Railnet, Wi-Fi System, PRS, UTS & FOIS (ST-48)

Component of Data Communication

- MESSAGES - The information to be communicated
  - It consists of text, numbers, pictures, sound & video.
- SENDER - Device that sends the message (data).
  - It can be a computer, server, video camera etc.
- RECEIVER - Device that receives the message (data).
  - It can be a computer, server, television.
- MEDIUM - Physical path by which messages travels from sender to receiver.
  - It may be twisted pair, coaxial cable , OFC, radio waves etc.
- PROTOCOLS - Set of rules that governs data communication.
  Protocol represents an agreement between communicating devices.
  - Protocol defines what is communicated, how it is communicated and when it is communicated .

Network classification

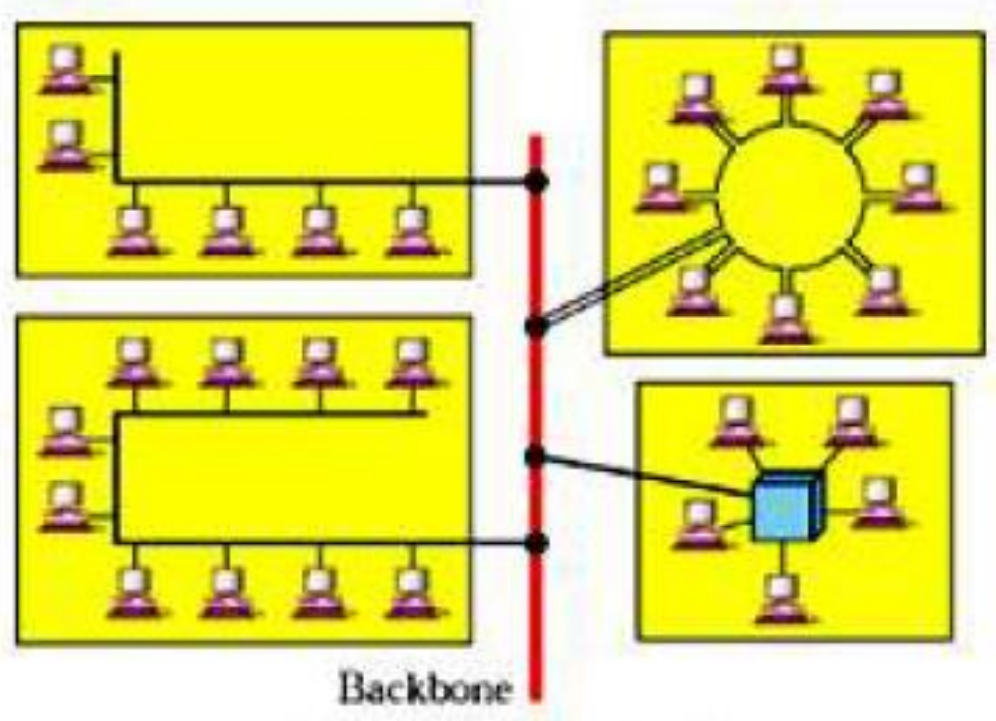
- All Data communication circuits are a combination of various networks.
- Network is a set of devices connected by media links.
- Link may be wired or Wireless

Classification of network (based on physical connections)

(i) LAN - Local Area Network
(ii) MAN- Metropolitan Area Network
(iii) WAN- Wide Area Network

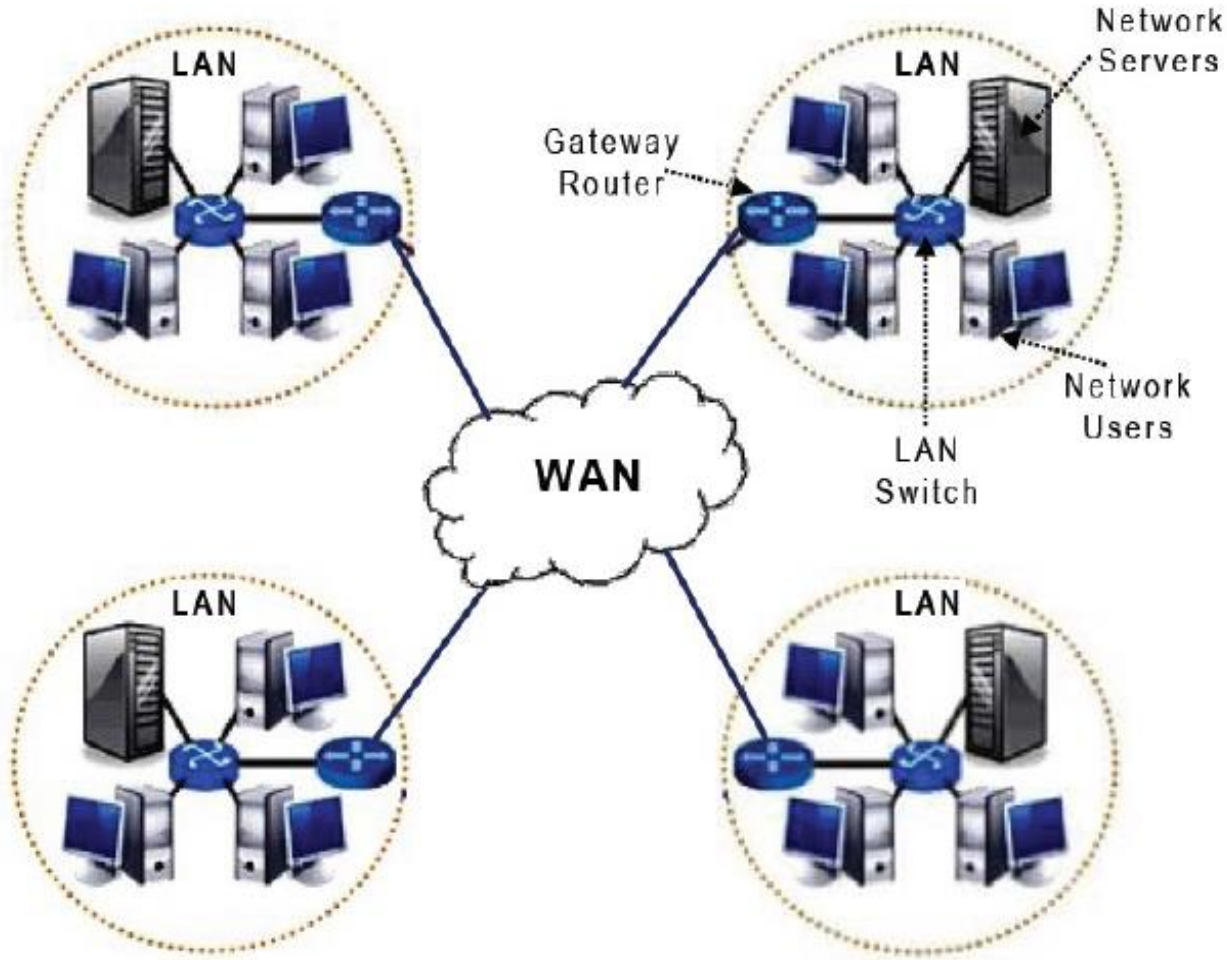
LAN

- Nodes are interconnected within a geographically limited area, such as a building or a campus.
- They transfer data at high speeds (higher bandwidth).
- They exist in a limited geographical area.



WAN

- A wide area network (WAN) interconnects LANs.
- They exist in an unlimited geographical area.
- They usually interconnect multiple LANs.
- They often transfer data at lower speeds (lower bandwidth).



Intranet

- Intranet: Intranet is the system in which multiple PCs are connected to each other.
- PCs in intranet are not available to the world outside the intranet.
- Each computer in Intranet is also identified by an IP Address which is unique among the computers in that Intranet.



Internet

- Internet is a network of networks. It is the worldwide collection of multiple computer networks.
- Internet is a network of thousand of computer networks. It is capable to transfer information across the geographical boundaries in an electronic format at a very fast speed. It is a huge reservoir of information.



Intranet Vs Internet

Intranet	Internet
Private Network	Public Network
Single Network Administrator	No network administrator
Private IP is used	Public IP is used
Limited number of users	Large number of users
Highly secure	Limited security

Network Interface Card (NIC)

- **NIC** provides a hardware interface between a computer and a network.
- NIC allows both wired and wireless communications.
- Provides physical addressing system (MAC) for computer



Switches

- Usually configured with 8, 12, or 24 RJ-45 ports
- Often used in a star or tree topology
- Sold with specialized software for port management
- Also called intelligent HUBS.



