# COMPANY INFRASTRUCTURE

### Info-com Service

Info−com Service is the part of ONGC which deals with all the matters of communication among the officials in and out of the offices. This is done by dividing the task of Info−com into two groups Telecom Group and IT group. The Telecom group takes care of all the matters regarding EPABX (INTERCOM & ICNET), BSNL Landlines, mobile phones and WLL & VHF devices whereas the IT group looks after the servers, SCADA system and laptop & desktop computers.

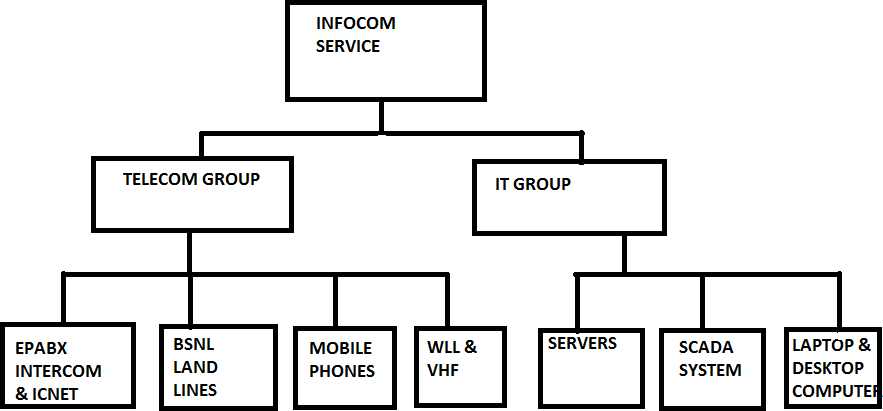


Fig:−INFOCOM SERVICES,TRIPURA ASSET

# IT SERVICES

### Network services

1. More than 400 LAN nodes, 25 L2 switches, 1 L3 switch at Base office complex.
2. Leased lines terminated on two routers.
3. SCOPE Minar Delhi.
4. Kolkata.
5. Jorhat.
6. Baramura GCS.

### Desktop Infrastructure Management thru. Enterprise wide contract with M/c CMC Ltd.

1. 430 Desktop, 400laptop.
2. 250 printers
3. 35 scanners

### NETWORKING: An Overview

A network is a group of interconnected systems which share services and interact with each other by means of a shared communication link.

These systems can be located anywhere.

Network is often classified according to its geographical size.

### BENEFITS OF NETWORKING

Goal of having network environment is to provide services and to reduce the equipment costs. The primary reasons for networking PC’s are as follows:

* 1. Sharing printers and other devices
  2. Providing Distributed Computing
  3. Sharing files
  4. Centralized administration of resources
  5. Security of Resources
  6. Personal communication (like e−mail, chat, audioƒvideo conferencing )
  7. World Wide Web. and many other users.

### NETWORKING BASICS

When looking at networking basics, understanding how a network operates is the first step to understanding routing, switching, and wireless. The network operates by connecting computers and peripherals using switches, routers, and access points. These devices are the essential networking basics that allow the various pieces of equipment connected to your network to communicate with one another, as well as with other networks.

Routers, switches, and access points perform very different functions in a network.

### SWITCHES

Switches are used to connect multiple devices on the same network within a building or campus. For example, a switch can connect your computers, printers, and servers, creating a network of shared resources.

The switch, one aspect of your networking basics, would serve as a controller, allowing the various devices to share information and talk to each other. Through information sharing and resource allocation, switches save you money and increase productivity.

* An unmanaged switch works out of the box and does not allow you to make changes. Home networking equipment typically includes unmanaged switches.
* A managed switch can be accessed and programmed. This capability provides greater network flexibility because the switch can be monitored and adjusted locally or remotely.

With a managed switch, you have control over network traffic and network access.

### ROUTERS

Routers analyze the data being sent over a network, change how it is packaged, and send it to another network or to a different type of network. They connect your business to the outside world, protect your information from security threats, and can even decide which computers get priority over others.

Depending on your business and your networking plans, you can choose from routers that include different capabilities. These can include networking basics such as:

* Firewall: Specialized software that examines incoming data and protects your business network against attacks.
* Virtual private network (VPN): A way to allow remote employees to safely access your network.
* IP phone network: Combines your company's computer and telephone network, using voice and conferencing technology, to simplify and unify your communications.

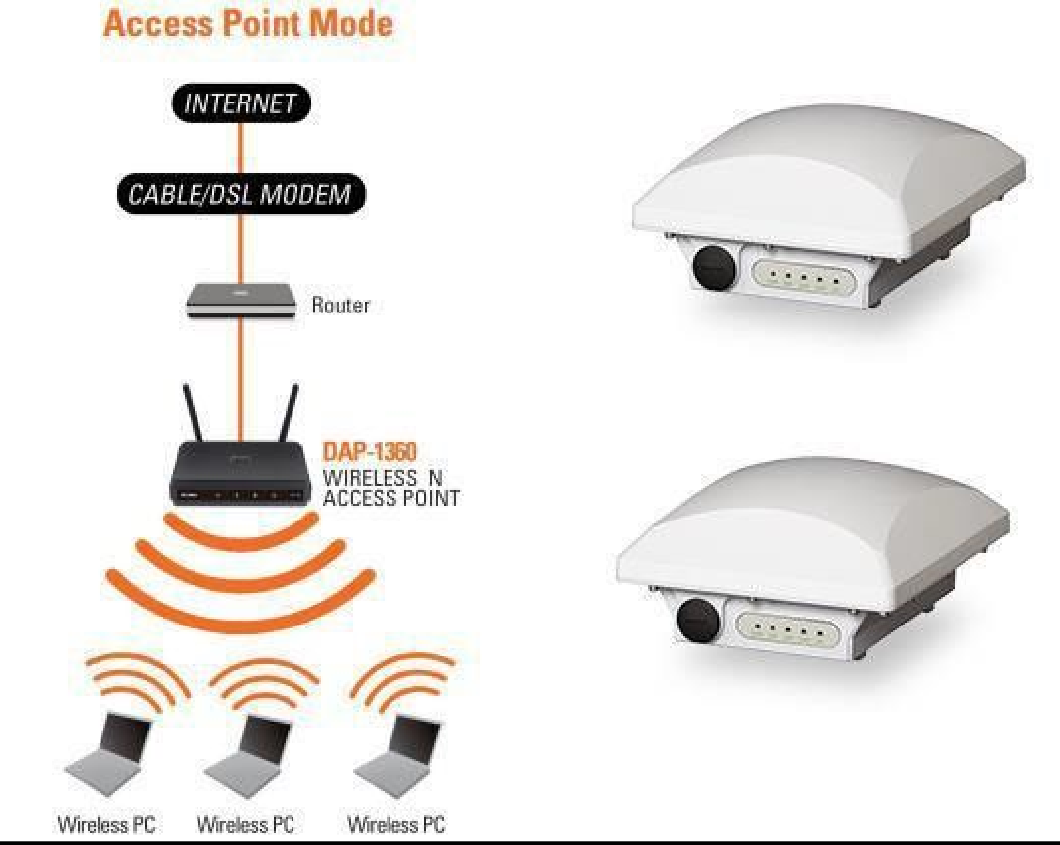


### ACCESS POINTS

An access point allows wireless devices to connect to the network. Having a wireless network makes it easy to bring new devices online and provides flexible support to mobile workers.

There are four different types of deployments that an organization can choose from to create a wireless network. Each deployment has its own attributes that will work better for different solutions. They are:

* **Cisco Mobility Express:** A simple, high−performance wireless solution for small or medium−sized organizations. Mobility Express has the full complement of advanced Cisco features. These features are preconfigured with Cisco best practices. The defaults allow for a quick and effortless deployment that can be operational in minutes.
* **Centralized deployment:** The most common type of wireless network, traditionally deployed in campuses where buildings and networks are in close proximity. This deployment consolidates the wireless network, allowing for easier upgrades and enabling advanced wireless functionality. Controllers are based on−premises and are installed in a centralized location.
* **Converged deployment:** A solution tailored for small campuses or branch offices. It allows customers consistency in their wireless and wired connections. This deployment converges wired and wireless on one network device—an access switches—and performs the dual role of both switch and wireless controller.
* **Cloud-based deployment:** A system that uses the cloud to manage network devices deployed on−premises at different locations. The solution requires Cisco Meraki cloudmanaged devices, which have full visibility of the network through their dashboards



**SOFTWARE IN NETWORKING BASICS**

### PROTOCOL

* Are standards that allow computers to communicate.
* Define how computer identify one another on a network.
* How information be processes once it reach its final destination.
* Define procedure for handling lost or damaged packets.

