INDEX

1 CSC AND VARIOUS SALES CHANNELS

1.1 LEARNING OBJECTIVES

- Explain the Internal and External Sales Channels of BSNL.
- Explain the Role of Internal sales channels (CSC).
- Explain the Role of External sales channels.

1.2 INTERNAL SALES CHANNELS (CSC)

1.2.1 Services Offered By BSNL CSC

a. Mobile service- BSNL CSC is providing mobile service in form of New connection, SIM replacement, Re-connection, Customer records updation, C-TOP UP, recharge, mobile number porting & post paid customer's service etc.

b. Landline Service- BSNL CSC is also providing Landline service in form of New connection, shifting, Plan change, Disconnection etc

c. Broadband service

d. FTTH service

e. BSNL Wings service

f. Supporting DSA & Franchisee for expanding business through outdoor sales channels.

1.3 EXTERNAL SALES CHANNELS

a. Franchisee
b. e-Distributor
c. DSA
d. Rural Distributor

1.3.1 Franchisee

Franchisee will be responsible for selling of all the BSNL products to the BSNL subscribers, directly or through Rural Distributors (RDs) / retailers within a defined territory. To facilitate retailers, provision of three tier structure has been made by including Rural Distributor between franchisee and retailers only in rural territories to serve the area within the rural BTS.

1.3.2 Responsibilities Of Franchisee

a) Selling of all BSNL Products purchased by Franchisee directly or through Rural Distributors (RDs) or retailers.

b) Two tier structure for urban and three tier structure for rural areas by incorporating intermediate channel of RDs.

c) Franchisee to make best efforts to actively market and promote the BSNL Products as permitted by BSNL.

d) Franchisee must appoint sufficient numbers of retailers in the territory.

e) Retailers in the rural areas will be appointed and served by RDs.

f) Meeting all sales targets set by SSA/Circle for the franchisee territory.

g) CAF collection, documentation (physical documentation as well as electronic documentation) and timely submission of documents to BSNL as per regulatory guidelines and BSNL instructions.

h) Verification of credentials of customers – Verification of POI/POA (photo, identity and address) of customer at the POS (Point of Sale) has to be done as per the various guidelines issued by DoT and BSNL from time to time.

i) BSNL reserves the right for CAF entry/CAF collection/CAF submission through any third party on outsourced model.

j) Operation of IT tools and systems provided by BSNL as specified from time to time, including hiring data entry operator if required.

k) Appointing required number of FoS (Feet-on-Street) exclusively for BSNL Products to serve retailers as per guidelines in force.

l) Assist and cooperate and with the Franchisee Manager or any other BSNL employee appointed by BSNL in respect of sale of BSNL products, and provide him/her with the required details as specified by BSNL.

m) Providing List/Details of FOS and retailers to BSNL.

n) After sales services to end-customers in its own capacity and at its own cost, which shall include receiving, attending & rectifying complaints.

o) All forms of complaint handling on phone and walk-in-complaints (hardware related, billing, service, performance related etc.) will be handled directly by Franchisee.

p) Serving retailers and Rural Distributors at their doorsteps.

q) The margin/ discount/ incentives / commissions extended by BSNL to franchisee and eligible retailers in their chain/ network

r) Receiving advertisement/ marketing material from BSNL, and displaying it at POS and distribution to Rural Distributors.

s) Promotion of BSNL Products at Franchisee‟s own cost.

t) Arranging special promotional events, as per BSNL requirements, at Franchisee‟s own cost, which shall include events and camps/canopy in unreached and potential areas.

u) Timely submission of bills and claims to the nodal officer .

v) Storage of SIM‟s, data cards and other telecom products purchased by the Franchisee from BSNL in a proper manner.

w) Provide all necessary information to BSNL including but not limited to its books of accounts, or any other information for the purpose of submitting the same in any proceedings before any Government Authority or against any third parties.

x) Issue receipts: At the time of booking of any new connection, franchisee shall issue its formal receipt / invoice to the Rural Distributors (RDs) / retailers.

y) Franchisee will be responsible for all the work done through its distribution network. The franchisees will be responsible for intimating their GSTN No. to BSNL for billing purpose.

1.3.3 Responsibilities Of BSNL

a. Appoint sufficient number of Retailer Managers, Retailer Manager Coordinator (RMC), and Franchisee Managers for providing time-to-time guidance, and addressing issues/ concerns raised by franchisees.

b. BSNL shall communicate to the Franchisee the minimum sales required to be made by them on quarterly/ monthly basis, in order to remain eligible for the Franchiseeship Agreement

c. Resolution of issues (including supply of SIMs, payments, servicing of retailers, cross-selling, etc.) raised by franchisees, rural distributors, franchisee managers, RMC, retailer managers, retailers and any other member of the Sales & Marketing team.

d. It will be the responsibility of the Account Officer to remit the collection from the franchisee to credit to Company’s account on as and when purchases of

BSNL Products (except post-paid products) are made by the Franchisee and ensure realization of the cheque.

e. The cheque deposited by the Franchisees should be deposited with bank for realization in a manner that it is realized latest by 3rd day (Date of purchase + 2 working days). The Account Officer shall be responsible for ensuring collection, deposit with the bank and realization of the cheque(s).

f. Franchisee manager / SSA Sales Head (Mobility) to ensure that all sales made by BSNL to franchisee and is recorded in BSNL specified IT system.

g. The Sancharsoft & stock register giving details of material sold to the Franchisee should be properly maintained and monitored on regular basis by SSA Sales Head (Mobility).

h. MRP of the products should be displayed. The stocks and distribution of publicity materials like brochures etc., preferably in local languages also should be available in sufficient quantity.

i. In order to promptly receive CAFs, there should be at least one desk counter, totally dedicated to accept CAFs from Franchisees/DSAs at a prominent location in every city and should be manned on all days, including holidays.

j. Ensure timely payments to all channel partners preferably online.

k. It will be mandatory on monthly basis to reconcile the account of prepaid product along with IN report.

l. The following items shall be given free of cost to franchisees for performing their responsibilities, including for demo purpose, and are not linked with the sales targets to be made by the franchisees:

- One rent free landline connections with unlimited on net local calls (LL + Mobile) within circle.

- One rent free landline connection for incoming calls with Broadband plan BBG Combo ULD 850 (350 monthly free call with unlimited download/Upload).

- One rent free VPN over Broadband (512 kbps VPNoBB plan)

- One rent free GSM post-paid Plan – 525, calls beyond freebies shall be payable.

1.3.4 Eligibility Requirements For BSNL Franchisee-Ship

All proprietorship firm, partnership firms and company of Indian origin fulfilling following criteria are eligible to apply.

a. Turn over**:** Turnover is defined as sales proceeds as per audited P&L account of the firm, submitted for last financial year. A copy of income tax return should also be submitted along with.

b. Rs.50 Lakhs for A class territory

c. Rs.30 Lakhs for B class territory

d. Rs.6 Lakhs for C class territory

e. Experience: Interested firms must be distributor/dealer of Telecom / FMCG / Electronics / Electrical / any other products with established retail chain for :

f. 2 years for class A territory out of last 5 years

g. 3 years for class B territory out of last 4 years

h. 1 year for class C territory out of last 3 years

i. Space: Interested party must ensure office/ showroom space (carpet area) of minimum size of 200 sqft for BSNL franchisee ship within operational area of the territory. CGMs are authorized to relax the space upto minimum size of 120 sqft as per local need. However it should be clearly mentioned in EoI document.

j. Interested party should have a valid PAN. And TAN.

k. Interested party should have a valid Goods and Services Tax (GST) registration Certificate No. for respective state

l. Interested party should provide a self-declaration along with the evidence that the bidder is not black listed by the GST authorities

m. In case the interested party gets black-listed during the tenure of the BSNL contract, then BSNL will not be responsible for any loss of input tax credit (ITC) to the franchisees.

1.4 TARGET SETTING AND PERFORMANCE MANAGEMENT

Circles will assign targets to SSAs on monthly basis for the following based on:

1.4.1 For GSM Connections:

The target among SSAs may be apportioned on the basis of – Type of territory, total number of BTS (2G + 3G) in SSA in previous month, market potential, competition, desire growth etc.

1.4.2 For Recharge:

Recharge targets must be apportioned among SSAs as per total no. of active prepaid connection, ARPU in the previous month plus other important parameters like potential of the area, urban-rural mix industry growth rate etc.

1.4.3 For POS :

Based on number of BTS

Each SSA must conduct a review meeting in first week of every calendar month where each franchisee's performance in previous month must be evaluated. Each Circle must conduct a review meeting every quarter to review the same. This meeting must be conducted within fifteen days of quarter ending.

1.5 E-DISTRIBUTOR

BSNL is serving customers through Franchisees/ Rural Distributors/ DSAs/ Retailers in the defined geographical area. To serve the customers through webportal/ Koisk/ ATMs/POS (Retailers) and other electronic mode. There is a need to appoint Zonal level franchisees and will be known as e-Distributors.

To serve BSNL customers through web portal / Kiosk /ATMs /POS (Retailers) and other electronic mode, there is a need to appoint Zonal Level franchisees to be known as e-Distributors. There will be three types of e-Distributors:

I. Cat -1 : who is applying for single zone

II. Cat -2 : who is applying for two zones.

III. Cat-3 : who is applying for all four zones i.e. on PAN India basis

Following key features are there for e-Distributor Policy

a. e-Distributors have to sell e-recharge/ top-up to prepaid connections and / or postpaid bill payment and / or other BSNL products purchased by them from BSNL, from time to time through web based platform / Kiosk ATMs/ POS

(Retailers) using Internet /API / mobile apps/ data access or other electronic modes.

b. e-Distributor and BSNL shall act on a principal to principal basis and at no time, the distributor shall act in the capacity of an agent of BSNL.

c. The e-Distributor shall be responsible for investment in setting up requisite infrastructure viz. Outlets, portals, servers, leased connectivity etc.

d. e-Distributor shall integrate its system with BSNL‟s zonal C-top up systems and will ensure security of data link by way of Firewall/ IDS etc. C-top up vendor will share APIs for the integration purpose.

e. The reports needed by BSNL for reconciliation and monitoring purpose will have to be developed by both parties and will be validated by BSNL team appointed by the GM (CMTS), Nodal Center before start of actual application.

f. A secured password based account shall be created for BSNL to facilitate remote login to the server by designated BSNL staff. BSNL shall be permitted to view all reports and track sale and distribution to the EFTPOS terminals/NET/SMS.

g. Messaging facility shall be provided between the central server and the EFTPOS terminals wherein BSNL shall be able to pass on marketing related information, special promotional schemes etc to the EFTPOS terminals.

h. The e-Distributor shall store all records of sale at the Central server for a period of at least one year to enable tracking of Sale etc by Law enforcement agencies in India.

i. BSNL may from time to time provide information, training and assistance relating to the services.

j. BSNL may provide the marketing material to the e-Distributor.

k. BSNL shall not be liable for any loss, pilferage or damage to the goods stored and sold at the premises and the merchandise shall be the entire responsibility of the eDistributor.

1.5.1 Eligibility Requirement

a. It should be an Indian registered proprietorship firm, partnership firms or company.

b. The company should not have substantial equity stake (10 % or more) in & of any Basic services/Cellular services/Internet services/Unified Access

services/National Long Distance services operating company / companies in India.

c. The company should not be a Licensed Service Provider to provide Basic services/Cellular Services/ Internet services/ Unified access services/NLD services anywhere in India

d. It should have a turnover of Rs. 10 crores for Cat-1 e-Distributor and Rs. 15 crores for Cat -2 & Rs. 20 Crores for Cat-3 e-Distributor during the last 12 months.

e. It should have a minimum of one year experience of e-Distributor

f. The Company should have a valid PAN and TAN .

g. The Company should have a valid Goods and Services Tax (GST) registration Certificate No. For respective state.

h. The Company should provide a self-declaration along with the evidence that the bidder is not black listed by the GST authorities.

i. In case the Company gets black-listed during the tenure of BSNL contract, then adequate indemnity clause should be inserted to ensure that no loss of credit is borne by BSNL due to a default of e-distributor.

1.5.2 DSA

a. The Direct Selling Agent shall market and sell all BSNL Products to customers at their door steps. BSNL and DSA shall observe the following procedure in connection with purchase and sale of BSNL Products:

b. The DSA shall place an order for purchase of products from BSNL.

c. Upon dispatch of ordered products, BSNL shall raise an invoice on the DSA, net of applicable discount to be provided to DSA

d. BSNL will charge GST on the price at the transaction value i.e. the price at which BSNL sells its products to DSA. BSNL would raise sale invoice for sale of BSNL products to DSA.

e. GST paid by DSA to BSNL shall be available to DSA as input tax credit which can be set off against the GST charged by DSA to the retailer

f. Secondary / subsequent incentives such as incentive on FRC/RC, any scheme based incentive, FOS incentive etc. to DSA shall be given online in the form

of c-top-up value through any platform like Sancharsoft/Pyro/ERP after levy of applicable taxes i.e. TDS /GST etc, wherever applicable.

g. For the subsequent incentives provided by BSNL (refer point 18 above), DSA will raise an invoice (along with applicable GST) on BSNL. Since incentive is paid to DSA in the form of c-topup, BSNL will also raise an invoice (along with applicable GST) on DSA for allocation of such c-topup value .

h. Where DSA is not registered under GST Act, it shall be the responsibility of BSNL to discharge liability under reverse charge mechanism. It is further agreed that DSA shall not charge tax on invoice .

i. BSNL shall, withhold tax at source under Chapter XVIIB of the IT Act, 1961 on the secondary/ subsequent incentive provided by BSNL to the DSA for sale of BSNL Products .

j. GST paid by DSA to BSNL and by BSNL to franchisees (as the case maybe w.r.t. secondary / subsequent incentive provided by BSNL) shall be available to DSA and BSNL, respectively, as input tax credit which can be set off against the GST charged by DSA or BSNL x. Methodology and applicable tax deduction/reconciliation on payment like discount at the time of sale of BSNL Products, discount on FRC/RC, any scheme based incentive, FOS incentive etc. to DSA may be changed time to time & necessary instructions shall be issued by concerned cell of BSNL CO.

k. The invoices raised by DSA and BSNL should comply with all the conditions as prescribed under the tax invoice rules under Central Goods and Service Tax Rules, 2017.

l. Where DSA is not registered under GST Act, it shall be the responsibility of BSNL to discharge liability under reverse charge mechanism.

m. Applicable Tax deductions/ reconciliation/ accounting related instructions/ guidelines shall be issued by concerned cell of BSNL CO, which shall be applicable to circle/SSA.

n. Rate of discount/ margin/ incentive needs to be reviewed with every change in the rate of GST in order to keep it at par with or lower than the current rate applicable on face value.

o. Methodology of calculation of discount/ margin, Applicable Tax deductions/ reconciliation/ accounting related instructions/ guidelines shall be issued by concerned cell of BSNL CO will be issued time to time, which shall be applicable to circle/SSA.

p. In case of any deviation, default or negligence on the part of DSA due to which it is liable to pay penalty to BSNL, the same shall be recovered by BSNL from DSA along with applicable GST tax (as may be applicable)

q. BSNL shall deduct tax at source if required under GST Act and GST regulations, any law or any regulation.

r. In case of any deficient supply or incomplete supply, it shall be the responsibility of DSA to issue GST compliance credit note (both at the time of sale of BSNL products or at the time of subsequent incentives provided to the DSA)) within the reasonable time and take tax adjustment.

s. GST (if applicable) on account of liquidated damages due to delay in supply would be borne by DSA.

1.6 RURAL DISTRIBUTOR

Rural distributors will cater to rural areas and engagement of these distributors will be through a committee constituted by the SSA Head. The committee will recommend suitable persons/agency from amongst working FMCG distributors/retail shop OR any other suitable person of the area. Based on recommendation of committee, RDs will be selected by the SSA Head.

1.6.1 Key Features Of Rural Distributor Policy

a. Rural distributors may work on non-exclusive basis i.e., they may also sell products of other operators.

b. Rural distributors will be assigned an exclusive area of 4-5 BTS sites within one franchisee territory such that they handle total turnover of approximately Rs.5 Lakhs/Month.

c. The territory of Rural Distributor should be designed in such a manner that maximum distance to be served by Rural Distributor is less than 15 km.

d. Rural distributors must be residents of one of the villages of the area which they are serving so that they have good knowledge of local conditions and local market. They are able to push the product deep into the market due to their personal relations with local people.

e. Rural distributors directly serve the retailers and they do not have any employee(s). They will primarily be served by existing franchisee of that area. In case, the franchisee fails to serve, the RD will be served by BSNL directly.

f. Retailer/POS in the area of RD will be managed by Rural Distributors and franchisee will have no direct role to play in that area.

1.6.2 Service To Rural Distributor (Rds)

a. RDs will be served by the Territory Franchisee at his doorstep.

b. If Territory Franchisee does not serve the RDs properly then RDs will be served by BSNL directly.

c. Territory Franchisee will collect all CAFs from RDs and will provide them SIM as well as Recharge Coupon/C-TOPUP.

d. RDs will make payment at the time of delivery of stock. Representatives of Territory Franchisee will deliver the stock at their doorstep.

e. Suitable unlimited Broadband plan will be given to willing RD free of cost.

1.6.3 Responsibilities Of Rural Distributor:

It is the responsibility of RDs to generate demand for providing services permitted by BSNL. Selling of all BSNL Products assigned to them, directly or through retailers. Not only the targets set are to be achieved but also efforts are to be made to surpass it.

a. Timely submission of bills and claims to the nodal officer/ franchisee.

b. MIS as per BSNL format to BSNL officials/ Franchisee as per frequency specified.

c. Rural Distributor must ensure that BSNL products are available in retail networks in sufficient quantity on demand.

d. Verification of credentials of customers .

e. Rural distributors will be responsible for all the work done through retailers.

f. Rural distributors are required to attend meetings in SSA/ Franchisee as and when needed. Rural Distributor must ensure availability of BSNL products.

1.6.4 Responsibilities Of BSNL

a. BSNL shall from time to time or in response to specific request by the Rural Distributor provide information, training and assistance relating to the services and arrange for qualified personnel / representatives of BSNL to render such training and assistance.

b. BSNL may provide the marketing material to the Rural distributor.

c. In order to manage returns of defective products, BSNL may, with prior approval of the Rural Distributor, inspect the stock at Rural Distributor‟s

location to evaluate whether or not the products are maintained in proper condition.

d. BSNL / its representative will ensure no black marketing happens & also have periodic inspection / surprise check to ensure all channels are working properly.

e. The discounts offered by BSNL are subject to variation during the term of this Agreement at the sole discretion of BSNL.

f. The Rural Distributor can supply the printed / display material etc. at his own cost without any liability on BSNL. He will keep BSNL indemnity from the content of the publicity/ display material so supplied.

1.6.5 Eligibility Of Selection :

a. Educational qualification: 8th passed

b. Rural shop/distributor of any product preferably of FMCG products / electronic / mobile products etc.

c. Resident of the same territory with proof of residence.

d. PAN Number.

e. Valid Goods and Services Tax (GST) registration Certificate No. For each state

f. Interested party should provide a self-declaration along with the evidence that the bidder is not black listed by the GST authorities

g. In case the interested party gets black-listed during the tenure of BSNL contract, then BSNL will not be responsible for any loss of ITC to the franchisees. Further, the franchisee will be responsible to indemnify to BSNL any loss incurred by it.

1.7 ROLES OF SALES TEAM MEMBER

Roles of different members of the mobility sales team are mentioned below

1.7.1 Roles Of Circle Sales Team:

a. Appointment of franchisees.

b. Monitoring of SSA / Franchisee wise sales and performance w.r.t. target.

c. Ensuring the growth of sales channel network.

d. Ensuring appointment of sales team in SSA.

e. Monitoring the performance of FM/ RMC/ RM.

f. Ensuring the action to be taken by the SSAs.

g. Ensuring the smooth functioning of sales tools such as Sancharsoft, C-TOPUP, B&CCS terminals etc.

h. Redressal of issues / queries reported by the SSAs/ Franchisees.

i. Redressal of cross selling.

j. Escalating the unresolved problems and suggestion to improve the sale to BSNL.

1.7.2 Roles Of Ssa Sales Team:

a. Fixing of target for franchisees.

b. Monitoring the sales and performance of sales partner w.r.t. the target on daily / weekly basis.

c. Growth of sales channel network.

d. Appointment of required sales team of FM/ RMC/ RM.

e. Monitoring the performance and visit of FM/ RMC/ RM.

f. Set-up and smooth functioning of sales tools such as Sancharsoft, C TOPUP, B&CCS terminals etc.

g. Area demarcation and allotment of retailers.

h. Consolidation of priority list of retailers.

i. Support in ordering and delivering of material to sales channel.

j. Ensuring the availability of BSNL product, tariff details, advertising material to all POS.

k. Redressal of cross selling.

l. Payment of allowances / KPA.

m. Redressal of issues / queries reported by Sales partner/ sales channel team.

n. Escalating the unresolved issues and suggestions to improve the sale to Circle office.

1.7.3 Roles Of SSA Franchisee Manager:

a. Communicating target before beginning of month i.e. by 25th of previous month.

b. Support in ordering and delivery of material to Franchisee doorstep.

c. Communication /action raised by the RMCs / RMs.

d. Collection of data from franchisee.

e. Review of franchisee data with SSA sales team.

f. Supply of POS material to franchisee.

g. Ensure proper uses of Sancharsoft and data entry by Franchisee.

h. Redressal of issues / queries of Franchisee.

1.7.4 Roles Of SSA Retail Manager Coordinator (RMC):

a. Plan RM visit to existing retailers and to potential area for appointment of new retailer.

b. Daily review of RM performance.

c. Appointment of new retailers in potential area.

d. Verification of cross selling cases.

e. Compilation of daily report submitted by the RM.

f. Submission of retailer wise data regarding material availability, issues etc to FM with a copy to SSA Sales Head for action.

g. Providing the information regarding BSNL product / schemes / trade schemes/ VAS etc to retailer manager for further publicity.

h. Conduct validation visits with RMs and FMs.

i. Entry of new C-TOPUP retailers‟ information in Sancharsoft.

j. Organization of joint visit of RM and FOS to some distressed retailers.

1.7.5 Roles Of SSA Retail Manager (RM):

a. Auditing the no. of visits by the FOS to retailers.

b. Auditing the incentives paid to retailers by the Franchisee.

c. Providing the information regarding BSNL product / schemes / trade schemes/ VAS etc to retailer for further publicity.

d. Feedback about replacement of damaged material by the franchisee.

e. Feedback on supply of POS material such as Glow sign board etc.

f. Assessment of potential area for appointment of new retailers.

g. Combined visit with FOS and on spot issuing of C-TOPUP.

1.8 CONCLUSION

Initially BSNL was having one sales channel, that is Customer Care Center (CSC) through which BSNL was selling its product & services. Now as per the changing needs of the customer BSNL has opened up lots off sales Channel like Franchisee, e-Distributor, DSA, Rural Distributor etc. to better serve its customers.

2 TCP/IP, IP ADDRESSING (IPV4 & IPV6)

2.1 LEARNING OBJECTIVES

- TCP/IP architecture and the TCP/IP model
- Internet Protocol (IP)/ Internet Layer
- Class full and classless addressing scheme
- VLSM – Variable Length Subnet Mask
- CIDR – Classless Inter Domain Routing
- Differentiate Between Public And Private Ip Address
- Limitations Of IPV4
- Features and uses Of IPV6

2.2 ORIGIN OF TCP/IP

Transmission Control Protocol (TCP) and Internet Protocol (IP) came about due to the various networking needs of the US government. TCP/IP was developed to satisfy the need to interconnect various projects that included computer networks and also allow for the addition of dissimilar machines to the networks in a systematic, standardized manner. While it is quite true that smaller defense projects may not have warranted the use of TCP/IP for project aspects, edicts from various DOD concerns such, as the Undersecretary of Defense for Research and Development forced many government contractors and in-house developed projects to use the suite to conform with DOD requirements.

2.3 TCP/IP ARCHITECTURE AND THE TCP/IP MODEL

The OSI Reference Model's seven layers divide up the tasks required to implement a network. However, it is not the only such model. In fact, the TCP/IP protocol suite was developed before the OSI Reference Model; as such, its inventors didn't use the OSI model to explain TCP/IP architecture (even though the OSI model is often used in TCP/IP discussions today). The developers of TCP/IP created their own architectural model, which goes by different names including the TCP/IP model, the DARPA model (after the agency that was largely responsible for developing TCP/IP) and the DoD model (after the United States Department of Defense). Most people call it the TCP/IP model.

Regardless of the model you use to represent the function of a network, the model's functions are pretty much the same. The TCP/IP and the OSI models are really quite similar, even if they don't carve up the network functionality precisely the same way

Since the OSI model is so widely used, it is common to explain the TCP/IP architecture both in terms of the TCP/IP layers and the corresponding OSI layers. Figure below shows the relationship between the two models. The TCP/IP model does not address the physical layer, where hardware devices reside. The next three layers—network interface, internet, and host-to-host transport—correspond to layers 2, 3, and 4 of the OSI model. The TCP/IP application layer conceptually blurs the top three OSI layers. Note, too, that some people consider certain aspects of the OSI session layer to be part of the TCP/IP host-to-host transport layer

As shown in Figure 1, the TCP/IP model uses four layers that logically span the equivalent of the top six layers of the OSI model. (The physical layer is not covered by the TCP/IP model because the data link layer is considered the point at which the interface occurs between the TCP/IP stack and the underlying networking hardware.) Starting from the bottom, the TCP/IP layers are described in the following sections.

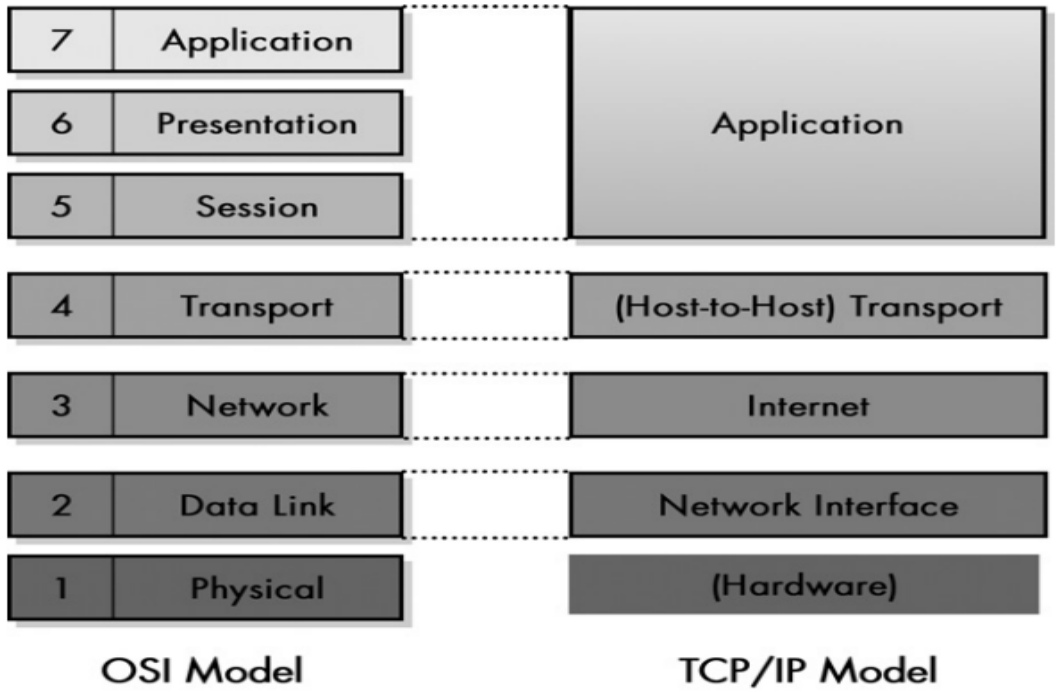


Figure 1: **OSI and TCP/IP Model**

The Internet architecture is of a layered design, which makes testing and future development of Internet protocols easy. To send data/information form one user toanother user through machine, layers interact with each other. One layer uses the service of its next lower layer and provides the service to the next higher layer. Once one layer receives the data/information from its next higher layer it attaches its own header information. The attaching the header to the received information, received from the higher layer before handing over to the next lower layer is called encapsulation. The procedure of encapsulation is shown in figure.

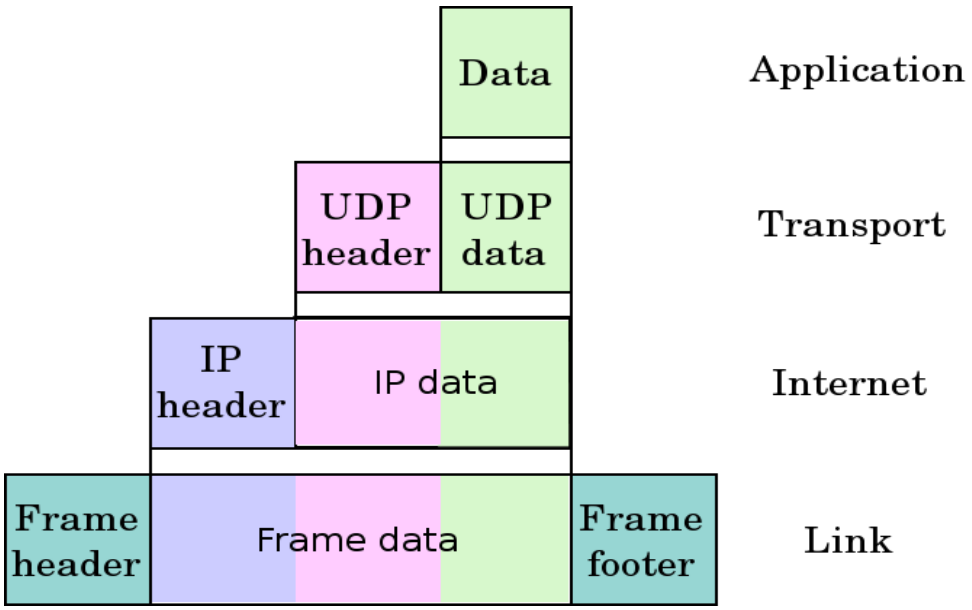


Figure 2: **TCP layers and encapsulation method**

2.4 INTERNET PROTOCOL (IP)/ INTERNET LAYER:

The Internet Layer is responsible to connect to two machines through internet. In its operation, the Internet Layer is not responsible for reliable transmission. It provides only an unreliable service, and "best effort" delivery. This means that the network makes no guarantees about packets' proper arrival

The function of providing reliability of service is the duty of higher level protocols, such as the Transmission Control Protocol (TCP) in the Transport Layer.

Integrity of packets is guaranteed in IPv4 through checksums computed for IP packets also define how to choose the initial path over which data will be sent, and defines a set of rules governing the unreliable datagram service.

The datagram consists of a header and data. Figure-2 identifies each field of the header, and is followed by a description of each field.

2.4.1 Header Length – 4 Bit Field

The value represents the number of octets in the header divided by four, which makes it the number of 4-octet groups in the header. The header length is used as a pointer to the beginning of data. The header length is usually equal to 5, which defines the normal, 20-octet header without options. When options are used, padding may be required to make the total size of the header an even multiple of 4-octet groups. The range of value for the header length is 5 to 15.

2.4.2 Version – 4 Bit Field

All other values are reserved or unassigned. Although the range of values is 0 to 15, the value used by IP is 4. By means of this field, different versions of the IP could operate in the Internet.

2.4.3 Type Of Service – 8 Bit Field

Specifies the precedence and priority of the IP datagram.

Bits +5, +6, and +7 make up the precedence field, with a range of 0 to 7. Zero is the normal precedence and 7 is reserved for network control. Most gateways presently ignore this field.

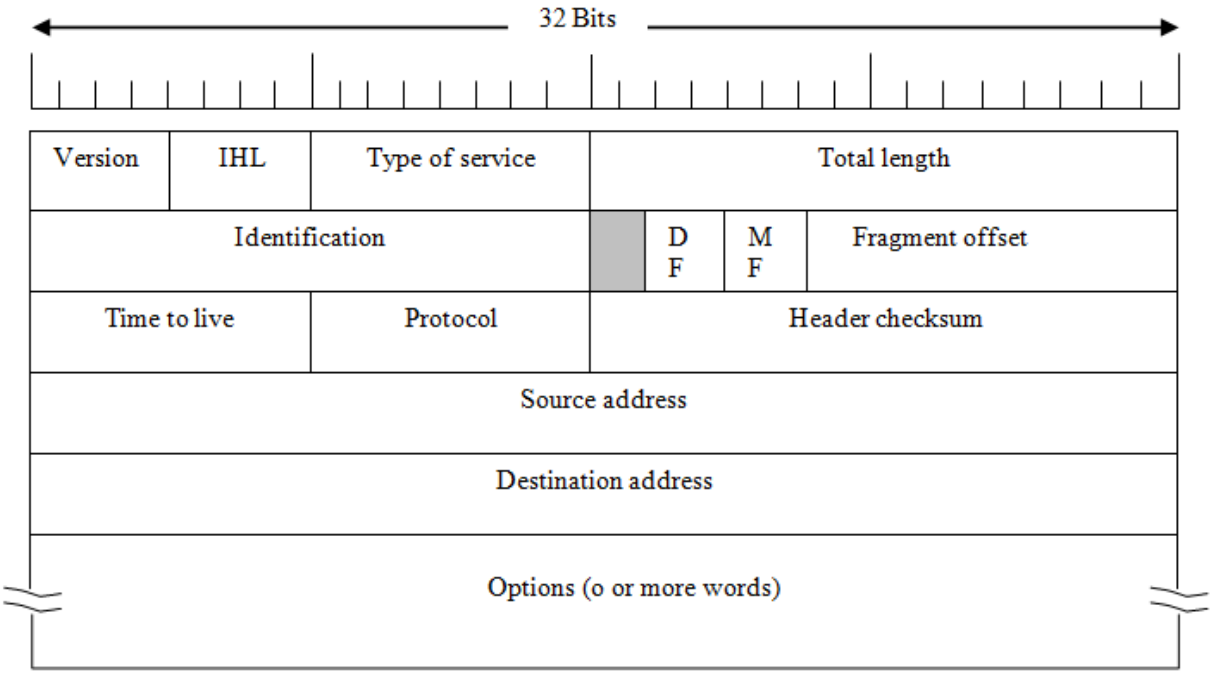


Figure 3: **IP Datagram Format**

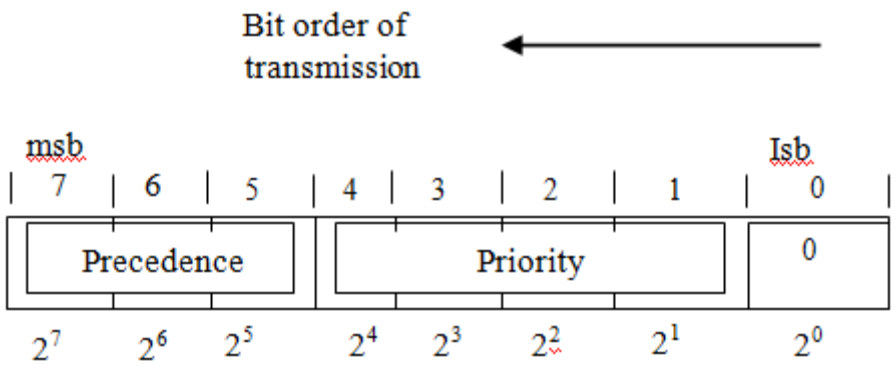


Figure 4: **Type-of-service field**

2.4.4 Total Length – 16 Bit Field

The total length field is used to identify the number of octets in the entire datagram. The field has 16 bits, and the range is between 0 and 65,535 octets. Since the datagram typically is contained in an Ethernet frame, the size usually will be less than 1,500 octets.

2.4.5 Identification – 16 Bit Field

The value of the identification field is a sequential number assigned by the originating host. The numbers cycle between 0 and 65,535.

2.4.6 Fragment Offset – 13 Bit Field

When the size of a datagram exceeds the maximum of an intermediate network, it is segmented by that network. The fragment offset represents the displacement (in increments of eight octets) of this segment form the beginning of the entire datagram. This is a 13-bit field and provides an offset to the proper location within the original datagram of this fragmented segment. Since the value represents groups of eight octets, the effective range of the offset is between 0 and 8191 octets.

2.4.7 Flags – 2 Bits

The flag field contains two flags. The low-order bit (MF) of the flags fields is used to denote the last fragmented datagram when set to zero. That is, intermediate (not-last) datagrams have the bit set equal to one to denote more datagrams are to follow. The high-order bit (DF) of the flags field is set by an originating host to prevent fragmentation of the datagram. When this bit is set and the length of the datagram exceeds that of an intermediate network, the datagram is discarded by the intermediate network and an error message returned to the originating host via the ICMP.

2.4.8 Time To Live (TTL) – 8 Bit Field

It represents a count set by the originator that the datagram can exist in the Internet before being discarded. Hence, a datagram may loop around an internet for a maximum of $2^8 – 1$ or 255 before being discarded. The current recommended default TTL for the IP is 64. Since each gateway handling datagram decrements the TTL by one, the TTL can also represent a hop count.

2.4.9 Protocol – 8 Bit Field

The protocol field is used to identify the next higher layer protocol using the IP. It will normally identify either the TCP (value equal to 6) or UDP (value equal to 17) transport layer, but may identify up to 255 different transport layer protocols. An upper layer protocol using the IP must have a unique protocol number.

2.4.10 Checksum – 16 Bit Field

The checksum provides assurance that the header has not been corrupted during transmission. The checksum includes all fields in the IP header, starting with the version number and ending with the octet immediately preceding the IP data field, which may be a pad field if the option field is present. The checksum includes the checksum field itself, which is set to zero for the calculation. The checksum represents the 16-bit, one's complement of the one's complement sum of all 16-bit groups in the header.

An intermediate network (node or gateway) the changes a field in the IP header (e.g., time-to-live) must recompute the checksum before forwarding it.

Users of the IP must provide their own data integrity, since the IP checksum is only for the header.

2.4.11 Source Address – 32 Bit Field

The source address field contains the network identifier and host identifier of the originator.

2.4.12 Destination Address – 32 Bit Field

The destination address field contains the network and identifier & Host identifier of the destination.

2.4.13 Options – Variable Field

The presence of the "options" field is determined from the value of the header length field. If the header length is greater than five, at least one option is present.

Although it is not required that a host set options, it must be able to accept and process options received in a datagram. The options field is variable in length. Each option declared begins with a single octet that defines that format of the remainder of the option.

2.4.14 Timestamp Option

The timestamp option provides the user with a technique of recording the precise route taken by a datagram and the time that each element (node or gateway) handling the datagram processed it.

2.4.15 Record/Strict/Loose Source Routes

This provides a routing trace of the datagram. The strict source route option permits the originator to can be useful to force all traffic over a particular path for testing. The strict source routing option is coded with the precise successive IP addresses, with a pointer set to the first hop. Each node handling the datagram increments the pointer to the next IP address. Loose source routing is similar, except only the major IP addresses are entered in

the list of IP addresses. The Internet my take any desired intermediate path so long as the datagram visits the IP nodes identified.

2.4.16 Padding – Variable Field

The pad field, when present, consists of 1 to 3 octets of zero, as required, to make the total number of octets in the header divisible by four. (The header length is in increments of 32-bit groups.)

2.5 HOST-TO-HOST TRANSPORT LAYER

This primary job of the host-to-host transport layer is to facilitate end-to-end communication over an internetwork. It is in charge of allowing logical connections to be made between devices that allow data to be sent either unreliably (with no guarantee that it gets there) or reliably (where the protocol keeps track of the data sent and received in order to make sure it arrives, and resends it if necessary). It is also here that identification of the specific source and destination application process is accomplished.

The formal name of this layer is often shortened to just the transport layer. The key TCP/IP protocols at this layer are TCP and UDP. The TCP/IP transport layer corresponds to the layer of the same name in the OSI model (layer 4) but includes certain elements that are arguably part of the OSI session layer. For example, TCP establishes a connection that can persist for a long period of time, which some people say makes a TCP connection more like a session

2.6 APPLICATION LAYER

The application layer is the highest layer in the TCP/IP model. It is a rather broad layer, encompassing layers 5 through 7 in the OSI model. While this seems to represent a loss of detail compared to the OSI model, that's probably a good thing. The TCP/IP model better reflects the somewhat fuzzy nature of the divisions between the functions of the higher layers in the OSI model, which in practical terms often seem rather arbitrary. It really is hard to separate some protocols in terms of which portions of layers 5, 6, or 7 they encompass.

Numerous protocols reside at the application layer. These include application protocols such as HTTP, FTP, and SMTP for providing end-user services as well as administrative protocols like Simple Network Management Protocol (SNMP), Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS).

2.7 TCP/IP TRANSPORT LAYER PROTOCOLS

This session provides a description of the transport layer protocols, user datagram protocol (UDP), and transmission control protocol (TCP).

The selection by an applications program to use either UDP or TCP is based on the requirement for reliability, primarily. Some application layer protocols were designed to operate with either UDP or TCP. The selection by the IP of either the UDP or TCP is based on the protocol number in the IP header.

Although ICMP and IGMP gain control as transport layer functions, they function as a utility to the network layer (IP). The TCP/IP designers used the protocols number in the IP header to demultiplex to distinct services.

TCP rides the unreliable, connectionless IP in the same manner as the UDP. That is, it has a unique protocol number (# 6) in the IP datagram that signals the IP to pass that data from the datagram (TCP header and data) to the TCP processing layer. TCP provides a transport layer service in terms of the OSI reference model – it functions as layer 4. The transmission unit for IP is called datagram, for UDP it is called user datagram, and for TCP it is called segment or (sometimes) packet.

2.7.1 TCP Segment Format

The TCP segment consists of a TCP header and data. The header portion of the TCP segment is relatively fixed in size. The only optional field is the options field, which may necessitate a pad field to assure that the overall header length is a multiple of four-octet groups. The format of the TCP segment is illustrated in Figure 5. The following is a description of each of the fields in the TCP segment, and general characteristics of TCP associated with each field description.

2.7.2 Source/Destination Port Numbers

Each port number is an unsigned integer occupying 16 bits.

2.7.3 Sequence Numbers

The sequence numbers in the TCP header is 32 bits long and first time randomly generated by the System . The SN of the first TCP segment identifies the first octet of the entire stream. Assume this value is n, which was established when the TCP connection was made. Then, the value of the SSN of the second TCP segment equals n + m, where m is the octet displacement within the total stream to the beginning of the second TCP segment.

2.7.4 Acknowledgement Numbers

The second sequence number is called the expected receive sequence number (AKN) – also called the acknowledgement number. The AKN is a 32 – bit field. The AKN acknowledges the receipt of m – 1 octets by stating the next expected SSN of m.

From the scenario above with the SN of n for the first segment and n + m for the second segment, the receiver of the first segment would send an ACK with the AKN equal to n + m, which acknowledges the receipt of octets n through n + m – 1 by advising that the next expected SSN is equal to n + m.

2.7.5 Header Length

The header length is a 4-bit field. It contains an integer equal to the total number of octets in the TCP header, divided by four. That is, it represents the number of 4-octet groups in the header. The value of the header length field is typically equal to five unless the there are options. Since there may be options in the TCP header, the pad field is used to force the number of octets in the header equal to a multiple of four. There may be up to three octets in the pad field, each containing the value zero.

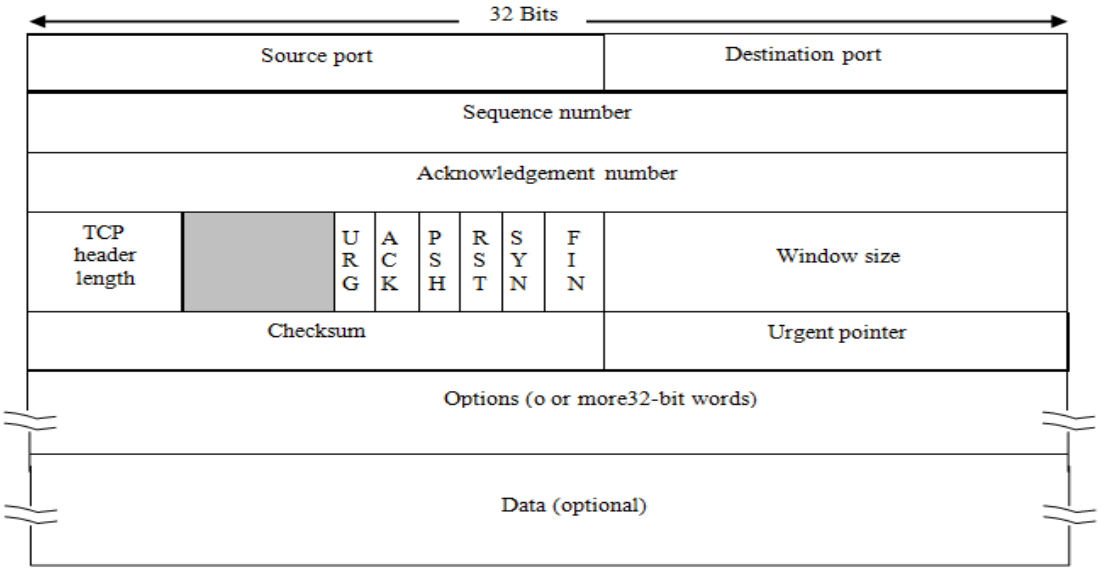


Figure 5: **TCP format**

2.7.6 Code Bits

The purpose and content of the TCP segment is determined by the settings to the bits in the code bit field.

- URG bit –when urgent bit is set to one then urgent pointer is checked to know the beginning of the urgent information.
- ACK bit – When the ACK bit is equal to one, the acknowledgement number is valid. And the TCP segment is carrying the acknowledgment otherwise not.

- PSH bit – Although a transmit buffer may not be full, the sender may force it to be delivered by setting PSH(Push) flag as one.
- RST bit – Setting the RST bit in a segment causes the connection to be aborted. All buffers associated with the connection are released and the entry in the TCB is deleted.
- SYN bit – The SYN bit is set during connection establishment only to synchronize the sequence numbers.
- FIN bit – The FIN bit is set during connection closing only.

2.7.7 Window

The window field is a 16-bit unsigned integer. The window field is used to advertise the available buffer size (in octets) of the sender to receive data.

2.7.8 Options

The option field permits the application program to negotiate, during connection set up, characteristics such as the maximum TCP segment size able to receive. Some future options may not be linked to connection setups. Ideally, the TCP segment size would be the maximum possible without causing fragmenting. If the option is not used, any segment size is allowed. The TCP maximum-segment-size option is illustrated in the Figure.

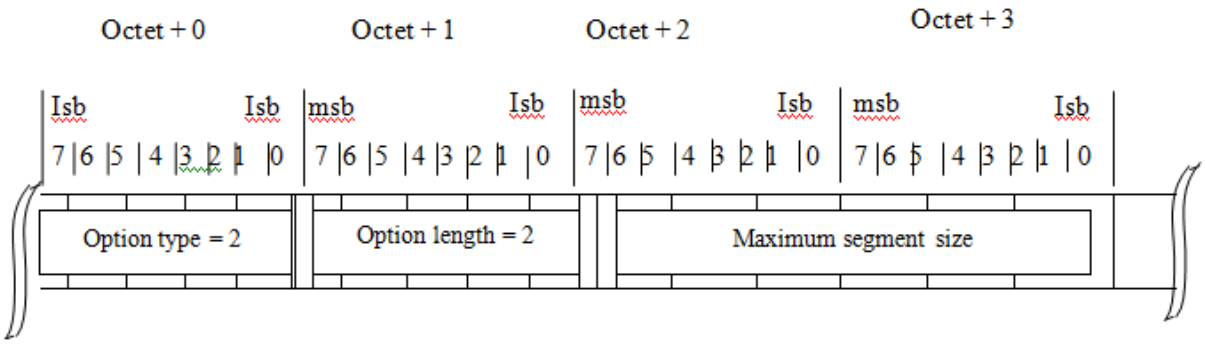


Figure 6: **TCP maximum-segment-size option.**

2.7.9 Padding

The padding field, when present, consists of one to three octets, each equal to zero, to force the length of the TCP header to be in multiples of four octets. If options are nor used, padding is not required. If options are used, padding may or may not be required.

2.7.10 Checksum

Since the IP layer does not include the data portion of the datagram in its checksum (protects the IP header only), TCP has its own checksum to provide data integrity.

2.8 IP ADDRESSING

2.8.1 Ipv4 Addressing

Each host on the internet is assigned a 32-bit integer address called its internet address or IP address. The clever part of internet addressing is that the integers are carefully chosen to make routing efficient. Every host and router on the internet has an IP address, which encodes its network number and host number. The combination is unique: no two machines have the same IP address. The address is coded to allow a variable allocation of bits to specify network and host

Internet Protocol version 4 (IPv4) is the fourth revision in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. Together with IPv6, it is at the core of standards-based internetworking methods of the Internet. As of 2012 IPv4 is still the most widely deployed Internet Layer protocol. IPv4 is described in IETF publication RFC 791 (September 1981).

IPv4 is a connectionless protocol for use on packet-switched Link Layer networks (e.g., Ethernet). It operates on a best effort delivery model; in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).

IPv4 uses 32-bit (four-byte) addresses, which limits the address space to 4.3 billion (2^32) addresses. Addresses were assigned to users, and the number of unassigned addresses decreased. IPv4 address exhaustion occurred on February 3, 2011. It had been significantly delayed by address changes such as classful network design, Classless Inter-Domain Routing, and network address translation (NAT).

The IP address scheme is to break up the binary number into pieces and represent each piece as a decimal number. A natural size for binary pieces is 8 bits, which is the familiar byte or octet (octet is the telecommunication term, but two words can be used interchangeably). So let’s take our binary number , write it using groups of 8 bits, and then represent each group as a decimal number:

Example 1: 140.179.220.200

It is sometimes useful to view the values in their binary form.

140 .179 .220 .200

10001100.10110011.11011100.11001000

Every IP address consists of two parts, one identifying the network and one identifying the host. The Class of the address and the subnet mask determine which part belongs to the network address and which part belongs to the host address.

We can use a dot as a separator. Now our IP address has the form which is referred to as the dotted decimal notation.

Example 2: 156.26.30.60

10111100	00011010	000111110	00111100
156	26	30	60

2.8.2 Ip Address Should Be Hierarchical

For a protocol to be routable, its address structure must be hierarchical, meaning that the address must contain at least two parts: the network portion and the host portion. A host is an end station such as a computer workstation, a router or a printer, whereas a network consists of one or more hosts.

2.8.3 Ipv4 Addressing Scheme

- Classful
- Classless

2.8.4 Classful Addressing Scheme

This was the original addressing scheme in which IPv4 address space was structured into five classes (A, B, C, D and E). The value of first octet of an IP address determines the class of network to which it belongs in classful addressing scheme.

2.8.5 Classless Addressing Scheme

In classless addressing scheme, classful networks are subnetted or super netted and their default subnet mask are changed, thereby just by analyzing the class of address by analyzing initial few bits will not help in determining the network ID and for this subnet mask is must.

2.9 ADDRESS CLASSES

This encoding provides flexibility in assigning addresses to host and allows a mix of network sizes on an internet. In particular, the three network classes are best suited to the following conditions:

- Class A: Few networks, each with many hosts. It allows for up to 126 networks with 16 million hosts each.
- Class B: Medium number of networks, each with a medium number of hosts. It allows for up to 16,328 networks with up to 64K hosts each;

- Class C: Many networks, each with a few hosts. It allows for up to 2 million networks with up to 254 hosts each;
- Class D: Reserved for IP Multicasting.
- Class E: Reserved for future use. Addresses beginning with 1111 are reserved for future use.

The Following table lists the capabilities for class A, B and C addresses.

Class	**Networks**	**Hosts**
A	126	16,777,214
B	16,384	65,534
C	2,097,152	254

MORE ABOUT IP ADDRESS CLASSES

You can determine which class any IP address is in by examining the first 4 bits of the IP address.

- **Class A** addresses begin with **0xxx**, or **1 to 126** decimal.
- **Class B** addresses begin with **10xx**, or **128 to 191** decimal.
- **Class C** addresses begin with **110x**, or **192 to 223** decimal.
- **Class D** addresses begin with **1110**, or **224 to 239** decimal.
- **Class E** addresses begin with **1111**, or **240 to 254** decimal.

Addresses beginning with **01111111**, or **127** decimal, are reserved for loopback and for internal testing on a local machine. [You can test this: you should always be able to ping **127.0.0.1**, which points to yourself] Class D addresses are reserved for multicasting. Class E addresses are reserved for future use. They should not be used for host addresses.

Now we can see how the Class determines, by default, which part of the IP address belongs to the network (N) and which part belongs to the host (h).

- Class A -- NNNNNNNN.hhhhhhhh. hhhhhhhh. hhhhhhhh
- Class B -- NNNNNNNN.NNNNNNNN. hhhhhhhh. hhhhhhhh
- Class C -- NNNNNNNN.NNNNNNNN.NNNNNNNN. hhhhhhhh

In the example, 140.179.220.200 is a Class B address so by default the Network part of the address (also known as the Network Address) is defined by the first two octets (140.179.x.x) and the host part is defined by the last 2 octets (x.x.220.200).

In order to specify the network address for a given IP address, the host section is set to all "0"s. In our example, 140.179.0.0 specifies the network address for 140.179.220.200. When the host section is set to all "1"s, it specifies a broadcast that is sent to all hosts on the network. 140.179.255.255 specifies the example broadcast address. Note that this is true regardless of the length of the host section.

2.10 PUBLIC AND PRIVATE IP ADDRESS

On the basis of usage of IP address in networks it can be classified as

- **Public IP Addresses**

  These are the address spaces that are used in Public Networks like the Internet.

- **Private IP Addresses**

  These are used in Private Networks like LAN.

2.10.1 Private Subnets

There are three IP network addresses reserved for private networks. The addresses are 10.0.0.0/8 (10.0.0.0 to 10.255.255.255), 172.16.0.0/12 (172.16.0.0 to 172.31.255.255), and 192.168.0.0/16 (192.168.0.0 to 192.168.255.255. They can be used by anyone setting up internal IP networks, such as a lab or home LAN behind a Router performing NAT (Network Address Translation) or proxy server. It is always safe to use these because routers on the Internet will never forward packets coming from these addresses. These addresses are defined in RFC 1918.

2.10.2 Subnetting

Sub netting an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. The most common reason is to control network traffic. In an Ethernet network, all hosts on a segment see all the packets transmitted by all the other hosts on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

2.10.3 Subnetting Using 1 Bit

Depending upon number of subnets to be carved out of given network, no of bits from host part can be used for creating these subnets. Example, 1 bit can create 2 subnets, 2 bits for 4 subnet and so on.

Example: Subnetting using 1 bit can be performed in order to divide a network into 2 equal sub-networks.

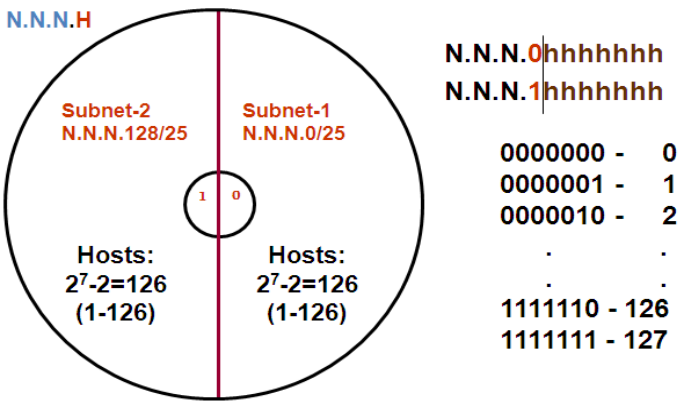


Figure 7: **Subnetting using 1 bit**

2.11 SUBNET MASKING

Applying a subnet mask to an IP address allows you to identify the network and host parts of the address. The network bits are represented by the 1s in the mask, and the host bits are represented by the 0s. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the *Network Address* or Number.

Eg, using our test IP address and the default Class B subnet mask, we get:

10001100.10110011.11110000.11001000 140.179.240.200 Class B IP Address

11111111.11111111.00000000.00000000 255.255. 0. 0 Default Class B S/M

10001100.10110011.00000000.00000000 140.179.0.0 Network Address

Default Subnet masks:

- **Class A** - 255.0.0.0 - 11111111.00000000.00000000.00000000
- **Class B** - 255.255.0.0 - 11111111.11111111.00000000.00000000
- **Class C** - 255.255.255.0 - 11111111.11111111.11111111.00000000

To calculate the number of subnets or hosts, use the formula (2^n-2) where n = number of bits in either field, and 2^n represents 2 raised to the nth power. Multiplying the number of subnets by the number of hosts available per subnet gives you the total number of hosts available for your class and subnet mask. Also, note that although subnet masks with non-contiguous mask bits are allowed, they are not recommended.

Example:

10001100.10110011.11011100.11001000 140.179.220.200 IP Address

11111111.11111111.**111**00000.00000000 255.255.**224**.000 Subnet Mask

---

10001100.10110011.11000000.00000000 140.179.192.000 Subnet Address

10001100.10110011.11011111.11111111 140.179.223.255 Broadcast Address

In this example a **3 bit subnet mask** was used. There are 6 (2^3-2) subnets available with this size mask (remember that subnets with all 0's and all 1's are not allowed). Each subnet has 8190 (2^{13}-2) hosts. Each subnet can have hosts assigned to any address between the Subnet address and the Broadcast address. This gives a total of 49,140 hosts for the entire class B address subnetted this way. Notice that this is less than the 65,534 hosts an unsubnetted class B address would have.

You can calculate the Subnet Address by performing a bitwise logical AND operation between the IP address and the subnet mask, then setting all the host bits to **0**s. Similarly, you can calculate the Broadcast Address for a subnet by performing the same logical AND between the IP address and the subnet mask, then setting all the host bits to **1**s. That is how these numbers are derived in the example above.

Subnetting always reduces the number of possible hosts for a given network. There are complete subnet tables available here for Class A, Class B and Class C. These tables list all the possible subnet masks for each class, along with calculations of the number of networks, hosts and total hosts for each subnet.

2.12 SUPER NETTING

The "classful" system of allocating IP addresses can be very wasteful; anyone who could reasonably show a need for more that 254 host addresses was given a Class B address block of 65533 host addresses. Even more wasteful were companies and organizations that were allocated Class A address blocks, which contain over 16 Million host addresses! Only a tiny percentage of the allocated Class A and Class B address space has ever been actually assigned to a host computer on the Internet.

People realized that addresses could be conserved if the class system was eliminated. By accurately allocating only the amount of address space that was actually needed, the address space crisis could be avoided for many years. This was first proposed in 1992 as a scheme called **Supernetting**. Under supernetting, the classful subnet masks are extended so that a network address and subnet mask could, for example, specify multiple Class C subnets with one address. For example, If I needed about 1000 addresses, I could supernet 4 Class C networks together:

192.60.128.0 (11000000.00111100.10000000.00000000) Class C subnet address

192.60.129.0 (11000000.00111100.10000001.00000000) Class C subnet address

192.60.130.0 (11000000.00111100.10000010.00000000) Class C subnet address

192.60.131.0 (11000000.00111100.10000011.00000000) Class C subnet address

---

192.60.128.0 (11000000.00111100.10000000.00000000) Supernetted address

255.255.252.0 (11111111.11111111.11111100.00000000) Subnet Mask

192.60.131.255 (11000000.00111100.10000011.11111111) Broadcast address

In this example, the subnet 192.60.128.0 includes all the addresses from 192.60.128.0 to 192.60.131.255. As you can see in the binary representation of the subnet mask, the Network portion of the address is 22 bits long, and the host portion is 10 bits long.

2.13 CIDR – CLASSLESS INTER DOMAIN ROUTING

One solution that gives the Internet a bit of extra breathing room is CIDR (Classless Inter Domain Routing). The basic idea behind CIDR, which is described in RFC 1519, is to allocate the remaining class C networks, of which there are almost two million, in variable-sized blocks. If a site needs, say, 2000 addresses, it is given a block of 2048 addresses (eight contiguous class C networks), and not a full class B address. Similarly, a site needing 8000 addresses gets 8192 addresses (32 contiguous class C networks).