Types Of Switches

- Unmanageable switch
- Manageable switch
- Layer-3 switch

Unmanageable switch

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

Manageable switch

- These switches also operate at Layer 2 of the OSI model like unmanageable switch.

- This supports additional functionality and manageability like STP, VLANS, SNMP etc.

- High-end or "enterprise" switches, provide a serial console and command-line access via telnet and SSH, as well as management via SNMP. More recent devices also provide a web interface.

Layer 3 switch

- Layer 3 switch Operates at Layer 3 of the OSI model.

- It has the functionality of switch and router hence works either as a switch or a router based on configuration.

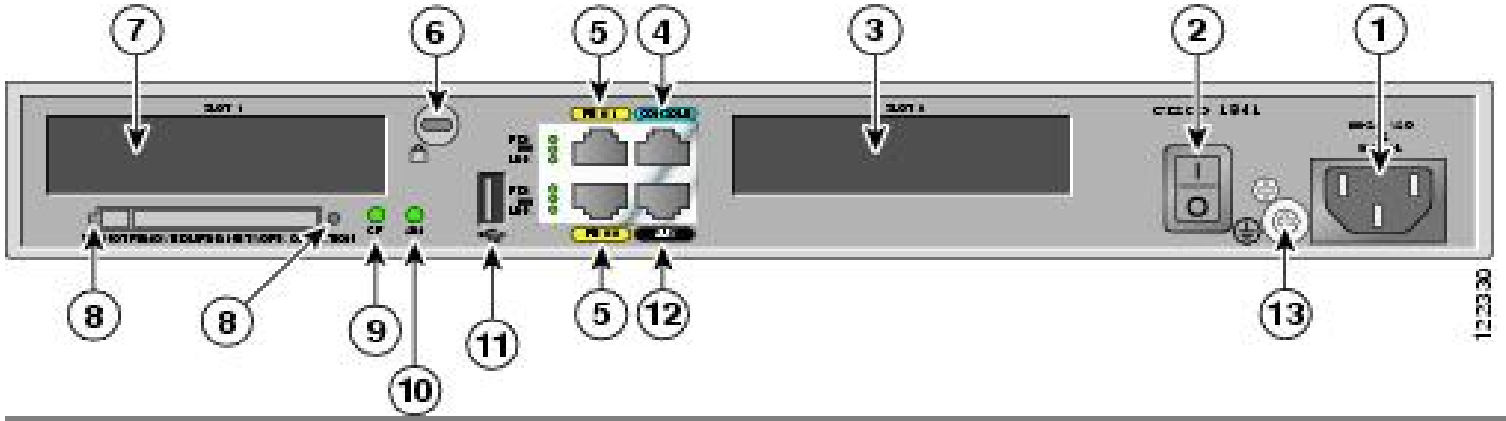
- Layer 3 switches actually differ very little from routers.
- A Layer 3 switch can support the same routing protocols as network routers do.
- The Only difference is, a Layer 3 switch will typically posses only Ethernet interfaces and will not possess any WAN ports.

Routers

- Routers are used to connect remote LANs technologies.
- A router uses a combination of hardware and software to actually "route" data from its source to its destination.
- It works at the network layer (layer 3).



Router’s port details



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

IP Addresses

- IP Address is a Logical Address
- It works on Network Layer (Layer 3)
- Each & every device existing on the network should be given with one IP address
- Two Versions of Address Scheme

(i) IP version 4 (IPv4) – 32 bit address - written Dotted decimal notation Ex- 10.1.2.21

(ii) IP version 6 (IPv6) – 128 bit address –written in Colon-Hex notation Ex- FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

IPv4 Representation

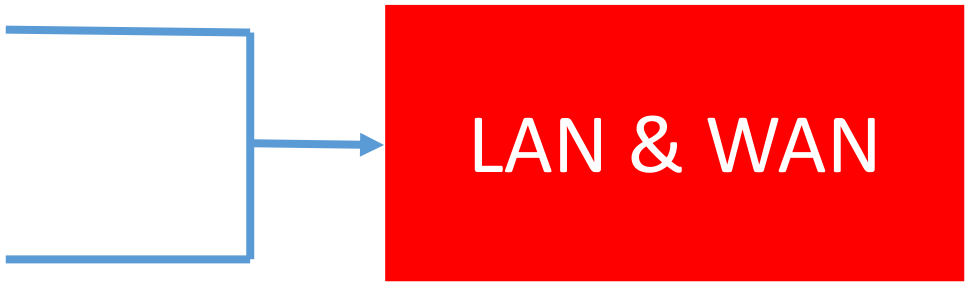
- IPv4 is 32-bit address.
- These 32 bits are shown as 4 octets known as Dotted Decimal Notation
- 1st Octet 2nd Octet 3rd Octet 4th Octet



01010101. 00000101. 10111111. 00000001

IPv4 classification

- Total IP Address Range is 0 . 0 . 0 . 0 to 255.255.255.255
- IPv4 is divided into 5 classes.
- Class A
- Class B
- Class C



- Class D



- Class E

IPv4 classification

IP Class	From	To	Remarks
Class A	0.0.0.0	127.255.255.255	
Class B	128.0.0.0.	191.255.255.255	
Class C	192.0.0.0	223.255.255.255	
Class D	224.0.0.0.	239.255.255.255	
Class E	240.0.0.0	255.255.255.255	

Network ID & Host ID

- IPv4= 32 bits= Network bits + Host bits
- Network bits(NID) determines the subnet mask.
- Subnet mask is used to extract the Network address of IP address.

Network bits/Host bits/Subnet mask

Class of IP	Default Network bits	Default Host bits	Default Format of IP	Default Subnet mask
Class A	8	24	N.H.H.H	255.0.0.0
Class B	16	16	N.N.H.H	255.255.0.0
Class C	24	8	N.N.N.H	255.255.255.0

Default subnet mask

- Class A IP address

  Default Format N.H.H.H

  11111111.00000000.00000000.00000000

  Default Subnet Mask for Class A is 255.0.0.0

- Class B IP address

  Default Format N.N.H.H

  11111111.11111111.00000000.00000000

  Default Subnet Mask for Class B is 255.255.0.0

  Class C IP address

  Default Format N.N.N.H

  11111111.11111111.11111111.00000000

  Default Subnet Mask for Class C is 255.255.255.0

Customized Subnet Mask

- Take an IP address 192.168.1.1 /26
- This is a class C address. Here 26 represents network bits. Although a class C address has 24 default network bits.
- Hence, the customized subnet mask for the given IP is 255.255.255.192
- 192.168.1.1 /27
- Here subnet mask is calculated as 255.255.255.224

Private IP addresses(PIPA)

- Class A 10.0.0.0 to 10.255.255.255
- Class B 172.16.0.0 to 172.31.255.255
- Class C 192.168.0.0 to 192.168.255.255
- These addresses are not routable & invalid over the Internet.
- They can be used for: LAN, Private Networks, home & office networks, ATM machines, networks not connected to Internet.

Public Vs Private IP

Public IP	Private IP
1. Used on the internet (i.e Public network)	Used within the Organization (i.e Private network or LAN)
2. It should be unique over the internet.	It should be unique within the LAN.
3. Assigned by the Internet Service provider(ISP)	Assigned by the Network administrator

Reserved or Special IPv4

- Universal Loopback address - address range of 127.x.x.x

  (address from 127.0.0.0 to 127.255.255.255)

  Used for testing NIC card.

- Universal network - 0.0.0.0 is called universal network address.
- Universal host or universal broadcast address - 255.255.255.255 used for sending the broadcast messages.

Assigning IP addresses to Hosts

- IP address to a host can be assigned in two ways
  (i) Static method -Static IP address is a permanent number assigned to a computer by Network administrator. Assigning static IP addresses is a time consuming job, will burden the Network administrator.

(ii) Dynamic method- Dynamic IP addresses are assigned to a computer by DHCP Server, using DHCP protocol, with no time entire network can be configured.

DHCP -Dynamic Host Configuration Protocol

Need of DHCP

- Every device on a TCP/IP-based network must have a unique IP address.
- IP configuration must be done for
  - all new computers.
  - computers moving from one subnet to another.
  - computers removed from the network.