### DEVICE DRIVERS

* Is a hardware level program that control NIC
* NIC, provide an interface for its hosts operating system
* Communication Software
* That enables the users to communicate and share resources
* Windows Explorer, WWW, Telnet, FTP.

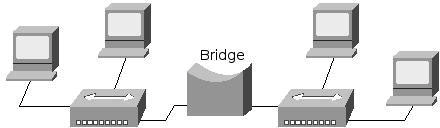
### REPEATERS

* Extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction.
* Copies bits from one network to another
* Does not look at any bits.



### BRIDGE

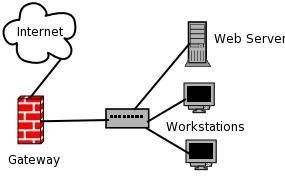
* Copies frames from one network to another.
* Can operate selectively− does not copy all frames (must look at data−link headers).
* Extends the network beyond physical length limitations.



### GATEWAY

* Operates as a router.
* Data conversions above the network layer.
* Conversions: Encapsulation− uses an intermediate network.

Translation− connects different application protocols. Encryption− could be done by a gateway.

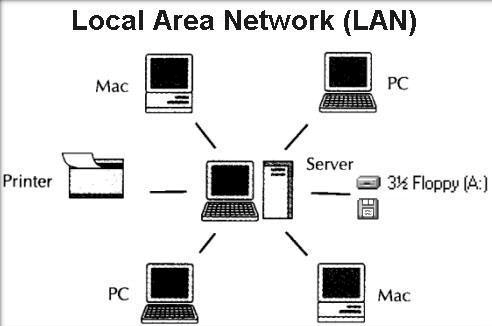


# TYPES OF NETWORKS

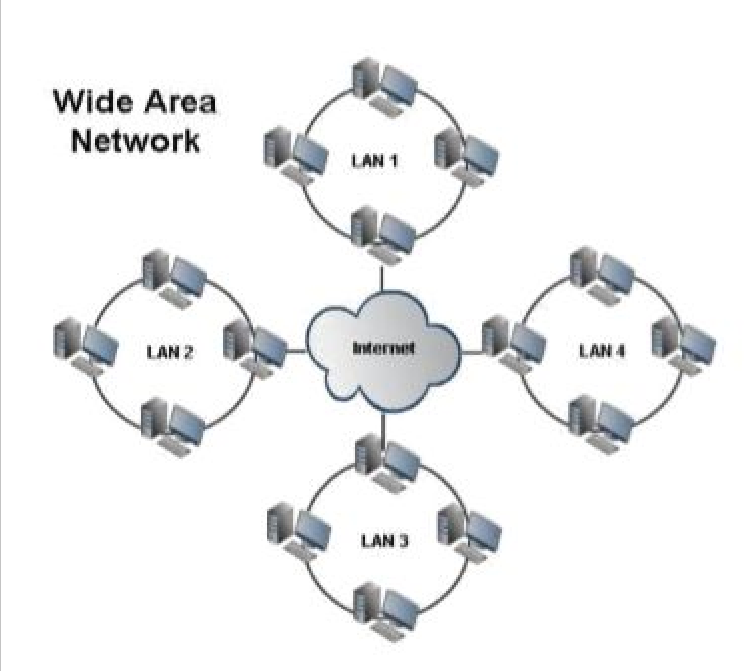
### LOCAL AREA NETWORK (LAN)

Local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building and has its network equipment and interconnects locally managed. The most common type of local area network is an Ethernet LAN.

* Connects computers that are physically close together(<1mile). ➢ High speed ➢ Multi− access
* Technologies ➢ Ethernet 10Mbps, 100Mbps, 1Gbps.



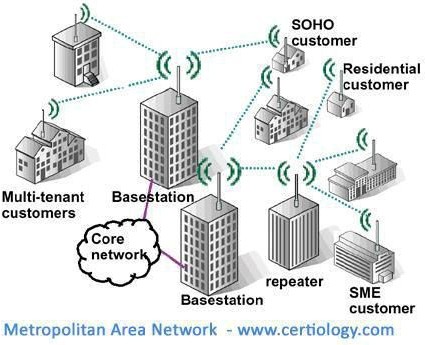
WIDE AREA NETWORK (WAN)

* A wide area network (WAN) is a network that exists over a large−scale geographical area. A WAN connects different smaller networks, including local area networks (LANs) and metro area networks (MANs).
* This ensures that computers and users in one location can communicate with computers and users in other locations. WAN implementation can be done either with the help of the public transmission system or a private network.
* A WAN connects more than one LAN and is used for larger geographical areas. WANs are similar to a banking system, where hundreds of branches in different cities are connected with each other in order tosharetheirofficialdata
* A WAN works in a similar fashion to a LAN, just on a larger scale. Typically, TCPƒIP is the protocol used for a WAN in combination with devices such as routers, switches, firewalls

and modems.

### METROPOLITAN AREA NETWORK (MAN)

* A metropolitan area network (MAN) is similar to a local area network (LAN) but spans an entire city or campus. MANs are formed by connecting multiple LANs. Thus, MANs are larger than LANs but smaller than wide area networks (WAN)
* A MAN is ideal for many kinds of network users because it is a medium−size network. MANs are used to build networks with high data connection speeds for cities and towns.
* The working mechanism of a MAN is similar to an Internet Service Provider (ISP), but a MAN is not owned by a single organization. Like a WAN, a MAN provides shared network connections to its users. A MAN mostly works on the data link layer, which is Layer 2 of the

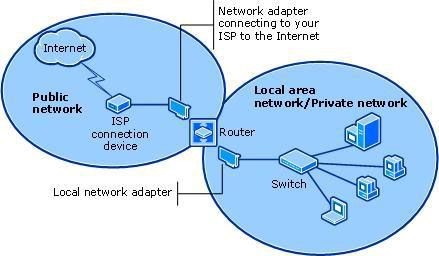
Open Systems Interconnection (OSI)

# NETWORK ADDRESSING

### LAN vs INTERNET

When a group of computers are connected together within a relatively small area, it is referred to as a local area network (LAN). If a LAN is available only to certain people (such as employees of a company), it is called a private or internal network. The Internet is a public network because it is accessible to many users and computers from different networks. The network shown in Figure 6 is a LAN that can be used to connect to the Internet.

A gateway is a combination of hardware and software that connects two different types of networks, for example a private network and a public network. There must be at least two network adapters installed on a gateway, one to connect to the Internet (ISP network adapter) and the other to connect to the private or local network (local network adapter).



### IP ADDRESSING

* An IP address is an address used in order to uniquely identify a device on an IP network. The address is made up of 32 binary bits, which can be divisible into a network portion and host portion with the help of a subnet mask.
* The 32 binary bits are broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.81.100). The value in each octet ranges from 0 to 255 decimal, or 00000000 − 11111111 binary.

This sample shows an IP address represented in both binary and decimal. 10. 1.23.19 (decimal) 00001010.00000001.00010111.00010011 (binary)

### Classification of IP address: IP address is divided into five classes:

1. Class A network address of 1.0.0.0−127.255.255.255

2. Class B network address of 128.0.0.0−191.255.255.255 3. Class C network address of 192.0.0.0−223.255.255.255 4. Class D network address of 224.0.0.0−239.255.255.255 5. Class E network address of 240.0.0.0−255.255.255.255

* + In a Class A address, the first octet is the network portion. Octets 2, 3, and 4 (the next 24 bits) are for the network manager to divide into subnets and hosts as heƒshe sees fit. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16777214 hosts!).
  + In a Class B address, the first two octets are the network portion. Octets 3 and 4 (16 bits) are for local subnets and hosts. Class B addresses are used for networks that have between 256 and 65534 hosts.
  + In a Class C address, the first three octets are the network portion. Octet 4 (8 bits) is for local subnets and hosts − perfect for networks with less than 254 hosts.

