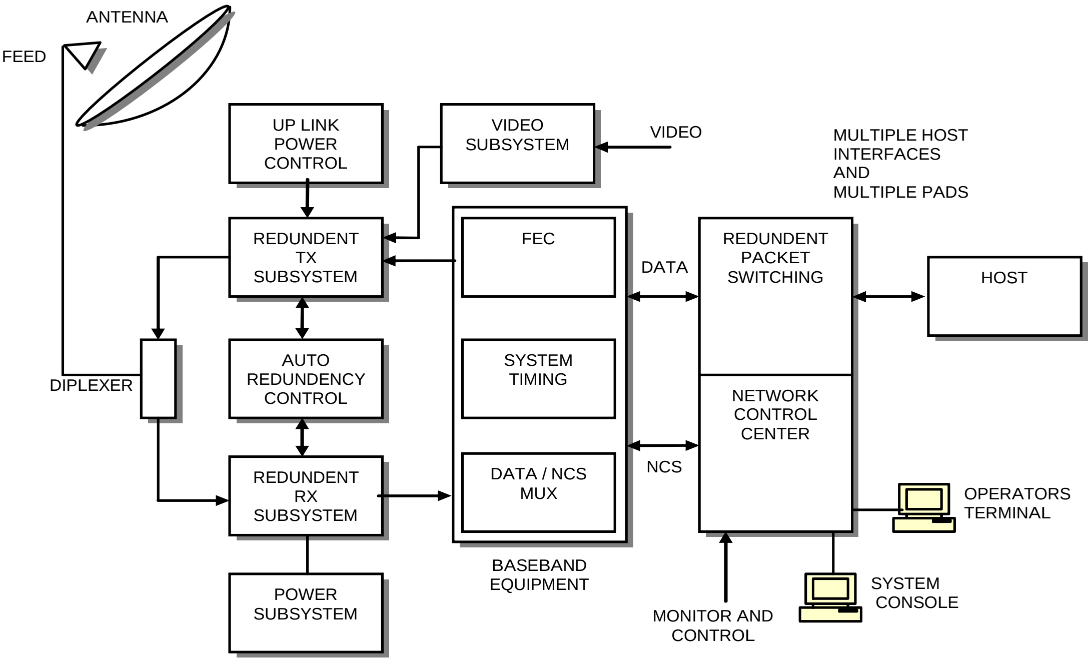


Fig. 1.14 VSAT Hub Station Block Diagram

1.8.7 Space Segment Support

The ideal orbit for a communications satellite is geostationary, or motionless relative to the ground. Satellites used for communications are almost exclusively in the geostationary orbit, located at 36000 km above the equator. In line with ITU stipulations, for avoiding interference, all satellites are placed 2 degree apart. This places a maximum limit of 180 satellites operating in a geostationary orbit.

i. Space segment

Space Segment is available from organizations which have procured satellites, arranged launches and conducted preliminary tests in-orbit and who then operate these satellites on commercial basis.

ii. Transponders

Contained in the satellite body are a number of transponders, or repeaters. These transponders as shown in **Fig 1.15** perform the following functions:

- Signal Reception - it receives the signal uplinked by a VSAT and/or hub

- Frequency Translation - the frequency of the received signal is translated to a different frequency, known as the downlink frequency. The frequency translation ensures that there is no positive feedback and also avoid interference related issues.
- Amplification - the transponder also amplifies the downlink signal

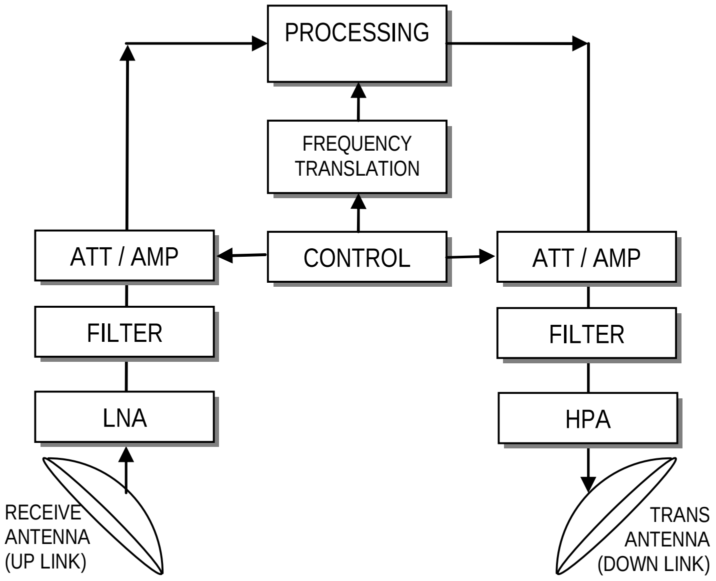


Fig. 1.15 Satellite Anatomy

The number of transponders determines the capacity of a satellite. The INSAT series of satellites have typically 12/18 transponders in various frequency bands. Each transponder typically has a bandwidth of 40 MHz.

1.8.8 VSAT advantages and Drawbacks

i. Advantages

- Great flexibility to accommodate growth and changes;
- Broadcasting and distribution/collection capabilities to/from remote locations;
- Distance insensitive, long haul communications, wide geographic coverage;
- Rapid installation of equipment at the customer’s premises with limited infrastructure and independence from earth networks and infrastructure;
- Better (high) quality of services, very high reliability and high availability (99.9 %) is far better than the availability of ground networks;
- Low maintenance requirements;
- Centralized control and monitoring;
- Large bandwidths allow high traffic speed and density;
- Emergency back-up.

ii. Drawbacks

- Loss of transponder may lead to loss of network; Communication links can be restored by using a spare transponder.
- Propagation delay (using star topology, double hop = 0.5s).

This may prevent the use of voice communications, at least with commercial standards, in a star shaped VSAT network.

Review Questions:

Objective:

1. In coaxial Ethernets, the transmission is

a) Full duplex b) Half duplex c) Simplex d) All

2. Ethernet network will typically be found in configuration
a) Mesh b) Ring c) Bus (or) Star d) Star

3. 10 baseT is implementation on
a) Co-axial cable b) Wire less c) OFC d) UTP / STP

4. The hardware (or) MAC address is burnt on which part of NIC
a) RAM b) ROM c) NVRAM d) Flash

5. A switch controls flow of data using
a) IP address b) Port address c) MAC address d) None of above

6. Routers are used to connect
a) Similar LANs b) Similar WANs c) Different networks d) None of the above

7. The standard complaint & cost effective solution for connecting dumb terminal and thin clients at remote site for PRS – UTS integration is
a) Statmux b) Terminal Server c) DCM d) NeTS

8. Traditional network switch operates at layer
a) One b) Two c) Three d) None of above

Subjective:

1. What are the different media for connectivity in LAN networks? and state the LAN standards presently available?
2. List various network connectivity devices & explain?
3. What is VSAT? Explain the system with a suitable diagram?
4. State why VSAT communication is suitable for Indian Railways network?

CHAPTER-2

RAILNET

2.0 INTRODUCTION:

The interconnection of a large number of data processing devices through suitable communication links enabling data transfer between the data processing devices constitutes a DATA NETWORK. Several data networks are functional over Indian Railways and year by year, rapid expansion of the networks takes place to cover more and more activity centers. The architecture of the networks is also upgraded in a phased manner to keep in tune with the technological developments. Several applications are already operating over the networks and many new applications are contemplated .The various applications are as under:

i. Passenger Reservation System (PRS)
ii. National Train Enquiry System (NTES)
iii. Unreserved Ticketing System (UTS)
iv. Freight Operations Information System (FOIS)
v. Coaching operations Information System (COIS)
vi. Control Office Automation (COA)
vii. Crew Management System (CMS)
viii. Material Management Information System (MMIS)
ix. Management Information System (MIS) which is made up of a large No. of applications for various departments like AFRES (Accounting), PRIME (Personnel) etc.
x The data networks can also be used for other applications like video conferencing, data conferencing, VOIP, IVRS, disaster management, office automation etc.

RAILNET

2.1 AN OVERVIEW

RAILNET is the name of the Corporate Wide Information System (CWIS) of Indian Railways. It is aimed to provide computer connectivity between Railway Board, Zonal Railways, Production units, RDSO, Centralized Training Institutes, CORE, and MTP / Kolkata etc.

2.2 OBJECTIVES

RAILNET has been established with these objectives in mind:

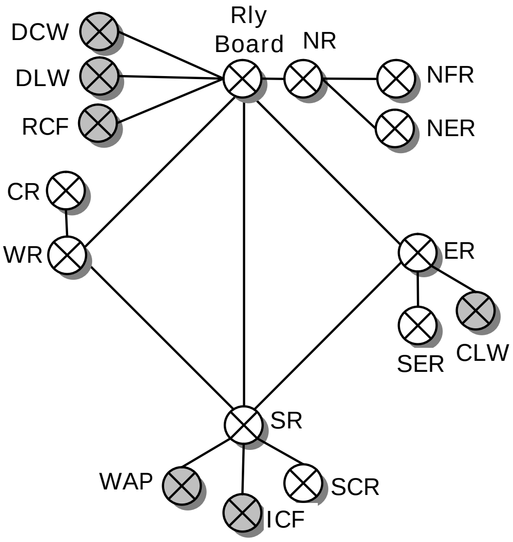
- Eliminate the need to move paper documents between different units and Change from “Periodic Reporting” to “Information on Demand”.
- RAILNET will expedite and facilitate quick and efficient automatic status update between Railway Board and Zonal Railway, as well as between divisions and Zonal Railway.
- Internet gateways have been established at Delhi, Mumbai, Chennai, Kolkatta

2.3 IMPLEMENTATION

Phase I of RAILNET was commissioned by **IRCOT** (Indian Railway Central Organization of Telecom) through a contract agreement with Tata-InfoTech.

The connectivity diagram of RAILNET Phase I is shown in **Fig. 2.2**. This constitutes the backbone of RAILNET. This phase connects the zonal headquarters of WR, ER, SR, NR to the Railway Board. The zonal HQ of SER, NFR, NER, CR and SCR are connected to one of the zonal HQ so as to get connectivity with Railway Board. The production units are also connected to the zones nearest to them so as to get connected with Railway Board.