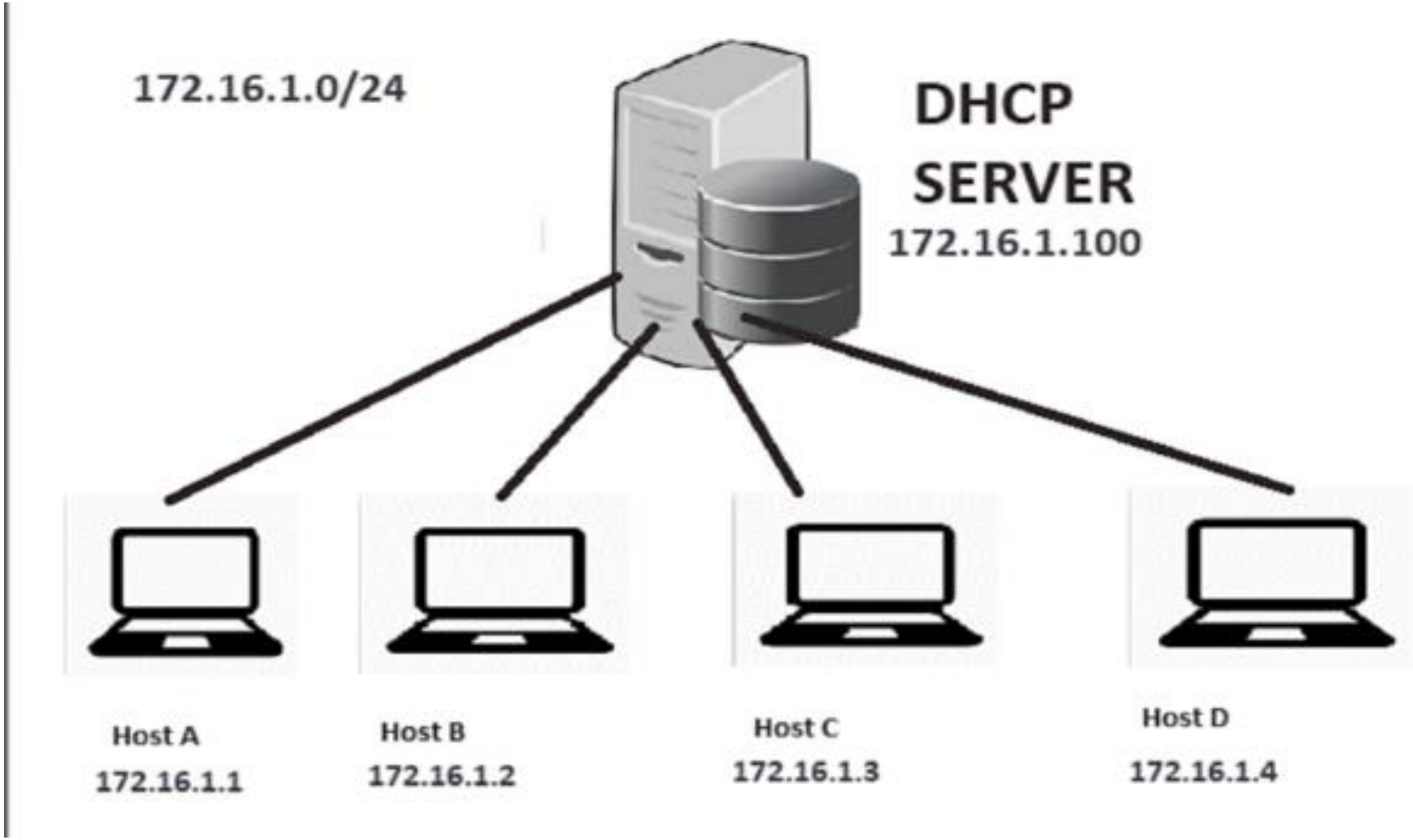


By deploying DHCP in a network, this entire process is automated and centrally managed.

How DHCP works



How DHCP works



DNS(Domain Name System)

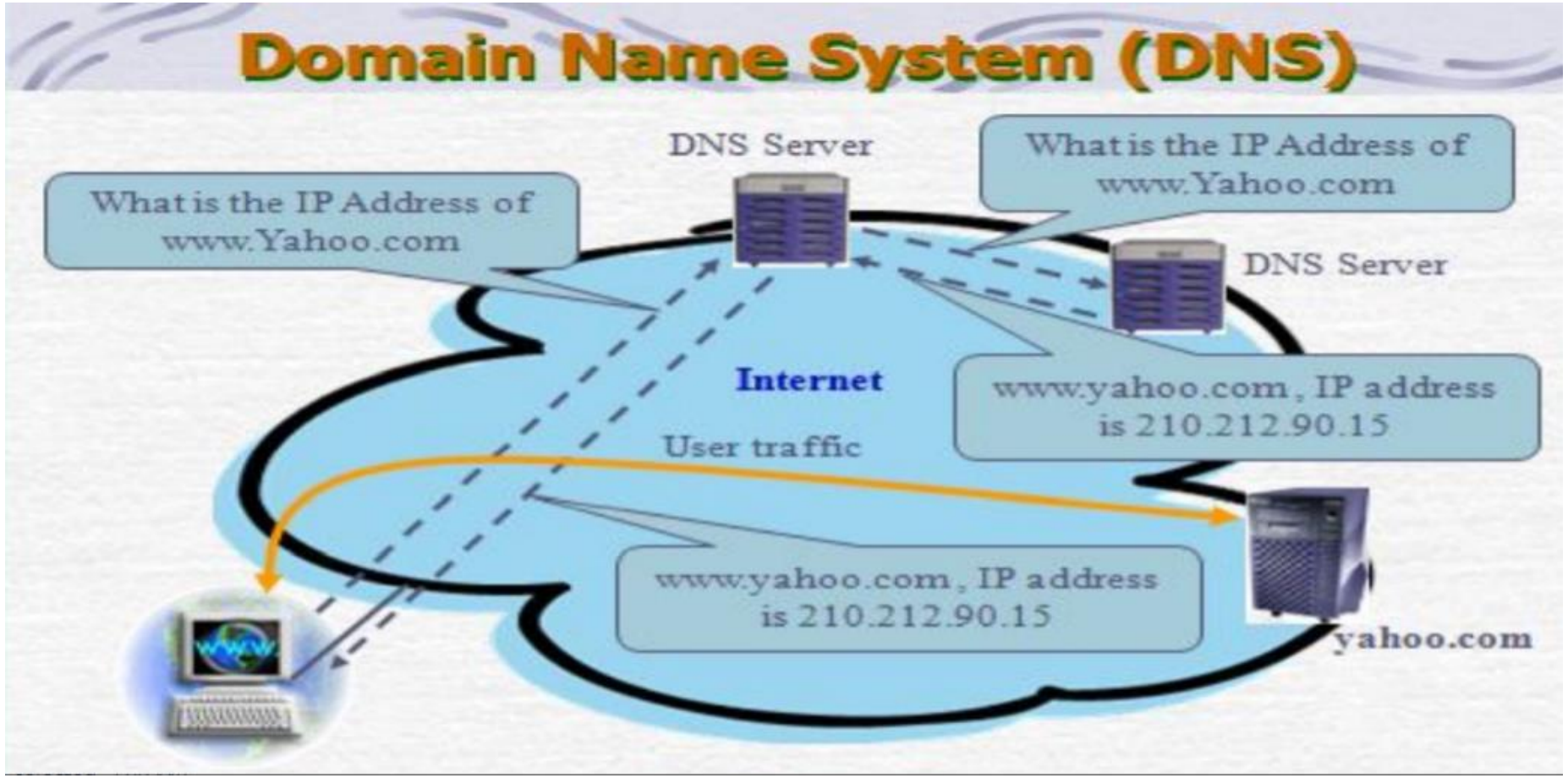
- DNS server resolves URL address into IP address.

- DNS is a mechanism which translates host name to IP address in Internet ▪All the network elements in Internet understand only IP address. To reach a site host name is to be converted to IP address.

▪DNS servers in the Internet search IP address of these host names.

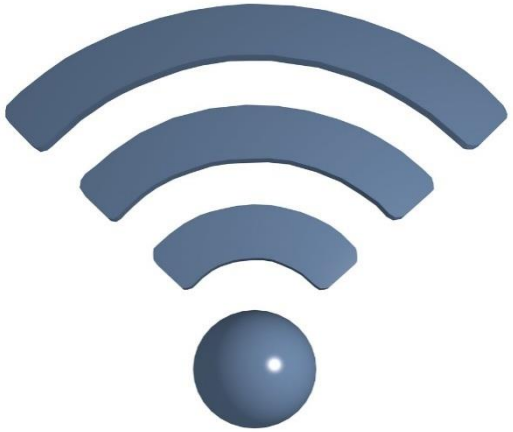
- To access Internet, these DNS servers is maintained by ISPs.