### NETWORK MASKS

* A network mask helps you know which portion of the address identifies the network and which portion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:

1. Class A: 255.0.0.0

2. Class B: 255.255.0.0

3. Class C: 255.255.255.0

* An IP address on a Class A network that has not been subnetted would have an addressƒmask pair similar to:

8.20.15.1 255.0.0.0. In order to see how the mask helps you identify the network and node parts of the address, convert the address and mask to binary numbers.

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000

* Once we have the address and the mask represented in binary, then identification of the network and host ID is easier. Any address bits which have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the node ID.

8.20.15.1 = 00001000.00010100.00001111.00000001

255.0.0.0 = 11111111.00000000.00000000.00000000

**net id | host id**

netid = 00001000 = 8

hostid = 00010100.00001111.00000001 = 20.15.1

### HARDWARE USED IN ONGC-A: GENERAL OVERVIEW

##### EPABX (Electronic Private Automatic Branch Exchange):

* A private branch exchange (PBX) is a telephone exchange that serves a particular business or office, as opposed to one that a common carrier or telephone company operates for many businesses or for the general public. PBXs are also referred to as PABX − private automatic branch exchange and EPABX.
* The EPABX may be defined as a switching system that makes available both internal and external stitching functions of any organization.
* The selection of an EPBAX is a difficult task and requires deep knowledge of traffic pattern of the office. By using an EPABX both the internal and external needs of the organization are fully served. With the advent of powerful microprocessors and advancements in the field of computers, the EPBAX can boast of versatile features.
* Auto−conferencing and automatic redialing of numbers found engaged on the first trial are some of other advancements in the features of the EPBAX.

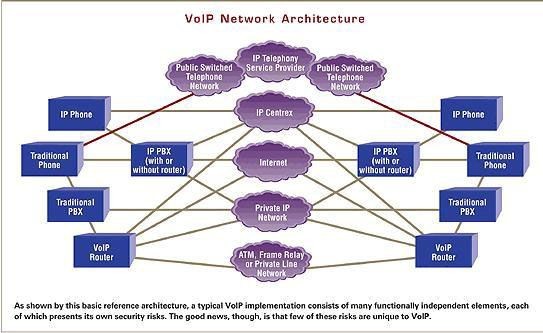
##### PBX (Private Branch Exchange):

A PBX (private branch exchange) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines. The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

A PBX includes:

* Telephone trunk (multiple phone) lines that terminate at the PBX
* A computer with memory that manages the switching of the calls within the PBX and in and out of it
* The network of lines within the PBX
* A console or switchboard for a human operator (optional)

##### VoIP (Voice over IP)

* VoIP (voice over IP) is the transmission of voice and multimedia content over Internet Protocol (IP) networks. VoIP is enabled by a group of technologies and methodologies used to deliver voice communications over the internet, enterprise local area networks or wide area networks.
* VoIP encapsulates audio via a codec into data packets, transmits them across an IP network and unencapsulates them back into audio at the other end of the Connection.VoIP endpoints include dedicated desktop VoIP phones, soft−phone applications running on PCs and mobile devices, and WebRTC−enabled browsers.
* VoIP endpoints typically use International Telecommunication Union (ITU) standard codec, such as G.711, which is the standard for transmitting uncompressed packets, or G.729, which is the standard for compressed packets.
* Many equipment vendors also use their own proprietary codec. Voice quality may suffer when compression is used, but compression reduces bandwidth requirements. VoIP typically supports non−voice communications via the ITU T.38 protocol for sending faxes over a VoIP or IP network in real time.
* Once voice is encapsulated onto IP, it is typically transmitted via the real−time transport protocol or through its encrypted variant, secure real−time transport protocol.
* The Session Initiation Protocol (SIP) is most often used for signalling that is necessary to create, maintain and end calls. Within enterprise or private networks, quality of service is typically used to prioritize voice traffic over no latency−sensitive applications to ensure acceptable voice quality.

### CORAL ISBX

* Coral is a digital communication switching system based on PCM switching technology. The active circuitry of the system is contained on removable Printed Circuit Board (PCB) assemblies or cards.
* Coral users could access content through the Coral Cache by adding .nyud.net to the hostname in the site's URL, resulting in what is known as a 'coralized link'. So, for example,

http:ƒƒexample.com becomes, http:ƒƒexample.com.nyud.net

* Coral avoided high loads on individual nodes through an indexing abstraction called a distributed sloppy hash table (DSHT); DSHTs create self−organizing clusters of nodes which fetch information from each other to avoid communicating with more distant or heavily− loaded servers.

### TELECOM NETWORK

A telecommunication network is a collection of terminal nodes; links are connected so as to enable telecommunication between the terminals. The transmission links connect the nodes together. The nodes

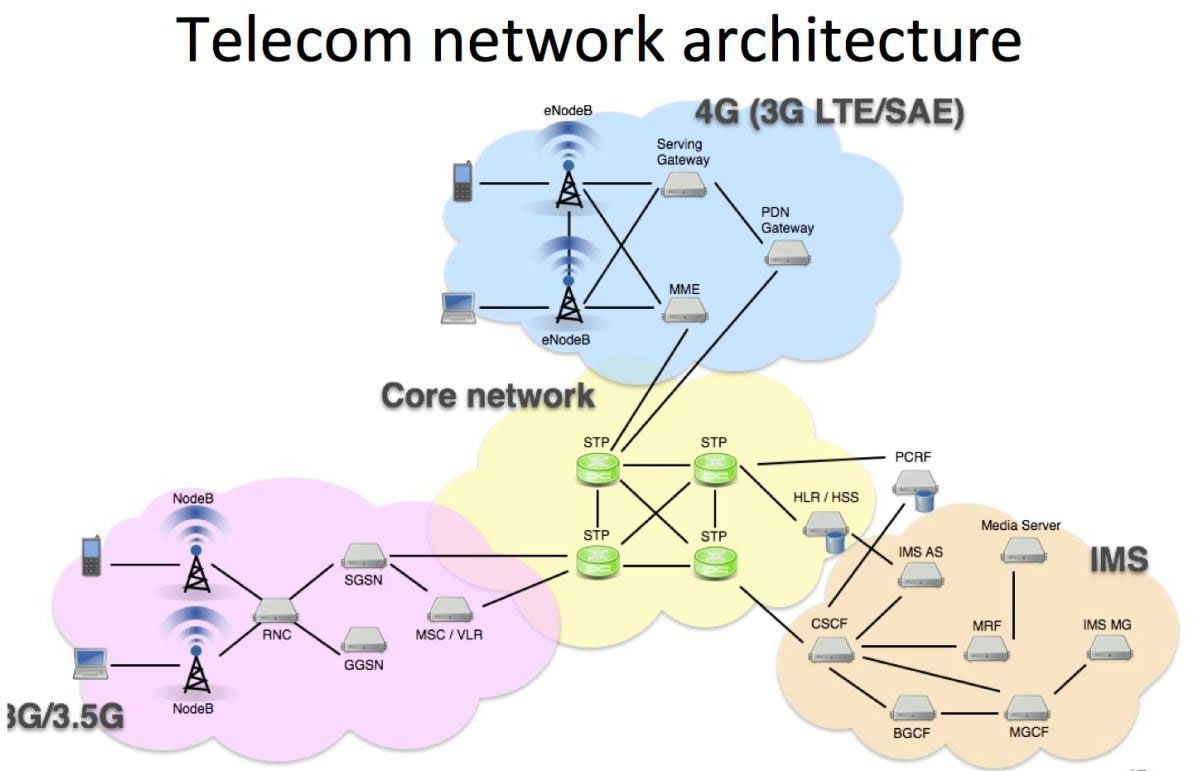
use circuit switching, message switching or packet switching to pass the signal

through the correct links and nodes to reach the correct destination terminal. A telecommunication network is a collection of terminal nodes; links are connected so as to enable telecommunication between the terminals. The transmission links connect the nodes together. The nodes use circuit

Switching, message switching or packet switching to pass the signal through the correct links and nodes to reach the correct destination terminal.

##### Peripherals connected

* DKT2321
* DKT1110
* FCBC
* Digital operator console
* BI instrument



### WIRELESS COMMUNICATION

Wireless communication involves the transmission of information over a distance without the help of wires, cables or any other forms of electrical conductors.