In addition to using blocks of contiguous class C networks as units, the allocation rules for the class C addresses were also changed in RFC 1519. The world was partitioned into four zones, and each one given a portion of the class C address space. The allocation was as follows:

Addresses 194.0.0.0 to 195.255.255.255 are for Europe

Addresses 198.0.0.0 to 199.255.255.255 are for North America

Addresses 200.0.0.0 to 201.255.255.255 are for Central and South America

Addresses 202.0.0.0 to 203.255.255.255 are for Asia and the Pacific

In this way, each region was given about 32 million addresses to allocate, with another 320 million class C addresses from 204.0.0.0 through 223.255.255.255 held in reserve for the future. The advantage of this allocation is that now any router outside of Europe that gets a packet addressed to 194.xx.yy.zz or 195.xx.yy.zz can just send it to its standard European gateway. In effect 32 million addresses have now been compressed into one routing table entry. Similarly for the other regions.

The routing tables all over Europe are now updated with three entries, each one containing a base address and a mask. These entries (in binary) are:

Address	Mask
11000010 00011000 00000000 00000000	11111111 11111111 11111000 00000000
11000010 00011000 00010000 00000000	11111111 11111111 11110000 00000000
11000010 00011000 00001000 00000000	11111111 11111111 11111100 00000000

Example: Following networks can be represented as single network.

i. 192.168.0.0/24
ii. 192.168.1.0/24
iii. 192.168.2.0/24
iv. 192.168.3.0/24

} 192.168.0.0/22

2.14 VLSM: VARIABLE LENGTH SUBNET MASK

Subnetting creates subnets with equal number of hosts, in a network. The number of bits subnetted i.e. the length of subnet mask will be same for all the subnets. To co-op with the variable number of hosts in subnets, in a network, number subnetted bits i.e. the length of subnet mask for the subnets will also vary. The method of achieving subnetting, with variable length of subnet mask, is known as Variable Length Subnet Mask.

Example:
For the Class – C network 202.195.32.0 determine Network ID, Subnet mask, CIDR notation, IP Range and Broadcast IP for the given network topology.

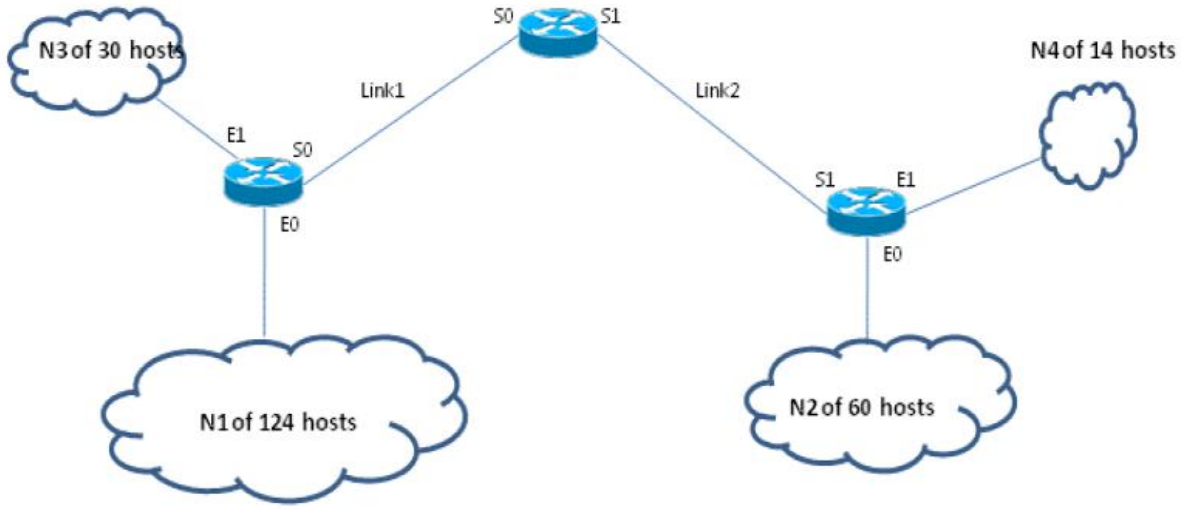


Figure 8: **Example**

Solution:

Step 1:
Calculate the no of bit required for sub netting (no of bits used for host allocation) for each sub network.

For network N1 no of host required is 124
Then required no of bit for host allocation = 7 (2^7 =128)

Network	**No of Host**	**Bit required for subnet**	**Valid Host = 2^n-2**	**Subnet Mask**
N1	124	7	126	/25
N2	60	6	62	/26
N3	30	5	30	/27
N4	14	4	14	/28
Link-1	2	2	2	/30
Link-2	2	2	2	/30

Calculate the subnet mask (subnet mask = 32 – subnetting bit) of each subnetwork.

Get the no of valid host in each subnetwork.

Step 2:

Calculate the IP range of each subnetwork according to the no of required IP address.

For subnetwork N1

No of IP = 128

IP Range is 202.195.32.0 to 202.195.32.127

<table>
<tr><td>202.195.32.0/25
N1 (128)
210.195.32.127</td><td colspan="5"></td></tr>
<tr><td rowspan="6">202.195.32.128/25
(128)

202.195.32.255</td><td>.128/26
N2 (64)
.191</td><td colspan="4"></td></tr>
<tr><td rowspan="5">.192/26
(64)</td><td>.192/27
N3 (32)
.223</td><td colspan="3"></td></tr>
<tr><td rowspan="4">.224/27
(32)</td><td>.224/28
N4(16)
.239</td><td colspan="2"></td></tr>
<tr><td rowspan="3">.240/28
(16)</td><td>.240/29</td><td>.240/30 (Sl-1)(4)</td></tr>
<tr><td></td><td>.244/30(SL-2)(4)</td></tr>
<tr><td>.248/29
(8)</td><td>(free)</td></tr>
</table>

2.15 NETWORK ID, SUBNET MASK, CIDR NOTATION, IP RANGE AND BROADCAST ID OF EACH SUB NETWORK.

Sub Network	N/W ID	Subnet mask	CIDR	IP Range	Broadcast ID
N1 (126 IP)	202.195.32.0	255.255.255.128	/25	202.195. 32.1 to 202.195. 32.126	202.195.32.127
N2 (62 IP)	202.195.32.128	255.255.255.192	/26	202.195. 32.129 to 202.195. 32.190	202.195.32.191
N3 (30 IP)	202.195.32.192	255.255.255.224	/27	202.195. 32.193 to 202.195. 32.222	202.195.32.223
N4 (14 IP)	202.195.32.224	255.255.255.240	/28	202.195. 32.225 to 202.195. 32.238	202.195.32.239
Link1 (2 IP)	202.195.32.240	255.255.255.252	/30	202.195. 32.241 to 202.195. 32.242	202.195.32.243
Link2 (2 IP)	202.195.32.244	255.255.255.252	/30	202.195. 32.245 to 202.195. 32.246	202.195.32.247

2.16 IP ADDRESSING (IPV6)

2.16.1 Introduction

Internet Protocol version 6 (IPv6) is the sixth revision in the development of the Internet Protocol (IP) and the second version of the protocol to be widely deployed. Together with IPv4, it is at the core of standards-based internetworking methods of the Internet.

The current version of IP - IPv4 has not changed substantially since RFC 791, which was published in 1981. IPv4 has proven to be robust, easily implemented, and interoperable. It has stood up to the test of scaling an internetwork to a global utility the size of today's Internet. This is a tribute to its initial design.

However, the initial design of IPv4 did not anticipate the areas like growth of internet, need for simpler configuration, security consideration, support for prioritized and real-time delivery of data etc.

2.17 LIMITATIONS OF IPV4

2.17.1 Addressing Problem

Although the 32-bit address space of IPv4 allows for 4.38 billion addresses, previous and current allocation practices limit the number of public IPv4 addresses to a few hundred million. As a result, public IPv4 addresses have become relatively scarce, forcing many users and some organizations to use a NAT (Network Address Translation) to map a single public IPv4 address to multiple private IPv4 addresses.

Additionally, the rising prominence of Internet-connected devices and appliances ensures that the public IPv4 address space will eventually be depleted.

2.17.2 Routing Crises

Initially, IPv4 addressing scheme was following classful addressing. However, with the expansion of Internet and re-allocation of IPv4 address space, this classful addressing form lost its original shape and transformed into classless addressing by opting for options like subnetting and VLSM. This resulted in loss of aggregation of routes and routing entries have increased tremendously resulting in routing crises for the router for routing the traffic.

2.17.3 End To End Problem

As current IPv4 address space provides only few hundred million public addresses, which are insufficient for fulfilling the need of hosts in the Internet world. In order to overcome this limitation, with the help of NAT single global address is being mapped with private address space. Although NATs promote reuse of the private address space, they violate

the fundamental design principle of the original Internet that all nodes have a unique, globally reachable address, preventing true end-to-end connectivity for all types of networking applications.

2.17.4 Security

Private communication over a public medium such as the Internet requires cryptographic services that protect the data being sent from being viewed or modified in transit. Although a standard now exists for providing security for IPv4 packets (known as Internet Protocol security, or IPsec), this standard is optional for IPv4 and additional security solutions, some of which are proprietary, are prevalent.

2.17.5 Mobility

The problem of mobility for IPv4 was first addressed in a standards track specification, RFC 2002, "IP Mobility Support," in 1996. But this mobility is limited in true sense.

2.17.6 Performance And Cost

The performance of IPv4 network will deteriorate if the infrastructure is not upgraded with time to match the traffic requirement which is increasing with application as well as user base along with routing entries because of increasing network complexity. This also involves cost in terms of trained man-power to maintain it. Also it requires efforts for configuring services like NAT which is mainly because of scarcity of IPv4 resource.

2.18 IPV6 ADDRESS PRESENTATION

2.18.1 Ipv6 Address In Binary Form:

00100001110110100000000011010011000000000000000000010111100111011

00000010101010100000000011111111111111000101000100111000101101O

2.18.2 Divided Into 8 Blocks Of 16 Bit

0010000111011010 0000000011010011 0000000000000000 0010111100111011

0000001010101010 0000000011111111 1111111000101000 1001110001011010

- **Each 16-bit block is converted to hexadecimal and separated with colons:**

21DA : 00D3 : 0000 : 2F3B : 02AA : 00FF : FE28 : 9C5A

Suppression of Zeros

Suppress leading zeros within each 16-bit block:

2000:1110 :1287 : 0003 : F7A9 : 00FF : FE14 : 7AD2

As 2000 :1110 :1287 : 3 : F7A9 : FF : FE14 : 7AD2

But trailing 0s cannot be removed as shown:

2000 : 1110 : 1287 : 3000 : F7A9 : FF00 : FE14 :7AD2

cannot be written as:

2000 : 1110 : 1287 : 3 : F7A9 : FF : FE14 : 7AD2

Compression of Zeros

All zeros in a 16 bit block can be represented by single zero

2345 : 0000 : 0000 : 0000 : 0000 : 1234 : 3458 : AC19

can be represented as :

2345 : 0 : 0 : 0 : 0 : 1234 : 3458 : C19

An Address having more than one zeros can be represented as double colon ::

(Double Colon)

2345 : 0 : 0 : 0 : 0 : 1234 : 3458 : C19

becomes 2345 :: 1234 : 3458 : C19

FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 2 becomes FF02::2

0 : 0 : 0 : 0 : 0 : 0 : 0 : 1 becomes ::1

FF02 : 0 : 0 : 0 : 0 : 0 : 0 : 0 becomes FF02 ::

Double colon :: can be used only once in an address.

2001 : 0 : 0 : 0 : 1234 : 0 : 0 : C1C0

can be written as

2001 :: 1234 : 0 : 0 : C1C0

Or 2001 : 0 : 0 : 0 : 1234 :: C1C0

but not as 2001 :: 1234 :: C1C0

2.19 FEATURES OF IPV6

2.19.1 Large Address Space

IPv6 has 128-bit (16-byte) addresses. Although 128 bits can express over 3.4 × 1038 possible combinations, the large address space of IPv6 has been designed to allow for multiple levels of subnetting and address allocation, from the Internet backbone to the individual subnets within an organization.

Even with all of the addresses currently assigned for use by hosts, plenty of addresses are available for future use. With a much larger number of available addresses, address-conservation techniques, such as the deployment of NATs, are no longer necessary.

2.19.2 Global Reachability

With IPv4 NATs, there is a technical barrier for applications that rely on listening or peer based connectivity because of the need for the communicating peers to discover and advertise their public IPv4 addresses and ports.

With IPv6, NATs are no longer necessary to conserve public address space, and the problems associated with mapping addresses and ports disappear for developers of applications and gateways. More importantly, end-to-end communication is restored between hosts on the Internet by using addresses in packets that do not change in transit. This functional restoration has immense value when one considers the emergence of peer-to-peer telephony, video, and other real-time collaboration technologies for personal communications etc.

By restoring global addressing and end-to-end connectivity, IPv6 has no barrier to new applications that are based on ad hoc connectivity and peer-based communication.

2.19.3 Scoped Address And Address Selection

Unlike IPv4 addresses, IPv6 addresses have a *scope*, or a defined area of the network over which they are unique and relevant. For example, IPv6 has a global address that is equivalent to the IPv4 public address and a unique local address that is roughly equivalent to the IPv4 private address. Typical IPv4 routers do not distinguish a public address from a private address and will forward a privately addressed packet on the Internet. An IPv6 router, on the other hand, is aware of the scope of IPv6 addresses and will never forward a packet over an interface that does not have the correct scope.

There are different types of IPv6 addresses with different scopes. When multiple IPv6 addresses are returned in a DNS name query, the sending node must be able to distinguish their types and, when initiating communication, use a pair (source address and destination address) that is matched in scope and that is the most appropriate pair to use. For example, for a source and a destination that have been assigned both global (public) and link-local addresses, a sending IPv6 host would never use a global destination with a link-

local source. IPv6 sending hosts include the address selection logic that is needed to decide which pair of addresses to use in communication. Moreover, the address selection rules are configurable.

This allows you to configure multiple addressing infrastructures within an organization. Regardless of how many types of addressing infrastructures are in place, the sending host always chooses the "best" set of addresses. In comparison, IPv4 nodes have no awareness of address types and can send traffic to a public address from a private address.

The benefit of scoped addresses is that by using the set of addresses of the smallest scope, your traffic does not travel beyond the scope for the address, exposing your network traffic to fewer possible malicious hosts.

2.19.4 New Header Format

The IPv6 header has a new format that is designed to minimize header processing. This is achieved by moving both nonessential and optional fields to extension headers that are placed after the IPv6 header. The streamlined IPv6 header is more efficiently processed at intermediate routers.

IPv4 headers and IPv6 headers are not interoperable. IPv6 is not a superset of functionality that is backward compatible with IPv4. A host or router must use an

Implementation of both IPv4 and IPv6 to recognize and process both header formats. The new default IPv6 header is only twice the size of the default IPv4 header, even though the number of bits in IPv6 addresses is four times larger than IPv4 addresses.

2.19.5 Stateless And Stateful Address Configuration

To simplify host configuration, IPv6 supports both stateful address configuration (such as address configuration in the presence of a DHCP for IPv6) and stateless address configuration (such as address configuration in the absence of a DHCPv6 server).

With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses), with IPv6 transition addresses, and with addresses derived from prefixes advertised by local routers.

2.19.6 IPsec Header Support Required

Support for the IPsec headers is an IPv6 protocol suite requirement. This requirement provides a standards-based solution for network protection needs and promotes interoperability between different IPv6 implementations. IPsec consists of two types of extension headers and a protocol to negotiate security settings. The Authentication header (AH) provides data integrity, data authentication, and replay protection for the entire IPv6

packet (excluding fields in the IPv6 header that must change in transit). The Encapsulating Security Payload (ESP) header and trailer provide data integrity, data authentication, data confidentiality, and replay protection for the ESP-encapsulated payload.

2.19.7 Better Support For Prioritized Delivery

New fields in the IPv6 header define how traffic is handled and identified. Traffic is prioritized using a Traffic Class field, which specifies a DSCP value just like IPv4. A Flow Label field in the IPv6 header allows routers to identify and provide special handling for packets that belong to a flow (a series of packets between a source and destination). Because the traffic is identified in the IPv6 header, support for prioritized delivery can be achieved even when the packet payload is encrypted with IPsec and ESP.

2.19.8 New Protocol For Neighboring Node Interaction

The Neighbor Discovery protocol for IPv6 is a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages that manages the interaction of neighboring nodes (nodes on the same link). Neighbor Discovery replaces and extends the Address Resolution Protocol (ARP) (broadcast-based), ICMPv4 Router Discovery, and ICMPv4 Redirect messages with efficient multicast and unicast Neighbor Discovery messages.

2.19.9 Extensibility

IPv6 can easily be extended for new features by adding extension headers after the IPv6 header. Unlike options in the IPv4 header, which can support only 40 bytes of options, the size of IPv6 extension headers is constrained only by the size of the IPv6 packet.

2.19.10 Efficient Forwarding

IPv6 is a streamlined version of IPv4. Excluding prioritized delivery traffic, IPv6 has fewer fields to process and fewer decisions to make in forwarding an IPv6 packet. Unlike IPv4, the IPv6 header is a fixed size (40 bytes), which allows routers to process IPv6 packets faster.

Additionally, the hierarchical and summarizable addressing structure of IPv6 global addresses means that there are fewer routes to analyze in the routing tables of organization and Internet backbone routers. The consequence is traffic that can be forwarded at higher data rates, resulting in higher performance for tomorrow’s high-bandwidth applications that use multiple data types.

2.19.11 Support For Security And Mobility

IPv6 has been designed to support security (IPsec) (AH and ESP header support required) and mobility (Mobile IPv6) (optional). Although one could argue that these features are available for IPv4, they are available on IPv4 as extensions, and therefore they have

architectural or connectivity limitations that might not have been present if they had been part of the original IPv4 design. It is always better to design features in rather than bolt them on. The result of designing IPv6 with security and mobility in mind is an implementation that is a defined standard, has fewer limitations, and is more robust and scalable to handle the current and future communication needs of the users of the Internet.

The business benefit of requiring support for IPsec and using a single, global address space is that IPv6 can protect packets from end to end across the entire IPv6 Internet. Unlike IPsec on the IPv4 Internet, which must be modified and has limited functionality when the endpoints are behind NATs, IPsec on the IPv6 Internet is fully functional between any two endpoints.

2.20 IPV6 HEADER FORMAT

The format of the IPv6 packet header is simplified from its counterpart in IPv4. The length of the IPv6 header increases to 40 bytes (from 20 bytes) and contains two 16-byte addresses (source and destination), preceded by 8 bytes of control information, as shown in Figure.

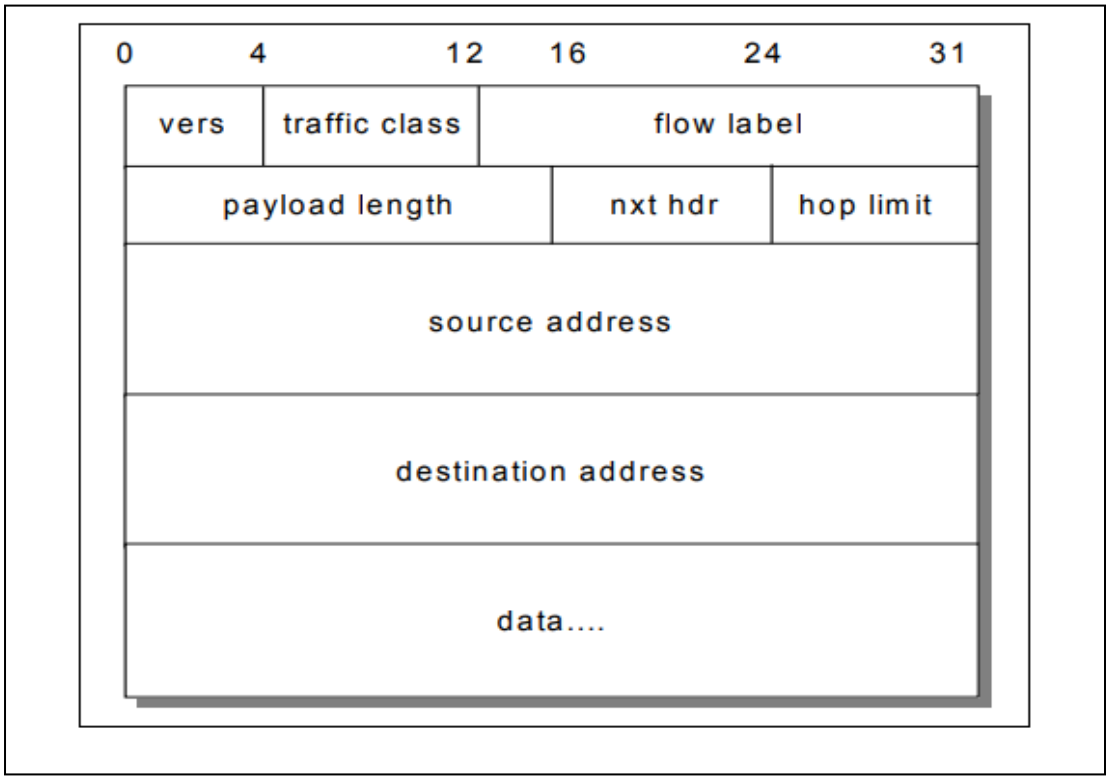


Figure 9: **Ipv6 header format**

The IPv4 header has two 4-byte addresses preceded by 12 bytes of control information and possibly followed by option data. The reduction of the control information and the elimination of options in the header for most IP packets optimizes the processing time per packet in a router. The infrequently used fields removed from the header are moved to optional extension headers when they are required.

The IPv6 header has 8 fields and is 320 bits long. It has been considerably streamlined compared to its IPv4 counterpart, which has 12 fields and is 160 bits long.

Field	**Length**	**Description**
Version	4 bits	Version of IP (in this case, IPv6)
Traffic Class	8 bits	Classifies traffic for QoS
Flow Label	20 bits	Identifies a flow between a source and destination
Payload Length	16 bits	Length of data in packet
Next Header	8 bits	Specifies the next upper-layer or extension header
Hop Limit	8 bits	Decremented by each router traversed
Source Address	128 bits	Source IPv6 address
Destination Address	128 bits	Destination IPv6 address

The Next Header field is of some importance. This field can identify either the next upper-layer header (for example, UDP, TCP or ICMP), or it can identify a special Extension Header, which placed in between the IPv6 and upper layer header.

Several such extension headers exist, and are usually processed in the following order:

Hop-by-Hop Options – specifies options that should be processed by every router in the path. Directly follows the IPv6 header.

Destination Options – specifies options that should be processed by the destination device.

Routing Header – specifies each router the packet must traverse to reach the destination (source routing)

Fragment Header – used when a packet is larger than the MTU for the path

Authentication Header – used to integrate IPSEC Authentication Header (AH) into the IPv6 packet

ESP Header – used to integrate IPSEC Encapsulating Security Payload (ESP) into the IPv6 packet

2.21 IPV6 PREFIXES & TYPES OF IPV6

Prefix is the part of the address where the bits have fixed values or are the bits of a route or subnet identifier.

Prefixes for IPv6 subnet identifiers, routes, and address ranges are expressed in the same way as Classless Inter-Domain Routing (CIDR) notation for IPv4.

An IPv6 prefix is written in address/prefix-length notation.

Examples:

21DA:D3::/48 for a route

21DA:D3:0:2F3B::/64 for a subnet

No more dotted decimal subnet masks

Typical unicast IPv6 address:

64 bits for subnet ID, 64 bits for interface ID

Full Address: 1254:1532:26B1:CC14:123:1111:2222:3333/64

Prefix ID: 1254:1532:26B1:CC14:

Host ID: 123:1111:2222:3333

The /64 indicates that the first 64 bits of this address identify the prefix.

2.21.1 The IPv6 Interface Id And Eui-64 Format

The host portion of an IPv4 address is not based on the hardware address of an interface. IPv4 relies on **Address Resolution Protocol (ARP)** to map between the logical IP address and the **48-bit** hardware **MAC address**.

IPv6 unicasts generally allocate the first 64 bits of the address to identify the network (**prefix**), and the last 64 bits to identify the host (referred to as the **interface ID**). The interface ID *is* based on the interface's hardware address.

This interface ID adheres to the IEEE **64-bit Extended Unique Identifier** (**EUI-64**) format. Since most interfaces still use the 48-bit MAC address, the MAC must be converted into the EUI-64 format.

Consider the following MAC address: 1111.2222.3333. The first 24 bits, the Organizationally Unique Identifier (OUI), identify the manufacturer. The last 24 bits uniquely identify the host. To convert this to EUI-64 format:

1. The **first 24 bits** of the MAC **(**the **OUI**), become the first 24 bits of the EUI-64 formatted interface ID.
2. The ***seventh*** bit of the OUI is changed from a "**0**" to a "**1**".
3. The next 16 bits of the interface ID are **FFFE.**
4. The **last 24 bits** of the MAC (the **host ID**), become the last 24 bits of the interface ID.

Thus, the MAC address 1111.2222.3333 in EUI-64 format would become

1311:22FF:FE22:3333, which becomes the interface ID.

2.22 THE IPV6 ADDRESS HIERARCHY

IPv4 separated its address space into specific **classes.** The class of an IPv4 address was identified by the high-order bits of the first octet:

- **Class A** - (00000001 – 01111111, or 1 - 127)
- **Class B -** (10000000 – 10111111, or 128 - 191)
- **Class C -** (11000000 – 11011111, or 192 - 223)
- **Class D -** (11100000 – 11101111, or 224 - 239)

IPv6's addressing structure is far more scalable. Less than 20% of the IPv6 address space has been designated for use, currently. The potential for growth is enormous.

The address space that *has* been allocated is organized into several types, determined by the high-order bits of the first field:

- **Special Addresses –** addresses begin **00*xx*:**
- **Link Local –** addresses begin **FE8*x*:**
- **Site Local –** addresses begin **FEC*x*:**
- **Aggregate Global –** addresses begin **2*xxx*:** or **3*xxx*:**
- **Multicasts –** addresses begin **FF*xx*:**
- **Anycasts**

(Note: an "x" indicates the value can be any hexadecimal number)

There are **no broadcast addresses** in IPv6. Thus, any IPv6 address that is not a multicast is a unicast address.

Anycast addresses identify a group of interfaces on multiple hosts. Thus, multiple hosts are configured with an *identical* address. Packets sent to an anycast address are sent to the *nearest* (i.e., least amount of hops) host.

Anycasts are indistinguishable from any other IPv6 unicast address.

Practical applications of anycast addressing are a bit murky. One possible application would be a server farm providing an identical service or function, in which case anycast addressing would allow clients to connect to the nearest server.

2.22.1 Special (Reserved) Ipv6 Addresses

The first field of a **reserved** or **special** IPv6 address will always begin **00*xx*.**

Reserved addresses represent 1/256th of the available IPv6 address space. Various reserved addresses exist, including:

- **0:0:0:0:0:0:0:0** (or **::**) – is an **unspecified** or **unknown** address. It is the equivalent of the IPv4 0.0.0.0 address, which indicates the absence of a configured or assigned address. In routing tables, the unspecified address is used to identify **all** or **any** possible hosts or networks.

- **0:0:0:0:0:0:0:1 (**or **::1**) – is the **loopback** or **localhost** address. It is the equivalent of the IPv4 127.0.0.1 address.

RESERVED ADDRESSES - IPV4 AND IPV6 COMPATIBILITY

To alleviate the difficulties of immediately migrating from IPv4 to IPv6, specific reserved addresses can be used to *embed* an IPv4 address into an IPv6 address.

Two types of addresses can be used for IPv4 embedding, **IPv4-compatible IPv6 addresses**, and **IPv4-mapped IPv6 addresses**.

0:0:0:0:0:0:a.b.c.d (or **::a.b.c.d)** – is an **IPv4-compatible IPv6 address**. This address is used on devices that support both IPv4

- and IPv6. A prefix of /96 is used for IPv4-compatible IPv6 addresses:

2001 ::192.168.1.1/96

- **0:0:0:0:0:FFFF:a.b.c.d** (or **::FFFF:a.b.c.d) –** is an **IPv4-mapped IPv6 address.** This address is used by IPv6 routers and devices to identify non-IPv6 capable devices. Again, a prefix of /96 is used for IPv4-mapped IPv6 addresses:

2002 ::FFFF:192.168.1.1/96

2.23 LINK-LOCAL IPV6 ADDRESSES

Link-local IPv6 addresses are used only on a single link (subnet). Any packet that contains a link-local source or destination address is *never routed* to another link. Every IPv6-enabled interface on a host (or router) is assigned a link-local address. This address can be manually assigned, or auto-configured.

The first field of a link-local IPv6 address will always begin FE8x (1111 1110 10). Link-local addresses are unicasts, and represent 1/1024th of the available IPv6 address space. A prefix of /10 is used for link-local addresses**.**

FE80::1311:22FF:FE22:3333/10

There is no hierarchy to a link-local address:

- The first 10 bits are fixed (**FE8**), known as the **Format Prefix (FP).**
- The next 54 bits are set to **0.**
- The final 64 bits are used as the **interface ID**.

2.24 SITE LOCAL IPV6 ADDRESSES

Site-local IPv6 addresses are the equivalent of "private" IPv4 addresses. Site-local addresses can be routed within a *site* or *organization*, but cannot be globally routed on the Internet. Multiple private subnets within a "site" are allowed.

The first field of a **site-local** IPv6 address will always begin **FECx (1111 1110 11).** Site-local addresses are **unicasts,** and represent 1/1024th of the available IPv6 address space.

FEC0::2731:E2FF:FE96:C283/64

Site-local addresses do adhere to a hierarchy:

- The first 10 bits are the fixed FP (**FEC**).
- The next 38 bits are set to **0.**
- The next 16 bits are used to identify the **private subnet ID**.
- The final 64 bits are used as the **interface ID**. To identify two separate subnets

(1111 and 2222):

FEC0::1111:2731:E2FF:FE96:C283/64
FEC0::2222:97A4:E2FF:FE1C:E2D1/64

2.25 AGGREGATE GLOBAL IPV6 ADDRESSES

Aggregate Global IPv6 addresses are the equivalent of "public" IPv4 addresses. Aggregate global addresses can be routed publicly on the Internet. Any device or site that wishes to traverse the Internet must be uniquely identified with an aggregate global address.

Currently, the first field of an **aggregate global** IPv6 address will always begin **2*xxx* (001).** Aggregate global addresses are **unicasts,** and represent $1/8^{th}$ of the available IPv6 address space.

2000::2731:E2FF:FE96:C283/64

Aggregate global addresses adhere to a very strict hierarchy:

- The first 3 bits are the fixed FP.
- The next 13 bits are the **top-level aggregation identifier (TLA ID).**
- The next 8 bits are **reserved** for future use.
- The next 24 bits are the **next-level aggregation identifier (NLA ID).**
- The next 16 bits are the **site-level aggregation identifier (SLA ID).**
- The final 64 bits are used as the **interface ID**.

By have multiple **levels**, a consistent, organized, and scalable hierarchy is maintained. High level registries are assigned ranges of TLA IDs. These can then be subdivided in the NLA ID field, and passed on to lower-tiered ISPs.

Such ISPs allocate these prefixes to their customers, which can further subdivide the prefix using the SLA ID field, to create whatever local hierarchy they wish. The 16-bit SLA field provides up to 65535 networks for an organization.

Note: Do not confuse the SLA ID field of a global address field, with a site- local address. Site-local addresses cannot be routed publicly, where as SLA ID's are just a subset of the publicly routable aggregate global address.

2.26 MULTICAST IPV6 ADDRESSES

Multicast IPv6 addresses are the equivalent of IPv4 multicast addresses. Interfaces can belong to one or more multicast **groups**. Interfaces will accept a multicast packet only if they belong to that group. Multicasting provides a much more efficient mechanism than **broadcasting**, which requires that every host on a link accept and process each broadcast packet.

The first field of a **multicast** IPv6 address will always begin **FF*xx* (1111 1111).** The full multicast range is **FF00** through **FFFF**. **Multicasts** represent 1/256th of the available IPv6 address space.

FF01:0:0:0:0:0:0:1

Multicast addresses follow a specific format:

- The first 8 bits **identify the address** as a **multicast** (1111 1111)
- The next 4 bits are a **flag value**. If the flag is set to all zeroes (0000), the multicast address is considered *well-known*.
- The next 4 bits are a **scope value**:
    - 0000 (0) = Reserved
    - 0001 (1) = Node Local Scope
    - 0010 (2) = Link Local Scope
    - 0101 (5) = Site Local Scope
    - 1000 (8) = Organization Local Scope
    - 1110 (e) = Global Scope
    - 1111 (f) = Reserved
- The final 112 bits identify the actual **multicast group**.

IPv4 multicast addresses had no mechanism to support multiple "**scopes."** IPv6 scopes allow for a multicast hierarchy, a way to *contain* multicast traffic.

2.27 COMMON IPV6 MULTICAST ADDRESSES

The following is a list of common, well-known IPv6 multicast addresses:

Node-Local Scope Multicast Addresses

- FF01::1 – All-nodes address
- FF01::2 – All-routers address

Link-Local Scope Multicast Addresses

- FF02::1 – All-nodes address
- FF02::2 – All-routers address
- FF02::5 – OSPFv3 (OSPF IPv6) All SPF Routers
- FF02::6 – OSPFv3 Designated Routers
- FF02::9 – RIPng Routers
- FF02::13 – PIM Routers

Site-Local Scope Multicast Addresses

- FF05::2 – All-routers address

All hosts must join the **all-nodes** multicast group, for both the node-local and link-local scopes. All routers must join the **all-routers** multicast group, for the node-local, link-local, and site-local scopes.

Every site-local and aggregate global address is assigned a **solicited-node multicast** address. This solicited-node address is created by appending the last 24 bits of the interface ID to the following prefix: FF02::1:FF/103.

Thus, if you have a site-local address of:

FEC0::1111:2731:E2FF:FE96:C283

The corresponding solicited-node multicast address would be:

FF02::1:FF96:C283

Solicited-node multicast addresses are most often used for neighbor discovery (covered in an upcoming section in this guide).

2.28 REQUIRED IPV6 ADDRESSES

At a minimum, each IPv6 interface on a **host** must recognize the following IPv6 addresses:

- The loopback address
- A link-local address
- Any configured site-local or aggregate global addresses
- Any configured multicast groups
- The all-nodes multicast address (both node-local and link-local scopes)
- The solicited-node multicast address for any configured unicast addresses

In addition to the above addresses, each IPv6 interface on a **router** must recognize the following IPv6 addresses:

- The subnet-router anycast address
- Any configured multicast groups
- The all-routers multicast address (node-local, link-local, and site-local scopes)

2.29 CONCLUSION

IPv4 address is a 32 bit number which is used to identify network devices on the network. Since, the complete IPv4 address space is finite number i.e. 4.38 billion addresses out of which few hundred million addresses are usable for Internet; therefore, it is vital to efficiently manage this resource for proper functioning of network and Internet. Understanding the addressing concepts helps in building the network and provisioning of addresses to various network components. This has been done with Subnetting, VLSM and to aggregate the routes CIDR is used.

There are many reasons for IPv6 support and there is also a need to migrate from the current version of Internet IPv4 to IPv6 for availing additional benefits of Internet. However, for quite some time, things will move in parallel and smooth transition will be in benefit for the Internet world. Therefore, we will see IPv4 and IPv6 simultaneously being used by the Internet users, and the service provider. Also the application that will be developed during this phase will also keep in mind the requirement of IPv4 and IPv6.

3 MULTIPLAY BROADBAND NETWORK & SERVICES

3.1 LEARNING OBJECTIVES

- Broadband Multiplay – Components & Architecture
- Customer Premises Equipments and installation
- Broadband Multiplay Services

3.2 WHAT IS BB MULTIPLAY?

The multiplay service means providing the multiple service to the customer, which are as follows: -

- Data (Internet)
- Voice (VoIP and not the PSTN which is already provided on broadbandalso)

Video (IPTV, VoD or in general live broadcast and stored broadcasting using video streaming protocols)

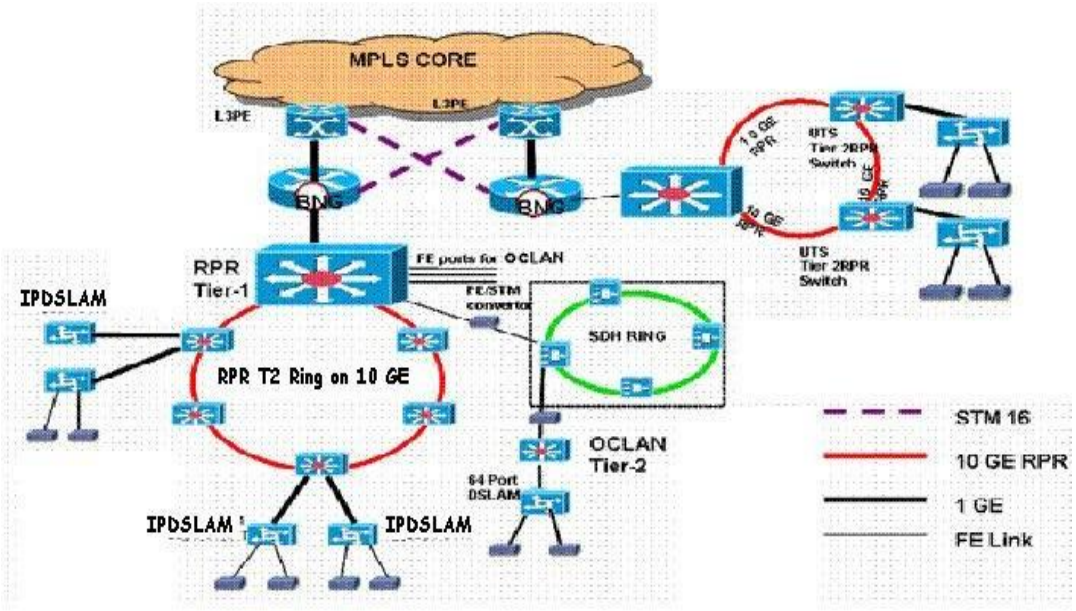


Figure 10: **Architecture Broadband Multiplay**

3.3 COMPONENTS OF BROADBAND MULTIPLAY

The BSNL's Broadband multiplay network consists of the following components:

1. L3PE (MCR / PE Router of NIB-2 Project 1 – Supplied by HCL).
2. BNG – Broadband Network Gateway (Connects Multiplay Network to NIB2 Backbone Project 1, through L3PE).

3. RPR (Tier-1 Switch and Tier-2 switches in the ring Provides connectivityto BNG & vice versa).
4. OC LAN Tier-2 Switch.
5. DSLAM.
6. ADSL CPE.
7. DSL Tester

3.3.1 DSLAM

DSL Access Multiplexor or Demultiplexor.

- Supports PPP and ATM for xDSL services.
- Supports GE and FE connectivity for uplink, cascading, and other types of data connectivity.
- Supports VLAN.

3.3.2 RPR

Resilient Packet Ring(RPR) Switch:

- The traffic from access devices and remote aggregation devices is aggregated in RPR and forwarded to the Core Network.
- Resilience: Proactive span protection automatically avoids failed span within 50ms.
- Ring Topology gives the scalable option of having more than 100 nodes in a ring.
- RPR has the ability to differentiate between low & high priority packets.

3.3.3 Broadband Network Gateway(BNG)

- It routes traffic to and from broadband remote access devices DSLAMs /OLTs on an Internet service provider's (ISP) network.
- It works as Multi Service Edge Router(MSER).
- Service specific logical mini routers are configured in BNG called context or routing instances.
- BNG maps the traffic coming from access networks elements and forward to uplink L3PE VLANs IP MPLS Network through corresponding service context.
- Authentication, Authorization and accounting processes happen via radius servers configured logically in BNG.

3.3.4 Customer Premises Equipments

Splitter:

- The filter separates out the signal for telephone i.e. voice and data signals are segregated and vice versa.
- High Pass and Low Pass Filter used at both ends, CPE and ACCESS NE sides.

- CPE(Modem /ONT):
- The CPE directs the signal to PC and TV. Service Specific ATM PVC Values and subscribers' secrets are configured.
- Enable security features to avoid botnet and Man in the Middle(MITM) attacks.

3.3.5 Customer Premises Installation

Single User (SU): Only one PC can be connected to BSNL Broadband connection.

Multi User (MU): Customer is allowed to share one BSNL broadband connection among multiple PCs (Often a need of Cyber Cafes, Business setups)

Static IP address: For many services such as video conferencing, VPN etc. a fixed IP known as Static IP is required.

Dynamic IP: For normal internet browsing, the customer does not require static IP. In such cases, BSNL allocates temporary IP address to the customer when a session is initiated.

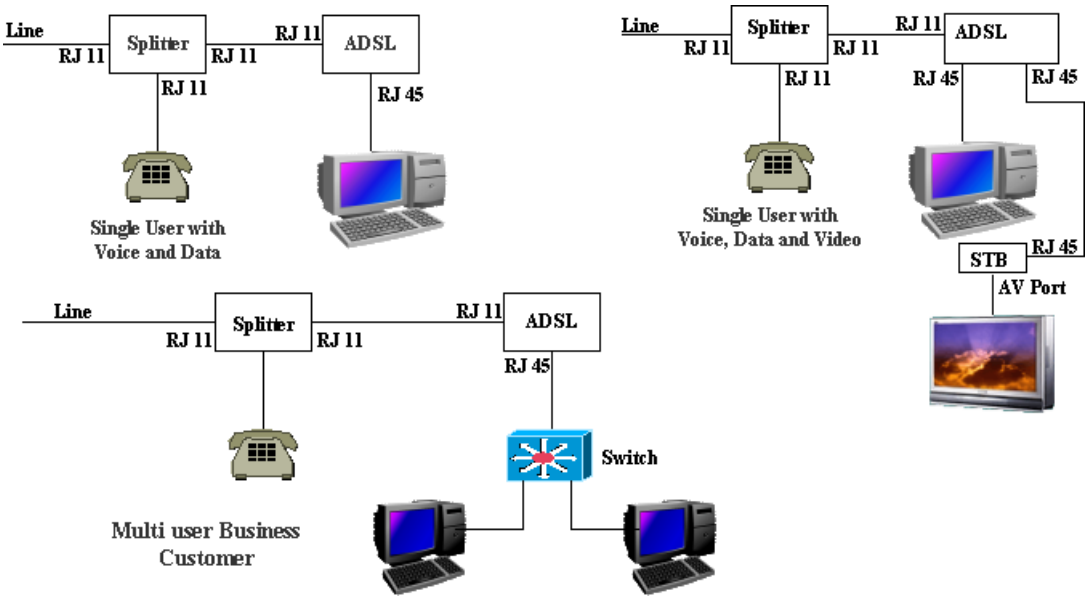


Figure 11: **CPE Installation**

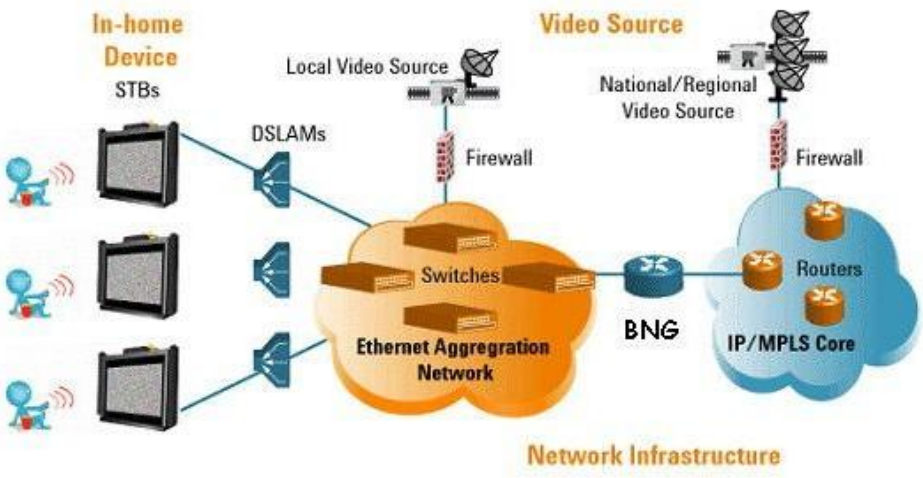


Figure 12: **Network Infrastructure**

3.4 SERVICES

- IPTV/ TVoIP
- Video on Demand (VoD)
- Games on Demand (GoD)

IPTV or TVoIP delivers television programming to households via broadband connection using Internet protocols. It requires a subscription and IPTV set-top box(STB), this box will connect to the home DSL line and is responsible for reassembling the packets into a video stream and then decoding the contents. IPTV is typically bundled with other services like Video on Demand (VOD), Voice Over IP (VOIP) or digital Phone, and Web access. IPTV viewers will have full control over functionality such as rewind, fast-forward, pause, and so on.

If you've ever watched a video clip on your computer, you've used an IPTV system. The video stream is broken up into IP packets and dumped into the core network, which is a massive IP network that handles all sorts of other traffic (data, voice, etc.). VOD (Video on Demand) service allows the user the luxury of watching the movie of his / her choice at his / her convenience.

3.5 DIFFERENCE BETWEEN VOD ON BB & VOD ON DTH

In DTH, as it is broadcasting and not communication so the request for VOD has to be registered through some other mean than the Set top Box say can be through phone call, SMS or Internet and the same four to five movies are broadcasted and the viewers have to choose among them only and at predefined timings.

In true VOD, as offered by BSNL, the set-top box behaves just like a DVD player and viewer can select a movie from the boutique, view it at his / her desired time and day, pause it, rewind it, forward it or can have the exactly same experience has viewing froma personalized DVD player. This is only possible because of the two-way communication between the set-top box and the server. In BSNL one has a choice of selecting from hundreds of movies while VOD offered by DTH providers may haveonly few movies to offer.

3.6 SET-TOP-BOX

The set-top box is a smart solid-state device that acts as the gateway to a host of services offered on the BSNL Multiplay network. On one side the set-top box interfaces with the television using the 3-RCA or the S-Video ports, and on the other side it is connected to broadband ADSL modem via the Ethernet port. BSNL franchisee in Pune has named the set-top box as WICE Box (Window for Information, Communication and Entertainment) and supports all sorts of inputs like audio, video, tablet data, text data, pointer devices etc. it has a USB port and a microphone and headphone jack in addition to essential ports. In future, it will be possible to connect keyboard, mouse, web cams, pen-drives and other such devices for various applications that will be provided on the box. The WICE box is fully upgradeable through the network. This means, any newapplication launched will be directly uploaded into WICE box without getting the boxto service center. All software upgrade will be handled this way.

3.7 VOIP

- The technology used to transmit voice conversations over a data network using the Internet Protocol.
- A category of hardware and software that enables people to use the Internetas the transmission medium for telephone calls.
- VoIP works through sending voice information in digital form in packets,
- VoIP also is referred to as Internet telephony, IP telephony, or Voice overthe Internet (VOI)

3.8 CONCLUSION

Broadband Multiplay network provides voice, data and video services, and hence called multiplay (Multiple Services). Major components CPE, DSLAM, RPR Switches, monitors each and every packet and its quality parameters and accordingly provides services to end users.

4 OVERVIEW OF OFC NETWORK

4.1 LEARNING OBJECTIVES

- Fiber-Optic Applications
- Basic optical fiber communication system:
- The Structure of an Optical Fiber
- Principle of Operation

4.2 INTRODUCTION

The use of light for transmitting information from one place to another place is a very old technique. In 800 BC., the Greeks used fire and smoke signals for sending information like victory in a war, alerting against enemy, call for help, etc. Mostly only one type of signal was conveyed. During the second century B.C. optical signals were encoded using signaling lamps so that any message could be sent. There was no development in optical communication till the end of the 18th century. The speed of the optical communication link was limited due to the requirement of line of sight transmission paths, the human eye as the receiver and unreliable nature of transmission paths affected by atmospheric effects such as fog and rain.

In the late 19th and early 20th centuries, light was guided through bent glass rods to illuminate body cavities. Alexander Graham Bell invented a 'Photophone' to transmit voice signals over an optical beam. By 1964, a critical and theoretical specification was identified by Dr. Charles K. Kao for long-range communication devices, the 10 or 20 dB of light loss per kilometer standard. Dr. Kao also illustrated the need for a purer form of glass to help reduce light loss. By 1970 Corning Glass invented fiber-optic wire or "optical waveguide fibers" which was capable of carrying 65,000 times more information than copper wire, through which information carried by a pattern of light waves could be decoded at a destination even a thousand miles away. Corning Glass developed fiber with loss of 17 dB/ km at 633 nm by doping titanium into the fiber core. By June of 1972, multimode germanium-doped fiber had developed with a loss of 4 dB per kilometer and much greater strength than titanium-doped fiber.

In April 1977, General Telephone and Electronics tested and deployed the world's first live telephone traffic through a fiber-optic system running at 6 Mbps, in Long Beach, California. They were soon followed by Bell in May 1977, with an optical telephone communication system installed in the downtown Chicago area, covering a distance of 1.5 miles (2.4 kilometers). Each optical-fiber pair carried the equivalent of 672 voice

channels. Today more than 80 percent of the world's long-distance voice and data traffic is carried over optical-fiber cables.

An **optical fiber** is a thin, flexible, transparent fiber that acts as a waveguide, or "light pipe", to transmit light between the two ends of the fiber. Optical fibers are widely used in fiber-optic communications, which permits transmission over longer distances and at higher bandwidths (data rates) than other forms of communication. Fibers are used instead of metal wires because signals travel along them with less loss and are also immune to electromagnetic interference.

With increase in population struggle for survival increased Its impacts on appearing in human life in many ways. There have been shortage of utilizes resources. The resources consist of materials, technology, money, human recourse, information, interconnectivity etc.

Due to consistent pressure there has been different ways of innovations in almost every stream of life. In the field of telecommunication also development are happening in the fields of client terminals access technique, aggregation technique, multiplexing technique, transport technique. There has been different access technique and different type of client terminals as per respective access technique. The basic contents were limitations of transmission media and low order multiplexing and switching. The initial transmission started with attaching information leaflet with visions. The same concept was utilized on building semaphore. That came the evolution telegraphs lines after the invention of more score in which use of guided media has got important. In this era use of open wire communications having overhead line with minimal multiplexing was the latest things. However has the requirement of reliable telecommunication has increased need was well to have proper voice communications and switching like manual, electro mechanical, fully digital involving automatic increasing order of multiplexing were implemented. In this era the main access network comprised of cable network made up of copper and transmission network was predominately of over head lines. Later on seeing the limitations of over head lines like deterioration weather due to electro magnetite interference less carrying capacity ete. were found. Use of optical fibre as a transmission media got thrust due to less cost, improve technology in multiplexing, virtually infants capacity and immunity to electro-magnetic interference. Requirement of bandwidth which was around 20Kbps have reached to around 1Gbps. The accesses network is also converging with the development of IP & MPLS technologies of dada communication. Multiplexing is also migrating in TDM, FDM to packet base statistical multiplexing. Client terminals are also converging having all capabilities of voice, video, text, web and multimedia. The network is converging to one by using architecture of Next Generation network. Applications which were accesses network depended are also becoming universally accessible and a accesses network agnostic. The human interface is also improve presentably because of manufacturing line terminal incorporating signals of sensory organs like touch, vision, mind etc.. Today client terminals have improve GUI

based web interface having faster processing multimedia capacity and capability to communicate to multiple secessions over multiple windows having full mobility as well as portability.

Due to competitions and rapid growth of innovation, the world are become faster and expectations of prominent service delivery are also been increased. Delay in providing services has also been reduced and overall connectivity in becoming P-P i.e. pair to pair.

4.3 FIBER-OPTIC APPLICATIONS

The use and demand for optical fiber has grown tremendously and optical-fiber applications are numerous. Telecommunication applications are widespread, ranging from global networks to desktop computers. These involve the transmission of voice, data, or video over distances of less than a meter to hundreds of kilometers, using one of a few standard fiber designs in one of several cable designs.

- Long distance communication backbones
- Inter-exchange junctions
- Video transmission
- Broadband services
- Computer data communication (LAN, WAN etc.)
- High EMI areas
- Non-communication applications (sensors etc…)

4.4 ADVANTAGES OF OPTICAL FIBER COMMUNICATION

Fiber Optics has the following advantages:

Wider bandwidth: The information carrying capacity of a transmission system is directly proportional to the carrier frequency of the transmitted signals. The optical carrier frequency is in the range 10^{13} to 10^{15} Hz while the radio wave frequency is about 10^{6} Hz and the microwave frequency is about 10^{10} Hz. Thus the optical fiber yields greater transmission bandwidth than the conventional communication systems and the data rate or number of bits per second is increased to a greater extent in the optical fiber communication system. Further the wavelength division multiplexing operation by the data rate or information carrying capacity of optical fibers is enhanced to many orders of magnitude.

Low transmission loss: Due to the usage of the ultra low loss fibers and the erbium doped silica fibers as optical amplifiers, one can achieve almost lossless transmission. In the modern optical fiber telecommunication systems, the fibers having a transmission loss of 0.2dB/km are used. Further, using erbium doped silica fibers over a short length in the transmission path at selective points; appropriate optical amplification can be achieved. Thus the repeater spacing is more than 100 km. Since the amplification is done in the optical domain itself, the distortion produced during the strengthening of the signal is almost negligible.

Dielectric waveguide: Optical fibers are made from silica which is an electrical insulator. Therefore they do not pickup any electromagnetic wave or any high current lightning. It is also suitable in explosive environments. Further the optical fibers are not affected by any interference originating from power cables, railway power lines and radio waves. There is no cross talk between the fibers even though there are so many fibers in a cable because of the absence of optical interference between the fibers.

Signal security: The transmitted signal through the fibers does not radiate. Further the signal cannot be tapped from a fiber in an easy manner. Therefore optical fiber communication provides hundred per cent signal security.

Small size and weight: Fiber optic cables are developed with small radii, and they are flexible, compact and lightweight. The fiber cables can be bent or twisted without damage. Further, the optical fiber cables are superior to the copper cables in terms of storage, handling, installation and transportation, maintaining comparable strength and durability.

4.5 FIBER OPTICS BASICS: PRINCIPLES OF OPTICAL COMMUNICATION

Optical Fiber is new medium, in which information (voice, Data or Video) is transmitted through a glass or plastic fiber, in the form of light, following the transmission sequence give below:

(1) Information is encoded into Electrical Signals.

(2) Electrical Signals are converted into light Signals.

(3) Light Travels down the Fiber.

(4) A Detector Changes the Light Signals into Electrical Signals.

(5) Electrical Signals are decoded into Information.

- Inexpensive light sources available.

- Repeater spacing increases along with operating speeds because low loss fibres are used at high data rates.

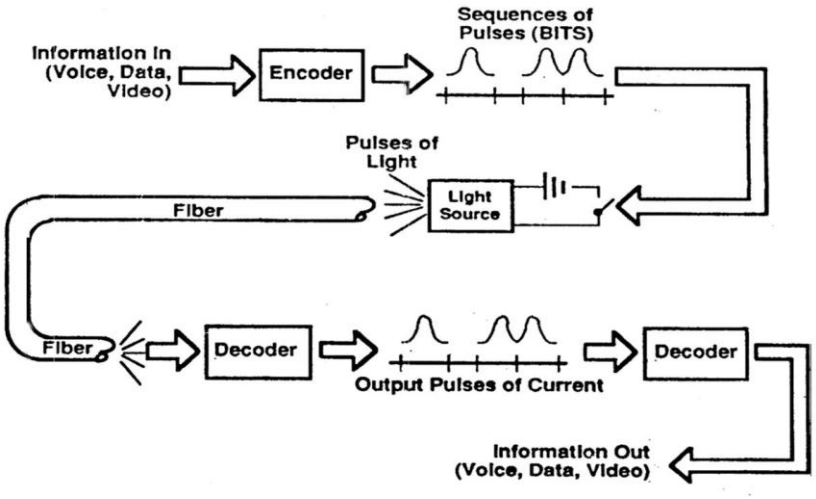


Figure 13: **Fiber Optic System**

4.6 PRINCIPLE OF OPERATION - THEORY

Speed of light is actually the velocity of electromagnetic energy in vacuum such as space. Light travels at slower velocities in other materials such as glass. Light travelling from one material to another changes speed, which results in changing its direction of travel. This deflection of light is called Refraction. The amount that a ray of light passing from a lower refractive index to a higher one, is bent towards the normal, but light going from a higher index to a lower one, refracting away from the normal, as shown in the figures.

The basics of light propagation can be discussed with the use of geometric optics. The basic law of light guidance is Snell's law . Consider two dielectric media with different refractive indices and with n1 >n2 and that are in perfect contact, as shown in Figure. At the interface between the two dielectrics, the incident and refracted rays satisfy Snell's law of refraction—that is,

$n1\sin\phi1 = n2\sin\phi2$

In addition to the refracted ray there is a small amount of reflected light in the medium with refractive index n1. Because n1 is greater than n2 then always **$\phi2 > \phi1$**. As the angle of the incident ray increases there is an angle at which the refracted ray emerges parallel to the interface between the two dielectrics . This angle is referred to as the critical angle, ϕcrit, and from Snell's law is given by

$\sin\phi crit = n2/n1$

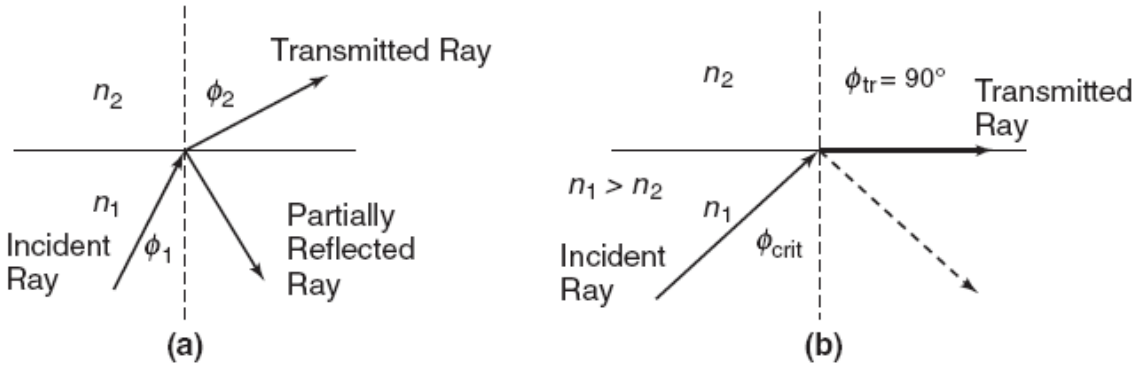


Figure 14:**Snell's law**

If the angle of incidence increases more than the critical angle, the light is totally reflected back into the first material so that it does not enter the second material. The angle of incidence and reflection are equal and it is called **Total Internal Reflection**.

4.6.1 Propagation Of Light Through Fibre

The optical fiber has two concentric layers called the core and the cladding. The inner core is the light carrying part. The surrounding cladding provides the difference refractive index that allows total internal reflection of light through the core. The index of the cladding is approximately 1% lower than that of the core. Typical values for example are a core refractive index of 1.47 and a cladding index of 1.46. Fiber manufacturers control this difference to obtain desired optical fiber characteristics. Most fibers have an additional coating around the cladding. This buffer coating is a shock absorber and has no optical properties affecting the propagation of light within the fiber. Figure shows the idea of light travelling through a fiber. Light injected into the fiber and striking core to cladding interface at greater than the critical angle, reflects back into core, since the angle of incidence and reflection are equal, the reflected light will again be reflected. The light will continue zigzagging down the length of the fiber. Light striking the interface at less than the critical angle passes into the cladding, where it is lost over distance. The cladding is usually inefficient as a light carrier, and light in the cladding becomes attenuated fairly. Propagation of light through fiber is governed by the indices of the core and cladding by Snell's law.

Such total internal reflection forms the basis of light propagation through a optical fiber. This analysis consider only meridional rays- those that pass through the fiber axis each time, they are reflected. Other rays called Skew rays travel down the fiber without passing through the axis. The path of a skew ray is typically helical wrapping around and around the central axis. Fortunately skew rays are ignored in most fiber optics analysis.