DNS


Domain Name System (DNS)
DNS Server
What is the IP Address of www.Yahoo.com
What is the IP Address of www.Yahoo.com
DNS Server
Internet
www.yahoo.com, IP address is 210.212.90.15
User traffic
www.yahoo.com, IP address is 210.212.90.15
yahoo.com

Wireless LAN (WLAN)

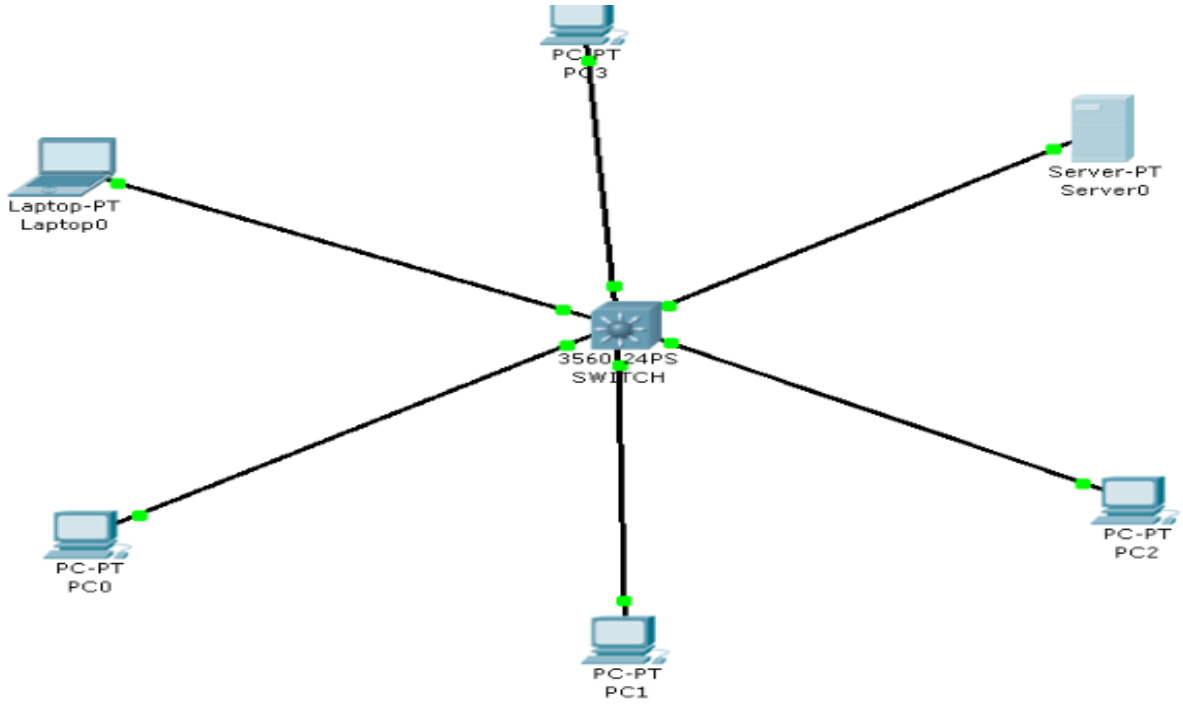
- IEEE standard for WLAN is IEEE 802.11.
- IEEE 802.11 is further divided into various sub-categories depending on frequency band, speed, typical output power, range of coverage etc.



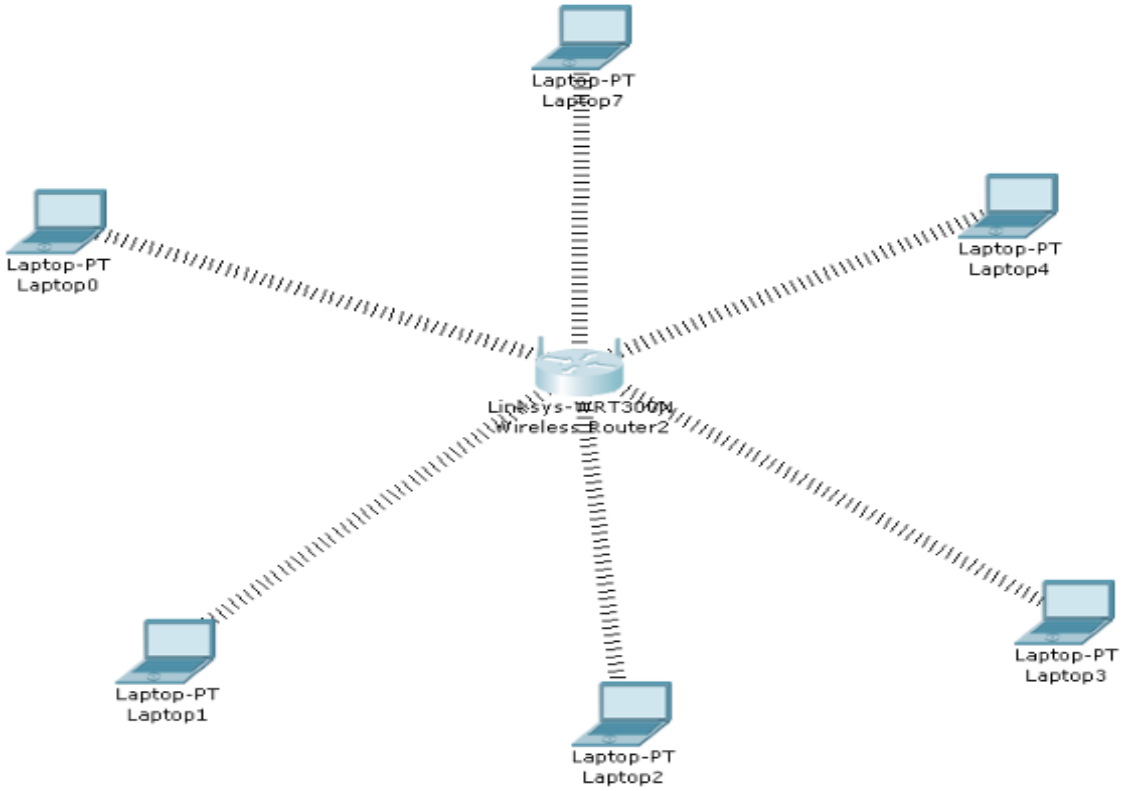
- IEEE 802.11 a - 5.0GHz - 54Mbps
- IEEE 802.11 b - 2.4 GHz - 10Mbps
- IEEE 802.11g - 2.4 GHZ - 54 Mbps
- IEEE 802.11n -2.4 GHz - 300Mbps
- Frequency band used in WLAN is either 2.4GHz or 5GHz band.
- CSMA/CA (Carrier sense Multiple access with collision avoidance) technology is used.
- Modulation techniques used in WLAN are
  Frequency Hopping Spread Spectrum (FHSS) and
  Direct Sequence Spread Spectrum (DSSS)

Wi-fi (Wireless Fidelity)

- In a wired LAN, switches are used to interconnect the computing devices.



- In Wi-Fi or Wireless network, Access Points(APs) are used to interconnect the computing devices.



Wi-Fi (Wireless Fidelity)

- Wi-Fi network can cover an area wherein one can access internet without wire. This coverage area is called Hot-Spots.

- Each “HOT-SPOT” can have number of Access Points (APs) .
- Wi-Fi Components-

  (i) Access Points (AP)

  (ii) Antenna

  (iii) PCI wireless card (peripheral component Interconnect)
  (iv) CAT 6 cable
  (v) Back-bone connectivity

Access Points (AP)

- main component of Wi-Fi systems.

- It converts data into microwave signals.
- It works on 220 V AC.