Wireless communication is a broad term that incorporates all procedures and forms of connecting and communicating between two or more devices using a wireless signal through wireless communication technologies and devices.

### TYPES OF WIRELESS COMMUNICATION

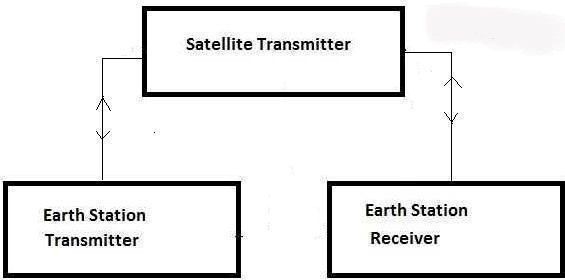
#### SATELLITE COMMUNICATION

A communications satellite is an artificial satellite that relays and amplifies radio telecommunications signals via a transponder; it creates a communication channel between a source transmitter and a receiver at different locations on Earth. Communications satellites are used for television, telephone, radio, internet, and military applications.

Two satellites which are commonly used in satellite communication are Active and passive satellites.

**Passive satellites:** It is just a plastic balloon having a metal coated over it. This sphere reflects the coming microwave signals coming from one part of the earth to other part. This is also known as passive sphere. Our earth also has a passive satellite i.e. moon.

**Active satellites:** It basically does the work of amplifying the microwave signals coming. In active satellites an antenna system, transmitter, power supply and a receiver is used. These satellites are also called as transponders. The transmitters fitted on the earth generate the microwaves. These rays are received by the transponders attached to the satellite. Then after amplifying, these signals are transmitted back to earth. This sending can be done at the same time or after some delay. These amplified signals are stored in the memory of the satellites, when earth properly faces the satellite. Then the satellite starts sending the signals to earth. Some active satellites also have programming and recording features. The signals coming from the satellite when reach the earth, are of very low intensity. Their amplification is done by the receivers themselves



### INFRARED COMMUNICATION

Infrared wireless communication communicates information in a device or systems through IR radiation. IR is electromagnetic energy at a wavelength that is longer than that of red light. It is used for security control, TV remote control and short range communications. In the electromagnetic spectrum, IR radiation lies between microwaves and visible light. So, they can be used as a source of communication.

For a successful infrared communication, a photo LED transmitter and a photo diode receptor are required. The LED transmitter transmits the IR signal in the form of non visible light, that is captured and saved by the photoreceptor. So the information between the source and the target is transferred in this way.

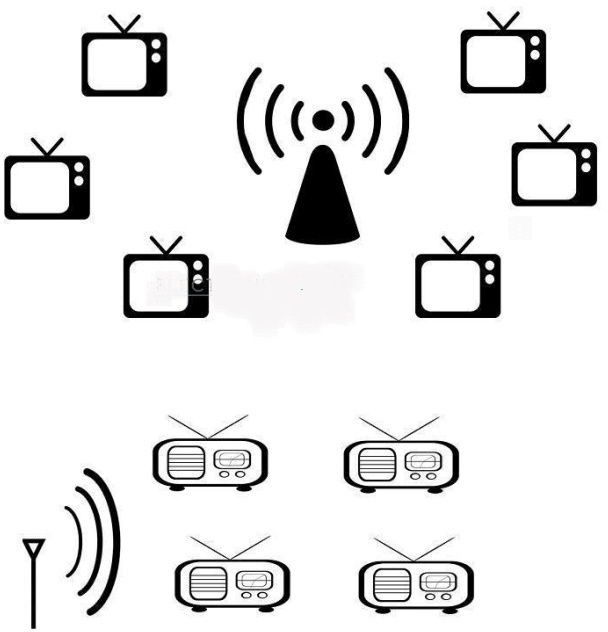


### BROADCAST RADIO

Handy multichannel radios permit a user to speak over short distances, whereas citizen’s band and maritime radios offer communication services for sailors. Ham radio enthusiasts share data and function emergency communication aids throughout disasters with their powerful broadcasting gear, and can even communicate digital information over the radio frequency spectrum.

Mostly an audio broadcasting service, radio broadcasts sound through the air as radio waves. Radio uses a transmitter which is used to transmit the data in the form of radio waves to a receiving antenna. To broadcast common programming, stations are associated with the radio NƒW’s. The broadcast happens either in simulcast or syndication or both. Radio broadcasting may be done via cable FM, the net and satellites. A broadcast sends information over long distances at up to two megabitsƒSec (AMƒFM Radio).

For example, you can take a radio station. When the RJ says you are listening to 92.7 BIG FM, what he really means is that signals are being broadcasted at a frequency of

92.7megahertz, that successively means the transmitter at the station is periodic at a

frequency of 92.700,000 Cyclesƒsecond.

### MICROWAVE COMMUNICATION

Microwave wireless communication is an effective type of communication, mainly this transmission uses radio waves, and the wavelengths of radio waves are measured in centimeters. Stations on the earth send and receive data signals from the satellite with a frequency ranging from 11GHz−14GHz and with a transmission speed of 1Mbps to 10Mbps.



### BLUETOOTH TECHNOLOGY

The main function of the Bluetooth technology is that permits you to connect a various electronic devices wirelessly to a system for the transferring of data. Cell phones are connected to hands free earphones, mouse, wireless keyboard.

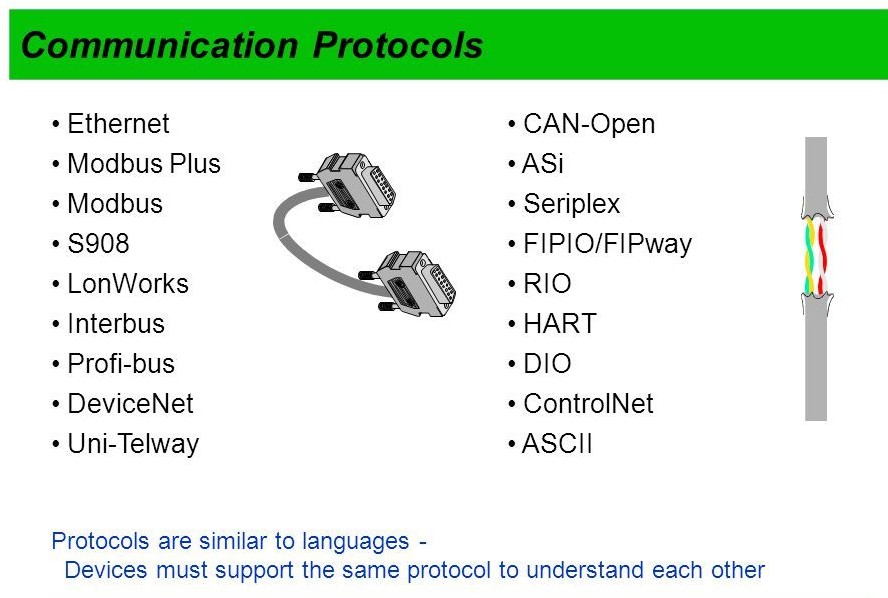
When two Bluetooth devices want to talk to each other, they need to pair. Communication between Bluetooth devices happens over short−range, ad hoc networks known as piconets.

