**Summer Training Report**

*Submitted in partial fulfilment of the requirements for the degree of*

**Bachelor of Technology (B.Tech)**

*By*

**Mayur Mahanta**

CSE/4th Semester/201600491

June-2018



**SIKKIM MANIPAL INSTITUTE OF TECHNOLOGY**

**Approved by AICTE, Min of HRD, Govt of India & DTE, Govt of Sikkim**

**Affiliated to Sikkim Manipal University(SMU), Gangtok**

**Majitar, Rangpo, Pin-737132, East Sikkim**

**E-Mail:** [**smit@smu.edu.in**](mailto:smit@smu.edu.in) **Contact No: +91-9635527557**

**[1]**

**CERTIFICATE**

This is to certify that the Project titled RAILNET-INDIAN RAILWAY INTRANET and submitted by MAYUR MAHANTA having Registration no: 201600491 (B.Tech/CSE/4th Semester) for the partial fulfilment of the requirements for the degree of Bachelor of Technology/Engineering (B.Tech/B.E), embodies the bonafide work done by him/her under my supervision.

**[2]**

**Acknowledgement**

This report gives the details of the project work done at the end of IV semester during the summer vacation for partial fulfilment of the requirements for the degree of Bachelor of Technology/Engineering (B.Tech/B.E) under the Supervision of

I am very grateful to my supervisor for his/her help and able guidance for the project. I am very thankful to my Institute, for providing me resources and facilities to help me in the project.

**Signature of Student**

**Name: Mayur Mahanta**

**Date:**

**[3]**

**Table of Contents**

Introduction......................................................................6

Objective of the project…………………………………………………7

Railnet Arrangement at HQ N.F Railways……………………….8

1.Network……………………………………………………………………..9

1.2.Local Area Network……………………………………………….9

1.3.Wide Area Network……………………………………………… 10

1.4.Protocol…………………………………………………………………11

2.Ethernet (Physical/Data Link Layers)………………………….. 12

2.1.Ethernet……………………………………………………………….. 13

2.2.Fast Ethernet………………………………………………………… 13

2.3.Gigabit Ethernet……………………………………………………. 13

2.3.IP and IPX (Network Layer)……………………………………. 14

2.4.TCP and SPX (Transport Layer)………………………………. 14

2.5.HTTP,FTP,SMTP and DNS………………………………………. 15

3.Network Hardware…………………………………………………….. 16

3.1.File/Network Servers…………………………………………….. 16

3.2.Workstations…………………………………………………………. 17

3.3.Network Interface Cards……………………………………….. 17

3.3.1.Ethernet Cards……………………………………………….. 18

3.3.2.Wireless Adapters………………………………………….. 18

[4]

3,3,3,Switches,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,18

3.3.4.Repeaters……………………………………………………………19

3.3.5.Bridges………………………………………………………………..19

3,3,6,Routers,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,.20

3,3,7,Firewalls………………………………………………………………22

4.Topology…………………………………………………………………………….23

4.1.Linear Bus…………………………………………………………………….23

4.2.Star………………………………………………………………………………24

4.3.Tree or Expanded Star………………………………………………….25

5.Network Operating System………………………………………………..26

5.1.Peer-to-Peer………………………………………………………………..26

5.2.Client/Server………………………………………………………………..27

6.Network Infrastructure and Security Trends……………………….28

7.Equipment used in Railnet………………………………………………….30

8.Features……………………………………………………………………………..34

9.Power Supply Arrangement………………………………………………..35

10.Failures and trouble shooting Railnet……………………………….35

11.Suggestion to minimize failure………………………………………….36

12.Conclusion……………………………………………………………………… 37

[5]

**Introduction**

Indian Railways have decided to set up their own Corporate Wide Information System (CWIS) called RAIL-NET to provide computer connectivity between Railway Board with Zonal Railways, Production Units, Centralized Training Institutes, RDSO, CORE & major Training Centres.

[6]