In the phase II implementation of RAILNET, divisions are connected with their zonal head quarters, all the centralized training institutes i.e. RSC, IRISET, IRICEN, IRIMEE, IRIEEN and Railway organizations RDSO, CORE and METRO Railways are connected to RAILNET from the nearest zonal HQ.



Connectivity by 64Kbps Leased lines
of Railway/BSNL

Fig. 2.3 Phase - 1 implementation of RAILNET

2.4 RAILNET GENERAL ARRANGEMENT:

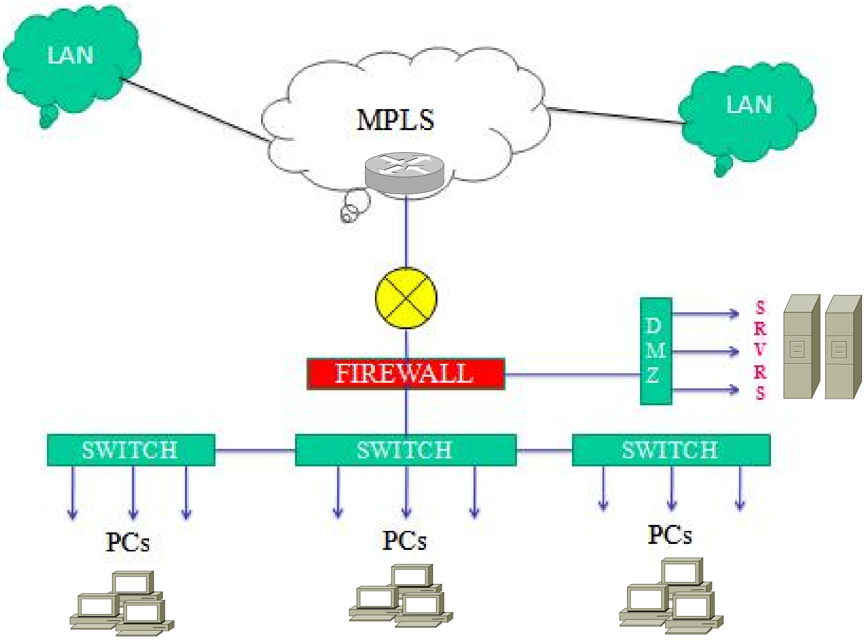


Fig. 2.4 RAILNET general arrangement

The WAN link (or the RAILNET link) terminates at the router. The router in turn is connected to the switch. All the computers including the server is are connected to the switch. Additional hubs/switches may be connected to this switch so as to extend the RAILNET LAN further.

2.5 RAILNET HARDWARE/SOFTWARE DETAILS

RAILNET employs the following hardware components:

- Compaq Server Compaq Proliant 1600R Rack Mounted.
- Cisco Router Cisco 3640 and Cisco 2610.
- Switches Cisco Catalyst 2924 XL with 22 10/100Mbps RJ45 port and 2 FX (optical fibre) ports.
- Modem RAD V.35/64kbps modems.

RAILNET employs the following soft ware on Servers:

- Windows NT Server 4 as the Network OS.
- IIS 4.0 as the Web and FTP Server.
- Lotus notes as a Mail Server.

2.6 IP SCHEME

RAILNET uses the TCP/IP protocols because of the proven strength of these protocols; RAILNET can be easily scaled for Internet as well. There will be no compatibility problem in scaling and the technology will be able to scale well for a large network. RAILNET has used the private IP address of 10.x.0.0/16. The IP addressing scheme is uniform and consistent as shown in table 2.5. As uniform measure all the web servers are given with an IP 10.x.2.19 and Router with an IP 10.x.2.1

RB	10.1.0.0	SWR	10.205.0.0
CR	10.31.0.0	WR	10.3.0.0
ER	10.4.0.0	WCR	10.150.0.0
ECR	10.170.0.0	METRO	10.160.0.0
ECOR	10.180.0.0	WAP	10.52.0.0
NR	10.2.0.0	ICF	10.53.0.0
NCR	10.102.0.0	DCW	10.11.0.0
NER	10.24.0.0	RDSO	10.100.0.0
NFR	10.42.0.0	CORE	10.101.0.0
NWR	10.141.0.0	RSC	10.140.0.0
SR	10.5.0.0	IRICEN	10.152.0.0
SCR	10.51.0.0	IRIEEN	10.151.0.0
SER	10.41.0.0	IRIMEE	10.161.0.0
SECR	10.206.0.0	IRISET	10.195.0.0

Table 2.5 IP scheme of Railnet

2.7 EMAIL ADDRESSING

The entire RAILNET is under a single domain **railnet.gov.in.**The generic email address of RAILNET users will be **user (official designation)**@railway**(code**).railnet.gov.in

Example

- Chairman, Railway Board ⟶ crb@rb.railnet.gov.in
- Director, IRISET ⟶ director@iriset.railnet.gov.in
- CSTE, SCRailway ⟶ cste@scr.railnet.gov.in

2.8 APPLICATIONS

- RAILNET users can exchange emails on the Internet. Commercial Dept. is extensively using RAILNET for their "Complaint Center."
- Railways have launched their web pages and they keep up to date information in these web pages.
- A RAILNET authorized user can browse the Internet through RAILNET.
- A RAILNET user can share resources with a co-user on RAILNET.

2.9 GUIDELINES FOR RAILNET NETWORKs

(Ref: RB letter No. 2000/Tele/TW/1/Railnet works/Pt. New Delhi, dt.30.04.2007)

Railway Board undertook Security and Network Architecture Review & Audit of RAILNET to assess adequacy of present security architecture as well as auditing the configuration and design of network architecture for optimum utilization and efficiency

A Committee consisting of CCE/CR, CCE/WCR, GM/RailTel and Director/Tele was constituted to examine the existing RAILNET architecture on Indian Railways taking into account Security Audit Report, which have been conducted and suggest measures to improve functioning of RAILNET on IR. Based on the Committee's recommendations following broad guidelines are issued:-

There is a need for central monitoring of the RAILNET functioning to ensure

- Uniformity of practices,
- Uniform architecture,
- Central management of e-mail and web-servers and monitoring.

Till a separate organization is set up for this purpose, this job would be undertaken by IRPMU directly under the guidance of Railway Board.

2.9.1 LAN INFRASTRUCTURE

1. All backbone wiring of LAN should be on the fiber which is capable of working on 1GBPS
2. Manageable switches providing higher processing speed needs to be used.
3. Network should be designed in such a way as to provide sufficient redundancy and the concept of V-LAN should be introduced for traffic segregation wherever required
4. There will be four Internet Gateways at Delhi, Mumbai, Kolkata, & Chennai provided by RailTel. The distribution of Zonal Railways which will be served by these Gateways will be as shown in table 2.9.1

Region	Internet GATEWAY	Zonal railways served
Northern	Delhi	NR, NCR, NWR, NER, RDSO, CORE, DLW, RCF
Western	Mumbai	WR, CR, WCR
Eastern	Kolkata	ER, SER, ECR, NFR, ECoR, SECR, CLW
Southern	Chennai	SR, SWR, SCR., ICF, WAP

Table 2.9.1 Railnet gateways

5. To ensure the uniformity of network across IR, It has been decided that

- RAILNET will be setup on MPLS network of RailTel as an MPLS based VPN.
- All the RAILNET locations viz., zonal Railways, Divisions, CTIs, PUs etc. will be connected to the MPLS network of RailTel using 2 MBPS links preferably on Ethernet with a provision of upgrading it in near future.
- Railway Board will be connected to the MPLS network with 10MBPS link to start with.

2.9.2 Typical Layout

The typical layout of network arrangements is as shown in Fig. **2.9.2a & 2.9.2b.** It is designed such a way that the path redundancy is inbuilt in the RAILNET connectivity viz., use of two sets of L3/GBIC switches and two independent routers with 2MB connectivity to lower hierarchy and as well for connecting to the higher hierarchy of the network through RAILTEL MPLS network.

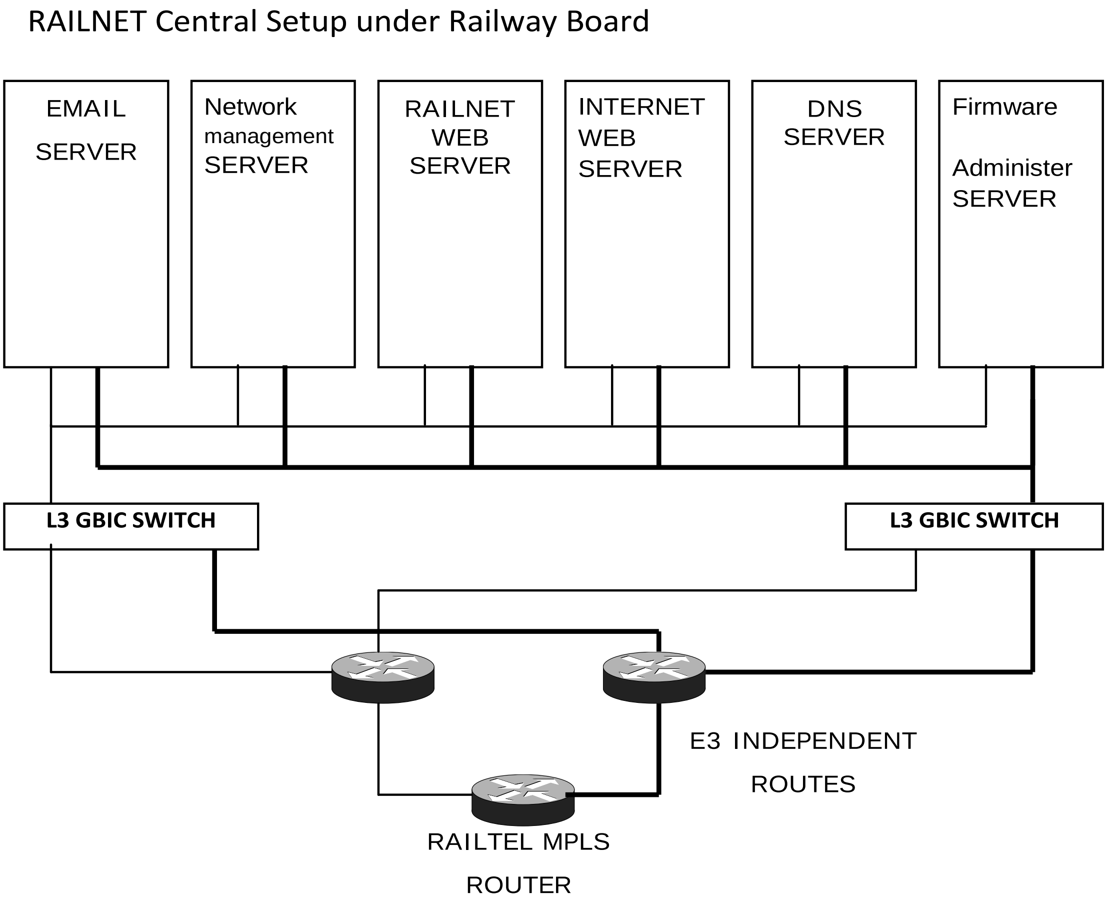


Fig. 2.9.2a RAILNET central setup under Railway Board

Review Questions:

Objective:

1. Railnet is a
   a) Extranet b) Internet c) Intranet d) Piconet

2. A switch controls flow of data using
   a) IP address b) Port address c) MAC address d) None of above

3. IP Addressing scheme for Railnet is
   a) Public b) Private c) Automatic private d) None of the above

4. IP nos. allotted to Web server on Railnet as a uniform measure are
   a) 192.X.2.19 b) 10.x.x.19 c) 10.x.2.19 d) None of the above

5. IP nos. allotted to Router on Railnet as a uniform measure are
   a) 192.X.2.1 b) 10.x.x.1 c) 10.x.2.1 d) None of the above

6. Subnet mask used for Railnet is
   a) 255.0.0.0 b) 255.255.0.0 c) 255.255.255.0 d) None of the above

Subjective:

1. State the objectives of Railnet?

2. Draw and describe the setup of Railnet, required at Zonal Railway Head quarters and at Divisional Railway Head quarters?

3. State the revised guide lines of Railway Board for implementation of Railnet both on LAN & WAN?

CHAPTER-3

FREIGHT OPERATIONS INFORMATION SYSTEM (FOIS)

3.0 INTRODUCTION

Indian Railways have decided not only to perform the traditional tasks of carrying passengers and goods efficiently, but also to change the mindset of working in a closed system. There has been a longstanding demand of the industry for transparency in sharing of information to give the customers an up to date businesslike environment.

Continuous cargo visibility has always been viewed as the most critical component of any physical distribution system. FOIS enables freight customers to have instant access to information regarding the current status of their consignments in transit, for just in time inventory. It is a system for management and control of freight movement that also assists managers to optimize asset utilization.

3.1 SYSTEM COMPONENTS

FOIS comprises the Rake Management System (RMS) for handling the operating portion and Terminal Management System (TMS) pertaining to the commercial transactions. TMS has been installed at more than 300 locations and with the availability of infrastructure will cover all major handling points. As of June 2005, about 1500 reporting devices have been commissioned at more than 500 locations of Indian Railways. Railway owned digital microwave communication facilities complemented by channels hired from the Bharat Sanchar Nigam Ltd., (BSNL) have been used to establish the network. The network is continuously being expanded to meet the growing demand.

3.2 SYSTEM DESIGN

FOIS has been designed to give strategic advantages to both Indian Railways and its customers. The implementation of the system is envisaged to eventually achieve the following:

i. Extension of the current business practice of bulk movement in train, load formation to piecemeal traffic to increase the market share by clubbing and moving together similar type of stock of "Hub & Spoke" arrangement.
ii. Global tracking of consignments in real time, whether in rakes or in individual wagons. The insight and pipeline of consignments would be seamlessly available for timely planning and just in time inventory management.
iii. Facilitate acceptance of customer’s orders, billing and cash accountal from identified nodal customer centers which, may not necessarily be the handling terminals. These facilities could even get extended to customer’s premises and along with introduction of e-commerce benefit both by reducing the burden of logistics management.

3.3 SYSTEM PERFORMANCE

The system as implemented up to now performs the following functions:

i. Monitoring of all freight trains indicating their position in computerized territory and their expected time of arrival at destination.

ii. Commodity wise flow of freight trains for customers like Power Houses, Refineries, Fertilizers and Cement Plants, Steel Depots and Public Freight Terminals enabling the recipients of consignments to have an accurate forecast of cargo arrivals giving them adequate time to complete preparatory arrangement to handle the cargo.

iii. Out bound loaded rakes from the computerized territory are also monitored in the same manner

iv. Full particulars of detachments from block rakes are recorded and updated eliminating chances of wagons getting unconnected or missing.

v. Details of rakes/Wagons in various yards, their phase-wise detention in different terminals, eliminating the need for costly manual documentation and tedious retrieval systems and inaccuracies.

vi. Managerial reports regarding availability of rolling stock, i.e. wagons and locomotives at any instant of time to plan for their most efficient utilization.

3.4 ADVANTAGES

With the use of the system there has been a visible reduction in the anxiety levels mental stress and confusion amongst railway customers and its operating staff. The voluminous and repetitive exchange of data on telephones round the clock has now been reduced and is gradually being replaced by minimum data input. The improved work environment has significantly simplified planning and execution of assigned tasks. The system information is being used to club less than train load consignments from different loading stations. The words of appreciation from bulk customers who are being advised through e-mail the status of their consignments, is a clear indication that the anticipated benefits from FOIS have already begun to accrue to the customers. Interactive web based solutions to give customized reports to Railway Board, Zonal Railways and Divisions.

FOIS provides tremendous opportunities to both the Railways and their customers, to improve existing business practices and consequently reduce the operating costs while enhancing the quality of service. A full fledged Domestic Terminal Management System for CONCOR is already in place.

3.5 E-PAYMENT OF FREIGHT

A pilot project has been implemented for electronic payment of freight for coal booked for Badarpur Power House from collieries on ECR. Originating point intimates electronically the freight charges to the bank (SBI). After receipt of "Successful Transaction" message (electronic confirmation from the bank, confirming the debit from BTPS account) RR is printed at the originating point. It is a synchronous transaction and reply is received within 150 seconds.

3.6 FUTURE APPROACH:

Design & Development of MIS, Data Ware House & Data Mining capabilities: Provision of MIS reports enabling trend analysis, statistical reports, Data Warehousing and thereby enabling Data mining activities are also envisaged in the future.

WEB Enabled reports: It is contemplated to give web access to Railways customers for obtaining information regarding pipeline of their incoming outgoing rakes, details of Closed Circuit rakes and tracking of interplant movement’s transfers.

3.7 FOIS SYSTEM ARCHITECTURE

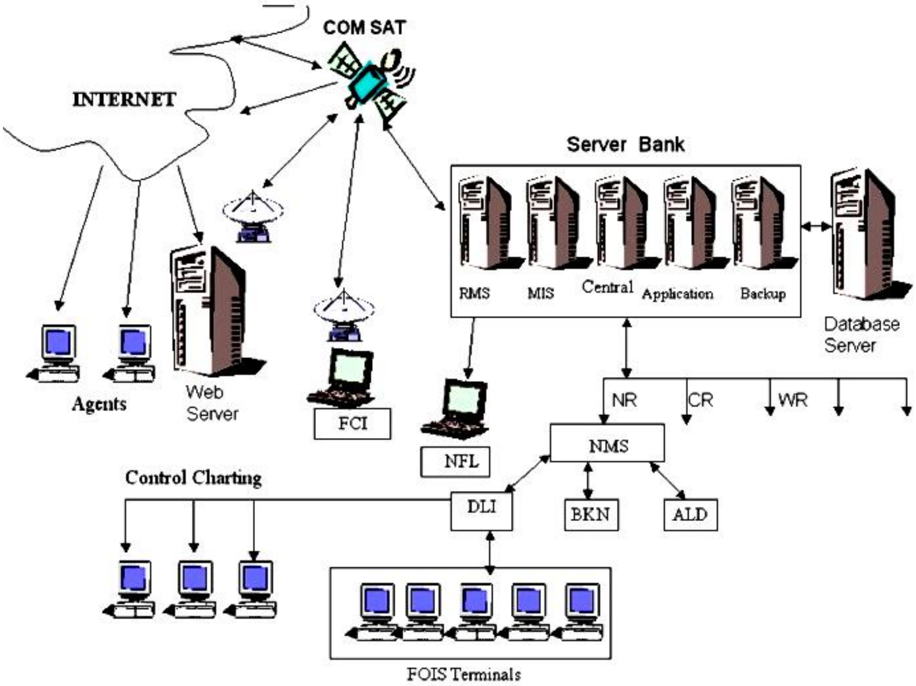


Fig. 3.7 System architecture

Key components of the system architecture as shown in fig 3.7

i. Intelligent terminals will be placed at the field locations to capture the data from the place of activity namely control offices, yards, goods sheds, C & W depot, Loco sheds etc., and connected to the identified Application Server through reliable communication links for transaction processing.

ii. Application servers are centrally placed at CRIS office. These servers are connected to the Zonal Hd. Qrs., Divisional Control Offices, yards, interchange points, and good sheds etc., with a reliable and integrated network. The servers are networked amongst themselves and to the central server for global level transactions.