- It radiates power from 1 mw to 100 mw (0dBm to +20 dBm)

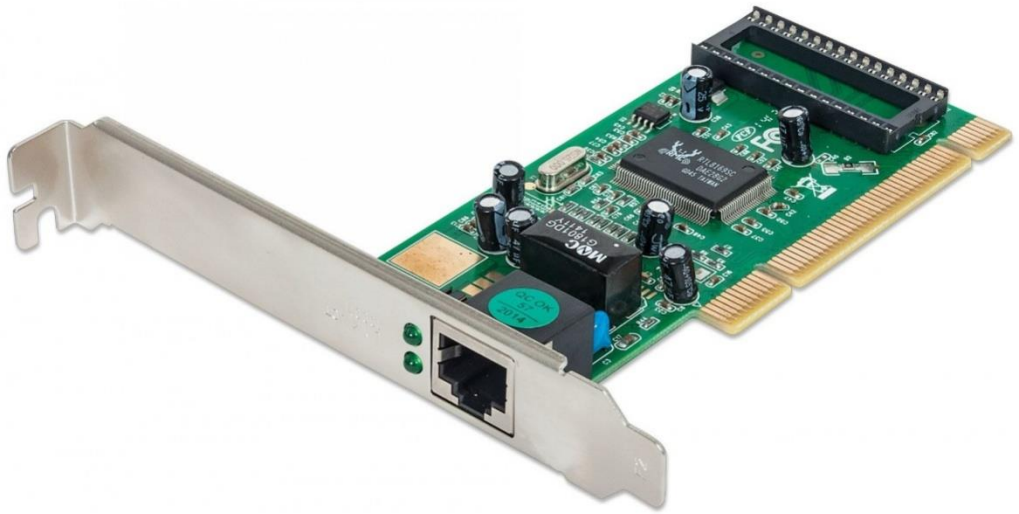


- Each AP with 100 mille water power can cover an average 50-100 meters radius depending on obstructions.

Wi-Fi components

- Antenna- There are different types antennas with gains ranging from 1dB to 5dB to suit to the coverage needs.

PCI Wireless Card - This is used for connecting the Computer/ Laptop to the Internet in a Hot Spot.



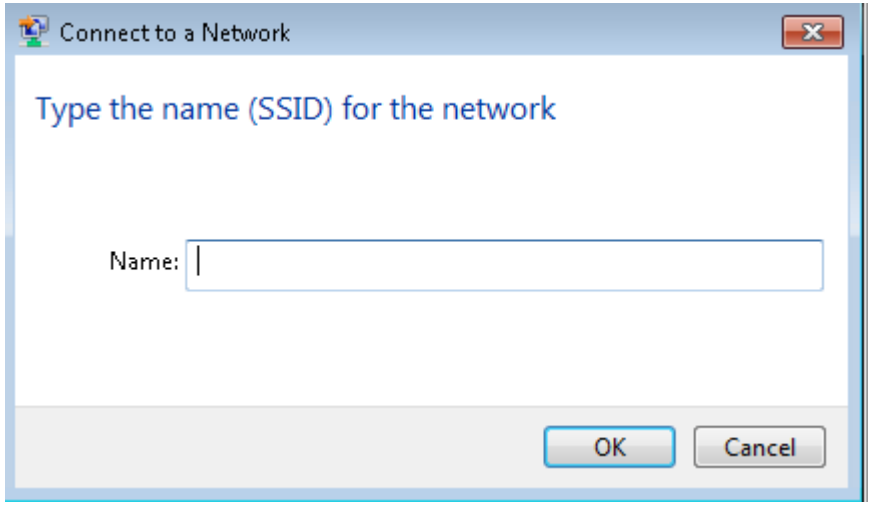
Wi-Fi components

- CAT 6 Cable - It is a Category 6 twisted pair cable and carry up to 1000 Mbps.
- It is used for connecting the AP to the back haul Network



Wi-fi Parameters

- SSID (Service Set Identifier)- It is a name that identifies a particular wireless LAN
- A client device receives broadcast messages from all access points within range advertising their SSIDs.



Wi-Fi Security



Various Wi-Fi Protocols are

- WEP- Wired Equivalent Privacy, developed in 1999. uses 40-bit encryption key, easily hackable.no longer used
- WPA- Wi-fi Protected Access, uses stronger encryption method called TKIP(Temporal key Integrity Protocol) TKIP dynamically changes its key
- Although WPA is also vulnerable, but WPA is stronger encryption technique than WEP.
- WPA2- provides stronger security than WPA.WPA2 uses AES(advanced encryption standard) as encryption technique.
- Some Wi-Fi routers uses mixed security standard such as WPA2 & WPA
- WPA3- introduced in 2018. – stronger than WPA2

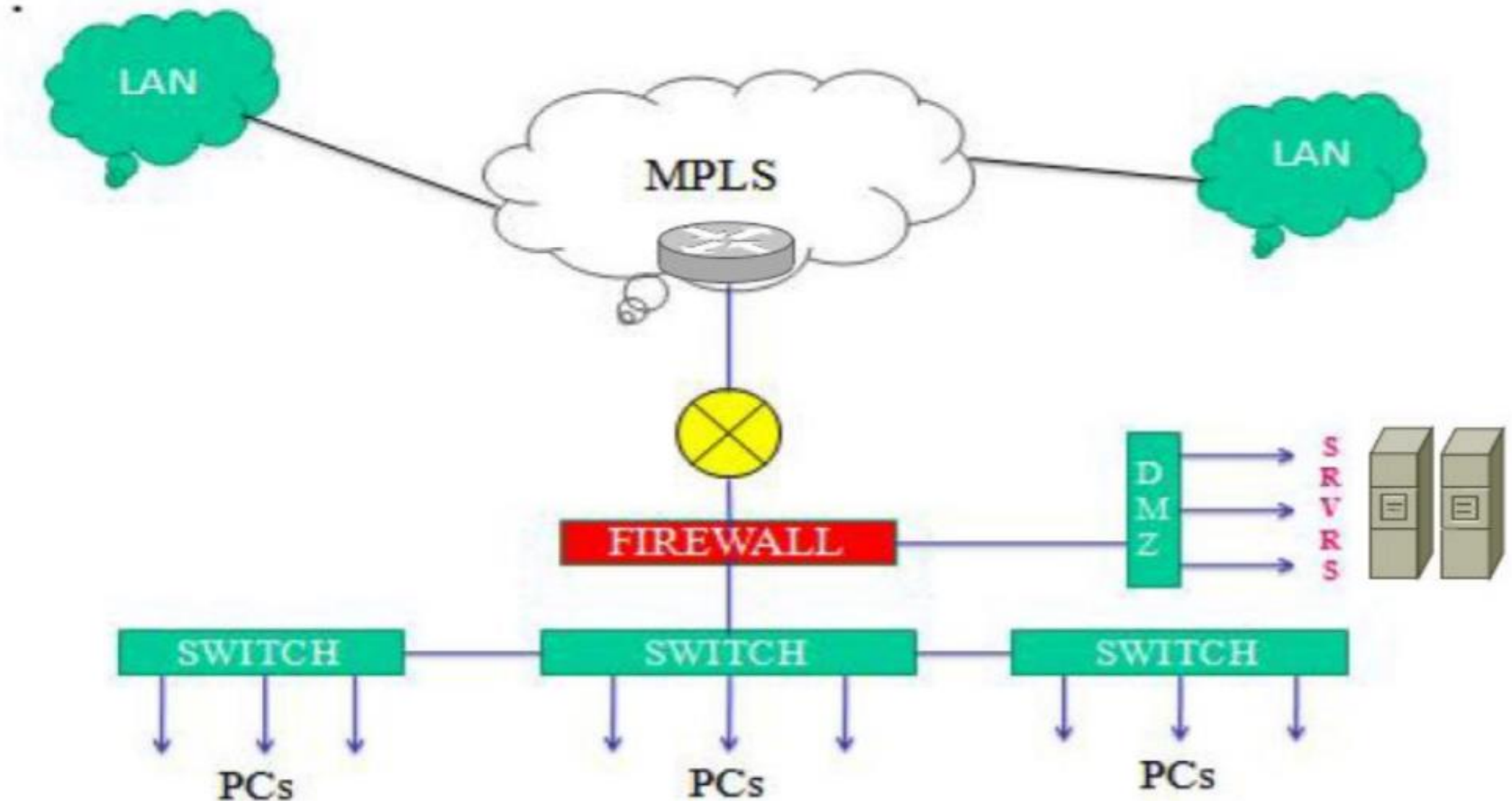
Railnet

- RAILNET is a corporate wide information system (CWIS)
- provides computer connectivity between Railway Board, Zonal Railways, Production units(Pus), RDSO, Centralized Training Institutes(CTIs), CORE, and MTP / Kolkata etc.
- It is an Intranetwork of Railways.