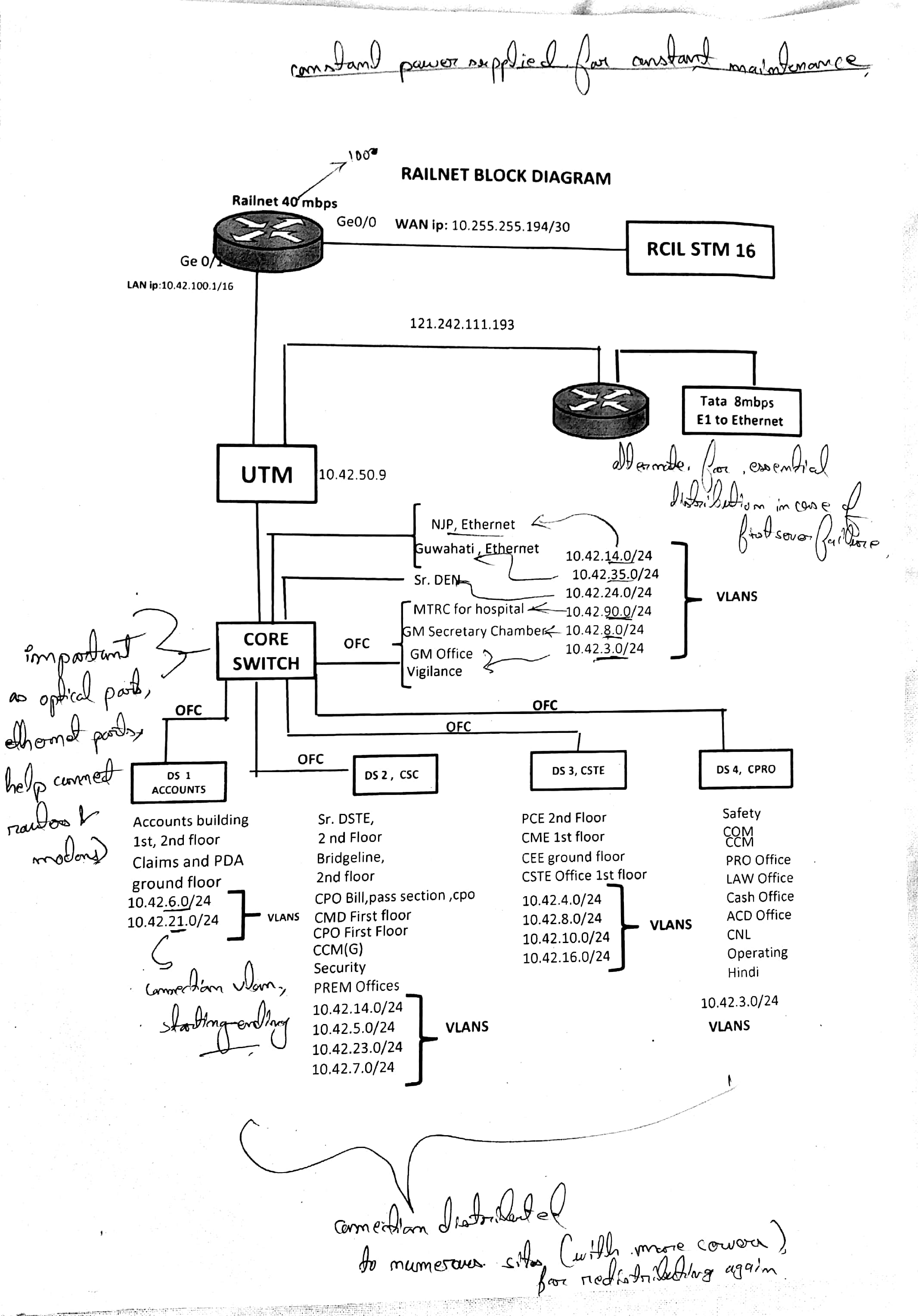
**Objective of the project**

The main object of the project are :-

* To study the various equipment used in the Railnet.
* To understand the installation and construction of the equipment.
* Failure and trouble shooting.
* Maintenance of the system.

[7]

**Railnet Arrangement at HQ N.F Railways**

****

**NETWORK**

A network consists of two or more computers that are linked in order to share resources, exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites or infrared light beams. Two very common types of networks include:

* Local Area Network (LAN)
* Wide Area Network (WAN)

**Local Area Network**

A Local Area Network is a network that is confined to a relatively small area. It is generally limited to a geographical area such as a writing lab, school or building.

Computers connected to a network are broadly categorized as servers or workstations. Servers run continuously to provide services to the other computers on the network. Services provided can include printing, faxing, software hosting, file storage and sharing, messaging, data storage and retrieval, complete access control for the network’s resources and many others.

Workstations are called such because they typically do have a human user which interacts with the network through them. Workstations were traditionally considered a desktop with integrated I/Os. With the advent of tablet computer, our definition of workstation is quickly evolving.

Servers tend to be more powerful than workstations, although configurations are guided by needs. However, the size and speed of the server’s processors, hard drive and main memory might dramatically add to the cost of system unlike workstation.

[9]

On a single LAN, computers and servers may be connected by cables and wirelessly. Wireless access to a wired network is made possible by wireless access points (WAPS). These WAP devices provide a bridge between computers and networks. A typical WAP might have the theoretical capacity to connect hundreds or even thousands of wireless users to a network, although practical capacity might be far less.

Nearly always servers will be connected by cables to the network because the cable connections remain the fastest. Workstations are also usually connected by a cable to the network, although the cost of wireless adapters has dropped to the point that, when installing workstations in an existing facility with inadequate wiring. It can be easier and less expensive to use wireless for a desktop.