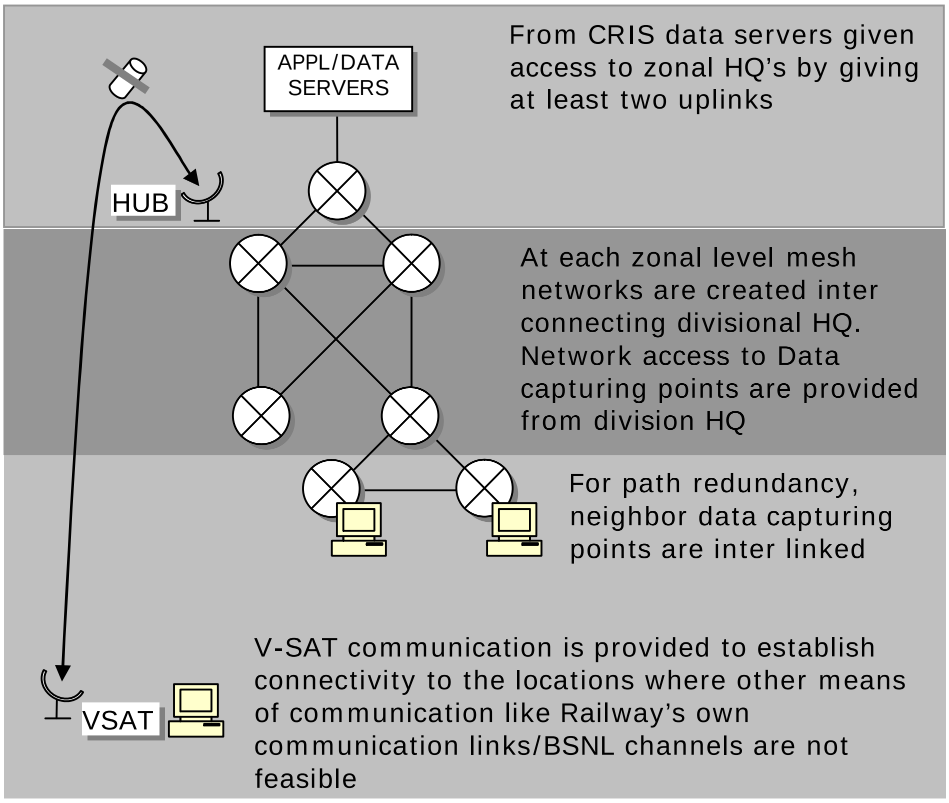
iii. The Central Server provides management Reports at board level and acts as repository of all the global data and also provides global services to maintain referential integrity of the databases including master files.

3.8 NETWORK TOPOLOGY

In view of the Centralized application architecture, a star based network topology has been designed as shown in **Fig. 3.8**. However, in order to provide alternate paths (to meet the up time requirement of 99.9%) from reporting locations, a mesh has been created within each zone so that every location has at least two paths to reach CRIS. Each zonal HQ has been connected to central location (CRIS) on high bandwidth pipes. In addition to this, another zonal location has been connected to CRIS using high capacity link. Hence these two high bandwidth links shall cater to the entire transaction load generated by a zone.

Railway telecommunication network, leased lines, DOT, VSAT Technology as communication media has been provided for reliable and fast means of data transfer.

V-SAT communication is provided to establish connectivity to the locations where other means of communication like Railway’s own communication links/BSNL channels are not feasible.



From CRIS data servers given access to zonal HQ's by giving at least two uplinks

At each zonal level mesh networks are created inter connecting divisional HQ. Network access to Data capturing points are provided from division HQ

For path redundancy, neighbor data capturing points are inter linked

V-SAT communication is provided to establish connectivity to the locations where other means of communication like Railway's own communication links/BSNL channels are not feasible

Fig. 3.8 FOIS network topology

Back bone connectivity

Back bone connectivity of FOIS in initial phase is as shown in the **Fig. 3.8a** subsequently after formation of new zones; the proposed backbone connectivity network is as shown in **Fig. 3.8b**

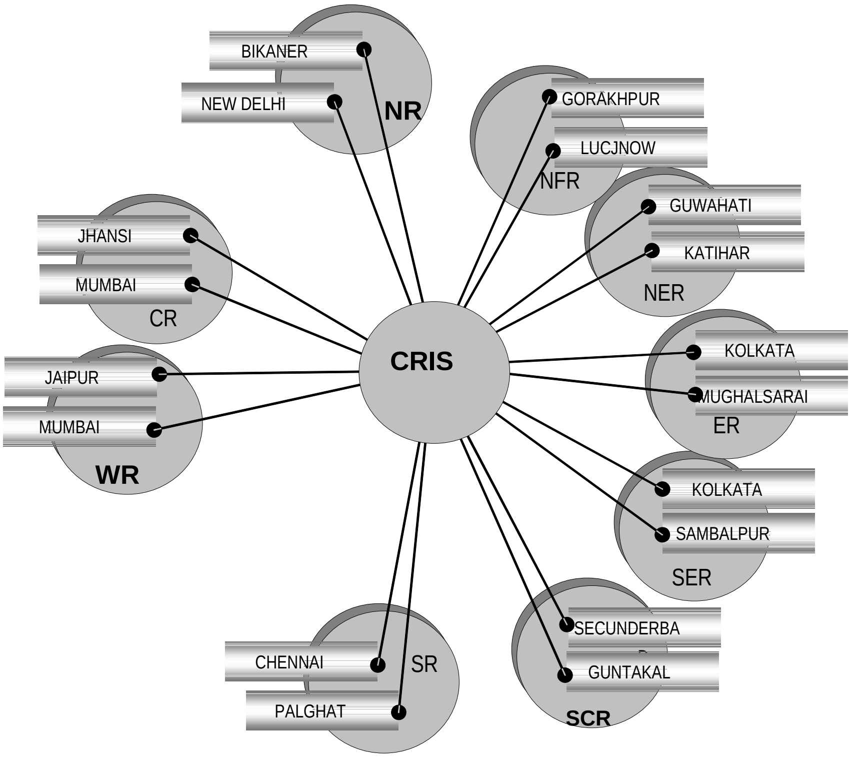


Fig. 3.8a Backbone connectivity of FOIS network with 64Kbps links (Initial phase)

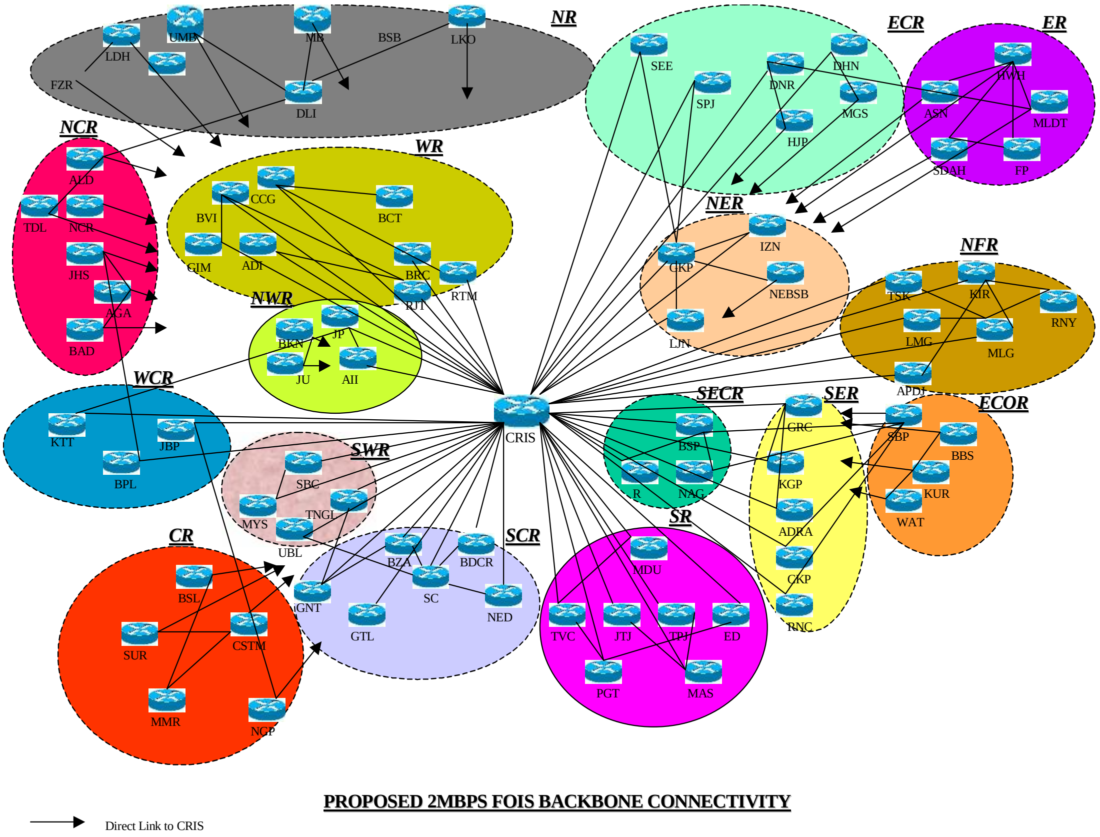


Fig. 3.8b Proposed 2Mbps FOIS backbone connectivity

Review Questions:

Objective:

1. FOIS network is for

   a. Rack management system b. Terminal management system
   c. RR generation d. All the above

2. Architecture of FOIS network is based on

   a. Star topology b. Mesh topology
   c. Mixed (Star + Mesh) d.None of the above

3. Applications on FOIS network on

   a. Master – Slave mode b. Main frame mode
   c. Client – Server mode d. All of the above

4. Back bone connectivity of FOIS network is on

   a. VSAT links b. 64 Kbps data lines
   c. 2 Mbps data lines d. All of the above

5. Application Servers of FOIS are located at

   a. Divisional Hq. b. Zonal Hq c. Rly Board d. CRIS / NDLS

Subjective:

1. State the objectives of FOIS and its advantage for Railways?
2. Discuss with diagram FOIS system architecture and its network topology?

CHAPTER-4

PASSENGER RESERVATION SYSTEM (PRS)

4.0 Introduction

Indian Railways is the world's second-largest railway, with 6,853 stations, 63,028 kilometers of track, 37,840 passenger coaches and 2,22,147 freight cars. Annually it carries some 4.83 billion passengers and 492 million tons of freight.

Of the 11 million passengers who climb aboard one of 8,520 trains each day, about 5,50,000 have reserved accommodations. Their journeys can start in any part of India and end in any other part, with travel times as long as 48 hours and distances up to several thousand kilometers. The challenge is to provide a reservation system that can support such a huge scale of operations regardless of whether it's measured by kilometers, passenger numbers, routing complexity, or simply the sheer scale of India.