Objectives Of Railnet

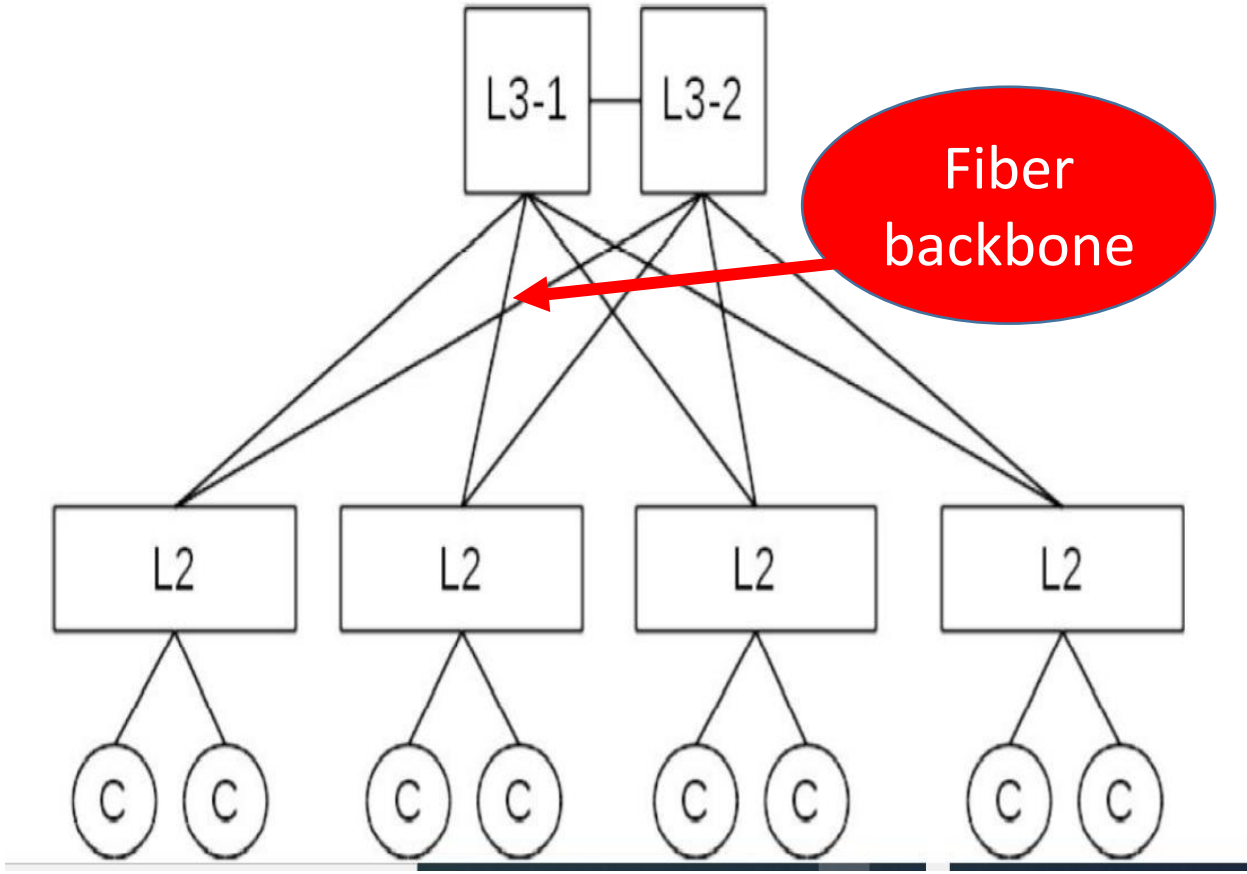
- Paperless working
- Information on Demand (no periodic reporting)
- Automatic Status Update
- Promote E-governance.

RAILNET GENERAL ARRANGEMENT

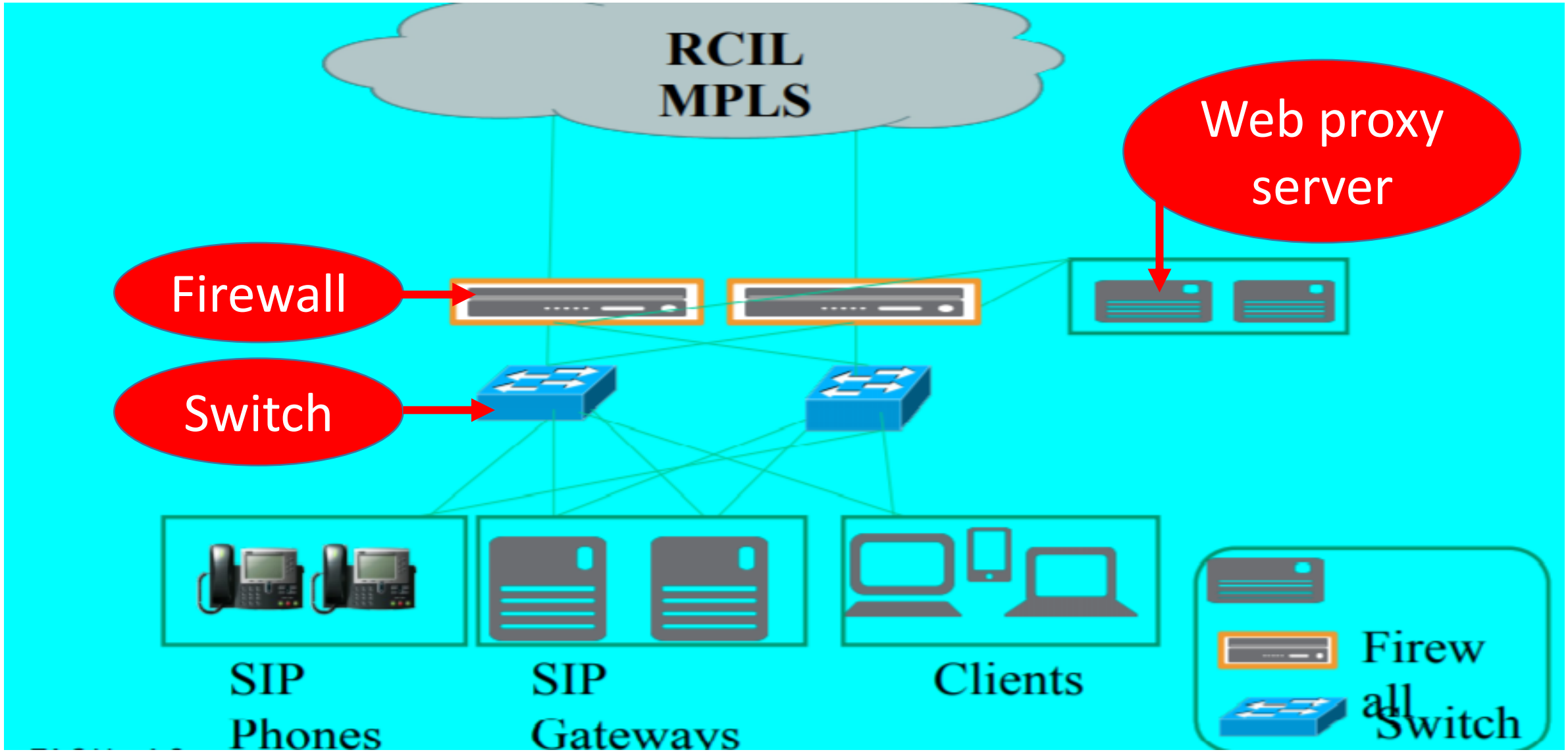


LAN ARCHITECTURE –BOARD'S GUIDELINES

- All backbone wiring of LAN should be on the fiber which is capable of working on 1GBPS.
- Layer -3 switches at the core. Two numbers. Should work as backup to each other.
- Layer-2 switch stack connected to both the L3 switch using OFC forming a network.
- L3 switches need not be PoE.
- L2 switches should be PoE enabled to support VoIP telephony.