**Wide Area Network**

Wide Area Networks connect networks in larger geographical areas. Dedicated transoceanic cabling or satellite uplinks may be used to connect this type of the global network. A WAN is complicated. It uses multiplexers, bridges, and routers to connect local and metropolitan networks to global communications networks like the internet.

**Advantages of installing a Campus Network**

* **User Access Control**
* **Information storing and sharing**
* **Connections**
* **Services**
* **Internet**
* **Computing Resources**
* **Flexible Access**
* **Workgroup Computing**

[10]

**Protocol**

A protocol is a set of rules that govern the communications between computers on a network. Many different types of network protocols and standards are required to ensure that your computer can communicate with another computer. The OSI (Open Systems Interconnection) Reference Model defined seven layers of networking protocols. The complexity of these layers is vast; however, they can be simplified into four layers to help identify some of the protocols.

|  |  |  |
| --- | --- | --- |
| **OSI Layer** | **Name** | **Common Protocols** |
| 7 | Application | HTTP|FTP|SMTP|DNS|Telnet |
| 6 | Presentation |  |
| 5 | Session |  |
| 4 | Transport | TCP|SPX |
| 3 | Network | IP|IPX |
| 2 | Data Link | Ethernet |
| 1 | Physical | Ethernet |

Figure illustrates how some of the major protocols would correlate to the OSI model in order to communicate via the internet.

[11]

**Ethernet (Physical/Data Link Layers)**

The physical layer of the network focuses on hardware elements, such as cables, repeaters, and network interface cards. By far the most common protocol used as the physical layer is Ethernet. For ex, an Ethernet network such as 10BaseT or 100BaseTX specifies the type of cable that can be used, the optimal topology (star vs bus, etc. ), the maximum length of cables, etc. The data link layer of the network addresses the way that data packets are sent from one node to another. Ethernet uses and access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). This is a system where each computer listens to the cable before sending anything through the network. If the network is clear, the computer will transmit. If some other node is already transmitting on the cable, the computer will wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant. When this happens a collision occurs. Each computer then backs off and waits a random amount of time before attempting to retransmit. However, the delay caused by collisions and retransmitting is very small and does not normally effect the speed of transmission on the network.

[12]

**Ethernet**

The original Ethernet standard was developed in 1983 and had a maximum speed of 10 mbps over coaxial cable. The Ethernet protocol allows for bus, star or tree topologies, depending on the type of cables used and other factors. This heavy coaxial cabling was expensive to purchase, install and maintain, and very difficult to retrofit into existing facilities. The current standards are now built around the use of twisted pair wire. Common twisted pair standards are 10BaseT, 100BaseT and 1000BaseT. The number 10,100,1000 stands for the speed of the transmission, megabits per second; the “Base” stands for “baseband” meaning it has full control of the wire on a single frequency; and “T” stands for “twisted pair” cable. Fibre cable can also be used at this level in 10BaseFL.

**Fast Ethernet**

The Fast Ethernet protocol supports transmission up to 100 mbps. Fast Ethernet requires the use of different, more expensive network concentrators/hubs and network interface cards. In addition, category 5 twisted pair or fibre optic cable is necessary. Fast Ethernet standards include:

* 100BaseT-100 Mbps over 2-pair category 5 or better UTP cable.
* 100BaseFX-100 Mbps over fibre cable.
* 100BaseSX-100 Mbps over multimode fibre cable.
* 100BaseBX-100 Mbps over single mode fibre cable.

**Gigabit Ethernet**

Gigabit Ethernet Standard is a protocol that has a transmission speed of 1 Gbps. It can be used with both fibre optic cabling and copper.

* 1000BaseT-1000 Mbps over 2-pair category 5 or better UTP cable.

[13]

* 1000BaseTX-1000 Mbps over 2-pair category 6 or better UTP cable.
* 1000BaseFX-1000 Mbps over fibre cable.
* 1000BaseSX-1000 Mbps over multimode fibre cable.
* 1000BaseBX-1000 Mbps over single mode fibre cable.

**IP and IPX (Network Layer)**

The network layer is in charge of routing network messages (data) from one computer to another. The common protocols at this layer are IP (which is paired with TCP at the transport layer for Internet Network) and IPX (which is paired with SPX at the transport layer for some older Macintosh, Linus, Unix, Novell and Windows networks). Because of the growth in Internet-based networks, IP/TCP are becoming the leading protocols for most networks.

Every network device have a physical address called a MAC (Media Access Control) address. When you purchase a network card, the MAC address is fixed and cannot be changed. Networks using the IP and IPX protocols assign logical addresses to the devices on the network. This can all become quite complex-suffice it to say that the network layer takes care of assigning the correct addresses (via IP or IPX) and then used the routers to send the data packets to other networks.