PRS started in 1985 as a pilot project in New Delhi. The avowed objective was to provide reserved accommodation on any train from any counter, preparation of train charts and accountal of the money collected. When initial pilot project was implemented at Delhi, the software (referred to as version I) had a number of limitations. These were mainly removed in next version i.e. version II implemented in in 1987.With the addition of new locations and many redefinitions needed the new version III evolved in 1990.Even the version III of the earlier software called **IMPRESS** fell far short of the growing expectations of the travelling public and the need was felt to have a software which has the capabilities of providing the Networking of the five independent PRS nodes namely Secunderabad, Delhi, Calcutta, Mumbai and Chennai. On 18th April 1999, with the networking of Chennai PRS, all the five PRS namely Secunderabad, New Delhi, Kolkata, Mumbai and Chennai were finally networked together.

Now anywhere to anywhere reserved ticketing became a possibility on any PRS booking terminal. In order to facilitate the availability, PNR status and other journey planning information to the common public various interfaces like the Interactive Voice Response System (IVRS) on the telephone, Touch Screens at selective locations, RAPID, DISPLAY, Passenger Operated Enquiry Terminals (POET) and Daily Press Availability Reports through newspapers have been provided.

4.1 CONCERT

COUNTRY-WIDE NETWORK FOR COMPUTERIZED ENHANCED RESERVATION AND TICKETING (CONCERT) developed by ***CRIS, Chanakya Puri, New Delhi***, is a total networking solution to Indian Railways Passenger Reservation System. Indian Railways computerized Passenger Reservation System (PRS) currently operates from five regional centers located at Delhi, Bombay, Calcutta, Madras and Secunderabad.

All of the five sites have been internet-worked using routers, on leased communication line connections from Railtel (RCIL) and Department of Telecom (DOT) as shown in **fig 4.1.** Thus PRS network of the Indian Railways will enable reservations in any train, date, or class, between any pair of stations to the travelling public on about 2000 terminals across the country.

Under the network environment it is proposed to provide "Universal Terminals". Universal Terminals are those from where any reservation activity on network can be done transparently.

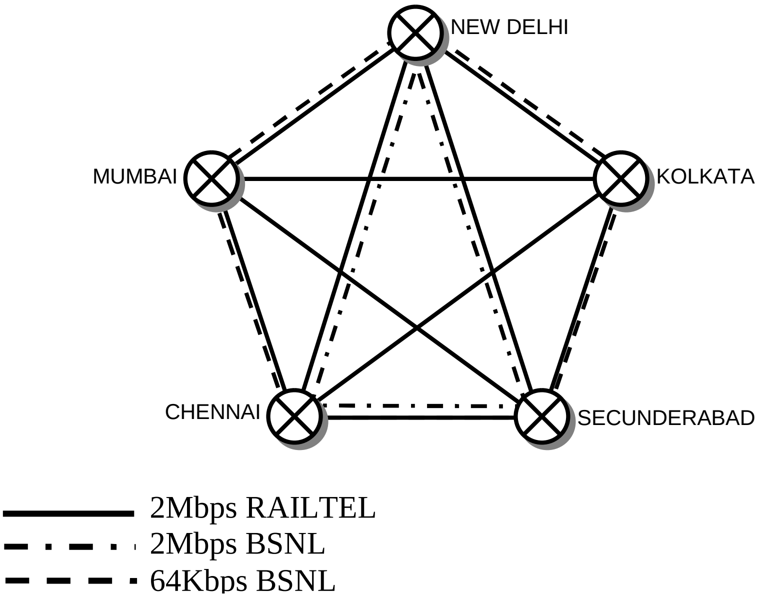


Fig. 4.1 Intra PRS connectivity - CONCERT

The entire CONCERT application since its inception had been hosted on 5 VAX-VMS clusters located at the five PRS sites New Delhi, Mumbai, Kolkata, Chennai and Secunderabad. With the tremendous growth of PRS terminals all over the country and the extra load of various interface software such as Internet enquiries, the overall load on the backend PRS system had increased manifold. A need was felt to move the existing application from the VAX-VMS servers to Alpha VMS servers.

The new On-line Passenger Reservation System -CONCERT - developed using client-server model for distributed computing is a total solution to the networking of the PRSs.

4.2 Typical arrangement of Terminals

PRS Terminals are dumb terminals or thin clients. The connectivity to the server is on Ethernet to Terminal servers. Terminal server is a network terminal switch for Ethernet Local Area Networks, providing a convenient method to logically connect up to eight or sixteen DIGITAL asynchronous terminals to one or more service nodes (hosts) on an Ethernet. The client terminals connectivity to PRS Center is illustrated in **Fig 4.2**

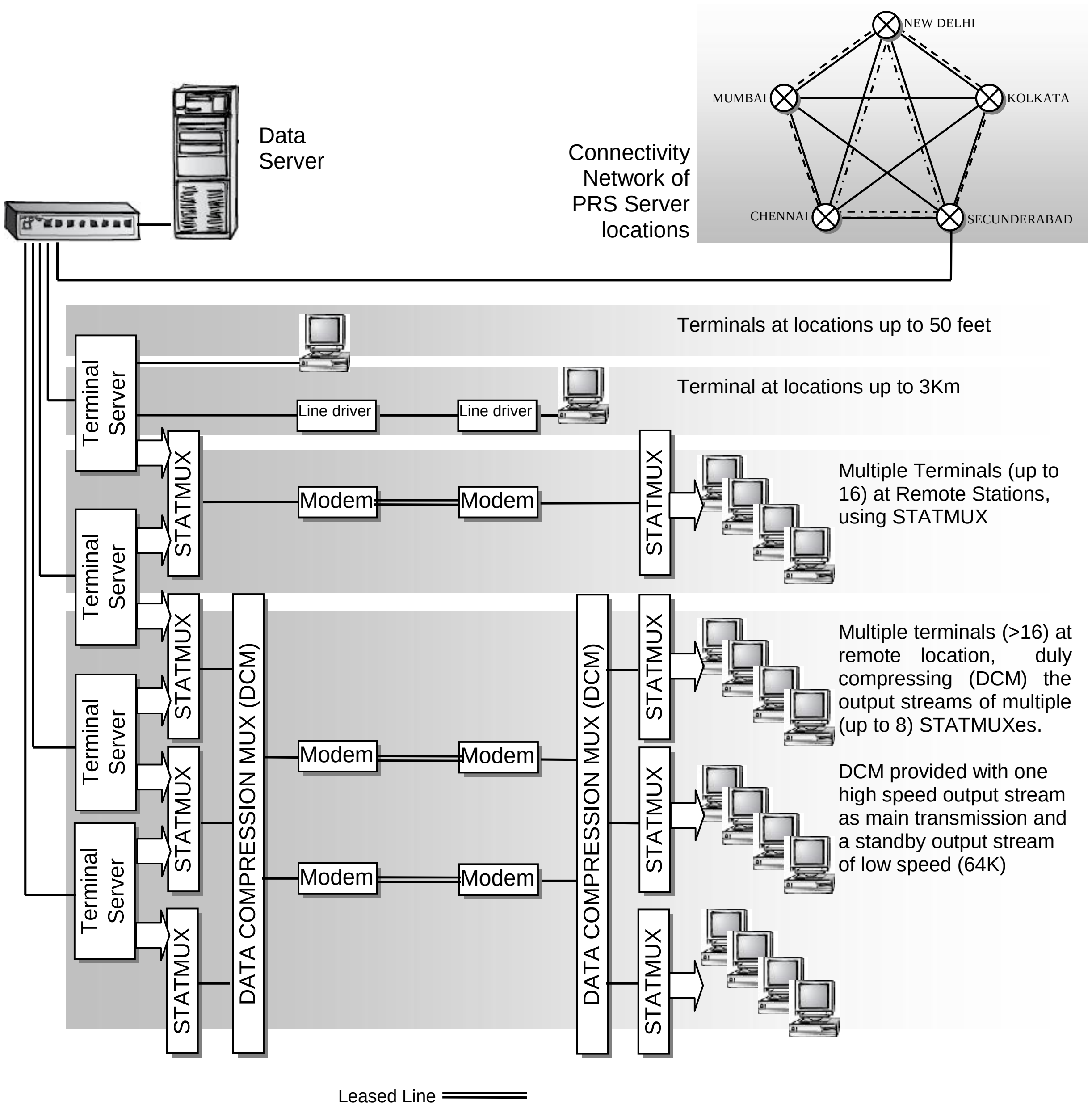

NEW DELHI
MUMBAI
KOLKATA
CHENNAI
SECUNDERABAD
Data Server
Connectivity Network of PRS Server locations
Terminal Server
Terminal Server
Terminal Server
Terminal Server
Terminals at locations up to 50 feet
Terminal at locations up to 3Km
Line driver
Line driver
STATMUX
Modem
Modem
Multiple Terminals (up to 16) at Remote Stations, using STATMUX
DATA COMPRESSION MUX (DCM)
DATA COMPRESSION MUX (DCM)
Multiple terminals (>16) at remote location, duly compressing (DCM) the output streams of multiple (up to 8) STATMUXes.
DCM provided with one high speed output stream as main transmission and a standby output stream of low speed (64K)
Leased Line

Fig. 4.2 Typical arrangement of PRS terminals

Case 1: Client Terminals are derived from the output of Terminal servers and can operate up to a distance of 50 feet.

Case 2: If the Distance is greater than 50 feet line drivers are used to extend the connectivity up to 3 Kms.

Case 3: For extending multiple number of client terminals, the asynchronous output of Terminal server are multiplexed through STATMUX. The composite output signal is driven through leased lines for remote locations

Case 4: For Extending multiple number of Composite output of Stat Muxes to a major location or a hub location, the composite output derived are compressed using Data compression Multiplexer (DCM) (up to 8 composite inputs) and driven through leased lines. DCMs are provided with a Primary compressed output to transfer over high speed data links (2Mbps) and a redundant secondary port to drive over low speed network (64Kbps) during primary path failure.