A piconet is a network of devices connected using Bluetooth technology. When a network is established, one device takes the role of the master while all the other devices act as slaves



### PROTOCOL COMMUNICATIONS

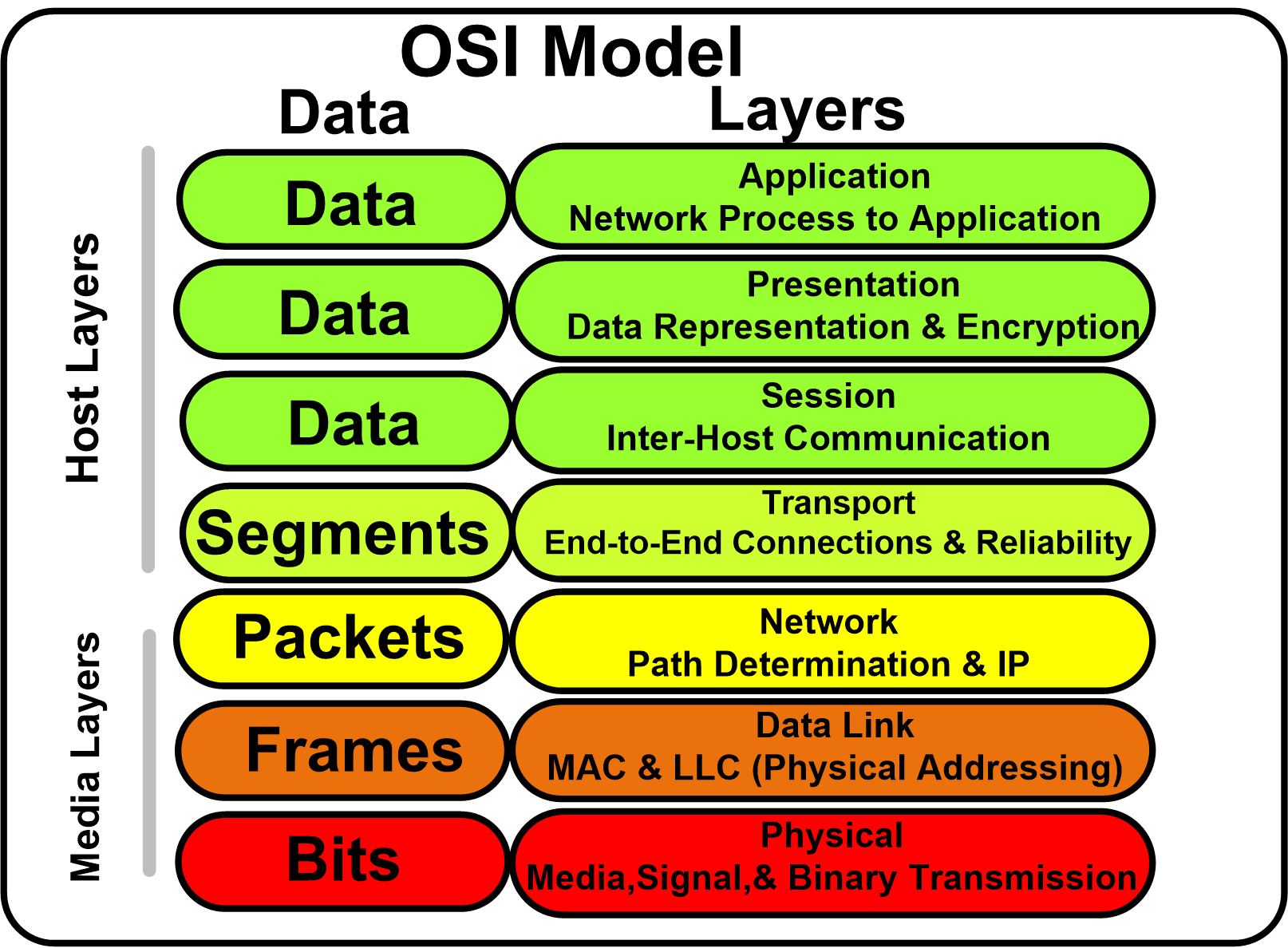
A communications protocol defines the rules for sending blocks of data (each known as a Protocol Data Unit (PDU)) from one node in a network to another node. Protocols are normally defined in a layered manner and provide all or part of the services specified by a layer of the OSI reference model. A protocol specification defines the operation of the protocol and may also suggest how the protocol should be implemented.



### OSI LAYER MODEL

The Open Systems Interconnection (OSI) model defines a networking framework to implement protocols in layers, with control passed from one layer to the next. It conceptually divides computer network architecture into 7 layers in a logical progression. These are:

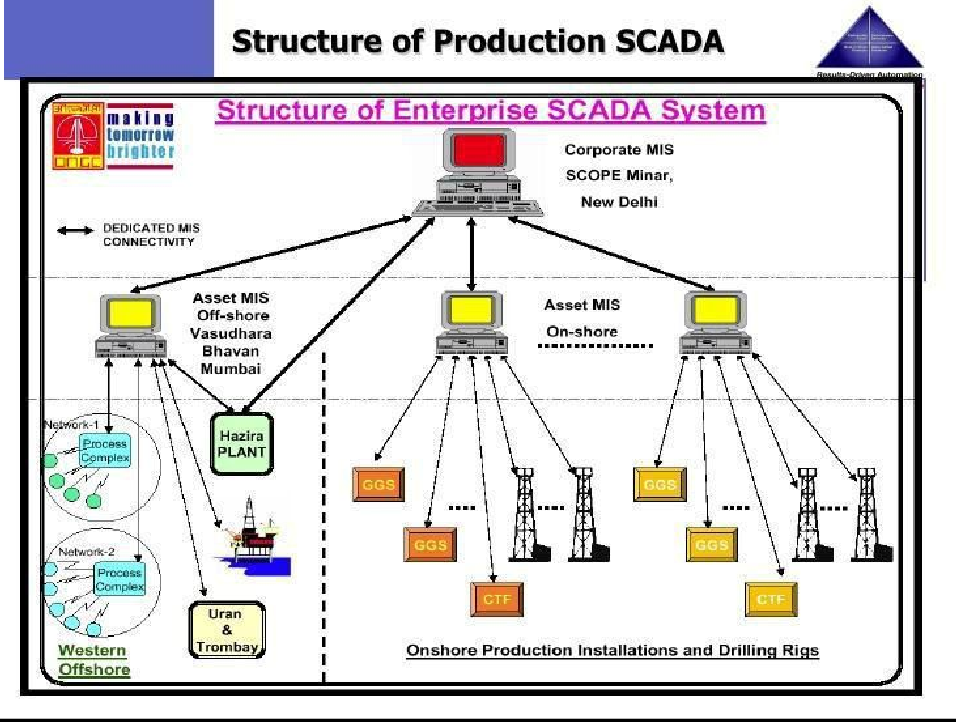
1. **Physical layer:** It is responsible for ultimate transmission of digital data bits from the Physical layer of the sending (source) device over network communications media to the Physical layer of the receiving (destination) device. Examples are Ethernet cables and Token− ring network.
2. **Data link layer:** When obtaining data from the Physical layer, the Data Link layer checks for physical transmission errors and packages bits into data "frames". It is often divided into two parts, the "Media Access Control" sub layer and the "Logical Link Control" sub layer.
3. **Network layer:** When data arrives at the Network layer, the source and destination addresses contained inside each frame are examined to determine if the data has reached its final destination. If the data has reached the final destination, this Layer 3 formats the data into packets delivered up to the Transport layer. Otherwise, the Network layer updates the destination address and pushes the frame back down to the lower layers.
4. **Transport layer:** The Transport Layer delivers data across network connections.
5. **Session layer:** The Session Layer manages the sequence and flow of events that initiate and tear down network connections.
6. **Presentation layer:** it handles syntax processing of message data such as format conversions and encryption ƒ decryption needed to support the Application layer above it.
7. **Application layer:** The Application layer supplies network services to end−user applications. Network services are typically protocols that work with user's data.



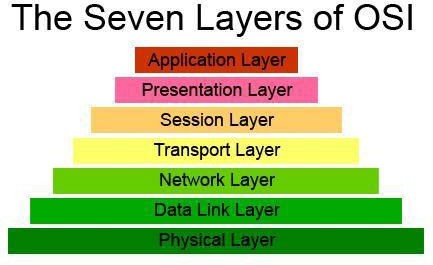
### SCADA (Supervisory Control And Data Acquisition) INTRODUCTION TO SCADA:

Supervisory control and data acquisition (SCADA) is a control system architecture that uses computers, networked data communications and graphical system interfaces for highlevel process supervisory management, but uses other peripheral devices such as programmable logic controllers and discrete PID controllers to interface to the process plant or machinery. The operator interfaces which enable monitoring and the issuing of process commands, such as controller set point changes, are handled through the SCADA supervisory computer system. However, the real−time control logic or controller calculations are performed by networked modules which connect to the field sensors and actuators.

The SCADA concept was developed as a universal means of remote access to a variety of local control modules, which could be from different manufacturers allowing access through standard automation protocols. In practice, large SCADA systems have grown to become

very similar to distributed control system in function, but using multiple means of

interfacing with the plant. They can control large−scale processes that can include multiple sites, and work over large distances. It is one of the most commonly−used types of industrial control system; however there are concerns about SCADA systems being vulnerable to cyber warfareƒcyber terrorism attacks.