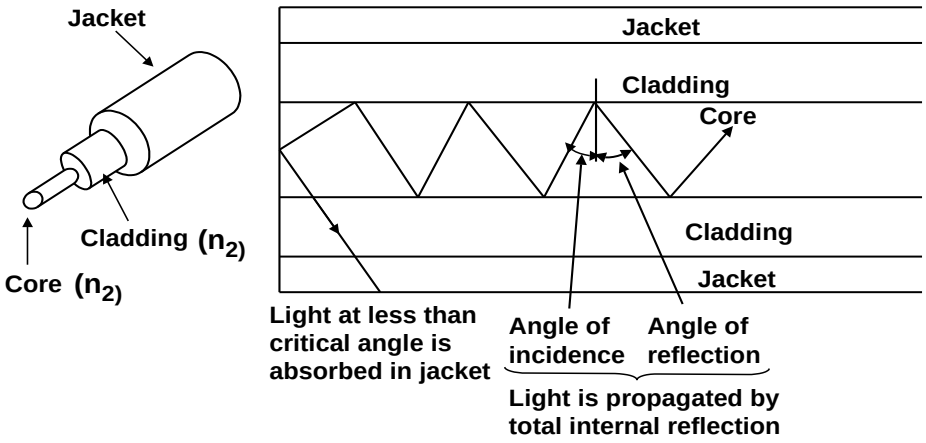


Figure 15: **Propagation of light through fiber**

The specific characteristics of light propagation through a fiber depends on many factors, including

- The size of the fiber.
- The composition of the fiber.

The light injected into the fiber

4.6.2 Geometry Of Fiber

The optical fibers used in communications have a very simple structure. A hair-thin fiber consist of two concentric layers of high-purity silica glass the core and the cladding, which are enclosed by a protective sheath . Core and cladding have different refractive indices, with the core having a refractive index, n1, which is slightly higher than that of the cladding, n2. It is this difference in refractive indices that enables the fiber to guide the light. Because of this guiding property, the fiber is also referred to as an "optical waveguide." As a minimum there is also a further layer known as the secondary cladding that does not participate in the propagation but gives the fiber a minimum level of protection, this second layer is referred to as a coating. Light rays modulated into digital pulses with a laser or a light-emitting diode moves along the core without penetrating the cladding.

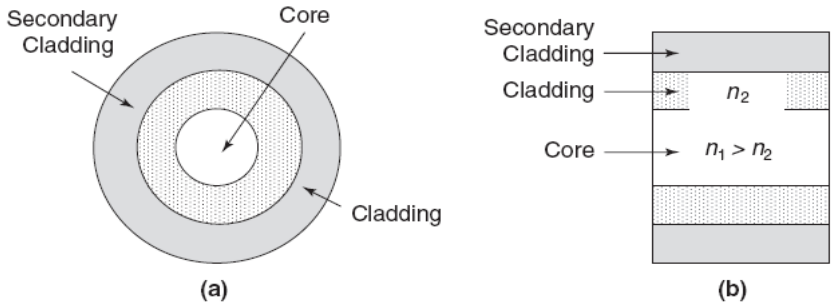


Figure 16: **(a) Cross section (b) longitudinal cross section of a typical optical fiber**

The light stays confined to the core because the cladding has a lower refractive index—a measure of its ability to bend light. Refinements in optical fibers, along with the development of new lasers and diodes, may one day allow commercial fiber-optic networks to carry trillions of bits of data per second.

The light stays confined to the core because the cladding has a lower refractive index—a measure of its ability to bend light. Refinements in optical fibers, along with the development of new lasers and diodes, may one day allow commercial fiber-optic networks to carry trillions of bits of data per second.

The diameters of the core and cladding are as follows.

Core (μm)	**Cladding (μm)**
8	125
50	125
62.5	125
100	140

Fibre sizes are usually expressed by first giving the core size followed by the cladding size. Thus 50/125 means a core diameter of 50μm and a cladding diameter of 125μm.

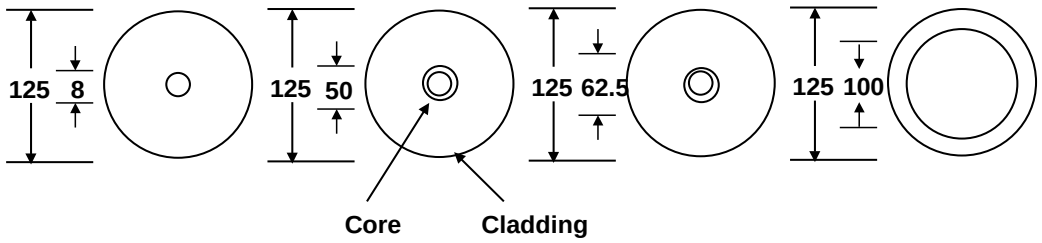


Figure 17: **Typical Core and Cladding Diameter**

4.7 FIBRE TYPES – SINGLE MODE AND MULTI-MODE

The refractive Index profile describes the relation between the indices of the core and cladding. Two main relationships exist:

(I) Step Index

(II) Graded Index

The step index fibre has a core with uniform index throughout. The profile shows a sharp step at the junction of the core and cladding. In contrast, the graded index has a non-uniform core. The Index is highest at the center and gradually decreases until it matches

with that of the cladding. There is no sharp break in indices between the core and the cladding.

By this classification there are three types of fibres :

(I) Multimode Step Index fibre (Step Index fibre)

(II) Multimode graded Index fibre (Graded Index fibre)

(III) Single- Mode Step Index fibre (Single Mode Fibre)

4.7.1 Step-Index Multimode Fiber

Step Index multimode Fiber has a large core, up to 100 microns in diameter. As a result, some of the light rays that make up the digital pulse may travel a direct route, whereas others zigzag as they bounce off the cladding. These alternative pathways cause the different groupings of light rays, referred to as modes, to arrive separately at a receiving point. The pulse, an aggregate of different modes, begins to spread out, losing its well-defined shape. The need to leave spacing between pulses to prevent overlapping limits bandwidth that is, the amount of information that can be sent. Consequently, this type of fiber is best suited for transmission over short distances, in an endoscope, for instance.

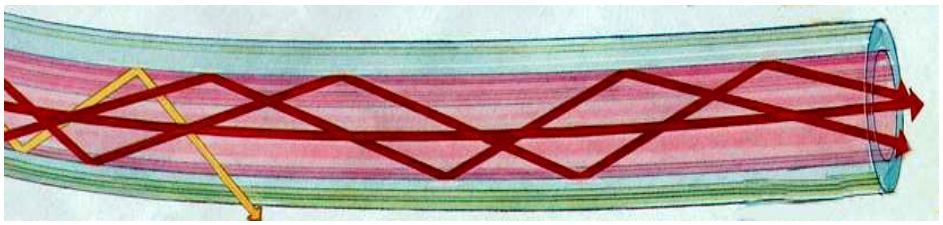


Figure 18: **STEP-INDEX MULTIMODE FIBER**

4.7.2 Graded-Index Multimode Fiber

It contains a core in which the refractive index diminishes gradually from the center axis out toward the cladding. The higher refractive index at the center makes the light rays moving down the axis advance more slowly than those near the cladding.

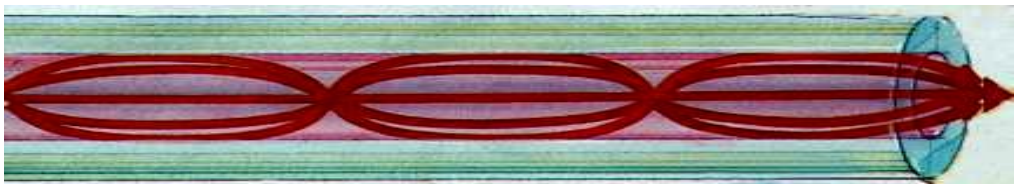


Figure 19: **GRADED-INDEX MULTIMODE FIBER**

Also, rather than zigzagging off the cladding, light in the core curves helically because of the graded index, reducing its travel distance. The shortened path and the higher speed allow light at the periphery to arrive at a receiver at about the same time as the slow but straight rays in the core axis. The result: a digital pulse suffers less dispersion.

4.7.3 Single-Mode Fiber

It has a narrow core (nine microns or less), and the index of refraction between the core and the cladding changes less than it does for multimode fibers. Light thus travels parallel to the axis, creating little pulse dispersion. Telephone and cable television networks install millions of kilometers of this fiber every year.

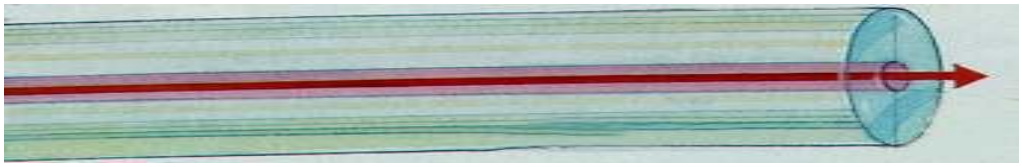


Figure 20: **SINGLE-MODE FIBER**

4.8 CABLE CONSTRUCTION

There are two basic cable designs are:

1. Tight Buffer Tube Cable
2. Loose Buffer Tube Cable

Loose-tube cable is used in the majority of outside-plant installations and tight-buffered cable, primarily used inside buildings.

4.8.1 Tight Buffer Tube Cable

With tight-buffered cable designs, the buffering material is in direct contact with the fiber. This design is suited for "jumper cables" which connect outside plant cables to terminal equipment, and also for linking various devices in a premises network. Single-fiber tight-buffered cables are used as pigtails, patch cords and jumpers to terminate loose-tube cables directly into opto-electronic transmitters, receivers and other active and passive components. Multi-fiber tight-buffered cables also are available and are used primarily for alternative routing and handling flexibility and ease within buildings. The tight-buffered design provides a rugged cable structure to protect individual fibers during handling, routing and connectorization. Yarn strength members keep the tensile load away from the fiber.

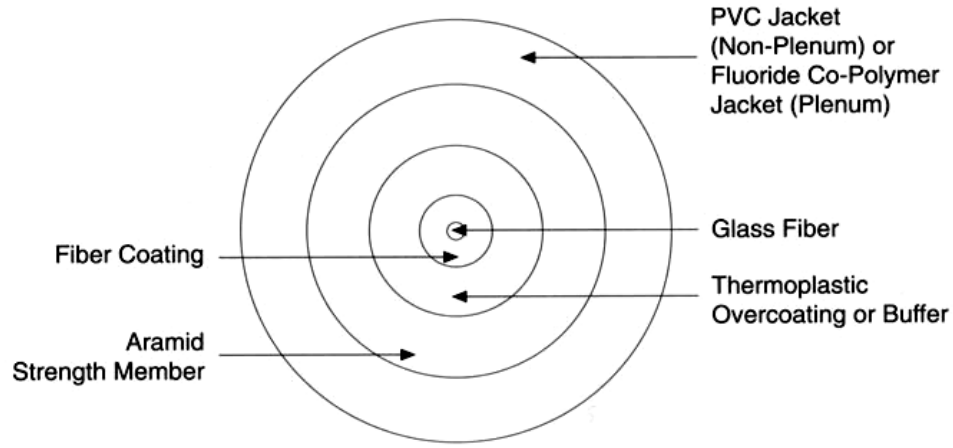


Figure 21: **Tight Buffer Tube Cable**

The structure of a 250um coated fiber (bare fiber)

- Core (9um for standard single mode fibers, 50um or 62.5um for multimode fibers)
- Cladding (125um)
- Coating (soft plastic, 250um is the most popular, sometimes 400um is also used)

4.8.2 Loose-Tube Cable

The modular design of loose-tube cables typically holds **6, 12, 24, 48, 96 or even more than 400 fibers per cable**. Loose-tube cables can be all-dielectric or optionally armored. The loose-tube design also helps in the identification and administration of fibers in the system.

In a loose-tube cable design, color-coded plastic buffer tubes house and protect optical fibers. A gel filling compound impedes water penetration. Excess fiber length (relative to buffer tube length) insulates fibers from stresses of installation and environmental loading. Buffer tubes are stranded around a dielectric or steel central member, which serves as an anti-buckling element.

The cable core, typically uses aramid yarn, as the primary tensile strength member. The outer polyethylene jacket is extruded over the core. If armoring is required, a corrugated steel tape is formed around a single jacketed cable with an additional jacket extruded over the armor. Loose-tube cables typically are used for outside-plant installation in aerial, duct and direct-buried applications.

Loose tube cable is designed to endure outside temperatures and high moisture conditions. The fibers are loosely packaged in gel filled buffer tubes to repel water.

Recommended for use between buildings that are unprotected from outside elements. Loose tube cable is restricted from inside building use.

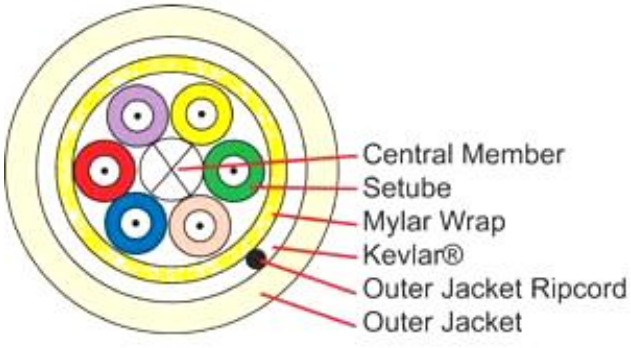


Figure 22: **Loose Tube Cable**

Elements in a loose tube fiber optic cable:

1. Multiple 250um coated bare fibers (in loose tube)
2. One or more loose tubes holding 250um bare fibers. Loose tubes strand around the central strength member.
3. Moisture blocking gel in each loose tube for water blocking and protection of 250um fibers
4. Central strength member (in the center of the cable and is stranded around by loose tubes)
5. Aramid Yarn as strength member
6. Ripcord (for easy removal of inner jacket)
7. Outer jacket (Polyethylene is most common for outdoor cables because of its moisture resistant, abrasion resistant and stable over wide temperature range characteristics.)

4.9 TYPES OF FIBER OPTIC CABLE (MOST POPULAR FIBER OPTIC CABLE TYPES)

4.9.1 INDOOR CABLES

Simplex Fiber Cables

A single cable structure with a single fiber. Simplex cable varieties include 1.6mm & 3mm jacket sizes.

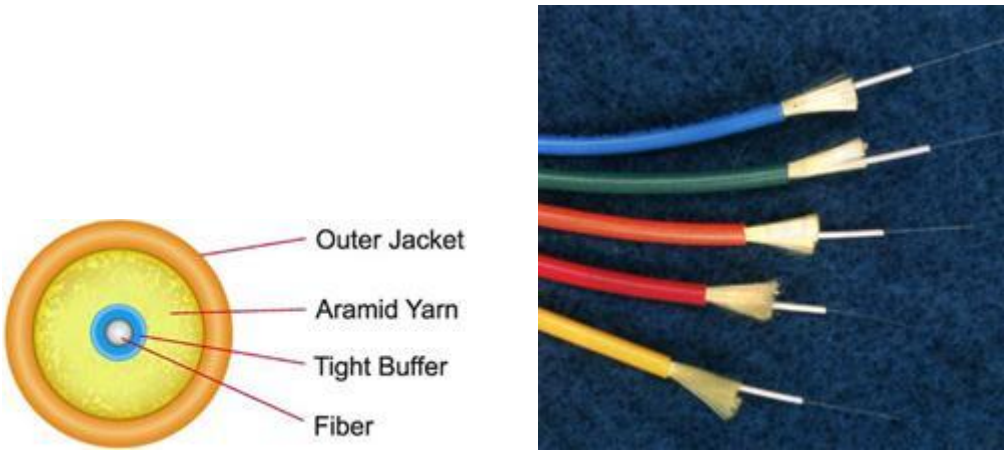


Figure 23: **Simplex Fiber Cables**

a) Duplex Fiber Optic Cable

This cable contains two optical fibers in a single cable structure. Light is not coupled between the two fibers; typically one fiber is used to transmit signals in one direction and the other receives.

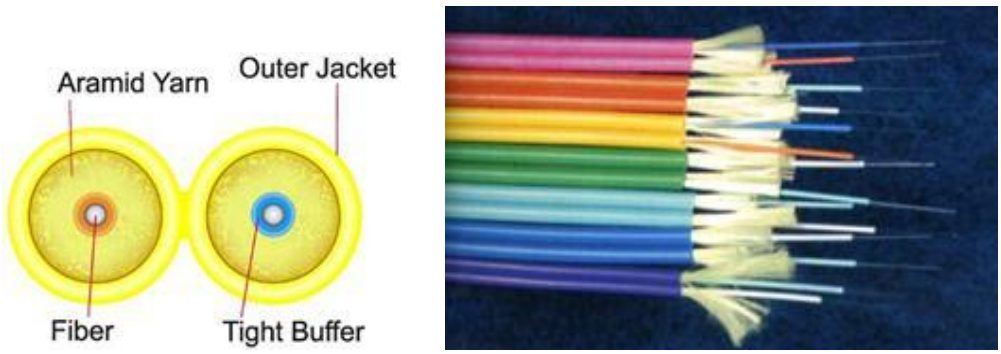


Figure 24: **Duplex Fiber Optic Cable**

4.9.2 Outdoor Loose Tube Fiber Optic Cables

Tube encloses multiple coated fibers that are surrounded by a gel compound that protects the cable from moisture in outside environments. Cable is restricted from indoor use, typically allowing entry not to exceed 50 feet.

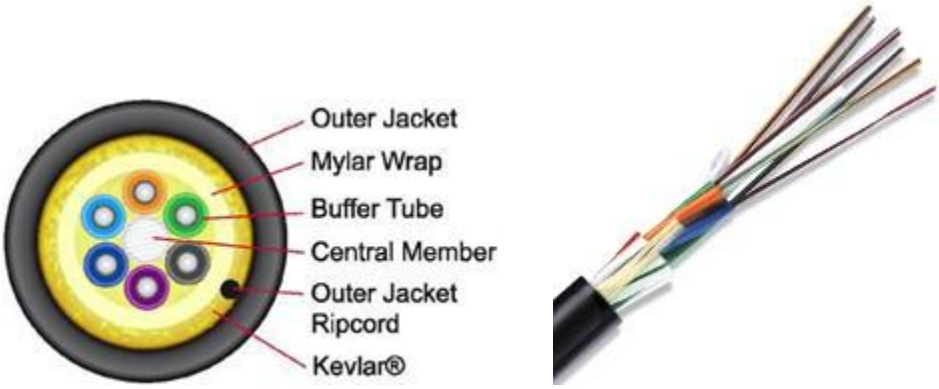


Figure 25: **Outdoor Loose Tube Fiber Optic Cables**

4.9.3 Aerial/Self-Supporting

Figure below (aerial/self-supporting) fiber cables are designed to be strung from poles outdoors and most can also be installed in underground ducts. They have internal stress members of steel of steel or aramid yarn that protect fibers from stress.

Aerial cable provides ease of installation and reduces time and cost. Figure 8 cable can easily be separated between the fiber and the messenger. Temperature range -55 to +85°C.

Figure 26: **Aerial cable**

4.9.4 Direct-Buried Armored Fiber Optic Cable

Armored cables are similar to outdoor cables but include an outer armor layer for mechanical protection and to prevent damage. They can be installed in ducts or aerially, or directly buried underground. Armor is surrounded by a polyethylene jacket.

Armored cable can be used for rodent protection in direct burial if required. This cable is non-gel filled and can also be used in aerial applications. The armor can be removed leaving the inner cable suitable for any indoor/outdoor use. Temperature rating -40 to +85°C.

Figure 27: **Armored cable**

4.9.5 Submarine Fiber Optic Cable (Undersea Fiber Optic Cable)

Submarine cables are used in fresh or salt water. To protect them from damage by fishing trawlers and boat anchors they have elaborately designed structures and armors. Long distance submarine cables are especially complex designed.

Figure 28: **Submarine cables**

4.10 ITU-T COMPLAINT FIBERS

- G.651 Multimode Fiber
- G.652 Standard Fiber
- G.653 Dispersion Shifted Fiber
- G.654 Loss minimized Fiber
- G.655 Non Zero Dispersion Shifted Fiber
- G.656 Medium Dispersion Fiber (MDF), designed for local access
- G.657 Bending Loss Insensitive Fiber

4.11 CONCLUSION

Fiber optic technology is a revolutionary technological departure from the traditional copper wires twisted-pair cable or coaxial cable. The usage of optical fiber in the telecommunications industry has grown a few decades ago. Today, many industries particularly telecommunications industry chooses optical fiber over copper wire because of its ability to transmit large amount of information at a time.

An optical fiber is a flexible filament of very clear glass capable of carrying information in the form of light. Optical fibers are hair-thin structures created by forming pre-forms, which are glass rods drawn into fine threads of glass protected by a plastic coating.

5 FIBER TO THE HOME (FTTH)

5.1 LEARNING OBJECTIVES

- Concept of FTTH.
- Network Architecture of FTTH
- GPON and GEPON technology.

5.2 INTRODUCTION

Growing demand for high speed internet is the primary driver for the new access technologies which enable experiencing true broadband. Today's, there is an increasing demand for high bandwidth services in market around the world. However, traditional technologies, like Digital Subscriber Line (DSL) and cable modem technologies, commonly used for "broadband access," which have access speeds to the order of a megabit per second, with actual rates strongly dependent on distance from the exchange (central office) and quality of the copper infrastructure, can not fulfill today's customer demand for bandwidth hungry applications such as high-definition TV, high-speed Internet access, video on demand, IPTV, online gaming, distance learning etc. Amongst various technologies, the access methods based on the optical fiber has been given extra emphasis keeping into long term perspective of the country. It has many advantages over other competing access technologies of which 'Being Future Proof' and providing 'True Converged Network' for high quality multi-play are the salient ones. The stable and long term growth of Broadband is, therefore, going to be dependent on robust growth of fiber in the last mile.

However, for providing multi-play services (voice, video, data etc.) and other futuristic services fiber in the local loop is must. The subscriber market for multi-play is large and growing and includes both residences and businesses. Businesses need more bandwidth and many of the advanced services that only fiber can deliver. All view Multi- Play as a strong competitive service offering now and into the future and are looking at fiber as the way to deliver. Optical fiber cables have conventionally been used for long-distance communications. However, with the growing use of the Internet by businesses and general households in recent years, coupled with demands for increased capacity, the need for optical fiber cable for the last mile has increased. A primary consideration for providers is to decide whether to deploy an active (point-to-point) or passive (point-to-multipoint) fiber network.

5.3 FIBER TO THE X (FTTX)

Today, fiber networks come in many varieties, depending on the termination point: building (FTTB), home (FTTH), curb (FTTC) etc. For simplicity, most people have

begun to refer to the fiber network as **FTTx,** in which x stands for the termination point. As telecommunications providers consider the best method for delivering fiber to their subscribers, they have a variety of FTTx architectures to consider. FTTH, FTTB, and FTTC each have different configurations and characteristics.

5.3.1 FTTH (Fiber To The Home):

FTTH is now a cost-effective alternative to the traditional copper loop. "Fiber to the Home" is defined as a telecommunications architecture in which a communications path is provided over optical fiber cables extending from an Optical Line Terminal (OLT) unit located in central office (CO) connects to an Optical Network Terminal (ONT) at each premise. Both OLTs and ONTs are active devices. This communications path is provided for the purpose of carrying telecommunications traffic to one or more subscribers and for one or more services (for example Internet Access, Telephony and/or Video-Television). FTTH consists of a single optical fiber cable from the base station to the home. The optical/electrical signals are converted and connection to the user's PC via an Ethernet card. FTTH is the final configuration of access networks using optical fiber cable.

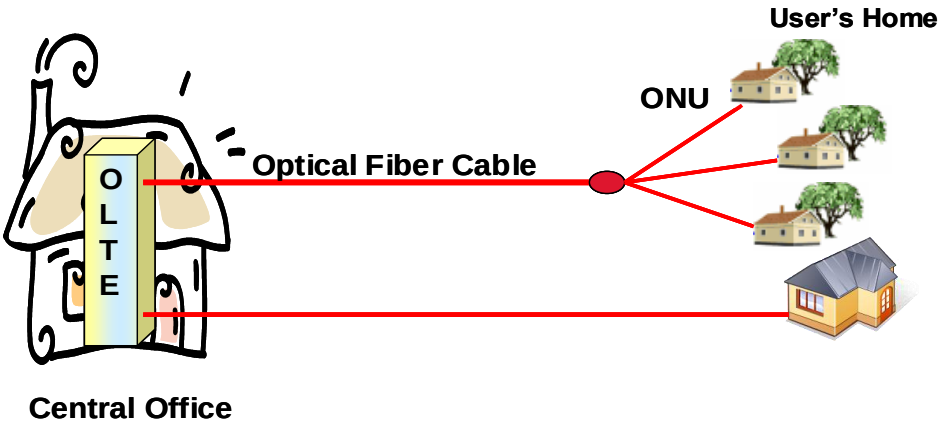


Figure 29: **FTTH Configuration**

5.3.2 FTTB (Fiber To The Building):

"Fiber to the Building" is defined as a telecommunications architecture in which a communications path is provided over optical fiber cables extending from an Optical Line Terminal (OLT) unit located in central office (CO) connects to an Optical Network Unit (ONU at the boundary of the apartment or office or building enclosing the home or business of the subscriber or set of subscribers, but where the optical fiber terminates before reaching the home living space or business office space and where the access path continues to the subscriber over a physical medium other than optical fiber (for example copper loops).

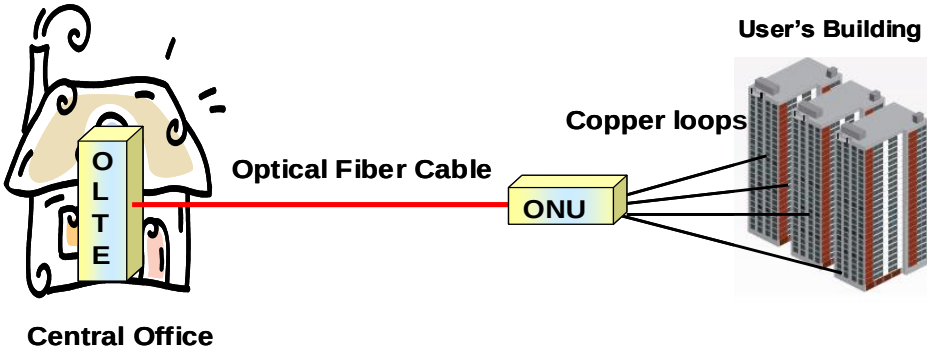


Figure 30: **FTTB Configuration**

FTTB regarded as a transitional stage to FTTH. By introducing fiber cables from the fiber termination point to the home living space or business office space FTTB can be converted to full FTTH. Such a conversion is desirable as FTTH provides better capacity and longevity than FTTB. Optical fiber cable is installed up to the metallic cable installed within the building. A LAN or existing telephone metallic cable is then used to connect to the user.

5.3.3 FTTC (Fiber To The Curb):

A method of installing optical fiber cable by the curb near the user's home. An optical communications system is then used between the ONU installed outside (such as near the curb or on Street Cabinet) from the installation center. Finally, copper cable is used between the ONU and user.

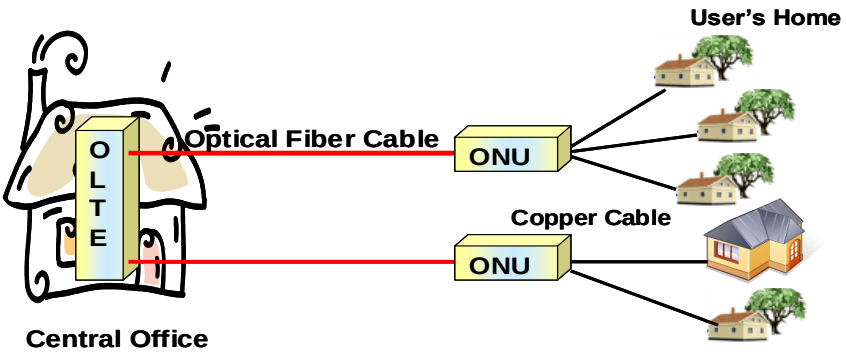


Figure 31: **FTTC Configuration**

5.4 WHY FTTH?

FTTH is a true multi-service communications access which simultaneously handles several phone calls, TV/video streams, and Internet users in the home/office. There are several advantages of deploying FTTH over other traditional access technologies as given below:

- FTTH provides end-users with a broad range of communications and entertainment services, and faster activation of new services.

- Competition is beginning to offer a "multi-play" (i.e., voice, video, data etc) bundle.
- FTTH provides Service Provider's with the ability to provide "cutting edge" technology and "best-in-class" services.
- Deploying a fiber optic cable to each premise will provide an extraordinary amount of bandwidth for future services.
- FTTH provides carriers with an opportunity to increase the average revenues per user (ARPU), to reduce the capital investment required to deliver multiple services, and to lower the costs of operating networks (fewer outdoor electronics, remote management, ..) will result in less operational expense.
- FTTH provides the community in which it's located with superior communications which enhance the efficiency of local business and thus deliver economic advantage for the community.
- Around the world FTTH is viewed as strategic national infrastructure similar to roads, railways, and telephone networks.

5.5 TECHNOLOGY OPTIONS FOR FTTH ARCHITECTURE:

When deciding which architecture to select a provider has many things to consider including the existing outside plant, network location, the cost of deploying the network, subscriber density and the return on investment (ROI). At present different technology options are available for FTTH architecture .The network can be installed as an **active optical network**, or **a passive optical network (PON)**.

5.5.1 Active Optical Network

The active optical network implementation is known as the "Active Node" and is simply described as a "point-to-point" solution. Subscribers are provided a dedicated optical cable and the distribution points are handled by active optical equipment. These active architectures have been setup as either "**Home Run Fiber**" or "**Active Star Ethernet**".

5.5.2 Home Run Fiber (Point-To-Point) Architecture

A Home Run Fiber architecture is one in which a dedicated fiber line is connected at the central office (CO) to a piece of equipment called an Optical Line Terminator (OLT). At the end user location, the other side of the dedicated fiber connects to an Optical Network Terminal (ONT). Both OLTs and ONTs are active, or powered, devices, and each is equipped with an optical laser The Home Run fiber solution offers the most bandwidth for an end user and, therefore, also offers the greatest potential for growth. Over the long

term Home Run Fiber is the most flexible architecture; however, it may be less attractive when the physical layer costs are considered. Because a dedicated fiber is deployed to each premise, Home Run Fiber requires the installation of much more fiber than other options, with each fiber running the entire distance between the subscriber and the CO.

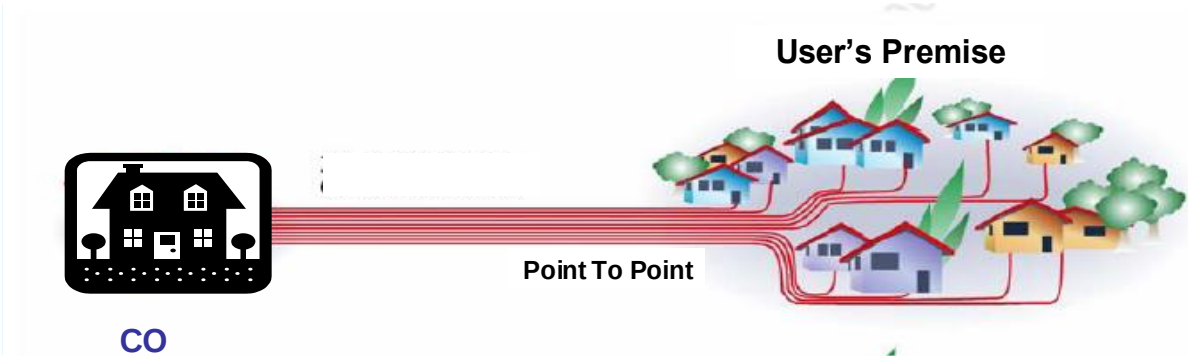


Figure 32: **Home Run Fiber (Point-to-Point) architecture**

5.5.3 Active Star Ethernet (Point-To-Multi Point) Architecture

Active Star Ethernet (ASE) architecture is a point-to-Multipoint architecture in which multiple premises share one feeder fiber through a Ethernet switch located between the CO and the served premises.

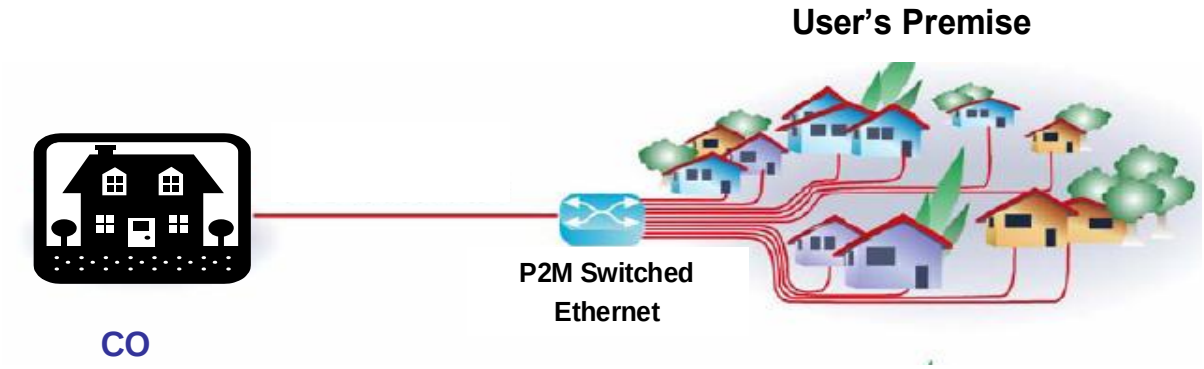


Figure 33: **Active star Ethernet**

5.5.4 Active Star Ethernet (ASE) Architecture

With Active Star Ethernet (ASE) architecture, end users still get a dedicated fiber to their location; however, the fiber runs between their location and Ethernet switch. Like Home Run Fiber, subscribers can be located as far away from the Ethernet switch and each subscriber is provided a dedicated "pipe" that provides full bidirectional bandwidth. Active Star Ethernet reduces the amount of fiber deployed; lowering costs through the sharing of fiber.

5.6 PASSIVE OPTICAL NETWORK (POINT-TO-MULTIPOINT) ARCHITECTURE

The key interface points of PON are in the central office equipment, called the OLT for optical line terminal, and the CPE, called ONU for optical network unit (for EPON) and ONT for optical network terminal (for GPON). Regardless of nomenclature, the important difference between OLT and ONT devices is their purpose. OLT devices support management functions and manage maximum up to 128 downstream links. In practice, it is common for only 8 to 32 ports to be linked to a single OLT in the central office. On the other hand the ONT (or ONU) devices in the CPE support only their own link to the central office. Consequently, the ONT/ONU devices are much less expensive while the OLTs tend to be more capable and therefore more expensive.

5.6.1 OLT

The OLT resides in the Central Office (CO). The OLT system provides aggregation and switching functionality between the core network (various network interfaces) and PON interfaces. The network interface of the OLT is typically connected to the IP network and backbone of the network operator. Multiple services are provided to the access network through this interface,.

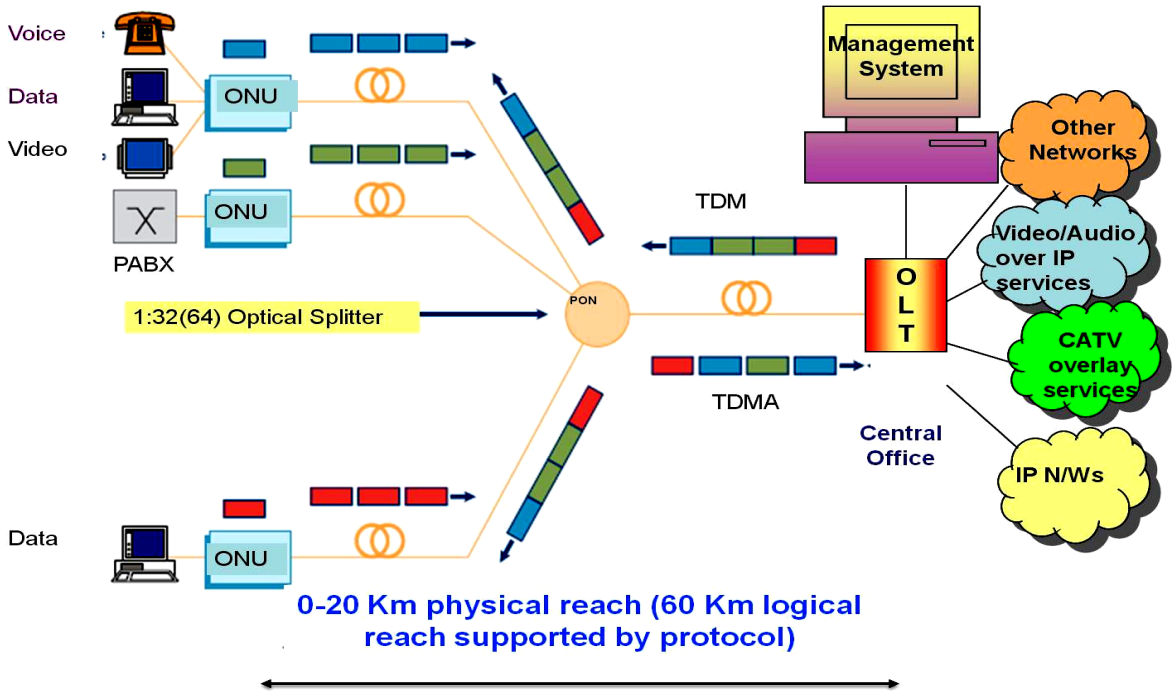


Figure 34: **PON Architecture.**

5.6.2 ONU/ONT:

This provides access to the users i.e. an External Plant / Customer Premises equipment providing user interface for many/single customers. The access node installed within user premises for network termination is termed as ONT. Whereas access node installed at other locations i.e. curb/cabinet/building, are known as ONU. The ONU/ONT provide, user interfaces (UNI) towards the customers and uplink interfaces to uplink local traffic towards OLT.

5.6.3 PON:

Distributed or single staged passive optical splitters/combiners provide connectivity between OLT & multiple ONU/ONTs through one or two optical fibers. Optical splitters are capable of providing up to 1:64 optical split, on an end to end basis. These are available in various options like 1:4, 1:8, 1:16, 1:32 and 1:64.

5.6.4 NMS:

Management of the complete PON system from OLT.

- One OLT serves multiple ONU/ONTs through PON
- TDM/TDMA protocol between OLT & ONT
- Single Fiber/ Dual Fiber to be used for upstream & downstream
- Provision to support protection for taking care of fiber cuts, card failure etc.
- Maximum Split Ratio of 1:64
- Typical distance between OLT & ONT can be greater than 15Km (with unequal splitting - up-to 35Km)
- Downstream transmission I.e. from OLT to ONU/ONT is usually TDM
- Upstream traffic I.e. from ONU/ONT to OLT is usually TDMA
- PON system may be symmetrical or asymmetrical
- PON and fiber infrastructure can also be used for supporting any one way distributive services e.g. video at a different wavelength

PON is configured in full duplex mode in a single fiber point to multipoint (P2MP) topology. Subscribers see traffic only from the head end, and not from each other. The

OLT (head end) allows only one subscriber at a time to transmit using the Time Division Multiplex Access (TDMA) protocol. PON systems use optical splitter architecture, multiplexing signals with different wavelengths for downstream and upstream.

5.7 SPLITTER CONFIGURATIONS

There are two common splitter configurations are being used for PON architecture i.e. **centralized and the cascaded** approaches.

5.7.1 Centralized Splitter Approach

In Centralized Splitter Approach typically uses a 1x32 splitter in an outside plant enclosure, such as a fiber distribution terminal. In the case of a 1x32 splitter, each device is connected to an OLT in the central office. In this approach, optical splitters are concentrated in a single location from which all customer's optical network terminals (ONTs) at 32 homes are connected as shown in figure.

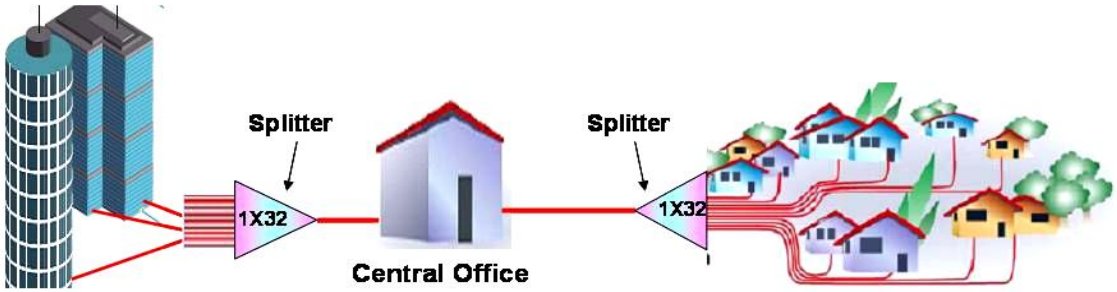


Figure 35: **Centralized Splitter Approach**

5.7.2 Cascaded Splitter Approach

A cascaded split configuration results in pushing splitters deeper into the network as shown in fig.8. Passive Optical Networks (PONs) utilize splitter assemblies to increase the number of homes fed from a single fibre. In a Cascaded PON, there will be more than one splitter location in the pathway from central office to customer. Currently, standard splitter formats range from 1 x 2, 1 x 4, 1 x 8, 1 x 16 and 1 x 32 so a network might use a 1 x 4 splitter leading to a 1 x 8 splitter further downstream in four separate locations. Optimally, there would eventually be 32 fibers reaching the ONTs of 32 homes.

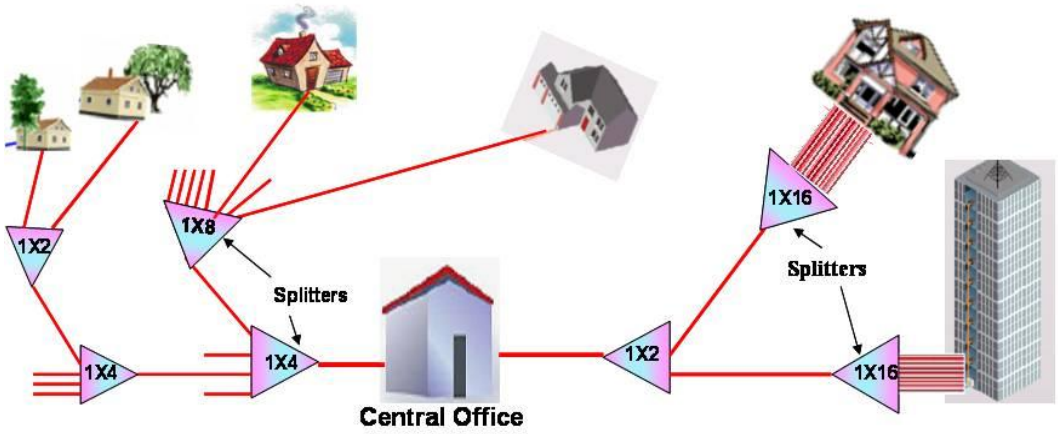


Figure 36: **Cascaded splitter approach**

There are several "flavors" of PON technology, i.e. new access technology named **APON** (ATM Passive Optical Network), **BPON** (Broadband Passive Optical Networking), **EPON** (Ethernet Passive Optical Networking) and **GPON** (Gigabit Passive Optical Networking) which delivers gigabit-per-second bandwidths while offering the low cost and reliability.

5.7.3 APON

ATM PON (APON) was standardized by the ITU in 1998 and was the first PON standard developed. It uses ATM principles as the transport method and supports 622 Mbps downstream services and 155 Mbps upstream service shared between 32-64 splits over a maximum distance of 20 km.

5.7.4 BPON

Shortly after APON, Broadband PON (BPON) followed and is very similar to APON. BPON also uses ATM, but it also boasts superior features for enhanced broadband services like video. BPON has the higher performance numbers then APON pre-splitting maximum of 1.2 Gbps downstream and 622 Mbps upstream.

5.7.5 EPON

The IEEE standardized Ethernet PON (EPON) in the middle of 2004. It uses Ethernet encapsulation to transport data over the network. EPON operates at rates of 1.25Gbps both downstream and upstream (symmetrical), using 8B/10B encoding over a maximum reach of 20. EPON is also called now as Gigabit Ethernet PON (GE-PON). It is defined as a single fiber network using Wavelength Division Multiplexing (WDM) operating at a wavelength of 1490 nm downstream and 1310 nm upstream. This leaves the 1550 nm window open for other services, such as analog video or private WDM circuits.

5.7.6 GPON

Gigabit PON (GPON) is the next generation of PON's from the line of APON and BPON. The ITU has approved standard G.984x for it. GPON will support both ATM and Ethernet for Layer 2 data encapsulation so is clearly an attractive proposition. GPON supports two methods of encapsulation: the ATM and GPON encapsulation method (GEM). GEM supports a native transport of voice, video, and data without an added ATM or IP encapsulation layer. GPONs support downstream rates as high as 2.5 Gbits/sec and an upstream rate from 155 Mbits/sec to 2.5 Gbits/sec. BSNL is procuring the GPON that will support downstream rate 2.5Gbps and upstream 1.25 Gbps.

5.8 THE FEATURES OF DIFFERENT PON STANDARD

Features	**BPON**	**GPON**	**EPON**
Responsible Standard body	FSAN & ITU-T SG15 (G-983 Series)	FSAN & ITU-T SG15 (G-984 Series)	IEEE 802.3ah
Bandwidth	Down Stream up to 622 Mbps Up Stream up to 155.52 Mbps	Down Stream up to 2.5 Gbps Up Stream up to 2.5 Gbps	Down Stream up to 1.25 Gbps Up Stream up to 1.25 Gbps
Downstream ג	1490 nm & 1550 nm	1490 nm & 1550 nm	1490 nm
Upstream ג	1310 nm	1310 nm	1310 nm
Layer-2 Protocols	ATM	ATM, Ethernet, TDM over GEM	Ethernet
Frame	ATM	GPON Encapsulation Method	Ethernet Frame
Max. Distance (OLT to ONU)	20 km	20 Km(supports logical reach up to 60 Km)	10 and 20 Km.
Split Ratio	1:16, 1:32 and 1:64	1:16, 1:32 and 1:64	1:16 and 1:32
Line Codes	NRZ (Scrambled)	NRZ (Scrambled)	8B/10B
Downstream Security	**AES:** Advanced Encryption Standard -128 bit key	**AES:** Advanced Encryption Standard (Counter mode)	Not Defined
FEC	None	Yes	Yes
No. of fibers	1 or 2	1 or 2	1

Protection Switching	Support multiple protection configuration	Support multiple protection configuration	None

5.9 PROPOSED SERVICES ON FTTH NETWORK OF BSNL

The first and foremost service proposed in the deployment of these PON technologies is to roll out the **Next Generation Play Network (NGPN).** The following services are proposed on the FTTH network:

- Basic internet Access Service controlled and uncontrolled from 256Kbps to 1000Mbps.
- TV over IP Service (MPEG2).
- Video on Demand (VoD)(MPEG4) play like VCR.
- Audio on Demand Service
- Bandwidth on Demand (User and or service configurable)
- Remote Education
- Point to Point and Point to Multi Point Video Conferencing, virtual classroom.
- Voice and Video Telephony over IP: Connection under control of centrally located soft switches.
- Interactive Gaming.
- Layer 3 VPN
- VPN on broadband
- Dial up VPN Service
- Virtual Private LAN Service (VPLS)

5.10 CONCLUSION

From the BSNL network point of view GPON and GEPON, being the TDM based technology, shall integrate into the existing switching network.

6 CDR (CRM/CLARITY)

6.1 LEARNING OBJECTIVES

- Components of a billing system
- CDR based customer care and convergent billing system-project 1 & 2
- Disaster recovery in CDR project

6.2 INTRODUCTION

The telecommunication environment has become very competitive with multiple operators and multiplicity of services by each operator. In order to be more competitive, companies need to identify customer needs and provide high quality services. The company's ability to provide an accurate and simple bill itself will be an ordeal with the increasing number of services and their complexities. With this demanding requirement and to maintain the competitive edge, BSNL has decided to implement the CDR based billing. This is a big project undertaken by any Telecom service provider in India. It is around 1200 Crore Project.

The implementation of CDR based Billing project will have a number of positive fallouts:

1. Standardization of systems and processes - Instead of varieties of systems all over BSNL, a single seamlessly integrated standard operation system will support all the operational activities providing the associated advantages. The overall quality of billing and payment accrual systems should improve.
2. High quality Customer Care - The seamless integration will make possible single point high quality customer care.
3. Paradigm change of CDR based billing - The shift from call meter base to CDR base will make possible flexible call dependent charging and customer segment based marketing schemes. In addition, this paradigm change in billing will make possible new mandatory TRAI functions such as Carrier selection.
4. Value added functionalities - The additional value added functionalities will make possible new powerful functionalities such as formal Revenue Assurance, formal improved CRM, Marketing Campaign Management and so on.
5. E-Stapling - Through a special mechanism of E-Stapling, charges of various BSNL services of one customer will be billed together.
6. Time to Market – The new convergent billing solution and a services layer built into the integration layer will facilitate the launch of new functionality and products faster into the market.
7. Process Efficiency – New Systems will incorporate Industry best practices that should significantly improve the process efficiency in some of the areas.

To understand the billing process the following figure may be studied.

The figure above shows how a basic billing process works. After a call is made the collector gathers data from the switch and builds a call detail record(Call detail record).The CDR contains the originating number, terminating number, the start time and duration of the call, The CDR is then stored until it can be rated. After rating, the credits and other charges are added. Thereafter the invoices are produced and mailed to the customer in a simple format. Call data is also shared between different service providers which are commonly known as IUC. Issues that must be addressed while managing billing system are reliability, accuracy and readability. Billing different types of services is also a complex issue.

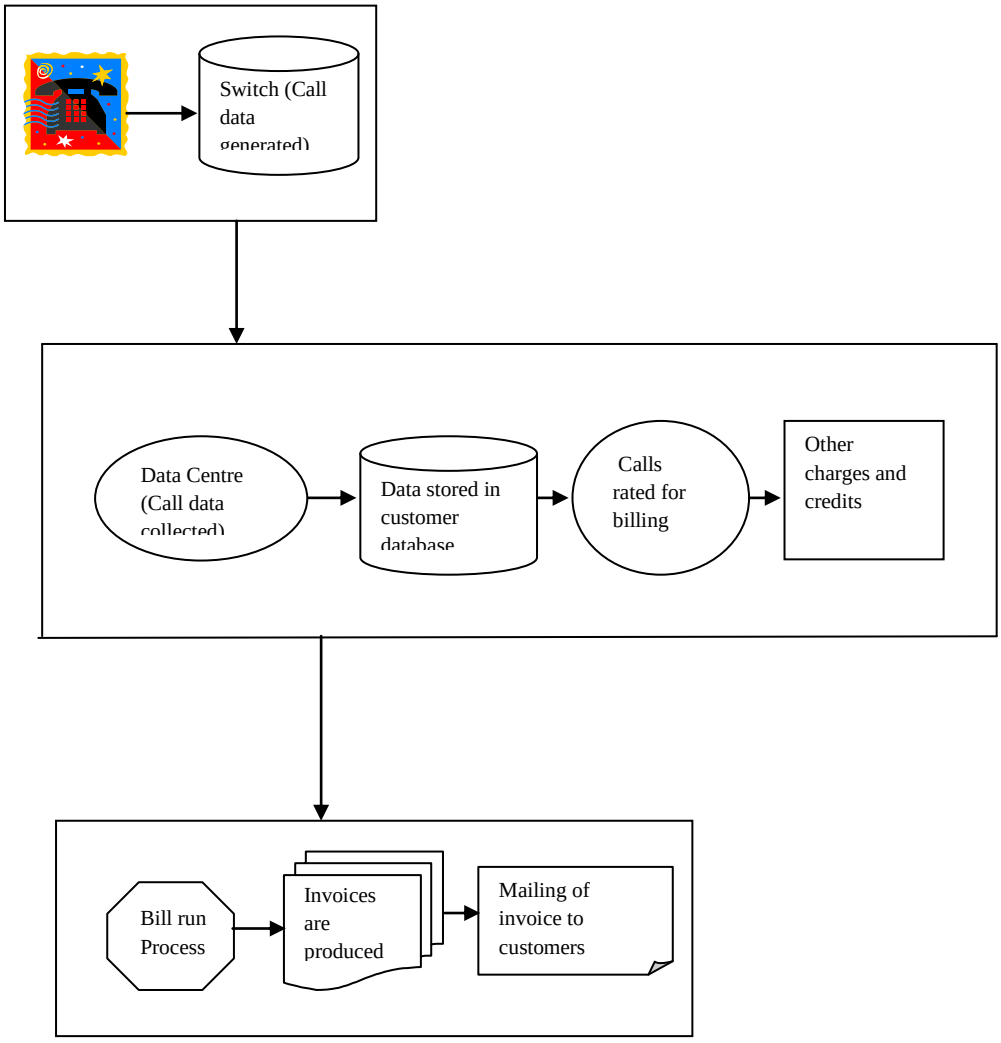


Figure 37: **Basic billing process**

6.3 COMPONENTS OF A BILLING SYSTEM

A billing system is composed of a series of independent applications that, when run together, are referred to as the billing system. Its major components are as follows:

CDR— This is used to record the details of the call. Usual information on a CDR includes start time of call, type of call, duration of call, originating number, and terminating number. The CDR is stored until time of billing.

Rating application— This matches calls to customer calling plans. The application uses the start, end number, duration, date and time of call to decide what the charge should be, based on the calling plans on the customer's record. This program applies the rate for the individual guided calls. Rating gives the call a value to be charged at the time of billing (not including any promotions, discounts, or taxes).

Billing–This is usually performed once a month. This job collects all of the rated calls that have been stored over the past 30 days. The program adds any promotions and discounts that are associated with the customer account. For example, if customers have called over a certain number of minutes, they might get a volume discount. In addition, taxes and credits are applied.

Formatting -- When the billing job is complete, a file is created that includes all of the customer's information. This file is sent to a print house to be converted to paper invoices. These invoices are then stuffed into envelopes, along with specific inserts targeted to the customer. Many companies will also create electronic statements and send customers their invoices via diskette, tape, or even e-mail; alternative billing practice is especially common for business customers.

6.4 CDR BASED CUSTOMER CARE AND CONVERGENT BILLING SYSTEM-PROJECT 1 & 2

Bharat Sanchar Nigam Limited (BSNL) is having countrywide presence with over 55 million wire line & wireless telephone subscribers and offer hosts of other services like Data communication, National long distance, International Long Distance, Internet, Leased Line, etc. The Company has decided to implement next generation State-of-Art Call Detail Record (CDR) based Customer Care and Convergent Billing System. This assignment involves deployment of Centralized Integrated Billing Systems with supporting technological and communication infrastructure.

Convergent Billing would be based on Call Detail Records (CDRs) obtained from different type of Network elements capable of generating billable information, using centralized Mediation System.

The project enables BSNL to face new challenges due to competition by providing effective and efficient Billing & Customer Care Solutions. It envisages building of

country wide intranet, reduce the cost of operation, increase revenue realization, stop leakage of revenue besides providing round-the-clock best customer care operations.

BSNL implemented the CDR based Billing and customer care solution through out India with four zones and four data centers. This was be achieved by carrying out implementation in two zone-pairs each to be referred as CDR Project 1 and CDR Project 2.

6.4.1 Implementation Plan

The implementation plan is indicated below:

- **Proof of concept Phase**– Setting up of data centers at East-South Zones (CDR Project 1) and North-West zones (CDR Project 2) and implementing all the software solutions along with the networking components meant for the SSAs mentioned below.
- **Roll out Phase** – Implementation of CDR based billing and customer care system in all the remaining SSAs.

The two phases can be summarized as below:

CDR Sub Project	**Data Center**	**CDR Project**	**POC Phase**	**Roll out Phase**
1.1	South	CDR Project 1	4 SSA (Hyderabad, Bangalore, Thiruananthpuram, Chennai,	66
1.2	East	CDR Project 1	8 SSA (Kolkata, Patna ,Kamrup, Ranchi, Raipur, Shillong, Puri, Kharagpur)	59
2.1	North	CDR Project 2	7 SSAs (Chandigarh, Ambala, Lucknow , Noida, Dharamshala, Dehradun, Jammu)*	103
2.2	West	CDR Project 2	4 SSAs (Pune, Ahmedabad, Bhopal, Raipur)	83

Table 1. POC Phase

There would be two different Billing Application Software solutions for the two projects.

Scenario is depicted in the table below:

CDR Project 1 (South & East Zones)		**CDR Project 2(North & West Zones)**	
CDR Sub Project 1.1	**CDR Sub Project 1.2**	**CDR Sub Project 2.1**	**CDR Sub Project 2.2**
System Integrator A	System Integrator A	System Integrator B	System Integrator B
HCL	HCL	TCS	TCS

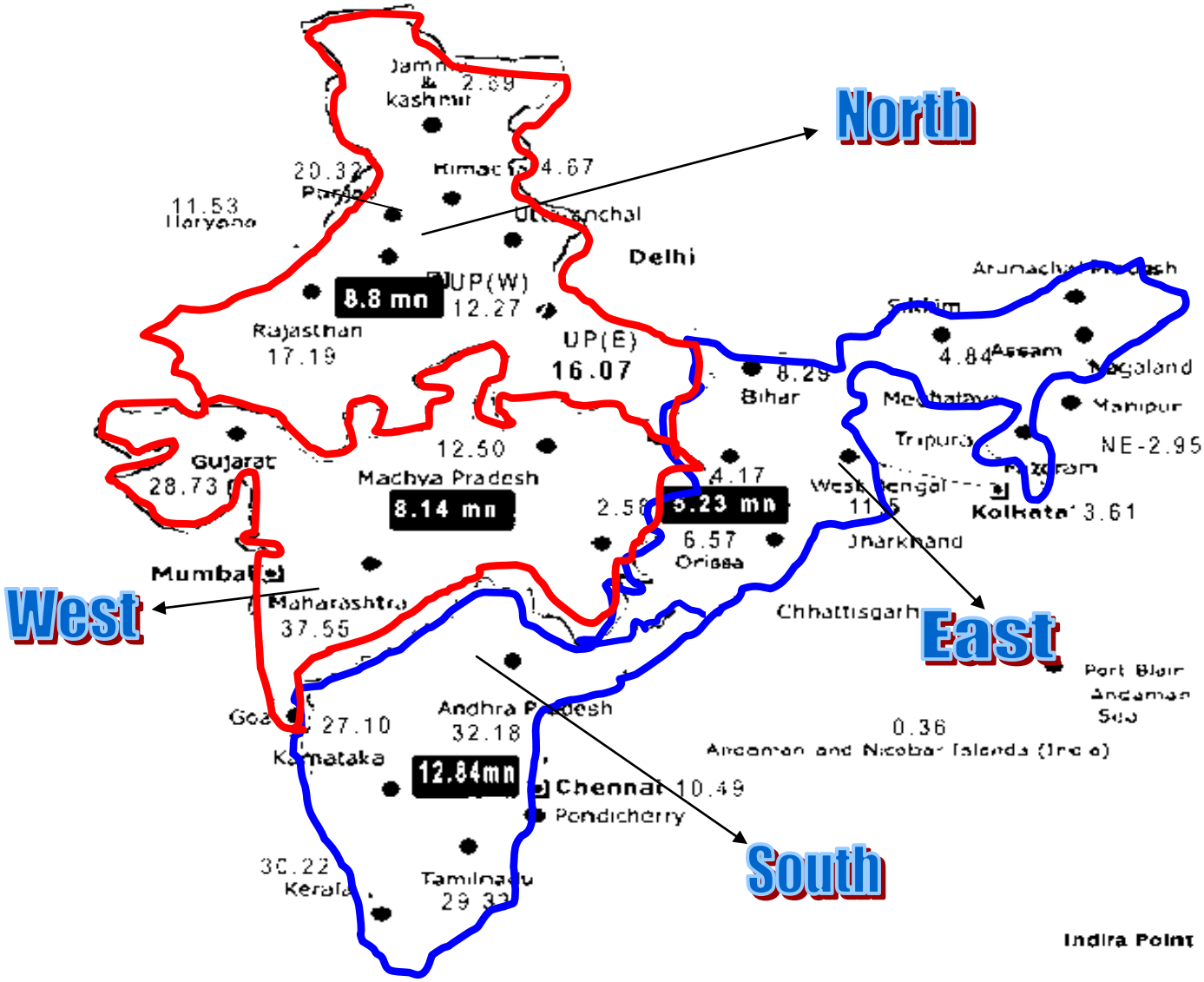


Figure 38: **DEL connections**

The DEL figures shown in the above figure are approximate figures only.