Review Questions:

Objective:

1. The additional services provided through PRS network are

a) IVRS b) POET c) Rapid display d) All the above

2. CONCERT stands for ---

3. The PRS network is operated through ------------------ nos. of regional centers.

Subjective:

1. Draw and explain about a PRS site, suitably connecting it to PRS network?

2. State the function of Statmux, Terminal server & Network terminal server?

3. What are the benefits of using Network terminal servers?

CHAPTER-5

UNRESERVED TICKETING SYSTEM (UTS)

5.0 OBJECTIVE

More than 1.2 crore Rail passengers travel in unreserved coaches every day and thus form the bulk of rail users. For this category of passengers Railways have introduced the facility of Computerized Unreserved Ticketing System was initially provided at 10 stations of Delhi area in the first stage as a pilot project on 15 August 2002. Another 13 stations of Delhi area were provided with UTS counters in the second stage on 2nd Oct, 2002. It has since been extended in an integrated manner to more than 180 stations all over the country. UTS system has been planned to take over the Printed Card Tickets or tickets issued by self Printing Ticket Machines gradually.

UTS will provide the facility to purchase Unreserved Ticket 3 days in advance of the date of journey. A passenger can buy a ticket for any destination from the UTS counter for all such destinations which are served by that station. The cancellation of tickets has also been simplified. Passengers can cancel their tickets one day in advance of the journey from any station provided with a UTS counter. On the day of journey, the ticket can be cancelled from station from which the journey was to commence.

5.1 ADVANTAGES OF UNRESERVED TICKETING SYSTEM

- Reduced queue length
- Enable advance planning of unreserved journey also
- Reduced crowds at booking offices and stations, making ticket purchase more comfortable
- Allow Indian Railways to plan extra trains and coaches as per trend of sales registered in the system.
- Unreserved itinerary planning possible, tickets available from any station to any station.
- Unreserved ticketing constitutes major component of the overall ticketing in Indian Railways. It contributes a large amount of earning for Indian Railways.

5.2 UTS NETWORK INFRASTRUCTURE

UTS is the complete solution to provide computerized unreserved tickets to railway passengers from dedicated counter terminals, hand held terminals, smart card, automatic vending machines etc. The backend architecture is 3 tiered. The 4th tier will consist of ticketing terminals (dumb, Win terms), ATM m/c, Hand held terminals.

UTS Application is dividing into two parts front-end and back-end. Front-end is developed using C++ on UNIX platform and the backend is Sybase, which is used to store information generated at, front-end and supply input value. Application is dividing into modules like ticketing subsystem, fare and UDM & TDM.

5.2.1 Communication Interfaces

Connectivity between Station servers and Zonal servers as well as between Zonal server and Central server is over WAN. Terminal connectivity is over LAN. TCP/IP is used as network protocol. Preferably, RAIL Tel is going to provide Bandwidth. The Station server is connected to Zonal server by 64 kbps line. For Inter Zone connectivity existing PRS channels would be used.

Review Questions:

Objective:

1. UTS stands for ____ .

2. UTS is a complete solution for providing computerized tickets through

   a. Dedicated counter terminals
   b. Smart card
   c. Automatic vending machines
   d. All the above

3. The back end architecture of UTS network is ______________ tire system.

Subjective:

1. State the advantages of UTS network?

2. Draw & explain the architecture of UTS network tier wise?

CHAPTER-6

UNIFICATION OF PRS AND UTS

6.0 Object

The object of network is designed in such a way so that the PRS application & UTS application can be benefited from each other in terms of reliability and recurring cost optimization through efficient uses of network resources.

Single terminal runs PRS as well as UTS applications as TWO separate sessions. Hot keys for switching sessions and Separate Ticket Printers for PRS & UTS connected to the parallel (LPT) and serial (RS-232) port respectively or both the printers can be connected through APS (Automatic Printer Switch).

6.1 NETWORK ARCHITECTURE

i. It's a 4 tier architecture (refer **Fig. 6.2a** and **6.2b**)

- Tier-1 is the zonal server
- Tier-2 is the divisional hub centers
- Tier-3 is Locations
- Tier-4 is the Terminals

ii. Each individual zone will form as a single autonomous system (AS) of OSPF ROUTING DOMAIN

iii. OSPF AREA 0 shall be limited with in Central data center and the Routers in Area 0 act as AREA BORDER ROUTER (ABR) for all the remaining AREAs.

iv. The remaining network is divided into different AREAs i.e. Division wise.

v. The number of locations that can be configured in an AREA depends on many factors such as media stability and processing capabilities of Router etc. On the basis of past experience **it shall not exceed 70 locations per AREA**. Hence each division depending on number of locations can be divided into more AREAs.

vi. **Each OSPF area shall have at least two tier-2 locations**, so that there are adequate uplinks available to upper tier location. It is however desirable to have more than two tier-2 locations in one area provided the number of tier-2 locations in an Area is confined to 4-5% of the total location within the Area.

vii. No communication channel shall traverse two different OSPF Areas to ensure acceptable Route convergence time i.e. time required to utilize the alternate path in the event of primary path failure and scalability in Network.

viii. The stations below tier-1 location shall be networked by using mix of 'inverted tree' and 'partial mesh' topology.

ix. Each location shall be provided with a minimum of one alternate path to reach central data center location.

x. To the extent possible, the two links providing the primary and the secondary path for a given location build using channels provided by different service providers (service provider diversity).

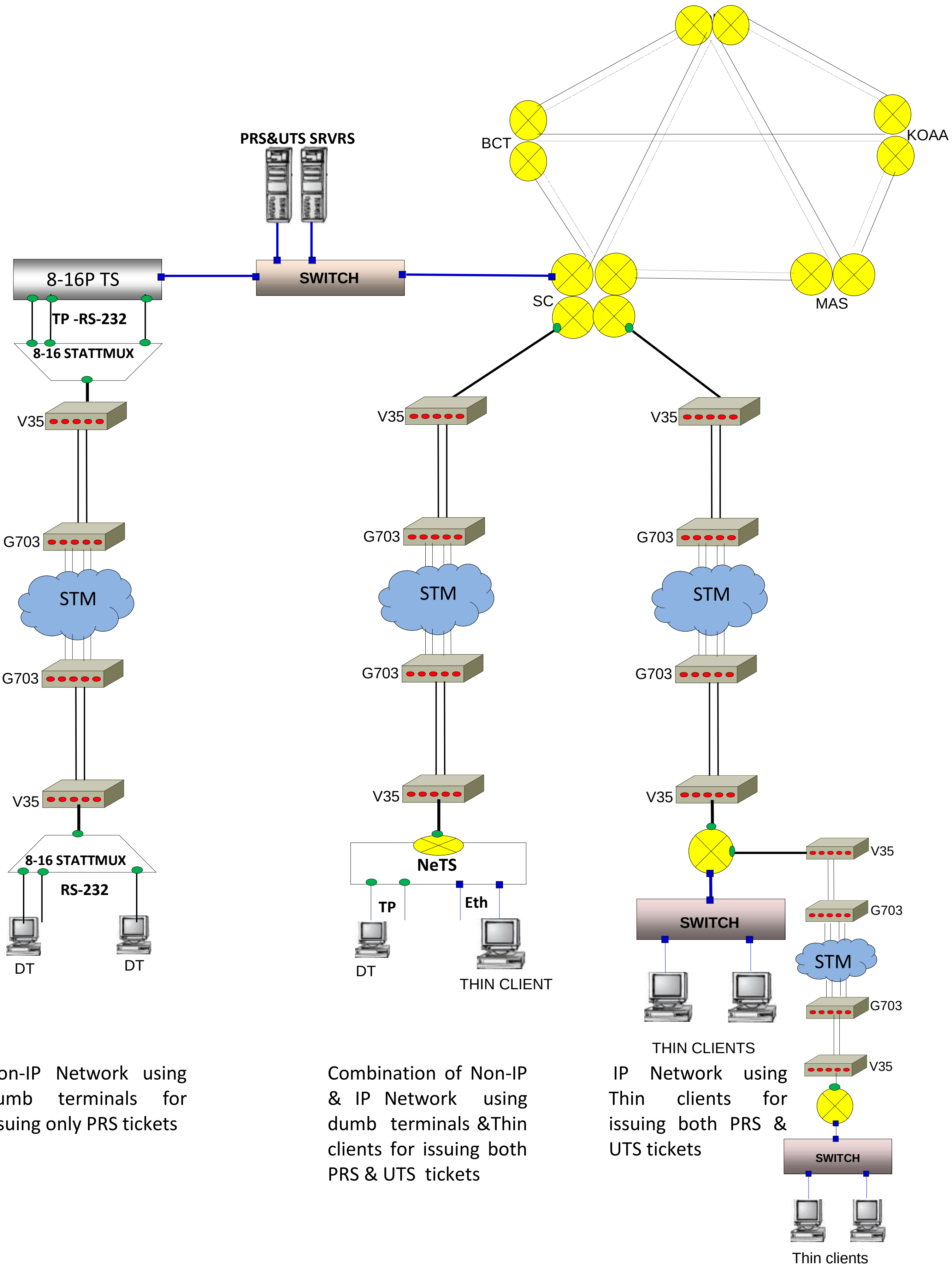
xi. Maximum number of hops between booking location and central location for primary and alternate (secondary) path shall be limited to 4 and 5 respectively such that, not to exceed the comfortable level of 'Round Trip Time' (RTT) between client terminal and Server (130-150m.secs) for smooth operations.

xii. The network **shall utilize SDH based communications channels** only to take the advantage of inherent feature of SDH networks ring protection of SDH links. While configuring communication channel ring protection is available at the physical/media level in the service providers network shall be kept in view.

xiii. In the network below the Tier-1 level, communication channels be built using 2Mbps preferably on Railway owned OFC networks. However, channels hired from BSNL or other service providers may be of 64Kbps.