**TCP and SPX (Transport Layer)**

The transport layer is concerned with efficient and reliable transportation of the data packets from one network to another. In most case, a document, e-mail message or other piece of information is not sent as one unit. Instead, it is broken into small data packets, each with header information that identifies its

[14]

correct sequence and document. When the data packets are sent over a network, they may or may not take the same route- it doesn’t matter. At the receiving end, the data packets are reassembled into the proper order. After all packers are received, a message goes back to the originating network. If a packet does not arrive, a message to “re-send” is sent back to the originating network. TCP, paired with IP, is by far the most popular protocol at the transport level. If the IPX protocol is used at the network layer, then it is paired with SPX at the transport layer.

**HTTP, FTP, SMTP and DNS**

**(Session/Presentation/Application Layers)**

Several protocols overlap the session, presentation and application layers of networks. There protocols listed below are a few of the more well-known:

* DNS- Domain Name System- translates network address (such as IP addresses) into terms understood by users (such as Domain Names) and vice-versa.
* FTP- File Transfer Protocol- a protocol that is used to transfer manipulate files on the internet.
* HTTP- HyperText Transfer Protocol- An Internet-based protocol for sending and receiving webpages.
* SMTP- Simple Mail Transfer Protocol- A protocol for e-mail messages on the Internet.
* DHCP- Dynamic Host Configuration Protocol- can automatically assign Internet addresses to computers and users.
* IMAP- Internet Message Access Protocol- A protocol for e-mail messages on the Internet.
* IRC- Internet Relay Chat- a protocol used for internet chat and other communications.

[15]

**Networking Hardware**

Networking hardware includes all computers, peripherals, interface cards and other equipment to perform data-processing and communications within the network. This section provides information on the following components:

* Network Servers
* Workstations
* Network Interface Cards
* Switches
* Repeaters
* Bridges
* Routers
* Firewalls

**File/Network Servers**

One or more network servers is a part of nearly every local area network. These are very fast computers with a large amount of RAM and storage space, along with one or more fast network interface card(s). The networking operating system provides tools to share server resources and information with network users. A sophisticated permissions-handling system is included, so that access to sensitive information can be carefully tailored to the needs of the users. For small networks, a single network server may provide access control, file sharing, printer sharing, email, database, and other services. The network server may be responding to request from many network users simultaneously. For example, it may be asked to load a word processor program to one workstation, receive a database file from another workstation, and store and e-mail message during the same time period. This requires a computer that can store and quickly share large amounts of information.

[16]

When configuring such a server, budget is usually the controlling factor. The following guidelines should be followed:

* Fastest Processor(s)
* Large amount of RAM
* Multiple large, fast hard drives
* Extra expansion slots
* Fast network interface card(s).

*Optionally (if no other such devices are available on the network):*

* A RAID (Redundant Array of Inexpensive Disks) to preserve large amounts of data (even after a disk failure).
* A back-up unit (i.e. DAT tape drive, removable hard drives, or CD/DVD/BluRay burner).

**Workstations**

Computers that humans use are broadly categorized as workstations. A typical workstation is a computer that is configured with a network interface card, networking software, and the appropriate cables. Workstations do not necessarily need large storage hard drives, because files can be saved on the file server. Almost any computer can serve as a network workstation.

**Network Interface Cards**

The network interface card (NIC) provides the physical connection between the network and the computer workstation. Most NICs are internal, and they are included in the purchase of most computers. Network interface cards are a major factor in determining the speed and performance of a network. It is a good idea to use the fastest network card available for the type of workstation you are using.

[17]

The most common network interface connections are Ethernet Cards and wireless adapters.

**Ethernet Cards**

Ethernet cards are usually included with a computer, although additional Ethernet cards can be purchased and installed on most computers. Ethernet cards can contain connections for either coaxial or twisted pair cables (or both). If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have RJ-45 connection. Some Ethernet cards will also contain an AUI connector. This can be used to attach coaxial, twisted pair, or fibre optics cable to an Ethernet card. When this method is used, there is always and external transceiver attached to the workstation. Only the RJ-45 connector is found on most modern Ethernet Cards.

**Wireless Adapters**

Wireless adapters are found in most portable devices, such as laptops, smart phones, and tablet devices. External wireless adapters can be purchased and installed on most computers having an open USB (Universal Serial Bus) port, or unused expansion slot.

**Switches**

An Ethernet switch is a device that provides a central connection point for cables from workstations, servers and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central switch/hub. Most switches are active, that is they electrically amplify the signal as it moves from one device to another. The predecessor of the switch was the hub, which broadcasted all inbound packets out all ports of the device, creating huge amounts of unnecessary network traffic. Modern switches build a port map of all IP address which respond on each port, and only broadcasts on all ports when it doesn’t have a packet’s target IP address already in its port map.

[18]

Switches are:

* Usually configured with 8,12 or 24 RJ-45 ports.
* Often used in a star or tree topology.
* Available as “managed” or “unmanaged”, with the later less expensive, but adequate for smaller networks.
* Direct replacements for hubs, immediately reducing network traffic in most networks servers, bridges, or routers.