CDR Project I: Region marked in Blue **(South and East Zones)**	**CDR Project II: Region marked in Red** **(North and West Zones)**

6.4.2 Functionality

The overall functionality of the system have all the functionalities that were available in the previous packages like DOTSOFT. The commercial, Telecom revenue and accounting and FRS functionalities available in those packages is be available in the CDR system also.

This project will replace all the existing systems of Commercial, TRA (Telecom Revenue Accounting), FRS (Fault Repair Service) and DQ (Directory Enquiry).The project will cover the customer care and billing for the following services:

1. Landline
2. Broadband
3. Leased line

The project is not simply a replacement of the existing systems, but it is much more than that. For the first time in the history of BSNL, we are going to have State-of-the-Art Customer Relationship Management (CRM) software. This software will take care of all types of requests from the customers and integrate with other systems such as Order Management and Billing systems.

This software will also provide a Web Self Care (WSC) module, which will enable customers to access the system through Internet for placing any request, for making payments, or for general enquiry.

6.5 ORGANIZATIONAL STRUCTURE OF BSNL FOR SERVICES

For the purpose of operations and revenue BSNL is divided into circles and each circle is further subdivided into SSAs (Secondary Switching Area).

While circles are typically the same as States, SSAs are same as districts in most of the cases. For the purpose of charging SSA boundary is normally co-terminus with LDCA (Long Distance Charging Area). Each LDCA is further divided into number of SDCA (Short Distance Charging Area). Headquarter of the SDCA in most cases handles complaints and fault repair service pertaining to the area of SDCA.

Each SSA is like a separate profit centre.

Typically each SSA is responsible for providing service to the customers and subsequent customer support.

Each SSA has both indoor and outdoor staff. Indoor staff is responsible for Network Element maintenance, provisioning, etc while outdoor staff is responsible for building and maintaining the access circuit from NE to the customers premise.

Customer touch points are Customer support centers located in various SDCAs, which are responsible for Service registration and related commercial formalities followed with collection of payments against demand notes and bills.

Back Office operations are offered through commercial offices, accounts offices, operational & maintenance units. Commercial offices are responsible for different kind of service request.

There are well laid out accounting practices which ensures that a proper record is maintained both at the commercial and accounts office for the customer.

Under Zonal Data Centre, BSNL envisages setting up an OSS(Operation Support system) and BSS (Base-station system) infrastructure, which is centralized but has decentralized roles and privileges based access to Customer Service Representatives (CSR) and Account Mangers (all concerned for back office operation) in view of the BSNL's organizational structure described above. Roles and Privileges based access is intended to provide limited access to CSRs/ Account Managers on the system based on different criterion like SSA, Circle and Service center with a permission to carry out one or combination of functions including create, delete, view, print, etc. on different application running at Data Center.

6.5.1 Data Center

The entire project is going to be implemented with four Data Centre :-

Hyderabad

Kolkata

Pune

Chandigarh

These four Data Centre will take care of all the activities of the Circles in the respective Zones.

Establishment of data centre to host the hardware and software required for all applications. The Network Operation Center (NOC) and Server room shall preferably be located nearby. All Gigabit connectivity between different Data Center equipment shall be on optical / electrical interface. Provision of CCTV based Surveillance System & Access Control System at the Data Center. A separate enclosure shall be provided for monitoring screens

6.6 COMPUTER HARDWARE

Hardware requirement is categorized in two broad levels for all categories of applications.

First category of servers is of Connection or Presentation Servers for Applications which are multi instance and scale horizontally. For such category of applications, Rack mounted Blade Servers/ Rack mounted Stand Alone Servers shall have to used. These type of servers shall be utilized as: EMS Gateways, HTTP servers, SMTP servers, Print Servers, AAA Servers, Logical Security Elements, Network Device Management Servers, DNS Servers, IVRS, Proxies, etc.

Second category is of Datacenter class Servers for the purpose of Database where persistent data is stored and Application Servers where business logic resides within which data is manipulated in response to a client's request. Here database and application can scale diagonally i.e. scales vertically to an extent and horizontally beyond that. These services can run on multiple mid range servers or on a few high end servers having multiple instances of application running. Following applications shall run on these servers:

Billing and Accounting (Including Rating, OM (if part of Billing) and all other related functionalities), Revenue assurance, Mediation, Provisioning, EAI, CRM (Including CHS, WSC, OM (if part of CRM) and all other related functionalities), Directory Enquiry, EMS, IOBAS,FMS(Fraud Management System), Backup.

Mediation Servers or partitions running Mediation application have X.25 adapters with redundant configuration.. There would be a scenario where X.25 and other type of connectivity are achieved through separate stand alone server to act as collection server and DC class of Server for further processing. Additional collectors would be configured at each data center for the failover site to take care of 100% collection requirement in DR scenario.

System Architecture would be modular in design allowing future expansions. The Hardware design is done in such a way that there would be no single point of failure. Operational and monitoring tools for each and every hardware system would be provided. Hardware System shall provide status information of the various processes to an industry standard EMS (Third party)

6.7 SOFTWARE

Various software applications with functional modules are Data Mediation System, Billing and accounting, Service Provisioning, CRM & Web Self Care, Directory Enquiry, Revenue Assurance, Enterprise Application Integration, Enterprise Management System, Enterprise Reporting, RDBMS and Security System etc

Customer Relationship Management (CRM) system is the single point customer interface inter-linking Convergent Billing, accounting, commercial, fault control, order and provisioning status, etc. CRM also provides for management of all types of post-paid and prepaid as well as discrete products & services rendered by BSNL. Provision exists for on-line and batch methods of feeding all types of data in each application.

All software modules in OSS are tightly integrated with each other as per BSNL's business requirement. The integration is achieved under EAI (Enterprise Application Interface) framework using industry standard connector/ adapter.

The system is required to be interfaced with existing software application like IVRS, FRS, Billing, Commercial and Directory Inquiry system as per specific need for continuity of the business. Self Care Service through Internet would be provided for identified services by taking due care of system security.

All the software systems would have easy integration capability by supporting industry standard open transport technologies and middleware product. The software systems would offer the capability to import and export information to/from external files or system. The Software System shall support XML and HTML standards for Internet Data Exchange. Software Systems should have capability to apply software or parameter changes without stopping the system.

Software System like Billing, CRM etc would support clear demarcation for the core layer and the customization layer. All business process reengineering would be done through customization layer. All future versions would have backward compatibility to ensure safe upgrades.

The Software Systems would be able to scale both vertically and horizontally in order to utilize in-box capability of Servers (hardware) and if required by deploying additional Servers.

There would be operational and monitoring tools for each and every software & hardware system.

6.8 DISASTER RECOVERY IN CDR PROJECT

The customer care and billing and other related operations of 334 SSAs are going to be migrated to the four Data Centre. It is very important therefore to have business

continuity Plan in case of a disaster.

A disaster is defined as an event that makes continuation of normal functions of a Data Centre impossible. An event could be any one of the incidents like Flood, Fire, prolonged power shut down, strike, earthquake, etc.

In this project, Hyderabad is configured as the DR site for Kolkata and vice versa. Similarly Pune is configured as the DR site for Chandigarh and vice versa. The degradation of performance for the applications failing over to the DR site is permitted up to 50%. This means for example, a billing operation taking 8 hours in the normal course, can take up to 16 hours in case of a disaster.

6.9 NETWORK FOR CDR PROJECT

This project shall implement a countrywide Intranet.This network will connect all SSAs, Circles and the Corporate Office, providing connectivity to all its main exchanges, all officers dealing with customers, such as JTOs, SDEs, AOs, and the entire management.So far, each SSA or Circle has established networks for implementing DOTSOFT and other local systems. This project is going to integrate all the networks and provide a countrywide IP network with MPLS as the backbone. This network will be used not only for implementation of the CDR project, but also for implementing all other IT projects in future, such as ERP.

The following figure shows in general the exchange network and the collection methodology of CDR.

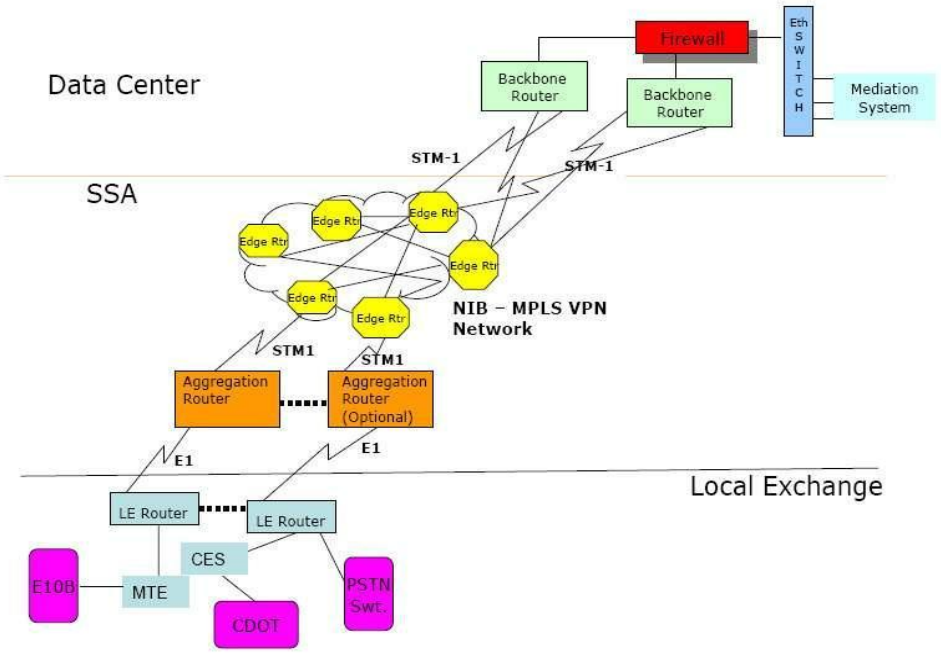


Figure 39: **CDR connectivity**

6.10 CDR PROJECT CONNECTIVITY TO EXCHANGES

Each exchange is connected to a router, which is called LE router (Local Exchange router). All new technology switches such as OCB, EWSD, 5ESS, AXE, shall be connected using X.25 cards and Ethernet interface (wherever available). All CDOT exchanges will be connected to the LE router using CES equipment supplied by CDOT through HCL. All E10B exchanges will be connected to the LE router through MTE (Magnetic Tape Emulator). Each LE router is connected to the Aggregation Router through E1 links. All the E1s coming from the different exchanges will be aggregated to the Aggregation Router. Each Aggregation Router in each SSA shall be connected over STM-1 link to the nearest MPLS node. For redundancy purposes, the connectivity shall be established to two MPLS nodes. The Data Centre is also connected to the MPLS network presently through STM-1 links, to start with.This end link will be enhanced to 1 GBPS link or more, later. Thus, each exchange shall be connected to the Data Centre over E1 end links and through the MPLS network.

6.10.1 Cdr Project Connectivity To Terminals

The existing CSR network will also get connected to the Aggregation Router.Thus, all the terminals of Commercial, TRA, FRS and Directory Enquiry which are now connected to the local systems, will be connected to the Data Centre through the Aggregation Router. The project envisages establishment of new network for collection of CDR from the exchanges, Usage of existing CSR network, with addition of a few CSR, if necessary, And re-utilization of existing PCs in the network.

6.11 CONVERGENT BILLING AND ADVANTAGES

6.11.1 Single Convergent Bill

A customer Account having multiple services with each service having multiple instances shall have the option to get a single Bill. It shall also be required to give single bill for multiple of such accounts arranged in hierarchy under a Corporate/individual Account

6.11.2 Individual Account

Data consolidation for service and multi instance Customer Account, within a zone, shall be done from existing billing system. Invoice would be generated for each service, the customer has opted for. Individual invoices for a single customer shall be received from different billing system and then a single invoice shall be generated at all four zonal billing centers, after taking in to account bulk discount if any

Extension of Customer care to such customer shall have hierarchical view and the same shall be covered under web self care as well as corporate self care.

6.12 CORPORATE BILLING

Three zonal billing centers (South, West and North) and other Billing centers meant for billing other services like GSM based Mobile Telephone, IP Billing, Leased Line Billing, Intelligent Network, etc shall be connected to East Zone to support Corporate Convergent Billing, payment collection etc. In short, BSNL will have multiple Billing System considering multi service environment, which will continue to be in operation even after full commissioning of proposed system. Hence, it is of utmost requirement for the proposed solution to be able to work in conjunction with other Billing system.

The billing system shall be able to collect processed bills from the billing system of following networks existing in BSNL such as MLLN System, CMTS located at 5 different locations, NIB-II, IN System etc

In addition, Billing of Broadband services, CLI based Internet service and other IP services on the same landline is also required. In this scenario usage information (rated CDRs) shall be taken from the billing system of NIB-II. CDMA Technology presently deployed in the BSNL network shall be provisioned and billed through the proposed solution.

For Management through Enterprise Management System.

- All the APIs for integration with 3rd Party Applications shall be provided.
- It would allow the users to use the standby database for read-only access while the synchronization between the primary and standby systems happen simultaneously.
- Access to all RDBMS stored procedures shall be available through JDBC, ODBC, C and Active X
- Detailed documentation shall be provided for Database Management specific to the project and the applications deployed.
- GUI based tool shall be provided to manage, test and tune the database.

All the applications implemented shall have provision for optimizing the number of static connections to the database using connection pooling. All the applications implemented shall also optimize the duration of connection to the database by using techniques like session time out.The database should be able to support partitioning of tables to support linear data scalability and parallel utility processing.

Integration with IN: BSNL presently offers IN Services like Virtual Calling Card (Brand Name – India Telephone Card), Account Calling Card(ACC), Free Phone, Premium Calling Rate, Universal Access Number, Virtual Private Network, Tele Voting, Universal Personal Number etc. The purpose of integration is to dynamically transfer the

Pre-paid amount from the IN Platform to increase in credit limit of a subscriber of a landline to enable bill payment for the post-paid services availed by the subscriber etc. . After integration it would be possible to offer following functionalities:-

The integrated system would have the capability to accommodate for IN and retail customers in a single customer account hierarchy with dynamic transaction guidance from one account to another account in the hierarchy based on service.

The system would have the ability to transfer the balance from IN service like Virtual Credit Card to post-paid service like landline telephone. This will facilitate landline subscriber to pay his retail bills through a Virtual Calling Card which means VCC amounts have to be debited from IN platform and same has to be credited to the Billing System.

The interface between IN Server and Billing Server shall be on secured layer for any transaction. Proven secured protocols shall be used for the purpose.

It shall be possible to redeem loyalty points earned in post-paid service in terms of Virtual Calling Card etc.

All account transaction shall be accompanied with detail log entry in the billing system and the same in readable format may be required to be given to the customers in their normal monthly bills as information.

6.13 CHANGES AFTER CDR PROJECT

- The introduction of this new project will eliminate the need of individual SSAs maintaining and operating TI systems for all the four functionalities, i.e. Commercial, TRA, FRS and DQ.
- The SSAs shall be the end-users of the systems and will have better tools and software at their disposal to provide better customer services.
- The database related jobs would be with the IT team at the Data Centres.
- Change certain business processes within BSNL, a few of them are explained below:

Business processing going to change due to CDR Project

Because of the introduction of new systems and to take advantage of the features of the system, it is proposed to change some Business processes within BSNL that are proposed to change for CDR project

a. Revenue Accounting:

b. Surcharge/Late Fee

c. PCO Billing

d. Deposits

e. Billing Cycles

f. CDR based billing

6.13.1 Revenue Accounting:

In the new system Balance brought forward accounting method shall be used instead of invoice based accounting. For example, a June Bill issued to a customer if not paid, will be added to the July Bill and the July Bill will be issued for an amount, which is equal to both the June and July amounts.

Every customer will be identified by an Account Number, which shall be unique throughout the country. Revenue booking shall be based on the Account even though the services under the account are scattered across the various SSAs. The customers can pay any amount at any time and it shall be credited to the account and adjusted against the outstanding

6.13.2 Surcharge/Late Fee

Surcharge will be treated as late fee, which will be a percentage of the outstanding instead of at the slab rate as is being done today. The late fee concept is already introduced in the GSM billing system and the same shall be followed here.

6.13.3 PCO Billing

For PCO billing, the commission payable and the minimum guarantee will be as per the billing cycle instead of on a monthly basis. PCO operators are now eligible for discounts instead of commission. These changes are already done in the existing systems and shall be continued in the new system.

6.13.4 Deposits

Deposits are already made uniform i.e. Rs.500/- for Local, Rs.1000/- for STD and Rs.2000/-for ISD. This shall be common for all the Plans. Therefore, we shall not be offering any OYT or TATKAL deposits/schemes. The existing OYT subscribers shall continue to be billed till the completion of 20 years. However, no new OYT connection shall be provided.

6.13.5 Billing Cycles

The number of billing cycles in an SSA may increase. The new system is going to have a centralized billing process common for all the SSAs in a zone.Therefore, the customers in the entire zone shall be divided into different billing cycles to evenly distribute the process load on the servers.

The number of billing cycles may even go up to 15 once the project is rolled out in all the SSAs.

6.13.6 CDR Based Billing

The existing tariff, which is based on MCUs and number of calls, will get migrated to MOU (Minutes of Usage) based system.

The discounts may be given not in terms of Free Calls, but shall be in terms of Free Talk Time given as Minutes per month or Rupees per month.

Though the system offers lot of flexibility in configuring different Plans, BSNL in turn may have to follow certain discipline in offering various Plans to the customers.

It is proposed to authorize the Circle Office team to configure the plans as per business requirements and in future SSAs may not be able to configure new Plans on their own. Each Plan shall be identified by a Plan Code in the system.

This discipline will help the organization in monitoring the launch of tariff Plans across the country and it will help BSNL to take correct business decisions.

The products and services that would be supported by the new billing system would be

Wire line Services: Basic Telephony (PSTN), WLL Fixed, National Long Distance, International Long Distance, ISDN, ATM and IP Services, IN services like Free phone, VCC, ACC, Premium rate services, etc.),Centrex, PBX & PABX, Leased lines, E1/ ISDN-PRI (in the context of reverse charging),

Wireless Services: GSM – (Pre-Paid and Post-Paid),CDMA – Pre-Paid and Post-Paid),Roaming, GPRSWAP on Mobile including applications like - mobile banking, weather update, news update, Stock update, Travel guide, etc

Data Services: Data calls, IP packets, Content Delivery, Internet services (including VoIP), Fax over IP (FoIP), E-mail services, Video on Demand (VoD),Video & audio conferencing,Internet Roaming

Other Services: Unified Messaging Service, Short Messaging Service, Voice Mail Service, INMARSAT,VSAT, Hotline, IVR based customer service, Virtual Private Network (VPN),xDSL access services, QoS, Frame Relay

Call Management Services: Caller Line Identification Presentation & Restriction, Call Waiting, Call Barring, Call Forward, Call Conferencing, Call Transfer, Malicious Call Tracking,

Miscellaneous requirements Ability to bundle services and the associated default products into one unit so as to make it easy for the CSR to associate it to the Subscription / Customer, Ability to support Number Portability, Grouping of DELs like in ISDN,

Level DID, There shall not be any limitation on specifying the number and types of categories for any type of service. For eg. for fixed line services there can be tens of categories such as Residential, Commercial, SME, etc. Similarly there can be sub-categories in each service type eg. In leased line service there may be 64 kbps, nx64 kbps etc.

6.14 CONCLUSION

In competitive era of telecommunication, telecom companies need to identify customer needs and provide high quality services. The company's ability to provide an accurate and simple bill itself a challenge along with the increasing number of services and their complexities. With this demanding requirement and to maintain the competitive edge, BSNL has implemented the CDR based billing. - Instead of varieties of systems all over BSNL, a single seamlessly integrated standard operation system of CDR will support all the operational activities providing the associated advantages.

7 PSTN NETWORK AND SERVICES

7.1 LEARNING OBJECTIVES

- Explain the PSTN Network Organization
- Explain the phone plus Services.
- Explain the IN services.

7.2 INTRODUCTION

Telecommunication industry is changing at a rapid pace. Telephony was invented in 1876 and automatic telephone exchanges were developed in 1895. At that time these exchanges were analogue. Then there were digital exchanges in the network, which worked on circuit switching principle, these were called new technology switches e.g. E10B, C.DOT, EWSD, OCB-283,5ESS, AXE-10, etc. Now, packet switching principle is used in the network which is known as NGN switches.

7.2.1 Switching In Telecom Network:

In normal telephone service, basically, a circuit or channel between the calling party and called party is set up (temporarily) and this circuit is kept reserved till the call is completed. Here two speech time slots are involved -one of the calling subscriber and other of the called subscriber. It is called circuit switching.

The data networks, on the other hand use the principle of Packet Switching. In Packet switching the information (speech, data etc) is divided into packets each packet containing piece of information also bears source and destination address. These packets are sent independently through the network with the destination address embedded in them. Each packet may follow different path depending upon the network. At the destination point all these received packets are reassembled.

7.3 PSTN NETWORK:

The telephone network used for fixed line services is also referred as PUBLIC SWITCHED TELEPHONE NETWORK (PSTN). There are different types of the telephone exchanges(switching systems) in PSTN. Earlier there were manual type, Electro mechanical type like Strowger and Cross bar.E10B was the first digital electronic exchange to be inducted in the network. But it had certain limitations like:

- The ISDN and CCS7 signalling was not supported.
- The traffic handling capacity and BHCA capacity was low.

- In the RLUs in case of link failure with the main exchange local switching within RLU subscribers was not possible.To avoid these problems new technology switching systems were inducted in our network. Mainly 4 NT switching systems were inducted in BSNL network:

- EWSD Supplied by M/s Siemens, Germany

- OCB-283 Supplied by M/s Alcatel, France

- 5ESS Supplied by M/s Lucent, USA

- AXE-10 Supplied by M/s Ericsson

Some new Salient features of New technology switches are:

- All NT exchanges support ISDN, C#7, V5.2, centrex facility.

- The traffic handling capacity and BHCA capacity are sufficient.

- Standalone RSU : All exchanges have this facility while in case of main link with the exchange is down subs of RSU can call among themselves. In 5ESS in standalone condition metering is done while in case of OCB-283 and EWSD metering is not possible. In case of OCB-283 double remoting is possible.

For rural area in our country where small capacity exchanges were required, CDOT equipment (CDOT 128P, 256P, SBM, MBM etc) was installed. CDOT technology is indigenously developed technology in our country. Initially standalone 128P, 256 P CDOT exchanges were installed but later these small independent exchanges had been converted into AN-RAX (Access Network Rural Automatic Exchange) and which were parented to nearby CDOT SBM/MBM or NT exchange. With this development all remote ANRAXs could be maintained from the SBM/MBM . It improved O& M functions/issues of small exchanges. In the BSNL network about 40% of the total switching capacity is on CDOT technology. The PSTN network has now migrated to NGN. Next Generation Network is the framework where a common transport network based on Internet Protocol for provides all kinds of telecommunication services.

7.4 PSTN NETWORK ORGANIZATION

In BSNL (Earst while DOT), the whole network is divided into circles (25 circles), each circle is divided into SSA (Secondary Switching Area) as an administrative unit. SSA is also known as LDCA(Long Distance Charging Area) and then further one LDCA is divided into many SDCAs(Short Distance Charging Area). This division of LDCA and SDCA is for charging purposes. Normally an inter SDCA but within same LDCA call is charged on the SDCC distance basis and an inter circle call is charged on

LDCC distance basis .The telephone network is also referred as PUBLIC SWITCHED TELEPHONE NETWORK (PSTN) .The offered voice service is referred as PLAIN OLD TELEPHONE SERVICE (POTS).

The PSTN network was organized in a hierarchical manner with Lev-1/Lev2/Tandem/Local Exchanges. The calls from a local exchange is routed to lev-I TAX either directly or through Lev-II TAX. From Lev-I TAX it is routed to the destination exchange either directly or through another Lev-I/Lev-II TAX. For ISD calls ISD Gateway is used.

The next generation networks is based on packet switching which involves voice, data and multimedia such as audio and video. The BSNL has planned a huge network wherein all the traditional voice and data customers migrate from C-DOT TDM towards NGN C-DOT. There are phases of migration from circuit switched PSTN to NGN. NGN provides new services to the customers such as Multi media video conferencing, Wide Area IP Centric, prepaid solution with all functionalities, Personalized Ring Back Tone (PRBT), Fixed Mobile convergence, etc.

7.5 INTERCONNECTION WITH THE PRIVATE OPERATOR:

Any operator can take license for providing Basic telephone service on circle basis Licenses are issued by DOT. Once an operator gets a license in a particular circle, after installing the necessary equipment it is required to be interconnected with the BSNL network for making the calls into/from BSNL network. For this either the connectivity is taken at local exchange level for local calls and also at Lev-I/Lev-II TAX for long distance calls. It is called POI (Point of Interconnection). POI charges are prescribed by TRAI.

7.6 NUMBERING SCHEME IN BSNL

DOT assigns the initial code for all the operators. BSNL having licenses in all the circle in the whole country except Delhi and Mumbai has been assigned digit ‘2’. The actual number which is dialed by the calling subscriber is prefixed with the SDCA code.At present the SDCA code+ Local no are of 10 digits e.g in Jaipur SDCA the local number is identified as 141 (SDCA Code)+2601602(local Number).Some special services like Directory Enquiry (197)., Fault Booking (198), Railway Enquiry (139) etc are provided by standard short codes using digit ‘1’.

7.7 SERVICES OFFERED ON LANDLINE

7.7.1 ISDN (Integrated Service Digital Network)

ISDN is a powerful tool worldwide for provisioning of different services like voice, data and image transmission over the telephone line through the telephone network. An ISDN subscriber can establish two simultaneous independent calls (except

when the terminal equipment is such that it occupies two 'B' channels for one call itself like in video conferencing etc.) on existing pair of wires of the telephone line (Basic rate ISDN) where as only one call is possible at present on the analog line /telephone connection. The two simultaneous calls in ISDN can be of any type like speech, data, image etc. ISDN also supports a whole new set of additional facilities, called Supplementary Services.

7.7.2 Services Offered By ISDN

- Normal Telephone & Fax (G3) and G4 Fax
- Digital Telephone -with a facility to identify the calling subscriber number and other facilities
- . Data Transmission at 64 Kbps with ISDN controller card
- Video Conferencing.

7.7.3 Variety Of Supplementary Services Are Supported By ISDN:

- Calling Line Identification Presentation(CLIP)
- Calling Line Identification Restriction(CLIR)
- Multiple Subscriber Number(MSN)
- Terminal Portability(TP)
- Call Hold(CH)
- Call Waiting(CW)
- User to User Signaling (UUSI)

7.8 TYPES OF ACCESS

There are two types of "access" (connections) for ISDN.

1. Basic Rate Access(BRA): 2B+D 2 Channels of 64 Kbps for Speech And Data, 1 Channel of 16 Kbps for Signalling
2. Primary Rate Access (PRA): 30 B+D 30 Channels of 64 Kbps for speech and data, 1 Channel of 64 Kbps for signalling.

7.9 SUPPLEMENTARY SERVICES (PHONE PLUS SERVICES)

7.9.1 Abbreviated Dialing

You may be calling a few people very frequently. It is possible to program these numbers as abbreviated codes of 1 or 2 digits. A maximum of 20 numbers can be

programmed for abbreviated dialing. It is ideal for STD/ISD. For registration Dial 110+short code (say15)+destination number(with STD code)

For use Dial 111+short code i.e. 11115

7.9.2 Call Waiting

This facility lets you receive incoming calls even when your telephone is busy. You will get a short duration pip-pip tone when you are busy talking , indicating that another call is waiting for you , provided you have activated this facility. You can talk to any one of the callers keeping the other waiting. Complete secrecy of communication between the two callers is maintained. For activation of the service dial: 118 (wait for the tone). For deactivation of the service dial: 119 (wait for the tone).

7.9.3 Hot Line

You may want to be connected directly to a predetermined number as soon as you lift the hand set even without dialing. At the same time you may want to have the flexibility to dial any other number of your choice. It is possible to have this facility in the digital exchanges by the delayed hotline feature. The number of your choice can be programmed by the exchange staff at your request. After doing so if you lift the telephone and do not dial within 5 seconds , you will be automatically connected to the programmed number. However if you start dialing with in 5 seconds , you can make an outgoing call as usual.

7.9.4 Call Transfer (Call Forward)

Useful for very mobile persons who may not want to miss incoming calls. Using this facility Calls can be forwarded to another telephone number designated by you. For activation Dial 114 and the number for which the call is to be transferred. For deactivation dial 115 and wait for acceptance tone.

7.9.5 Automatic Wake-Up/Reminder Call Service

When you want to be given reminder at a specific time, all you have to do is to call the

exchange and leave the time you want to be reminded. The facility allows you to initiate a call automatically by the exchange at a fixed time specified by the user of the telephone.Dial 116 followed by the time you wish to be reminded or woken-up say at 06.15am(06.15hrs), you will dial 1160615.

Dial 117 (the cancellation code) followed by the time you booked the call.

7.9.6 Number/Call Hunting Service

If you have more than one telephone line, this facility is very helpful for your caller. If the called line is engaged, your caller does not have to disconnect and dial other line(s).

This facility automatically transfers the incoming call to whichever line is free.

7.9.7 Calling Line Identification Presentation (CLIP)

The subscriber has to buy separately the CLIP display device from market. Using this facility you can see the number of the calling party before lifting your telephone. Very useful to trace malicious caller. However, the CLIP instrument shall be procured and installed by the users themselves.

7.9.8 Calling Line Identification (CLI) Announcement Service

Dial 164 and listen to the number of the phone line that you have used to make the call. Very useful when in doubt about your phone number.

7.9.9 Electronic Locking For Std/Isd (Dynamic Locking Facility)

For 100% protection against improper use, you can lock your telephone electronically.

Here, you only know the secret code. You can lock/allow Local, STD or ISD calls in many way viz. all calls allowed, only local calls allowed, only STD & Local calls allowed, all outgoing calls barred etc.

To Register Secret Code

Dial 123 0000 ABCD then wait for the acceptance tone (ABCD is the secret code chosen by the subscriber).

To use:

dial 124 ABCD 1 STD/ISD will be barred

dial 124 ABCD 0 STD and ISD will be opened

dial 124 ABCD 3 STD will be opened, ISD barred

dial 124 ABCD 4 STD/ISD and local will be barred

dial 124 ABCD 2 STD/ISD /Trunk call/95 will be barred.

10.Call Conferencing

With this service telephonic conference can be set up within 3 or more parties. This

service is available subject to technical feasibility.

7.10 IN SERVICES

The term Intelligent Networks (IN) is used to describe an architectural concept which is intended to be applicable to all telecommunications networks and aims to ease the introduction and management of new services. The objective of IN is to allow the inclusion of additional capabilities to facilitate provisioning of service, independent of the existing network capabilities. There are many new services implementation of which requires substantial changes in the existing switches belonging to different vendors. It not only very time consuming but often uneconomical too. Now, with IN technology it is possible to introduce new services rapidly without affecting the available services.

The IN's main advantage is the ability to control switching and service execution from a small set of Intelligent Network nodes known as Service Control Points (SCP).These SCPs are though very few in numbers (four in BSNL network) but can control thousands of switches.

7.10.1 Why It Is Called Intelligent?

An Intelligent Network (IN) Is A Service-Independent Telecommunications Network. That Is, Intelligence Is Taken Out Of The Switch And Placed In Computer Nodes That I.E. SCP. So To Implement A IN Service, Intelligence Of The Switch With Which The Customer (Sending The Request For An IN Service By Dialling) Is Connected, Is Not Used. Switches Simply Forward The Requests Of Customers For IN Services To Concerned IN Node I.E. SCP. It Is This SCP Which Uses Its Intelligence And Directs The Requesting Node To Take Particular Action. Forwarding Switches Simply Obey The Orders Of Their IN Nodes. As Scps Are Servers Based, Implementation Of An Advanced Service Is Much Easier.

7.10.2 In Architecture

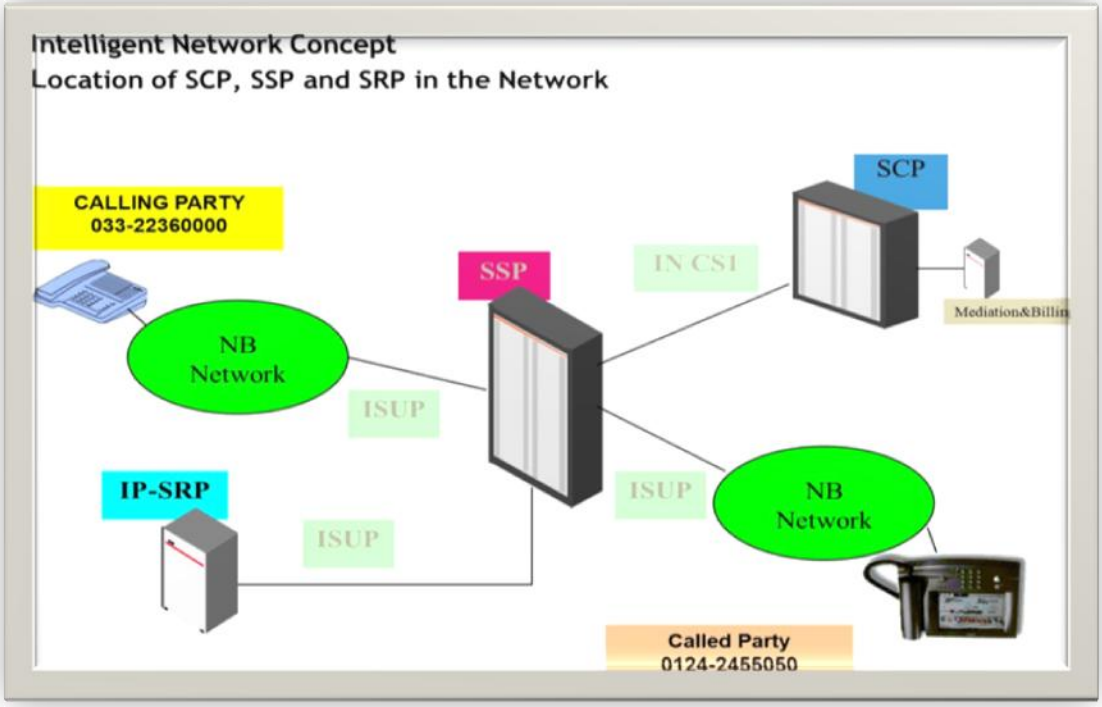


Figure 40: **IN ARCHITECTURE**

7.10.3 Network Elements Of In Platform

1. SCP: Service Control Point
2. SSP: Service Switching Point
3. SMP: Service Management Point
4. IP : Intelligent Peripheral

Service Switching Point (SSP)

The SSP serves as an access point for IN services. All IN service calls must first be routed through the PSTN to the "nearest" SSP. The SSP identifies the incoming call as an IN service call by analysing the initial digits (comprising the "Service Key")dialled by the calling subscriber and launches a Transaction Capabilities Application Part (TCAP) query to the SCP after suspending further call processing. When a TCAP response is obtained from SCP containing advice for further call processing, SSP resumes call processing.

The interface between the SCP and the SSP is G.703 digital trunk. The MTP,SCCP, TCAP and INAP protocols of the CCS7 protocol stack are defined at this interface

Service Control Point (SCP)

The SCP is a fault-tolerant online computer system. It communicates with SSP's and the IP for providing guidelines on handling IN service calls. The physical interface to the SSP's is G.703 digital trunk. It communicates with the IP via the requesting SSP for

connecting specialized resources.SCP stores large amounts of data concerning the network, service logic, and the IN customers. For this, secondary storage and I/O devices are supported. The service programs and the data at the SCP are updated from the SMP.

Service Management Point (SMP)

The SMP, which is a computer system, is the front-end to the SCP and provides the user interface. It is sometimes referred to as the Service Management System (SMS). It updates the SCP with new data and programs (service logic) and collects statistics from it. The SMP also enables the service subscriber to control his own service parameters via a remote terminal connected through dial-up connection or X.25 PSPDN. This modification is filtered or validated by the network operator before replicating it on the SCP.The SMP may contain the service creation environment as well. In that case the new services are created and validated first on the SMP before downloading to the SCP.One SMP may be used to manage more than one SCP's.

Intelligent Peripheral (IP)

The IP provides enhanced services to all the SSP's in an IN under the control of the SCP. It is centralized since it is more economical for several users to share the specialized resources available in the IP which may be too expensive to replicate in all the SSPs. The following are examples of resources that may be provided by an IP:

- Voice response system
- Announcements
- Voice mail boxes
- Speech recognition system
- Text-to-speech converters

7.10.4 In Services

The various IN services are :

- **Televoting** : Televoting is unique service used in collecting public opinion. A user who wishes to vote, can dial the specific voting number to register his vote of choice. Televoting is possible from STD barred phones also. Televoting is a more cost-effective method of democratic deliberation as it does not require the participants/voter to meet in person. Televoting numbers are 13 digit number :

  1803-424-ABCD-XY (no charge to voter, service subscriber to pay)

  1861-424-ABCD-XY (unit pulse charge to voter)

  1862-424-ABCD-XY (two pulse charge to voter)

- **Voice VPN** : What is true of all VPNs is that they provide connectivity between two or more places using a previously established, shared network infrastructure rather than having to deploy new, dedicated hardware specifically for this purpose. Combined voice VPN can be provided for fixed line telephones of BSNL/MTNL and BSNL mobile. Use this service by dialing short codes to have a private network using public network resources. This service brings down telephone bills due to special package tariff for calls within VPN.
  11 digit number 1801-XYZ-ABCD

- **Toll Free Number** : This service shows the new function in charging, a call to a service subscriber will be paid by the called party. All charges are levied on the service subscriber. The service is free of any charge to the calling user. Service is accessible from networks of other Operators also
  11 digit number 1800-XYZ-ABCD

7.11 CONCLUSION

PSTN services once implemented, they were not easily modified to meet individual customer's requirements. Often, the network operator negotiated the change with the switch vendor. As a result of this process, it took years to plan and implement services. Intelligent network (IN) services are service-independent telecommunications network. That is, intelligence is taken out of the switch and placed in computer nodes that are distributed throughout the network. This provides the network operator with the means to develop and control services more efficiently. New capabilities can be rapidly introduced into the network. Once introduced, services are easily customized to meet individual customer's needs.

8 SIGNALING IN TELECOM NETWORK & SSTP

8.1 LEARNING OBJECTIVES

- Types of signaling
- Role of SSTP
- Functions of SSTP
- SSTP deployment in BSNL

8.2 INTRODUCTION

A telecommunication network establishes and realizes temporary connections, in accordance with the instructions and information received from subscriber lines and interexchange trunks, in form of various signals. Therefore, it is necessary to interchange information between an exchange and it external environment i.e. between subscriber lines and exchange, and between different exchanges. Though these signals may differ widely in their implementation they are collectively known as telephone signals.

A signalling system uses a language which enables two switching equipments to converse for the purpose of setting up calls. Like any other language. it possesses a vocabulary of varying size and varying precision, ie. a list of signals which may also vary in size and a syntax in the form of a complex set of rules governing the assembly of these signals. This handout discusses the growth of signalling and various type of signalling codes used in Indian Telecommunication.

Signalling has diversified area like land line telephone communication, mobile communication or data communication. In this chapter, signaling in land line telephone communication will be discussed in brief.

8.2.1 Types Of Signalling

a) Subscriber Line signaling

b) Inter-Exchange Signalling

Subscriber Line signaling

I. Calling Subscriber Line Signaling

In automatic exchanges the power is fed over the subscriber's loop by the centralized battery at the exchange. Normally, it is 48 V. The power is fed irrespective of the state of the subscriber, viz., idle, busy or talking.

II. Call request

When the subscriber is idle, the line impedance is high. The line impedance falls, as soon as, the subscriber lifts the hand-set, resulting in increase of line current. This is detected as a new call signal and the exchange after connecting an appropriate equipment to receive the address information sends back dial-tone signal to the subscriber.

III. Address signal

After the receipt of the dial tone signal, the subscriber proceeds to send the address digits. The digits may be transmitted either by decade dialing or by multifrequency pushbutton dialling.

IV. End of selection signal

The address receiver is disconnected after the receipt of complete address. After the connection is established or if the attempt has failed the exchange sends any one of the following signals.

- ✓ Ring-back tone to the calling subscriber and ringing current to the called subscriber, if the called line is free.
- ✓ Busy-tone to the calling subscriber, if the called line is busy or otherwise inaccessible.
- ✓ Recorded announcement to the calling subscriber, if the provision exists, to indicate reasons for call failure, other than called line busy.

Ring back, tone and ringing current are always transmitted from the called subscriber local exchange and busy tone and recorded announcements, if any, by the equipment as close to the calling subscriber as possible to avoid unnecessary busying of equipment and trunks.

V. Answer Back Signal

As soon as the called subscriber lifts the handset, after ringing, a battery reversal signal is transmitted on the line of the calling subscriber. This may be used to operate special equipment attached to the calling subscriber, e.g., short-circuiting the transmitter of a CCB, till a proper coin is inserted in the coin-slot.

VI. Release signal

When the calling subscriber releases i.e., goes on hook, the line impedance goes high. The exchange recognizing this signal, releases all equipment involved in the call. This signal is normally of more than 500 milliseconds duration.

VII. Permanent Line (PG) Signal

Permanent line or permanent glow (PG) signal is sent to the calling subscriber if he fails to release the call even after the called subscriber has gone on-hook and the call is released after a time delay. The PG signal may also be sent, in case the subscriber takes too long to dial. It is normally busy tone.

8.3 CALLED SUBSCRIBER LINE SIGNALS.

8.3.1 Ringing Signal

On receipt of a call to the subscriber whose line is free, the terminating exchange sends the ringing current to the called telephone. This is typically 25 or 50Hz with suitable interruptions. Ring-back tone is also fed back to the calling subscriber by the terminating exchange.

8.3.2 Answer Signal

When the called subscriber, lifts the hand-set on receipt of ring, the line impedance goes low. This is detected by the exchange which cuts off the ringing current and ring-back tone.

8.3.3 Release Signal

If after the speech phase, the called subscriber goes on hook before the calling subscriber, the state of line impedance going high from a low value, is detected. The exchange sends a permanent line signal to the calling subscriber and releases the call after a time delay, if the calling subscriber fails to clear in the meantime.

IV. Register Recall Signal

With the use of DTMF telephones, it is possible to enhance the services, e.g., by dialing another number while holding on to the call in progress, to set up a call to a third subscriber. The signal to recall the dialling phase during the talking phase, is called Register Recall Signal. It consists of interruption of the calling subscriber's loop for duration less than the release signal. it may be of 200 to 320 milliseconds duration.

8.4 INTER-EXCHANGE SIGNALING

The two type of inter-exchange signaling are channel associated signaling and common channel signaling.

8.4.1 Channel- Associated Signalling

In the PCM systems the signalling information is conveyed on a separate channel which is rigidly associated with the speech channel. Hence, this method is known as channel associated signalling (CAS). Though the speech sampling rate is 8 Khz, the signals do not change as rapidly as speech and hence, a lower sampling rate of 500 Hz, for digitisation of signals can suffice. Based on this concept, TS 16 of each frame of 125 microseconds is used to carry signals of 2 speech channels, each using 4 bits.

Hence, for a 30 channel PCM system, 15 frames are required to carry all the signals. To constitute a 2 millisecond multiframe of 16 frames. F 0 to F 15 TS 16 of the frame F 0 is used for multiframe synchronisation. TS 16 of F1 contains signal for speech channels 1 and 16 being carried in TS 1 and TS 17, respectively, TS16 of F2 contains signals of speech channels 2 and 17 being carried in TS2 and TS 18, respectively and so on, Both line signals and address information can be conveyed by this method.

Although four bits per channel are available for signalling only two bits are used. As the transmission is separate in the forward and backward direction, the bits in the forward link are called af and bf, and those in the backward link are called ab and bb.

As the dialling pulses are also conveyed by these conditions, the line state recognition time is therefore, above a threshold value. The bit bf is normally kept at 0, and the value 1 indicates a fault. However, the utilisation of such a dedicated channel for signalling for each speech channel is highly inefficient as it remains idle during the speech phase. Hence, another form of signalling known as common-channel signalling evolved.

8.4.2 Common Channel Signaling

Signaling System No. 7 (SS7) is a signaling protocol that has become a worldwide standard for modern telecommunications networks. SS7 is a layered protocol following the OSI reference model .It enables network elements to share more than just basic call-control information through the many services provided by the SS7's Integrated Services Digital Network-User Part (ISUP), and the Transaction Capabilities Application Part (TCAP). The functions of the TCAP and ISUP layers correspond to the Application Layer of the OSI reference model, and allow for new services such as User-to-User signaling, Closed-User Group, Calling Line Identification, various options on Call Forwarding and the rendering of services based on a centralized database (e.g., 800 and 900 service). All of these services may be offered between any two network subscribers.

8.5 CCS NETWORK ARCHITECTURE

The CCS Network is comprised of Four Major Components:

- Service Switching Points [SSP]

- Signaling Transfer Points [STP]
- Service Control Points [SCP]
- Data Signaling Links (SLK)

An SS7 Network consists of a flat non-hierarchical configuration enabling peer-to-peer Communication. Figure depicts the makeup and connectivity of SS7 Common Channel Signaling networks.

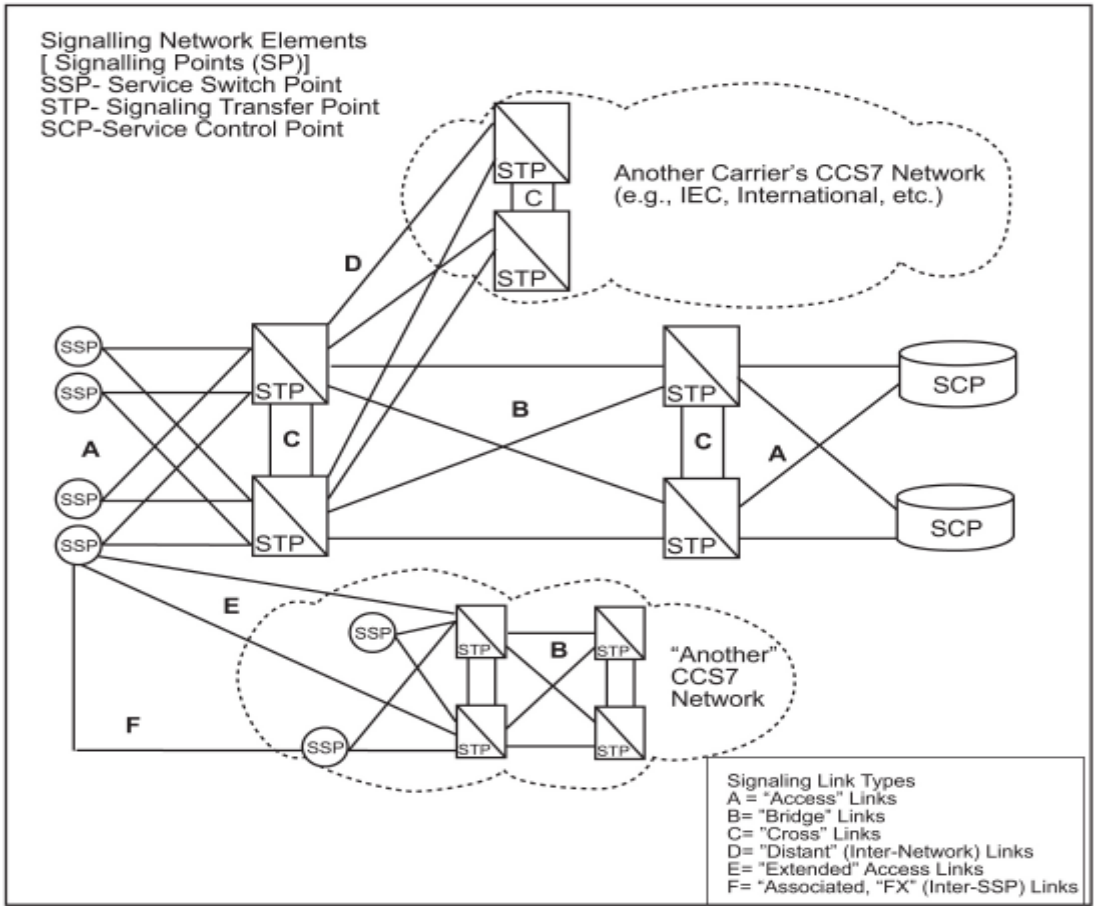


Figure 41: **Common channel signaling networks**

SS7 Common Channel Signaling Networks shows the three principal network elements of SS7 Common Channel Signaling networks, interconnected by the six standard types of signaling links currently in use. Signaling links are data transmission links that ordinarily operate on digital carrier facilities at 64,000 bits per second in most regions of the world. High Speed Links (HSLs) at 2.048 Mbps are used.

Signaling links between any two signaling network elements are deployed in groups called "link sets," dimensioned to carry the estimated signaling traffic between two STPs. Because STPs are deployed in pairs, as shown in Figure, SS7 Common Channel Signaling Networks, an alternate route always exists between any two STPs. One combination of the link sets interconnecting an SSP or SCP with both members of the

STP pair is called a "combined link set." The traffic carried between any two signaling network elements is load-shared across links in a link set, rotating through all links available according to the rules of the SS7 protocol.

Traffic destined for any network element through the STP pair is further load-shared over the combined link set, unless restricted by network management rules also established by the SS7 protocol.

8.5.1 Service Switching Point (SSP)

The SSPs are the legacy switches of the telecommunications network. SSPs are referred to as an "*End Office switch*", "*Central Office switch*", "Toll Tandem switch", etc. The central offices that house the SSP are identified by classes of ranging from a class 5-lowest, to a class 1 – highest office. The lowest class office in a network will be the one providing dial tone to subscribers. SSP is typically found in tandem or Class 5 offices and is the interface to the networks outside of SS7.

A SSP can be any of the following:

- Customer switch
- End office
- Access tandem
- Tandem

Usually, a switch is used to interface to the customer premise, The CO switch then interfaces to the SS7 network via the SSP. The SSP is the interface between the subscriber and the telecom network, and provide the following functions:

8.5.2 Call Processing Function

- Provides dial tone
- Routes calls between links and trunks
- Provides tones, and announcements
- Maintenance and revenue collection and generation

8.5.3 Query Processing

When necessary, it generates queries toward another signaling node or database to receive information necessary for certain calls.

8.5.4 SS7 Response Processing

Upon receiving queried information, carries out the connection function for proper handling of calls.

8.5.5 Resource Interface

For AIN services, establishes and maintains connections to Intelligent Peripherals (IPs)

8.5.6 Service Control Point (SCP)

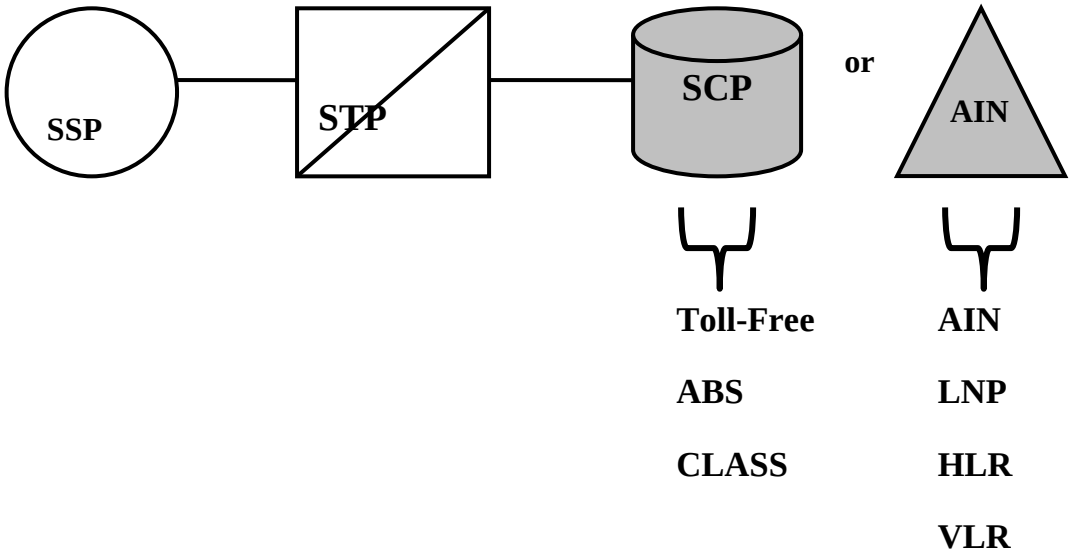


Figure 42: **SCP Connectivity**

The SCPs and AIN SCPs are centralized database that provide real-time access to call completion and information services such as:

- Toll-Free Database Service
- Alternate Billing Service (ABS)
- Custom Local Area Signaling Services (CLASS)
- Advanced Intelligent Network Services (AIN)
- Local Number Portability (LNP)
- Home Location Register (HLR)

- Visitor Location Register (VLR)

Signaling Transfer Point (STP)

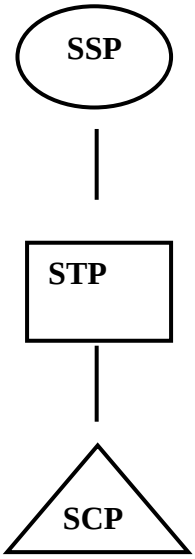


Figure 43: **Signaling transfer point (STP)**

STPs are routers that are placed within the heart of the CCS Networks. STPs are packet switches that provide common channel message routing and transport. STPs are stored programmed control switches that use information contained in messages in conjunction with information stored in memory to route message to the appropriate destination signaling point.

8.5 STP two-level Architecture in CCS Network

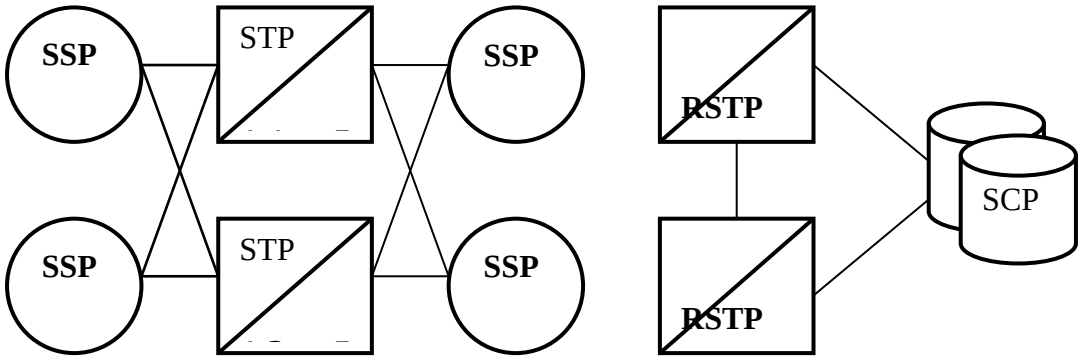


Figure 44: **2 level architecture in CCS network**

In large CCS networks, STPs are deployed in a hierarchical arrangement, and typically identified as Regional STPs, and Local STPs.

There are no functional differences in the two STPs.

The LSTP handles call set-up and network management traffic within the network.

The RSTP only handles query traffic within the network requiring access to SCP databases.

STPs are mainly of two types:

1. **Integrated STP**
   When STP functionality is incorporated along with 'Service Switching Point' in the 'Service Switching Node', it is known as Integrated Signalling Transfer Point. It performs call switching functions as well as Signalling transfer functions
2. **Standalone STP**
   Standalone STP performs only the core function of SS7 signalling transfer, It enables the operator to manage the network resources in more effective way and to host more applications.

8.6 SSTP FUNCTIONS

- SS7 Message routing
- Global Title Translation
- SS7 Network Management
- Network Interconnection
- Gateway Screening

8.6.1 SSTP Function – Message Routing

Message Routing: By using outgoing DPC contained in MTP's routing label in a datagram environment (where a separate route may be chosen for each message packet) Routing tables which are prepared to allow message transport between any given pair of SSTPs are stored and maintained within SSTPs. The SSTP's SNM (signaling network management) functions control message routing during periods of link congestion or failure.

- Routing is performed using Destination Point Codes (DPCs) similar to street address for the Postal Service. STPs have the ability to route messages to all types of signaling points.
- All nodes in the network are identified by a unique point code. This point code is used by CCSS #7 as the Origination Point Code (OPC) and the Destination Point Code (DPC) in the routing label of all Message Signaling Units (MSUs).

8.6.2 SSTP Function – Global Title Translation

Global Title translation : By using SCCP to translate addresses (Global titles) from signaling messages that do not contain explicit information allowing the MTP to route the message. For (e.g. SSTP translates dialed 1+ 800 number into an SCP's DPC for MTP routing and gives sub system number SSN for delivery of the good data base application at the SCP. When more information is needed to process a call, such as an 800 number, queries are processed for SSPs. STPs contain a GTT table with routing information for the type of query and address of SCP.

8.6.3 SSTP Function – Network Management

Acts as traffic cop to route traffic around failures in a network, and to control link congestion.

TFP Transfer Prohibited tells the connecting nodes not to send anything that is destined for the affected node.

TFR Transfer Restricted tells the connecting nodes – if all possible, not to send anything that is destined for the affected node.

8.6.4 SSTP Function – Gateway Screening

Screening is the capability to examine Incoming and Outgoing packets and allow those which are authorized. This is done by going through a series of Gateway screening tables that must be configured by the service provider. For example out of the messages which are coming via a link set only ISUP messages can be allowed whereas on another link only SCCP messages can be allowed by utilizing two basic function allow and block..

Software in SSTPs with inter-network connection is used to control who has access into a Telco's network.

8.7 OBJECTIVES OF SSTP'S

a. Following were the main objectives:-

b. Regulate, measure, and account for inter-network traffic including SMS messages from mobile networks including GSM and CDMA

c. Achieve a flexibility and transparency in management of signalling for BSNL's wired and wireless networks.

d. Optimal expansion of GSM & CDMA network of BSNL

e. Introduction of new services.

f. Offer CCS7 & IP Signaling Services to other Wire line & Wireless Network Operators.

8.8 STAND-ALONE STP NETWORK IN BSNL

Advantages:

- Dedicated signaling processors, resources
- Upgrade path divorced from MSC / SSP functions, growth
- Most effective method to manage network level resources, features
- Frees up processing capacity from the switches
- Can host most of the applications, centrally
- Full mated pair redundancy

Disadvantages**:**

- Requires additional investment (However compensated by freeing up extra resources of the switches)
- Requires traffic study, SS7 management

The P.O.No. SE/PO/005/2016-17/SSTP/New/UTStarcom dtd.01.03.2017 was issued by BSNLCO, for Supply, Installation, Commissioning and Migration to replace the existing SSTP network of M/s.Tekelec (now M/s. Oracle), with a new SSTP network to M/s.UTStarcom India Telecom Private Ltd., Gurgaon. As per the tender and PO, there are a total 18 SSTP nodes (with EMS NOC at Bangalore & DR EMS NOC at Mumbai. M/s UTStarcom has supplied all equipment, installed and ATed at all nodes.

iSG6400: The new UTSTARCOM SSTP iSG6400 primarily implements translation, adaptation and distribution functionality for SIGTRAN and SS7 signaling messages on the bottom layer, and the translation, adaptation and distribution functionality for M3UA-based SIGTRAN signaling、M2UA-based SIGTRAN signaling , SIP and Diameter signaling. The iSG6400 has the following features:

- Flexible Hardware and Software Platforms
- Carrier-Class High Availability
- Powerful System Functions
- MTP Message Screening
- Number Portability
- Diameter Signaling Controller
- Graphical and Convenient Network Management.

BSNL existing SSTP network comprising of 16 SSTP nodes installed in mated pair configuration. The SSTPs at Delhi, Chennai, Pune, & Ernakulum shall be with International Signaling Gateway functionality

Each of the TAXs/IP TAXs & MSCs in BSNL Network shall be connected to at least two SSTPs through IP and/or E1 link per SSTP on load balancing and failover manner

The MSCs in the Indian Telecom Network connected to TAXs/IP TAXs of BSNL Network shall be routed through one of the sixteen SSTPs installed as part of this tender .

SSTPs shall be connected with the BSNL's IP MPLS network through two L3 LAN switch with minimum two GE interfaces The Layer-3 switches shall be deployed in high availability mode (Active-Active) across different arms of each site.

