# CHAPTER XV

# D A T A- N E T W O R K

**15.1** 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 centres . 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.

The data networks can also be used for other applications like video conferencing, data conferencing, VOIP, IVRS, disaster management, office automation etc.

**15.2 Private and Public Networks:**

**15.2.1** Railway applications primarily run over Railways' Private Network, i.e. only Railway applications are transported by the network. In contrast, in the Public

Networks, like INTERNET, various applications used by the public are carried by the data networks. In special cases, Railway may make use of public networks using Virtual Private Network (VPN) solutions.

**15.2.2** Railways Private Network is built up by utilising bandwidth from Railways' own Railtel Corporation of India (RCIL) or leasing bandwidth from BSNL or other service providers.

## 15.3 Communication Media:

The communication links making up the data network may be over a combination of any of the following media :

OFC, Digital MW, IP Radio links, VSAT, Analog MW, Twisted pair copper for last mile connectivity. For Local Area Network (LAN) in the same building Optic Fibre Cable/Cat 6 cables are used. Wherever feasible wireless LAN (WiFi, WiMax) as per latest international standards may also be adopted.

### 15.4 Classification of Networks :

Networks can be classified into 2 main categories:

**(i)** **IP Networks**: Networks which adopt packet data transmission and use IP protocol are called IP networks. In Railways all packet data transmission is done on IP protocol. In these networks, virtual connection is established between the client and server and data transmission takes place in packets. For delay to be within limits , maximum of 3 router hops is permitted in the primary path between the client and the server. In the alternate routed paths, the router hops should be limited to a maximum of 5. All new networks should preferably be IP based.

**(ii)** **Non-IP networks:** In these networks, direct connection exists between the client and server. Non-IP networks adopt either synchronous or asynchronous transmission. Synchronous transmission is followed for transmission of large blocks of data .

### 15.5 Network Speeds :

**15.5.1** The earlier networks were non-IP based and worked at speeds of 9.6 Kbps. Gradually some of the non-IP based network speeds were upgraded to 64 Kbps. Generally higher speeds are not adopted in non-IP networks.

**15.5.2** Presently networks are mostly IP based and operate at speeds of 2 Mbps at the core and distribution levels and 64 kbps at the access level. Speeds of n x 64 Kbps may be used at important access points depending on the network traffic. Similarly at the core level n x 2 Mbps may also be adopted. In a centralized system as in FOIS, the core level comprises the communication links between CRIS (Centre for Railway Information System)/ Rly.Board and zonal Hqrs. Distribution level comprises the communication links between zonal Hqrs. and divisions and access level is made up of links connecting the division to the activity centres In a distributed system as in PRS, the computers at the 5 metro cities are connected in a mesh topology and form the core network. The network connecting the 5 locations to other zonal headquarters and divisional headquarters forms the distribution layer and the connections from the zonal/divisional headquarters to the other locations forms the access network.

**15.5.3 Bandwidth Requirement for Applications:**

The Bandwidth requirement will depend on

1. Network Architecture: Access layer, Distribution and Core layer- lowest for access layer and highest in the core in that order
2. Type of Application design: Text/Character based-PRS,GUI-FOIS/CAD/Graphics/Video- lowest for character based and highest for Video in that order. Ex: for a town like Nellore in AP- a 64Kbps bandwidth is sufficient for UTS and PRS combined.
3. Number of concurrent users at that location.
4. Type of Process: transactional process/ Batch process
5. Database design: Distributed-PRS/Centralised-FOIS

## 15.6 Network Topology :

**15.6.1** Local Area Network (LAN) is an interconnection of data devices using speeds of 10 Mbps/ 100 Mbps/ 1Gbps.

The network topologies commonly used for LAN are:

i. Bus : Data devices are connected to a common bus which is linear.

ii. Ring: Data devices are connected in a ring from which gives an alternative path during failure of any one link. Generally not followed.

iii. Star / Hub: Number of data devices connected to a data device at a central location.

iv. Combination of the above depending on geographical lay out.

LAN is adopted at the lowest level of the network.

**15.6.2 CERTIFICATION OF LAN CABLES:**

The LAN cables after drawing through the casing are to be certified by the firm executing the work through suitable measurements that the characteristics of the cables are within the standards.