**Repeaters**

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called repeater. The repeater electrically amplifies the signal it receives and rebroadcasts it. Repeaters can be separate devices or they can be incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100 metre limit.

**Bridges**

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

[19]

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct station. Most bridges can “listen” to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. The bridge keeps information flowing on both sides of the network, but it does not allow unnecessary traffic. Bridges can be used to connect different types of cabling, or physical topologies. They must however, be used between networks with the same protocol.

**Routers**

Routers are the traffic directors of the global internet. All routers maintain complex routing tables which allow them to determine appropriate paths for packets destined for any address. Routers communicate with each other, and forward network packets out of or into a network. Here’s an example:

You want to search for something on the internet using a search engine. You open a browser on your workstation. The browser opens to a blank page. You type “<http://www.google.com>” into the URL address line of the browser The browser software packages up the URL you typed, and sends it with a request for an IP address to the DNS that has been set in your network adapter’s configuration. The domain server returns an IP, such as 74.125.67.103 (actual address returned by DNS for google.com on June 7th, 2011). The browser ships the request for that IP address off to the network card, which bundles the request into an Ethernet packet, destined for 74.125.67.103. The network card sends the packet to the gateway of your network, which opens the header of the packet, and makes a

[20]

Determination that the packet is travelling out of your network, in search of 74.125.67.103. Your network’s router has routing tables which it has been building from communicating with other routers, and potentially augmented with “static routes”, which are specific paths added by your network’s administrators to make the task of accessing certain networks about another router at my ISP (Internet Service Provider), which in turn has several more routers that are all on networks of which 1 am just a small node, much like finding an atom of a molecule of a piece of dust on a rock on a moon of a planet of a sun of a galaxy of the universe. In any case, the packet gets passed from router to router, each time moving out of the subnets of the packet sender towards a router that will know where the desired server is. The packet finally reaches the router of the network at 74.125.67.103 which dutifully delivers the packet to the server at that IP address. The server carefully crafts a response, and sends a reply back, which follows the same process to get the “go” signal back to the requester, And that’s just the initial request.

While bridges know the address of all computers on each side of the network, routers know the addresses of the other routers which in turn know about their own networks. Routers can even “listen” to entire networks to determine which sections are busiest – they can then redirect data around those sections until traffic congestion clears.

So routers are network gateways. They move network packets from one network to another, and many can convert from one network protocol to another as necessary. Routers select the best path to route a message, based on the destination address of the packet. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.

[21]

**Firewalls**

A firewall is a networking device that is installed at the entrance to a LAN when connecting a networks together, particularly when connecting a private network to a public network, such as the internet. The firewall uses rules to filter traffic into and out of the private network, to protect the private network users and data from malevolent hackers. Firewalls are either hardware or software, depending on their intended use. A firewall used to protect a network is a hardware device that should be installed on the network between the router and the network. Almost all hardware firewalls will have at least two ports, labelled “Trusted” and “Untrusted”. These terms imply the true nature of the firewall’s responsibility to the private network. The public network is connected to the untrusted network port, and the private network is connected to the trusted port. Firewall rules are usually simple, consisting of a verb, either allow or deny, the direction of the traffic, either inbound or outbound, and an address or other network traffic identifier. Firewall rules are cumulative, so general rules may be specified, and exceptions added as necessary. Some examples are:

* Allow outbound all.
* Deny outbound all.
* Allow inbound port 80.
* Allow inbound port 80 destined to 170.200.201.25
* Deny inbound from 201.202.1.1/24

Software firewalls are commonly included in modern workstation and server operating systems. They operate in a similar way as hardware firewalls, except that they filter traffic in and out of the machine itself. These software firewalls are typically unnoticed by machine users, and only need attention occasionally when an internet-connected application don’t work as expected.

[22]

**Topology**

The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations.

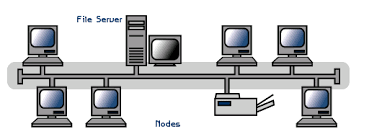
**Main types of Physical Topologies**

The following sections discuss the physical topologies used in networks and other related topics.

* **Linear Bus**
* **Star**
* **Tree (Expanded Star)**

**Linear Bus**

A linear bus topology consists of a main run of cable with a terminator at each end. All nodes (file servers, workstations and peripherals) are connected to the linear cable.



**Advantages of a Linear Bus Topology**

* Easy to connect a computer or peripheral to a linear bus.
* Requires less cable length than a star topology.

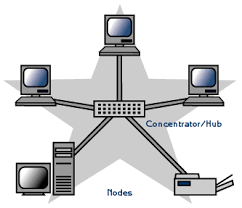
**Disadvantages of a Linear Bus Topology**

* Entire network shuts down if there is a break in the main cable.
* Terminators are required at both ends of the backbone cable.