SSTPs shall be interconnected with mated SSTP node with FE links /HSL links through the SDH network of BSNL for redundancy purposes in addition to interconnecting the SSTPs amongst themselves and to the EMS locations on the IP MPLS networks. Some network elements are also connected with HSL/FE links. NOC/ DR NOC at Bangalore and Mumbai.

Unique features of UTSTARCOM SSTP :

1. MNP capacity is 250M NP entries and can be further expanded
2. UT SSTP uses Oracle DB for eMS and NP DB. Oracle database is a truly carrier-class DB, with high reliability, centralized data management
3. UT SSTP network is composed of distributed SSTP nodes and Centralized eMS/NP SRV /DB SRV, it is more flexible and a better cost structure. All SSTP node share the centralized DB/eMS/NP SRV
4. Centralized DB means low CAPEX and OPEX
5. Veritas used to synchronize the Oracle DB between different NOC/DR-NOC to implement DB Geographic Redundancy. Veritas is most reliable tools to do this
6. Centralized eMS manages all the SSTP nodes which are deployed around PAN India.
7. eMS is GUI based, easy to operate and use, and more friendly
8. Support SS7 and SIGTRAN
9. Support the emerging DIAMETER AND SIP protocol.

8.9 CONCLUSION

The efficiency of SS7 had made a numbers of applications possible with e.g. fast connection setup in PSTN, "short message service" and "location update" messages in GSM world. The introduction of Standalone Signal Transfer Point (SSTP) was a historic step from that perspective. It immediately solved issues related to the complexity by converting the mesh networks into the star networks. It is now able to handle the signaling

very efficiently. SSTP also handle the non call related messages efficiently. The new SSTPs will be capable of supporting new signaling technologies like SIP and diameter, in addition to existing SS7/SIGTRAN and planned to cater to the signaling needs of BSNL network for future.

9 CDOT MAX NG

9.1 LEARNING OBJECTIVES

- Learn the Basic building blocks of MAX Family
- Requirement of MAX-NG
- Changes to be done while migration to MAX NG
- MAX-NG Components Core/Access and its function

9.2 INTRODUCTION

9.2.1 CDOT DSS

C-DOT DSS MAX is a universal digital switch which can be configured for different applications as local, transit, or integrated local and transit switch. High traffic/load handling capacity up to 8,00,000 BHCA with termination capacity of 40,000 Lines as Local Exchange or 15,000 trunks as Trunk Automatic Exchange, the C-DOT DSS family is ideally placed to meet the different requirements of any integrated digital network.

The equipment practices provide modular packaging. Common cards and advanced components have been used in the system hardware in order to reduce the number and type of cards. Standard cards, racks, frames, cabinets and distribution frames are used which facilitate flexible system growth. Interconnection technology has been standardized at all levels of equipment packaging. All these features, together with ruggedised design, make C-DOT DSS MAX easy to maintain and highly reliable.

9.3 BASIC GROWTH/BUILDING MODULES

C-DOT DSS MAX exchanges can be configured using four basic modules

- **Base Module**
- **Central Module**
- **Administrative Module**
- **Input Output Module**

9.3.1 Base Module

The Base Module (BM) is the basic growth unit of the system. It interfaces the external world to the switch. The interfaces may be subscriber lines, analog and digital trunks, CCM and PBX lines. Each Base Module can interface upto 2024 terminations. The number of Base Modules directly corresponds to the exchange size. It carries out

majority of call processing functions and, in a small-exchange application, it also carries out operation and maintenance functions with the help of the Input Output Module.

In Single Base Module (SBM) exchange configuration, the Base Module acts as an independent switching system and provides connections to 1500 lines and 128 trunks. In such a configuration, the Base Module directly interfaces with the Input Output Module for bulk data storage, operations and maintenance functions. Clock and synchronization is provided by a source within the Base Module. It is a very useful application for small urban and rural environments.

With minimum modifications in hardware through only one type of card, a Base Module can be remotely located as a Remote Switch Unit (RSU), parented to the main exchange using PCM links.

9.3.2 Central Module

Central Module (CM) consists of a message switch and a space switch to provide inter-module communication and perform voice and data switching between Base Modules. It provides control message communication between any two Base Modules, and between Base Modules and Administrative Module for operation and maintenance functions. It also provides clock and synchronization on a centralized basis.

9.3.3 Administrative Module

Administrative Module (AM) performs system-level resource allocation and processing function on a centralized basis. It performs all the memory and time intensive call processing support functions and also administration and maintenance functions. It communicates with the Base Module via the Central Module. It supports the Input Output Module for providing man- machine interface. It also supports the Alarm Display Panel for the audio-visual indication of faults in the system.

9.3.4 Input Output Module (I0P)

Input, Output Module (IOM) consists of duplicated Input Output Processor (IOP). The Input Output Processor (IOP) is a general-purpose computer with UNIX Operating System. It is used as the front-end processor in C-DOT DSS. It handles all the input and output functions in C-DOT DSS. The IOP is connected to AP/BP via HDLC links. During normal operation, two IOP’s interconnected by a HDLC link, operate in a duplex configuration. Working as front-end processor, it provides initial code down load to the subsystems, man machine interface and data storage for billing and other administrative information.

IOP interfaces various secondary storage devices like' disk drives, cartridge tape drive and floppy drive. It supports printers and upto 8 serial ports for video display units

which are used for man- machine communication interface. All the bulk data processing and storage is done in this module

Thus, a C-DOT DSS exchange, depending upon its size and application, consists of Base Modules (maximum 32), Central Module, Administrative Module, Input/Output Module and Alarm Display Panel. The Base Modules can be remotely located or co-located depending on the requirement.

9.4 REMOTE SWITCH UNIT

Remote Switch Unit (RSU) is an integral part of C-DOT DSS architecture. In order to realise a RSU, the normal BM can be modified for remoting with the host exchange via 2 Mbps digital links. The number of 2 Mbps links between the Main Exchange and RSU is primarily determined by the traffic. A maximum 16 PCMs can be provided between a RSU & Main exchange. Analog and Digital trunk interfaces are also implemented in RSU to support direct parenting of small exchanges from RSU itself instead of parenting it to the main exchange which will ultimately save the media required from main exchange. As far as call processing is concerned, RSU is an autonomous exchange capable of local-call completion. Operation and maintenance functions are handled by the host exchange. In the event of failure of PCM links, RSU goes into standalone mode of operation. In case it is not possible to process a call request due to unavailability of links to the host, the subscriber is connected to appropriate tone or announcement.

During standalone mode of operation, the local and incoming terminating calls in RSU are switched and the metering information of all the RSU subscribers is stored in the RSU. It is sent to the host whenever the PCM links are available again.

Only the even numbered BMs can be configured as RSU i.e. a maximum 16 RSUs are possible in C-DOT DSS MAX-XL and 8 RSUs in MAX-L.

9.5 SYSTEM FEATURES

9.5.1 General Features

This section includes system features related to the CTOD DSS MAX. They are:

TYPES OF SERVICES- The CDOT DSS of different capacities can be put to use at various switching nodes in the telecommunication network.

MAX

Main Automatic Exchange MAX is expandable to large capacities of order of 2000 lines or beyond. The MAX may have Remote Modules (RM) and Remote Line Concentrators (RLC) connected to it.

RAX

Rural Automatic Exchange (RAX) is a small exchange and is expandable upto 2000 lines capacity. Single Base Module configuration (i.e. CDOT SBM RAX with or without concentration) comes under the RAX category.

9.6 TYPES OF APPLICATION

The system can be put to the following applications:

Replacements

The exchange can serve as replacement of an existing switching system due to be phased out from the network.

New Exchanges

Wherever new exchanges are opened, the CDOT DSS MAX can provide the switching network within the existing telecom network.

Extensions

The capacity of an existing CDOT switching system can be increased. For example if the capacity of an existing CDOT exchange is 512 points, it can be increased, to say, 4000 lines.

TYPE OF SYSTEM

The system is Stored Programme Controlled (SPC) which makes it possible to work in attended/non-attended type of working environment.

TYPE OF NETWORK

The switching network within the system is 4-wire digital.

TYPE OF COMPONENTS

The different type of components used include integrated circuits, miniature relays, PCB, etc. The connecting scheme between various modules emphasis connectorised hardware.

9.7 WHY MAX-NG ?

a. Consolidation of Data and Voice-Converged Services & Networks

b. Less Infrastructure cost in installation & expansion

c. Better enhanced services such as Video calling, Centrex, Multilingual announcements etc.

d. Distributed architecture & Centralized Control

e. More calls with less bandwidth

f. Lower costs per call, especially for long-distance calls

g. Involves more of software, simplified hardware infrastructure and changing upgrade economics, hence ease in upgradation

h. Remote support

i. Taking care of Component obsolescence

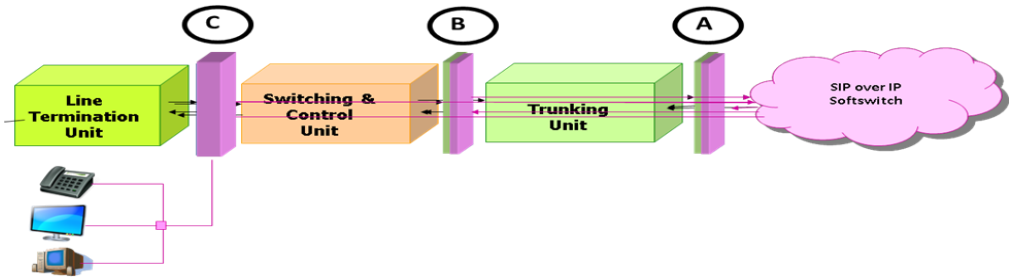


Figure 45: **Options for Upgrading to All-IP**

9.8 DSS MAX UPGRADE PROCEDURE

a. A Retain and convert line termination units to VoIP Access Gateways(LAG)

b. Convert trunk interfaces to VoIP Trunk Media Gateways(MG)

c. Convert the SS7 unit to a Signalling Gateway with STP functionality(SG)

d. Retain the Integrated Local and Tandem (ILT) functionality by moving Class 4 and Class 5 switching functions to an external softswitch (C4/C5)

e. Replace internal media and control paths with IP-enabled routing

f. Add on broadband interfaces for copper and wireless access.

9.9 MAX-NG COMPONENT

1. CORE COMPONENT
2. ACCESS COMPONENT

The MAX-NG network is structurally divided into the following four sub-network segments

a. NGN Core Network for delivery of Services

b. NGN Access Network consisting of MAX exchanges upgraded to MAXNG exchanges

c. Operations Support Network consisting of

d. MAX-NG Billing System Interface

e. MAX-NG Service Provisioning Interface

f. MAX-NG Network Management

g. The existing IP/MPLS based NIB/NIB-II Transport Network

The NGN Core Network handles

- All Session Establishment, Call Processing and Service
- Delivery functions centrally.

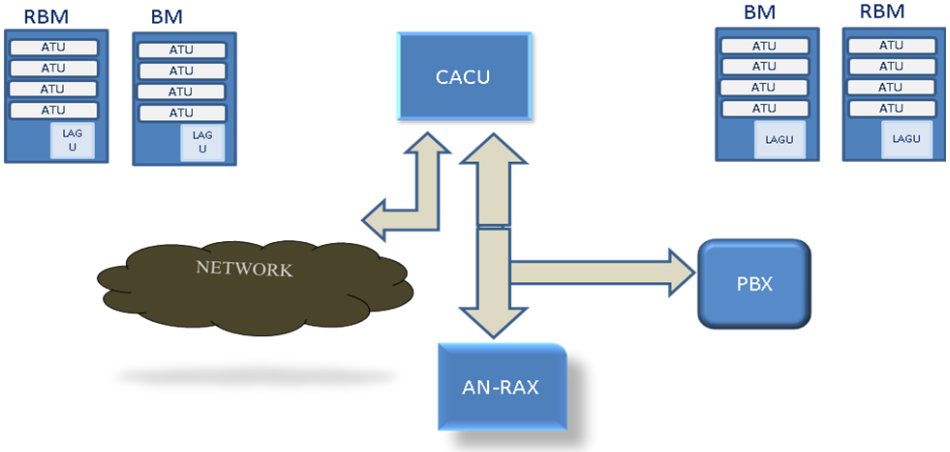


Figure 46: **MAX NG Architecture**

9.9.1 Core Component

The core network consists mainly of following servers.

• C5 Softswitch

• C4 Softswitch

• Session Border controller (SBC)

• Rating Engine

• SG Server

• EMS Server

• LIS Server

9.9.2 C5 Softswitch

A central device in a telecommunications network which connects telephone calls from one phone line to another, entirely by means of software running on a server. SIP protocol is used to establish calls.Currently in MAX N/W switching is carried out by hardware, with physical switchboards to route the calls.

• Soft switch

– Class 5 SS – Call Agent, Caller Server.

– Class 4 SS – Media Gateway Controller

9.9.3 C4 Softswitch

Class 4 soft switch is used to deliver calls of MAX-NG subscribers to PLMN/PSTN network via Signaling and Media Gateway and vice-versa MGC perform call control and signaling routing for PSTN and Signaling System 7 (SS7) voice traffic. MGC uses a Signaling Gateway (SG) to get SS7 signaling over IP, and provides ISUP to SIP and back translation. MGC controls Media Gateway (MG) using MEGACO/H.248 to translate the voice/media call component from TDM to RTP and back.

9.9.4 Session Border Controller (SBC)

A Session Border Controller (SBC) is a network function which secures voice over IP (VoIP) infrastructures while providing interworking between incompatible signaling messages and media flows (sessions) from end devices or application servers. Along with processing signaling messages, Session Border Controllers also handle all media traffic, typically in the form of RTP.

9.9.5 Rating Engine

The Rating engine is a system used to determine the customer chargeable units based on:

- Type of the day
- Time of day
- Call duration

9.9.6 SG Server

A Signaling Gateway is a network component solely responsible for translating signaling messages between one medium (usually IP) and another (PSTN) .

9.9.7 EMS Server

EMS (Element Management System) is a GUI based solution for configuring and monitoring the different systems installed as MAX-NG components.

9.9.8 LIS Server (Lawful Interception System)

- Monitoring the calls of a particular subscriber.
- The calls are diverted to another number as configured

9.9.9 Access Componnet

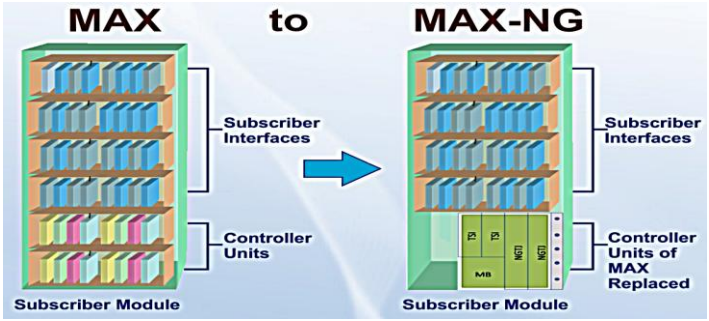


Figure 47: **MAX to MAX NG**

9.9.10 Line Access Gateway Unit(LAGU)

- C-DOT LAGU is designed to migrate fixed line TDM based technology of DSS-MAX to IP based technology.
- It converts basic voice into RTP and Signaling information to SIP and connects to the IP network.
- LAGU provides gateway functionality through a pair of network gateway cards working in active-standby mode.
- LAGU systems are installed at all co-located and remote Base Modules of the MAX exchanges.
- A BM system is converted to LAGU system replacing BPU and TSU with NGTJ cards and TSI cards.
- All TUs with PSUs, TCs (LCC), TIC, SPC and TUI cards are retained.
- 2-slot chassis consists of NGTJ card and TSI card interfacing with TUI cards in ATU frame.
- Supports maximum 32 E1s from RBM site to co-located BM site.

LAGU Chassis

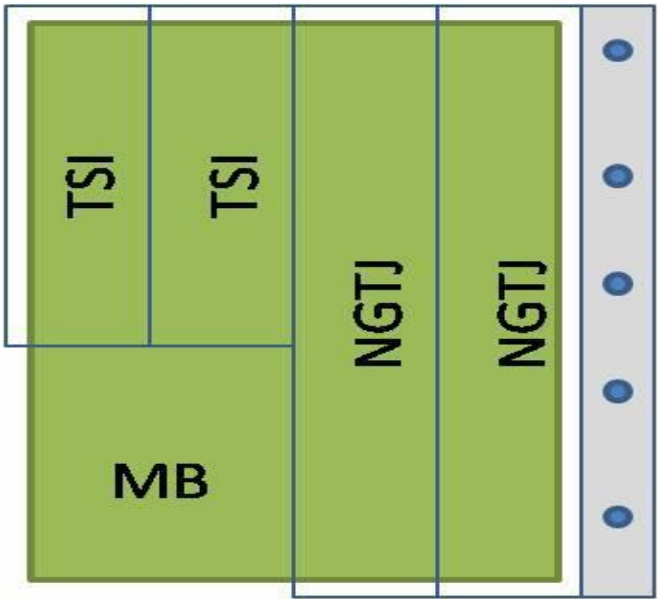


Figure 48: **LAGU Chasis**

- LAGU chassis contains two NGTJ & two TSI cards.
- TSI cards interface with TUI cards in ATUs through TT cables.
- NGTK variants are NGTK-A00 (EEB integrated) and NGTK-B00 (EEB not integrated).
- LAGU Chassis operates at -48V DC.
- 5VDC & 12 VDC for LAGU is fed from ATU.

9.9.11 Central Access Control Unit(CACU)

KEY COMPONENTS IN CACU CHASSIS-The 6-slot MAX-NG Card Frame (CACU) variant consists of the following components:

- Four Universal slots
- Pair of redundant aggregation slots
- Pair of redundant Shelf Management and Controller slots
- Pair of redundant -48V power feeds
- A FAN tray at the bottom
- Temperature sensor card with digital temp sensing for each slot

9.10 CARDS INSTALLED IN CACU CHASSIS

- ***Shelf Manager (SLM) cards***: A pair of SLM cards will be installed in the two

slots at the lower left side of CACU Chassis.

- ***NGTKcards***: NGTK cards can be installed in any of the first four universal slots. These cards work in 1+1 configuration.
- ***EBM cards***: EBM cards can be installed/jacked in into any of the first four universal slots. These cards work in 1+1 configuration.
- ***MLS cards***: A pair of MLS cards can be installed in the last two slots.
- ***TSN cards*** : Temperature sensor cards

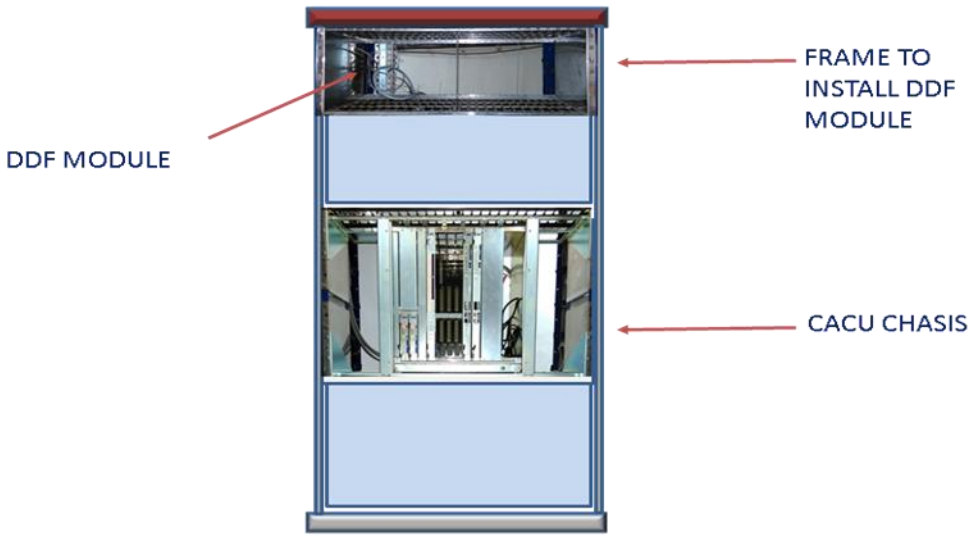


Figure 49: **CACU unit**

9.10.1 Media Gateway

- Media gateways are any type of device that allows for the conversion of data from one format to another.
- A Media Gateway (MG) function provides :
- the media mapping and/or transcoding functions between potentially dissimilar networks
- One of which is presumed to be a packet, frame or cell network.

9.10.2 Signalling Gateway

- In the MAX-NG network Signalling Gateway Comprise of Server and Line Card.
- The Line card at Every Access site for the interface with local exchange/TAX

exchange.

- At the other end (over IP) it interfaces with the softswitch/MGC through SG Server

9.10.3 V5.2 Access Gateway

- MAXNG is a MAX system with the functionalities of switching and control moved out to a Soft switch.
- V5AG is one of the MAXNG component which transport V5 signaling from TDM (PSTN) to IP network and convert media from TDM to IP Packet network & vice versa.

9.10.4 Ethernet To E1 Bridge Main

- Installed at the erstwhile of CM Site in 6-Slot CACU Chassis.
- Terminate the E1 links carrying the Ethernet traffic from the remote LAGU (the MAX-NG upgraded RSUs).
- The remote BM is upgraded to LAGU having the internal EBM card.

9.11 CONCLUSION:

The CDOT MAX NG seems to be the technology that will prevail in Next Generation Networks (NGNs) and its main goal to make convergence between any IP networks and a vertical handoff may happening depend on the user requirements (services, QoS..etc). This chapter provides a summary of CDOT MAX NG architecture for NGN and how two different IP based network can be involved in a session under the umbrella.

10 IP MULTIMEDIA SUBSYSTEM

10.1 LEARNING OBJECTIVES

- Learn about the Architecture of IMS
- Different working elements of IMS Core
- IMS interfaces
- Application Servers to provide functionality.
- Basic Call Flow in IMS

10.2 INTRODUCTION

Many successful services are available today on the Internet, including e-mail, web browsing, chat, and audio and video downloading/streaming, Internet telephony and Multimedia Communications Services.

Both fixed and mobile operators face problem of subscriber churn, and the issue is getting worse as new service providers offers cheap, or free, calls over the Internet continue to arrive on the scene and gain market share.

- One key way to attract and retain subscribers is to offer differentiation in areas like personalization, service bundling, co-branding, business-to-business relations, tariffs, single sign-on and quality of service.

- Another key way to retain subscribers is to build on and strengthen the customer relationship so that subscribers are far more reluctant to switch suppliers, even if switching means lower call charges in the short term.

In this case, they will have to rapidly push IMS before proprietary solutions become largely adopted. IMS is the only standardized solution in the telecommunications world.

10.2 What is IMS?

IMS – IP Multimedia Subsystem standardized by the telecommunications world is a new architecture based on new concepts, new technologies, new partners and ecosystem.

IMS provides real-time multimedia sessions (voice session, video session, conference session, etc) and non real-time multimedia sessions (Push to talk, Presence, instant messaging) over an all-IP network.

IMS targets convergence of services supplied indifferently by different types of networks : fixed, mobile, Internet. IMS is also called Multimedia NGN (Next Generation Network).

IMS deployment is a strategic decision, not a network technology decision. It can be taken either by a traditional service provider in the context of repositioning its business on IP services or by any entity that would decide to start an activity in IP services even without owning an access or transport network.

IMS offers standardized service enablers and network interfaces that will make interoperability of new MM services easier to achieve.

IMS is a tool for operators that enable the creation and delivery of PS based person-to-person MM services in a way that protects the operator business model and generates new revenue.

Service scalability is solved by the IMS architecture. It offers support to compose services and expand existing services.

The core of IMS is combining the best of two worlds datacom industry & telecom industry.

10.3 WHY IMS?

Operator perspective	End-user perspective	General
Quality Of Service	New, exciting services and enhancements of existing services	Faster time to market with new services
Service Integration	Same services available regardless of terminal and access type	Grow and protect subscriber base, increase ARPU
Keeps charging relation with user	Ease of use & Security	Controlling CAPEX and OPEX

10.3.1 IMS Standardization

The IMS was initially standardized by the 3rd Generation Partnership Projects (3GPP) as part of its Release 5 specifications & is practically speaking targeted at supporting non – real time services .The second release is 3GPP Release 6 & is targeted at supporting real time services .3GPP release added inter-working with WLAN.

With the increasing penetration of Wireless Local Area Networks (WLANs) and emerging Wireless Metropolitan Area Networks (WiMax) as access network technologies, the IMS scope is now extended within the ongoing Release 7 standardization for any IP access network, including fixed access networks, i.e. DSL.

10.3.2 IMS Architecture As Defined By 3 GPP

The IMS provides all the network entities and procedures to support real-time voice and multimedia IP applications. It uses SIP to support signaling and session control for real-time services Depending on the specific tasks performed by a CSCF, CSCFs can be divided into three different types.

- Serving CSCF (S-CSCF).
- Proxy CSCF (P-CSCF).
- Interrogating CSCF (I-CSCF).

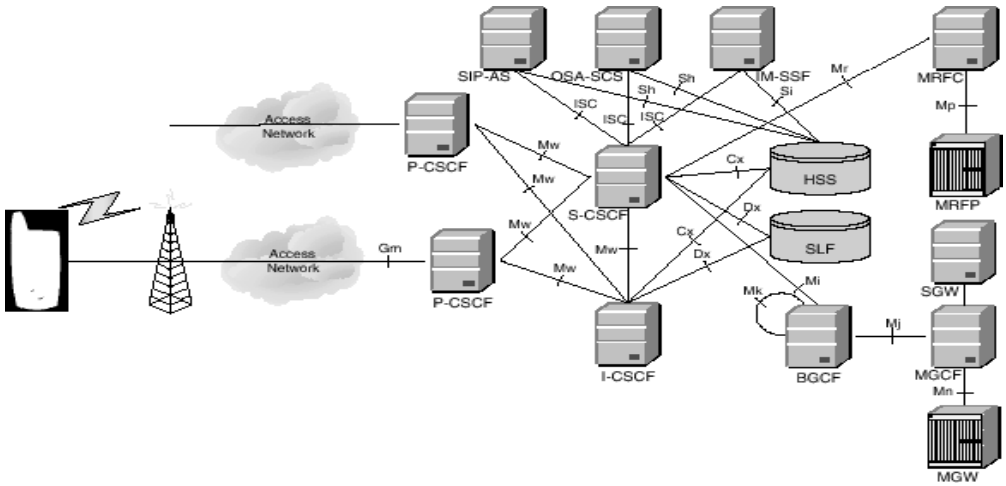


Figure 50: **GPP IP Multimedia Subsystems**

10.3.3 S-CSCF (Serving Call State Control Function)

An S-CSCF provides session control services for a user. It maintains session states for

a registered user's on-going sessions and performs the following main tasks.

a. Registration: An S-CSCF can act as a SIP Registrar to accept users' SIP registration requests and make users' registration and location information available to location servers such as the HSS (Home Subscriber Server).

b. Session Control: An S-CSCF can perform SIP session control functions for a registered user. Relay SIP requests and responses between callingand called parties.

c. Proxy Server: An S-CSCF may act as a SIP Proxy Server that relays SIP messages between users and other CSCFs or SIP servers.

d. Interactions with Application Servers: An S-CSCF acts as the interface to application servers and other IP or legacy service platforms.

e. Other functions: An S-CSCF performs a range of other functions not mentioned above. For example, it provides service-related eventnotifications to users and generates Call Detail Records (CDRs) neededfor accounting and billing

10.3.4 P-CSCF

A P-CSCF is a mobile's first contact point inside a local (or visited) IMS. It acts as a SIP Proxy Server. In other words, the P-CSCF accepts SIP requests from the mobiles and then either serves these requests internally or forwards them to other servers. The P-CSCF includes a Policy Control Function (PCF) that controls the policy regarding how bearers in the packet-switched network should be used. The P-CSCF performs the following specific functions:

- Forward SIP REGISTER request from a mobile to the mobile's home network. If an I-CSCF is used in the mobile's home network, the P-CSCF will forward the SIP REGISTER request to the I-CSCF. Otherwise, the P- CSCF will forward the SIP REGISTER request to an S-CSCF in the mobile's home network. The P-CSCF determines where a SIP REGISTER request should be forwarded based on the home domain name in the SIP REGISTER Request received from the mobile.

- Forward other SIP messages from a mobile to a SIP server (e.g. the mobile's S-CSCF in the mobile's home network). The P-CSCF determines to which SIP server the messages should be forwarded based on the result of the SIP registration process.

- Forward SIP messages from the network to a mobile.

- Compression and decompression of SIP messages. Compression is required to minimize the air-interface time.
- Perform necessary modifications to the SIP requests before forwarding them to other network entities.
- Maintain a security association with the mobile.
- Detect emergency session.
- Create CDRs.

10.3.5 I-CSCF

An I-CSCF is an optional function that can be used to hide an operator networks internal structure from an external network when an I-CSCF is used. It serves as a central contact point within an operator's network for all sessions destined to a subscriber of that network or a roaming user currently visiting that network. Its main function is to select an S-CSCF for a user's session, route SIP requests to theselected S-CSCF. The I-CSCF selects an S-CSCF based primarily on the following information:

- Capabilities required by the user.
- Capabilities and availability of the S-CSCF and
- Topological information, such as the location of an S-CSCF and the location of the users P-CSCFs if they are in the same operators network as the S-CSCF.

10.3.6 The Databases: (HSS And SLF)

HSS (Home Subs Server):

• It is just like HLR & Authentication Centre (AuC).
• All the database of users are stored in HSS ie, authentication data , service profile ,charging etc will be in HSS.
• No VLR concept in IMS.
• HSS is mandatory. Whereas SLF is optional.

• HSS is master user database that supports IMS N/W entities that actually handle call.

• It contain subscriber profile , perform authentication & authorisation of the user & can provide information about subscriber location & IP information.

SLF (Subs Location Function)

•Whenever n/w size is so big that if one HSS cannot store data then SLF is required ,this is an addl. Component.

•Suppose S-CSCF has done some authorisation then it has to contact HSS for

downloading ,authentication etc .

–If one HSS is there then no ambiguity.

–But if more than one HSS then SLF will check which HSS.

•Both HSS & SLF communicate through Diameter protocol.

•This diameter is called as AAA protocol.

•SLF will have -(User-ID/ HSS-ID).

Both the HSS and the SLF implement the Diameter protocol (RFC 3588) with an IMS-specific Diameter application.

- The Media Gateway Control Function (MGCF) and the IM Media Gateway(IM-MGW) are responsible for signaling and media inter-working, respectively, between the PS domain and circuit-switched networks (e.g. PSTN).
- Multimedia Resource Function Processor (MRFP) –Provides resources to be controlled by the MRFC
  - Sources media streams (for multimedia announcements)
  - Processes media streams (e.g. audio transcoding, media analysis)
  - Tones and announcements –Applied on receipt of ACK, self-timed with BYE or stopped on BYE
  - Support DTMF within the bearer path.
- The Multimedia Resource Function Controller (MRFC) interprets signaling information from an S-CSCF or a SIP-based Application Server and controls the media streams resources in the MRFP accordingly.

The Breakout Gateway Control Function (BGCF) selects to which PSTN network a session should be forwarded. IT will then be responsible for forwarding the session signaling to the appropriate MGCF and BGCF in the destination PSTN network

10.6 Service Architecture:

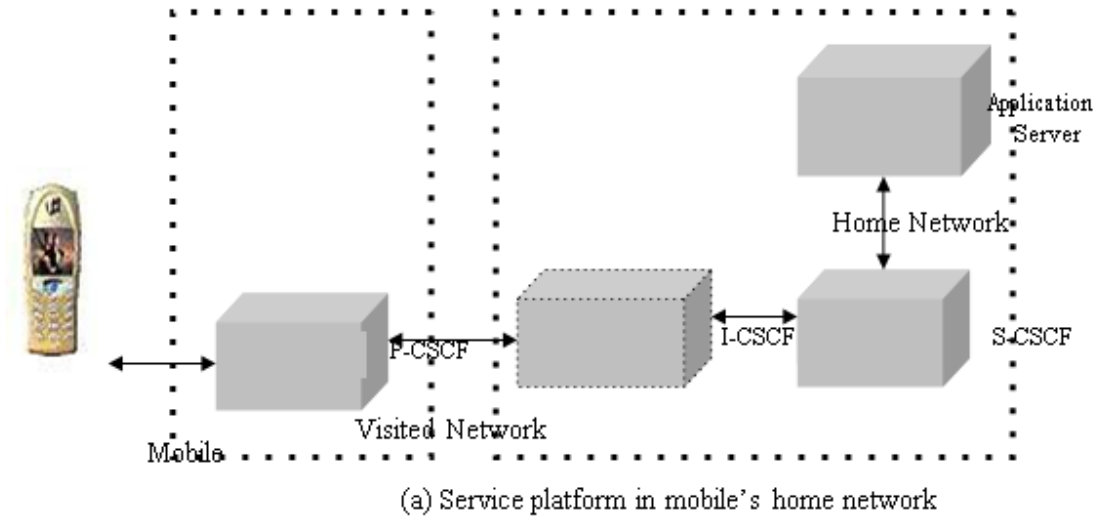


Figure 51: **Service architecture**

With both service architectures, the initial SIP request from a mobile travels from the originating mobile to the visited P-CSCF first, which then forwards the request to the I-CSCF (if used) in the originating mobiles home network. This I-CSCF selects an S-CSCF in the home network for this user session and forwards the SIP request to session will travel directly between the visited P-CSCF and the S-CSCF in the mobiles home network.

The S-CSCF is responsible for interfacing with internal and external service platforms as illustrated in Figure below. There are three types of standardized platforms:

(1) SIP application server
(2) Open Service Access (OSA) Service Capability Server (SCS) and
(3) IP Multimedia Service Switching Function (IM-SSF).

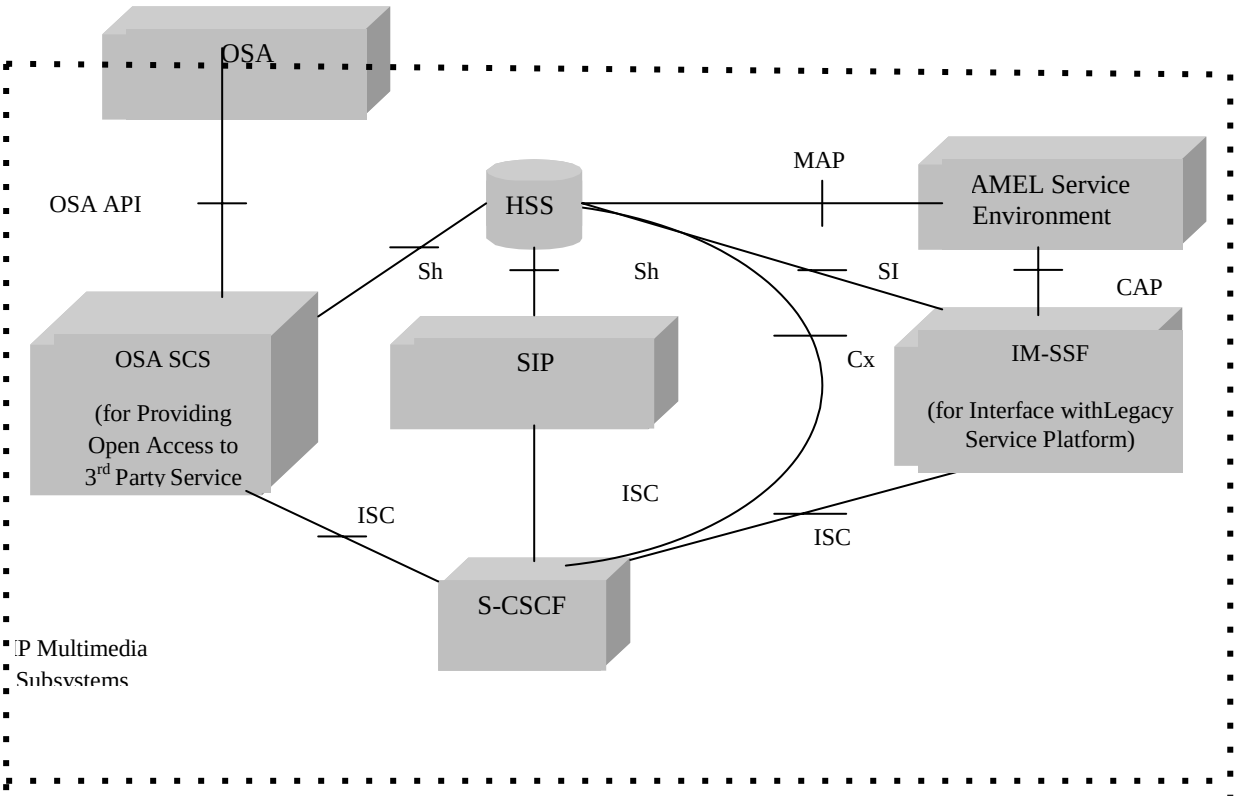


Figure 52: **Interaction between SCSCF and service platforms**

The services offered by them are value-added services (VAS or operator-specific services. The S-CSCF uses the same interface, IMS Service Control (ISC) interface, to interface with all service platforms. The signaling protocol over the ISC interface is SIP.

The OSA SCS and IM-SSF by themselves are not application servers. Instead, they are gateways to other service environments. As depicted in Figure, the OSA SCS and IM-SSF interface to the OSA application server and CAMEL Service Environment (CSE), respectively. From the perspective of the S-CSCF, however, they all exhibit the same ISC interface behavior. The services are briefly described:

10.4 SIP APPLICATION SERVER:

In addition to session control, a SIP server can also provide various value-added services. A lightweight SIP-based server enables the CSCF to utilize the SIP-based services and interact with the ISP application servers without additional components

10.4.1 Camel Service Environment (CSE):

The CSE provides legacy Intelligent Network (IN) services. It allows operators leverage existing infrastructure for IMS services. As specified earlier, the CSCF interacts with CSE through IM-SSF. The IM-SSF hosts the CAMEL features and interfaces with CSE by CAP (CAMEL Application Part).

10.4.2 OSA Application Server:

Applications may be developed by a third party that is not the owner of the network infrastructure. The OSA application server framework provides a standardized way for a third party to secure access to the IMS. The OSA reference architecture defines an OSA Application Server as the service execution environment for third-party applications. The OSA application server then interfaces with the CSCF through the OSA SCS by OSA API (Application Programming Interface).

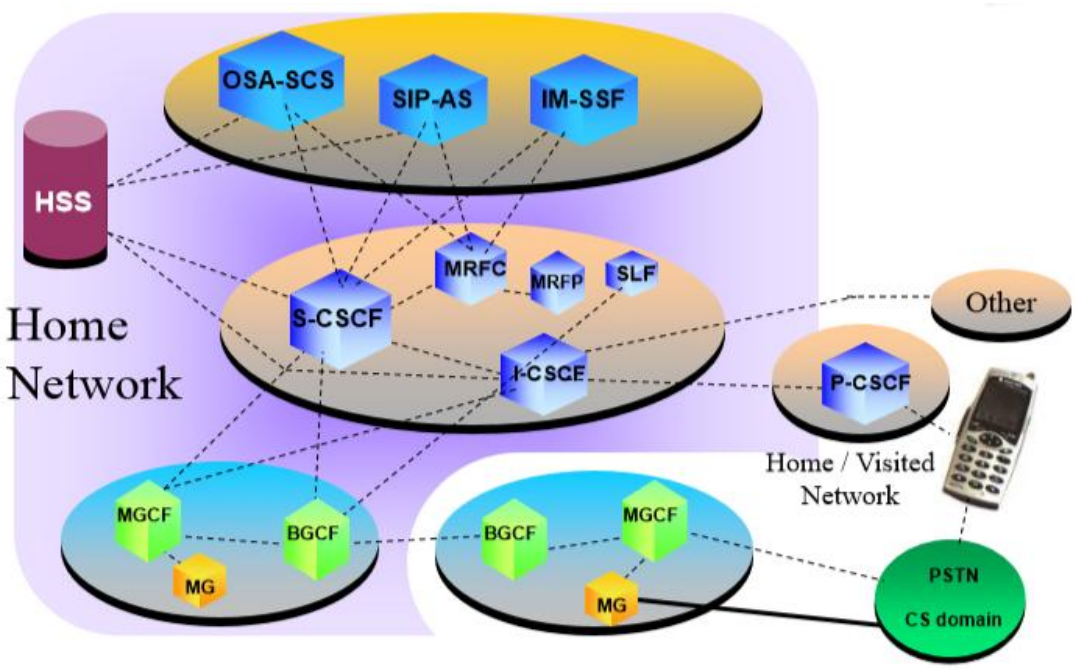


Figure 53: **Simplified 3GPP IMS Architecture**

Examples of Flow of Information:

Registration and Re-Registration

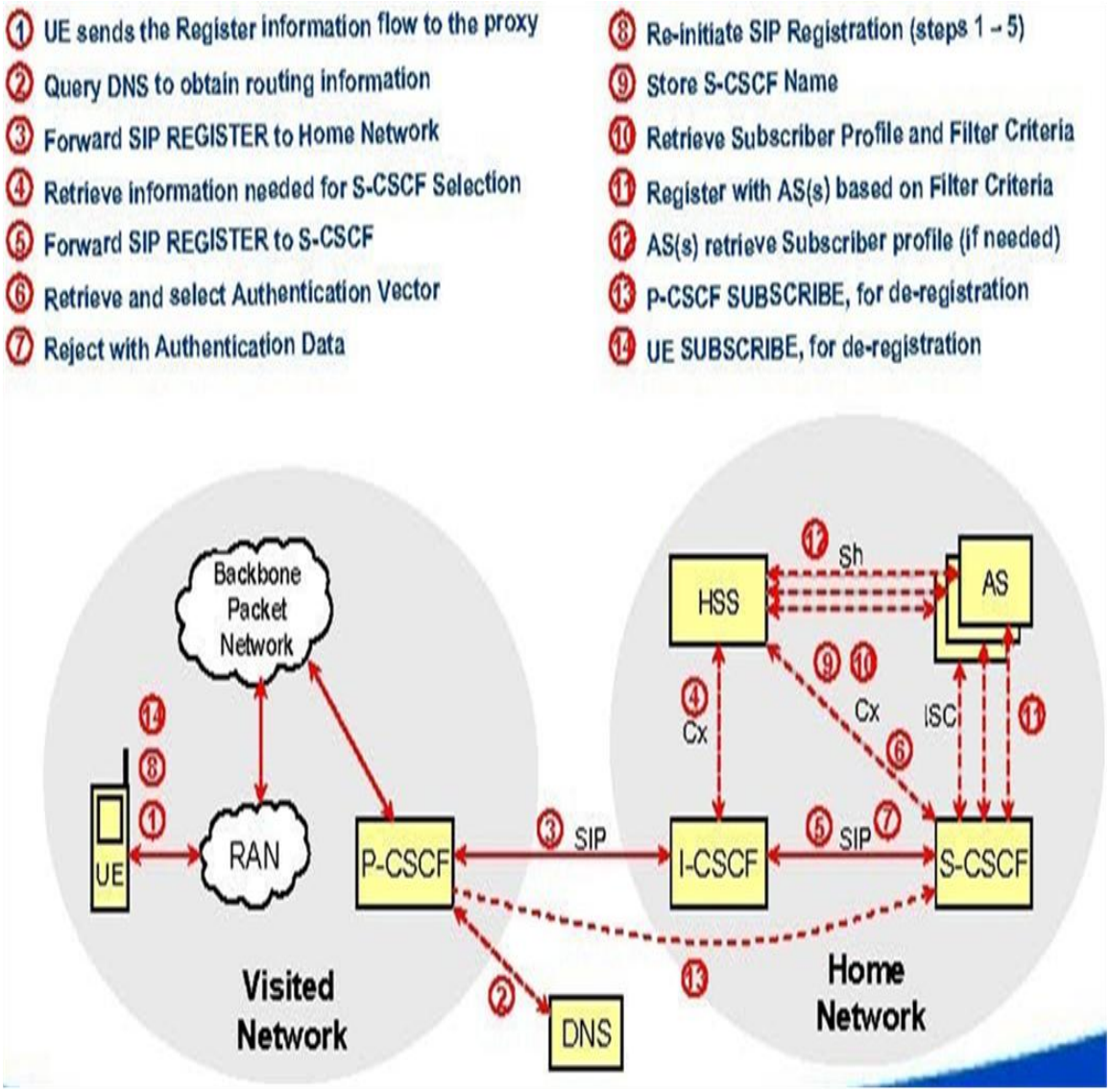


Figure 54: **Basic Message Flow**

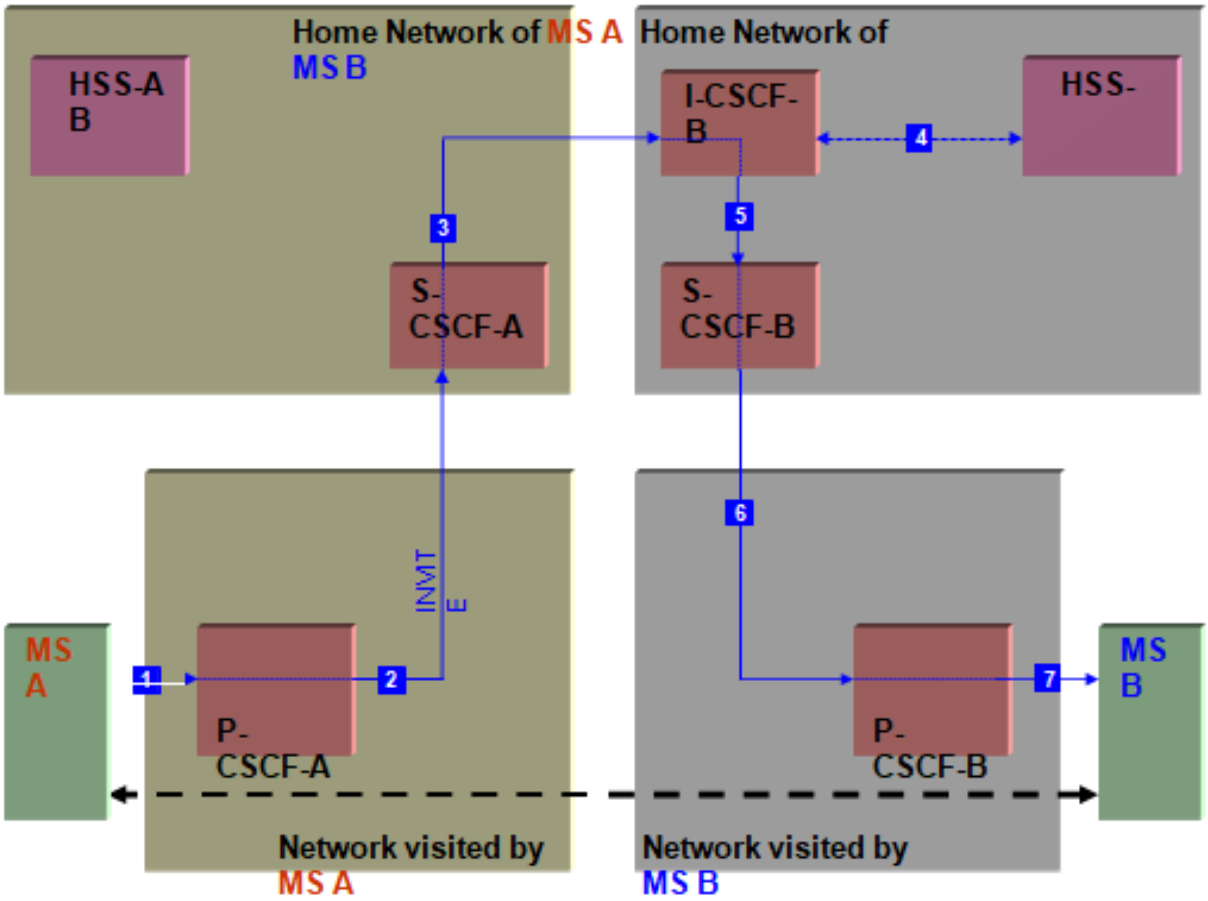


Figure 55: **Routing of Mobile-To-Mobile Calls - Session Initiation**

10.5 CONCLUSION:

The IP Multimedia Subsystem (IMS) seems to be the technology that will prevail in Next Generation Networks (NGNs) and its main goal to make convergence between any IP networks and a vertical handoff may happening depend on the user requirements (services,QoS,.etc). In this chapter it was presented an IMS based interworking architecture for NGN networking through which it prevail that how any two user from any two different IP based network can be involved in a session under the umbrella of IMS management. By presenting a complete signaling flow for concerning the authorization, registration, session set up and vertical handoff processes between two networks.

11 ADVANCED MPLS NETWORK

11.1 LEARNING OBJECTIVES

- Drawbacks of traditional IP forwarding
- MPLS advantages
- MPLS header
- MPLS operation
- MPLS router functionality
- MPLS VPN – overlay and peer to peer model
- MPLS LER architecture

11.2 INTRODUCTION

Multi Protocol Label Switching (MPLS) is an efficient encapsulation mechanism that uses “Labels” appended to packets (IP packets, AAL5 frames) for transport of data. MPLS packets can run on other layer 2 technologies such as ATM, FR, PPP, POS, Ethernet. Other layer 2 technologies can be run over an MPLS network. Labels can be used as designators. For example—IP prefixes, ATM VC, or a bandwidth guaranteed path.

It operates at a layer that is generally considered to lie between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer or IP Layer), and thus MPLS is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients, which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, Frame relay and Ethernet frames. The IP network has emerged as the network for providing converged, differentiated classed of services to user with optimal use of resources and also to address the issues related to Class of service (CoS) and Quality of Service (QoS). MPLS is the technology that addresses all the issues in the most efficient manner. MPLS is a packet-forwarding technology that uses labels to make data forwarding decisions.

11.3 DRAWBACKS OF TRADITIONAL IP FORWARDING

- Routing protocols are used to distributeLayer 3 routing information and therefore every router may need full Internet routing information (more than100,000 routes).
- Forwarding is based on the destination address only.
- Routing lookups are performed on every hop that slows down the forwarding

operation.

- Packets can't be given priority. Though TOS field is there in IP packets through which priority can be given to packets but routers are designed to bypass the TOS field.
- Layer 2 devices have no knowledge of Layer 3 routing information —virtual circuits must be manually established.

11.4 MPLS ADVANTAGES

1. Specifies mechanisms to manage traffic flow of various granularities, such as flows between different hardware, machines, or even flows between different applications.
2. Create new services via flexible classification
3. Provides the ability to setup bandwidth guaranteed paths
4. Enable ATM switches to act as routers
5. MPLS remains independent of the Layer-2 & layer-3 protocols. Meaning thereby that label encapsulating the data packet does not depend upon layer 3 /layer 2 protocol of data. This justifies the name as multi protocol label switching.
6. Provides a means to map IP addresses to simple, fixed-length labels used by different packet-forwarding and packet-switching technologies
7. Interfaces to existing routing protocols such as resource reservation protocol (RSVP) and open shortest path first (OSPF).
8. Supports the IP, ATM, and frame- relay Layer-2 protocols.
9. MPLS gives network operators a great deal of flexibility to divert and route traffic around linkfailures, congestion, and bottlenecks.
10. From a Quality of Service (QoS) standpoint, ISPs will better be able to manage different kinds of data streams based on priority and service plan. For instance, those who subscribe to a premium service plan, or those who receive a lot of streaming media or high-bandwidth content can see minimal latency and packet loss.
11. Enable ATM switches to act as routers

11.5 MPLS HEADER

11.5.1 What Is A MPLS Header?

MPLS works by prefixing packets with an MPLS header containing one or more 'labels'.

This is called a label stack. Each label stack entry contains four fields: -

- 20-bit label value (This is MPLS Label)
- 3-bit Experimental field used normally for providing for QoS (Quality of Service)
- 1-bit bottom of stack flag. If this is 1, signifies that the current label is the last in the stack.

- 8-bit TTL (time to live) field.

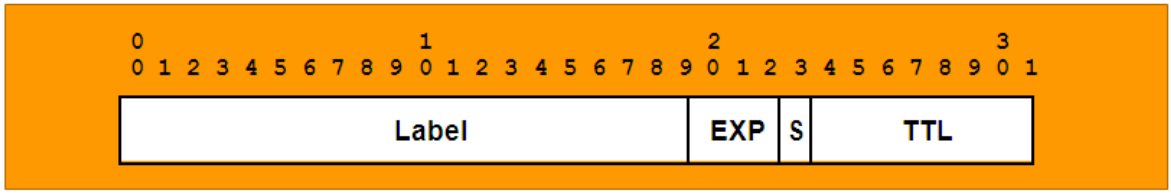
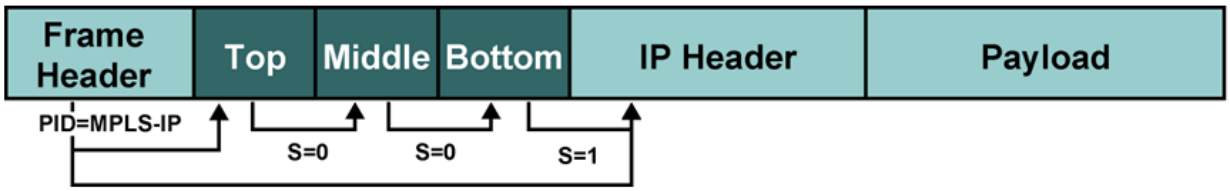


Figure 56: **MPLS Header format**

11.5.2 MPLS Label Stack



- Protocol identifier in a Layer 2 header specifies that the payload starts with a label (labels) and is followedby an IP header.
- Bottom-of-stack bit indicates whether the next header is another label or a Layer 3 header.
- Receiving router uses the top label only.
- Usually only one label is assigned to a packet.
- The following scenarios may produce more thanone label:
  - MPLS VPNs (two labels: The top label points to the egressrouter and the second label identifies the VPN.)
  - MPLS TE (two or more labels: The top label points to the endpoint of the traffic engineering tunnel and the second label points to the destination.)
  - MPLS VPNs combined with MPLS TE (three or more labels.)

11.6 VARIOUS ROUTING FUNCTION UNITS & ROUTERS IN MPLS

Routing function in MPLS can be described on the basis of some units, which are defined as follows:

Label: A label is an identifier, which indicates the path a packet, should traverse. Label is carried along with the packet. The receiving router examines the packet for its label content to determine the next hop. Once a packet has been labeled, the rest of the journey of the packet through the backbone is based on label switching. Since every intermediate

router has to look in to the label for routing the decision making at the level of router becomes fast.

Label Creation: Every entry in routing table (build by using any IGP protocol) is assigned a unique 20-bit label.

SWAP: Every incoming label is replaced by a new outgoing label (As per the path to be followed) and the packet is forwarded along the path associated with the new label.

PUSH: A new label is pushed on top of the packet, effectively "encapsulating" the original IP packet in a layer of MPLS.

POP: The label is removed from the packet effectively "de-encapsulating". If the popped label was the last on the label stack, the packet "leaves" the MPLS tunnel.

LER: A router that operates at the edge of the access network and MPLS network LER performs the PUSH and POP functions and is also the interface between access and MPLS network, commonly known as **Edge** router.

LSR: An LSR is a high-speed router device in the core of an MPLS network, normally called Core routers. These routers perform swapping functions and participate in the establishment of Label Switch Path (LSP)

Ingress / Egress Routers: The routers receiving the incoming traffic or performing the first PUSH function are ingress routers and routers receiving the terminating traffic or performing the POP function are Egress routers. The same router performs both functionality i.e. Ingress and Egress. The routers performing these functions are LER.

FEC: The forward equivalence class (FEC) is a representation of a group of packets that share the same requirements for their transport. All packets in such a group are provided the same treatment en route to the destination. As opposed to conventional IP forwarding, in MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network at the edge router.

11.7 BASIC MPLS OPERATION

When packets enter a MPLS-based network, **Label Edge Routers (LERs)** give them one or more labels (identifiers). These labels not only contain information based on the routing table entry (i.e., destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service.

Once this classification is complete and mapped, different packets are assigned to corresponding **Labeled Switch Paths (LSPs)**, where **Label Switch Routers (LSRs)**

place outgoing labels on the packets. With these LSPs, network operators can divert and route traffic based on data-streamtype and Internet-access customer

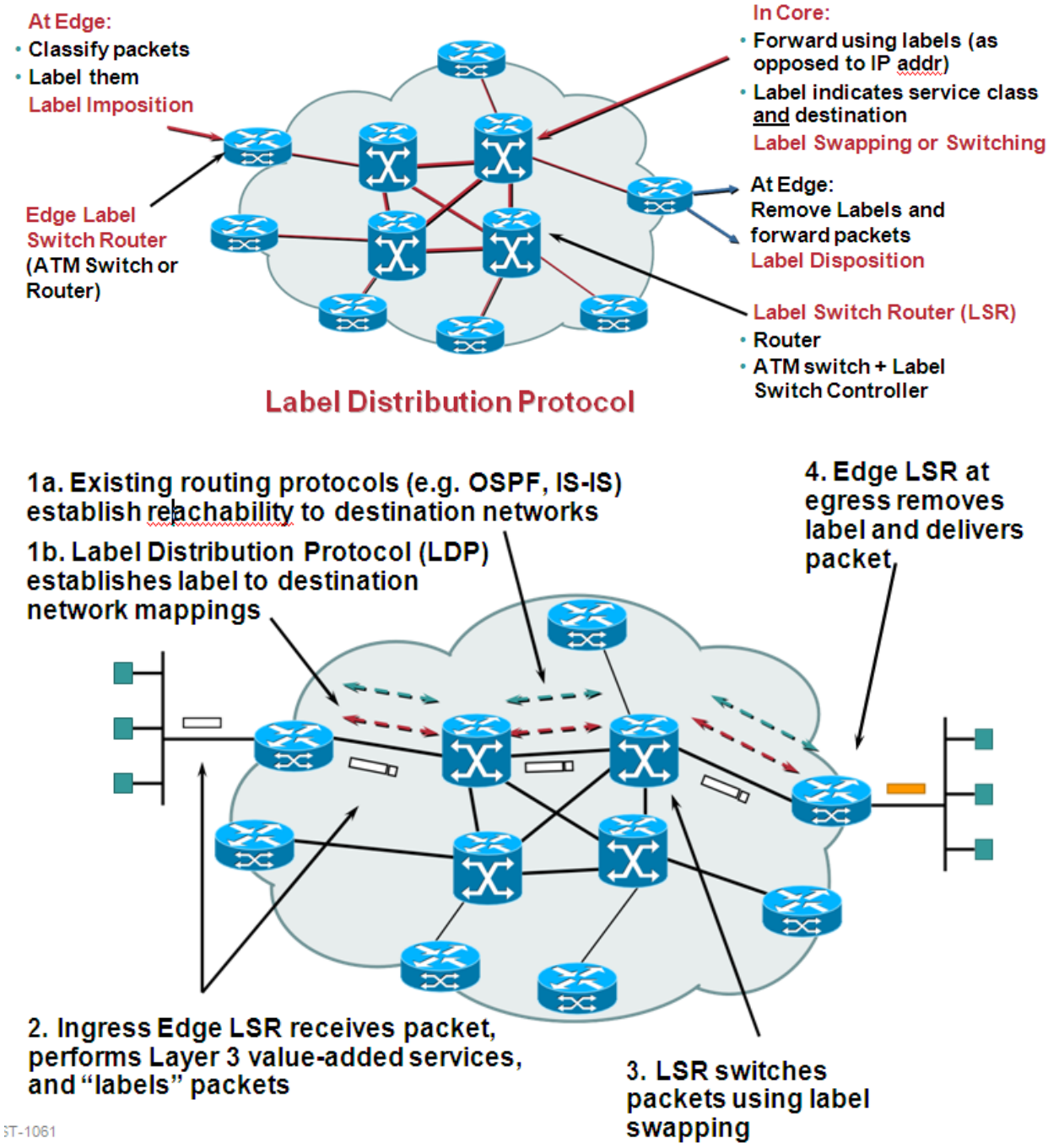


Figure 57: **Forwarding of Packets in MPLS network**

The following steps must be taken for a data packet to travel through an MPLS domain:

- Label creation and distribution

- Table creation at each router
- Label-switched path creation
- Label insertion/table lookup
- Packet forwarding.