**15.6.3** Wide Area Network (WAN) is formed when data devices are located far away and cannot be connected together to form a LAN. In other words, WAN is an interconnection of LANs with communication links of required speed. The network topologies in WAN are:

i. Point-to-point : In this configuration, two locations are connected together by a communication link.

ii. Point – to –multipoint. In this configuration, central location is connected to many locations by communication links.

iii. Mesh: Interconnection of every data device to every other data device in the network.

iv. Combination of the above.

**15.6.4** The network topology is to be decided according to the type, size and requirement of the application. Mesh architecture is recommended at the core

and distribution levels. At the access level, point-to-point or point-to-multipoint architecture is followed.

**15.7 Network path protection:** Data networks are mission critical applications for Railway operation and the data devices at various locations are required to remain connected to the network all the time. At the core and distribution levels, the availability of 100% is required and this is achieved by adopting mesh architecture. Besides, it should be ensured that disruption of physical media will not cause interruption of all alternative paths. At the access level, availability of better than 99.9% is required for each location. This can be achieved only through provision of an alternative path to the main path. Wherever feasible channels utilized from RCIL shall be protected by provision of alternative path either by automatic protection switching or manual protection switching. In the case of locations not connected on Railtel channels, the locations should be connected on two channels leased from different service providers. In the event of any of the communication links being provided by the operators through public networks, adequate protection in the form of VPN and using encryption is to be taken.

**15.8 Network Devices :** The various devices used in the data network other than the nodes on which the applications reside, along with their interface specifications are given below:

**15.8.1 Non-IP Networks**

Modems : V.24, RS 232.
Statistical Multiplexers
Line drivers

**15.8.2 IP Networks**

Modems : ( 64 Kbps/2 Mbps) V.35, G.703.
Hub: Ethernet ( 10/100/1000 Mbps) IEEE 802.

Switches ( level 2) : Ethernet ( 10/100/1000 Mbps)

Managed switches (level 3) : Ethernet ( 10/100/1000 Mbps)

LAN extenders.

Routers : a) Ethernet ( 10/100/1000 Mbps)

b) WAN ports ( 64 Kbps, 2 Mbps), ISDN, Voice etc.

Firewalls

Soft switch ( for VOIP applications): H323,SIP

Gateways

Link balancers

The complexity of the data devices will depend on their capabilities to handle various functionalities like support for VPN, data encryption, data handling capacity, compression, Memory, data logging, remote monitoring and configuration, Number of ports, expandability, security etc.

IEEE standards of some of the Datacom equipment and Ethernet cable standards used are given in the table. The standards are to be updated when ever changed.

| ***Network Hardware*** | ***IEEE STANDARD*** | ***Network Hardware*** | ***IEEE STANDARD*** |
|---|---|---|---|
| Ethernet 100BaseT | IEEE 802.3/95 | Wireless access point | IEEE 802.11f |
| Ethernet 1000BaseT | IEEE 802.3/99 | | IEEE 802.16 |
| Ethernet 10GBaseT | IEEE 802.3/06 | Link/Load Balancer | IEEE 802.1d |
| WireLess Router | IEEE 802.16 | Network Interface Card | IEEE P 802.11 |
| Router | IEEE 802.16 | Multiplexer | IEEE P 802.3ah |
| Switch | IEEE 802.3ae | Line Drivers | IEEE 802.3 |
| HUB | IEEE 802.1 | LAN Extenders | IEEE P 802.3ae |
| MODEMS | IEEE 802.16 | Communication Analyser | IEEE 802.3ae |
| | ITU-R 215 | Ethernet Analyser | IEEE 802.3 |
| Firewall | IEEE P 1363 | Protocol Analyser | IEEE 802.11lb |
| VOIP Gateway | IEEE 802.3af | LAN Cable Meter | IEEE 802.11/5 |
| UPS | IEEE 802.3af | BER Meter | IEEE 802/99 |
| Personal Computer | IEEE 802 P600 | Printer | IEEE 802/ |
| Server | IEEE P802 | | IEEE P1394 |