### DESCRIPTION OF SCADA

The key attribute of a SCADA system is its ability to perform a supervisory operation over a variety of other proprietary devices.

The accompanying diagram is a general model which shows functional manufacturing levels using computerized control.

Referring to the diagram,

* Level 0 contains the field devices such as flow and temperature sensors, and final control elements, such as control valves.
* Level 1 contains the industrialized inputƒoutput (IƒO) modules, and their associated distributed electronic processors.
* Level 2 contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.
* Level 3 is the production control level, which does not directly control the process, but is concerned with monitoring production and targets.
* Level 4 is the production scheduling level.

**Level 1** contains the programmable logic controllers (PLCs) or remote terminal units (RTUs).

**Level 2** contains the SCADA software and computing platform. The SCADA software exists only at this supervisory level as control actions are performed automatically by RTUs or PLCs. SCADA control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process to a set point level, but the SCADA system software will allow operators to change the set points for the flow. The SCADA also enables alarm conditions, such as loss of flow or high temperature, to be displayed and recorded. A feedback control loop is directly controlled by the RTU or PLC, but the SCADA software monitors the overall performance of the loop.

**Levels 3 and 4** are not strictly process control in the traditional sense, but are where production control and scheduling takes place.

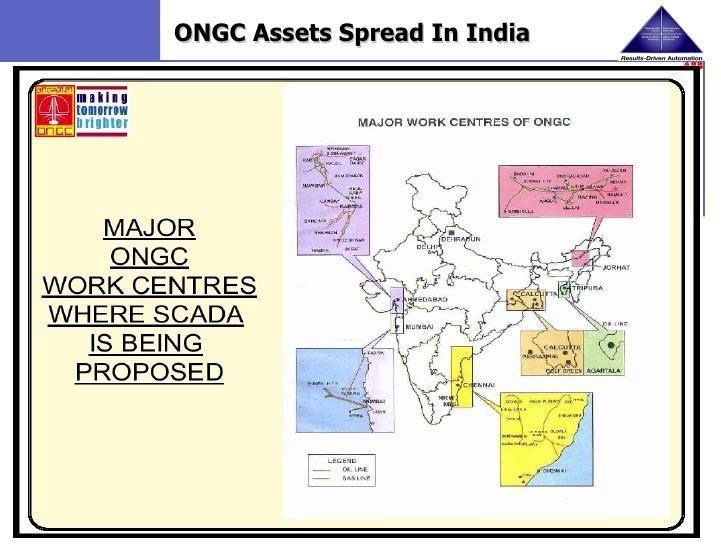
Data acquisition begins at the RTU or PLC level and includes instrumentation readings and equipment status reports that are communicated to level 2 SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI (Human Machine Interface) can make supervisory decisions to adjust or override normal RTU (PLC)

controls. Data may also be fed to a historian, often built on a commodity database management system, to allow trending and other analytical auditing.

SCADA systems typically use a tag database, which contains data elements called tags or points, which relate to specific instrumentation or actuators within the process system according to such as the piping and instrumentation program. Data is accumulated against these unique process control equipment tag references.

### ROLES/RESPONSIBILITIES OF SCADA

1. A SCADA system when applied properly helps industries to save time and money.
2. SCADA helps in the elimination of the need for site visits by the company personal for inspection adjustments and data collection.
3. SCADA software enables the user to monitor the operations in real time.
4. It can also make modifications to the system,auto−generate reports and troubleshoot.
5. The initial cost of software installation is high but once the system is installed, it reduces operation cost and improves the efficiency of the setup.
6. SCADA system are equipped to make the immediate corrections in the operating systems, so they can increase the life−period of the equipment in use and save on the need for costly repairs.
7. It also translates into man−hours saved and personal enabled to focus on tasks that require human involvement.
8. Further, the auto− generated reporting system ensures compliance with regulatory principles.
9. Drilling SCADA provides a set of productivity tools to the management through−
   1. Historical trends (time, depth base etc.)
   2. Database and data archiving
   3. Simultaneous availability of data to the driller, tool pusher, geologist and chemist.
   4. Reliability of data through tamper proof system.



### SYSTEM ANALYSIS OF SCADA

Level 1 contains the programmable logic controllers (PLCs) or remote terminal units (RTUs).

Level 2 contains the SCADA software and computing platform. The SCADA software exists only at this supervisory level as control actions are performed automatically by RTUs or PLCs. SCADA control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process to a set point level, but the SCADA system software will allow operators to change the set points for the flow. The SCADA also enables alarm conditions, such as loss of flow or high temperature, to be displayed and recorded. A feedback control loop is directly controlled by the RTU or PLC, but the SCADA software monitors the overall performance of the loop.

Levels 3 and 4 are not strictly process control in the traditional sense, but are where production control and scheduling takes place.

Data acquisition begins at the RTU or PLC level and includes instrumentation readings and equipment status reports that are communicated to level 2 SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI (Human Machine Interface) can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a historian, often built on a commodity database management system, to allow trending and other analytical auditing.

SCADA systems typically use a tag database, which contains data elements called tags or points, which relate to specific instrumentation or actuators within the process system according to such as the Piping and instrumentation diagram. Data is accumulated against these unique process control equipment tag references.

### SUPERVISORY COMPUTERS

This is the core of the SCADA system, gathering data on the process and sending control commands to the field connected devices. It refers to the computer and software responsible for communicating with the field connection controllers, which are RTUs and PLCs, and includes the HMI software running on operator workstations. In smaller SCADA systems, the supervisory computer may be composed of a single PC, in which case the HMI is a part of this computer. In larger SCADA systems, the master station may include several HMIs hosted on client computers, multiple servers for data acquisition, distributed software applications, and disaster recovery sites. To increase the integrity of the system the multiple servers will often be configured in a dual−redundant or hot−standby formation providing continuous control and monitoring in the event of a server malfunction or breakdown.

### REMOTE TERMINAL UNITS

Remote terminal units, also known as (RTUs), connect to sensors and actuators in the process, and are networked to the supervisory computer system. RTUs are "intelligent IƒO" and often have embedded control capabilities such as ladder logics in order to accomplish Boolean logic operations.

### PROGRAMMABLE LOGIC CONTROLLER

Also known as PLCs, these are connected to sensors and actuators in the process, and are networked to the supervisory system in the same way as RTUs. PLCs have more sophisticated embedded control capabilities than RTUs, and are programmed in one or more IEC 61131−3 programming languages. PLCs are often used in place of RTUs as field devices because they are more economical, versatile, flexible and configurable.

### COMMUNICATION INFRASTRUCTURE

This connects the supervisory computer system to the remote terminal units (RTUs) and PLCs, and may use industry standard or manufacturer proprietary protocols. Both RTUs and PLCs operate autonomously on the near−real time control of the process, using the last command given from the supervisory system. Failure of the communications network does not necessarily stop the plant process controls, and on resumption of communications, the operator can continue with monitoring and control. Some critical systems will have dual redundant data highways, often cabled via diverse routes.

### HUMAN-MACHINE INTERFACE

The human−machine interface (HMI) is the operator window of the supervisory system. It presents plant information to the operating personnel graphically in the form of mimic diagrams, which are a schematic representation of the plant being controlled, and alarm and event logging pages. The HMI is linked to the SCADA supervisory computer to provide live data to drive the mimic diagrams, alarm displays and trending graphs. In many installations the HMI is the graphical user interface for the operator, collects all data from external devices, creates reports, performs alarming, sends notifications, etc.

Mimic diagrams consist of line graphics and schematic symbols to represent process elements, or may consist of digital photographs of the process equipment overlain with animated symbols.

Supervisory operation of the plant is by means of the HMI, with operators issuing commands using mouse pointers, keyboards and touch screens. For example, a symbol of a pump can show the operator that the pump is running, and a flow meter symbol can show how much fluid it is pumping through the pipe. The operator can switch the pump off from the mimic by a mouse click or screen touch. The HMI will show the flow rate of the fluid in the pipe decrease in real time.