Railnet Setup at Zones

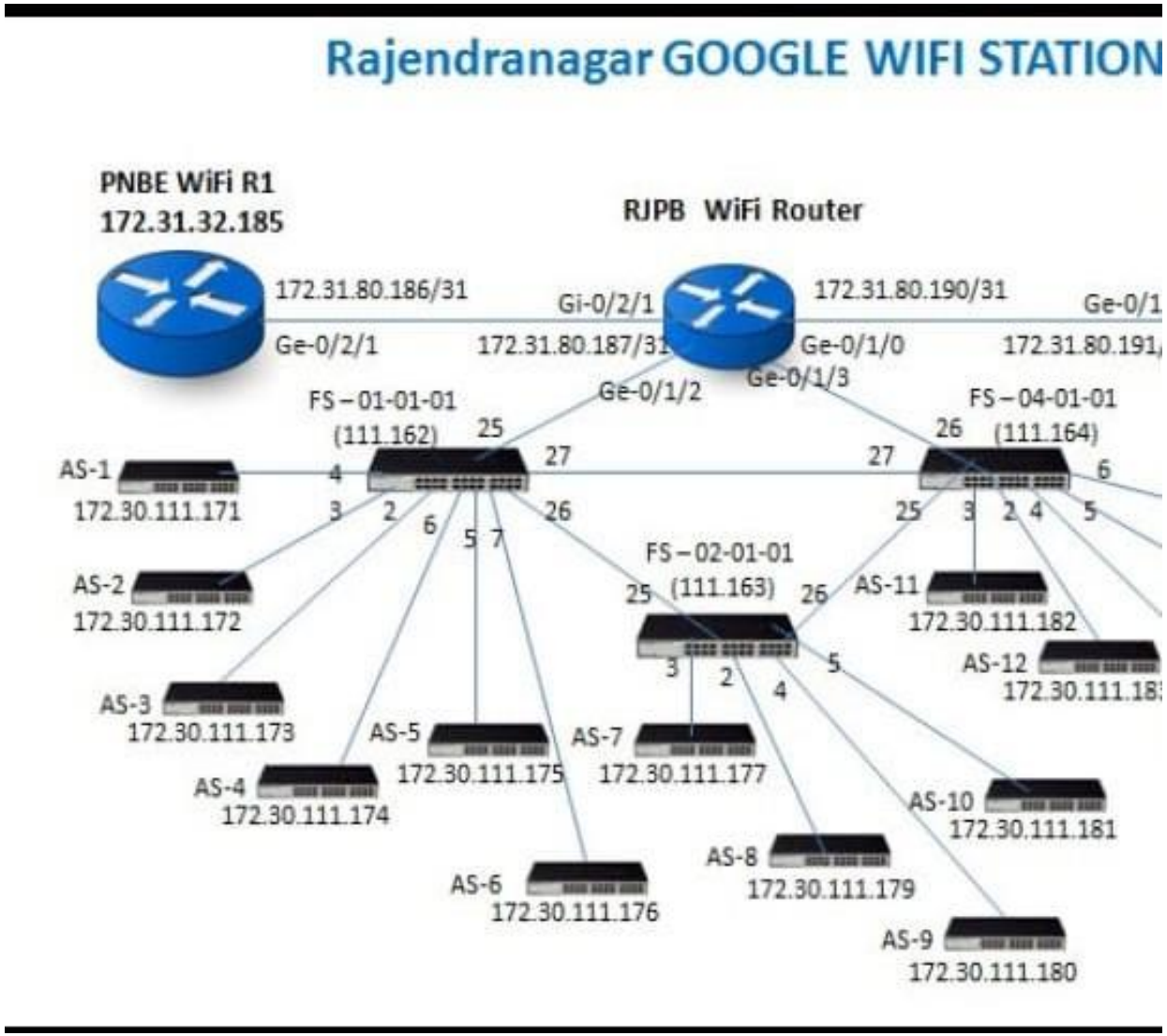


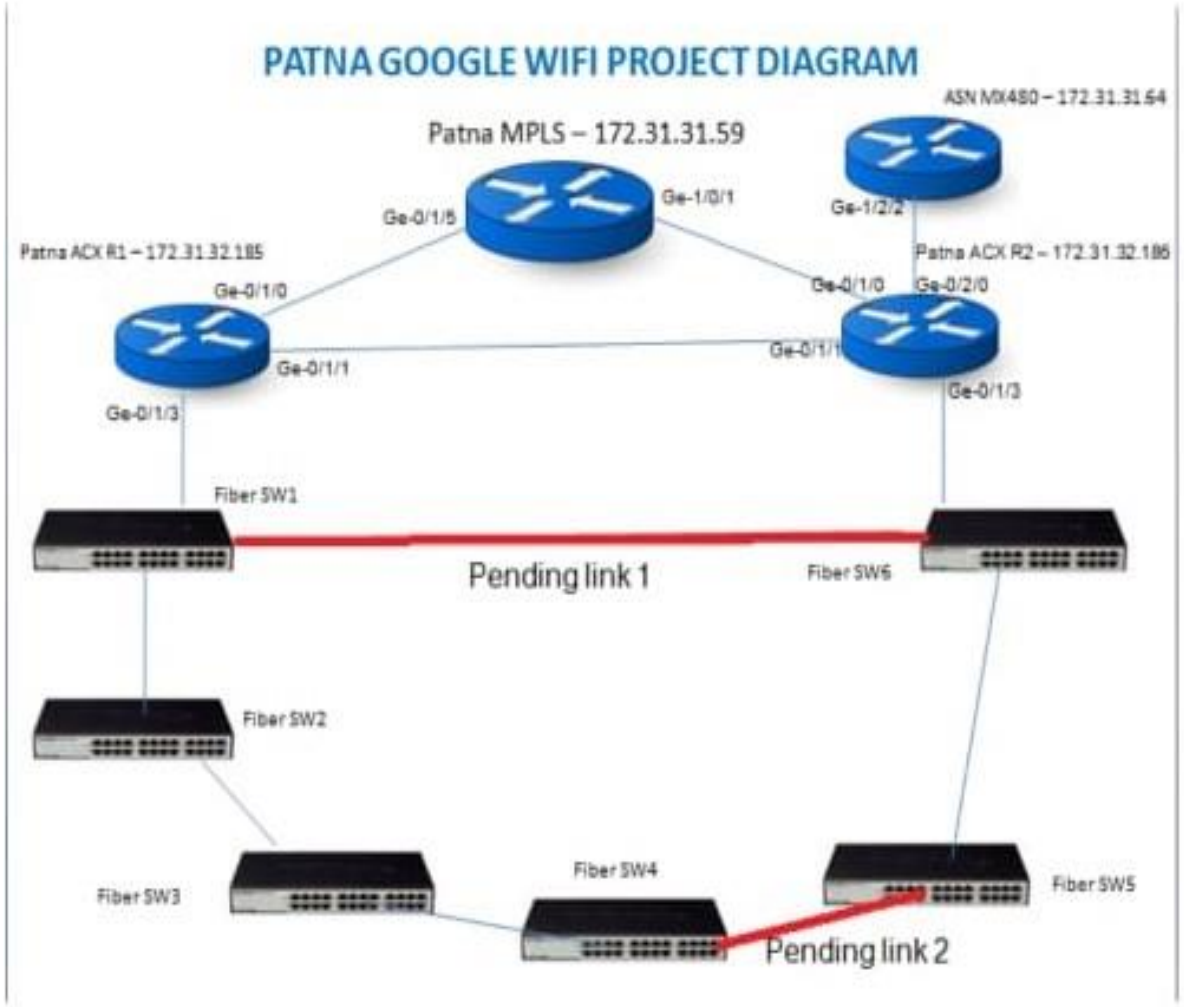
Implementation of Wi-Fi System in Trains & on Stations

- Indian Railways have partnered with Google to provide Wi-Fi Broadband facility to passengers at major railway stations across the country.
- The Google RailTel initiative named **Rail Wire** was launched in January 2016.
- Rail Wire is a free Wi-Fi internet project across major railway stations in India.