**Ethernet Cable Standards**

| Class / Category | Cable Standard | Connector Standard |
|---|---|---|
| Class D, Category 5e | IEC 61156-5 CAT 5e | IEC 60603-7-2 (UDP) |
| | | IEC 60603-7-3 (Screened) |
| Class E, Category 6 | IEC 61156-5 CAT 6 | IEC 60603-7-4 (UDP) |
| | | IEC 60603-7-5 (Screened) |
| Class F, Category 7 | IEC 61156-5 CAT 7 | IEC 60603-7-7 (Screened) |

**15.9 Network scalability:** It should be possible to add new network devices either at existing locations or at new locations by extending the WAN. The network components should be so selected to permit scalability without having to replace existing network components. At least 25% spare equipment shall be planned for equipment like modems, Hubs, UPSs, unmanageable switches, LAN Extenders, PCs etc., 1:1 ratio spares are recommendable for core level and distribution level network equipment like High end routers, manageable switches, Servers, Firewall etc., for efficient maintenance of the Networks.

**15.10 Access to public :** It is necessary to allow access to Railway Data networks for the public to access information from applications such as PRS, NTES, FOIS, claims Information System etc. It is necessary such access through Internet is permitted at a single point in the network and the gateway is adequately protected through provision of firewalls etc.

**15.11 Network Security :** The main aspects of security is :

Data sent by the sender should be received only by the intended receiver. This is achieved through encryption at various levels. Encryption can be built in at application level as well as network level. The various data encryption standards are IP sec. DES, 3 DES, AES, private/public key etc.

15.11.1 Access Control: The access control protocols perform three functions: Authentication, Authorization and Accounting.

(a) Authentication. : Authentication is the process of identifying and verifying a user. Only authorized personnel should be permitted access to use the network resources. This is import for dial-in and also wireless access. This is achieved through password protection. The standards are radius etc.

(b) Authorization: It determines what a user can do after being authenticated.

(c) Accounting: Accounting is recording what a user is doing or has done.

15.11.2 Another important aspect of security is to prevent outsiders from monitoring the network or disrupting the network. Intrusion Detecting and Intrusion Prevention are very important in network security. This is achieved through deployment of :

(a) Firewall: First level of defence at the network perimeter. State full inspection of packets based on protocols.

(b) Intrusion detection and Protection system: Signature identification, Protocol identification etc. Detects and Drop the suspected packets.

**15.12 Network Protection**: All computers on the network should be protected against viruses by installing suitable antivirus software. This is necessary as virus can also slow down the network speeds apart from affecting the computers. Enterprise level anti-virus software with control of the network administrator should be installed. All the servers should be protected by firewalls, intrusion detection and intrusion protection systems as well as by anti-virus programs.

**15.13 Network convergence:** A single data network can support many applications through selection of proper network devices like routers etc. and by providing communication links of adequate speeds. The early tendency to develop an independent network for each application should be given up and all the applications should be brought on to a common data network. It is however better to have separate networks for management information systems and for critical applications like PRS, FOIS, UTS and all other applications having financial data-basis and transactions. However, with very critical money value applications like PRS, FOIS, UTS already in operation this is required to be carried out very carefully and in a very coordinated manner.

## 15.14 Network Management system and Traffic Monitoring :

Network Management System (NMS) is an essential part of any data network to monitor the health of the network. It is vital tool for creating and operating a reliable, redundant and efficient data networks using SNMP protocol based on open

standards. The Network Management System can do various tasks like configuration, diagnostic, provisioning, security and originating various MIS reports to be utilized by the Network Manager.

Traffic monitoring software is required to monitor the traffic in the communication links and the link capacity should be increased wherever necessary. Packet Sniffer is a tool for monitoring the traffic in the network and generating various MIS reports which helps in planning and augmenting the network resources. Packet Sniffer can also be a part of NMS.

Multi Router Traffic Grapher: MRTG is a tool for monitoring the traffic loads on the network links and generates graphical images which provides live representation of the network traffic

Network administrator will exercise total control over the network through the NMS. Indian Railway Data Network being very large in size there will be several NMS at different locations controlling different segments of the network.

Traffic log: These are required for analyzing the network traffic as well as the actions of the users on the network whenever required.