The HMI package for a SCADA system typically includes a drawing program that the operators or system maintenance personnel use to change the way these points are represented in the interface. These representations can be as simple as an on−screen traffic light, which represents the state of an actual traffic light in the field, or as complex as a multiprojector display representing the position of all of the elevators in a skyscraper or all of the trains on a railway.

A "historian", is a software service within the HMI which accumulates time−stamped data, events, and alarms in a database which can be queried or used to populate graphic trends in the HMI.

# SCADA FOR DRILLING RIGS

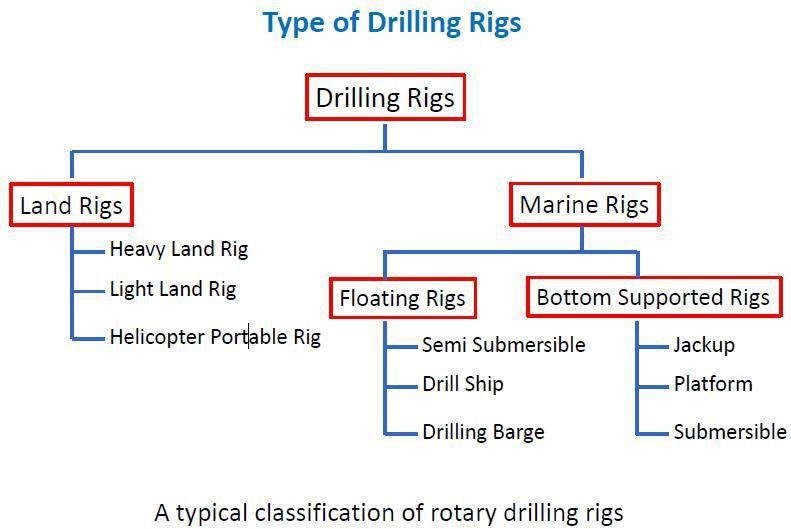
### OBJECTIVE

To ensure efficient monitoring of all drilling activities in the real time domain and also facilitate office analysis of valuable drilling data. The drilling rigs are used for drilling developmental and exploratory locations. Drilling rig instrumentation is a versatile tool of the driller which enables him to see what his eyes can’t see and reach where his hands can’t reach. Efficient real−time monitoring through systems, like drilling SCADA, can contribute

greatly in efficient and cost effective operations. The server for drilling SCADA is located at IDT Dehradun.

### Drilling parameters being monitored:

* + 1. Hock load, bit weight, bit position.
    2. In slips
    3. Rate of penetration, depth of hole, bit depth.
    4. Drill pipe rotary rate and torque.
    5. Active mud tank volume, trip tank volume, Gainƒloss.
    6. Return mud flow
    7. Pump rate, total strokes 8. Mud pressure.



### APPLICATIONS OF DRILLING SCADA

1. Real time display of all parameters.
2. Gas shows
3. Monitoring of Bit record
4. Daily drilling report
5. Quick access to important drilling information
6. Drilling break determination
7. Well kick identification
8. AudioƒVisual alarms for mud loss and circulating pressure loss
9. On line real time data acquisition and processing of all scientific parameters.
10. Online retrieval of data as log of either time or depth or both.

### SCADA ARCHITECTURE

**FIRST GENERATION: “MONOLITHIC”**

Early SCADA system computing was done by large minicomputers. Common network services did not exist at the time SCADA was developed. Thus SCADA systems were independent systems with no connectivity to other systems. The communication protocols used were strictly proprietary at that time. The first−generation SCADA system redundancy was achieved using a back−up mainframe system connected to all the Remote Terminal Unit sites and was used in the event of failure of the primary mainframe system. Some first generation SCADA systems were developed as turnkey operations that ran on minicomputers such as the PDP−11 series made by the Digital Equipment Corporation.

### SECOND GENERATION: “DISTRIBUTED”

SCADA information and command processing was distributed across multiple stations which were connected through a LAN. Information was shared in near real time. Each station was responsible for a particular task, which reduced the cost as compared to First Generation SCADA. The network protocols used were still not standardized. Since these protocols were proprietary, very few people beyond the developers knew enough to determine how secure a SCADA installation was. Security of the SCADA installation was usually overlooked.

### THIRD GENERATION: “NETWORKED”

Similar to a distributed architecture, any complex SCADA can be reduced to simplest components and connected through communication protocols. In the case of a networked design, the system may be spread across more than one LAN network called a process control network (PCN) and separated geographically. Several distributed architecture SCADAs running in parallel, with a single supervisor and historian, could be considered a network architecture. This allows for a more cost effective solution in very large scale systems.

### FOURTH GENERATION: “INTERNET OF THINGS”

With the commercial availability of cloud computing, SCADA systems have increasingly adopted internet of things technology to significantly reduce infrastructure costs and

increase ease of maintenance and integration. As a result, SCADA systems can now report state in near real−time and use the horizontal scale available in cloud environments to implement more complex control algorithms than are practically feasible to implement on traditional programmable logic controllers. Further, the use of open network protocols such as TLS inherent in the Internet of things technology, provides a more readily comprehensible and manageable security boundary than the heterogeneous mix of proprietary network protocols typical of many decentralized SCADA implementations. One such example of this technology is an innovative approach to rainwater harvesting through the implementation of real time controls (RTC) . This decentralization of data also requires a different approach to SCADA than traditional PLC based programs. When a SCADA system is used locally, the preferred methodology involves binding the graphics on the user interface to the data stored in specific PLC memory

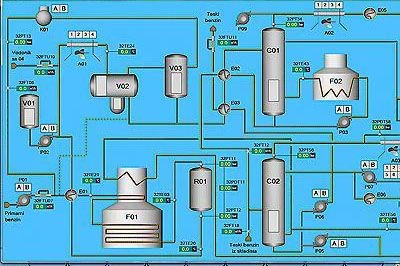
### SCADA FOR PRODUCTION OBJECTIVE

This fully integrated SCADA system acquires real time production data from different production and drilling installations, which, apart from efficient day to day operations, shall also use for supporting Scientific and Business decisions.

Production and Drilling information is required by different organizational, scientific as well as business functional groups and managers in respective Assets and Basins. This information is vital for planning and coordination of all E&P activities. Availability of on−line information shall result in timely and informed scientific and business decisions. The server for production SCADA is located at Delhi.

### The Tier-1 has following facilities:

1. Gas Gathering Stations(GCS)
2. Gas collecting Stations(GCS)
3. Central Tank Farm(CTF)
4. Effluent Treatment Plant(ETP)
5. Central Processing Facility(CPF)
6. Early Production System(EPS)
7. Gas Compressor Plant(GCP)
8. Water Injection Plant(WIP).



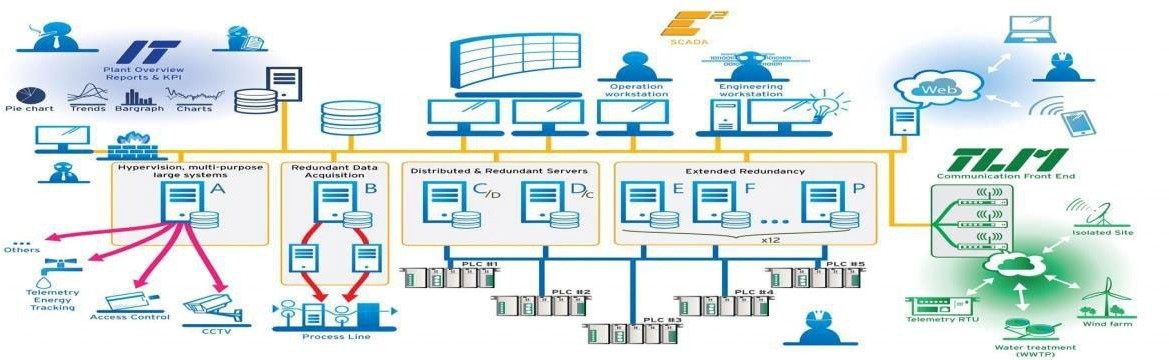
### Production parameters being monitored at GCS:

1. Flowing status for high producing Well Flow Line.
2. Pressure of Group Header
3. Test Gas Meter(PT,DPT,TT)
4. Test Liquid Meter(Tank Level)
5. Group Gas Meter(PT,DPT,TT)
6. GCS Group separator Liquid Meter
7. Flare Gas Meter
8. Mass Flow Meter(eg:−Coriolis Mass Flow Meter)
9. Level of all Tanks
10. Pumps on−off status.