6.2 Design of Network:

(Unified PRS and UTS networks connectivity diagram)



Non-IP Network using dumb terminals for issuing only PRS tickets

Combination of Non-IP & IP Network using dumb terminals &Thin clients for issuing both PRS & UTS tickets

IP Network using Thin clients for issuing both PRS & UTS tickets

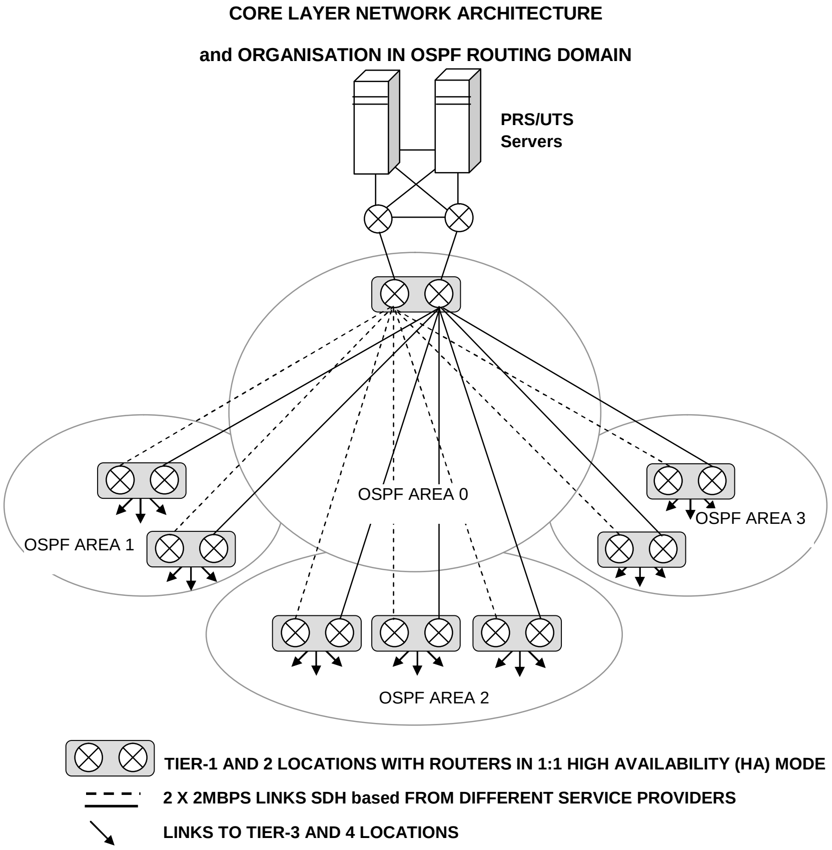

CORE LAYER NETWORK ARCHITECTURE
and ORGANISATION IN OSPF ROUTING DOMAIN
PRS/UTS
Servers
OSPF AREA 0
OSPF AREA 1
OSPF AREA 3
OSPF AREA 2
TIER-1 AND 2 LOCATIONS WITH ROUTERS IN 1:1 HIGH AVAILABILITY (HA) MODE
2 X 2MBPS LINKS SDH based FROM DIFFERENT SERVICE PROVIDERS
LINKS TO TIER-3 AND 4 LOCATIONS

Fig. 6.2a Core Layer network architecture and OSPF routing domain

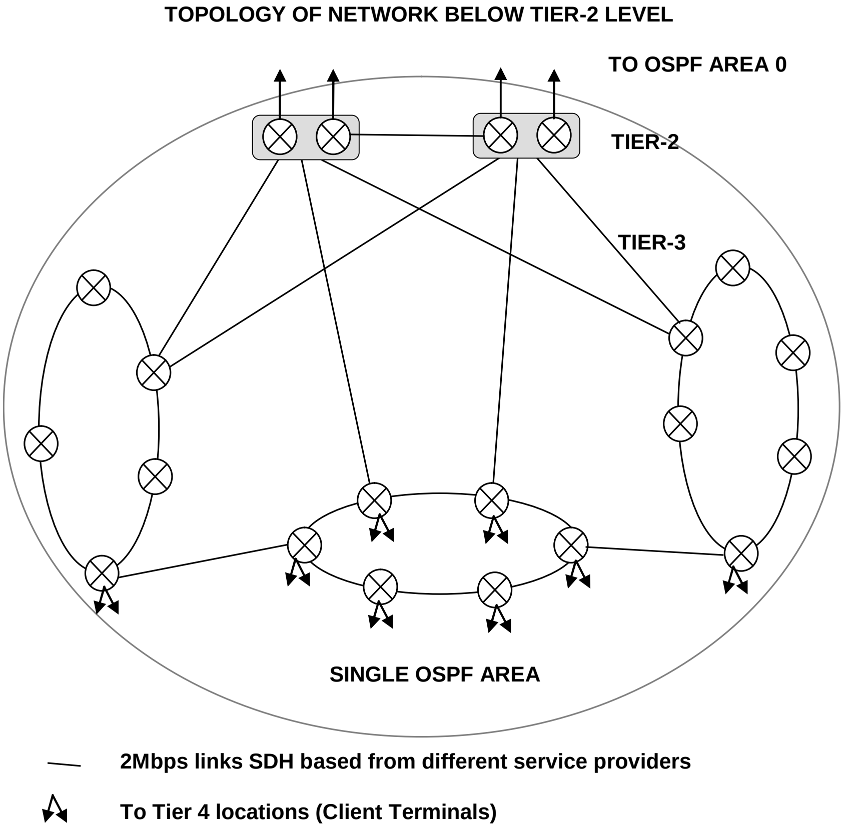
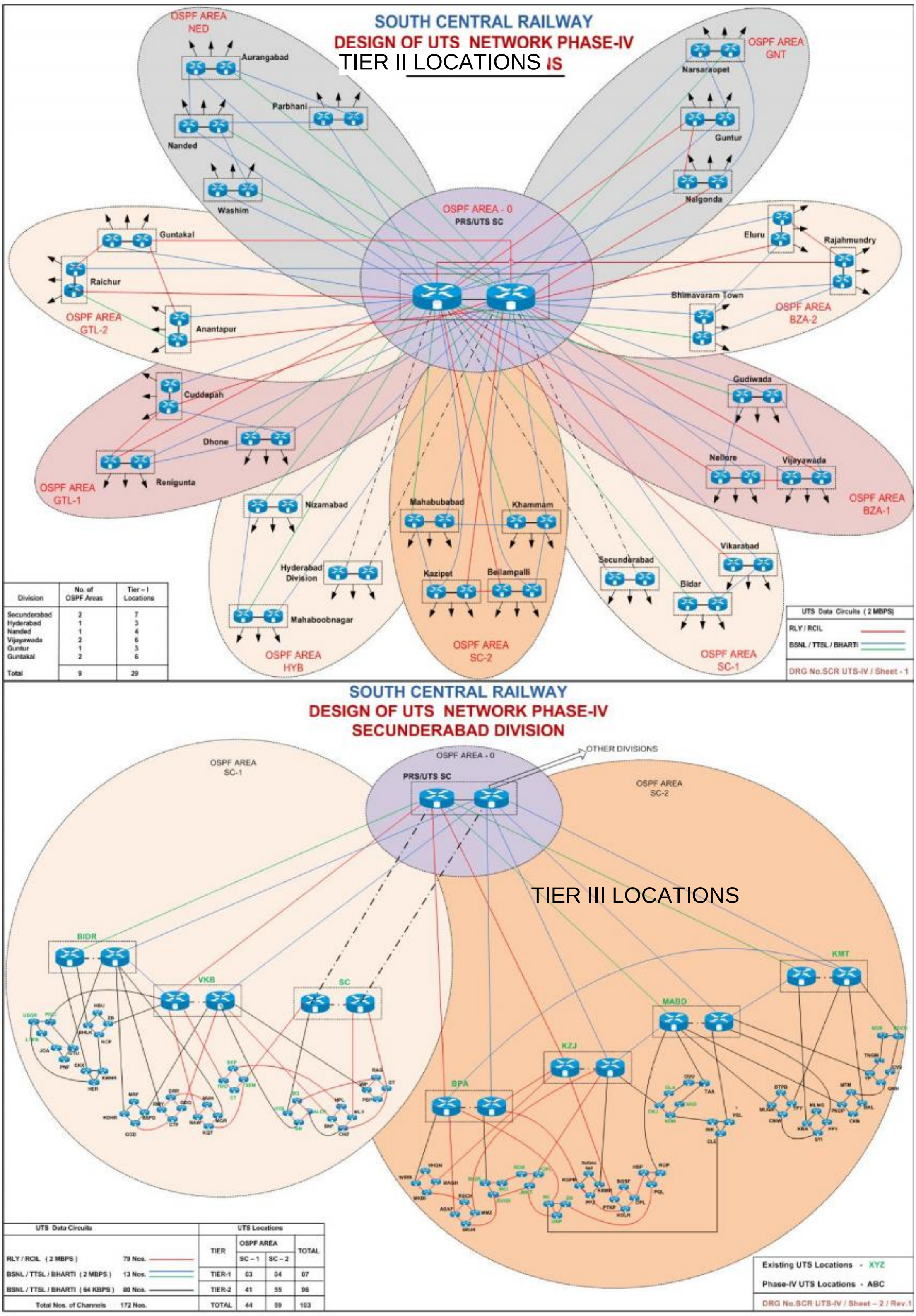

TOPOLOGY OF NETWORK BELOW TIER-2 LEVEL
TO OSPF AREA 0
TIER-2
TIER-3
SINGLE OSPF AREA
2Mbps links SDH based from different service providers
To Tier 4 locations (Client Terminals)

Fig. 6.2b Topology of Network below Tier-2 level

6.2.2 Typical example of PRS & UTS unification

Implementation of phase-4 for tier 2 & tier 3 locations of PRS & UTS unification setup at Secundrabad Division SC Railway is shown in fig 6.2.2



Division	No. of OSPF Areas	Tier – I Locations
Secunderabad	2	7
Hyderabad	1	3
Nanded	1	4
Vijayawada	2	6
Guntur	1	3
Guntakal	2	6
Total	9	29

UTS Data Circuits (2 MBPS)	
RLY / RCIL	🟥
BSNL / TTSL / BHARTI	🟦 🟩

DRG No.SCR UTS-IV / Sheet - 1

UTS Data Circuits		
RLY / RCIL (2 MBPS)	79 Nos.	🟥
BSNL / TTSL / BHARTI (2 MBPS)	13 Nos.	🟦 🟩
BSNL / TTSL / BHARTI (64 KBPS)	80 Nos.	▬
Total Nos. of Channels	172 Nos.	