## 15.15 List of the Test and Measuring Equipments:

Communication Analyzer

Ethernet Analyzer

Protocol Analyzer

The measuring instruments generally used are

BER meter

LAN cable meter

Other latest measuring instruments if any.

## 15.16 Measurements:

The various measurements which are required to be done on Data network for trouble- shooting and for performance monitoring of the network are listed below:

BERT: Simple bit error ratio test.

G. 821,G.826 and M.2100 performance analysis : The G.821 is an out of service measurement whereas G.826 and M.2100 are in-service measurements. The tests are normally conducted for 48hrs. These tests are required for the WAN

segment for different bandwidth. For the LAN segment Ethernet analyzer is used for testing and monitoring the performance.

Jitter and Wander:

Intrinsic Jitter

Maximum Tolerable Jitter

Jitter Transfer Function

Wander.

LAN cable: By using LAN cable meters.

Any other measurements or tests suggested by manufacturers.

## 15.17 FAULT DIAGNOSIS

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.

## 15.18 Environment, Rack and Flooring:

The Datacom equipments should be housed in dust free environment, preferable air-conditioned. The equipment should be housed in a standard 19" rack with front and back openings to facilitate ease of maintenance. The Datacom equipment rack should be provided with power supply distribution panel for AC/DC distribution. Good quality earth less than one Ohm should be provided. The rack

should be placed in such a way that sufficient space is available in the rear and sides of the rack from the walls, typically 1.2 mtrs to ease of maintenance and proper air circulation. DC cooling fans should be provided especially for the routers. False flooring is recommended for the **Data Centre** so that various cabling systems can be accommodated within the flooring. The flooring should be anti-static. Data Centre floor strength shall be designed to carry loads up to 600 Kg/sq.meter. Illuminated & usable clear space of at least 7.5 feet to 8.5 feet shall be provided between the false floor & false ceiling for housing the Data Centre equipment. The raised floor height should be 24" and in any case not less than 18". On-line UPS should be provided preferable with two UPS systems, one for main system and the other for backup supply.

The datacom equipment shall be installed in n x U size racks of required size. The equipment room shall be free from dust and temperature, within the room shall be maintained as per the equipment manufacturer data sheet. In addition to equipment room, maintenance supervisor room cum store room shall be provided to store spares and other important equipment. At Zonal Headquarters where Network management System is proposed, the room size can be decided as required.

## 15.19 Earthing:

Good quality earth is extremely important for reliable working of Datacom equipments and for protection from lightening and surges. The specified value of earth resistance for Datacom equipments is less than 1 Ohm. With RDSO type of ring earth it is possible to achieve less than 1 Ohm, however, in the long run it is difficult to sustain the earth value below 1 Ohm; a ground enhancement material(Specified by RDSO) is recommended to maintain constant earth resistance for life of the earth. It does not depend on the continuous present of moisture to maintain high conductivity and therefore helps to maintain integrity of the earthing system. The availability of the electrical earth having value within the limits is as per standards is to be ensured.

## 15.20 POWER SUPPLY

The power supply whether it is AC or DC is the heart of any equipment. Standard values at the input to be made available to the equipment. The type as well as capacity of power supply required for the equipment to be decided at the time of designing of new networks and for existing networks enhancement of power supply has to be done whenever necessary. Un-interrupted Power supply has to be provided to increase the life of the equipment as well as to keep up the availability of the location/node. The capacity of the UPS is to be decided taking in to consideration availability of local power supply, standby supply and importance of the location. Wherever feasible –48V DC supply shall be used for Data Communication Equipments.

## 15.21 MAINTENANCE SCHECULE:

i The datacom equipment shall be kept clean and tidy without dust and shall be cleaned daily.

ii The diversity channels shall be checked by switching of main channels and ensure that automatic switch over/routing is taking place.

iii 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.

iv Condition of underground cables to be checked by carrying out routine checks done for U/G cables.

v OFC cables and connectors to be checked as per routine checks done on OFC.

vi The Antivirus patches to be updated in NMS system time to time.

vii In addition to the above, any other checks suggested by manufacturers

## 15.22 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 recode 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.