However, when the data comes from a disparate mix of sensors, controllers and databases (which may be local or at varied connected locations), the typical 1 to 1 mapping becomes problematic. A solution to this is data modeling, a concept derived from object oriented programming.

In a data model, a virtual representation of each device is constructed in the SCADA software. These virtual representations (“models”) can contain not just the address mapping of the device represented, but also any other pertinent information (web based info, database entries, media files, etc.) that may be used by other facets of the SCADAƒIoT implementation. As the increased complexity of the Internet of things renders traditional

SCADA increasingly “house−bound,” and as communication protocols evolve to favor platform−independent, service−oriented architecture (such as OPC UA), it is likely that more SCADA software developers will implement some form of data modeling.



### ARCHITECTURE OF VSAT NETWORK

VSAT has been chosen as the effective means of communication in between the various tiers of SCADA because it is the most suitable and viable means for the SCADA system.

##### The VSAT network has two main ports:-

1. Hub Station
2. Remote station

##### Any satellite system can broadly be subdivided into three subsystems:

1. Antenna
2. RFƒIF units
3. Broadband

### It consists of:

**HUB STATION**

1. Satellite Antenna
2. Low Noise Amplifier(LNA)
3. High Power Amplifier(HPA)
4. Up converter & Diwn converter
5. VoiceƒData MUX
6. Digital Modem
7. Network Management System(NMS)

**REMOTE TERMINAL**

#### The VSAT terminal consists of:

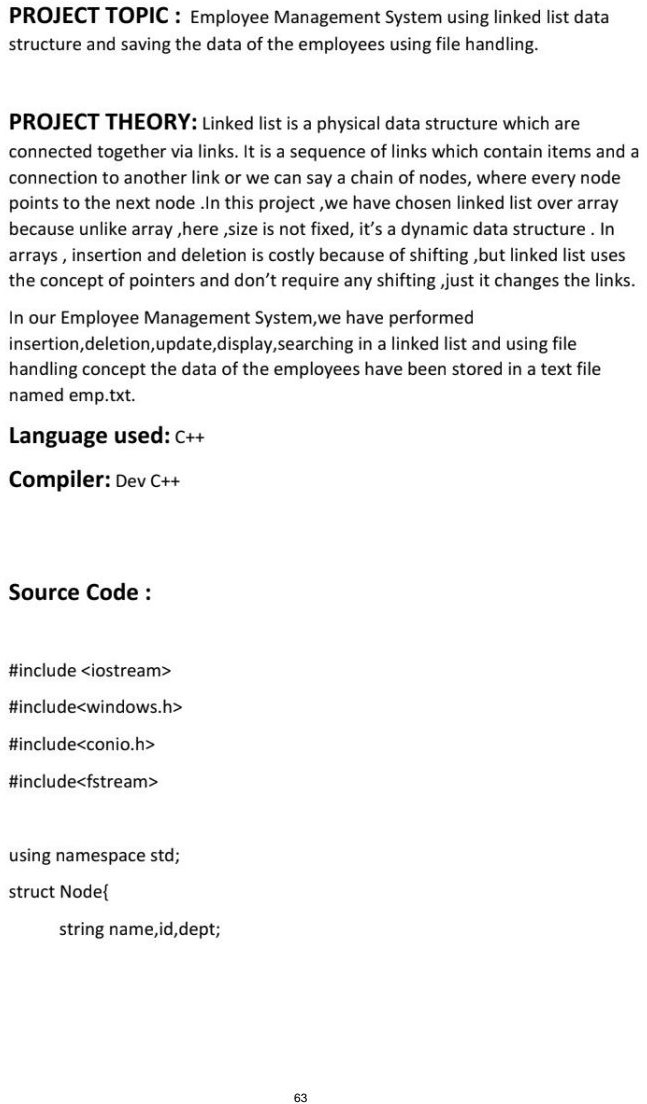
1. Off−set antenna
2. RF Out Door Unit(ODU)
3. IF In Door Unit(IDU)

The Network Management System(NMS) for centralized control of VSAT’s from hub station works on exclusive channel. The VSAT−NMS is microprocessor based. It interacts with various sub−systems and communicates continuously with Hub NMS.

#### BENEFITS OF VSAT NETWORK:

1. Being a modern telecom technology it is suitable for a large country and with areas of difficult terrain.
2. The user incurs a fixed cost per VSAT services, irrespective of distance.
3. Transmission of huge data in less time across long distances is feasible.
4. The cost of expansion is not dependent on distance.
5. It is more reliable, the call completion rate is very high (99.5 %).
6. Communication need not pass through ground facilities.





int sal;

struct Node \*next;

}\*head=NULL

void update(){

struct Node \*p=head;

if(p==NULL)return;

int f=0;

string id1;

cout<<"Enter id of employee you want to update: ";

cin>>id1;

while(p!=NULL){

if(p->id==id1){

f=1;

cout<<"Enter the new details of the employee: "<<endl;

string namen,idn,deptn;

int saln;

cout<<"enter new name: ";

cin>>namen;

cout<<"enter new id: ";

cin>>idn;

cout<<"enter new dept: ";

cin>>deptn;

cout<<"enter new salary: ";

cin>>saln;

p->name=namen;

p->id=idn;

p->dept=deptn;

p->sal=saln;

break;

}

else{

p=p->next;

}

}

if(!f)cout<<"Id not found!"<<endl;

}

void Delete(){

struct Node \*p=head,\*r=NULL;

string id1;

cout<<"Enter id of employee you want to delete: ";

cin>>id1;

if(p!=NULL && p->id==id1){

head=p->next;

delete p;

return;

}

else{

while(p!=NULL&& p->id!=id1 ){

r=p;

p=p->next;

}

if(p==NULL)return;

r->next=p->next;

delete p;

}

}

void search(){

struct Node \*p=head;

if(p==NULL)return;

int f=0;

string id1;

cout<<"Enter id of employee to search: ";

cin>>id1;

while(p!=NULL){

if(p->id==id1){

f=1;

cout<<"Name: "<<p->name<<endl;

cout<<"id: "<<p->id<<endl;

cout<<"dept: "<<p->dept<<endl;

cout<<"Sal: "<<p->sal<<endl;

cout<<"\n\n";

break;

}

else{

p=p->next;

}

}

if(!f)cout<<"Invalid id!"<<endl;

}

void writetofile(){

Node\* p=head;

ofstream outfile;

outfile.open("emp.txt",ios::app);

if(head==NULL)cout<<"No nodes";

else{

outfile<<"Name\t\t\id\t\tSalary\t\tDept"<<endl;

while(p!=NULL){

outfile<<p->name<<"\t\t"<<p->id<<"\t\t"<<p->sal<<"\t\t"<<p- >dept<<endl;

p=p->next;

}

}

outfile.close();

}

void display(){

struct Node \*p=head;

if(p==NULL)cout<<"List is empty: "<<endl;

cout<<"Name\t\t\id\t\tSalary\t\tDept"<<endl;

while(p!=NULL)

{

cout<<p->name<<"\t\t"<<p->id<<"\t\t"<<p->sal<<"\t\t"<<p->dept<<endl;

p=p->next;

}

writetofile();

**CONCLUSION**

Engineering services plays a vital role in the off shore design. It imparts extensive support in the designing and processing of various off shore production taking place in the sea. It looks after a number of various departments and hence its importance can be compared to none when the question of implementing and executing the process comes.

Oil and gas industry thus has a huge role to play not only in the generation of power but as well as blossoming India’s economy. They are the major contributors in Indian economy and hence continuous efforts are being made for their exploration in the near future.

Finally, summing it up I consider myself fortunate to be a part of India’s tycoon company for Oil &Gas Production, though for a short tenure only. I had a great exposure to the oil and gas industry during the training as it continuously facilitated me developing my knowledge to the where−about of oil and gas industry.

## REFERENCES

1. https://www.lifewire.com/NETWORKING/
2. Data Communications and Networking By Behrouz A.Forouzan
3. Mobile Communication By schiller
4. Computer Networks − A Tanenbaum − 5th edition
5. https://[www.elprocus.com/scada](http://www.elprocus.com/scada)−systems−work/