11.8 MPLS ROUTER FUNCTIONALITY

MPLS Router functionality is divided into two major parts

Control plane: Exchanges Layer 3 routinginformation and labels. Control plane contains complex mechanisms to exchange routing information, such as OSPF, EIGRP, IS-IS, and BGP, and to exchange labels, such as TDP,LDP, BGP, and RSVP.

Data plane: Forwards packets based on labels. Data plane has a simple forwarding engine.

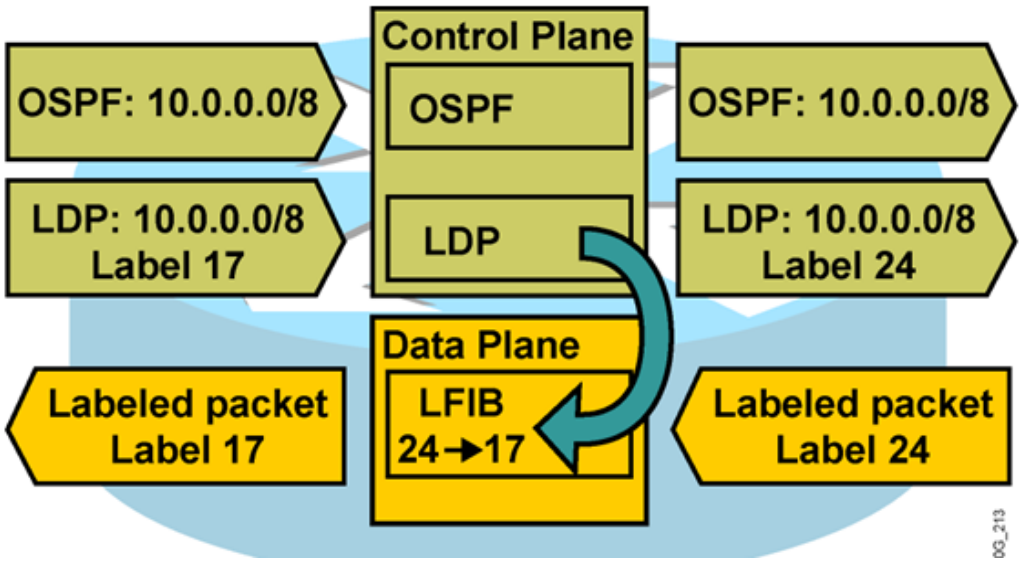


Figure 58: **MPLS functionality**

Architecture of LER:

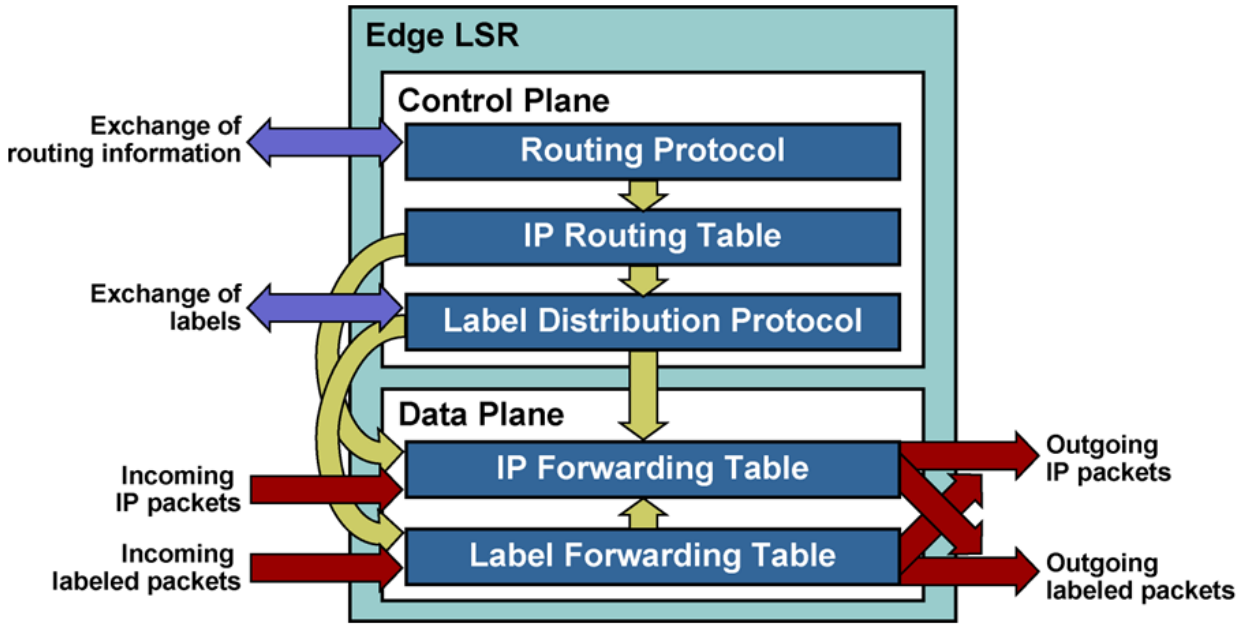


Figure 59: **Architecture of LER**

Architecture of LSR:

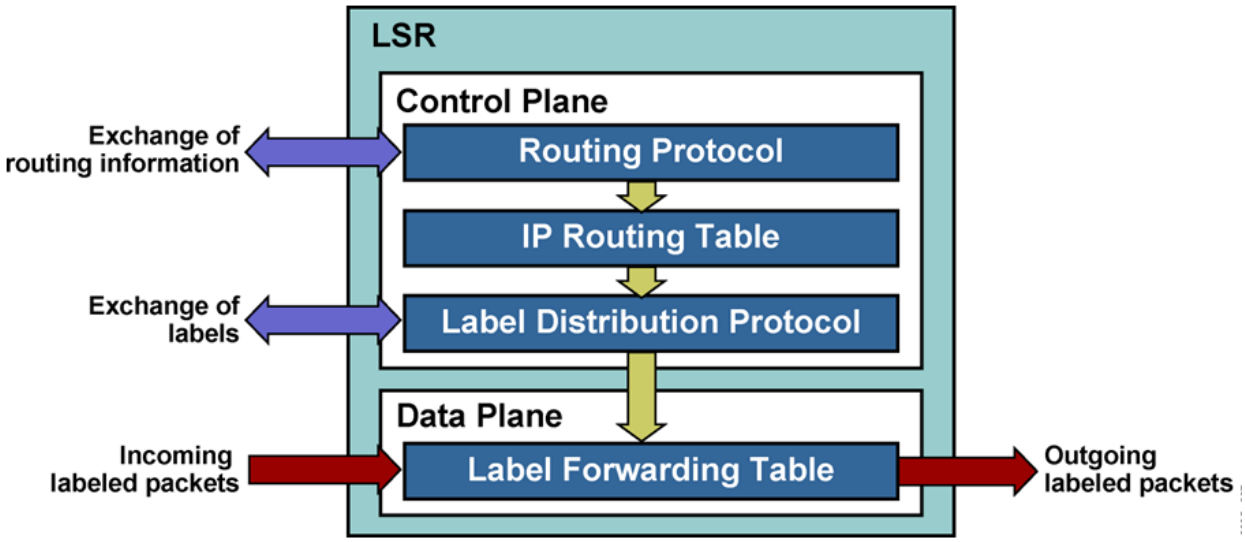


Figure 60: **LSR Architecture**

11.9 LABEL DISTRIBUTION AND FORWARDING OF PACKETS IN MPLS NETWORKS

- OSPF, IS-IS, BGP are needed in the network

- They provide reachability
- Label distribution protocols distribute labels for - prefixes advertised by unicast routing protocols using Either a dedicated Label Distribution Protocol (LDP, Extending existing protocols like BGP to distribute Labels
- Defined in RFC 3035 and 3036.
- It is used to distribute Labels in a MPLS network, Forwarding Equivalence Class(How packets are mapped to LSPs (Label Switched Paths)), Advertise Labels per FEC, Reach destination a.b.c.d with label x and Discovery

11.9.1 Router Example: Forwarding Packets

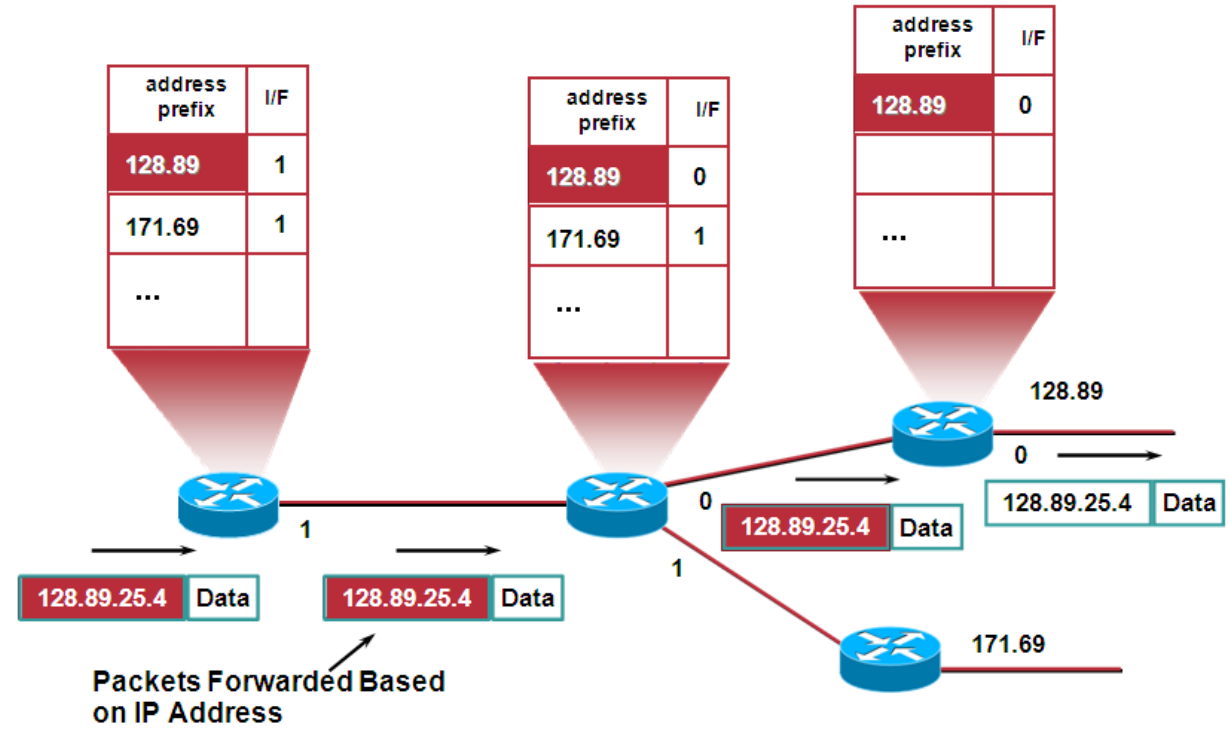


Figure 61: **Router EXAMPLE: Forwarding packets**

11.9.2 MPLS Example: Routing Information

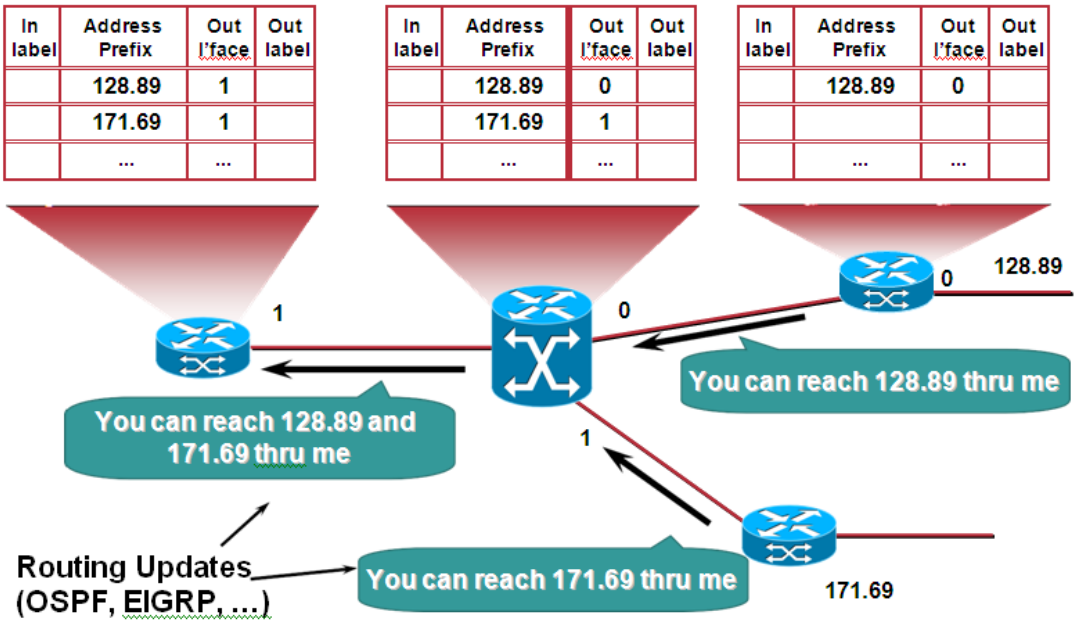


Figure 62: **MPLS Example: Routing Information**

11.9.3 MPLS Example: Assigning Labels

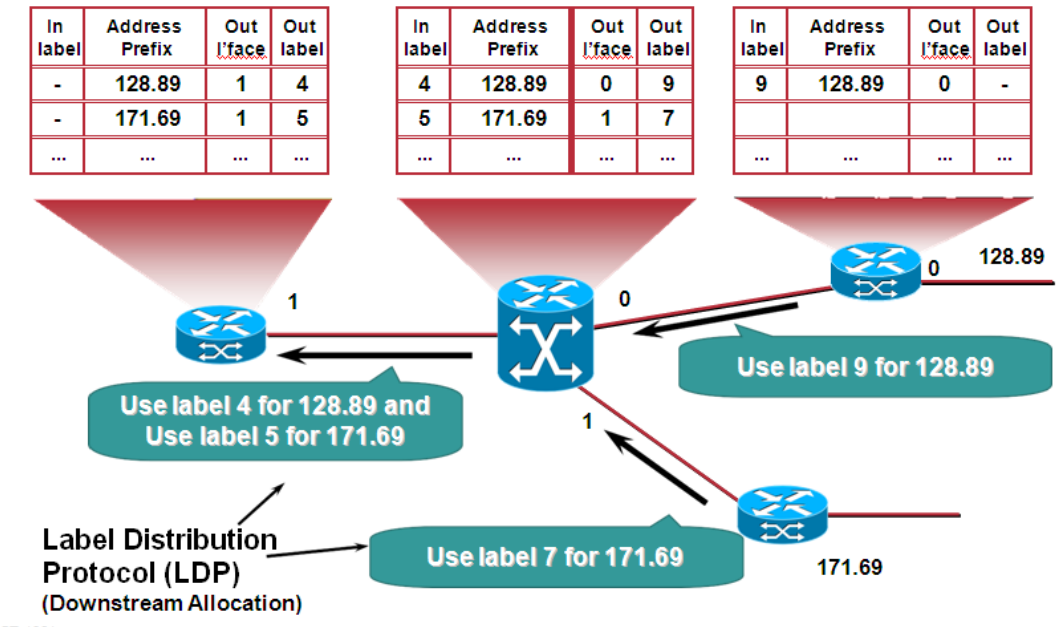


Figure 63: **MPLS Example: Assigning Labels**

11.9.4 MPLS Example: Forwarding Packets

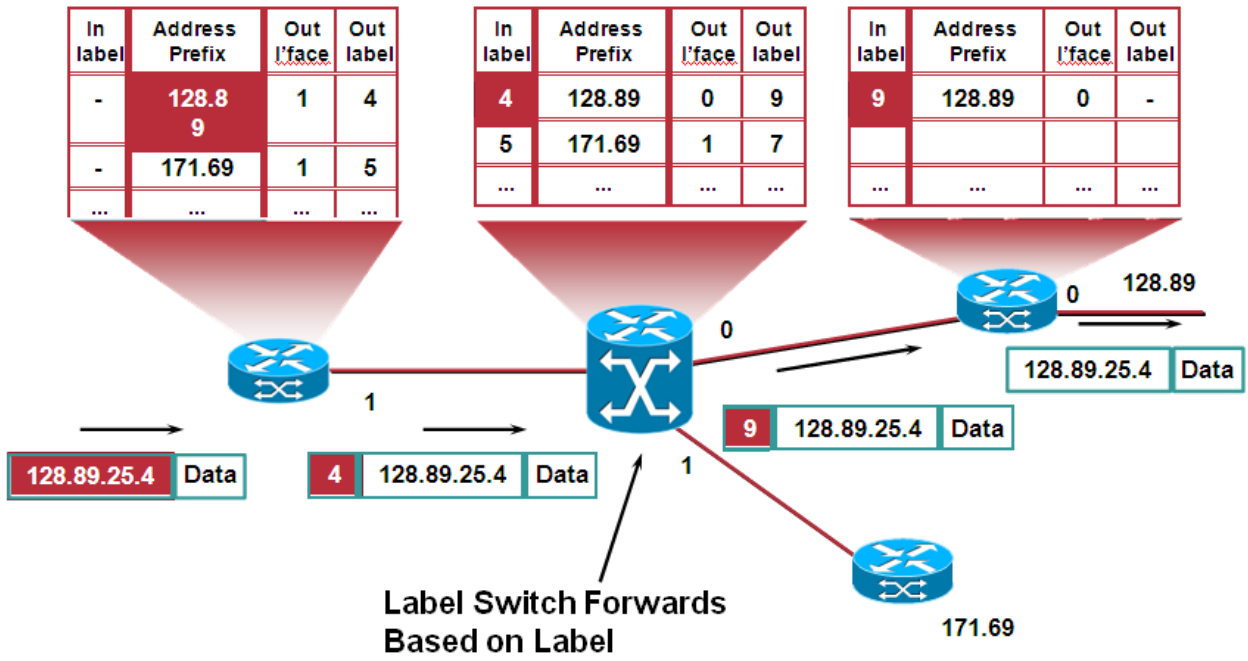


Figure 64: **MPLS Example: Forwarding packets**

11.10 MPLS LABEL DISTRIBUTION PROTOCOLS

MPLS architecture does not mandate a single method of signaling for label distribution. Existing routing protocols, such as the border gateway protocol (BGP), have been enhanced to piggyback the label information within the contents of the protocol. The

RSVP has also been extended to support piggybacked exchange of labels. A summary of the various schemes for label exchange isas follows:

- **LDP**—maps unicast IP destinations into labels
- **RSVP, CR–LDP**—used for traffic engineering and resource reservation
- **protocol-independent multicast (PIM)**—used for multicast states label mapping
- **BGP**—external labels (VPN)

The Internet Engineering Task Force (IETF) has also defined a new protocol known as the label distribution protocol (LDP) for explicit signaling and management of the label space. Extensions to the base LDP protocol have also been defined to support explicit routing based on QoS and CoS requirements. These extensions are captured in the constraint-based routing (CR)–LDP protocol definition. It is used to map FECs to labels, which, in turn, create LSPs. LDP sessions are established between LDP peers in the MPLS network (not necessarily adjacent)

11.11 LDP (LABEL DISTRIBUTION PROTOCOL)

LDP Protocol has the following functions:

- Neighbor discovery

  Discover directly attached Neighbors—pt-to-ptlinks (including Ethernet)

  Establish a session

  Exchange prefix/FEC and label information

- Extended Neighbor Discovery

  Establish peer relationship with another router thatis not a neighbor

  Exchange FEC and label information

  May be needed to exchange service labels

11.11.1 Tdp (Tag Distribution Protocol)

- Tag Distribution Protocol—Cisco proprietary
  - Pre-cursor to LDP
  - Used for Cisco Tag Switching
- TDP and LDP supported on the same device
  - Per neighbor/link basis
  - Per target basis
- LDP is a superset of TDP
- Uses the same label/TAG
- Has different message formats

11.12 OTHER LABEL DISTRIBUTION PROTOCOL – BGP

- Used in the context of MPLS VPNs
- Need multiprotocol extensions to BGP
- Routers need to be BGP peers

The peers exchange the following types of LDP messages:

- **discovery messages**—announce and maintain the presence of an LSR in a network
- **session messages**—establish, maintain, and terminate sessions between LDP peers

- **advertisement messages**—create, change, and delete label mappings for FECs
- **notification messages**—provide advisory information and signal error information

11.13 SETTING UP LABEL-SWITCHED PATHS (LSPS)

MPLS provides the following two options to set up an LSP:

- **hop-by-hop routing**—Each LSR independently selects the next hop for a given FEC. This methodology is similar to that currently used in IP networks. The LSR uses any available routing protocols, such as OSPF, ATM private network-to-network interface(PNNI), etc.

- **explicit routing**—Explicit routing is similar to source routing. The ingress LSR (i.e., theLSR where the data flow to the network first starts) specifies the list of nodes through which the ER–LSP traverses. The path specified could be non-optimal, as well. Along thepath, the resources may be reserved to ensure QoS to the data traffic. This eases traffic engineering throughout the network, and differentiated services can be provided using flows based on policies or network management methods.

The LSP setup for an FEC is unidirectional in nature. The return traffic must take another LSP.

11.14 MPLS VPNS

11.14.1 What Is A VPN:

- VPN is a set of sites which are allowed tocommunicate with each other
- VPN is defined by a set of administrative policies
- Policies determine both connectivity and QoS among sites
- Policies established by VPN customers
- Policies could be implemented completely by VPNService Providers
- Using BGP/MPLS VPN mechanisms
- Flexible inter-site connectivity ranging from complete to partial mesh
- Sites may be either within the same or in differentorganizations(VPN can

be either intranet or extranet)

- Site may be in more than one VPN (VPNs may overlap)
- Not all sites have to be connected to the same service provider (VPN can span multiple providers)

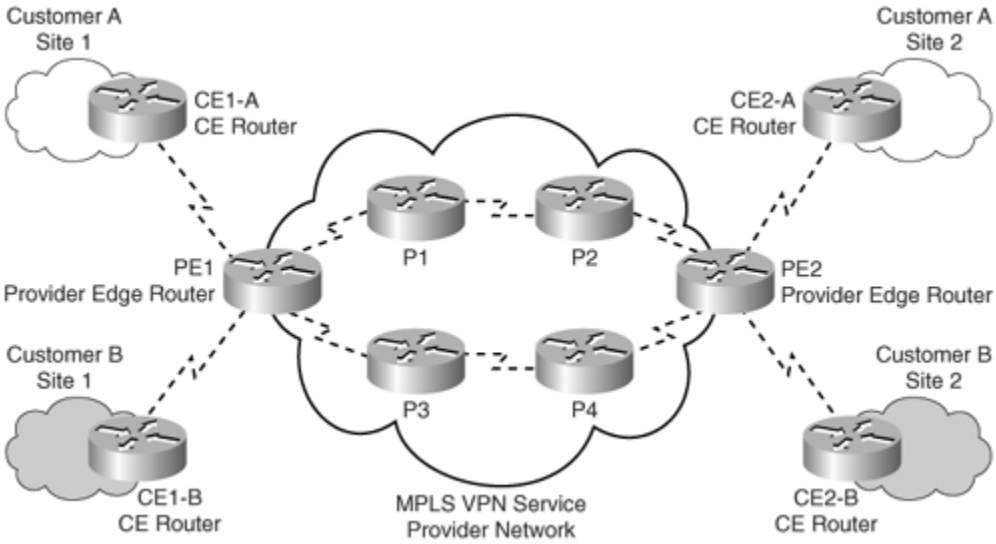


Figure 65: **MPLS VPN Architecture**

Customer network— Consisted of the routers at the various customer sites. The routers connecting individual customers' sites to the service provider network were called customer edge (CE) routers.
Provider network— Used by the service provider to offer dedicated point-to-point links over infrastructure owned by the service provider. Service provider devices to which the CE routers were directly attached were called provider edge (PE) routers. In addition, the service provider network might consist of devices used for forwarding data in the backbone called provider (P) routers.

11.15 CLASSIFICATION OF VPN IMPLEMENTATION

Depending on the service provider's participation in customer routing, the VPN implementations can be classified broadly into one of the following:

- Overlay model
- Peer-to-peer model

11.15.1 Overlay Model

1. Service provider doesn't participate in customers routing, only provides transport to customer data using virtual point-to-point links. As a result, the service provider would only provide customers with virtual circuit connectivity at Layer 2.
2. If the virtual circuit was permanent or available for use by the customer at all times, it was called a permanent virtual circuit (PVC).
3. If the circuit was established by the provider on-demand, it was called a switched virtual circuit (SVC).
4. The primary drawback of an Overlay model was the full mesh of virtual circuits between all customer sites for optimal connectivity. It resembles the physical mesh connectivity in case of leased lines. Overlay VPNs were initially implemented by the SP by providing either Layer 1 (physical layer) connectivity or a Layer 2 transport circuit between customer sites.

   In the Layer 1 implementation, the SP would provide physical layer connectivity between customer sites, and the customer was responsible for all other layers. In the Layer 2 implementation, the SP was responsible for transportation of Layer 2 frames (or cells) between customer sites, which was traditionally implemented using either Frame Relay or ATM switches as PE devices. Therefore, the service provider was not aware of customer routing or routes.

   Later, overlay VPNs were also implemented using VPN services over IP (Layer 3) with tunneling protocols like L2TP, GRE, and IPSec to interconnect customer sites. In all cases, the SP network was transparent to the customer, and the routing protocols were run directly between customer routers

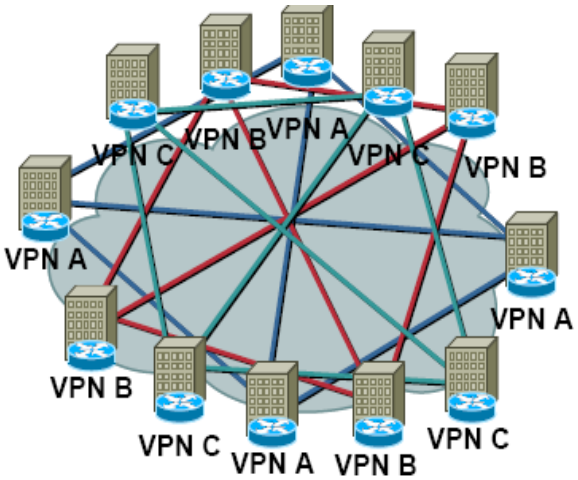


Figure 66: **Overlay VPN**

11.15.2 Peer-To-Peer Model

The peer-to-peer model was developed to overcome the drawbacks of the Overlay model and provide customers with optimal data transport via the SP backbone. Hence, the service provider would actively participate in customer routing. In the peer-to-peer model, routing information is exchanged between the customer routers and the service provider routers, and customer data is transported across the service provider's core, optimally. Customer routing information is carried between routers in the provider network (P and PE routers) and customer network (CE routers). The peer-to-peer model, consequently, does not require the creation of virtual circuits. The CE routers exchange routes with the connected PE routers in the SP domain. Customer routing information is propagated across the SP backbone between PE and P routers and identifies the optimal path from one customer site to another.

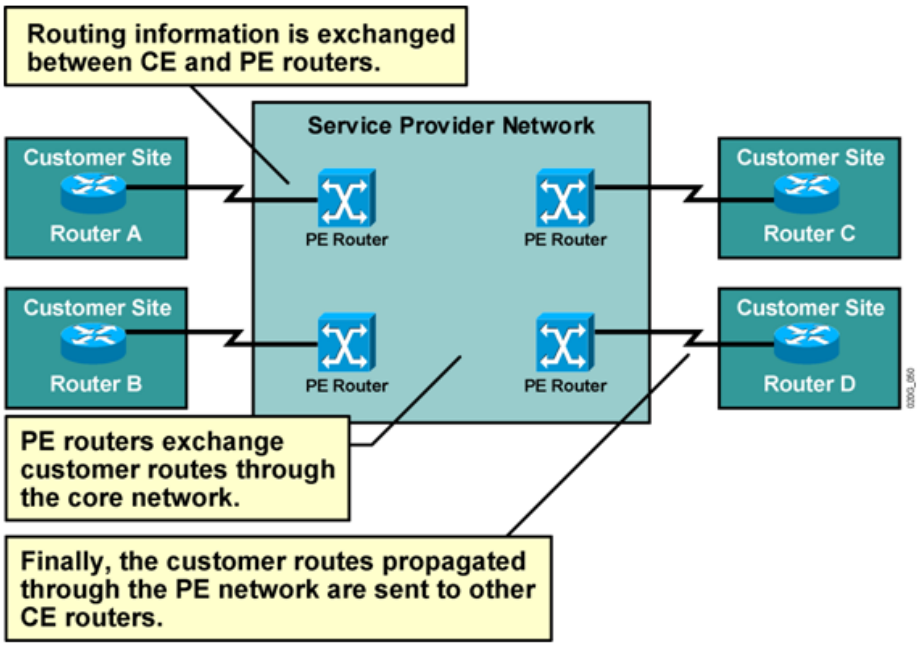


Figure 67: **Peer – to – Peer VPN**

11.16 DIAL VPN SERVICE

Mobile users of a corporate customer need to access their Corporate Network from remote sites. Dial VPN service enables to provide secure remote access to the mobile users of the Corporate. Dial VPN service, eliminates the burden of owning and maintaining remote access servers, modems, and phone lines at the Corporate Customer side. Currently accessible from PSTN (127233) & ISDN (27225) also from Broadband.

11.17 LAYER 2 AND LAYER 3 VPNS

- Layer 2 VPNs
  - Customer End points (CPE) connected via layer 2 such as FrameRelay DLCI, ATM VC or point to point connection
  - If it connects IP routers then peering or routing relationship is between the end points
  - Multiple logical connections (one with each end point)
- Layer 3 VPNs
  - Customer end points peer with provider routersSingle peering relationship
  - No mesh of connections
  - -Provider network responsible for
  - Distributing routing information to VPN sites
  - Separation of routing tables from one VPN to another

11.18 MPLS VPN WORKING

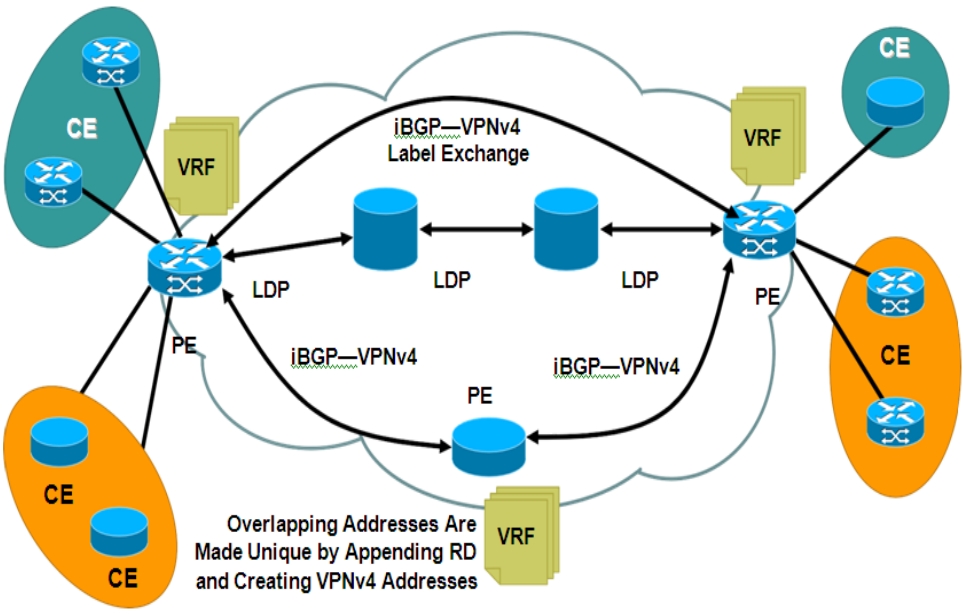


Figure 68: **MPLS VPN WORKING**

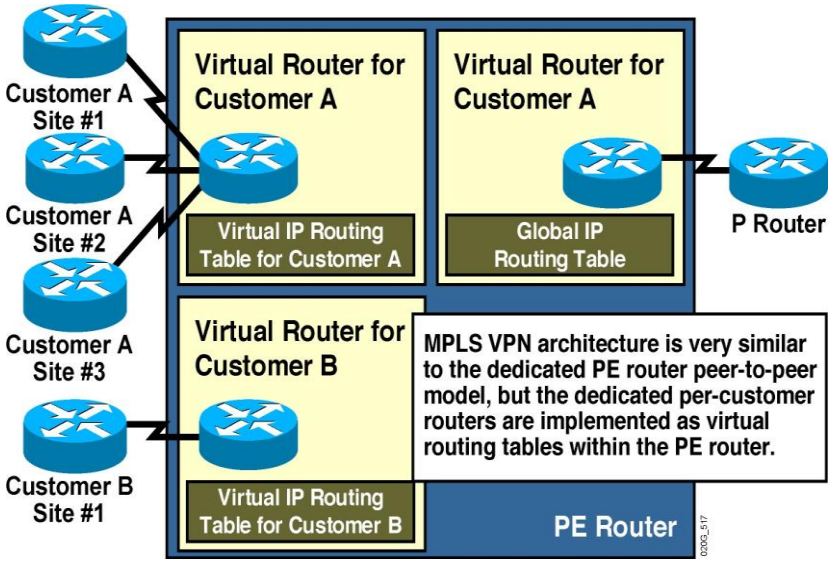
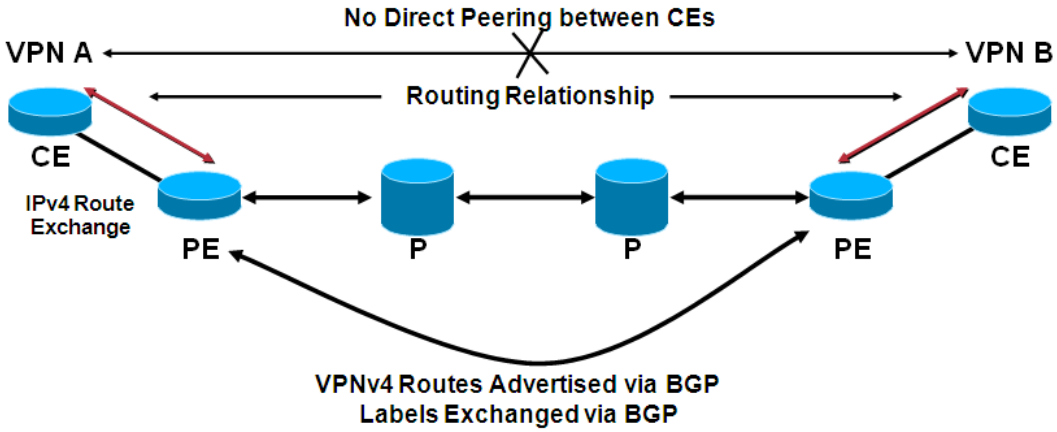


Figure 69: **MPLS LER Architecture:**

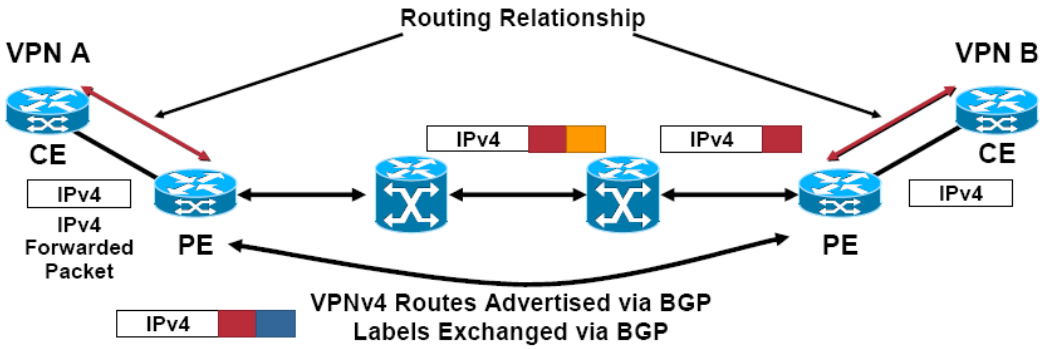
11.18.1 MPLS Control Plane Path:



- RD—8 Byte field—assigned by provider—significant to the provider network only
- VPNv4 Address: RD+VPN Prefix
- Unique RD per VPN makes the VPNv4 address unique

Figure 70: **MPLS CONTROL PATH**

11.18.2 MPLS Data Plane Path:



- **Ingress PE is imposing 2 labels**

Figure 71: **Ingress imposing in 2 labels**

11.19 ADVANTAGES OF MPLS VPNS OVER OTHER TECHNOLOGIES

BSNL's primary objectives in setting up the BGP/MPLS VPN network are:

1. Provide a diversified range of services (Layer 2, Layer 3 and Dial up VPNs) to meet the requirements of the entire spectrum of customers from Small and Medium to Large business enterprises and financial institutions.
2. Make the service very simple for customers to use even if they lack experience in IP routing.
3. Make the service very scalable and flexible to facilitate large-scale deployment.
4. Provide a reliable and amenable service.
5. Offering SLA to customers.
6. Capable of meeting a wide range of customer requirements, including security, quality of Service (QOS) and any-to-any connectivity.
7. Capable of offering fully managed services to customers.
8. Allow BSNL to introduce additional services such as bandwidth on demand etc over the same network.

11.20 CONCLUSION

MPLS was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients, which provide a data-gram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, Frame relay and Ethernet frames. The IP network has emerged as the network for providing converged, differentiated classed services to users with optimal use of resources and also to address the issues related to Class of service (CoS) and Quality of Service (QoS). MPLS is the technology that addresses all the issues in the most efficient manner. MPLS is a packet-forwarding technology that uses labels to make data forwarding decisions.

12 CONCEPT OF ONE NETWORK(CENTRALIZED NOC FOR CFA)

12.1 LEARNING OBJECTIVES

- Learn the concept and requirement of One Network
- Learn the activities involved in one network concept
- Implementation of one network program
- Learn about the network and partner team management

12.2 INTRODUCTION TO ONE NETWORK

The activities related to network management and customer management are being done currently at the exchange / equipment location level. Custer service management is generally done through indoor staff station at main exchange locations and outdoor takes care of last mile activities. The commercial activities related to partner (cluster, FTTH) management are being done in decentralized manner.

With the change in technology and management methodologies, it is very much desired that 24/7 network management is done through a centralized location for first level monitoring and corrective action required for the operational excellence. Wherever physical presence of staff is required for change of network card etc., there should be common staff at site to manage technical equipment, power plan, electrical infrastructure, etc.

One network program was started by BSNL on 16-12-2020

One network is Centralized NOC (Network operations center) for CFA (Consumer Fixed Assets)

12.3 ACTIVITIES IN ONE NETWORK

Following Activities are proposed for centralized network/customer/partner management.

(A) Network Management

- FTTH /OLT Management.
- OMCR- BTS Monitoring
- OF Route Patroller Monitoring

- NIB Network Elements Management (BNG/RPR/OCLAN/MNGPAN /Facebook Cache Server/Google Cache Server) Monitoring and Management

(B) Partner Management

A Centralized Group for Partner Support (CGPS) shall operate performing the following separate activities for the cluster / FTTH partners.

- Partner on boarding including all paper work for signing, creation of user id/login to various IT systems like FMS, DKYC, CDR systems, E-pay system, Wallet, etc.
- Monthly settlement of revenue share through ERP and Wallet.
- Exchange of all information related to sales and market activities.
- Common toll free number opened by ITPC is 18005991201 (created by Bangalore Telecom District for partner management activities) shall be mapped with the telephone number at respective BA level CGPS.

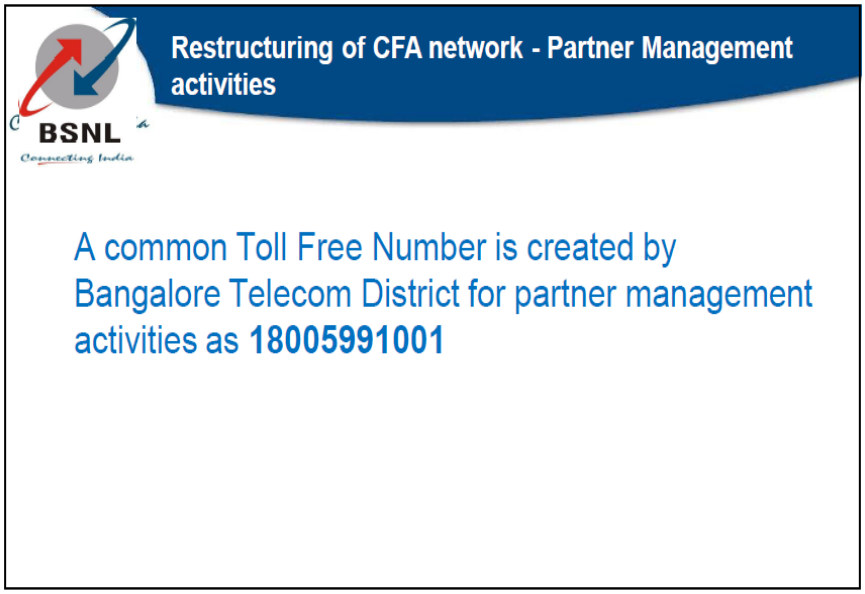


Figure 72: **Common Toll Free Number for partner management**

- A telephonic PIN (T-Pin) shall be issued to all partners so that call from the partners can be routed to the respective BA P-CSG.
- For this every BA will have its own 3-digit PIN and its corresponding destination number/ line hunting group.

12.4 NOC FOR ONE NETWORK

NOC of ONE Network has terminals of OMCRs, FTTH, NIB, eMS, Softswitch, ROT, CPAN, CDR, ERP extended for operations, monitoring and control. It is equipped with large LED screens for display of status and health of the network.

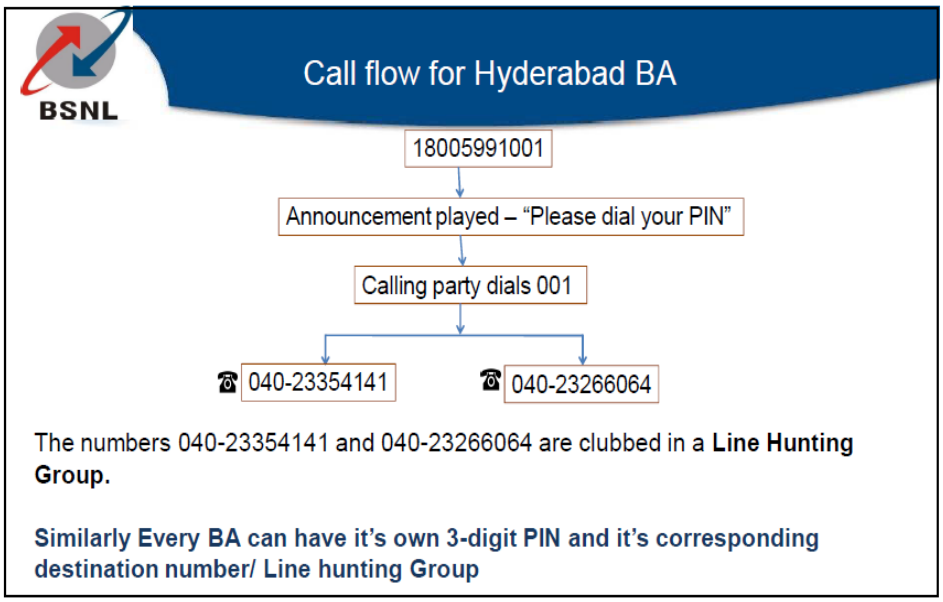


Figure 73: **Call flow for BA**

12.5 FTTH MANAGEMENT (BSNL OLT/TIP OLT/BBNL OLT)

- FTTH OLT Management (EMS)
- FTTH Soft Switch Management (Voice Creation)
- FTTH Lead Management.
- FTTH Fault Management.
- FTTH CAF Approval.
- CDR activities with respect to FTTH.
- FTTH TIP support.

12.6 OMCR ACTIVITIES

- BTS Monitoring (2G/3G/4G) and Reporting
- TRE/Combiner HW Reset

- Partial Fault Monitoring
- Attending calls from field persons
- BTS External Alarm Monitoring

12.7 OFC ROUTE PATROLLER MONITORING

- Patroller Monitoring and Reports.
- Updation of data for Patrollers and New OF route in Patroller Monitoring System.

12.8 MORE ACTIVITIES PROPOSED IN ONE NETWORK

- Transmission system monitoring and management
- NGN-LMGs/DSLAMs/OLTs/Exchange Monitoring and management
- NOFN – OLT/ONT monitoring and management
- PRI & SIP Monitoring and Management
- LEASED CIRCUIT & MLLN Monitoring and Management (DXC/V-MUX/Circuits)
- CDR/FMS SYSTEM management (Central Router/Exchange Router/MLLN Circuits)
- Wi-Fi Hotspots- monitoring & Management
- High Bandwidth Circuit Monitoring & management
- MPLS Monitoring (Edge Router/Core Router/Super Core Router/Circuits)

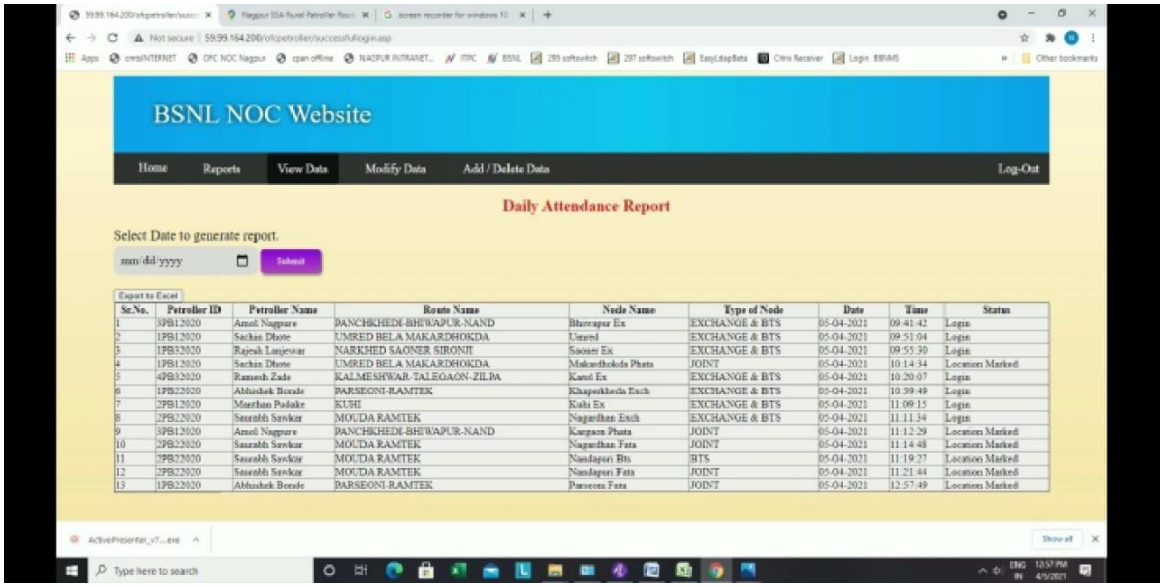


Figure 74: **BSNL NOC Website**

12.9 NETWORK MANAGEMENT BA TEAM

BA Team wise size required for centralized NOC activities and partner support group is to be prepared in following format

(A) Network Management Team Details

Name	Designation	Monitoring on network elements (FTTH/OLT/BNG etc.)	Mobile No.	E-mail ID

(B) Partner Management Team Details

Name	Designation	CLUSTER FTTH	Mobil No.	E-mail ID

12.1 ONE NETWORK BA TEAM CASE STUDY OF MAHARASHTRA CIRCLE

Sl. No.	Name of circle	Name of BA	BA Type	Members in the centralized NOC team for network management	Members in the CGPS for the cluster/FTTH partner
1	MH	Ahmednagar	Category-B	12	6
2	MH	Amaravati	Category-C	8	4
3	MH	Aurangabad	Category-C	8	4
4	MH	Chandrapur	Category-C	8	4
5	MH	Goa	Category-C	8	4

6	MH	Jalgaon	Category-C	8	4
7	MH	Kalyan	Category-B	12	6
8	MH	Kolhapur	Category-B	12	6
9	MH	Nagpur	Category-C	8	4
10	MH	Nandd	Category-C	8	4
11	MH	Nashik	Category-C	8	4
12	MH	Pune	Category-A	16	8
13	MH	Satara	Category-C	8	4
14	MH	Solapur	Category-C	8	4

12.10 CONCLUSION

As the name suggest one network program is a drive to monitor all the network components at a centralize location with 24x7 watch on the entire level and provide first level of escalation. With the growing number of subscribers and network elements to cater to such huge subscriber base, it is necessary to monitor the entire network for seamless services round the clock. One Network program is an initiative towards the NOC based approach.

13 ROUTER CONFIGURATION

13.1 LEARNING OBJECTIVES

The objective of this chapter is to familiarize participants about, the architecture of router, its interface, type of memory, forwarding mechanisms employed, its functions and its configuration.

13.2 INTRODUCTION

In today era of communication with the evolution of internet, the main expectation from communication devices is to provide global connectivity with a local presence. The networking devices such as routers play a very vital role in provision of such services. One can work in SOHO environment without routers but for medium and large sized organization/Units the routers presence is inevitable. The primary function of a packet switching network is to receive packets from a source and deliver them to the destination. To achieve this, a path or route through the network has to be determined. This requires a routing function/ algorithm to be implemented.

13.3 WHAT IS ROUTER?

A router is a device that forwards packets between networks. This forwarding is based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network.

Routing table information can be gathered automatically by routers using some standard type of routing protocols viz distance vector, link state or path vector protocols. Operator can call also enter network information in the routing table manually. Using this information, the router chooses the path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support

Traditionally routers were implemented in Software. Software implementation provided High degree of flexibility but the performance was limited because of the slow speed of processor.

13.4 FUNCTIONS OF ROUTER

- Interconnect communication links.
- Linking WANs and LANs
- Router routes packets as they travel from one network to another network.

- Path determination and packet switching
- Application of security rules (ACLs)
- Protocol conversion (encapsulation)
    - E.g. HDLC, PPP etc.

13.5 ROUTER OPERATION

- Accepts PDUs from incoming network.
- Examines PDU Header.
- Identify the paths available towards the destination with the help of routing table.
- Decide the best path based on different matrics.
- Passes PDU on to next node towards the destination.

13.5.1 Path Determination

- Router accepts packet and views inside Network Layer header
- IP address of destination carried in Network Layer header and other information.
- Destination IP address looked up in routing table
- Packet passed to appropriate exit interface

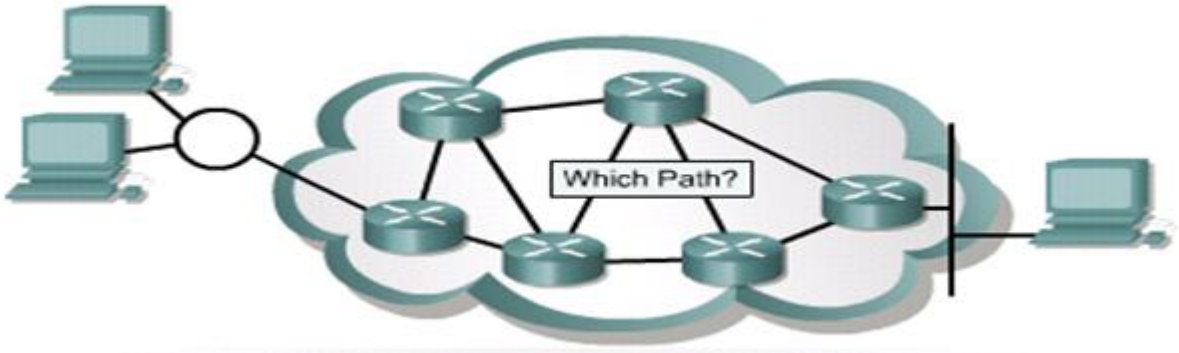


Figure 75: **Layer 3 functions to find the best path through the internetwork**

13.5.2 Transport Layer Determination

- Transport Layer header contents examined
- Source and destination port checked
- May trigger security of an Access Control List
- May drop packets under heavy load

13.5.3 Access Control List

- Used to identify incoming packets
- Can be used for security purposes
- E.g. do not allow TELNET traffic
    - Identified by destination port number 23
    - Found in Transport Layer header

13.6 ROUTER COMPONENTS AND THEIR FUNCTIONS

A router is a special type of computer. It has the same basic components as a standard desktop PC. It has a CPU, memory, a system bus, and various input/output interfaces.

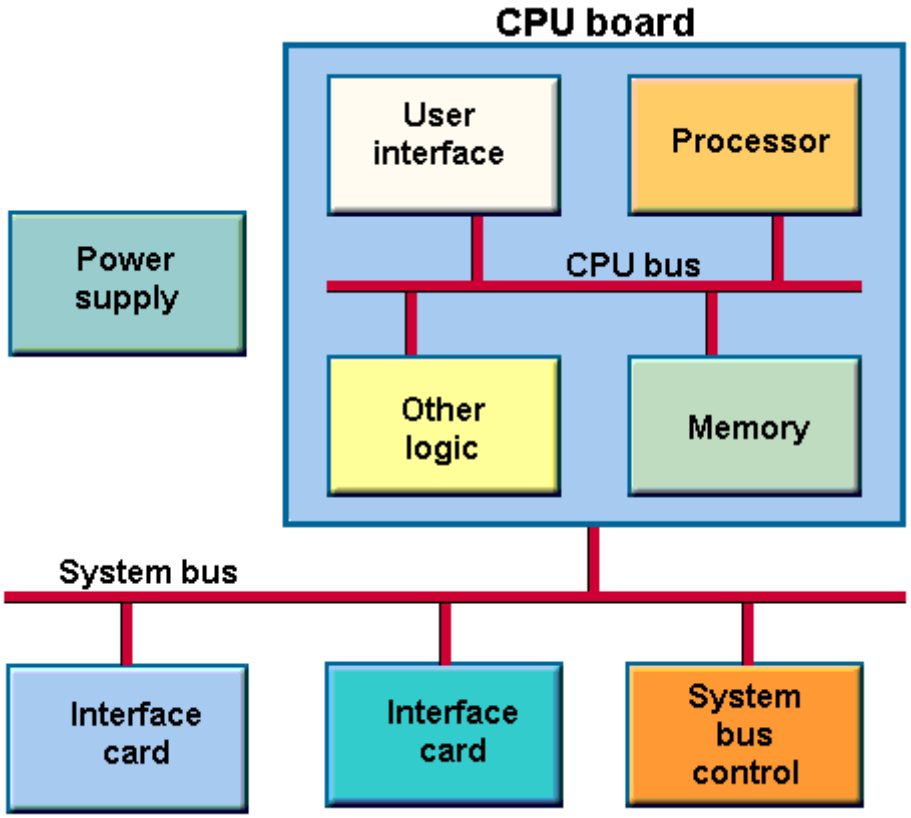


Figure 76: **Router components**

13.7 INTERNAL COMPONENTS OF A ROUTER

13.7.1 Boot ROM

It stores the mini IOS (Internet work Operating System) image (RX Boot) with extremely limited capabilities and POST routines and core level OS for maintenance.

- Maintains instructions for power-on self test (POST) diagnostics
- Starts and maintains the router
- Stores bootstrap program and basic operating system software
- Requires replacing pluggable chips on the motherboard for software upgrades

13.7.2 Flash

It is an EPROM chip that holds most of the IOS Image. It maintains everything when router is turned off.

- Holds the IOS image
- Allows software to be updated without removing and replacing chips on the processor

- Retains content when a router is powered down or restarted
- Can store multiple versions of IOS software
- Is a type of electrically erasable programmable read-only memory (EEPROM)

13.7.3 RAM

RAM holds running IOS configurations and provides caching. RAM is a volatile memory and loses its information when router is turned off. The configuration present in RAM is called Running configuration.

- Provides temporary memory for the configuration file of a router while the router is powered on.
- Stores routing tables
- Maintains packet-hold queues
- Loses content when a router is powered down or restarted

13.7.4 NVRAM

It is a re-writeable memory area that holds router's configuration file. NVRAM retains the information when ever router is rebooted. Once configuration is saved, it will be saved in NVRAM and this configuration is called Startup Configuration.

- Provides storage for the startup configuration file
- Retains content when a router is powered down or restarted

13.6 MEMORY ELEMETS OF A ROUTER

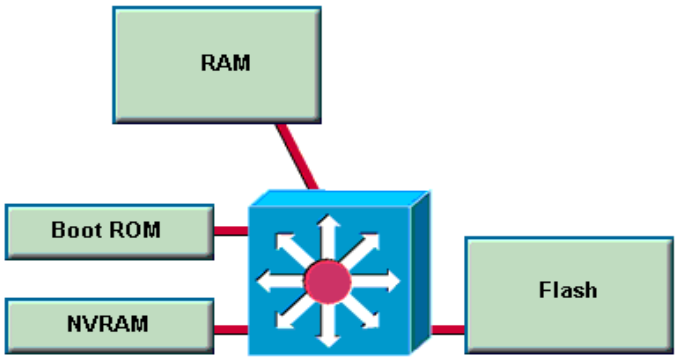


Figure 77: **memory elements of a router**

13.8 EXTERNAL COMPONENTS OF A ROUTER

13.8.1 Interfaces

- Connect routers to a network for packet entry and exit
- Can be on the motherboard or on a separate module

13.8.2 Type Of Interfaces

- The three basic types of connections on a router are
  - LAN interfaces,
  - WAN interfaces,

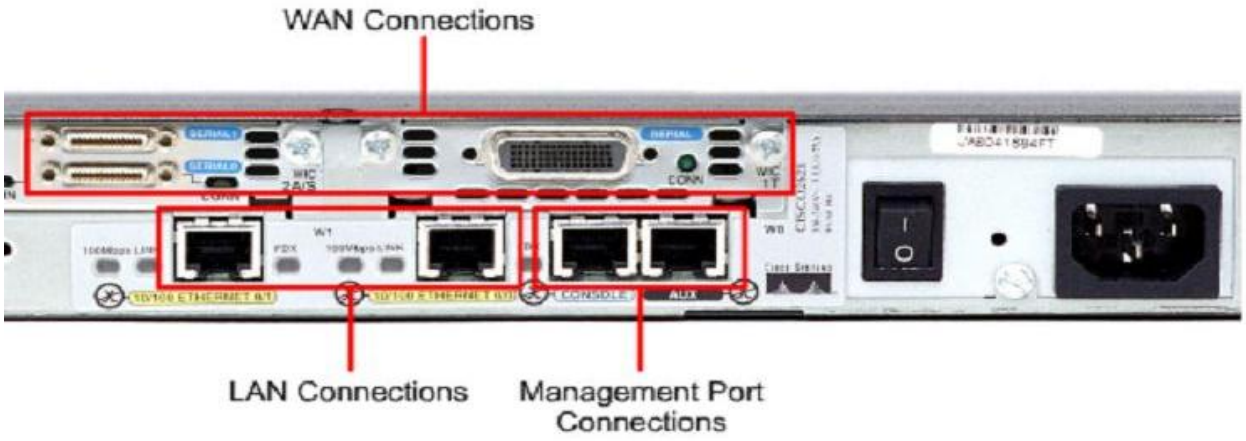


Figure 78: **Management ports**

- LAN interfaces allow the router to connect to the Local Area Network media.
- Wide Area Network connections provide connections through a service provider to a distant site or to the Internet.
- The management port provides a text-based connection for the configuration and troubleshooting of the router.
- The common management interfaces are the console and auxiliary ports.

13.9 ROUTE SWITCH PROCESSORS

A generic router model requires at least one Route Switch Processor (RSP), which can be procured in three ways: as part of an initial system, as a spare, or as an upgrade.

The RSP is the base system processor module for a router. The RSP contains the system CPU and system memory components. It maintains and executes the management functions that control the system.

Router's images reside in Flash memory, or on as many as two Flash memory cards. Storing IOS images in Flash memory allows you to download and boot from upgraded images remotely. This eliminates the need to remove and replace ROM devices for software updates.

13.10 POWER SUPPLIES

Most of the medium size and high end routers support dual power supplies. The optional additional power supply system provides dual load-sharing for protection against system interruption if one power supply system or one source of power fails.

Note Both dual power supplies must be AC-input or DC-input. The routers do not support mixed power supply types.