[23]

**Star**

A star topology is designed with each node connected directly to a central network hub, switch or concentrator. Data on a star network passed through the hub, switch or concentrator before continuing to its destination. The hub, switch or concentrator manages and controls all functions of the network. It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fibre optic cable.



**Advantages of a Star Topology**

* Easy to install and wire.
* Easy to detect faults and to remove parts.

**Disadvantages of a Star Topology**

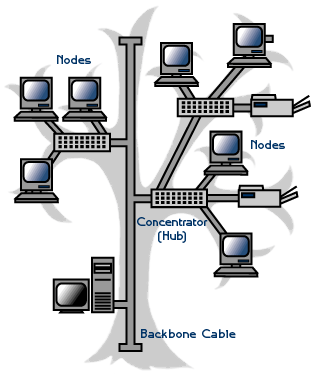
* Requires more cable length than a linear topology.
* If the hub, switch or concentrator fails, nodes attached are disabled.

**Tree or Expanded Star**

A tree topology combines characteristics of a linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable.

[24]

Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.



**Advantages of a Tree Topology**

* Point-to-point wiring for individual segments.
* Supported by several hardware and software venders.

**Disadvantages of a Tree Topology**

* More difficult to configure and wire than other topologies.
* If the backbone line breaks, the entire segment goes down.

**Considerations when choosing a Topology**

* **Money:** A linear bus network may be the least expensive way to install a network.
* **Length of cable needed:** The linear bus network uses shorter lengths of cable.
* **Future growth:** With a star topology, expanding a network is easily done by adding another concentrator.

[25]

**Network Operating System**

Unlike operating systems, such as Windows, that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

The two major types of network operating systems are:

* Peer-to-Peer
* Client/Server

Nearly all modern networks are a combination of both. The networking design can be considered independent of the servers and workstations that will share it.

**Peer-to-Peer**

Peer-to-Peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source. In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-Peer networks are designed primarily for small to medium local area networks. Nearly all modern desktop operating systems, such as Macintosh OSX, Linux and Windows, can function as Peer-to-Peer network operating systems.

**Advantages of a Peer-to-Peer network**

* Less initial expense- No need of dedicated server.
* Setup- An OS already in place may only need to be reconfigured for Peer-to-Peer operations.

[26]

**Disadvantage of a Peer-to-Peer Network**

* Decentralized- No central repository for files and applications.
* Security- Does not provide the security available on a client/server network.

**Client/Server**

Client/Server network OS allows the network to centralize functions and applications in one or more dedicated file servers. The file servers become the heart of the system, providing access to the resources and providing security. Individual workstations (Clients) have access to the resources available on the file servers. The network OS provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical location. UNIX/Linux and the Microsoft family of Windows Servers are examples of client/server network OS.

**Advantage of a client/server network**

* Centralized- Resources and data security are controlled through the server.
* Scalability- Any or all elements can be replaced individually as needs increase.
* Flexibility- New Technology can be easily integrated into system.
* Interoperability- All components work together.
* Accessibility- Severs can be accessed remotely and across multiple platforms.

**Disadvantages of a client/server network**

* Expense- Requires initial investment in dedicated server.

[27]

* Maintenance- Large networks will require a staff to ensure efficient operation.
* Dependence- When server goes down, operations will cease across the network.

**Big enterprise network infrastructure and security trends**

**Security breaches are harder to stop**

Security breaches and data leakage will continue to trouble companies of all sizes. The threat timeline over the last 10-15 years has shown that a new threat tends to be quickly answered by a new defence system. The threat then evolves, and a new defence system is needed. This has led to a myriad of desperate security appliances, software agents and management systems that in many cases are unable to talk to one other. When the bad guys tweak the Threat Life Cycle, for example, via the creation of Advanced Persistent Threats or APTs, it becomes very difficult to stay ahead of the curve. Next-generation security architectures will integrate discrete security systems into a platform, which can correlate threat life elements and break the infection chain in different places.

**Cloud technologies are finally taking root**

All forms of cloud are starting to make inroads as a viable part of the enterprise infrastructure. Software as a Service (SaaS) has reached a tipping point as most organizations trust a provider’s security capabilities. Infrastructure as a service (IaaS) is still focused on web applications for elasticity and redundancy. Cloud bursting, hybrid clouds and personal clouds will mean more sharing of distributed services, management and security.

[28]

**Diversity in mobile apps and management**

Unlike the PC market, the mobile device market (handsets and tablets) will not be dominated by Microsoft. There will be at least two or three platforms across the globe. This mobile diversity will mean management systems will need to be more flexible and open. Improved JavaScript performance will begin to push HTML5 and the browser as a mainstream enterprise application development environment. This will lead to richer applications and more focus on their usability, rather than larger and cumbersome applications.