UTS Locations			
TIER	OSPF AREA		TOTAL
	SC – 1	SC – 2	
TIER-1	03	04	07
TIER-2	41	55	96
TOTAL	44	59	103

Fig 6.2.2 PRS & UTS unification network (phase IV) at Secunderabad division of S C Railway

Review Questions:

Objective:

1. The Dynamic protocol used for unification of PRS & UTS is
   a) RIP b) OSPF c IGRP d) None of the above

2. The round trip time for smooth working between client terminal and server is
   a) 20 - 40m sec b) 60 – 80 m sec c) 100 – 110 m sec d) 130 – 150 m sec

3. Tier 2 location in an area shall be limited to ------------% of total area

4. Ring protected ------------------- based communication channels are required for path reliability.

5. Number of locations per area shall not exceed
   a) 30 b) 50 c) 70 d) 60

6. Topology used for PRS & UTS unification is
   a) Inverted Tree b) Partial Mesh c) Mesh d) Combination of a & b

Subjective:

1. State the objectives of PRS & UTS unification?

2. State the guidelines for unification of PRS & UTS in its network architecture?

3. State about the topologies required at different levels in PRS & UTS unification?

CHAPTER-7

MAINTENANCE AND TROUBLE SHOOTING PROCEDURES

7.1 FAULT DIAGNOSIS OF DATA NETWORKS (As per telecom manual):

The fault diagnosis is categorized into three

- Hardware
- Software
- Media/Channel

The datacom equipment is provided with visual indications by which the status of the equipment can be known. The next option is by login into the equipment and test the equipment with standard commands given by the manufacturer.

The software part like IOS of Routers and other intelligent/managed equipment can be checked or upgraded to higher versions depending on the type of the fault encountered.

The media which actually connects two locations through interface device can be checked with testing facility given on the interface device or through measuring instruments. The BER of the media/channel is generally measured to know the percentage of errors and other related information.

7.1.1 GENERAL MAINTENANCE

- The datacom equipment shall be kept clean and tidy without dust and shall be cleaned daily.
- The diversity channels shall be checked by switching of main channels and ensure that automatic switch over/routing is taking place.
- In case ISDN link is provided as backup to the main link, the connectivity of ISDN shall be checked by switching off main link. The voltage of ISDN channels to be measured at datacom equipment input termination and to be maintained with the standards.
- Condition of underground cables to be checked by carrying out routine checks done for U/G cables.
- OFC cables and connectors to be checked as per routine checks done on OFC.
- The Antivirus patches to be updated in NMS system time to time.
- The Datacom equipments shall be provided specified value of less than 1 Ohm earth resistance for reliable working of Datacom equipments and for protection from lightening and surges
- Ensure Un-interrupted Power supply, preferably with two UPS, to increase the life of the equipment as well as to keep up the availability of the location/node.
- The datacom equipment shall be installed in **n x U** size racks of required size and less than one ohm earth shall be provided
- In addition to the above, any other checks suggested by manufacturers

7.1.2 Do's and Don'ts

Do's

i. Do write the configurations changes if any done in a register so that proper documentation is done for performance analysis and recodes purpose.
ii. Take the print outs of the configuration of the routers and document them.
iii. Store the configuration files of the routers in softcopy so that they will be useful at emergency whereby with one command entire configuration can be copied thereby reducing the down time.
iv. Do proper lacing of the internal wiring,
v. Protect the cables form rodents where cabling is done through false flooring.
vi. Train the staff and update the knowledge to maintain the network more efficiently.
vii. Use ESD wrist bands while handling datacom equipments
viii. Use a good quality earth and maintain the earth resistance below 1 Ohms
ix. Change the password of router/servers once in a month
x. Take backup of the router configuration every time the configuration is changed.
This will help in faster restoration in the event of software error/Flash failure.
xi. Follow the housekeeping procedure of clearing the event and performance logs of the NMS at specified intervals.
xii. Plan replacement of UPS batteries as per the specified lifecycle.
xiii. Keep the operation and maintenance manual handy.
xiv. Check the backup links at least once a week.

Don't's

i. Do not change the hardware of the routers like data cards when the router power supply is ON unless it is clearly mentioned that it supports hot swapping.
ii. Do not change the V.35 Data cable when the router and modems are ON.
iii. Do not change the IP addressing scheme and IP address of the working network without the written permission of the Network Administrator.
iv. Do not change the configuration of the router without the permission of the Network administrator.
v. Do not run down the batteries of the UPS below specified level.
vi. Never switch off the datacom equipment without following the proper shut down procedure
vii Do not share the passwords of router's and servers with your colleagues.
viii. Never use water to clean the equipment room.
ix. Don't use water based fire extinguishers for datacom installations.

7.2 TROUBLE SHOOTING OF COMPUTER NETWORKS

The following step by step procedures can be performed for trouble shooting user's computer network connection after noticing that user system is out of network or performance is poor.

- Check whether local area connection icon is available or disabled or cross marked through network connection option in control panel.
- Check if yellow exclamatory mark appeared on network card in device manager
- Check for LED indications on RJ45 port of NIC card (back side of the PC)
- Check whether your system is assigned a valid IP addresses and subnet mask of your network.
- Check for DHCP issues if your IP address appears as 169.254.x.x (APIPA)
- Ping 127.0.0.1 for checking software integrity (i.e. TCP/IP protocol suit in your PC)

  ```
  C:\>ping 127.0.0.1
  ```
- Check whether appropriate services are running on that system. (DNS client, DHCP etc.)
- Check your windows firewall / antivirus software is properly configured
- Ping any IP address of your network preferably your gateway IP address.

  e.g. C:\>ping 10.195.2.2
- Use **tracert** command with destination ip address or URL to check further where packets are being dropped in a internetwork before reaching destination.

  e.g. C:\ >tracert www.iriset.indianrailways.gov.in
- Ping destination address continuously or pre-defined number of times to observe consistency between you and your destination. e.g.

  ```
  C:\>ping 10.195.2.2          (default 4 times only)
  C:\>ping 10.195.2.2 –t       (continuously)
  C:\>ping 10.195.2.2 -n 50    (pre-defined times-50)
  ```
- Check the delay time (RTT) and breaks if any by increasing the packet size to estimate link reliability and bandwidth issues when pinging.

  ```
  C:\>ping 10.195.2.19 -l 1000   (Max 65500 bytes and default 32 bytes)
  ```
- Ping the destination with increased packet size and pre-defined number of times in one go. e.g. C:\>ping 10.195.2.19 -l 1000 -n 50 (pings 50 times with 1000 bytes packet)

CHAPTER-8

DATA LOGGERS

8.0 INTRODUCTION:

A **data logger** (**data recorder**) is an electronic device that records data over time and data logging is the measuring and recording of physical or electrical parameters over a period of time.

Data loggers are used in a variety of applications such as in-vehicle data logging, environmental monitoring, structural health monitoring, and machine condition monitoring. Common measurements include temperature, strain, voltage, current, pressure, force, and acceleration.

The advantage of data loggers is that they can operate independently of a computer, unlike many other types of data acquisition devices. Data loggers are available in various shapes and sizes. The range includes simple economical single channel fixed function loggers to more powerful programmable devices capable of handling hundreds of inputs.

8.1 DATA LOGGERS IN RAILWAY NETWORK

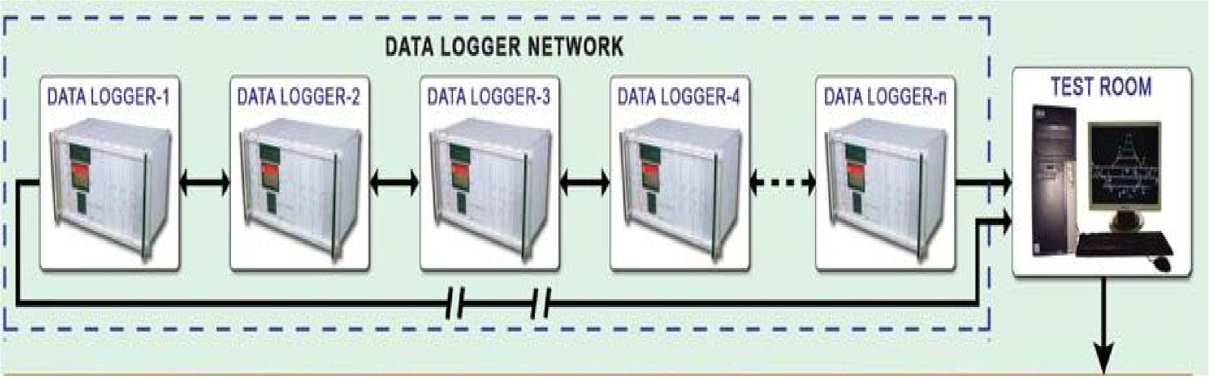
Data logger system is helpful in monitoring Railway Signal Control and Interlocking relays in order to verify their operation, diagnose faults and in maintenance. Data logger logs the change of status of relays & voltages of analog channels connected to it and transmits event information to the central place to generate various exceptions, reports and other information by application software.

Data logger‘s are mandatory for all new relay interlocking (PI/RRI), EI installations and it is also recommended to provide in all existing PIs/RRIs. Due to complexity of above interlocking systems and wiring sometimes it is very difficult to rectify the failures. So data logger can monitor these systems with real time clock. Thus, it can be named as black box of S& T equipments and hence it is a vital tool for accident investigation. Data logger is used at Stations/yards. Whereas in case of Auto Section & IBH Mini data loggers, called as Remote Terminal Unit (RTU), are used.

8.2 GENERAL SETUP OF DATALOGGER SYSTEM IN RAILWAYS

- Data logger is placed in the relay room of a station. The relays reflect the status of all assets present in the station yard. Data logger monitors the relay status and records the change of the asset status.
- Each data logger has multiple sets of data output ports for communicating the recorded information to the Central/ Local Fault Analyzing System (FAS).
- Data loggers in each Station present in a division will be connected to Front End Processor located in the Head Quarters through OFC and communicate the recorded information of each station to Head Quarters in Common Protocol (approved by RDSO as per IRS:S:99/2006).

- FEP communicates this recorded information of the Network to Central Monitoring Software called NMDL (Network Management Data Logger) through data output port of FEP. The software analyzes the information related to the assets operation for reporting the occurrence of faults in their operation, simulation of online train movement in the stations etc. Data backup can be done in both CMU and Server present in the Head Quarters for further analysis.



Typical network diagram of data loggers

(Note: Please refer signaling notes (S28) for further details on Data Loggers)