13.8 IMPORTANT SHOW COMMANDS

1. #show access-lists	List access lists
2. #show arp	Arp table
3. #show cdp	CDP information
4. #show clock	Display the system clock
5. #show controllers	Interface controllers status
6. #show crypto	Encryption module
7. #show debugging	State of each debugging option
8. #show dhcp	Dynamic Host Configuration Protocol status
9. #show flash:	display information about flash: file system
10. #show frame-relay	Frame-Relay information
11. #show history	Display the session command history
12. #show hosts	• IP domain-name, lookup style,

	name servers, and host table
13. #show interfaces	Interface status and configuration
14. #show ip	IP information
15. #show ospf	For OSPF debug only
16. #show ospfv3	For OSPFv3 debug only
17. #show processes	Active process statistics
18. #show protocols	Active network routing protocols
19. #show running-config	Current operating configuration
20. #show sessions	Information about Telnet connections
21. #show ssh	Status of SSH server connections
22. #show startup-config	Contents of startup configuration
23. #show tcp	Status of TCP connections
24. #show terminal	Display terminal configuration parameters
25. #show users	Display information about terminal lines
26. #show version	System hardware and software status

13.11 ROUTER BASIC CONFIGURATION

13.11.1 Management Port Connections

When the router is first put into service, there are no networking parameters configured. To prepare for initial startup and configuration, attach an RS-232 ASCII terminal, or a computer emulating an ASCII terminal, to the system console port. Then configuration commands can be entered to set up the router.

13.11.2 Console Port Connection

- The console port is a management port used to provide access to the router. It is used for the initial configuration of the router, monitoring, and disaster recovery procedures.
- To connect to the console port, a rollover cable and a RJ-45 to DB-9 adapter are used to connect a PC. Cisco supplies the necessary adapter to connect to the console port.
- The PC or terminal must support VT100 terminal emulation.
- Terminal emulation software such as HyperTerminal is usually used.

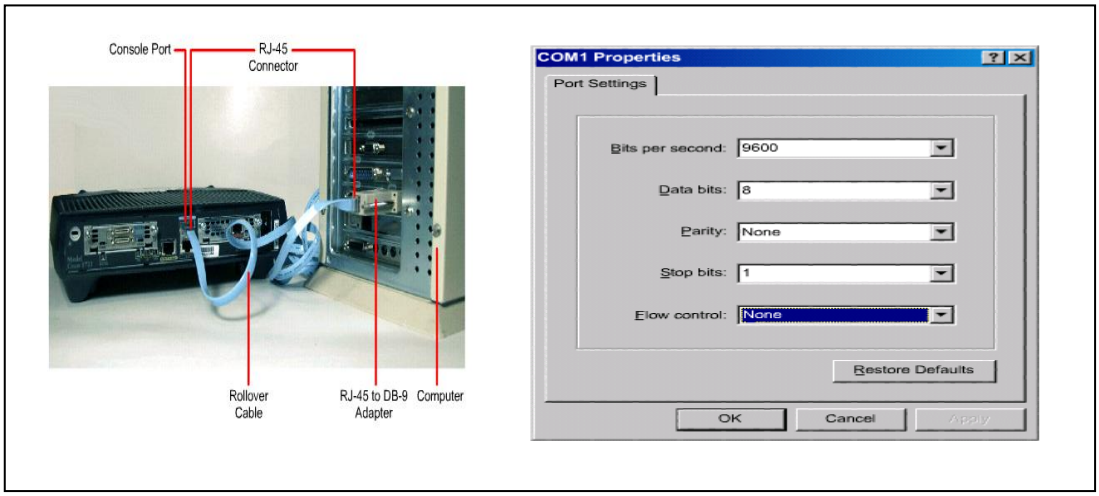


Figure 79: **Console port connection**

13.11.3 Auxiliary Port Connection

a. The router can also be configured from a **remote location** by dialing to a modem connected to the auxiliary port on the router.

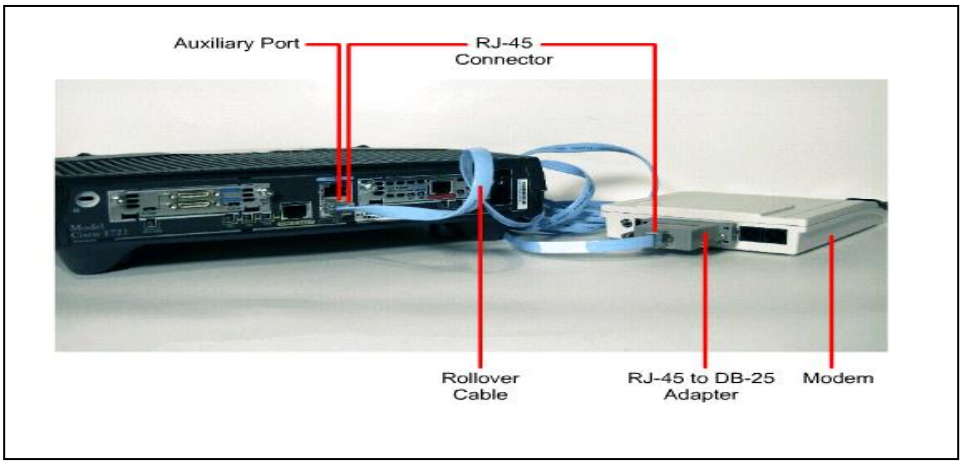


Figure 80: **Auxillary port connection**

13.12 ROUTER OPERATING SYSTEM

- A router or switch cannot function without an OS
- Router Operating system is known as Internetwork Operating System (IOS)
- Operating system stores in Flash memory (non-volatile)

13.13 OPERATION OF IOS SOFTWARE

The startup process of the router normally loads into RAM and executes one of 3 operating environments:

- ROM monitor: Performs the bootstrap process and provides low-level functionality and diagnostics. Used to recover from system failures and recover from a lost password. Available only through console.
- Boot ROM: limited subset of the Cisco IOS. Allows write operations to flash memory and is used primarily to replace the Cisco IOS image that is stored in flash ex: copy tftp flash
- Cisco IOS : Stored in Flash, but loaded and executed from RAM

13.14 INITIAL STARTUP OF CISCO ROUTERS

The startup routines done to start the router operations must accomplish the following:

- Make sure that the router hardware is tested and functional i.e. the CPU, memory, and interfaces
- Find and load the Cisco IOS softwa

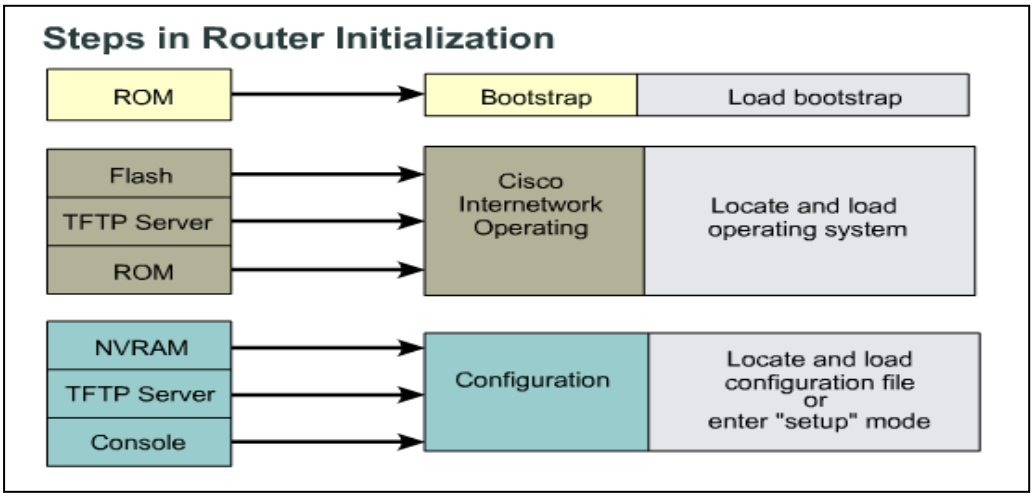


Figure 81: **steps in router operations**

13.15 ROUTER USER INTERFACE MODES

The IOS provides a command interpreter service known as the command executive (EXEC). The EXEC validates and executes the command

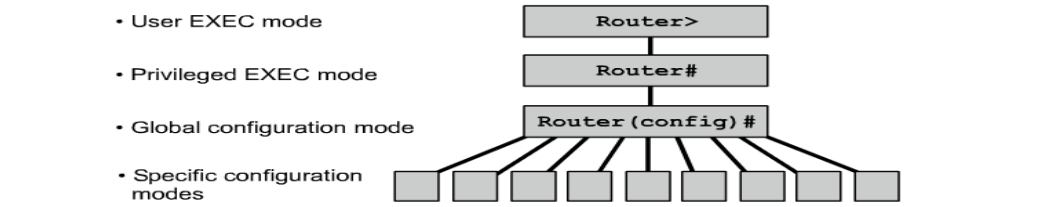
The EXEC session is separated in two 2 levels of access

User EXEC mode – allows the user to check the router status. No router configuration changes are allowed.

- > router

Privileged EXEC mode (Enable Mode) – allows the user to change the router configuration

- router#
- Enter the **enable** command at the ">" prompt
- Enter configuration and management commands



Configuration Mode	Prompt
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
IPX-router	Router(config-ipx-router)#
Route-map	Router(config-route-map)#

Figure 82: **Router interfaces**

13.16 ROUTER CONFIGURATION

13.16.1 Configuring A Router Name

Router#config t

Router(config)#hostname BSNL

BSNL(config)#

13.16.2 Backup And Restore

Copy Running-configuration File

Router#copy running-config tftp

Address or name of remote host [ ]? 10.10.10.2

Destination filename [Router-config]? RC

Writing running-config...!!

[OK - 497 bytes]

Router#copy tftp running-config

Address or name of remote host [ ]? 10.10.10.2

Source filename [ ]? RC

Destination filename [running-config]?

Accessing tftp://10.10.10.2/RC...

Loading RC from 10.10.10.2: !

[OK - 497 bytes

Router#show flash

System flash directory:

File Length Name/status

3 33591768 c2900-universalk9-mz.SPA.151-4.M4.bin

2 28282 sigdef-category.xml

1 227537 sigdef-default.xml

Router#copy flash tftp

Source filename []? c2900-universalk9-mz.SPA.151-4.M4.bin

Address or name of remote host []? 10.10.10.2

Destination filename [c2900-universalk9-mz.SPA.151-4.M4.bin]? 2911IOS

Router#copy tftp flash

Address or name of remote host []? 10.10.10.2

Source filename [ ]? 2911IOS

Destination filename [2911IOS]? c2800nm-advipservicesk9-mz.124-15.T1.bin

%Warning:There is a file already existing with this name

Do you want to over write? [confirm]y

Erase flash: before copying? [confirm]y

Erasing the flash filesystem will remove all files! Continue? [confirm]y

Erase of flash: complete

Accessing tftp://10.10.10.2/2911IOS...

Loading 2911 IOS from 10.10.10.2

13.17 ROUTING PRINCIPLES

The basic attributes of routing are as follows:-

- Correctness
- Simplicity
- Robustness
- Stability
- Fairness
- Optimality
- Efficiency

Robustness has to do with the routing of packets through alternate routes in the network in case of route failures or overloads

Stability is an important aspect of the routing algorithm. It implies that the routing algorithm must converge to equilibrium as quickly as possible, however some never converge, no matter how long they run.

Fairness and optimality are competing requirements. A trade-off exists between the two. Some performance criteria may give a higher priority to transportation of packets between adjacent/ nearby stations in comparison to those between distant stations. This results in higher throughput but is not fair to the stations which have to communicate with distant stations.

Efficiency of a routing technique/ algorithm gets decided by the quantum of overhead processing required. Of course these have to be kept to a minimum. Thus, Routing is essentially a method of path selection and is an overhead activity.

13.18 ROUTING & NETWORK LAYER ADDRESSES

Routers relay a packet from one data link to another. To relay a packet, a router employs two basic functions:

- a path determination function and
- a switching function.

Figure below illustrates how routers use the addressing for routing and switching functions. When a packet destined for network 100.1.0.0 arrives at Router 1, the router knows that the packet should be sent out on port S0.

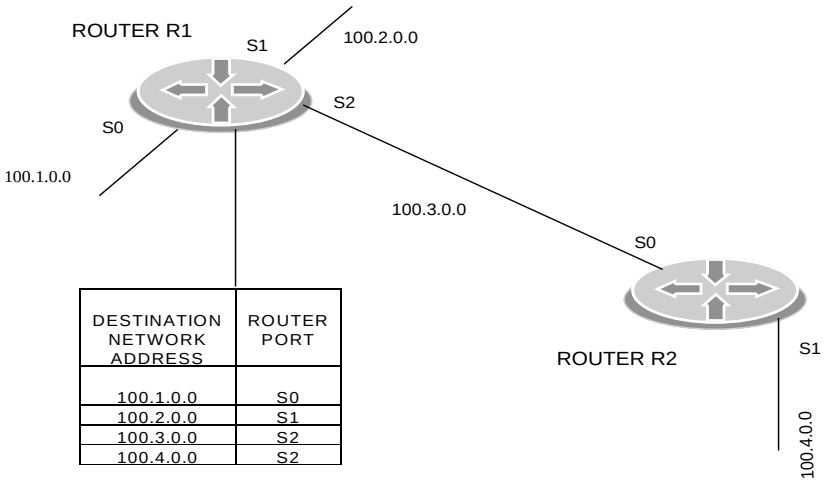


Figure 83: **routing and network layer address**

13.19 USE OF NETWORK LAYER ADDRESS IN ROUTING

From the router to the destination, a router is responsible only for passing the packet to the best network along the path. This best path is represented as a direction to a destination network. For example, in figure 2, if a packet that is destined for network 100.4.0.0 arrives at Router 1, the router knows that the best direction to send the packet out is interface S2. Router 2 is the next hop, or router, along the path. The router uses the network portion of the address to make these path selections.

The switching function enables a router to accept a packet on one interface and forward it on a second interface. The path determination function enables the router to select the most appropriate interface for forwarding a packet.

Routing assumes that addresses have been assigned to network elements to facilitate data delivery. In particular, routing assumes that addresses convey at least partial information about where a host is located. This permits routers to forward packets without having to rely either on broadcasting or a complete listing of all possible destinations. At the IP level, routing is used almost exclusively, primarily because the Internet was designed to construct large networks in which heavy broadcasting or huge routing tables are not feasible.

13.20 THREE GENERAL PREREQUISITES MUST BE MET TO PERFORM ROUTING

DESIGN: A plan must exist by which addresses are assigned. Typically, addresses are broken into fields corresponding to levels in a physical hierarchy. At each level of the hierarchy, only the corresponding field in the address is used, permitting addresses to be handled in blocks. In IP, the most common designs are IP Address Classes, Sub-netting, and CIDR.

IMPLEMENTATION : The design plan must be implemented in switching nodes, which must be able to extract path information from the addresses. Since router programming is generally not under a designer's control, designs must be limited by the features provided by manufacturers. Subnetting's great appeal lies in its great flexibility, while using a fairly simple implementation model.

ENFORCEMENT : The plan must be enforced in host addressing. A design is useless unless addresses are assigned in accordance with it. Addressing authority must be centralised.

In the Internet environment, routing is almost always used at the IP level, and bridging almost always used at the Data Link Layer.

For new network installations, the best approach is to plan for routing even if it's not used at first. This requires some advanced planning to design an addressing scheme that will

work. However, the overhead is all human - hardware won't know the difference between organised and haphazard addressing schemes. Network should be planned for the ability to put routers in strategic locations, even if those locations will initially use bridges or just signal boosters (such as Ethernet hubs and repeaters). In this manner, routers can be easily added later.

13.21 ROUTED PROTOCOL

A routed protocol is a protocol that contains sufficient network-layer addressing information for user traffic to be directed from one network to another network. Routed protocols define the format and use of the fields within a packet. Packets that use a routed protocol are conveyed from one end system to another end system through an internetwork.

The internet protocol IP and Novell's IPX are examples of routed protocols.

ROUTING PROTOCOL

A routing protocol provides mechanisms for sharing routing information. Routing protocol messages move between the routers. A routing protocol allows the routers to communicate with other routers to update and maintain routing tables. Routing protocol messages do not carry end-user traffic from network to network. A routing protocol uses the routed protocol to pass information between routers.

13.22 TYPES OF ROUTING: STATIC, DEFAULT, DYNAMIC

13.22.1 Static Routing:

Refers to routes to destinations being setup manually in the router. Network reachability in this case is not dependent on the existence and state of the network itself. Whether a destination is up or down, the static routes would remain in the routing table, and traffic would still be sent towards that destination. Static routing generally is not sufficient for large or complex networks because of the time required to define and maintain static route table entries.

13.22.2 Default Routing:

Refers to a "last resort" outlet – traffic to destinations that are unknown to the local router are sent to the default outlet router. Default routing is the easiest form of routing for a domain connected to a single exit point. A default route is a path on which a router should forward a packet if it does not have specific knowledge about the packet's destination. Figure below illustrates the concept of Static and default Routing.

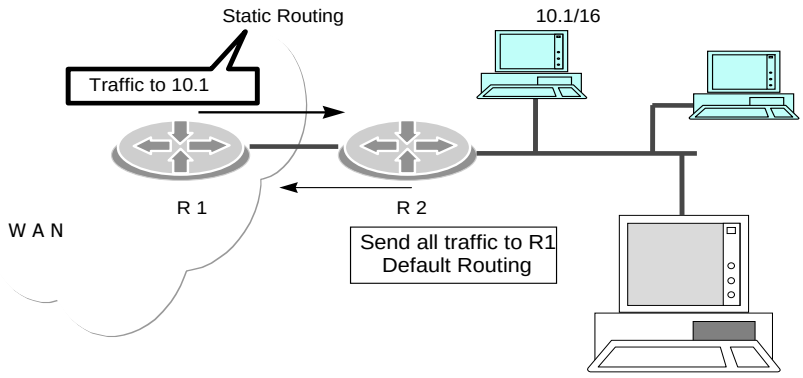


Figure 84: **Static routing**

Static and Default Routing

13.22.3 Dynamic Routing

Refers to routes being learnt via an internal or external routing protocol. Network reachability is dependent on the existence and state of the network. If a destination is down, the route would disappear from the routing table, and traffic will not be sent toward the destination. Dynamic routing is used to enable routers to build their routing tables automatically and make the appropriate forwarding decisions. This concept is illustrated in Figure below.

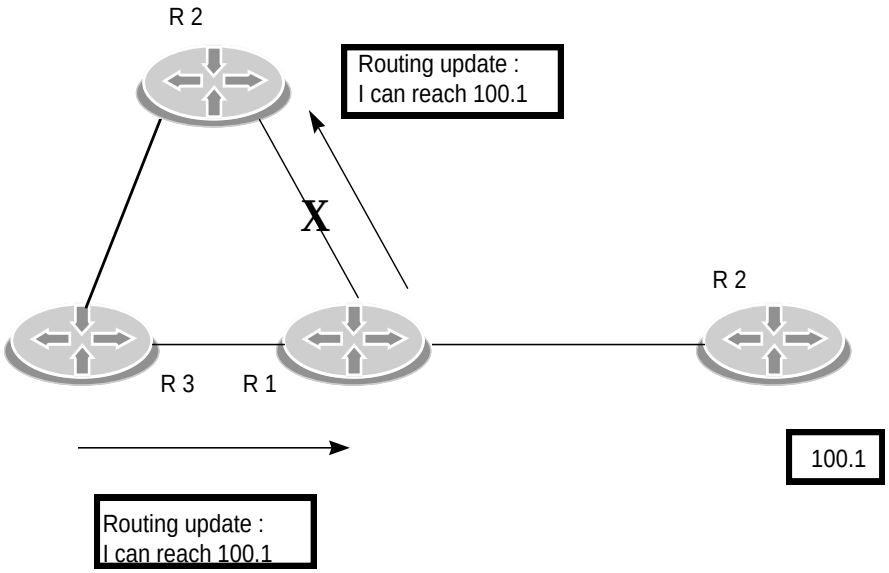


Figure 85: **Dynamic routing**

13.22.4 Dynamic Routing

Static and default routing is not our enemy. The most stable (but not so flexible) configurations are the ones based on static routing. Many people feel that they are not technologically up-to-date because they are not running dynamic routing. Trying to force dynamic routing on situations that do not really need it is just a waste of bandwidth, effort, and money.

As networks keep on growing in size, the routing tables also grow proportionately. Considerable amount of router memory is consumed by these ever increasing tables. In addition, the processor time is eaten up in scanning these tables and bandwidth is consumed in sending status reports about the updated routing tables. At a certain stage, the network size becomes so large that it becomes impossible to have every router keep an entry of every other router in the network. Ultimately, the routing has to be done **hierarchically**, similar to a telephone network.

13.23 ROUTING ALGORITHMS

Routing algorithms and protocols form the core of the hacker's Internet, because it is here that all the decisions get made. Network engineers assign costs to network paths, and routing protocols select the least-cost path to the destination.

Routing protocols bear a resemblance to capitalist market economics. In both systems, there is a large group of "nodes", the decisions of each being driven by a cost-minimisation algorithm. The end result is a reasonably efficient distribution of "resources". Furthermore, cost determination is done in similar ways. A router, like an import/export firm, will compute its cost, add on profit for its part in the transaction, and pass this cost along to customers. Both systems use this method to achieve reasonable efficiency.

Routing is the main process used by Internet hosts to deliver packets. Internet uses a hop-by-hop routing model, which means that each host or router that handles a packet examines the Destination Address in the IP header, computes the next hop that will bring the packet one step closer to its destination, and delivers the packet to the next hop, where the process is repeated.

To make this work, two things are needed:

First, routing tables match the destination addresses with next hops.

Second, routing protocols determine the contents of these tables.

Routing algorithms can be grouped into two major classes:

- Non-Adaptive or Static

- Adaptive or Dynamic

NON-ADAPTIVE ALGORITHMS do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use to get from I to J (for all I to J) is computed in advance, off-line, and downloaded to the routers when the network is booted. This procedure is also called as **Static Routing**.

ADAPTIVE ALGORITHMS change their routing decisions to take into account changes in the topology, and sometimes the traffic as well. Adaptive algorithms will be classified depending on

- where it gets the information from - whether locally, from adjacent Routers, or from all Routers
- When does the algorithm decide to change the routes - whether every ΔT sec, when the load changes, or when the topology changes, and what metric (parameter) is used for optimisation i.e. either distance, number of hops, or estimated transit time.

13.24 DYNAMIC ROUTING OPERATIONS

The success of dynamic routing depends on two basic router functions :

- Maintenance of a routing table
- Timely distribution of knowledge – in the form of routing updates – to other routers

Dynamic routing relies on a routing protocol to disseminate knowledge. A routing protocol defines the set of rules used by a router when it communicates with neighboring routers. Typically, a routing protocol describes:

- How updates are conveyed
- What knowledge is conveyed
- When to convey this knowledge
- How to locate recipients of the updates

13.25 REPRESENTING DISTANCE WITH METRICS

When a routing algorithm updates the routing table, its primary goal is to determine the best information to include in the table. Each routing algorithm will interpret “best” in its own way. The algorithm generates a number – called the metric- for each path through the network. Typically, the smaller the metric, the better is the path.

Metrics can be calculated based on a single characteristic of the path or by combining several key characteristics such as:

13.25.1 Hop Count

Refers to the number of routers a packet must go through, to reach a destination. The lower the hop count, the better is the path. Path length is used to indicate the sum of the hops to a destination.

13.25.2 Cost

Path cost is the sum of cost associated with each link to a destination. Costs are assigned (automatically or manually) to the process of crossing a network. Slower networks typically have a higher cost than faster networks. The lowest 'cost" route is the one believed to be the fastest route available.

13.25.3 Bandwidth

The rating of a link's throughput. Routing through links with greater bandwidth does not always provide the best routes. For example, if a high-speed link is busy, sending a packet through a slower link might be faster.

13.25.4 Delay

Depends on many factors, including the bandwidth of network links, the length of queues at each router in the path, network congestion on links, and the physical distance to be travelled. A conglomeration of variables that change with internetwork conditions, delay is common and useful metric.

13.25.5 Load

Dynamic factor that can be based on a variety of measures, including CPU and packet processed per second. Monitoring these parameters on a continual basis can be resource intensive.

Modern computer networks generally use dynamic routing algorithms rather than the static ones. Two dynamic algorithms in particular.

13.26 INTERIOR ROUTING

Interior routing occurs within an autonomous system. Most common interior routing protocols are **RIP and OSPF**. The basic routable element is the IP network or subnetwork, or CIDR prefix for newer protocols.

13.27 EXTERIOR ROUTING

Exterior routing occurs between autonomous systems, and is of concern to service providers and other large or complex networks. The basic routable element is the Autonomous System, a collection of CIDR prefixes identified by an Autonomous System number. While there may be many different interior routing schemes, a single exterior routing system manages the global Internet, based primarily on the **BGP-4 (Border Gateway Protocol Version 4)** exterior routing protocol.

13.28 INTERFACE CONFIGURATION OF ROUTER 0

Router>en

Router#conf t

Router(config)#int s0/0/0

Router(config-if)#ip address 172.16.16.2 255.255.255.252

Router(config-if)#no shut

Router(config-if)#

Router(config-if)#exit

Router(config)#int fa0/1

Router(config-if)#ip address 10.10.10.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#exit

Router#wr

13.29 INTERFACE CONFIGURATION OF ROUTER 1

Router>en

Router#conf t

Router(config)#int s0/0/0

Router(config-if)#ip address 172.16.16.1 255.255.255.252

Router(config-if)#no shut

Router(config-if)#

Router(config-if)#exit

Router(config)#int fa0/1

Router(config-if)#ip address 20.20.20.1 255.255.255.0

Router(config-if)#no shut

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 152.3.3.1 255.255.255.252

Router(config-if)#no shutdown

Router(config-if)#int loopback o

Router(config-if)#ip address 198.168.0.254 255.255.255.255

Router#end

Router#wr

13.30 INTERFACE CONFIGURATION OF ROUTER 2

Router>en

Router#conf t

Router(config)#int fa0/0

Router(config-if)#ip address 152.3.3.2 255.255.255.252

Router(config-if)#no shut

Router(config-if)#

Router(config-if)#exit

Router(config)#int fa0/1

Router(config-if)#ip address 30.30.30.1 255.255.255.0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#exit

Router#wr

13.31 STATIC ROUTING

13.31.1 Route To Be Entered For Router 0

Distance Network ID	Mask	Next HOP	Exit Interface
30.30.30.0	255.255.255.0	172.16.16.1	S0/0/0
152.3.3.0	255.255.255.252	172.16.16.1	S0/0/0
20.20.20.0	255.255.255.0	172.16.16.1	S0/0/0
198.168.0.254	255.255.255.255	172.16.16.1	S0/0/0

Router 0 (config)# ip route 30.30.30.0 255.255.255.0 172.16.16.1/s0/0/0

Router 0 (config)# ip route 152.3.3.0 255.255.255.252 172.16.16.1/s0/0/0

Router 0 (config)# ip route 20.20.20.0 255.255.255.0 172.16.16.1/s0/0/0

Router 0 (config)# ip route 198.168.0.254 255.255.255.255 172.16.16.1/s0/0/0

13.31.2 Route To Be Entered For Router 1

Distance Network ID	Mask	Next HOP	Exit Interface
10.10.10.0	255.255.255.0	172.16.16.2	fa0/0
30.30.30.0	255.255.255.0	152.3.3.2	S0/0/0

Router1 (config)#ip route 10.10.10.0 255.255.255.0 172.16.16.2 /fa0/0

Router1 (config)#ip route 30.30.30.0 255.255.255.0 152.3.3.2 /s0/0/0

13.31.3 Route To Be Entered For Router 2

Distance Network ID	Mask	Next HOP	Exit Interface
20.20.20.0	255.255.255.0	152.3.3.1	fa0/0
198.168.0.254	255.255.255.255	152.3.3.1	fa0/0
172.16.16.0	255.255.255.252	152.3.3.1	fa0/0
10.10.10.0	255.255.255.0	152.3.3.1	fa0/0

Router2(config)#ip route 20.20.20.0 255.255.255.0 152.3.3.1 /fa0/0

Router2(config)#ip route 198.168.0.254 255.255.255.255 152.3.3.1 /fa0/0

Router2(config)#ip route 172.16.16.0 255.255.255.252 152.3.3.1 /fa0/0

Router2(config)#ip route 10.10.10.0 255.255.255.0 152.3.3.1 /fa0/0

13.32 DEFAULT ROUTING

13.32.1 Route To Be Entered For Router 0

Distance Network ID	Mask	Next HOP	Exit Interface
0.0.0.0	0.0.0.0	172.16.16.1	S0/0/0

Router 0 (config)# ip route 0.0.0.0 0.0.0.0 172.16.16.1/s0/0/0

13.32.2 Route To Be Entered For Router 1

Distance Network ID	Mask	Next HOP	Exit Interface
10.10.10.0	255.255.255.0	172.16.16.2	fa0/0
30.30.30.0	255.255.255.0	152.3.3.2	S0/0/0

Router1 (config)#ip route 10.10.10.0 255.255.255.0 172.16.16.2 /fa0/0

Router1 (config)#ip route 30.30.30.0 255.255.255.0 152.3.3.2 /s0/0/0

13.32.3 Route To Be Entered For Router 2

Distance Network ID	Mask	Next HOP	Exit Interface
0.0.0.0	0.0.0.0.	152.3.3.1	fa0/0

Router2(config)#ip route 0.0.0.0 0.0.0.0. 152.3.3.1 /fa0/0

13.33 DYNAMIC ROUTING

13.33.1 Route To Be Entered For Router 0

Directly connected Network ID	172.16.16.0	10.10.10.0

Router0(config)#router rip

Router0 (config-router)#version 2

Router0 (config-router)#network 10.10.10.0

Router0 (config-router)#network 172.16.16.0

13.33.2 Route To Be Entered For Router 1

Directly connected Network ID	20.20.20.0	152.3.3.0	172.16.16.0	198.168.0.254

Router1(config)#router rip

Router1(config-router)#version 2

Router1(config-router)#network 20.20.20.0

Router1(config-router)#network 152.3.3.0

Router1(config-router)#network 172.16.16.0

Router1(config-router)#network 198.168.0.254

13.33.3 Route To Be Entered For Router 2

Directly connected Network ID	30.30.30.0	152.3.3.0

Router2(config)#router rip

Router2(config-router)#version 2

Router2(config-router)#network 30.30.30.0

Router2(config-router)#network 152.3.3.0

13.34 CONCLUSION

Knowing where and how to send data packet is the most important job of a router. Simple router does this and nothing more. Other routers add additional function including security features. The one constant is that the modern networks including internet could not exist without routers. Exterior routing occurs between autonomous systems, and is of concern to service providers and other large or complex networks. While there may be many different interior routing schemes, a single exterior routing system manages the global Internet, based primarily on the BGP-4 (Border Gateway Protocol Version 4) exterior routing protocol.

14 OPTICAL TRANSPORT NETWORK (OTN) TECHNOLOGY

14.1 LEARNING OBJECTIVES

After reading this unit, you should be able to understand:

- OTN Hierarchy.
- Multiplexing Structure of OTN
- Advantages of OTN
- OTN Interfaces and layer architecture of OTN

14.2 INTRODUCTION

With the growing demand for services and bandwidth, now telecom operators are trying to converge their networks in order to reduce Operational Expenses (OPEX), and also to eliminate additional Capital Expenditures (CAPEX) on multiple parallel networks. The amount of data traffic relative to voice traffic on optical networks and the total traffic volume keeps increasing.

These factors are the drivers behind emerging, flexible technologies to supplement the mature, voice optimized, SONET/SDH transport infrastructure and help manage network complexity. The aim of the optical transport network (OTN) is to combine the benefits of SONET/SDH technology with the bandwidth expandability of DWDM.

OTN (Optical Transport Network) provides a vehicle to enable convergence, and for providing a common and SONET/SDH-like operational model for network operations, administration, maintenance and provisioning (OAM&P) functionality, without altering the individual services. This newly developed OTN is specified in ITU-T G.709 Network Node Interface for the Optical Transport Network (OTN).

Since the 1980s, SONET/SDH is supporting a flexible and transparent mix of traffic protocols including IP, Fiber Channel, Ethernet and GFP by providing protection and performance monitoring. Whilst deployment of dense wavelength division multiplex (DWDM) networks during the following decade served to increase existing fiber bandwidth, it severely lacked the protection and management capabilities inherent in SONET/SDH technology.

The optical transport network (OTN) was created with the intention of combining the benefits of SONET/SDH technology with the bandwidth expansion capabilities offered by dense wavelength-division multiplexing (DWDM) technology.

14.3 WHAT IS OTN?

Networks employing OTN technology are designed and optimized to support current applications employing massive network capacity, and OTN is increasingly recognized as the transport standard of choice to meet the growing demand for network capacity.

The ITU Telecommunication Standardization Sector (ITU-T) defines OTN in a set of standards, with the G.709 specification acting as the core technology definition. The ITU-T standards cover the encapsulation format, multiplexing, switching, management, supervision, and survivability of optical channels carrying client payloads. OTN also provides the ability to measure network performance across multiple service providers' domains and to provide seamless, end-to-end monitored services.

An Optical Transport Network (OTN) is composed of a set of Optical Network Elements connected by optical fiber links, able to provide functionality of transport, multiplexing, routing, management, supervision and survivability of optical channels carrying client signals. A distinguishing characteristic of the OTN is its provision of transport for any digital signal independent of client-specific aspects, i.e. client independence.

ITU Standard G.709 is commonly called Optical Transport Network (OTN)– sometimes referred to as **digital wrapper (DW),** allows network operators to converge networks through seamless transport of the various types of legacy protocols while providing the flexibility required to support future client protocols.

OTN provides transport for all digital payloads with superior performance and support for the next generation of dynamic services with operational efficiencies not expected from current optical wavelength division multiplexing (WDM) transport solutions and support for a wide range of narrowband and broadband services like

- SDH/SONET
- IP based services
- Ethernet services
- ATM services
- Frame Relay services
- Audio/Video services etc.

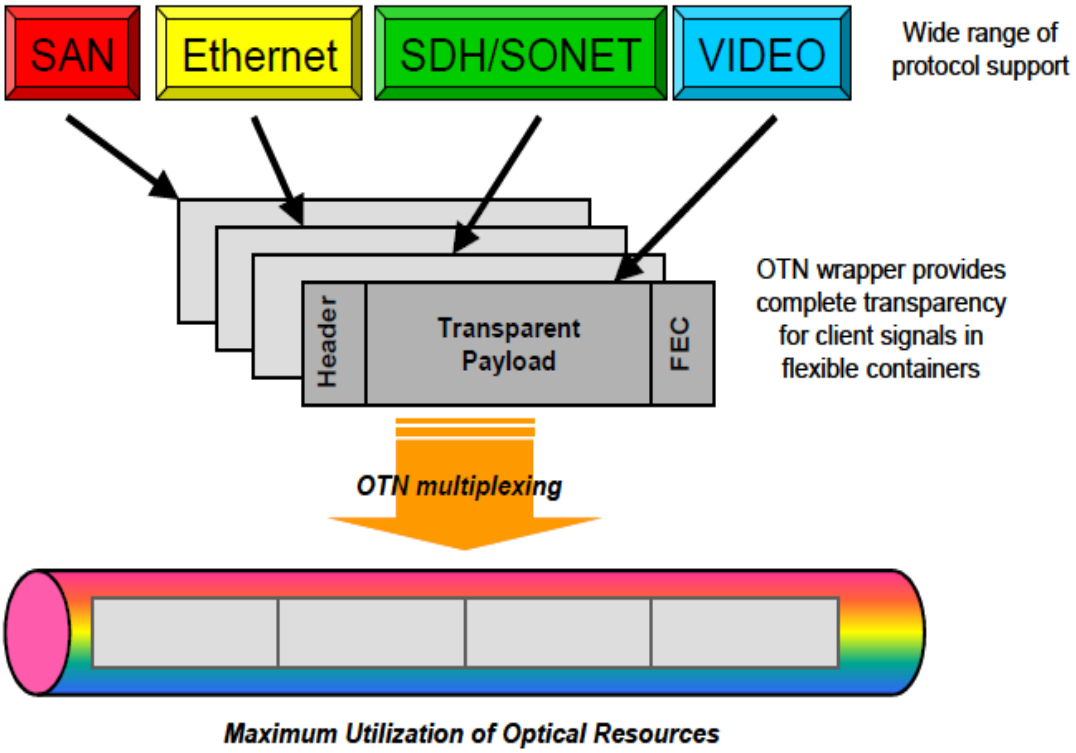


Figure 86: **Converged transport over OTN**

14.4 KEY ADVANTAGES OF OTN

Unlike SONET/SDH, OTN was designed to be an efficient transport layer for packet services such as Ethernet. At the same time, OTN is able to support the multiplexing of many different protocols including SONET/SDH, video, and storage protocols such as Fiber Channel.

OTN offers a number of advantages over legacy transport networks and the primary advantages of OTN include:

- **Reduction in transport costs:** By allowing multiple clients to be transported on a single wavelength, OTN provides an economical mechanism to fill optical network wavelengths.

- **Efficient use of optical spectrum:** OTN facilitates efficient use of DWDM capacity by ensuring fill rates are maintained across a network using OTN switches at fiber junctions.

- **Determinism:** OTN dedicates specific and configurable bandwidth to each service, group of services, or each network partition. This means that network capacity and managed performance (throughput, latency, jitter, and availability) are guaranteed for each client, and there is no contention between concurrent services or users.

- **Virtualize network operations:** The ability to partition an OTN-switched network into private network partitions, also referred to as Optical Virtual Private Networks (O-VPNs), provides a dedicated set of network resources to a client, independent of the rest of the network. Each network tenant sees only the resources associated with that tenant's private partition. Other resources associated with other tenants will not be visible. O-VPNs also ease network evolution because network upgrades can be tested or introduced in a protected network partition or 'sandbox,' without the risk of impacting day-to-day network operations in production partitions.

- **Flexibility:** OTN networks give operators the ability to employ the technologies needed now to support transport demands while enabling operators to adopt new technologies as business requirements dictate.

- **Secure by design:** OTN networks ensure a high level of privacy and security through hard partitioning of traffic onto dedicated circuits. This segregation of network traffic makes it difficult to intercept data transferred between nodes over OTN-channelized links. And because OTN-switched networks keep all applications and tenants separate, organizations can effectively stop hackers who access one part of the network from gaining access to other parts of the network.

- **Robust yet simple operations**: OTN network management data is carried on a separate channel completely isolated from user application data. This means OTN network settings are much more difficult to access and modify by gaining admittance through a client interface port.

- **Better Forward Error Correction**: OTN has increased the number of bytes reserved for Forward Error Correction (FEC), allowing a theoretical improvement

of the Signal-to-Noise Ratio (SNR) by 6.2 dB. This improvement can be used to enhance the optical systems in the following areas:

- Increase the reach of optical systems by increasing span length or increasing the number of spans.

- Increase the number of channels in the optical systems, as the required power theoretical has been lowered 6.2 dB, thus also reducing the non-linear effects, which are dependent on the total power in the system.

    - The increased power budget can ease the introduction of transparent optical network elements, which can't be introduced without a penalty. These elements include Optical Add-Drop Multiplexers (OADMs), Optical Cross Connects (OXCs), splitters, etc., which are fundamental for the evolution from point-to-point optical networks to meshed ones.

- **Tandem Connection Monitoring (TCM):** TCM enables the user and its signal carriers to monitor the quality of the traffic that is transported between segments or connections in the network.

14.5 OTN VS. SONET/SDH

Although OTN and SONET/SDH have similarities, there are also some significant design differences. Perhaps the biggest difference is that SONET/SDH was defined with fixed frame rates, while OTN was defined with fixed frame sizes.

Table 2. Comparison of SDH/SONET and OTN

OTN	**SONET/SDH**
Asynchronous mapping of payloads	Synchronous mapping of payloads
Timing distribution not required	Requires tight timing distribution across networks
Designed to operate on multiple	Designed to operate on multiple wavelengths

wavelengths (DWDM)	
Scales to 100 Gb/s (and beyond)	Scales to a maximum of 40 Gb/s
Performs single-stage multiplexing	Performs multi-stage multiplexing
Uses a variable frame size and increases the frame size as client size increases	Uses a fixed frame rate for a given line rate and increases frame size (or uses concatenation of multiple frames) as client size increases
FEC sized for error correction to correct 16 blocks per frame	Not applicable (no standardized FEC)

The G.709 standard defines client payload encapsulation, OAM overhead, FEC, and a multiplexing hierarchy. These functions deliver optical transport capabilities as robust and manageable as SONET/SDH, but with greater suitability for current traffic demands, and data center interconnection circuits in particular.

OTN is asynchronous and thus does not require the complex and costly timing distribution and verification of SONET/SDH. Instead, OTN includes per-service timing adjustments to carry both asynchronous (GbE, ESCON) and synchronous (OC-3/12/48, STM-1/4/16) services. OTN can additionally multiplex these services into a common wavelength.

Like SONET/SDH, OTN also offers comprehensive OAM, but with standardized FEC. OAM is used to efficiently manage network resources and services. FEC enables service providers to extend the distance between optical repeaters, reducing expenses and simplifying network operations.

14.6 OPTICAL TRANSPORT NETWORK (OTN) LAYERS

The optical transport hierarchy (OTH) is a new transport technology for optical transport networks developed by the ITU. It is based on the network architecture defined in various recommendations (e.g., G.872 on architecture; G.709 on frames and formats; and G.798 on functions and processes). OTH combines electrical and optical multiplexing under a common framework. The electrical domain is structured in a hierarchical order just like SONET/SDH, and the optical domain is based on DWDM multiplexing technology but with standardized interfaces and methods to manage the network. ITU-T recommendation G.872, Architecture for the Optical Transport Network (OTN), defines two classes of OTN interfaces:

- ***OTN inter-domain interface (IrDI)***: This interface connects the networks of two operators, or the subnetworks of one or multiple vendors in the same operator domain. The IrDI interface is defined with 3R (reshape, regenerate and retime) processing at each end. Since the IrDI is the interface for interworking, it was the focus of the initial standard development.

- ***OTN intra-domain interface (IaDI)***: This interface connects networks within one operator and vendor domain. Since the IaDI is typically between equipment of the same vendor, it can potentially have proprietary features added such as a more powerful FEC

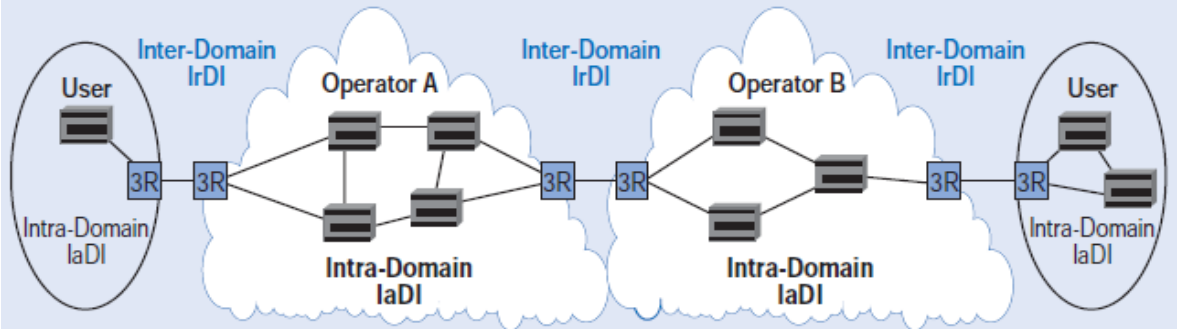


Figure 87: **: IrDI Vs IaDI**

The transport of a client signal in the OTN (shown in Figure i.e. Basic OTN Transport Structure) starts with the client signal (SONET/SDH, ATM, GFP, Ethernet etc.) being adapted at the optical channel payload unit (OPU) layer by adjusting the client signal rate to the OPU rate. The OPU overhead itself contains information to support the adaptation process of the client signal. Once adapted, the OPU is mapped into the optical channel data unit (ODU) with the necessary ODU overhead to ensure end-to-end supervision and tandem connection monitoring. Finally, the ODU is mapped into an OTU, which provides framing, as well as section monitoring and FEC.

Additional OH may be added to the OCh to enable the management of multiple colors in the OTN. The OMS and the OTS are then constructed. The result is an OCh comprising an OH section, a client signal, and a FEC segment.

The OCh OH, which offers the OTN management functionality, contains four substructures: the OPU, ODU, OTU, and frame alignment signal (FAS).

Each OPUk (k=0,1,2,2e,3,4,flex) is transported using an optical channel (OCh) assigned to a specific wavelength of the ITU grid. Several channels can be mapped into the OMS layer and then transported via the OTS layer. The OCh, OMS and OTS layers

each have their own overhead for management purposes at the optical level. The overhead of these optical layers is transported outside of the ITU grid in an out-of-band common optical supervisory channel (OSC). In addition, the OSC provides maintenance signals and management data at the different OTN layers.

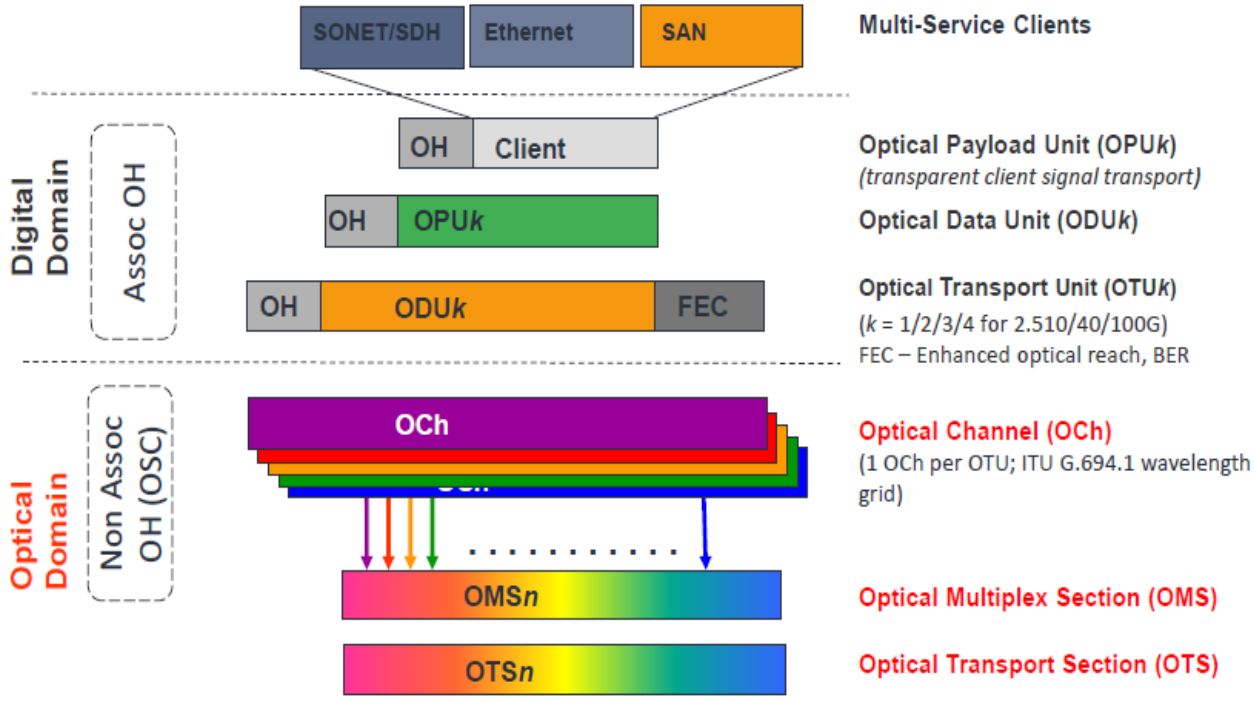


Figure 88: **Basic OTN Transport Structure**

14.7 OTN LAYER TERMINATION POINTS

The ITU G.872 recommendation also defines the optical network architecture based on the optical channel (OCh) carried over a specific wavelength. Different from that of legacy DWDM systems, the structure of this signal is standardized. The OTN architecture is composed of three layers, shown in Figure - OTN Layer Termination Points, and constructed using the OCh with additional overheads.

- **Optical Channel (OCh)** – represents an end-to-end optical network connection with the encapsulated client signal in the G.709 frame structure.
- **Optical Multiplex Section (OMS)** – refers to sections between optical multiplexers and demultiplexers.
- **Optical Transmission Section (OTS)** – refers to sections between any network elements in the OTN, including amplifiers.

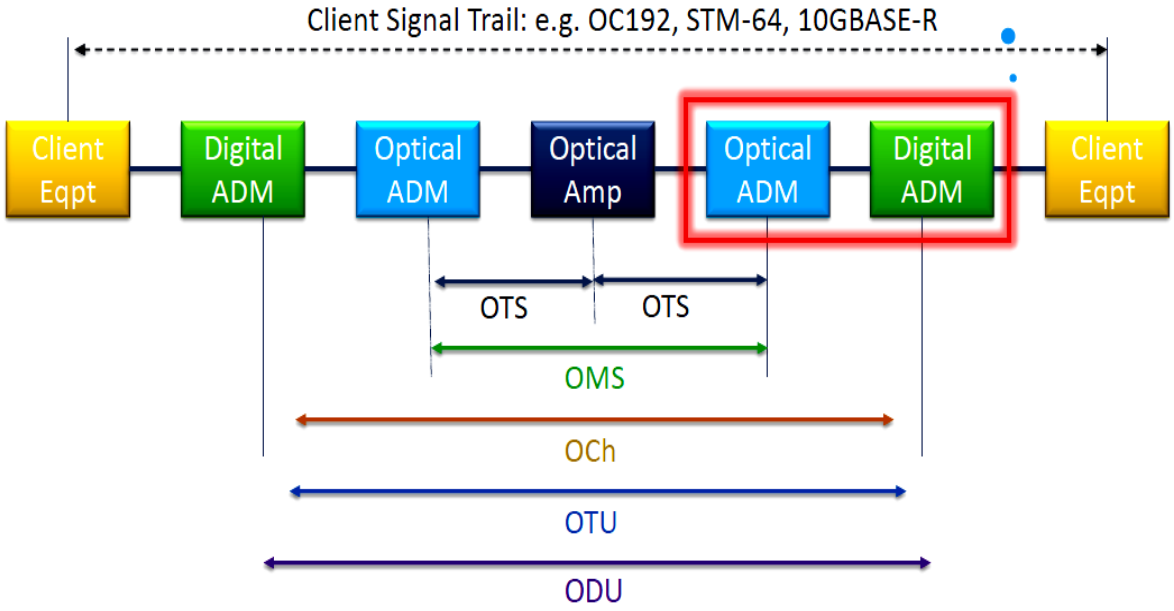


Figure 89: **OTN Layer Termination Points**

The termination of the OTS, OMS and OCh layers is performed at the optical level of the OTN. The OCh payload consists of an electrical substructure, where the optical channel transport unit (OTU) is the highest multiplexing level. This layer is the digital layer — also known as the "digital wrapper" - which offers specific overhead to manage the OTN's digital functions. The OTU also introduces a new dimension to optical networking by adding forward error correction (FEC) to the network elements, allowing operators to limit the number of required regenerators used in the network and in turn reduce cost.

14.8 STANDARD OTN LINE RATES

G.709 defines standard interfaces and rates. OTN rates are equal to or higher than the bit rates of the client traffic. Typical client signals and corresponding to G.709 rates are listed in the Table.

Table 3. OTN Rates

Client Signal Type	**Client Signal**	**OTN Line Signal (G.709)**	**OTUk Line Rate (kbit/s)**[	**OPUk Payload Rate (kbit/s)**	**OTUk frame period (µs)**	**OTUk frequency accuracy (ppm)**
SONET/SDH	STS-48/STM-16	OTU1	2,666,057	2,488,320	48.971	± 20
SONET/SDH	STS-192/STM-64	OTU2	10,709,225	10,037,629	12.191	± 20

Ethernet/Fibre Channel	10GBASE-R/10GFC	OTU2e	11,095,727	10,356,012	11.766	±100
SONET/SDH/Ethernet	STS-768/STM-256/ Transcoded 40GBASE-R	OTU3	43,018,413	40,150,519	3.034	±20
Ethernet	Up to 4 10GBASE-R	OTU3e2	44,583,355	41,611,131	2.928	±20
Ethernet	100GBASE-R	OTU4	111,809,973	100,376,298	1.167	±20
ODUflex signals are transported over ODU2, ODU3, ODU4						±100

Note: ODU0 signals are to be transported over ODU1, ODU2, ODU3, ODU4 or ODUCn signals, ODU2e signals are to be transported over ODU3, ODU4 and ODUCn signals and ODUflex signals are transported over ODU2, ODU3, ODU4 and ODUCn signals

Unlike SDH/SONET, the line rate is increased by maintaining the G.709 frame structure (4 rows x 4080 columns) and decreasing the frame period (in SDH/SONET the frame structure is increased and the frame period of 125 µs is maintained).

14.9 OTN FRAME STRUCTURE

There are three overhead areas in an OTN frame: the Optical Payload Unit (OPU) overhead, the Optical Data Unit (ODU) overhead, and the Optical Transport Unit (OTU) overhead. These overhead bytes provide path and section performance monitoring, alarm indication, communication, and protection switching capabilities. One additional feature is the inclusion of a Forward Error Correction (FEC) function for each frame. The FEC improves the Optical Signal-to-Noise Ratio (OSNR) by 4 to 6 dB, resulting in longer spans and fewer regeneration requirements.

Figure illustrates the three parts that constitute the G.709 OTN frame; **namely the overhead, the payload, and the FEC**.

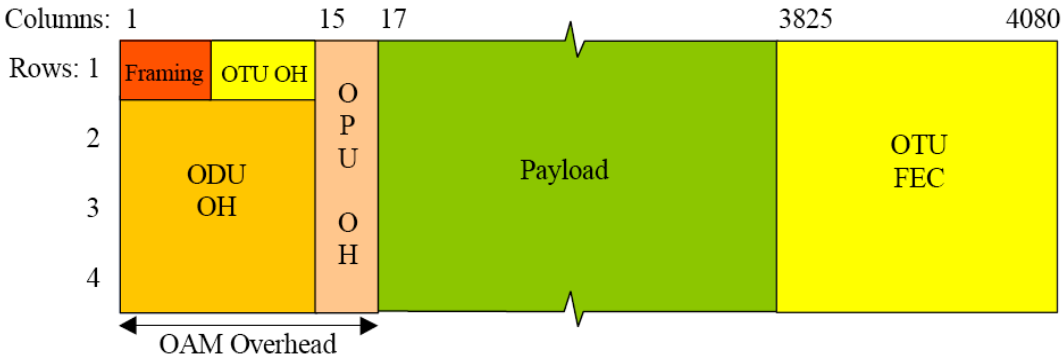


Figure 90: **OTN Frame**

Although OTN and SONET/SDH have similarities but the biggest difference in respect of frame structure is that SONET/SDH was defined with fixed frame rates, while OTN was defined with fixed frame sizes.Perhaps the biggest difference is that SONET/SDH was defined with fixed frame rates, while OTN was defined with fixed frame sizes.

14.10 OPTICAL TRANSPORT NETWORK EQUIPMENT

There are several different types of optical transport network equipment being deployed based on the OTN standards. The most common types include:

- Regenerators,
- OTN terminal equipment
- Optical Add/Drop Multiplexer (OADMs),
- Optical cross connect (OXCs).

OTN terminal equipment is used for point-to-point connections through WDM networks, mapping the client signals into OPUs, sometimes multiplexing multiple signals in the electrical domain, and finally performing mapping/multiplexing in the optical domain. OADMs, OXCs, and some types of regenerators primarily process the OTN signals in optical domain.

14.11 CONCLUSION

OTN-based backbones and metro cores offer significant advantages over traditional WDM transponder-based networks, including increased efficiency, reliability, and wavelength–based private services. The IP-over-OTN infrastructure also offers better management and monitoring, reduced hops, increased protection of services, and reduced costs for equipment acquisition. In addition to scaling the network to 100G and beyond,

OTN plays a key role in making the network an open and programmable platform, enabling transport to become as important as computing and storage in intelligent data center networking.

15 CPAN TECHNOLOGY

15.1 LEARNING OBJECTIVES

After reading this unit, you should be able to understand:

•Limitation of circuit switched network signals.

•CPAN Technology.

•Network Architecture of CPAN.

15.2 INTRODUCTION

The purpose of a transport network is to provide a reliable aggregation and transport infrastructure for any client traffic type. With the growth of packet-based services, operators are transforming their network infrastructures while looking at reducing capital and operational expenditures. In this context, a new technology is emerging: a transport profile of Multi-Protocol Label Switching called MPLS-TP.

Transport network requirements of BSNL in the present scenario requires packet transportation, as all the new network elements are generating IP Traffic which is to be reliably transported. Based on this requirement, Packet Transport Network Planning guidelines have been prepared which outlines the basic concepts, technology & network architecture for the future transport network of BSNL. The network basically comprises of MPLS-TP based nodes.

- In BSNL transport network was designed and deployed to carry basically TDM traffic comprising of Els, STM-1s & STM-16s. The network elements such as Switches, BTSs, BSCs& MSCs etc utilized TDM interfaces for transportation of information from one place to the other as part of service delivery. With the introduction of Broadband for which large number of DSLAMs were installed for high speed Broadband delivery, transport of Ethernet traffic was also introduced in BSNL network, through RPR Switches deployed in metro districts.

- To carry TDM traffic efficiently & reliably SDH network comprising of STM-1 CPE, STM-1 ADM, STM-4, STM-16 ADM, STM-16 MADM and STM-64 has been extensively deployed which carried all type of TDM traffic. For long distance transport, linear DWDM systems (2.5G& 10G) were deployed which carried mostly SDH traffic through its lambdas (STM-1, STM-4, STM-16). During 2009 Digital Cross Connect (DXCs) were also introduced in BSNL network with granularity of STM-1 Cross Connect along with aggregation and

ASON capability. Thus SDH, DXC and DWDM is presently the backbone of the transport network of BSNL.

- From 2006 onwards, with the advent of Ethernet over SDH (EoSDH) all SDH,DWDM& DXC Equipment procured by BSNL had the capability of transporting Ethernet traffic over SDH frame through Generic Framing Protocol (GFP) and Virtual Concatenation. This technology enabled BSNL to adapt to the transition phase in the technological development curve where the network elements were progressively switching towards Ethernet Interfaces (FE, GE) but continued to support TDM interfaces too. Further with deployment of large numbers of RPR Switches and OCLAN Switches with Broadband network the requirement of Ethernet transport through traditional TDM transport backbone was minimal.Even the routers of MPLS network (P&PE) had substantial TDM interfaces to enable the transportation of traffic in secure reliable media, utilizing BSNL's traditional TDM transport backbone.

- But the situation depicted above is rapidly changing with 100% network elements being deployed by Mobile, Broadband and NGN for fixed access supporting only Ethernet interfaces for interconnection. Thus the volume of transport requirement for Ethernet Interfaces has exponentially increased while the requirement of TDM transport is rapidly vanishing. The network transportation requirement has clearly shifted from TDM with a smaller portion of Packet to almost l00% Packet transport. As we move in the era of Packet transport, utilizing TDM networks for the same becomes inefficient and costly. Moreover, the packet network gives support to different class of services, aggregation and dynamic statistical multiplexing etc. in the transport layer for efficient delivery of services.

15.3 WHAT IS PACKET TRANSPORT NETWORK?

Attributes required for Ethernet transport.

Attributes	**Packet network**	**Transport network**	**Packet transport network**
Connection mode	Connectionless	Connection oriented	Connection oriented
OAM/Operation & maintenance	Out of band	In band	In band
Protection switching	Control plane depend	Data plane switching	Data plane switching

BW efficiency	Statistical multiplexing	Fixed bandwidth	Statistical multiplexing
Data rate granularity	Flexible	Rigid SDH hierarchy	Flexible
QoS	QoS differentiation	Single class	QoS differentiation

Table 4. Packet Transport->Packet efficiency + Transport grade

15.4 MPLS-TP

The goal of MPLS-TP is to provide connection-oriented transport for packet and TDM services over optical networks leveraging the widely deployed MPLS technology. Key to this effort is the definition and implementation of OAM and resiliency features to ensure the capabilities needed for carrier-grade transport networks – scalable operations, high availability, performance monitoring and multi-domain support.