**Software defined modular infrastructure becomes the norm**

The control layer is being detached and centralized for many different parts of the infrastructure. Most of the initial focus is on the data centre with virtualization. Software Defined Networking (SDN), Software Defined Storage (SDS) and standalone switch fabrics. The effect is that API’s are being consumed at a much higher rate in a world where the infrastructure is being dissected and segmented, API’s themselves are very important but is also a potential security hole to the network element.

**Internet of Things and Industrial Control Systems (ICS) collide**

The Internet of Things (IoT) is already estimated by Gartner to be made up of some 26 billion devices by 2020. Industrial control systems are rolling out IP all the way to the control and measurement points. These networks are separate today and individual in nature. However, both need to deal with cyber threats, which can cause huge damage across industrial complexes, public operational networks (i.e. power grids) or consumers.

[29]

**Networking bandwidth continues to double every 10 months**

Networking bandwidth requirements continue to expand at a rapid pace. The transition from 10G to 100G will be much faster. All parts of the infrastructure need to perform within the high-speed infrastructure. Traditionally CPU-based firewalls have fallen way behind the performance curve. Most recently ASIC-based firewall appliances have taken a quantum leap in performance, allowing 100G interfaces and throughput in the hundreds of Gbps, saving space and power. Now high-speed networks can design security into the architecture without creating bottlenecks.

**Analytics for everything that’s attached to the network**

Big Data and analytics can be applied for different reasons. The biggest need is business intelligence but it’s also very important for security. The amount of data being gathered is staggering but segmenting the data can lead to more actionable results. For ex, collecting WiFi presence of consumers in retail stores can lead to understanding their buying behaviour.

**Equipment used in Rail-net**

**Synchronous Transport Module (STM)-1:**

* The STM-1 is the SDH ITU-T fibre optical network transmission standard, it is the information structure.
* The basic rate of STM 1 is 155.520 mbps.
* **In Rail-Net Maligaon “Tejas TJ 100 CP” STM-1 is in use.**
* Input Voltage Range Normal Operation: -40V to -60V DC.
* Fuse A Slow Blow Glass fuse. Field replaceable.

[30]



**MAKE- CISCO 3800 series-**

* One router, having multiple WAN ports used in Rail-net, Maligaon

**IP: 10.24.2.2**

* The 3800 Series supports Secure Sockets Layer
* Network interfaces can be upgraded in the field to accommodate future technologies.
* Several Types of slots are available to add connectivity and services in the future in an “integrate-as-you-grow” basics.
* The Cisco 3800 supports more than 90 modules