Wi-Fi connectivity links at Stations





PASSENGER RESERVATION SYSTEM(PRS)

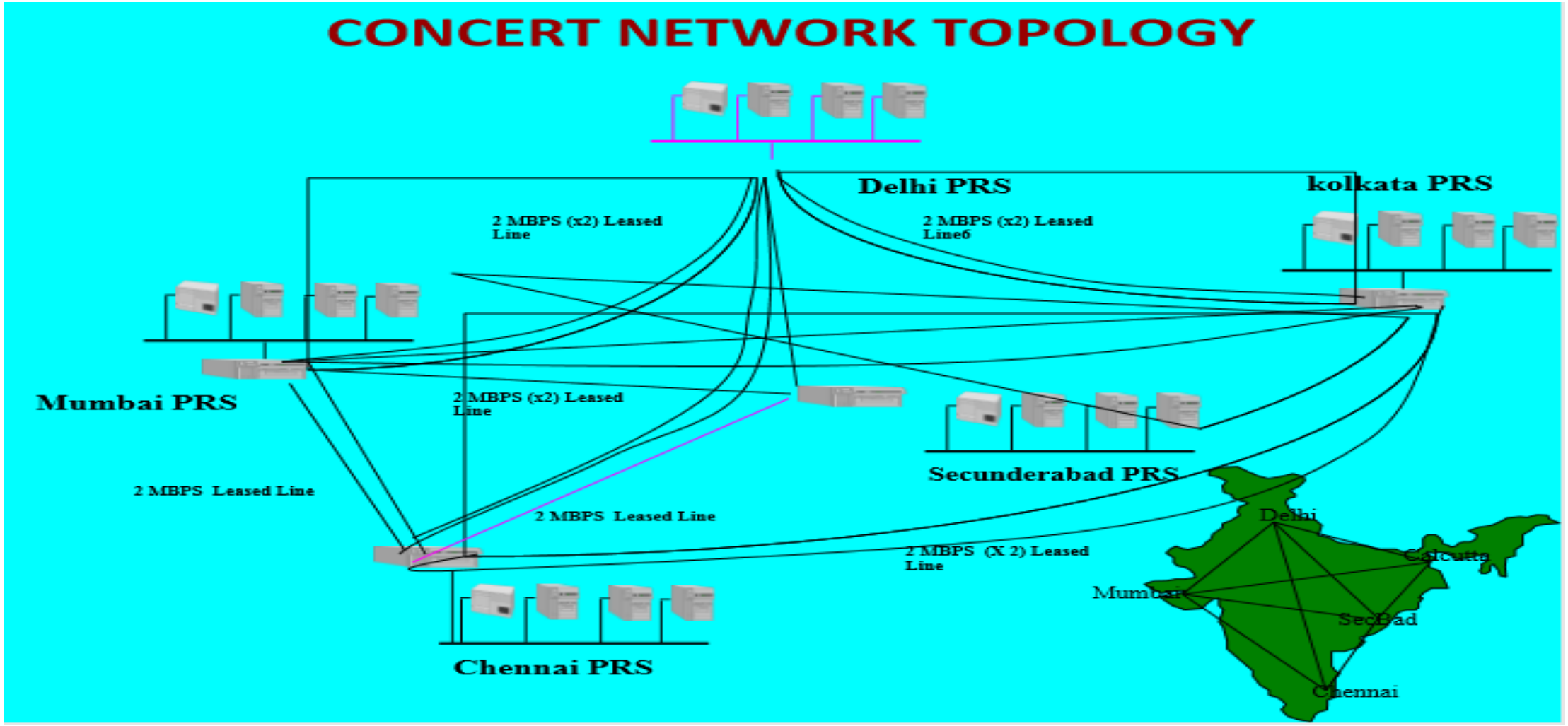
- PRS is a system that has been developed for reserving the seats in the trains in advance for passengers from different Railway reservation centers in India.

- COUNTRY-WIDE NETWORK FOR COMPUTERIZED ENHANCED RESERVATION AND TICKETING (CONCERT) developed by CRIS, is a total networking solution to Indian Railways Passenger Reservation System

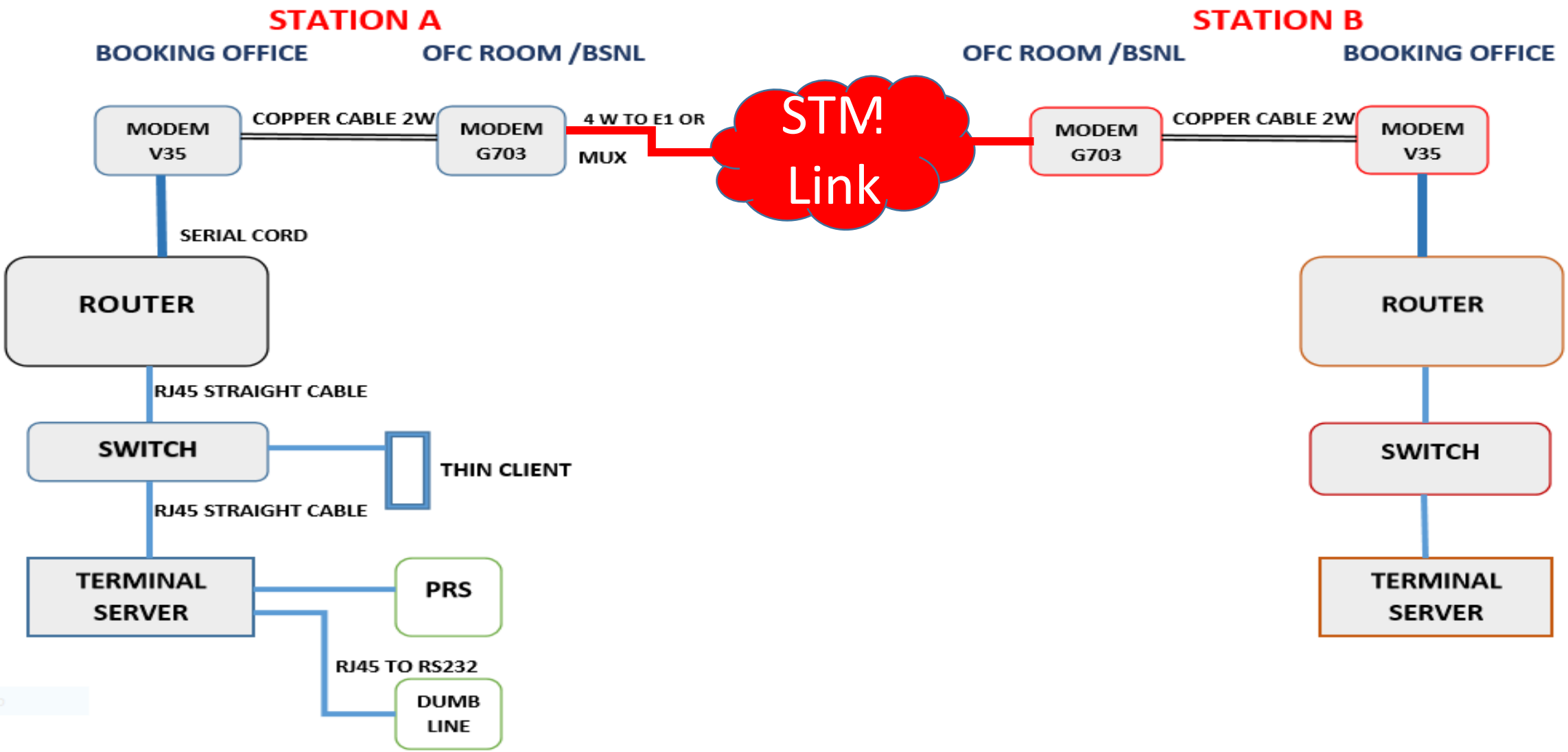
NETWORK CONNECTIVITY

- A Booking Terminal on any locations attached to assign PRS via dedicated 2 Mbps links through Router- Modem connectivity.
- All the locations have redundant links, either RCIL & BSNL or both.
- Each Dumb terminal port is connected to Terminal server port which in turn connected to central server via Switches, Router and Modems.
- PRS servers are located at 5 locations Delhi, Mumbai, Kolkata, Chennai & Secunderabad.
- These servers are connected in fully mesh topology .

PRS SERVERS connectivity diagram



Connectivity diagram of UTS/PRS



Freight Operations Information System(FOIS)

Advantages

- Increase business potentials
- Reduce operating costs
- Global tracking of consignments. in real time
- Promote e-commerce
- Ready details of wagons & racks.
- Monitoring of freights.
- Generate managerial reports.

FOIS Components

- Rake Management System (RMS) -for handling the operating portion
- Terminal Management System (TMS) –for commercial transactions.
- Coaching Operations Information System(COIS) or
- Integrated Coaching Management System (ICMS) - entire data of each coach on IR readily available on computer for its optimum use and traffic management at all levels.
- Crew Management System(CMS)
- Computerized Control Charting

FOIS Architecture

- Application servers are centrally placed at CRIS/NDLS
- CRIS SERVERS are connected to all Zonal HQ & Div HQ on 2 Mbps WAN links hired from RCIL.
- Wayside field locations connected in tandem order and terminated to div. or zonal HQ forming a mesh on 64 Kbps or 2 Mbps (WAN).
- VSAT communication is provided to establish connectivity to the locations where other means of communication like railway's own links or BSNL link is not feasible.
- FOIS is a CLIENT –SERVER working model.

Connectivity Diagram of FOIS