Objective of MPLS-TP is:

- To enable MPLS to be deployed in a transport network and operated in a similar manner to existing transport technologies (SDH/SONET/OTN)
- To enable MPLS to support packet transport services with a similar degree of predictability, reliability, and OAM to that found in existing transport networks

Current transport networks (e.g. SONET/SDH) are typically operated from a network operation center (NOC) using a centralized network management system (NMS) that communicates with the network elements (NEs) in the field via the telecommunications management network (TMN). The NMS provides well-known FCAPS management functions which are: fault, configuration, accounting, performance, and security management. Together with survivability functions such as protection and restoration, availability figures of >99,999% have been achieved thanks to the highly sophisticated OAM functions that are existing e.g. in SONET/SDH transport networks. This well proven network management paradigm has been taken as basis for the development of the new MPLS-TP packet transport network technology.

Moreover, MPLS-TP provides dynamic provisioning of MPLS-TP transport paths via a control plane. The control plane is mainly used to provide restoration functions for improved network survivability in the presence of failures and it facilitates end-to-end path provisioning across network or operator domains. The operator has the choice to

enable the control plane or to operate the network in a traditional way without control plane by means of an NMS. It shall be noted that the control plane does not make the NMS obsolete – the NMS needs to configure the control plane and also needs to interact with the control plane for connection management purposes.

One of the major motivations for developing MPLS-TP was the need for the circuits in Packet Transport Networks. Traditionally packet transport switches each packet independently. However with connection oriented transport a 'connection' is first setup between the end points and then all the traffic for that connection follows only that path through the network. This makes the Packet Transport Network very similar to the TDM networks and simplifies management and migration of the transport network.

The concept of Label Switched Paths or LSPs from MPLS technology is already tried and tested and successful in the internetworking world. It made sense to adapt it for use in Packet Transport Networks. However there was a need to simplify the working of MPLS to make it more suitable for use in the Packet Transport World.

With this in mind, some features were removed from the traditional MPLS, since it was felt that thesewere not needed in Transport World and would simply the network. The features from MPLS that arenot supported by MPLS-TP are:

a) MPLS Control Plane: MPLS-TP does not require LDP or any other control plane protocol toset up the circuits. Instead a user provisioned model is followed. The user can provision acircuit from a centralized Network Management System in a way similar to TDM networks.

b) Penultimate Hop Popping (PHP) : PHP is used by MPLS Edge Routers to reduce the load oftwo label lookups. However this causes problems with QoS and was disabled in MPLS-TP

c) LSP Merge: Merging two LSPs (going to the same destination) reduces the number of labelsbeing used in the network. However it makes it impossible to differentiate between trafficcommon from two different sources before the merging happened. To simplify things intransport networks, LSP merge was also disabled.

d) Equal Cost Multi Path: In traditional IP/MPLS networks different packets between a source-destinationpair can take different paths. This is especially true when multiple equal costpaths exist. However this is in conflict with the concept of a circuit where all the traffic shouldfollow the same path. Hence ECMP is disabled.

15.5 DIFFERENCES BETWEEN MPLS AND MPLS-TP

When it comes to the major differences between MPLS and MPLS-TP, here's what you need to know.

- **Bidirectional Label Switched Paths (LSPs).** MPLS is based on the traditional IP routing paradigm -- traffic from A to B can flow over different paths than traffic from B to A. But transport networks commonly use bidirectional circuits, and MPLS-TP also mandates the support of bidirectional LSPs (a path through an MPLS network). In addition, MPLS-TP must support point-to-multipoint paths.

- **Management plane LSP setup.** Paths across MPLS networks are set up with control-plane protocols (IP routing protocols or Resource Reservation Protocol (RSVP) for MPLS Traffic Engineering (MPLS-TE). MPLS-TP could use the same path setup mechanisms as MPLS (control plane-based LSP setup) or the traditional transport network approach where the paths are configured from the central network management system (management plane LSP setup).

- **Control plane is not mandatory.** Going a step farther, MPLS-TP nodes should be able to work with no control plane, with paths across the network computed solely by the network management system and downloaded into the network elements.

- **Out-of-band management.** MPLS nodes usually use in-band management or at least in-band exchange of control-plane messages. MPLS-TP network elements have to support out-of-band management over a dedicated management network (similar to the way some transport networks are managed today).

- **Total separation of management/control and data plane.** Data forwarding within an MPLS-TP network element must continue even if its management or control plane fails. High-end routers provide similar functionality with non-stop forwarding, but this kind of functionality was never mandatory in traditional MPLS.

- **No IP in the forwarding plane.** MPLS nodes usually run IP on all interfaces because they have to support the in-band exchange of control-plane messages. MPLS-TP network elements must be able to run without IP in the forwarding plane.

- **Explicit support of ring topologies.** Many transport networks use ring topologies to reduce complexity. MPLS-TP thus includes mandatory support for numerous ring-specific mechanisms.

15.6 MPLS AND MPLS-TP COMPONENTS

As mentioned previously, MPLS refers to a suite of protocols, and MPLS-TP refers to a set of compatible enhancements to the MPLS protocol suite. These protocols and new enhancements can be separated into the following categories:

- Network Architecture—Covers the definition of various functions and the interactions among them.
- Data Plane-Covers the protocols and mechanisms that are used to forward the data packets. This can further be divided into the following subcategories:
    - Framing, forwarding, encapsulation
    - OAM
    - Resiliency (protection and restoration)
- Control Plane—Covers the protocols and mechanisms used to set up the label-switched paths (LSPs) that are used to forward the data packets.
- Management Plane—Covers the protocols and mechanisms that are used to manage the network.

A list of protocols and mechanisms in each of these categories is provided in the Figure. The figure also highlights the set of enhancements that are being pursued by MPLS-TP. The protocol and mechanisms highlighted in blue are being added to the MPLS/GMPLS protocol suite as part of the MPLS-TP effort. In Figure, the protocols and mechanisms highlighted in red might not be needed for the transport networks and are, therefore, being made optional. Note that these mechanisms will remain as part of the MPLS/GMPLS protocol suite. It is IETF's guidance to vendors that these mechanisms do not need to be supported on the platforms that are being targeted towards transport networks.

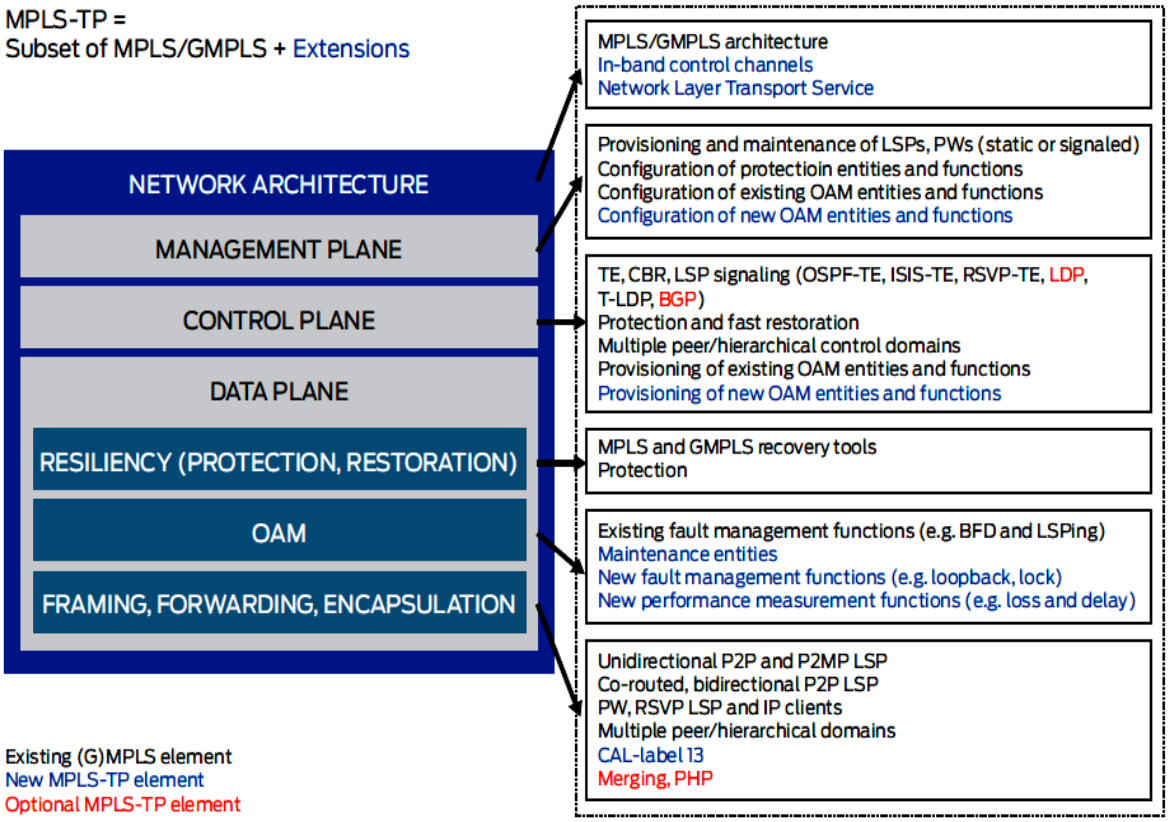


Figure 91: **Components of MPLS and MPLS-TP**

15.7 APPLICABILITY AND DEPLOYMENT OPTIONS FOR CPAN

MPLS-TP enhancements are primarily applicable to the access and aggregation networks, where the majority of the migration from circuit-switched networks to packet-based networks is currently occurring, and where higher scale and lower cost is required. Juniper believes that the OAM enhancements to the MPLS protocol suite, however, will be extremely valuable to all MPLS networks, especially in the MPLS-based core networks. These OAM enhancements will allow service providers to have better visibility into their existing MPLS-based core networks, which will allow further optimization. The new OAM capabilities will also help the wholesale business by improving the tools required to measure and enforce strict SLAs. Juniper, therefore, is prioritizing the implementation of these OAM enhancements, such as the enhancements to BFD and LSP ping. Figure 2 illustrates how IP/MPLS and MPLS-TP can be deployed together and are very complementary in nature.

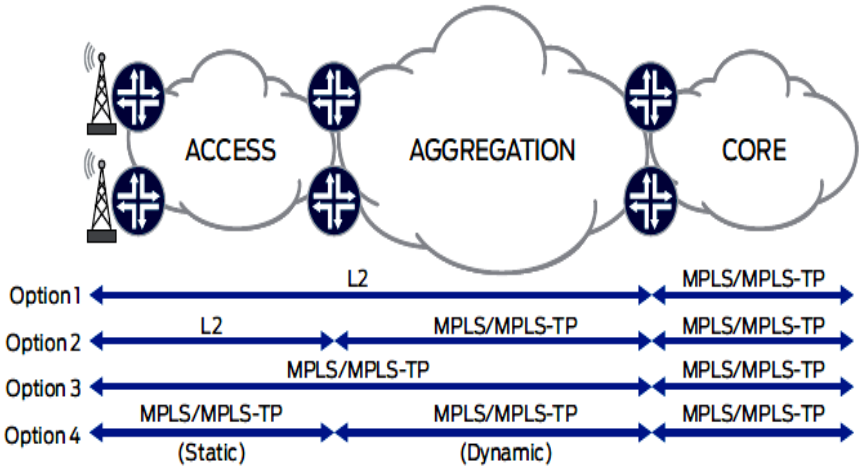


Figure 92: **MPLS and MPLS-TP Deployment Options**

Advantages of CPAN Technology:-

- Efficient bandwidth utilization,sharing bandwidth between services
- Includes the benefits of RPR.
- SDH packet switching based on statistical multiplexing.
- Path protection & recovery within 50 ms for any topology-Ring,Linear
- Support for TDM interfaces(E1,STM-1) & Multiservice traffic
- Both UNI & NNI interface upto max 100G capacity
- Access to last mile connectivity bandwidth upto 100G capacity.
- .bandwidth scalability -from 5G,40G to 100G
- OAM & Performance Monitoring-Proactive & Reactive
- Resiliency-1:1,1+1;Linear & Ring.
- GUI EMS provisioning.

15.8 BSNL NETWORK EVOLUTION

It is seen that BSNL requires immediate introduction of Packet Transport Network in order to provide reliable connectivity to the additional network elements and to meet the exponential growth in IP traffic. MPLS-TP enabled nodes with different configurations (as per the network requirement) maybe planned for transportation requirements in place of STM-1,16, 64 MADMs etc. where ever transport of packets is required. There is provision of carrying STM1 and E1 also in such devices.

15.8.1 Features:-

1. As these equipments are going to be used in place of SDH/TDM devices , which will be capable of servicing both TDM as well as packet (FE,GE etc.) clients, we need to have functionality similar to them and at the same time inefficiency of utilization of available bandwidth is to be minimized Hence for

the user it should look like a SDH equipment. OAM (operation administration and maintenance) like SDH are available in these equipment. Some of them are:-

- Point to point circuits can be provisioned.
- The devices can be connected in ring /mesh.
- End to end monitoring of each circuit is possible.
- Protection 1 : 1(PW) or even 1 :n(LSP) can be provisioned.
- It can transport synchronization information.

2. As switching in these devices are packet based ,it has features of packet based devices also. Some of these are:-

- Point to multipoint or multipoint to multipoint circuits can be created.
- Services can be provisioned at L1 or L2 layer.
- QoS can be defined for individual customers.

15.8.2 Proposed Configuration Of Nodes:-

Type-Al: (DC Powered Type)

Uplink	1GE (optical) -	2
Downlink	FE-4	
	FX-4	
	GE-2(Electrical)	
	STM1-2	
	E1-8	

Cross Connect Capacity - Minimum 5Gbps

Type-A2: (AC Powered Type)

Uplink	-	1GE	(optical) -	2
Downlink	-			FE-4
	FX-4			
	GE-2(Electrical)			
	STM1-2			
	E1-8			

Cross Connect Capacity - Minimum 5Gbps

Type-B1:

Uplink - 10 GE(optical)- 2
Downlink - 1GE-16 (8Electrical+8 optical)
FE -16
FX -16

STM1-8
E1 -64

Cross Connect Capacity- 40 Gbps

Type-B2:

Uplink 10GE(optical)-2
Downlink 10GE (optical) – 2

GE-32(16 Electrical + 16 Optical)

FE-16

FX-16

STM1-8

E1-64

Cross connect capacity- 80 Gbps

Type C:

Uplink 40 GE(optical)-2

Downlink 10GE(optical)-12

FE/GE—64(32 optical + 32 electrical)

(10/100/1000)

STM 1-8

E1-64

Cross connect capacity— 240 Gbps

(Uplink- Line side,Downlink-Traffic side)

DISTANCE BETWEEN TWO NODES:-

Type Al/A2	-	30 Km.
TypeBl/B2	-	50 Km.
Type C	-	50 Km.

POWER SUPPLY:-

Type Al /A2- AC Type or DC Type.

Type Bl /B2- DC Type.

Type C- DC Type.

15.9 TYPICAL NETWORK TOPOLOGY FOR MPLS-TP NODES

- Co-located network elements connected directly while the traffic betweennon co-located ones is transported through a packet transport network.
- Nodes to comply to the MPLS TP standards for OAM, Protection, Architecture, Synchronization etc.
- There will be minimum TDM interface and the existing infrastructure of SDH/DWDM will cater to the existing TDM traffic of BSNL where ever possible.
- Lower type nodes can be directly terminated on the interfaces of the higher level nodes i.e. I GE Uplink of Type-A node can be terminated on the I GE interface of Type-B nodes similarly 10GE Uplinks of Type-B node can be terminated on 10GE interface of Type-C nodes.
- Type-A,B& C shall have control card, switching fabric and power supply redundancy while Type-A will have only power supply redundancy.
- Exchange of traffic with MPLS will be through PE Routers on UNI interface at multiple points of connectivity.

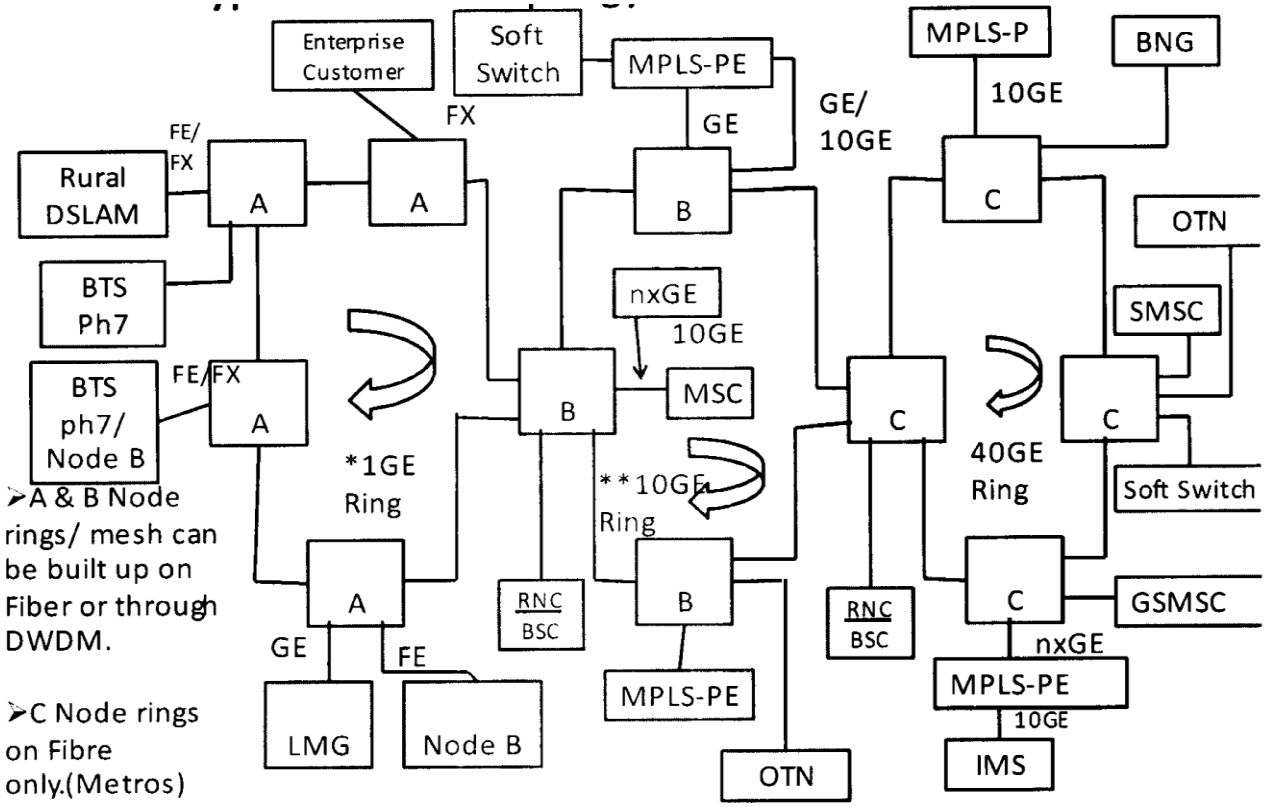


Figure 93: **Typical Network Topology for MPLS-TP Nodes**

The planned A,B & C Nodes will perform the function of transport &aggregation of traffic from all access points such as HTS, Node Bs, RNCs, MSCs, MPLS-PE Routers, FTTH OLTs, DSLAMs etc. All the traffic aggregation in major cities with high traffic between POPS located within same city will be served by Type C nodes. Thus the functions presently being done by STM-I CPE, STM-1 ADM, STM-16 MADM and STM-64 will be done by MPLS-TP enabled packet transport nodes with configurations as shown above for all the future packet transport requirements. Number of nodes in a ring will depend on the amount of client traffic at each node.

Type A nodes can be very effectively used to replace present CPEs. Normally it will be used to give connectivity to standalone small capacity nodes like BTSs, consumers demanding higher BW, small capacity DSLAMs etc. In such cases they can be used in linear mode also.

15.10 CONCLUSION

MPLS-TP is a set of enhancements to the already rich MPLS protocol suite. The current MPLS suite has successfully served packet-based networks for more than a decade. The

MPLS-TP enhancements will increase the scope of MPLS overall, allowing it to serve both the transport and the services networks.

The biggest and most important enhancements that are being developed under the MPLS-TP effort are OAM related (e.g., fault management and performance monitoring). These OAM enhancements will prove to be very valuable for the existing MPLS networks, as they will allow operators to improve the efficiency and effectiveness of their networks by enabling full end-to-end integration with the existing and the next-generation MPLS networks.

16 WI-FI HOTSPOT, LAN, WAN

16.1 LEARNING OBJECTIVES

- Benefits and disadvantages of Wi-Fi
- Wi-Fi standards, Architecture
- Media access control
- Wi-Fi connections, Wi-Fi security
- LAN topologies, Wide area network (WAN)

16.2 INTRODUCTION

WiFi is the wireless way to handle networking. It is also known as 802.11 networking. The big advantage of WiFi is its simplicity.

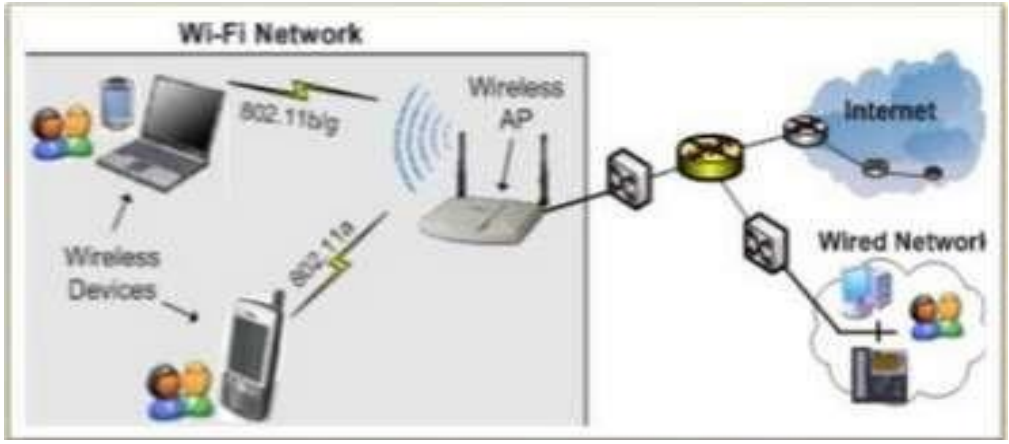


Figure 94: **Wi-Fi**

16.3 WIFI RANGE

You can connect computers anywhere in your home or office without the need for wires. The computers connect to the network using radio signals, and computers can be up to 100 feet or so a part.

Regardless of which setup you use, once you turn yourWireless Access Point on, you will have a WiFi hotspotin your house.In a typical home, this hotspot will provide coveragefor about 100 feet (30.5 meters) in all directions, although walls and floors do cut down on the range.

Even so, you should get good coverage throughout a typical home. For a large home, you can buy inexpensive signal boosters to increase the range of theHotspot.

16.4 ADDING WI-FI TO YOUR COMPUTER

- Many new laptops already come with a WiFi card built
- It is also easy to add a WiFi card to a laptop or a desktop PC.
- Buy a suitable standard network card.
- For a laptop, this card is a PCMCIA
- For a desktop machine, buy a PCI card or USB type
- Install the driver

Figure 95: **Wifi components**

16.5 BENEFITS & DISADVANTAGES

16.5.1 Benefits Of Wi-Fi

- Mobility
- Compatibility with IP networks
- High speed data
- Unlicenced frequencies
- Security
- Easy and fast installation
- Scalability
- Low cost

16.5.2 Disadvantages Of Wi-Fi

- Generates radiations which can harm the human health
- We must disconnect the Wi-Fi connection whenever not using
- Not very long distance communication
- Compared to wired connection, still costly

16.6 WI-FI STANDARDS

- Standards are mutually agreed upon rules adopted by the industry on how the wireless networks operate.
- The core protocols are listed in the 802.11 standards, which was originally available in 1997
- There are a couple of standards that describe Wi-Fi. All of them are part of the 802.11 suite.

16.6.1 IEEE 802.11 Suite

Network standard	Maximum Speed (Mbps)	Range (feet)	Frequency (GHz)	Power drain	Cost
802.11b	11	100-150	2.4	Moderate	Low
802.11a	54	60-100	5	High	High
802.11g	54	150-250	2.4	Moderate	Moderate
802.11n	200	Up to 300 feet	2.4 & 5	Moderate	Moderate

Figure 96: **IEEE 802.11 suite**

WiFi radios that work with the 802.11b and 802.11g standards transmit at 2.4 GHz, while those that complywith the 802.11a standard transmit at 5 GHz.Normal walkie-talkies normally operate at 49 MHz. Thehigher frequency allows higher data rates

WiFi radios use much more efficient coding techniques (process of converting 0's and 1's into efficient radio signals) that also contribute to the much higher data rates.The radios used for WiFi have the ability to changefrequencies

For example, 802.11b cards can transmit directly on any of three bands, or they can split the available radio bandwidth into dozens of channels and **frequency hop** rapidly between them.The advantage of frequency hopping is that it is much more immune to interference and can allow dozens of WiFi cards to talk simultaneously withoutinterfering with each other.

802.11b: First to reach the marketplace. It is the slowest and least expensive of the three. 802.11b transmits at 2.4 GHz and go up to 11Mbps.
802.11a: Was next. It operates at 5 GHz and can handle up to 54 Mbps.
802.11g: Mix of both worlds b & g. It operates at 2.4Ghz (giving it thecost advantage of 802.11b) but it has the 54 megabits per second speed of 802.11a. It is also backward compatible to 802.11b.
802.11ac : Backward compatible with 802.11n & its predecessors, maximum of 450 megabits per second on a single stream, sometimes called **5G WiFi** because of its frequency band, sometimes **Gigabit WiFi** because of its potential to exceed a gigabit per second on multiple streams

16.7 WI-FI BACKGROUND

1990 : 802.11 development started by IEEE

The aim was to develop a standards for medium access control (MAC) and physical layer (PHY)

1997 : First version of 802.11 standard was ratified

First version delivered 1Mb/s and 2Mb/s data rates

1999 : 802.11a and 802.11b amendments were released Data rates improved to 5.5Mb/s and 11Mb/s at 2.4GHz (802.11) Wired EquivalentPrivace (WEP) introduced 5GHz operation with OFDM modulation at 54Mb/s (802.11a)

2001 : FCC approved the use of OFDM at 2.4GHz

2003 : OFDM modulation at 54Mb/s at 2.4GHz (802.11g)

2009 : 801.11n amendment were ratified

- PHY relies heavily on multiple-input multiple-output (MIMO) technology
- Can use both 2.4Ghz and 5Ghz at the same time
- Throughput increased even up to 600Mbps

2009 : Bluetooth 3.0 + HS

802.11 selected as the Bluetooth high speed channel

2009 : Wi-Fi direct specification introduced

2011 : 802.11ac development started

More throughput with wider bandwith, more MIMO streams and wider
256-QAM modulation. Provides 500-1000Mbps throughput

16.8 802.11 ARCHITECTURE

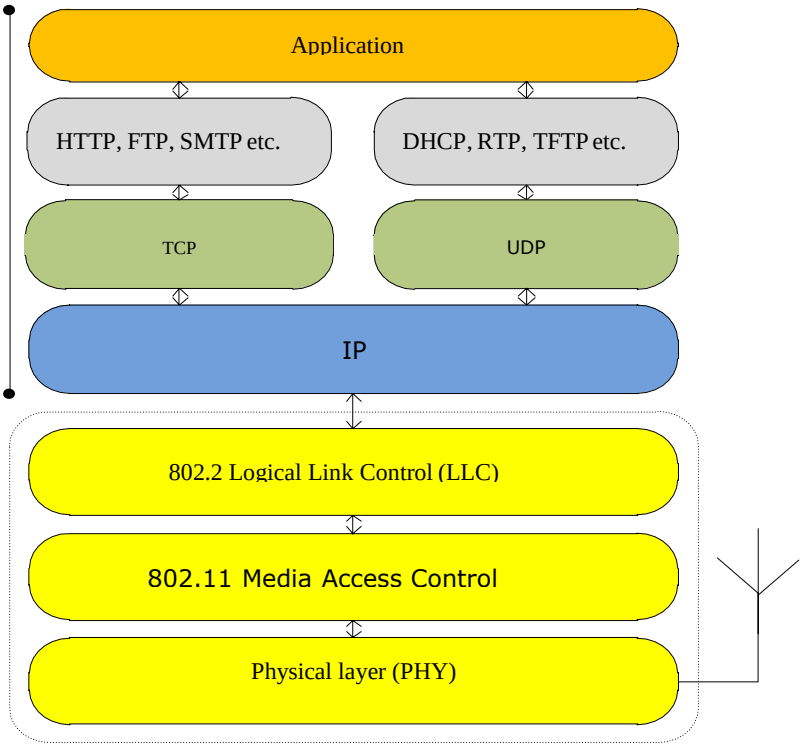


Figure 97: **802.11 architecture**

16.8.1 Physical Layer

2.4 GHz and/or 5GHz transceiver Industrial Scientific Medical (ISM) bandLicense free

Spread spectrum technology

- FHSS, DSSS and OFDM modulations

FHSS (Frequency Hopping Spread Spectrum)

- Bandwidth divided into 75 1MHz channels
- Data throughput limited to 2Mbps because of hopping overhead and FCCregulations (1 MHz channel bandwidth)

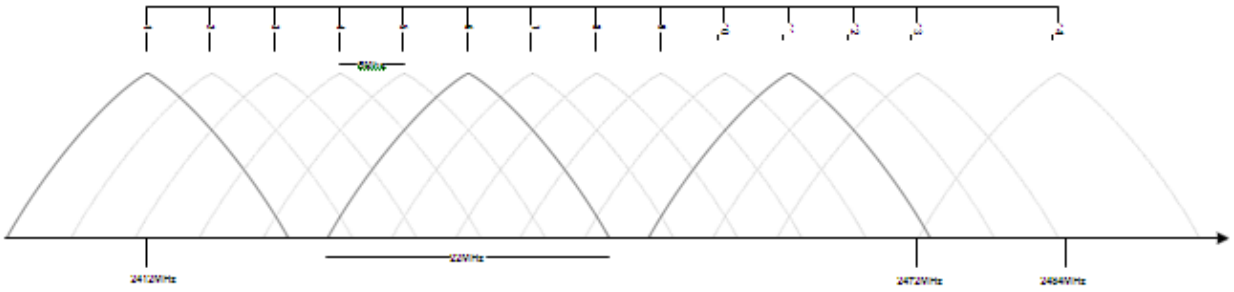
DSSS (Direct Sequence Spread Spectrum)

- Bandwidth divided into 14 22MHz channels overlap partially

OFDM (Orthogonal Frequency-Division Multiplexing)

- 20 or 40MHz bandwidth

Uses several non-overlapping channels overlap partially



Europe : channels 1-13
USA : channels 1-11
Japan : channels 1-14

Figure 98: **Wi-Fi Physical Layer Channels**

Standard	Frequency	Bandwidth (MHz)	Symbol rate (Mb/s)	MIMO streams	Modulation
802.11	2.4GHz	20	1, 2	1	DSSS, FHSS
802.11a	5Ghz	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM
802.11b	2.4GHz	20	5.5,11	1	DSSS
802.11g	2.4GHz	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS
802.11n	2.4/5GHz	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM
		40	15, 30, 34, 60, 90, 120, 135, 150		

Figure 99: **Comparison of various standards**

16.8.2 802.11 Media Access Control (MAC)

- Manages and maintains communications between 802.11 stations and clients
- Coordinates access to shared radio channels Uses CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) algorithm to access the media

- Similar to Bluetooth Link Layer
- Because of the shared media operation, all Wi-Fi networksare half duplex.
- All Wi-Fi networks are contention-based TDD systems, where the access point and the mobile stations all vie foruse of the same channel.
- There are equipment vendors who market Wi-Fi mesh configurations, but those implementations incorporatetechnologies that are not defined in the standards.

Function	**Explanation**
Scanning	Scanning of access points. Both active (probe) and passive (beacon) scanning are provided by the standard.
Authentication	Authentication is the process of proving identity between the client and the access point.
Association	Once authenticated, the client must associate with the access point before sending dataframes.
Encryption	Encryption of payload
RTS/CTS	The optional request-to send and clear-to-send (RTS/CTS) function allows the access point to control use ofthe medium for stations activating RTS/CTS.
Power Save Mode	The power save mode enables the user to turn on or off enables theradio.
Fragmentation	The fragmentation function enables an 802.11 station to divide data packets into smaller frames.

16.9 LOGICAL LINK CONTROL (LLC)

The LLC provides end-to-end link control over 802.11-based wireless LAN

LLC services:

Unacknowledged connectionless service

- Higher layers must take care of error and flow control mechanisms
- Peer-to-peer, multicast and broadcast communication

Connection-oriented service

- Error and flow control
- Peer-to-peer communication

Acknowledged connectionless service

- Flow and error control with stop-and wait ARQ
- Peer-to-peer, multicast and broadcast communication

16.10 WI-FI CONNECTIONS

- Connection (Logical) is the mutual agreement between two ports to have a communication.
- Wi-Fi networks can be of BSS and ESS types
- Two Wi-Fi devices can have mainly two types ofconnections.
    - Ad-hoc connection (Peer-to-Peer connection)
    - Infrastructure connection (AP Connection)

16.10.1 Ad-Hoc Mode

- Essentially a peer-to-peer(also called work group) model.

- Ad Hoc connections can be used to share information directlybetween devices. This mode is also useful for establishing a network where wireless infrastructure does not exist.

Some uses,

- Synchronize data between devices.
- Retrieve multimedia files from one device and "play" them onanother device.
- Print from a computer to a printer without wires.

There are many applications of ad hoc networking in the military and inspecialized networks

16.10.2 Infrastructure Mode

- Essentially a Client/Server model
- Infrastructure mode connection can be used to share information from one Wi-Fi client to AP.

Many Wi-Fi clients can access an AP at a time

- Normally used to access internet.

16.10.3 Basic Service Set (BSS)

- A set of stations controlled by a single "Coordination Function"
- Typically uses an Access Point (AP)
- All mobile stations must be accessible by theaccess point of the infrastructure BSS
- In the infrastructure network, stations must associate with the access point in order to getaccess to network services

16.10.4 Independent Basic Service Set (IBSS)

- A BSS without an Access-Point is basically ad-hoc networking

16.10.5 Extended Service Set (ESS)

- A set of one or more Basic Service Setsinterconnected by a Distribution System(DS)
- Traffic always flows via Access-Point

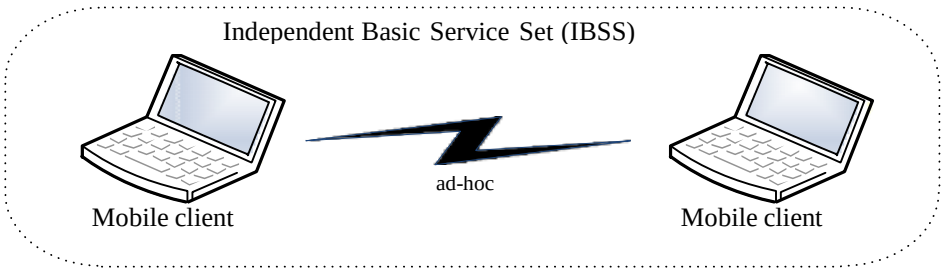


Figure 100: **ESS**

16.10.6 Distribution System (DS):

- A system to interconnect two or more BSS
- Typically wired Ethernet
- Could be also wireless like 802.11, WiMax,3G/4G etc.

AP – client services:

Authentication/ De-authentication: open, shared key or WPS

Privacy : WEP, WPA or WPA2

Distribution System services:

- Association: maps the client into the distribution system via access point
- Disassociation: release of association
- Distribution: used to deliver MAC frames across the distribution system
- Integration: enables delivery of MAC frames between DS and non 802.11
- Re-association: transition of association from one access point to an other

16.11 WI-FI SECURITY

- Wi-Fi hotspots can be open or secure.
- If a hotspot is open, then anyone with aWi-Fi card can access the hotspot.
- If it is secure, then the user needs to know a Security key

16.11.1 Wi-Fi Security Features

The 802.11 provides the following security features

- **Association -** Client needs to associate with the Access Point
- **Authentication-** Authentication is either open, shared key or WPS
- **Access control (MAC Filter)-** Access Point can decide which clients are allowed to associate based on MAC address Trivial to spoof MAC address.

16.11.2 Wi-Fi Security Types

1. **Encryption**

- Wired Equivalent Privacy (WEP)
- Wireless Protected Access (WPA)
- Wireless Protected Access 2 (WPA2)

2. **Data integrity**

- Data can not be modified on-the-fly. Quarantined by Encryption

3. **Data confidentiality**

- No eavesdropping with decryption of data. Quarantined by encryption.

16.11.3 WEP (Wired Equivalent Privacy)

- This encryption standard was the original encryption standard forwireless.
- Security issues known since 2001, can be cracked in <1minute
- WEP has two variations: 64-bit encryption and 128-bit encryption
- 64-bit encryption was the original standard but was found to be easily broken.
- 128-bit encryption is more secure and is what most people use if they enable WEP.
- For a casual user, any hotspot that is using WEP is inaccessible unless you know this WEP key.

16.11.4 WPA (Wi-Fi Protected Access)

- WPA is the successor to WEP
- WPA uses TKIP for encryption, some routers also support AES.
- Security issues known since 2008 in TKIP, considered insecure
- Latest version of WPA is WPA2 (Uses TKIP or AES)

16.11.5 Wireless Protected Access 2 (WPA2)

- WPA2 is a Wi-Fi Alliance branded version of the final 802.11i standard.
- The primary enhancement over WPA is the inclusion of the AES- algorithm as a mandatory feature.
- The CCMP/AES algorithm is considered secure, given a good enough password
- WPA2 Personal (WPA2-PSK): Uses a password, common.
- WPA2 Enterprise (WPA2-RADIUS): Certificates on server

Note: Wi-Fi Alliance will mandate Wi-Fi CERTIFIED products only to support WPA2 AES

16.12 SETTING UP WI-FI HOTSPOT AT HOME

If you already have several computers hooked together on an Ethernet network and want to add a wireless hotspot to the mix, you can purchase a **Wireless Access Point** and plug it into the Ethernet network.

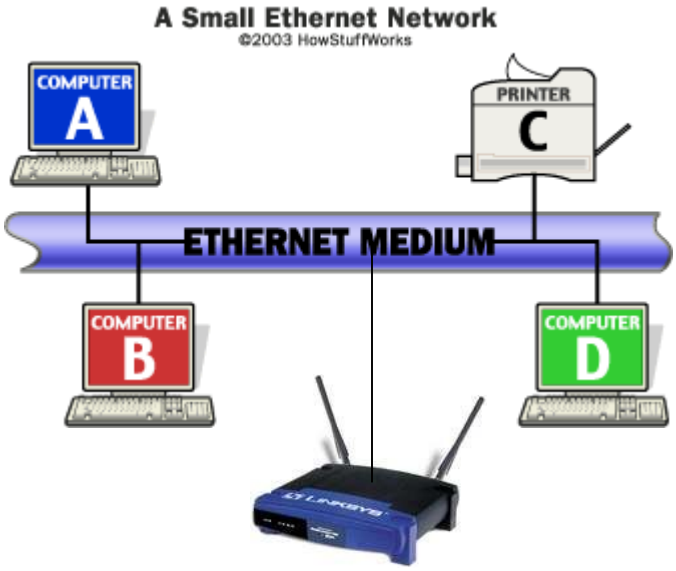


Figure 101: **Wireless Access PoinT**

16.13 DIFFERENT TYPES OF IPROUTING

Setup #1

Alternate Setup using a Wireless Router

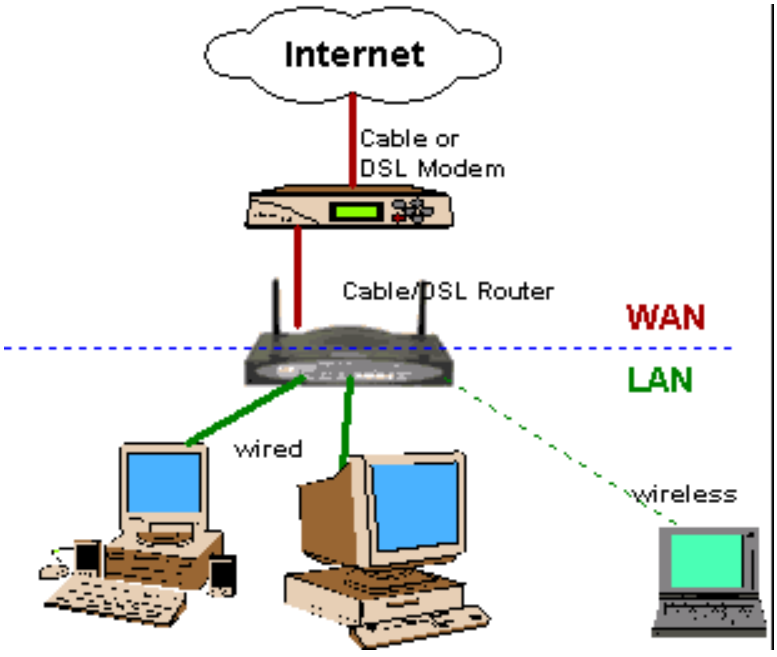


Figure 102: **Alternate Setup using a Wireless Router**

If you are setting up a network in your home for the first time, or if you are upgrading, you can buy a Wireless Access Point Router. This is a single box that contains:

- a port to connect to your cable modem or DSL modem,
- a router,
- an Ethernet hub,
- a firewall and
- a wireless access point.

You can connect the computers in your home to this boxeither with traditional Ethernet cables with wireless cards.

16.14 CONFIGURING A HOTSPOT

- Most wireless access points come with default values built-in.
- Once you plug them in, they start working with these default values.
- However, you may want to change things.
- You normally get to set three things on your access point.

16.14.1 Things To Configure In A Hotspot

- The SSID -- Service Set IDentifier is a sequence of characters that uniquely names a WLAN.
- The channel – the radio link used by access point/router to communicate to wireless devices. Normally it will default to channel 6.
- However, if a nearby neighbor is also using an access pointand it is set to channel 6, there can be interference. Chooseany other channel between 1 and 11.
- The WEP or WPA key – Normally select WPA
- Access points come with simple instructions for changing these three values. Normally you do it with a Web browser. Once it is configured properly, you can use your new hotspot to accessthe Internet from anywhere in your home.

- Additionally you can configure ACL (MAC Filter)

16.15 LAN, MAN AND WAN NETWORKS

16.15.1 Different Types Of Networks

Depending upon the geographical area coveredby a network, it is classified as:

A. Local Area Network (LAN)

B. Metropolitan Area Network (MAN)

C. Wide Area Network (WAN)

D. Personal Area Network (PAN)

16.15.2 A Local Area Network (LAN)

- A LAN is a network that is used for communicating among computer devices, usually within an office building or home.
- LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users
- Is limited in size, typically spanning a few hundred meters,and no more than a mile
- Is fast, with speeds from 10 Mbps to 10 Gbps
- Requires little wiring, typically a single cable connecting to each device
- Has lower cost compared to MAN's or WAN's
- LAN's can be either wired or wireless. Twisted pair, coax or fiber optic cable can be used in wired LAN's.
- Every LAN uses a protocol – a set of rules that governshow packets are configured and transmitted.
- Nodes in a LAN are linked together with a certain topology. These topologies include:

i. Bus,

ii. Star

iii. Ring

iv. Mesh

v. Hybrid

vi. Tree

Some common LAN technologies include the following:

- Ethernet
- Token Ring
- FDDI
- LANs are capable of very high transmission rates (100sMb/s to Gb/s)

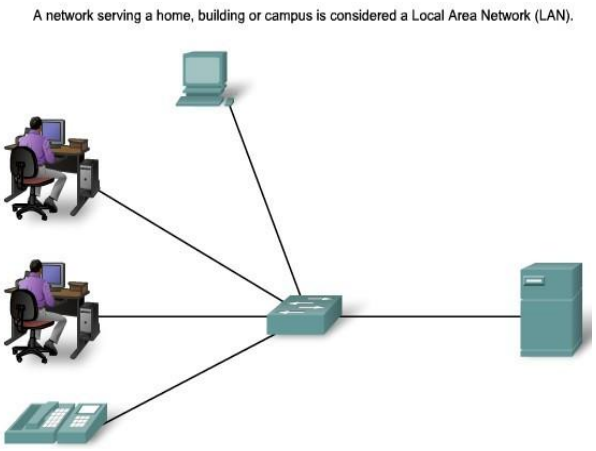


Figure 103: **A SIMPLE LAN**

LAN TOPOLOGIES

16.15.3 Bus Topology

Bus topology is a network type in which every computer and network device is connected to single cable

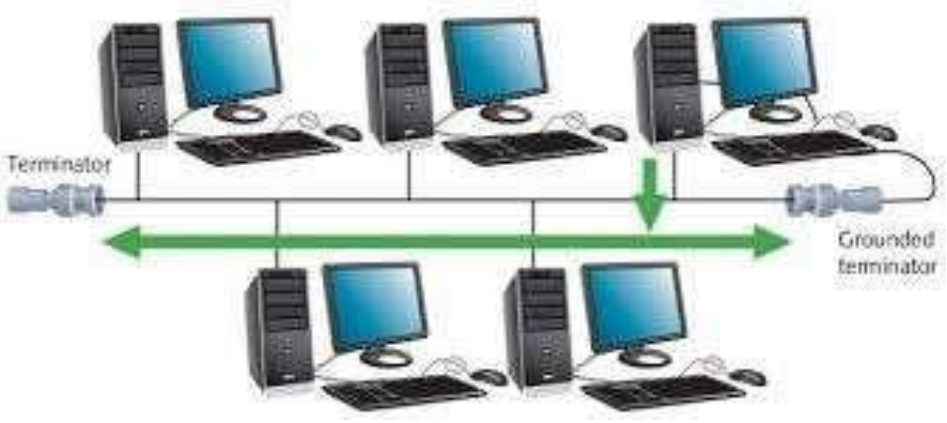


Figure 104: **Bus Topology**

Advantages of Bus Topology

- It is cost effective.
- It is simple to install and modify.
- Cable required is least compared to othernetwork topologies.
- Easy to expand joining two cables together

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- Broadcasts the data traffic thereby speed is less.
- If network traffic is heavy or nodes are more theperformance of the network decreases.
- Cable has a limited length.
- The end points of Cable (which is used as a bus) should be connected to high impedance to avoid signal reflection and hence further loss of data.
- Troubleshooting is difficult in bus topology.

16.15.4 Star Topology

In this topology all the computers are connected to a single switch through a cable. This switch is the central node and all others nodes areconnected to the central node.

Figure 105: **Star topology**

Advantages of Star Topology

- Easy to setup and modify.
- Easy to troubleshoot.
- Switch can be upgraded easily.
- Only that node is affected which has failed, rest of the nodes can work smoothly.
- Division of LAN into logical segments is possible, if the manageable switch is used.

Disadvantages of Star Topology

- Cost of installation is high due to central switch.
- If the switch fails then the whole network activity is stopped because all the nodes depend on the switch.
- Network performance like speed and no. of nodes depends on the capacity of switch

16.15.5 Ring Topology

Ring topology is so called because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

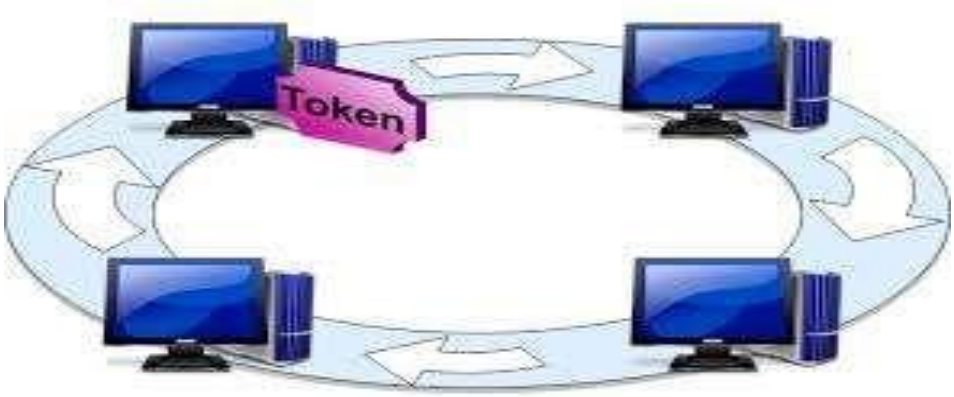


Figure 106: **Ring topology**

Advantages of Ring Topology

- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Data can transfer between workstations at high speeds.

Disadvantages of Ring Topology

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- Adding or deleting the computers disturbs the network activity.
- Troubleshooting is difficult in ring topology.

16.15.6 Mesh Topology

All the network nodes are connected to each other using dedicated links. It is a point-to-point connection to other nodes or devices. Mesh has n(n-1)/2 physical channels to link n devices.

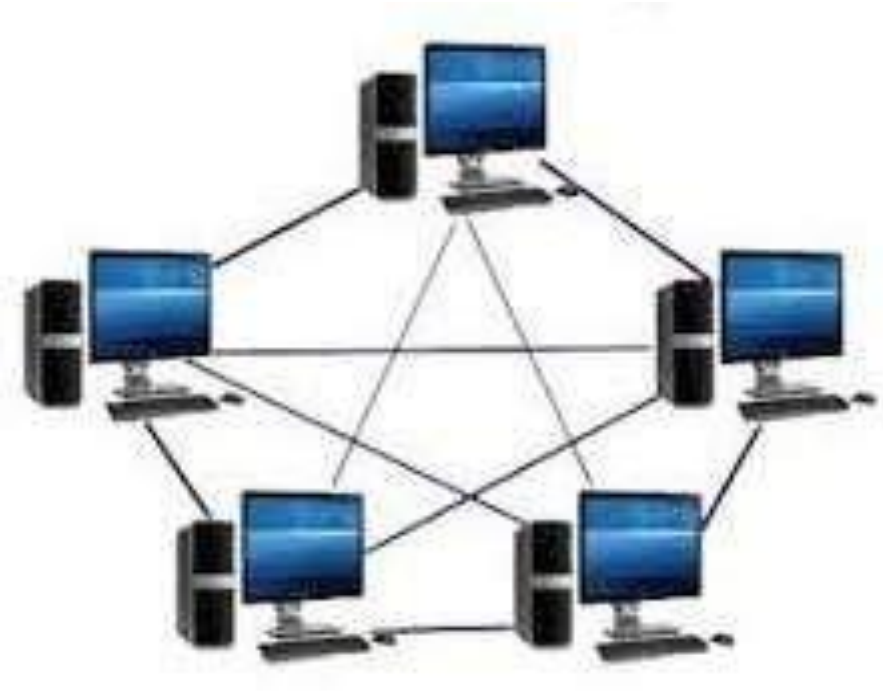


Figure 107: **Mesh topology**

Advantages of Mesh Topology

- Each connection can carry its own data load. There is no traffic problem as there are dedicated point to point links for each computer.
- It is robust. It has multiple links, so if one route is blocked then other can be accessed for data communication.
- Fault is diagnosed easily because of point-to-point connection.
- Provides security and privacy communication sessions. Disadvantages of Mesh topology
- Installation and configuration is difficult.
- Cabling cost is more. It also requires more I/O ports forcommunication.
- Bulk wiring is required.

16.15.7 Hybrid Topology

- It is combination of two or more different types of topologies.
- For example if in an office in one department ring topology is used and in another

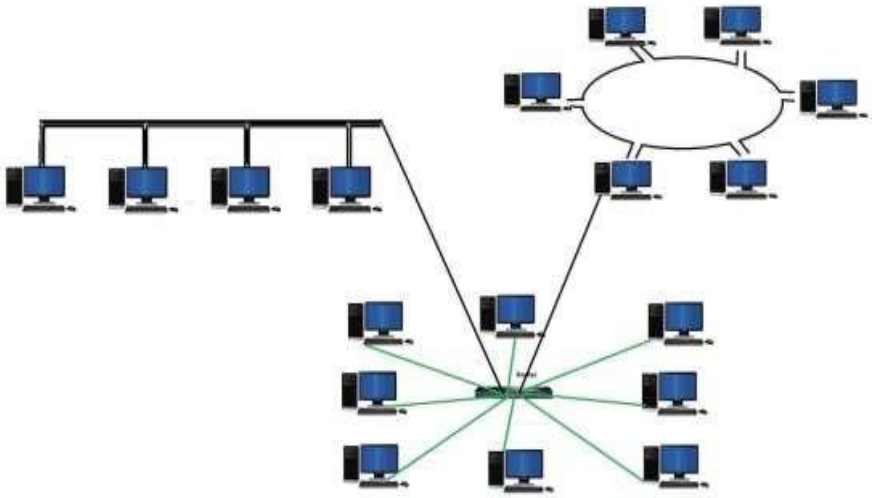


Figure 108: **Hybrid Topology**

star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

16.15.8 Tree Topology

It has a root node and all other nodes are connected to it forming a hierarchy.It is also called hierarchical topology. It should at least have three levels to the hierarchy

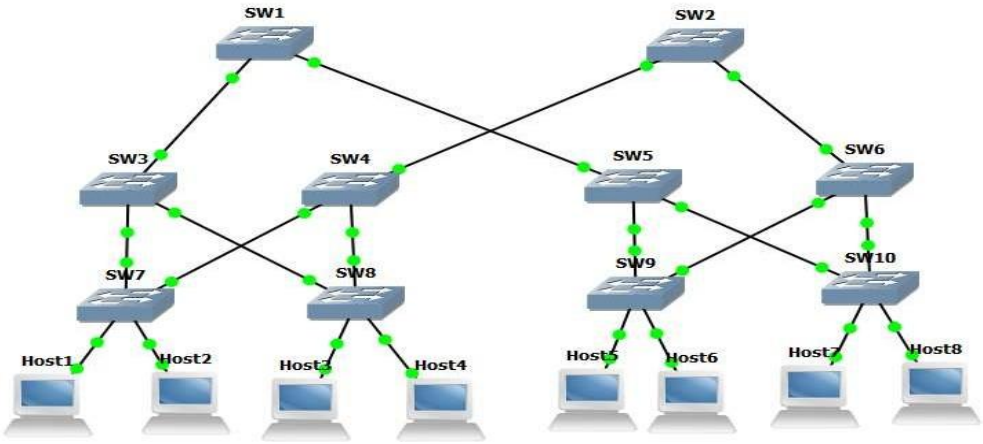


Figure 109: **Tree topology**

16.16 METROPOLITAN AREA NETWORK (MAN)

- A **metropolitan area network** (**MAN**) is a largecomputer network that usually spans a city or alarge campus.
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks ofbuildings to entire cities.
- A MAN might be owned and operated by a single organization, but it usually will be usedby many individuals and organizations.
- A MAN often acts as a high speed network toallow sharing of regional resources.
- A MAN typically covers an area of between 5and 50 km diameter.
- Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.

A MAN Network

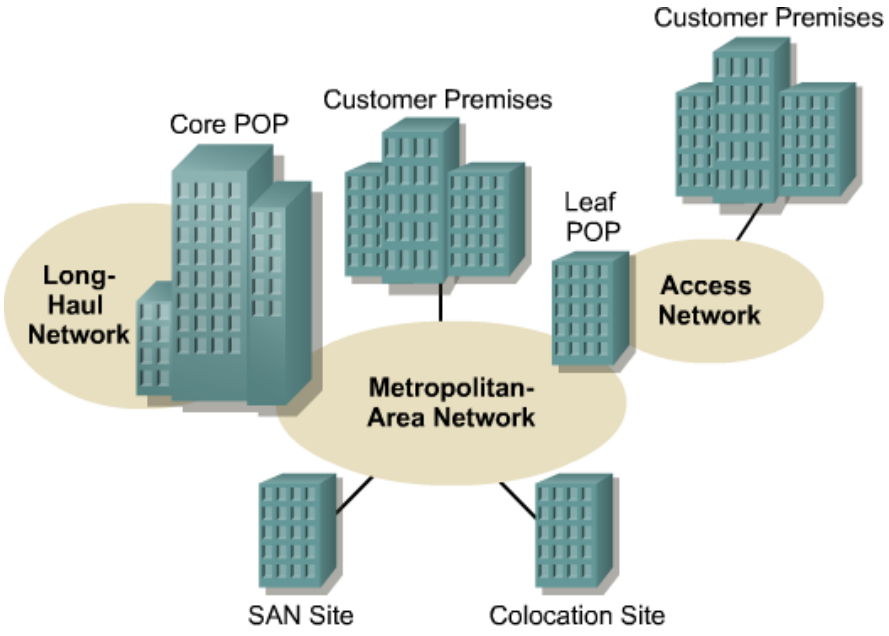


Figure 110: **A MAN network**

16.17 WIDE AREA NETWORK (WAN)

A network that spans broader geographical area than a local area network over public communication network. WANs interconnect LANs, which then provide access to computers or file servers in other locations. Because WANs connect user networks over a large geographical area, they make it possible for businesses to communicate across great distances. WANs allow computers, printers, and other devices on a LAN to be shared with distant locations. WANs provide instant communications across large geographic areas.

Collaboration software provides access to real-time information and resources and allows meetings to be held remotely. WANs have created a new class of workers called telecommuters. These people never have to leavetheir homes to go to work.

WANs are designed to do the following:

- Operate over a large and geographically separated area
- Allow users to have real-time communication capabilities with other users
- Provide full-time remote resources connected to local services
- Provide e-mail, Internet, file transfer, and e-commerce services

Some common WAN technologies include the following:

- Modems
- Integrated Services Digital Network (ISDN)
- Digital subscriber line (DSL)
- Frame Relay
- T1, E1, T3, and E3

➢ Synchronous Optical Network (SONET)

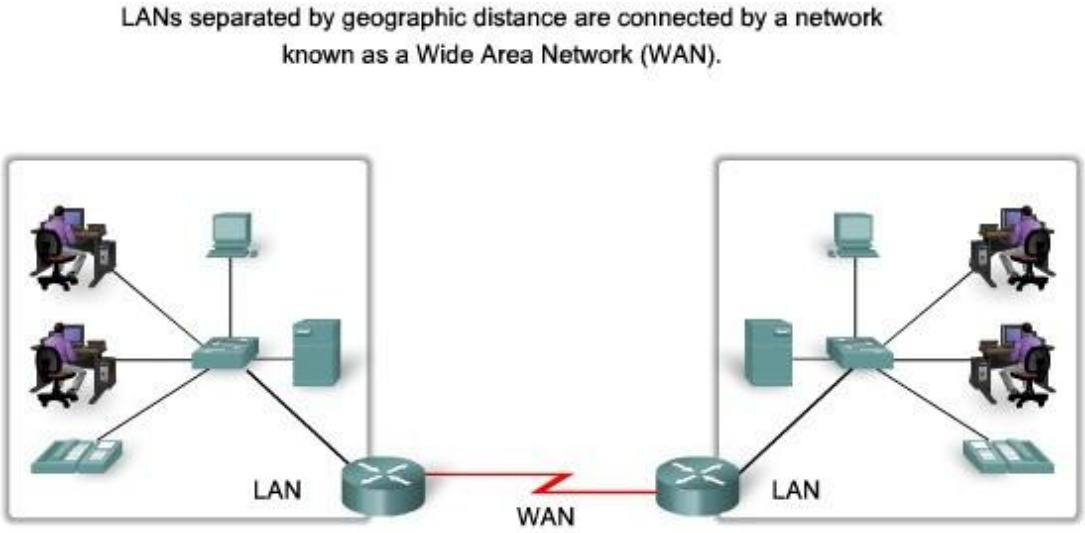


Figure 111: **LAN separated by geographic distance**

16.18 LAN VS WAN

LAN	**WAN**
Connects host within a relatively small geographical area. • Same Building • Same room • Same Campus	Hosts may be widely dispersed. • Across Campuses • Across Cities/countries/continent
Faster	Comparatively Slower
Cheaper	Expensive
Under the control of single ownership.	Not under the control of a single ownership.

Table 5. LAN vs WAN

16.19 CONCLUSION

Different types of networks can be created based on geographical coverage like LAN, MAN and WAN. Each of this network have its own importance as they have their own area of coverage to serve and hence the type of components they support. Wired connectivity gives promising speed but is complicated as use of cables and hence their management is required to maintain LAN whereas WIFI speed may be affected by interference but seems to very simple and does not requirement management of links.