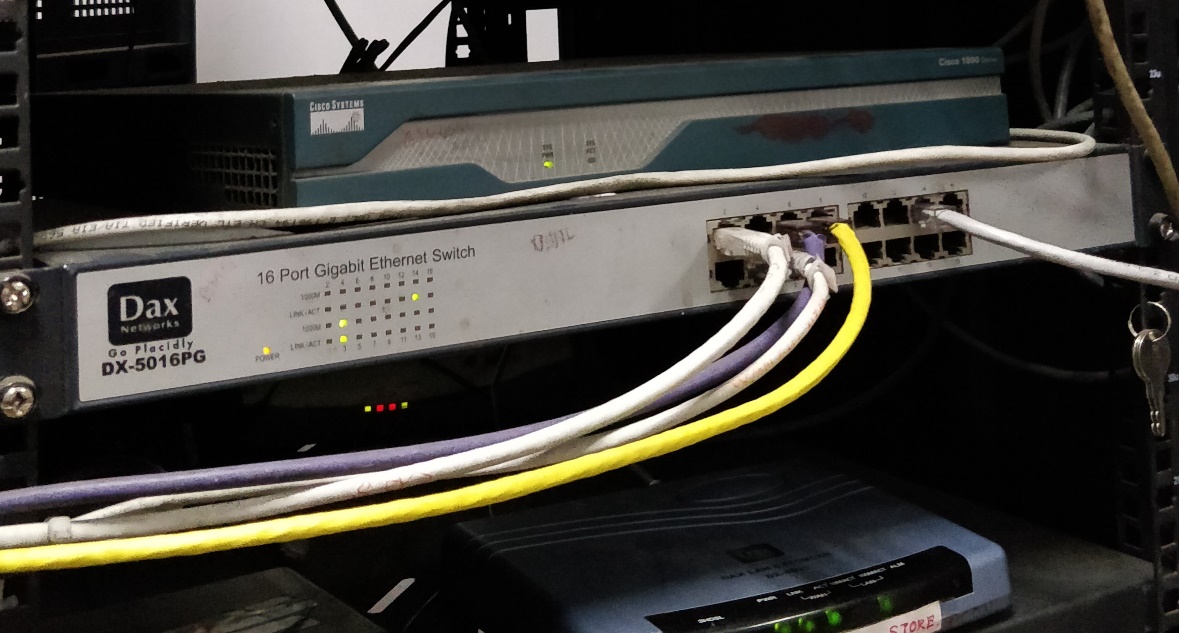


**Switch (In the HQs): -**

* In networks, a device that filters and forward packets between LAN segments. It works using the destination address of the individual frames.
* It can have 16/24/48 port. One port is used to receive data from router and all other to connect. T.S. Console port use for programming switch locally.
* One big difference between Layer 2 and Layer 3 switches is that we are able to do routing in intranetworking with Layer 3 switches which is not possible to do with Layer 2.
* In N.F Railway the Layer 3 switch is of Cisco 3750-G, which has 24 10/100/1000 Ethernet port and four SFP ports.
* The Cisco Catalyst 3750 Series stacks up to 9 switches as a single logical unit for a total of 468 Ethernet ports.
* IPv6 Capable- Getting ready for the future.
* A working stack is self-managing and self-configuring. When switches are added or removed, the master switch automatically updates all the routing tables to reflect changes.
* The layer 2 switch is of cisco 2950 series.
* The Catalyst 2950 Series Intelligent Ethernet Switches, is a fixed configuration, stackable switch that provides Fast Ethernet.
* The Catalyst 2950 Switch is combined with a Catalyst 3550 Series Switch, the solution can enable IP routing from the edge to the core of the network.
* Embedded in Catalyst 2950 Series switches is the Cisco Cluster Management Suite (CMS) Software, which allows users to simultaneously configure and troubleshooting multiple Catalyst desktop switches using a standard Web browser.

[31]





[32]

**Modem: -**

A device that coverts a serial data from a computer to analog data for transmission over ordinary or leaded telephone lines and coverts analog data back to digital at receiving end.

This is used when the terminal is to be connected a system located at remote locations.



[33]

**LAN Extender: -**

* LAN Extender is a device that is used to extend the local area network beyond 100 meters through the copper cable.
* LAN extender is connected on both sides of network.
* This is excellent for Ethernet Distance Extension over Existing Telephone Wire and with just one pair of twisted pair copper wire can easily connect to the Ethernet.

**Media Converter: -**

It is used to divert from one physical medium to other, for ex, from CAT 5 to OFC.

In Rail-net Maligaon HQ, DIGISOL DG-MC5123 is in use.

**DSLAM**

It is a network device located in the telephone exchanges of the service providers, that connects multiple customer Digital Subscriber Lines (DSLs).

The DSLAM acts like a network switch since its functionality is at Layer 2 of OSI model.

In N.F Railway, two numbers of DAS-3248 DSLAM is in use each having 48 ports.

**Features**

Railnet Maligaon use various ways to provide internet connectivity to its users.

Various number of users are as-

LAN – 400 users.

Broad band on residence – 96 users.

[34]

Dial up – 96 users.

The IP provided as 172.16.11.1, in this manner we can provide IP.

**Power Supply Arrangement**

All equipment in Railnet work on 230V AC supply. In Railnet Maligaon, two 5 KVA UPS (made by APC 5000 UX model) are used to provide power supply. One is main and other is stand by distribution board which is used to connect all equipment.

**Battery: -**

Maintenance Free batteries manufactured by Power Systems Limited (type EP 26 ) are used. Each battery is of 26 AH, 8 batteries in series and 8+8 batteries in parallel. They work on Oxygen Recombination principle. Requirement of water top up is completely eliminated.

**Earthing: -**

Conventional method of earthing is used in Railnet Maligaon. Earthing is maintained at less than 1 ohm.

**Failures and troubleshooting Railnet**

Following main failure attend by telecom staff in Railnet: -

* Power supply failure

Check the supply if it is okay, then check the fuse and earthing and rectify it.

* Link failure

Link down due to link error and Hang of equipment.

* Problems in accessing internet

Reset LAN Extender.

[35]

Check whether LAN driver is installed properly or not. If not installed, install it properly.

Or

Check cable pair fault and reset it. Lead faulty between jack panel to terminal.

* Patch card fault

Test patch card using LAN tester.

* Sometimes users face conflict in IP. It is when some other user is accessing the same IP.

**Suggestion to minimize failure**

* All equipment should be installed as their specification suggested by RDSO.
* The power supply must be constant.
* Fuse and Earth protection are provided with correct rating.
* Connector and cable should be right and light.
* All equipment deals with trend staffs.
* Never use any equipment without UPS or protection.
* Never use any extra unrequited device as load.
* All equipment should be cleaned and well temperature maintained.
* Schedule maintenance should be done properly.

[36]

**Conclusion**

As an undergraduate student of the Manipal Institute, I would like to say that this training program is an excellent opportunity for us to get to the ground level and experience the things that we would have never gained through going straight into a job. I am grateful to the Manipal Institute of Gangtok for giving us this wonderful opportunity

This project gives the idea about the working of RAIL-NET in N.F Railway, the equipment and technology used like server, routers, switches, modems, LAN extenders etc, requirements of the RAIL-NET setup, connectivity diagram of various locations. This also concerns about the various faults and how they are removed.

[37]